МИК review

УВИДЕТЬ И ОТЛИЧИТЬ: система распознавания объектов IBM PowerAI Vision

ОБЛЕГЧАЕМ ЖИЗНЬ: новые варианты подписки и удобные инструменты для облачных сервисов Microsoft

КУРС НА АВТОМАТИЗАЦИЮ: CISCO SD-WAN

ЭФФЕКТИВНАЯ ИНФРАСТРУКТУРА: DELL EMC POWEREDGE MX

ТАТЬЯНА БОЧАРНИКОВА:

«Наши самые успешные партнеры – те, которые, используя продукты и решения NetApp, предлагают собственные сервисы»

Microsoft 365 –

комплексное интеллектуальное решение для современного безопасного рабочего места

О группе компаний МУК

Группа компаний МУК начала свою деятельность в мае 1997 года. Основное направление деятельности МУК — дистрибуция комплексных решений и оборудования ведущих мировых производителей в сфере информационных технологий.

Группа компаний МУК предоставляет комплекс дополнительных услуг для своих дилеров, что позволяет говорить о ней как об уникальном дистрибуторе, развивающем модель Value Added Distribution (VAD) и осуществляющем продажи через дилерскую сеть в Беларуси, Молдове, Украине, странах Кавказа и Центральной Азии.

Постоянно расширяющееся портфолио компании включает контракты с более чем 50 мировыми брендами А-класса, среди которых — производители компьютерной техники, активного и пассивного сетевого оборудования, систем бесперебойного питания, а также разработчики программного обеспечения для построения ИТ-инфраструктуры любого масштаба и сложности.

Бизнес-направления группы компаний МУК

***Дистрибуция*:**

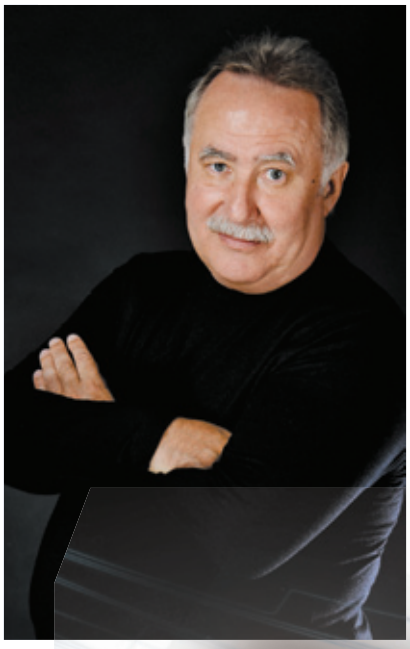
- проектная: серверы, системы хранения данных, сетевое оборудование, связь и телефония, защита данных, инфраструктурные решения;
- программное обеспечение;
- коробочная: ноутбуки, КПК, электронные книги, графические станции, ИБП, периферия, мониторы, принтеры, сканеры.

Учебный центр:

Авторизированные курсы на территории Беларуси, Украины, стран Кавказа и Центральной Азии от ведущих мировых производителей ИТ-индустрии, а также множество авторских курсов по заказу партнеров и заказчиков.

Сервисный центр:

Ремонт, настройка и модернизация ноутбуков, серверов, КПК, электронных книг, продажа и заказ комплектующих, обеспечение беспрерывности работы оборудования, расширенный гарантийный сервис.



УВАЖАЕМЫЕ ПАРТНЕРЫ!

В наше время внедрение новых технологий происходит настолько стремительно, что порой мы не успеваем осознавать всю масштабность изменений, происходящих вокруг. То, что еще вчера казалось невозможным, сегодня является обычным атрибутом повседневной жизни и воспринимается как нечто само собой разумеющееся.

Одним из ярких примеров таких технологий является искусственный интеллект. Казалось бы, только недавно сошедший со страниц романов Хайнлайна, Азимова, Лема и других признанных мастеров жанра научной фантастики, он постепенно приникает во все сферы жизни, попутно рождая мифы – например, о том, что искусственный интеллект заменит людей и оставит их без работы, что однажды машины восстанут против людей, и другие подобного рода заблуждения. Конечно, нельзя сказать, что мы сталкиваемся с ИИ на каждом углу, тем не менее, он уже достаточно широко используется многими производителями. В новом выпуске MUK Review вы узнаете о том, как искусственный интеллект успешно применяется в различных отраслях – в производстве, медицине, ретейле, финансовых и государственных учреждениях, телекоммуникационных компаниях и т. д., а также используется для обнаружения и распознавания объектов.

Помимо этого в номере вас ожидают обзоры новинок в сфере ИТ – технологии умной сети Cisco SD-WAN, модульной инфраструктуры Dell EMC PowerEdge MX, автономной базы данных Oracle Autonomous Database и ее новых возможностей, а также знакомство с Autodesk BIM 360 и другие, не менее интересные публикации.

#Читайте_с_пользой_MUKReview

С уважением,
И. И. Переверзев,
президент группы компаний МУК

Актуально

Крупным планом

Искусственный интеллект

Обзоры решений

Регионы присутствия МУК

АКТУАЛЬНО:

На волне инноваций

Группа компаний МУК и компания Lenovo, ведущий мировой производитель рабочих станций и мобильных интернет-устройств, расширили свое сотрудничество в Украине и подписали дистрибуторское соглашение на территории Армении и Грузии.

Согласно подписанному соглашению, МУК получает возможность поставок на рынок продуктов для корпоративных клиентов, малого и среднего бизнеса: настольных ПК (ThinkCentre и других серий) и рабочих станций, систем «все в одном», мониторов, линеек планшетов и ноутбуков (ThinkPad и т. д.), а также аксессуаров к ним.

Все решения Lenovo отличаются высокой производительностью, надежностью, простотой использования и наличием «зеленых» технологий.

МУК – дистрибутор PacketLight

Группа компаний МУК и компания PacketLight Networks, разработчик CWDM- и DWDM-решений для сетей хранения данных, ЦОД, передачи данных, голоса и видео, объявили о подписании дистрибуторского контракта на территории Азербайджана, Армении, Беларуси, Грузии, Казахстана, Кыргызстана, Молдовы, Монголии, Таджикистана, Туркменистана и Узбекистана. Портфель компании включает в себя продукты для построения высокоэффективной инфраструктуры метро-сетей C/DWDM, SDH и оптических сетей с использованием резервных каналов «темного волокна». Это набор решений операторского класса, характеризующихся высокой производительностью, удобством в работе и конкурентоспособной ценой. Устройства PacketLight отличаются универсальностью и могут применяться в составе WDM-инфраструктуры любой топологии: от сетей «точка-точка» до общегородских кольцевых сетей доступа операторского класса и линейных сетей с возможностью ввода/вывода. Продукты компании имеют применение в различных сферах – их используют операторы связи, сервис-провайдеры и строители оптоволоконных сетей, страховые и финансовые учреждения, организации правительственного и оборонного сектора, учебные заведения, железнодорожные, электроэнергетические, нефтяные и газовые компании.

В решениях PacketLight реализован ряд фирменных технологий компании. Так, технология грубого спектрального мультиплексирования Coarse Wavelength Division Multiplexing (CWDM) позволяет одновременно передавать несколько информационных каналов по одному оптическому волокну на разных несущих частотах. А WDM дает возможность наиболее эффективно использовать уже имеющуюся волоконную структуру без необходимости вложения средств в проект по созданию новой сети предприятия.

МУК расширяет сотрудничество с APC

Группа компаний МУК и компания APC by Schneider Electric, ведущий мировой производитель комплексных решений для ЦОД, подписали дистрибуторское соглашение на территории Беларуси, расширив таким образом сотрудничество, распространявшееся на Азербайджан, Грузию, Казахстан, Кыргызстан, Таджикистан, Туркменистан, Узбекистан и Украину.

Согласно договору, группа компаний МУК получает право на поставку в Беларусь всего спектра оборудования APC by Schneider Electric. Портфолио компании включает решения для защиты электропитания промышленного масштаба и для домашнего использования, кондиционеры, устройства для обеспечения безопасности и контроля условий окружающей среды серии NetBotz, аппаратурные стойки и шкафы NetShelter и аксессуары к ним, средства распределения питания внутри стойки, а также программное обеспечение для управления этими решениями. Кроме того, ассортимент продуктов APC содержит сборные модули для центров обработки данных. Среди них – силовые модули, модули охлаждения, а также ИТ-модули, представляющие собой простую в развертывании масштабируемую ИТ-инфраструктуру с изменяемой конфигурацией, оптимизированную для поставщиков услуг и крупных предприятий. Таким образом, портфель компании пополнился решениями для ЦОД, позволяющими реализовать проект любого масштаба.

В помощь разработчику

Группа компаний МУК и компания Delphix, разработчик интеллектуальных программных платформ для виртуализации баз данных, объявили о начале сотрудничества на территории Азербайджана, Армении, Беларуси, Грузии, Казахстана, Кыргызстана, Молдовы, Таджикистана, Туркменистана, Узбекистана и Украины.

Ключевым продуктом портфеля Delphix является платформа для виртуализации баз данных Delphix Data Platform. Решение обеспечивает гибкое управление данными путем виртуализации на уровне баз данных. Delphix Data Platform позволяет добиться повышения эффективности в процессах резервного копирования и восстановления данных после сбоя, а также значительного ускорения процесса разработки и тестирования ПО. Разработчики получают возможность создавать практически неограниченное количество виртуальных БД для более эффективной отладки и тестирования. Внедрение решения позволяет снизить совокупную стоимость владения инфраструктурой и ускорить процесс разработки информационных систем.

Платформа виртуализации баз данных Delphix используется целым рядом крупнейших международный компаний.

СОБЫТИЯ ИТ-РЫНКА

Властелин мобильных

Группа компаний МУК и компания Proget Software, разработчик программного обеспечения в области управления и защиты мобильных устройств, заключили дистрибуторский контракт на территории Азербайджана, Армении, Беларуси, Грузии, Казахстана, Кыргызстана, Молдовы, Монголии, Таджикистана, Туркменистана, Узбекистана и Украины. Флагманский продукт компании – платформа Proget, разработанная для управления парком мобильных устройств организации. Она позволяет администраторам активировать устройства в сети компании, централизованно устанавливать политики, программное обеспечение и обновления, а также обеспечивать их защиту.

Решение отличается интуитивно понятным интерфейсом. Proget работает с устройствами на базе iOS и Android OS, а также интегрировано с системой Samsung Knox.

Комплексная безопасность

Группа компаний МУК и компания Check Point Software Technologies, ведущий игрок рынка информационной безопасности, объявили о расширении сотрудничества в Азербайджане, Казахстане, Туркменистане и Украине и подписали дистрибуторский контракт на территории Грузии.

Компания Check Point обеспечивает своих клиентов самыми свежими данными о киберугрозах и защитой сетей с помощью интегрированной платформы межсетевого экрана нового поколения и ПО для защиты рабочих станций. Единая система управления упрощает обслуживание систем безопасности и снижает общую стоимость владения. Нужна ли вам защита нового поколения для дата-центра, корпорации, малого или среднего бизнеса, или домашнего офиса – у Check Point есть решение для вас.

Check Point предлагает всеобъемлющую систему безопасности сетей для защиты от новейших угроз. С ее помощью частные лица, компании и государственные организации могут работать в Интернете безопасно и без лишних ограничений. Также портфель компании предлагает защиту для виртуальных облачных сред – публичных, частных и гибридных. Продукты Check Point используются компаниями, входящими в первую сотню в списке Fortune. Файрвол нового поколения был удостоен ряда наиболее престижных наград в индустрии.

Поскольку неотъемлемой частью информационной безопасности являются люди – сотрудники организаций, важным компонентом продуктов Check Point является технология Check Point UserCheck. Она позволяет обучать пользователей политике информационной безопасности компании, объясняет риски и учит соблюдать правила.

Надежный Wi-Fi

Группа компаний МУК и компания EnGenius, производитель решений в области беспроводных коммуникаций и радиотехнологий, заключили дистрибуторское соглашение на территории Азербайджана, Армении, Беларуси, Грузии, Казахстана, Кыргызстана, Молдовы, Монголии, Таджикистана, Туркменистана, Узбекистана и Украины.

EnGenius разрабатывает коммуникационные решения высокопроизводительной беспроводной связи. В портфеле компании представлены решения для дома, малого и среднего бизнеса, а также корпоративных заказчиков. Они включают полную продуктовую линейку для всех беспроводных сред, в том числе внутренние и внешние точки доступа Wi-Fi, коммутаторы, контроллеры беспроводного доступа, ПО для управления и мониторинга, оборудование для городских mesh-сетей. Продукты EnGenius направлены на высокоскоростную передачу данных, для них характерны безопасность и простота использования. Это гибкие и универсальные решения с широкой функциональностью, отличающиеся высоким качеством и доступной стоимостью благодаря собственному производству.

Важной особенностью решений является то, что функционал контроллера беспроводного доступа встроен в коммутаторы и не требует лицензирования. ПО для мониторинга и управления прилагается к решению бесплатно.

A10 Networks – новый вендор МУК

Группа компаний МУК и компания A10 Networks, производитель решений в области оптимизации, балансировки и защиты приложений, подписали дистрибуторское соглашение на территории Азербайджана, Армении, Беларуси, Грузии, Казахстана, Кыргызстана, Молдовы, Таджикистана, Туркменистана и Узбекистана.

A10 Networks специализируется на решениях для балансировки трафика, оптимизации работы и обеспечения безопасности приложений для предприятий и операторов любого масштаба. Флагманом компании является линейка A10-Thunder и серия AX-контроллеров, обеспечивающих работу сетевых приложений. Оборудование этой серии внедрено у заказчиков по всему миру.

Платформы A10 предлагают решения для балансировки нагрузки, миграции IPv6 и виртуализации облачных вычислений. Линейка продуктов включает в себя продукты ADC для оптимизации работы приложений, CGN для трансляции IPv4/IPv6-адресов, TPS для обеспечения защиты от DDoS-атак и другие решения. Продукты A10 Networks отличаются высокими эффективностью, компактностью и уровнем энергосбережения, а также невысокими уровнем первичных затрат и стоимостью владения.

ТАТЬЯНА БОЧАРНИКОВА

Глава представительства NetApp в Беларуси, Молдове, России, Украине, странах Кавказа и Центральной Азии

Каким вы видите развитие компании и партнерской сети на таких рынках, как Беларусь, Молдова, Украина, страны Кавказа и Центральной Азии? Какие из этих регионов являются наиболее перспективными?

Фокусными странами, в которых бизнес NetApp развит наиболее всего, являются, безусловно, Украина, Казахстан и Беларусь. В этих регионах есть пул партнеров с компетенциями, опытом и желанием активно продвигать продукты и решения NetApp. Совместно с группой компаний МУК мы развиваем канал в Азербайджане, Грузии и Узбекистане. Также есть неплохая динамика в Кыргызстане. Так что больше всего ресурсов и усилий направляется туда, где можно получить отдачу, а также в те страны, в которых виден потенциал роста.

Расскажите про ваше видение цифровой трансформации бизнеса.

В наше время не мир меняет технологии, а наоборот – технологии, стремительно развиваясь, заставляют меняться мир вокруг нас. В любой отрасли лидируют компании, которые первыми применяют у себя новые решения и с их помощью создают максимальную выгоду для бизнеса. Цифровая трансформация позволяет находить новые точки соприкосновения с клиентами и потребителями, создавать возможности для роста бизнеса и оптимизировать деятельность. С новыми решениями компании становятся более конкурентоспособными и готовы не только к текущим вызовам, но и к тем, с которыми придется столкнуться в ближайшем будущем.

Главный двигатель трансформации – данные. Они же являются главным активом любой компании. И если раньше все данные находились внутри компании, то теперь неважно, где они хранятся. Гораздо важнее эффективно управлять ими, чтобы трансформировать их в выгоду для бизнеса. При этом цифровая трансформация затрагивает уже не только компании, ориентированные на конечных потребителей, но и те организации, клиентами которых является бизнес.

Какое место занимает NetApp в этом процессе – продукты, технологии и т. д.?

Цифровая трансформация позволяет переосмыслить способы взаимодействия людей, данных и процессов. Внедрение технологий цифровизации напрямую зависит от возможности ИТ-служб быстро реагировать на потребности бизнеса, не снижая эффективности и безопасности управления данными, обеспечивая ресурсами все большее количество пользователей. Справляться с такими задачами помогают технологии гибридного облака, позволяющие значительно расширить выбор ресурсов для хранения и управления данными в зависимости от их предназначения, объемов и требований к обработке. Стратегия и технологии NetApp Data Fabric предлагают заказчикам все необходимое, чтобы построить управление данными под их конкретные бизнес-задачи в любом облаке из единого окна управления. Портфель технологий Data Fabric включает в себя как on-premise решения, так и технологии построения частного облака и облачные сервисы для управления данными, доступные у всех ведущих гиперскейлеров.

Что, по вашему мнению, мешает цифровой трансформации компаний в этих странах?

В первую очередь, это состояние рынка ИТ в частности и экономики в целом. Проблемы развития мировой экономики в последние пять лет, несомненно, сказываются на развитии экономик этих стран. Существующие политические аспекты также влияют на развитие, и они очень разные в каждой отдельно взятой стране.

> «Цифровая трансформация позволяет компаниям находить новые точки соприкосновения с клиентами и потребителями, создавать возможности для роста бизнеса и оптимизировать свою деятельность»

«В наше время не мир меняет технологии, а технологии заставляют меняться мир вокруг нас»

Сегодня многие заказчики предпочитают получить комплексное решение, а не отдельные его компоненты, такие как серверы, СХД и т. д. У NetApp большой опыт разработки совместных решений с другими производителями. Расскажите немного о них. Возможно, у компании в ближайшем будущем есть планы на продолжение подобного сотрудничества с другими вендорами?

Развитие партнерской экосистемы – неотъемлемая часть бизнеса NetApp. Мы уже говорили о роли дистрибуторов и интеграторов в продвижении наших технологий. Партнеры по Глобальному альянсу – не менее важная часть экосистемы, и с самого начала своего существования компания NetApp создавала и предлагала рынку технологии и решения, интегрированные практически со всеми наиболее востребованными бизнес-приложениями и виртуальными средами, а также апробированные архитектуры для решения различных задач – от построения ЦОД до внедрения структуры машинного обучения.

Очень популярная сегодня архитектура FlexPod от NetApp и Cisco – пример такого многолетнего сотрудничества. Существующая почти 10 лет система для построения ЦОД насчитывает уже более 100 конфигураций для решения самого широкого спектра задач. У нас есть многолетние партнеры – такие, например, как SAP, Microsoft, Veeam Software, Brocade, а также производители, с которыми мы сотрудничаем не так давно, но очень успешно, как, например, NVIDIA. С приходом эры облачных сервисов к нашей экосистеме присоединились сервис-провайдеры и гиперскейлеры. Облачные сервисы NetApp, например Cloud Volumes ONTAP, Cloud Volumes Services for AWS, Cloud Volumes Services for Google Cloud, а также различные службы по управлению и аналитике данных, расширяют возможности заказчиков и позволяют наиболее полно использовать потенциал гибридного облака и получать максимальную отдачу от своих данных.

Как отличается структура облачных услуг на развитых, например в Западной Европе, и развивающихся рынках?

В некоторых странах, в которых мы работаем, уровень облачных услуг достаточно продвинутый – например, в Украине он сложился уже давно, и можно сказать, что уровень и спектр услуг местных сервис-провайдеров даже опережает потребности рынка. Гиперскейлеры также являются серьезными игроками в ряде стран, в первую очередь это, конечно, Microsoft и Amazon Web Services. В некоторых странах достаточно активно идет процесс развития аутсорсинговых проектов с использованием частных и государственных провайдеров. Например, в Молдове уже достаточно давно запущен проект по созданию и развитию государственного облака на самых современных технологиях. На мой взгляд, во всех странах основная проблема – дефицит квалифицированных кадров, а также государственное регулирование, которое не позволяет в полной мере использовать услуги глобальных сервис-провайдеров и потенциал гибридного облака.

Каким, по вашему мнению, должен быть идеальный ЦОД? Что требуется для его создания?

Сначала отмечу, что в эру цифровой трансформации сам по себе дата-центр для большинства компаний не является профильным направлением с точки зрения основного бизнеса. Если у компании есть дата-центр, это еще не значит, что она эффективно управляет данными. Чтобы быть эффективными, организациям сегодня необходимо больше концентрироваться на данных, прикладных приложениях, сервисах, поддерживающих и развивающих бизнес. Именно это направление приоритетно в плане инвестиций. Соответственно, затраты на ИТ все в большей степени переносятся из капитальных в операционные.

Максимальная плотность, эффективность, гиперконвергенция, широкое использование облачных сервисов – все это применяется для минимизации CAPEX. Это, в свою очередь, ведет к более эффективному использованию ресурсов и возможности реализовывать больше проектов. Современный ЦОД должен обеспечивать гарантированную производительность, управляемость на уровне API, горизон-

тальную масштабируемость. Исходя из этого, мы считаем, что необходимо переходить от построения дата-центра как уникального объекта к более промышленному подходу.

NetApp в этом направлении ведет активную работу: мы выпускаем новые линейки решений, ориентированные на ЦОД нового поколения (NetApp SolidFire, HCI, StorageGrid WebScale). При этом мы работаем и над модернизацией существующих ЦОД, в частности, продвигая флеш-технологии. Наконец, мы предоставляем заказчикам сервисы по управлению данными в публичных облаках гиперскейлеров. Это нужно для того, чтобы ЦОД заказчика мог работать с приложениями, уже размещенными в той или иной облачной среде.

Такие технологии, как IoT или искусственный интеллект, – насколько они используются сегодня в решениях NetApp?

NetApp уже применяет искусственный интеллект и Интернет вещей в работе с заказчиками. Например, в их распоряжении имеется виртуальный помощник Elio, который ведет мониторинг работы СХД заказчиков, использующих сервис AutoSupport.

С помощью базы данных NetApp и когнитивных технологий поиска, Elio находит нужные ответы в четыре раза быстрее, чем другие традиционные инструменты. Кроме того, совсем недавно мы создали для компании NVIDIA решение, сочетающее архитектуру GPU и сверхбыстрый флеш-СХД. Им закрывается весь процесс, начиная со сбора данных, где мы используем программно-определяемые системы, до процессинга on-premise с нашими флеш-системами.

Каковы, на ваш взгляд, наиболее важные факторы для успешной работы партнера?

Мы продаем достаточно сложные технологии, и партнер должен иметь компетенции для предоставления заказчикам лучших решений. Наши самые успешные партнеры – те, которые, используя продукты и решения NetApp, предлагают собственные сервисы, от самых простых задач до системной интеграции в прямом смысле этого слова, а также услуги по поддержке всей инфраструктуры заказчика, а не только конкретного оборудования.

Как вы считаете, изменится ли роль дистрибуторов в будущем, и если да, то каким образом?

Дистрибутор в виде логистического партнера перестанет играть вообще какую-либо роль в обозримом будущем. Дистрибуторы в основном будут и уже фокусируются на развитии партнерской сети, маркетинге и продвижении собственных компетенций, которые будут использовать их партнеры. То есть будет работать модель Value Added Distribution (VAD). Альтернатива – wholesale, то есть предложение максимально широкого спектра продукции по лучшим ценам.

Я думаю, что рано или поздно таких дистрибуторов заменят (или уже заменяют) глобальные компании, подобные Amazon и Alibaba, с которыми очень трудно конкурировать на местном уровне. Либо производители будут сами заниматься обработкой заказов и логистикой, как это уже делают некоторые наши коллеги-вендоры. После снятия границ и исчезновения таможен, хотя бы на уровне большого количества стран – а я верю, что это рано или поздно случится, – широкопрофильные дистрибуторы перестанут существовать, по крайней мере в том виде, в каком они существуют сейчас.

«Чтобы быть эффективными, компаниям сегодня необходимо больше концентрироваться на данных, прикладных приложениях, сервисах, поддерживающих и развивающих бизнес»

NetApp достаточно давно сотрудничает с группой компаний МУК в ряде стран. Как бы вы оценили это сотрудничество, насколько оно успешно?

МУК, по моему мнению, как раз и является ярко выраженным Value Added Distributor – именно поэтому мы и начали работать с группой компаний МУК в Украине. Компания зарекомендовала себя сильным игроком рынка, вносящим вклад в продвижение технологий в партнерский канал, заинтересованным в повышении квалификации партнеров и практикующим комплексный подход в подготовке решений. Отработав взаимодействие и нарастив компетенцию, мы постепенно расширили контракт на другие страны и будем развиваться дальше, решая поставленные задачи, как количественные, так и качественные.

НА ВСЕ РУКИ МАСТЕР:
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И СФЕРЫ ЕГО ПРИМЕНЕНИЯ

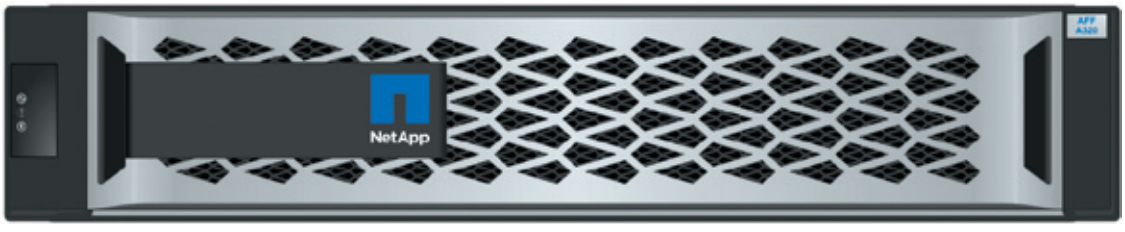
За последние несколько лет применение систем искусственного интеллекта стало обычным делом в самых разных сферах деятельности человека. Этому способствовало несколько факторов, среди которых основные – это рост мощностей вычислительных систем и развитие искусственных нейронных сетей. О том, какие основные возможности дает использование ИИ, поговорим далее

Один из главных прорывов, которые позволили говорить об искусственном интеллекте как о реальном инструменте, а не концепте из научной фантастики – изобретение нейронных сетей и моделей их глубокого обучения. Это позволило им учиться, самостоятельно анализировать данные и работать во многих сферах без предварительного программирования под конкретные задачи. Но для получения полноценного ИИ необходимы не только «код» и вычислительные мощности, но и специализированные массивы, так как для обучения требуются огромное количество информации и скорость ее передачи в вычислительные устройства. С учетом появления на рынке специализированных комплексов это стало еще ближе к каждой отдельной сфере. Так что теперь технологии искусственного интеллекта широко применяются в реальной жизни, а множество компаний (как известных корпораций, так и молодых стартапов) используют этот инструментарий для создания инновационных продуктов в разных сферах бизнеса. Давайте посмотрим, где и каким образом они применяются.

Производство

Применение ИИ вместе с инструментами Интернета вещей (IoT) приводит к созданию концепции умного производства. Данный подход позволяет добиться оптимизации рабочих процессов в таких областях, как, например, управление активами, цепочками поставок, автопарком и отслеживанием заказов. Умные системы мониторинга и обслуживания оборудования могут обнаруживать текущие неисправности и прогнозировать поломки оборудования заранее. Благодаря этому можно учесть вероятные сбои при планировании производственных циклов и сразу планировать бюджет на устранение возможных неисправностей.

Системы исуственного интеллекта позволяют снизить количество бракованной продукции. Так, в полупроводниковой промышленности количество брака



NetApp AFF A320 способствует ускорению работы традиционных и новых приложений, таких как искусственный интеллект и глубокое обучение, аналитика и базы данных

при производстве составляет весьма существенный процент. Искусственный интеллект дает возможность обнаруживать причины выпуска некачественной продукции и вносить соответствующие коррективы в рабочие процессы, тем самым снижая общее количество брака.

При тестировании и проверке продукции на качество могут применяться визуальные осмотры с поддержкой ИИ. Причем они оказываются более точными и быстрыми, чем обычные проверки людьми. Во время таких инспекций используются алгоритмы машинного обучения, которые позволяют выявить ранее известные дефекты продукции в автоматическом режиме, а также алгоритмы работы в полуавтоматическом режиме для обнаружения брака, который ранее не встречался. Хорошим примером внедрения подобных методов работы является компания Bosch, которой удалось добиться сокращения времени испытаний и калибровки на 35 % при производстве гидравлических насосов.

Улучшения в управлении запасами, более точное прогнозирование спроса, управление цепочками поставок – это другие важные области, в которых используются инструменты искусственного интеллекта. Так, американская международная корпорация Honeywell (производитель электронных систем управления и автоматизации, а также аэрокосмического оборудования) применяет систему прогнозирования спроса на основе ИИ, которая использует в качестве исходных данных различия и отношения индексов цен на сырую нефть.

Телеком

В сфере телекоммуникаций основными направлениями, где могут использоваться технологии искусственного интеллекта, по прогнозам экспертов, будут мониторинг и управление сетевыми операциями. С помощью ИИ можно разрабатывать оптимальные схемы развертывания сетей провайдеров, прогнозировать нагрузку и составлять планы по улучшению инфраструктуры. Подобные системы сосредоточатся вокруг интеллектуальных CRM-систем и кибербезопасности, а также обслуживания клиентов (виртуальные помощники). Последнее уже активно используют многие провайдеры, например, американский телеком-провайдер Spectrum использует автоматизированные чат-приложения на базе ИИ для обработки запросов клиентов и направления их к соответствующим специалистам. А телекоммуникационная компания CenturyLink использует умного помощника для решения маркетинговых задач: система отправляет десятки тысяч писем в месяц и интерпретирует ответы на них для определения клиентов, которые больше всего заинтересованы в новых услугах компании.

ONTAP AI – это полный инфраструктурный стек для работы систем ИИ и проведения машинного обучения

И, конечно, интеллектуальное обслуживание оборудования и инфраструктуры, например, вышек мобильной связи. При помощи искусственного интеллекта можно тестировать качество сигнала, обнаруживать неполадки в системах до того, как они проявили себя, выявлять места, где бывают перебои со связью, и т. д. Так, AT&T сейчас разрабатывает алгоритм на основе глубокого машинного обучения для полной автоматизации анализа видеоданных, поступающих с дронов, которые занимаются осмотром вышек связи.

Здравоохранение

Медицина – это отрасль, в которой технологии искусственного интеллекта могут найти (и уже находят) самое широкое применение. Одно из главных направлений – это диагностика заболеваний. Системы на базе компьютерного зрения, например, могут просматривать рентгеновские фотографии, снимки МРТ, результаты ультразвуковой диагностики и находить на них отклонения от нормы, что позволит обнаруживать

Пример применения платформы искусственного интеллекта ONTAP AI в медицине

В рамках изучения возможностей применения ИИ в разных сферах, компания NetApp провела обучение системы на базе ONTAP AI для диагностирования рака молочной железы. В результате модель достигла точности 79 % при идентификации доброкачественных клеток и 92 % точности обнаружения злокачественных клеток в тестируемом наборе данных. При этом использовался ограниченный объем информации (снимки из Университета Висконсина).
На практике, при обучении на большем количестве информации, можно достичь и лучших результатов.

NetApp HCI входит в концепцию Data Fabric, позволяя управлять данными в различных средах и организовывать обмен информацией между ними

болезни на ранних стадиях и применять соответствующие меры. Это очень поможет, например, в борьбе с раком.

Инструменты искусственного интеллекта могут помогать и в хирургии. Например, анализировать данные из медицинских карт до операции или физически направлять инструменты в режиме реального времени во время процедуры. Ожидаемый результат от таких действий – снижение ошибок и сокращение продолжительности пребывания пациентов в больнице после операций. Такие инструменты на данный момент производит израильская компания Mazor Robotics. Они пока применяются в простых операциях с минимальным хирургическим вмешательством.

Виртуальные медицинские ассистенты будут помогать на приемах пациентов и ранних этапах диагностики. Специальные голосовые и текстовые приложения смогут задавать вопросы и анализировать ответы пациентов. Это поможет снизить количество визитов в больницу, а при необходимости даст возможность сразу направлять пациентов к профильному специалисту. Как пример такого решения приведем виртуальную медсестру Sensely, которая проводит первичный опрос пациента через смартфон или планшет в качестве обычного мобильного приложения.

Ретейл

Использование искусственного интеллекта в розничном сегменте сосредоточено вокруг решения задач оптимизации в цепочке поставок, ценообразования и улучшения качества обслуживания клиентов. Один из главных источников убытков в торговле – залежи товаров на складах с одной стороны и отсутствие нужных позиций с другой. Особенно это актуально для больших сетей со множеством торговых точек в разных регионах.

Сейчас розничные магазины используют ИИ для прогнозирования спроса, понимания структуры покупок, управления заказами и сокращения потерь, связанных с отсутствием на складе и избытком запасов. Это получается за счет прогнозирования, анализа по каждому магазину, автоматического пополнения запасов до нужного уровня, оптимального размещения рекламы и т. д.

Для оптимизации ценообразования системы на основе искусственного интеллекта могут анализировать множество факторов, таких как погода, текущие рыночные условия, показатели продаж по конкретным магазинам, цены у конкурентов и т. д. Такие системы позволяют в автоматическом режиме предлагать наиболее подходящие цены на конкретные товары и группы, в том числе в ситуациях, когда на рынке появляются новинки, а спрос на их аналоги

Высокая производительность вычислительных систем – основа успешного применения ИИ

Чтобы быть конкурентоспособными на сегодняшнем рынке, компании во всех отраслях все больше инвестируют в решения искусственного интеллекта. Независимо от того, где они применяются, для их корректной и быстрой работы нужны большие вычислительные мощности. Успешное применение ИИ требует множества факторов, из которых можно выделить три ключевых компонента. Первый: большое количество обрабатываемых данных, причем чем больше – тем лучше. Второй: высокая скорость вычислений для быстрой обработки огромных массивов информации. Третий: системы хранения данных, которые бы позволяли хранить эти объемы и обеспечивать быстрый доступ к информации.

EF570 специально разработана для высокопроизводительных нагрузок, таких как аналитика больших данных, технические вычисления и видеонаблюдение, и позволяет быстро передавать необходимые данные в приложения ИИ

предыдущих серий или коллекций, соответственно, падает. Также это помогает организовывать распродажи и разнообразные акции со скидками. То же касается взаимодействия с клиентами. Системы ИИ смогут анализировать размещение товаров на полках магазинов и позиции стеллажей в торговом зале, а умные помощники дадут возможность сформировать персональные предложения для конкретного посетителя на основе его истории покупок и предпочтений. Как примеры подобных систем приведем FashionAI от Alibaba и Ask-eBay.

Искусственный интеллект также очень поможет в магазинах без касс, экспериментальные образцы которых от Amazon уже работают в США. Там будет использоваться компьютерное зрение и системы распознавания объектов, а виртуальные помощники помогут в осуществлении покупок.

Высокопроизводительные системы NetApp серии EF дают возможность хранить большие объемы информации и обеспечивают их быструю и непрерывную подачу в приложения ИИ. Устройства линейки имеют гибкие возможности масштабирования, что позволяет хранить информацию для глубокого машинного обучения систем искусственного интеллекта. Они поддерживают петабайты информации и разнообразные файловые системы, например, Luster, IBM Spectrum Scale и BeeGFS. Устройства обрабатывают до 1 млн операций ввода-вывода в секунду и записывают данные со скоростью до 14 Гбит в секунду. Кроме того, они имеют очень высокий уровень плотности относительно каждого мегабайта хранимых данных, что позволяет сократить расходы на электроэнергию, охлаждение и поддержку и значительно снизить совокупную стоимость использования.

Финансовый сектор

Сфера финансов является одной из самых востребованных для использования инструментов искусственного интеллекта. Тут надо обрабатывать и анализировать огромные объемы данных, учитывая при этом десятки индикаторов и сотни переменных. Инструменты ИИ можно применять в банковской сфере, страховании, инвестировании и т. д. В последнем случае, например, искусственный интеллект может более быстро и качественно оценить риски вложения денег в ту или иную компанию. Такие системы, помимо прочего, могут выдавать рекомендации по инвестированию на основе индивидуальных инвестиционных целей, склонности человека к риску, рыночной конъюнктуры. Алгоритмы ИИ могут рекомендовать пользователям оптимальные для них страховые или кредитные продукты, а менеджеры, наоборот, могут с их помощью анализировать риски для финансовой организации при выдаче кредитов или страховании. Подобная система уже работает в банке Morgan Stanley: она называется Next Best Action и автоматизирует многие рутинные задачи по обработке данных клиентов. А платформа AIERA от финансового холдинга Wells Fargo отслеживает цены на акции и формирует прогнозы о том, будут ли они расти или падать.

Еще одна важная сфера финансовой деятельности, где находят применение системы искусственного интеллекта, – это безопасность, в частности обнаружение мошенничества и противодействие киберпреступности. Там, например, можно использовать машинное обучение и наборы правил, чтобы выявлять подозрительные транзакции. Такие системы в автоматическом режиме выявляют определенные маркеры, которые могут указывать на взлом аккаунта пользователя и нелегальную отправку денег на другой счет. Среди них – необычное время или сумма транзакции, подозрительный адрес получателя, вход в систему с подозрительных IP-адресов или использование анонимайзеров. Вариантов может быть много, но главное, что ИИ может оперативно отследить эти маркеры, уведомить банковского работника или заблокировать операцию в автоматическом режиме до выяснения подробностей.

Платформа искусственного интеллекта ONTAP AI уже успела опробовать свои силы на медицинском поприще

Мощная платформа

Разработанная совместно NetApp и NVIDIA платформа искусственного интеллекта ONTAP AI – это полный инфраструктурный стек для работы систем ИИ и проведения машинного обучения. Системы хранения NetApp A800 NVMe обеспечивают скорость чтения до 25 ГБ/с и могут быть объединены в кластеры до 12 систем с совокупной скоростью доставки данных до 300 ГБ/с на серверы с графическими процессорами NVIDIA DGX-1, а технология томов FlexGroup позволяет отображать до 75 ПБ данных в одном пространстве имен. В системе также используются коммутаторы Cisco Nexus 3232C с поддержкой 100-гигабитного интерфейса Ethernet.

Одно из главных преимуществ системы – это быстрота и автоматизация развертки и настройки. Хоть все стремятся сделать ИТ-инфраструктуру максимально простой, решения искусственного интеллекта зачастую сложнее обычных ИТ-систем. Но, тем не менее, добиться упрощения некоторых задач можно и в них. Так, ONTAP AI поддерживает работу с инструментом Ansible, который де-факто стал стандартом для систем Red Hat. Он использует концепцию ролей для предоставления стандартного набора задач, которые можно выполнить несколько раз или на нескольких устройствах, просто изменив некоторые переменные. Каждая роль содержит специфичные для устройства, на котором она исполняется, задачи, а также любые переменные по умолчанию или другие файлы, необходимые для завершения настройки ONTAP AI.

И, конечно, один из самых распространенных методов применения ИИ для обслуживания клиентов в финансовой сфере – это разнообразные чатботы. Используя методы обучения, применяемые для интерпретации и автоматизации потребностей и проблем клиентов (в том числе с использованием подходов НЛП), они автоматизируют работу с обращениями клиентов и даже способны решать многие их проблемы без участия живого сотрудника.

Государственная сфера

Тут выделяются два основных направления работы систем ИИ – это повышение эффективности расходов за счет автоматизации в правительственных учреждениях, а также военная сфера. В государственном управлении искуственный интеллект может применяться там, где встречаются проблемы нехватки ресурсов, необходимости анализа большого количества информации и забюрократизованности. Приложения на базе ИИ могут сократить расходы и разобраться с нехваткой ресурсов за счет оптимизации и повышения точности обработки данных. По прогнозам аналитической компании Deloitte, при высоком уровне инвестиций в системы искусственного интеллекта, правительство США до 2020 года сможет сэкономить более $41 млрд.

Рынок робототехники и систем искусственного интеллекта в оборонной сфере в 2018 году оценивался в $39,2 млрд и, по прогнозам, вырастет до $61 млрд в 2027 году. Тут основное применение находят дроны и наземные роботы с возможностями компьютерного зрения, использование алгоритмов машинного обучения для проведения разведки и патрулирования, автономный транспорт, способный самостоятельно передвигаться на поле боя, системы распознавания речи и автоматического перевода. Еще одна важная сфера – это кибербезопасность. Государственные центры обработки данных могут стать целью атаки вражеских хакеров. Для их защиты также можно применять методы на основе систем ИИ.

Вместо послесловия

Как видим, уже сегодня сфер применения искусственного интеллекта достаточно много. И с каждым годом их количество будет увеличиваться. Поэтому для многих компаний уже сегодня важно инвестировать в платформы ИИ – внедрение подобных систем позволит сделать качественный рывок в развитии бизнеса и в будущем иметь преимущество перед конкурентами, которые только начнут внедрять такие системы у себя.

Также стоит обратить внимание и на разнообразный набор данных, который необходим для машинного обучения. В данный момент уже существуют компании, которые предлагают доступ по подписке к этим объемам. Хорошая альтернатива может быть предложена на базе решения StorageGRID Webscale, которое может хранить петабайты информации совершенно разрозненных данных.

По вопросам обращаться: *netapp@muk.ua*.

NetApp HCI.

Ready for Next.

We can help you transform and empower your organization to move faster, drive operational efficiency, and reduce costs.

- **Elastic scalability**
- **Data fabric and cloud services**
- **Guaranteed mixed workload performance**
- **Flexible delivery and consumption**

NetApp®

MUK
Classics of distribution

УВИДЕТЬ И ОТЛИЧИТЬ

ОБЗОР СИСТЕМЫ РАСПОЗНАВАНИЯ ОБЪЕКТОВ IBM POWERAI VISION

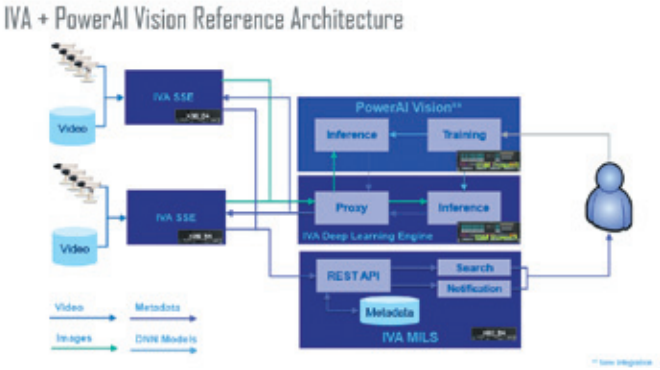
Для человека восприятие окружающего мира – дело само собой разумеющееся. У нас есть глаза, чтобы видеть окружающие объекты, уши, чтобы слышать звуки, нос, чтобы чувствовать запахи.

Компьютерные системы, с другой стороны, не могут этого делать по умолчанию, как человек, даже если имеют соответствующие сенсоры – камеры и динамики.

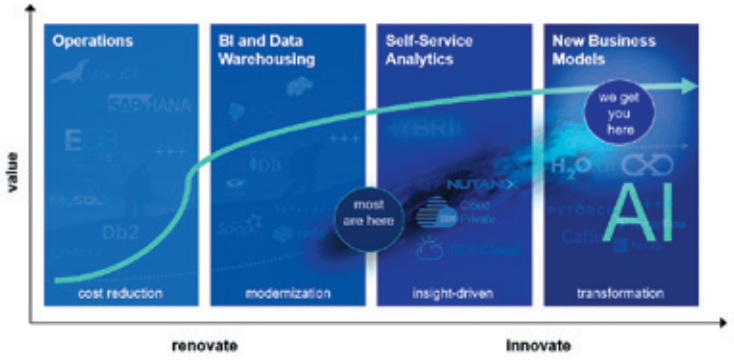
Но годы исследований привели к тому, что сегодня искусственный интеллект после длительного обучения может, например, корректно распознавать объекты на видео.

Один из таких инструментов – **IBM PowerAI Vision**, о котором пойдет речь далее

Компьютерное зрение и обнаружение объектов – это относительно новые, но очень полезные сферы работы вычислительных систем. Они функционируют при помощи машинного обучения, что позволяет с высокой эффективностью решать подобные задачи. Но сама настройка и установка моделей глубокого машинного обучения – это сложный и трудоемкий процесс, который требует задействования высокого класса специалистов и большого количества ресурсов. Продукт IBM PowerAI Vision способен решить эту проблему.



Эталонная архитектура IVA on Power с PowerAI Vision



Путь к внедрению искусственного интеллекта

Как это работает

Прежде чем говорить о возможностях IBM PowerAI Vision, давайте разберемся, где вообще применяются или могут применяться системы компьютерного зрения. На самом деле, много где. Например, для осмотра линий электропередач. Вместо того, чтобы посылать на инспекцию сотрудников, можно использовать дроны с камерами высокого разрешения, картинку с которых будет обрабатывать система искусственного интеллекта. Особенно этот вопрос актуален в гористой местности и на больших площадях, где подобные инспекции зачастую превращаются в настоящую проблему. По расчетам экспертов IBM, использование компьютерного зрения на 90% снизит затраты времени на проведение проверок. И, конечно, сведет к нулю риски для здоровья и жизни технических специалистов. Другая сфера применения компьютерного зрения – медицина. Сейчас множество диагнозов ставится на основе просмотров рентгеновских снимков или ультразвуковой диагностики. Использование компьютерного зрения в тандеме с искусственным интеллектом позволит врачам обрабатывать намного больше информации и ставить более точные диагнозы – ведь исключается человеческая ошибка вследствие усталости или невнимательности. Еще одна область, где данная технология может быть полезна, — соблюдение правил в сфере производственной безопасности. Системы компьютерного зрения могут идентифицировать рабочих, входящих в опасные зоны, или вести наблюдение за стройплощадками и уведомлять бригадиров о нештатных ситуациях. Как видим, вариантов применения технологии много – на самом деле намного больше, чем мы здесь описали.

Платформа PowerAI Vision функционирует на базе серверов линейки POWER с высокой производительностью. Это и не удивительно – такого рода задания требуют очень много вычислительных мощностей, а подобные серверы как раз и спроектированы для решения задач искусственного интеллекта. Как пример приведем модель IBM POWER AC922 (она, к слову, рекомендована для использования с платформой IBM Watson Machine Learning Accelerator). Конфигурация этого сервера состоит из процессорного ядра в составе двух чипов POWER9, накопителя и ОЗУ, а также дополнительными двумя, четырьмя или шестью графическими процессорами NVIDIA Tesla V100, каждый из которых оснащен 5120 вычислительными ядрами CUDA. Кроме того, система оборудована интерфейсом передачи данных нового поколения – PCIe Gen4, который в два раза быстрее PCIe 3. В конфигурации DDL (Distributed Deep Learning) можно добавить больше графических процессоров. Работает сервер на ОС семейства Linux – Ubuntu или Redhat. Установка платформы PowerAI Vision на него занимает менее часа.

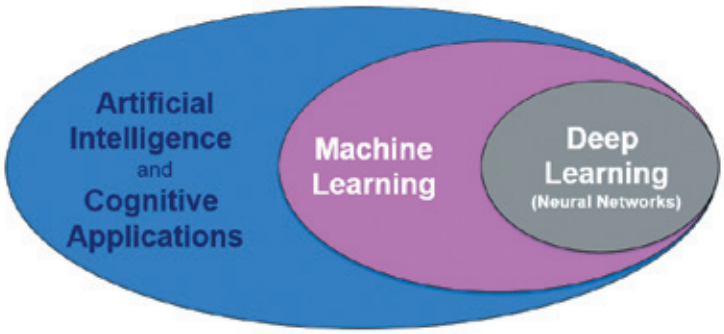
В своей работе система использует методы глубокого машинного обучения, при которых автоматически изучает функции и тренируется определять объекты из набора обучающих данных. Недостатки этих методов в том, что для качественного обучения необходимы большие объемы данных с вариациями объектов, на которых платформа тренируется. Но существуют моменты, когда большое количество вариаций недо-

По расчетам экспертов IBM, использование компьютерного зрения снизит затраты времени на проведение проверок на 90 %, а также сведет практически до нуля риски для здоровья и жизни технических специалистов

Немного истории и перспектив

Как уже было сказано в начале статьи, созданию функциональных систем компьютерного зрения предшествовали годы разработок. Существенный прогресс в этой сфере начался с 2012 года, когда нейронная сеть под названием Convolutional Neural Network смогла добиться точности распознавания в 83,6 %, тогда как годом ранее лучшие показатели достигали только 75 %. В 2015 году платформа ImageNet превзошла в работе человека-эксперта, ошибочно распознав лишь 5,1 % объектов. Этому способствовало, в первую очередь, развитие вычислительных технологий, а именно появление новых поколений графических процессоров, свежих алгоритмов глубокого машинного обучения и архитектур нейронных сетей. На данный же момент рекорд в распознавании принадлежит инструменту NASNet, который в 2017 году еще больше снизил уровень ошибок и продемонстрировал результат в 2,4 % неверных распознаваний.

Сейчас основной остается контролируемая модель обучения ИИ. Она подразумевает, что прежде чем система сможет работать автономно, ей нужно «скормить» тысячи образцов для каждой категории классифицируемых объектов. Только тогда она сможет с минимальной погрешностью определять необходимые объекты самостоятельно. Именно эту модель использует IBM PowerAI Vision в своей работе, но при этом существенно упрощает задачи, которые должен для обучения машины выполнить человек. Однако не стоит забывать, что многими компаниями (IBM, Google, Microsoft, Facebook, Amazon и др.) ведутся исследования в области альтернативных моделей обучения, в том числе без прямого участия человека. Правда, на данный момент они находятся на разных, далеких от финиша стадиях разработки, но не стоит исключать, что через несколько лет они появятся на рынке в качестве полноценных рабочих продуктов.



Путь к когнитивным вычислениям

После первичного обучения система позволяет разворачивать модели на удаленных конечных точках, имеющих минимум один ускоритель или даже без него, работающего только на центральном процессоре

ступно. Например, при облете вышек линий электропередач дрон не найдет много разных объектов. Поэтому при использовании обычной системы компьютерного зрения ее будет трудно обучить для выполнения инспекции таких конструкций. Подход PowerAI Vision к решению этого вопроса заключается в том, что при обучении есть возможность вносить коррективы в уже полученные изображения, например, обрезать их, делать менее четкими или более резкими, поворачивать и т. д. Причем делается это при помощи специальных алгоритмов, что дает возможность системе лучше обучаться при наличии ограниченного количества вариативных данных. Также PowerAI Vision может работать не только со статическими изображениями, но и с видеофайлами. Платформа позволяет импортировать видео и очень быстро разметить кадры для разметки наборов данных. К тому же доступна обработка и потокового видео.

После того как система прошла обучение, пользователям становится доступна функциональная панель инструментов. Представленные на ней средства помогают оценить точность моделей и пробелы в наборах данных, если таковые имеются. Выявление имеющихся пробелов необходимо для высокой точности работы системы и, в частности, получаемых моделей. Подобные статистические данные (например, матрица ошибок, общее количество отзывов и их точность) позволяют пользователям сосредоточиться на изображениях, которые либо не соответствуют заданным категориям, либо нуждаются в дополнении. То есть специалист может сосредоточиться именно на тех моментах, которые в первую очередь нуждаются в доработке. На панели мониторинга также отображаются параметры, которые необходимо настроить на следующем этапе обучения.

Особенности продукта

Одно из главных преимуществ IBM PowerAI Vision – это гибкость использования системы. Например, после первичного обучения система позволяет разворачивать модели на удаленных конечных точках, имеющих минимум один ускоритель (GPU или FPGA) или даже без него, работающего только на ЦП. Также обученные на IBM PowerAI Vision модели могут быть развернуты на системах x86, любых моделях линейки серверов IBM Power Systems и на открытых системах автоматического разворачивания приложений Kubernetes (правда, эта возможность ограничена облачным сервисом IBM Cloud Private), где акселераторы во всем кластере задействованы для обучения и развертывания моделей.

Еще одна полезная возможность IBM PowerAI Vision – поддержка работы с программируемыми матрицами (FPGA). Дело в том, что обычно модели, обученные на графических процессорах, не совместимы с FPGA. Но при этом такие матрицы дешевле, энергоэффективнее, легче программируются под конкретные задачи и достигают в их выполнении лучших показателей. При помощи системы IBM оптимизация моделей для использования с FPGA происходит в автоматическом режиме, а сами модели, созданные при помощи вычислений на графических процессорах, становятся доступными для выполнения на FPGA.

Что касается интерфейса и удобства работы, то в IBM пошли по принципу упрощения, сделав систему максимально доступной и комфортной. Платформа имеет легкую в использовании графическую оболочку и понятна для работы даже специалистам без навыков в сфере глубокого машинного обучения. Например, натренировать модели глубинного обучения классифицировать изображения и находить важные объекты можно без программирования, просто выбрав необходимые категории для изображений и обведя рамками нужные объекты. При этом технические детали вроде нейронных сетей и гиперпараметров настраиваются автоматически без участия пользователя. Это позволяет существенно ускорить работу и повысить ее продуктивность, ведь в среднем специалисты по анализу данных тратят около 80 % времени именно на разметку и подготовку наборов данных для обучения.

Краткий итог

Машинное обучение систем компьютерного зрения остается сложной задачей, но с использованием возможностей IBM PowerAI Vision оно существенно упрощается и становится доступным даже людям без специальных навыков. В работе инструмента используется итерационное обучение для автоматической разметки комплексов информации, что дает на выходе точно размеченные наборы данных, сразу подходящих для обучения. А это, в свою очередь, существенно сокращает затраты и ускоряет развертывание решений в сфере искусственного интеллекта.

По вопросам обращаться: *ibm@muk.ua*.

MUK
Classics of distribution

IBM

IBM Flash Storage

ускоряет и оптимизирует работу в мультиоблачных средах

Системы хранения данных на основе флеш-памяти, предназначенные для ускорения работы инфраструктуры

Спроектировано с учетом требований современных высокопроизводительных приложений

Ведущая технология с гарантированной эффективностью

Системы хранения данных на основе флеш-памяти, адаптируемые с учетом ваших потребностей

Представительства MUK

Азербайджан: ibm@muk.az
Беларусь: ibm@muk.by
Казахстан, Кыргызстан: ibm@muk.kz
Узбекистан: ibm @muk.uz
Туркменистан: office@tm.muk.international
Армения: ibm@muk.am
Грузия: ibm@muk.ge
Украина: ibm@muk.ua
Таджикистан: ibm@muk.tj

MUK review

JUNIPER CONTRAIL HEALTHBOT:
ОТ АНАЛИТИКИ К РЕКОМЕНДАЦИЯМ

Анализировать потоки данных, генерируемых в сети облачными и пользовательскими приложениями, в «ручном» режиме становится затруднительно, а порой и практически невозможно. Помочь в такой ситуации способна система Juniper Contrail HealthBot на базе искусственного интеллекта

Сегодня с распространением новых устройств и облачных приложений трафик растет в геометрической прогрессии. Операторам связи и предприятиям необходима сетевая аналитика в реальном времени, иначе обрабатывать растущие объемы и непрогнозируемые изменения трафика крайне сложно.

Для комплексного представления о состоянии отдельных приложений, сервисов, оконечных устройств абонентов необходимо проводить анализ сетевых данных. Но при растущем числе протоколов, форматов данных и показателей эффективности сетевых устройств этот процесс трудоемок и дорог. Извлечение производственной информации из телеметрии через традиционные CLI-интерфейсы требует высокой квалификации, что затрудняет освоение сетевой аналитики.

Машинное обучение позволяет существенно упростить и автоматизировать процессы извлечения, анализа и разбора сетевых данных. Специальные инструменты аналитики сопоставляют данные эффективнее традиционных сетевых устройств и позволяют детально анализировать отдельные приложения и сервисы. Современные алгоритмы сокращают время на анализ трафика – это дает возможность прогнозировать и действовать проактивно. Именно таким решением является Juniper Contrail HealthBot, которое сочетает в себе преимущества потоковой телеметрии и машинного обучения.

Особенности решения

Juniper Contrail HealthBot представляет собой программируемое решение с высоким уровнем автоматизации для проверки рабочего состояния и диагностики сетей, обеспечивающее единообразие и согласованность операционной аналитики для сетевых систем. Contrail HealthBot интегрирован с интерфейсом телеметрии Junos (JTI) и средствами телеметрии стандарта OpenConfig. Система собирает большие объемы оперативных данных и применяет машинное обучение для многомерного представления сети и приложений и преобразования результатов анализа в практические рекомендации.

Contrail HealthBot имеет модульную структуру и горизонтальную контейнерную архитектуру микросервисов. Для поддержки интенционно-ориентированных сетевых операций специальные алгоритмы, дополненные машинным обучением, сопоставляют данные из разных источников, задают операционные показатели и выполняют исторический и прогнозный анализ. Автоматизированная аналитика упрощает эксплуатацию сетей. Предприятия могут постоянно отслеживать и оценивать свою сетевую инфраструктуру для повышения эффективности эксплуатации и планирования мощностей.

Решение ориентировано на программируемость с поддержкой индивидуальных задач по мониторингу и диагностике с помощью программируемых сценариев. Информационная панель с интуитивно понятным веб-интерфейсом снимает завышенные требования к квалификации персонала для извлечения данных телеметрии. Анализ рабочего состояния и первопричин по модели YANG позволяет расширить и настроить обрабатываемые ключевые показатели, а также необходимую для анализа бизнес-логику.

Contrail HealthBot поддерживается инфраструктурой Juniper Networks Professional Services, а внедрение у 100 ведущих операторов связи дало ценные сведения по планированию, проектированию и эксплуатации в сетях, обеспечивающие успех следующих внедрений при минимуме риска.

Далее более подробно рассмотрим функции, которые реализованы в Contrail HealthBot для сбора аналитики в реальном времени с получением рекомендаций.

Машинное обучение

Машинное обучение позволяет системе понять исходные характеристики элементов инфраструктуры и сетевых приложений. Специальные алгоритмы выявляют аномалии, при которых отклонение текущих показателей от исторических значений выходит за допустимые пределы. В формируемой политике мониторинга учтена динамика поведения сети, вызывающая временные колебания требований к ресурсам.

Преимущества Juniper Contrail HealthBot

Улучшенная видимость сети

Contrail HealthBot позволяет избавиться от проблем, характерных для обслуживания традиционных систем мониторинга, обеспечивая современную многомерную аналитику по всем компонентам сети. Это дает возможность перейти от реактивной модели управления сетью к проактивной (прогнозной). Такая модель дает исчерпывающее представление о поведении сети, а также позволяет улучшить планирование использования ресурсов и минимизировать простои.

Автоматизация с обратной связью

Решение оптимизирует работу сетевых инфраструктур. Определение первопричин и источников инцидентов всегда было длительным процессом, накладывающимся на сложности технического обслуживания. Contrail HealthBot объединяет мощь поэлементной аналитики с автоматизацией процессов, позволяя оптимизировать диагностику, а также автоматизировать анализ первопричин возникновения инцидентов и действия по корректировке работы сети с учетом заданных KPI.

Повышенная окупаемость

Contrail HealthBot сокращает общие капитальные затраты. Благодаря алгоритмам машинного обучения и прогнозному анализу решение оптимизирует загрузку сети, позволяя операторам предлагать новые сервисы и при этом лучше планировать использование ресурсов и регулировать трафик.

Снижение операционных расходов

Реализованная в Contrail HealthBot функция машинного обучения сопоставляет данные из разных источников, задает исходные операционные показатели и упрощает эксплуатацию сети. Благодаря интуитивно понятному интерфейсу ИТ-департаменты получают нужные им сведения, улучшают эффективность эксплуатации, соблюдают положения соглашений SLA. Все это помогает спрогнозировать и предотвратить возможные сбои в работе сети.

Алгоритм машинного обучения помогает прогнозировать загрузку сети с учетом заданных шаблонов, автоматизировать сетевое планирование, оптимизировать элементы инфраструктуры для более эффективной эксплуатации ресурсов.

Мониторинг состояния и анализ причин

Функция мониторинга отображает рабочее состояние сети путем сведения исходных потоковых данных телеметрии в многомерное представление с отображением текущей картины и прогнозируемых угроз для инфраструктуры. Статус показывает, находится ли сетевой ресурс в рамках заданной политики рабочих характеристик, а анализ рисков на базе истории позволяет прогнозировать его возможное «нестандартное» состояние.

Функция мониторинга не только обеспечивает настраиваемое представление текущего состояния элементов сети, но и при необходимости запускает корректирующие действия в зависимости от положений соглашения об уровне обслуживания (SLA). Для пользовательской настройки профилей состояния используются определения YANG.

Программируемость

Ядро Contrail HealthBot программируется открытыми средствами, за счет чего поддерживаются мониторинг сети и адаптируемая диагностика. Простой конструктор позволяет операторам связи и предприятиям оперативно создавать политики и сценарии, рационально автоматизирующие эксплуатацию сервисов и обеспечивающие выполнение плановых показателей. Также через Juniper EngNet доступна библиотека готовых сценариев (Playbooks), созданных пользователями. Это позволяет снизить требования к персоналу, занимающемуся сетевой аналитикой, улучшить маневренность бизнеса и способствует внедрению инноваций в экосистему предприятия.

Графический интерфейс

На информационной веб-панели решения показаны количественные показатели для ресурсов, предупреждения, состояние системы и отчеты. Отображение связей между отдельными элементами (устройствами, службами, хостами, экземплярами) упрощает применение бизнес-логики и нужных политик.

Потоковая телеметрия

Для потоковой телеметрии в реальном времени в Contrail HealthBot используются интерфейс Junos Telemetry Interface (JTI) и OpenConfig. JTI — распределенный инструмент сбора данных, обеспечивающий потоковую передачу статистических сетевых данных в режиме, близком к реальному времени.

Данные передаются модулям сбора, сетевым контроллерам и аналогичным устройствам для оперативного анализа. Асинхронный push-метод передачи данных с использованием популярных протоколов MQ Telemetry Transport (MQTT) и JavaScript Object Notation (JSON) снимает ограничения, характерные для последовательного запроса к устройствам сети. В результате улучшается масштабируемость JTI, давая возможность отслеживать тысяч сетевых объектов.

В качестве послесловия

В целом, Contrail HealthBot можно назвать новым словом в эксплуатации сетей благодаря качественным улучшениям анализа и автоматизации. Объединяя потоковую телеметрию в реальном времени, высокосовершенные алгоритмы и машинное обучение, Contrail HealthBot сводит большие объемы оперативных данных для многомерного представления сети и приложений с преобразованием результатов анализа в точный прогноз поведения сети. Фокусируясь на практических рекомендациях, упрощении использования данных и программируемой структуре с конвейером и модулями сбора данных с открытым кодом, решение снижает требования к квалификации персонала для сетевой аналитики, устраняет дробление данных, способствуя взаимодействию подразделений компании, улучшению маневренности бизнеса и инновациям в экосистеме в целом.

По вопросам обращаться: *juniper@muk.ua*.

ЭФФЕКТИВНАЯ ИНФРАСТРУКТУРА:
DELL EMC POWEREDGE MX

Сегодня различные новые технологии создают для ИТ-отделов компаний проблему в том, как точно спрогнозировать потребность в вычислительных ресурсах для определенных рабочих нагрузок. Dell EMC PowerEdge MX дает возможность строить ИТ-системы путем сочетания серверов, хранилищ и коммутаторов, а также позволяет оптимизировать использование ресурсов инфраструктуры

Модульная инфраструктура PowerEdge MX разработана специально для программно-определяемых ЦОД. Она позволяет обеспечить функционирование таких ресурсоемких задач и ресурсов, как сложные проекты виртуализации, искусственного интеллекта и больших данных, программно-определяемых систем хранения и программно-конфигурируемых сетей.

В PowerEdge MX реализована поддержка высокоскоростных накопителей с интерфейсом NVMe, а также технологии сетевых подключений 25 Gigabit Ethernet. Конфигурация системы может быть подобрана в зависимости от пожеланий и индивидуальных потребностей заказчика. По мере возникновения новых задач есть возможность использовать общие пулы с ресурсами вычислений и хранения и извлекать лишь нужные, в то время как неиспользуемые ресурсы возвращаются в пул. Фактически это позволяет управлять мощностью на уровне центра обработки данных, а не на уровне каждого сервера, снизить переизбыток ресурсов и оптимизировать производительность и эффективность.

Особенности решения

В PowerEdge MX используется кинетическая инфраструктура, в которой отсутствует midplane – центральная объединительная плата. Это позволяет совмещать технологии нескольких поколений, различные процессоры, новые типы накопителей и сетевые интерфейсы в рамках одного решения. Например, отсутствие объединительной платы позволяет напрямую соединять вычислительные модули с модулями ввода-вывода, что дает возможность в будущем производить модернизацию системы без необходимости прерывания ее работы.

PowerEdge MX позволяет обеспечить выполнение таких ресурсоемких задач, как сложные проекты виртуализации, искусственного интеллекта и больших данных

DELL EMC | MUK Classics of distribution

Dell EMC PowerMax – самый быстрый массив хранения данных в мире[1]

Dell EMC PowerMax 8000

PowerMax — это быстрая, интеллектуальная и эффективная СХД без компромиссов. Массив PowerMax на базе процессоров Intel® Xeon® служит образцом современной системы хранения уровня 0 благодаря горизонтально масштабируемой архитектуре с несколькими контроллерами, машинному обучению и интеллектуальному сокращению объемов данных.

Dell EMC PowerMax 2000

- БЫСТРОТА
- ИНТЕЛЛЕКТУАЛЬНОСТЬ
- ЭФФЕКТИВНОСТЬ

БЕЗ КОМПРОМИССОВ

10 UP TO M IOPS[2]

Производительность до 10 млн IOPS[2]

50%

На 50% быстрее отклик[3]

150 Gb/s

150 Гбит/сек пропускная способность

1 По результатам внутреннего анализа Dell EMC, март 2018 г. В ходе анализа сравнивалась пропускная способность массива PowerMax 8000 и популярных конкурентных массивов (согласно опубликованным данным).

2 По результатам внутреннего анализа максимального показателя IOPS (в одном массиве) для PowerMax 8000, проведенного Dell EMC в марте 2018 г.

3 По результатам внутреннего тестирования Dell EMC, март 2018 г. В ходе тестирования сравнивались массивы PowerMax с накопителями SCM и VMAX 950F с флэш-накопителями SAS с помощью эталонного теста неудачных операций произвольного чтения. Фактическое время отклика может отличаться от указанного.

Платформа PowerEdge MX совмещает в себе технологии нескольких поколений, различные процессоры, новые типы накопителей и сетевые интерфейсы

Решение готово к поддержке дезагрегированных компонентов, включая устройства с обработкой данных в оперативной памяти, такие как память накопительного класса (Storage Class Memory), GPU и FPGA.

PowerEdge MX объединяет традиционные и программно-определяемые центры обработки данных с различными уровнями универсальности и оперативности. Корпус системы содержит разъединенные блоки сервера и системы хранения данных, позволяя выделять необходимые ресурсы по требованию. При этом система питания, охлаждения, организации сети, ввода-вывода и управления – общие для всей конструкции.

PowerEdge MX: составляющие

Линейка PowerEdge MX имеет гибкие возможности индивидуального конфигурирования за счет широкого выбора компонентов. Система включает в себя шасси и различные блоки ресурсов, и серверных, и для хранения данных, которые подключаются к сети через «умную» структуру ввода/вывода.

Шасси Dell EMC PowerEdge MX7000 представляет собой аппаратную основу с поддержкой большого числа поколений серверных процессоров. Главным преимуществом шасси являются масштабируемость, комплексное управление жизненным циклом и единый интерфейс для всех компонентов. PowerEdge MX7000 имеет форм-фактор 7U и включает восемь отсеков для разнообразных комбинаций вычислительных узлов и хранилищ данных.

В качестве вычислительных узлов используются мощные 2- и 4-сокетные модульные серверы Dell EMC PowerEdge MX740c и MX840c, отличающиеся превосходной производительностью и широким выбором накопителей, включая NVMe-устройства. MX740c представляет собой ординарный вычислительный узел и является единственным на рынке двухсокетным сервером, который может содержать до шести накопителей с интерфейсом NVMe, SAS или SATA формата 2,5'' с поддержкой многоуровневого хранения между ними. MX840c – узел двойной ширины, четырехсокетный сервер, поддерживающий до восьми накопителей. Обе модели поддерживают все процессоры семейства Intel Xeon Scalable и могут быть укомплектованы до 6 ТБ оперативной памяти.

Модульные серверы MX дополняют полноформатные узлы хранения высокой плотности Dell EMC PowerEdge MX5016s. Они вмещают до 16 жестких дисков с интерфейсом SAS с возможностью горячей замены. В одном корпусе MX можно поместить до семи узлов MX5016s, позволяющих, в свою очередь, разместить до 112 жестких дисков с прямым подключением. Эти накопители можно назначить серверам индивидуально, тем самым обеспечивая идеальный коэффициент емкости для решения специфических задач.

PowerEdge MX комплектуется коммутационными узлами типа Ethernet (25 Гбит/с) и Fibre Channel (до 32 Гбит/с). Это новые коммутирующие модули с низкой задержкой при передаче данных и широкой пропускной способностью. Они оснащены функцией автоматического соответствия топологии, технологиями приоритизации трафика и автоматического устранения проблем, а также имеют единый интерфейс управления PowerEdge MX.

Администрирование

Новое решение позволяет повысить эффективность и ускорить операции благодаря применению унифицированных средств автоматизации. Управление системой производится с помощью Dell EMC OpenManage Enterprise (Modular Edition), которое включает в себя программное обеспечение OpenManage Enterprise – оно дает возможность автоматически расширять систему от одного до нескольких шасси, а также масштабировать управление до нескольких тысяч серверов PowerEdge MX и стоечных серверов. Управление серверами с передней панели обеспечивает функция Quick Sync 2. Универсальный интерфейс RESTful API позволяет автоматизировать несколько задач и подключать инструменты сторонних производителей. Решение полностью интегрируется со встроенным контроллером удаленного доступа Dell 9 (iDRAC9) и контроллером жизненного цикла (LC).

По вопросам обращаться: *DellEMC@muk.ua*.

КУРС НА АВТОМАТИЗАЦИЮ:
CISCO SD-WAN

Сегодня для организаций, имеющих большие территориально распределенные сети с удаленными офисами и филиалами, важно реализовать связность и обеспечить политики работы приложений между этими филиалами. Это позволит сделать технология Cisco SD-WAN

Недавнее исследование IDC по итогам опроса большого количества компаний с территориально-распределенной инфраструктурой выявило три основные сложности, с которыми сталкиваются такие организации. Первая из них – это требования к безопасности, связанные с доступом к Интернету и веб-приложениям из филиалов. Пользователи все чаще используют для удаленного подключения к корпоративной сети собственные устройства, что обуславливает необходимость более тщательной защиты сети и самих устройств. Кроме того, чем дальше, тем больше появляется новых угроз, и технологии для защиты от них становятся все сложнее. Вторая проблема ассоциируется с использованием в отделениях нескольких различных каналов связи. Трудность заключается в необходимости использовать их для приложений и сервисов компании – механизмы, позволяющие применять все каналы одновременно, достаточно сложны. А при наличии большого числа филиалов эта сложность мультиплицируется. И третья – необходимость понимать и анализировать, какие типы данных передаются между филиалами, насколько загружены каналы между удаленными площадками, и насколько качественно они обслуживают работу бизнес-приложений компании.

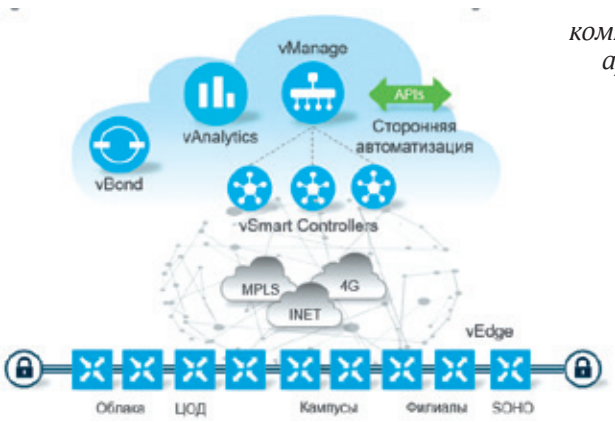
Для разрешения этих проблем традиционные подходы не годятся. Главная причина в том, что акцент делается на аппаратную составляющую. Оборудования в распределенных сетях достаточно много, его конфигурирование, как правило, осуществляется в ручном режиме. По мере того, как сеть расширяется, сложность настройки и поддержки увеличивается, проблемы устраняются в реактивном режиме, то есть уже после их возникновения.

Все эти процессы выполняются на так называемом «языке оборудования», или «языке сетевых намерений». Подход Cisco заключается в том, чтобы эти команды передавались более понятным для бизнеса языком, а бизнес-язык будет автоматически транслироваться в язык сетевого оборудования. Для реализации этого сеть становится программно-определяемой. Это означает, что определенное ПО позволяет автоматизировать процесс внедрения филиалов в распределенную сеть. Оно даст возможность обеспечить подключение сторонних приложений, и при необходимости внесения в конфигурацию каких-либо дополнительных параметров они будут применяться ко всей сети. Реактивный подход по устранению неисправностей останется в прошлом – сеть будет самостоятельно анализировать уровень загрузки каналов связи и качество обслуживания сервисов, автоматически распределять ресурсы, а также предупреждать о необходимости внесения определенных изменений для того, чтобы это качество обслуживания приложений оставалось на требуемом уровне.

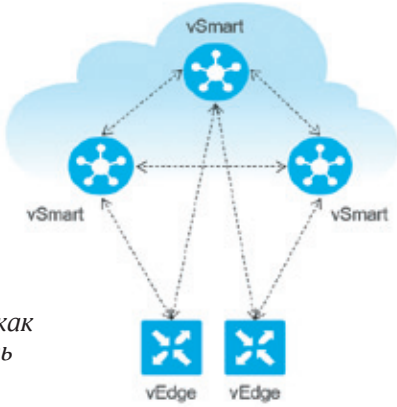
Ключевые аспекты

Именно такой подход реализован в решении Cisco SD-WAN, которое появилось в портфолио Cisco после

Четыре основных принципа Cisco SD-WAN



Три основных компонента (плоскости) архитектуры Cisco SD-WAN



Контроллеры vSmart передают маршрутизаторам централизованные политики и указывают, как обеспечивать связность между филиалами

приобретения компании Viptela – стартапа по разработке программно-определяемых WAN-сетей. Cisco SD-WAN имеет ряд основных фокусов – обеспечение безопасности, гибкая эксплуатация, обеспечение качества работы приложений и облачные технологии.

Обеспечение безопасности рассматривается в контексте того, что многие функции реализуются автоматически, и заказчику не нужно прилагать никаких усилий, чтобы обеспечить конфиденциальность передаваемых данных между филиалами. Решение SD-WAN позволяет гибко и быстро сегментировать сеть и обеспечивать селективную безопасность исходя из бизнес-задач и типа передаваемых данных в каждом отдельном сегменте. И эти функции доступны прямо «из коробки» – как только решение разворачивается, они тут же становятся доступны.

Возможность гибкой эксплуатации позволяет администратору управлять всей сетью из единого окна с помощью веб-интерфейса. Все настройки оборудования в каждом из отделений, все изменения в отдельном филиале или группе филиалов, смена сетевой топологии, подключение новых филиалов производятся централизованно согласно преднастроенным конфигурациям без необходимости какого-либо локального вмешательства. Например, при подключении в сеть нового оборудования автоматически применяются централизованные политики и настройки, и оно может быть сразу же запущено в эксплуатацию.

Обеспечение необходимого качества работы бизнес-приложений происходит благодаря использованию механизмов балансировки между доступными каналами связи исходя из замеров их параметров качества в реальном времени и оптимизации протоколов.

Говоря об облачных технологиях, подразумевается, что многие заказчики сегодня разворачивают свои сервисы в облаке, используя различные службы, такие как Amazon Web Services, Microsoft Azure, Office 365, Dropbox, приложения Google и другие. Все эти службы также имеют методы оптимизации в контексте архитектуры Cisco SD-WAN.

Особенности архитектуры SD-WAN

Архитектура Cisco SD-WAN состоит из трех основных компонентов, или плоскостей: плоскость передачи данных (Data Plane), плоскость управления (Control Plane) и плоскость администрирования, или оркестрации.

Первая плоскость – это плоскость передачи данных. Она представлена каналообразующим оборудованием, аппаратными или виртуальными маршрутизаторами, которые устанавливаются в офисах, филиалах и центрах обработки данных, и куда ведут каналы связи – выделенные каналы, MPLS, Интернет, 4G и т. д. Эти устройства направляют потоки трафика между этими каналами в зависимости от политик, установленных администратором. Они управляются централизованно с помощью специальных контроллеров.

vSmart-контроллеры представляют собой вторую плоскость – плоскость управления. Они передают маршрутизаторам централизованные политики и фактически указывают, как следует обеспечить связность между филиалами, как передавать трафик, как и где строить зашифрованные туннели между ними. vSmart-контроллеры управляются непосредственно администратором из плоскости оркестрации.

Третья плоскость, плоскость администрирования, представлена системой vManage. Это единая административная консоль с веб-интерфейсом, именно с ней взаимодействует администратор, и от нее «вниз» к контролерам поступают политики, затем передающиеся маршрутизаторам, раздающим трафик. vManage имеет открытый программный интерфейс (API), чтобы иметь возможность интегрироваться с внешними приложениями. Также к плоскости администрирования относится система vBond, которая отвечает за первоначальное подключение маршрутизаторов в сеть. Она является первичным узлом подключения и предоставляет каналообразующему оборудованию информацию, с какими контроллерами и какой системой управления ему следует взаимодействовать.

Между контроллерами и маршрутизаторами работает протокол плоскости управления, который называется Overlay Management Protocol (OMP). По этому протоколу контроллеры консультируют все маршрутизаторы относительно правил сетевой топологии и переадресации трафика различных приложений. Все коммуникации между контроллерами и маршрутизаторами происходят внутри DTLS-соединений, обеспечивающих шифрование передачи данных. Применение протокола OMP позволяет снизить нагрузку на каждый конкретный маршрутизатор. При традиционном подходе политики маршрутизации и построения VPN-туннелей необходимо прописывать отдельно для каждого маршрутизатора в каждом филиале. Взаимодействие происходит в линейном формате, поэтому снижается как вычислительная сложность на

самих маршрутизаторах, так и количество ресурсов, которые требуются для реализации там сетевых настроек. Между маршрутизаторами также по умолчанию устанавливаются шифрованные соединения – IPSec-туннели. Причем это происходит автоматически, как только разворачивается SD-WAN-фабрика. Если меняется сетевая топология, то IPSec-туннели автоматически перенастраиваются согласно новой топологии.

Кроме того, внутри IPSec-туннелей между маршрутизаторами также устанавливаются специальные BFD-сессии. Они дают возможность проверить жизнеспособность каналов связи между двумя площадками. Эти сессии работают по аналогии проверки пульса – если канал «падает», сессия нарушается, и сеть «понимает», что этот канал стал недоступен. А при увеличении задержки сессии – оповещает о том, что качественная характеристика канала поменялась.

Варианты развертывания

Фабрика SD-WAN имеет несколько вариантов развертывания. Если заказчик готов к облачному управлению, он может заказать оборудование, и центральные компоненты – плоскость управления и плоскость администрирования – будут развернуты под него в облаке Cisco, без необходимости подключения каких-либо дополнительных собственных ресурсов. Такой вариант предусматривает меньшие затраты времени на развертывание, и при этом заказчик избавлен от необходимости расходовать виртуальные ресурсы собственного ЦОД.

Весь комплекс может быть развернут в локальном или публичном центре обработки данных заказчика. В этом случае ему придется потратить определенные усилия, но при этом он получит определенный уровень закрытости своей сети.

SD-WAN-платформы

Существует несколько классов маршрутизаторов, которые поддерживают архитектуру SD-WAN. Первый – это маршрутизаторы vEdge, которые пришли из портфолио Viptela. Среди них есть модели с разной производительностью – 100 Мбит/с и 1/10/20 Гбит/с. Второй класс – это традиционные маршрутизаторы Cisco линеек ISR и ASR. Модели ASR предназначены для центральных офисов и центров обработки данных, ISR – для небольших и средних филиалов. Маршрутизаторы Cisco ISR можно использовать, установив на них специальное программное обеспечение. На этапе заказа, как правило, эти роутеры поступают к заказчику с этим ПО. Однако если у заказчика уже есть такие маршрутизаторы, можно доустановить его, таким образом переконвертировав оборудование в SD-WAN-совместимое. Также есть вариант, когда у заказчика есть сервисы в облаке MS Azure, Amazon Web Services или другого облачного провайдера – в нем можно установить виртуальные маршрутизаторы в виде виртуальных машин, которые также будут интегрированы в общую архитектуру, и использовать все преимущества SD-WAN.

Ключевые преимущества

При традиционных подходах в построении сети в ситуациях, когда филиал имеет несколько каналов связи, довольно сложно реализовать балансировку, то есть одновременное использование всех каналов. Обычно использовался один канал, и потоки трафика переключались на другие, когда основной пропадал. Это связано с определенными механизмами традиционных протоколов маршрутизации. Сложно реализовать систему Active/Active, когда два канала являются активными. Теперь появились механизмы, позволяющие одновременно использовать все доступные каналы связи несколькими способами. Трафик по умолчанию будет автоматически распределяться между всеми доступными каналами. Администратор может вносить изменения, применяя различные политики. Например, политику взвешенной балансировки, когда в каждый из каналов идет строго определенная пропорция трафика. Или принудительную политику, при которой трафик определенных приложений идет только в один канал (например, в выделенный канал MPLS), а в случае его отказа будет перенаправляться в другой (например, в Интернет). Есть возможность применить более «продвинутую» политику с учетом SLA, при котором происходит оценка качества канала связи и трафик приложения передается через него только в том случае, если его качественные характеристики соответствуют заданным.

Чтобы работала маршрутизация на основании состояния канала, нужно правильно определять тип трафика, который передается. В традиционных системах маршрутизации обычно используются протоколы и порты, что не позволяет определять конкретный тип приложения. В системе SD-WAN реализована технология глубокой инспекции пакетов (DPI), которая дает возможность «заглядывать» в заголовки и с помощью специальных метаданных определять передаваемое приложение. После этого можно обеспечить проверку этого трафика межсетевым экраном, обеспечить его приоритизацию и балансировку между различными каналами связи.

Еще одной важной функцией SD-WAN является сегментация сети. Сегодня во многих организациях есть различные подсистемы – например, корпоративные подсистемы, подсистемы гостевых пользователей, IoT, умный свет, системы контроля доступа и видеонаблюдения. И все они должны быть изолированы друг от друга, поскольку передают разные типы трафика и имеют различный уровень доверия. Cisco SD-WAN позволяет разделить их с точки зрения процессов маршрутизации. Формируются отдель-

Оптимизация TCP

Для расширения емкости каналов связи в Cisco SD-WAN есть функции, позволяющие оптимизировать передачу трафика, которая базируется на протоколе TCP. TCP включает в себя два вида трафика – сами данные, которые передаются, и контрольные сессии, позволяющие определять, как эти данные будут передаваться. При перегрузке канала для приложений, использующих протокол TCP, можно запустить механизм оптимизации, благодаря которому между двумя филиалами будет передаваться меньше контрольных данных. Это происходит за счет того, что маршрутизаторы будут терминировать TCP-сессии на себе, и посылать локальные подтверждения в сторону клиентских устройств. Таким образом, объем трафика будет снижен, что косвенно влияет на увеличение доступной полосы пропускания.

Варианты использования каналов Active/Active

ные сегменты сети – виртуальные частные сети (VPN), под каждую из которых создается своя виртуальная платформа маршрутизации (VRF). Маршрутизаторы разделяются на несколько виртуальных подмаршрутизаторов, каждый из которых имеет отдельные политики и процессы маршрутизации трафика. Когда трафик передается по сети между филиалами, каждый из таких сегментов помечается отдельной меткой. Это позволяет не смешивать трафик, а передавать его по отдельным микротуннелям, которые могут находиться внутри одного канала связи и внутри одного шифрованного IPSec-туннеля. Более того, под каждый из сегментов можно определить разный тип топологии. Например, для корпоративного сегмента можно построить полносвязную топологию, а для гостевого сегмента или систем видеонаблюдения – централизованную (Hub-and-Spoke).

Что касается работы со сторонними облачными сервисами, в SD-WAN реализованы несколько интересных технологий. Первая – Cloud onRamp for SaaS, которая при доступе к облачным приложениям, таким как Office 365, Salesforce, Dropbox и т. д., позволяет провести автоматическую оценку всех доступных интернет-соединений и определить качественную оценку каналов на предмет потерь и задержек для каждого из этих приложений. После чего трафик, который относится к этим приложениям, будет направлен в тот канал, который имеет более высокую оценку.

Вторая – Cloud onRamp for IaaS. Если заказчик имеет свои ресурсы в облаке Microsoft Azure или Amazon, есть возможность разместить там виртуальные маршрутизаторы (vEdge Cloud и CSR 1000V), которые будут напрямую интегрироваться в SD-WAN-фабрику. Это дает возможность создать полноценный ЦОД с точки зрения всего функционала SD-WAN. Все политики, которые распространяются на сеть заказчика, будут учитывать и виртуальные маршрутизаторы в удаленных облачных ресурсах.

Регистрация маршрутизаторов

На этапе заказа оборудования для заказчика создается учетная запись, где прописываются серийные номера всех заказанных маршрутизаторов. Когда маршрутизатор поступает на объект и подключается к сети, он автоматически отправляет запрос на внешний ресурс ztp.viptela.com и получает информацию о том, какой контроллер ему соответствует. Ресурс находится в центрах обработки данных Cisco, однако его можно разместить и на площадке заказчика, подменив его локальным адресом на DNS-сервере компании. Таким образом можно изолировать филиал от доступа в Интернет.

Функции безопасности

В последних релизах программного обеспечения Cisco SD-WAN появился целый ряд функций обеспечения безопасности. Они включают в себя межсетевой экран со знанием приложений, систему предотвращения вторжений (IPS), URL-фильтрацию, систему DNS безопасности и Advanced Malware Protection.

Межсетевой экран позволяет определять различные зоны безопасности и осуществлять зонированный доступ в сеть, инспектируя трафик между этими зонами на предмет сетевых аномалий. МСЭ разрешает или блокирует трафик категории приложений или отдельного приложения. На данный момент реализована классификация более 1400 приложений.

Система предотвращения вторжений позволяет с помощью заранее описанных специальных шаблонов инспектировать входящий трафик на предмет угроз. IPS в SD-WAN связана с Cisco Talos, обновления сигнатур происходят автоматически и регулярно.

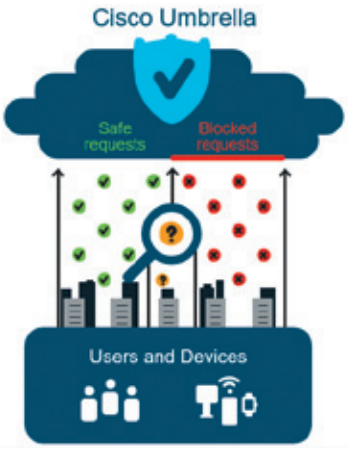
Система URL-фильтрации позволяет определить, какие ресурсы могут посещать пользователи. Определяется категория и репутация сайтов, на основе которых настраиваются политики доступа. Кроме того, предусмотрены индивидуально настраиваемые черные и белые списки веб-ресурсов.

DNS-безопасность дает возможность переправлять запросы к DNS-серверу на сервис Cisco Umbrella, в котором уже существуют белые и черные списки всех доменных имен по всему миру. В зависимости от того, в каком из этих списков находится запрашиваемый ресурс, пользователь либо получит доступ к нему, либо нет.

Advanced Malware Protection представляет собой наиболее продвинутую систему безопасности, анализирующую все входящие файлы на предмет легитимности. Для этого реализована синхронизация с облаком Cisco Talos, где содержится информация обо всех известных файлах, передающихся в Интернете. Если поступающий файл известен и является зловредным, он будет забло-

Система предотвращения вторжений инспектирует входящий трафик с помощью заранее описанных шаблонов

Система DNS безопасности использует в своей работе облачный сервис Cisco Umbrella



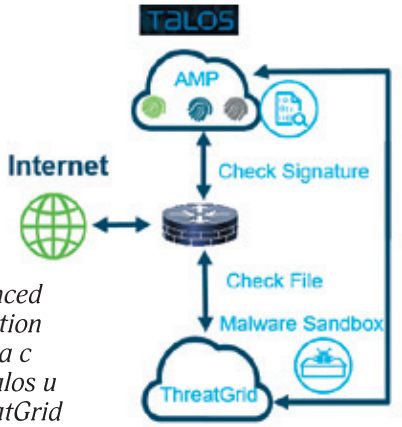
кирован, если безопасным – будет передаваться беспрепятственно. В случае, если данных о файле в облаке нет, он может быть направлен в «песочницу» для последующего анализа. Здесь снимается специальный хеш, своего рода отпечатки файла, и отправляется в облако для изучения, после чего файл получает определенную классификацию.

Важным аспектом является поддержка функций безопасности на оборудовании SD-WAN. Они полностью поддерживаются на маршрутизаторах Cisco ISR. А вот на моделях vEdge некоторые из этих функций не поддерживаются – в частности, IPS, URL-фильтрация и AMP. Причина этого в том, что для их работы требуется контейнеризация – выделение отдельных ресурсов для определенных процессов. Маршрутизаторы серии ISR требуют доукомплектовки дополнительной памятью и флеш-памятью. На моделях vEdge такая модернизация невозможна.

С помощью функций безопасности, доступных на маршрутизаторах SD-WAN, появляется возможность обеспечить прямой безопасный доступ в Интернет (DIA – Direct Internet Access) в филиале для необходимых приложений. Это могут быть SaaS-приложения (например, Office 365), выход в Интернет для сотрудников или только для гостевых пользователей. Таким образом, потоки трафика становятся более оптимальными – не загружаются WAN-каналы и обеспечивается безопасность интернет-подключений.

Виды подписок

Что нужно для развертывания сети SD-WAN? Все, что необходимо – приобрести маршрутизатор и подписку на него. Центральные компоненты, равно как и различные дополнительные устройства, которые будут работать в сети, не лицензируются.



Система Advanced Malware Protection интегрирована с облаком Cisco Talos и песочницей ThreatGrid

Есть несколько типов подписки. Также существует ряд факторов, на который стоит обратить внимание заказчику при выборе нужного типа подписки. Первый – это функциональность. Базовый сервис SD-WAN доступен в подписке DNA Essentials. Он включает в себя централизованное управление, автоматическое построение шифрованных туннелей, возможность применять принудительные политики маршрутизации, балансировку между всеми доступными каналами связи, маршрутизацию трафика приложений на основании качественных характеристик канала, возможность определять тип передающегося трафика, а также функции безопасности (Firewall, IPS, DNS-безопасность). Класс подписки DNA Essentials доступен тем компаниям, которые имеют в своем распоряжении до 50 филиальных маршрутизаторов.

Для того, чтобы использовать «продвинутые» возможности, такие как автоматическая работа с облачными сервисами, сегментация сети, функции безопасности URL-фильтрации и Anti-Malware Protection, функционал расширенной аналитики и прогнозирования загрузки каналов связи и качества работы приложений, необходима подписка DNA Advantage. Она же будет включать в себя класс DNA Essentials. Для того, чтобы использовать функцию «песочницы» в системе AMP, понадобится лицензия DNA Premier.

Приобретаются подписки на три или пять лет.

Помимо функциональности и срока действия, стоит учитывать и полосу пропускания. Нет необходимости приобретать подписку полностью на тот уровень производительности, который поддерживается аппаратно. Например, если заказчик покупает устройство производительностью 100 Мбит/с и при этом имеет два канала связи с полосой пропускания по 5 Мбит/с, достаточно подписки, активирующей производительность в 10 Мбит/с. В дальнейшем при увеличении числа каналов или росте их емкости можно перейти на подписку с более высокой полосой пропускания.

Также при заказе необходимо выбрать тип внедрения – либо все компоненты будут разворачиваться в облаке Cisco, либо заказчик получает возможность загрузить программное обеспечение и развернуть все локально. Стоит отметить, что итоговая стоимость подписки не зависит от типа внедрения.

По вопросам обращаться: *cisco@muk.ua*.

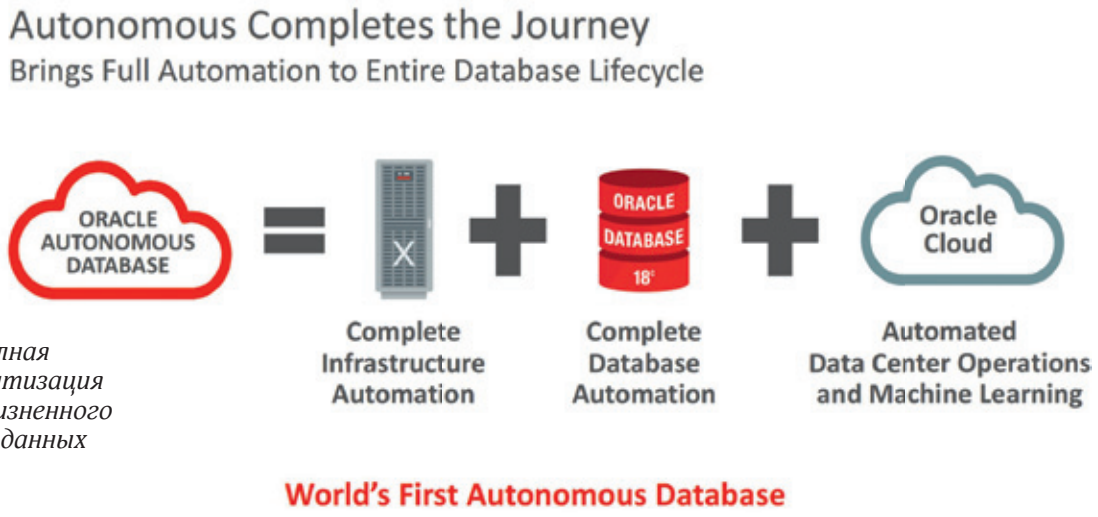
ORACLE AUTONOMOUS DATABASE: РЕВОЛЮЦИОННАЯ АВТОНОМНОСТЬ

Облачная версия одной из самых популярных корпоративных баз данных в мире – Oracle Database – обзавелась автономными функциями. Что подобная функциональность дает на практике? Как работает? Что ожидать дальше? Попробуем разобраться.

Oracle Autonomous Database – это облачный сервис, работающий на фирменном оборудовании Oracle Exadata Database Machine, которое специально разработано и настроено для высокопроизводительных рабочих нагрузок. В компании заявляют, что Autonomous Database является первой в мире технологией автономного управления данными в облаке, которая обеспечивает автоматизированные процессы исправления ошибок, обновления и настройки. Звучит действительно здорово: люди, работающие с базами данных, знают, сколько времени отнимает рутина. К тому же, в режиме ручного управления неизбежно появляются ошибки, вызванные человеческим фактором. Тут такая проблема отпадает сама собой. Еще один плюс – уменьшение размера эксплуатационных расходов за счет сокращения дорогостоящего ручного администрирования баз данных.

Основные возможности

Если говорить более конкретно, то автономная база открывает перед пользователями множество возможностей, которые были недоступны раньше. Поговорим о них поподробнее, но сначала выделим



Полная автоматизация всего жизненного цикла данных

одну особенность. В локальных центрах обработки данных программное обеспечение может работать на любом оборудовании, любой операционной системе, любом типе подключения к сети и диску и любых типах драйверов устройств. В отличие от такого подхода, Oracle Autonomous Database разработана специально для аппаратной платформы Oracle Exadata. С одной стороны, это ограничивает область ее применения – многие компании не захотят моментально переходить на этот продукт, особенно если инвестировали средства в собственные ЦОД и конкретное оборудование там. Но с другой – таким образом Oracle использует преимущества стандартизации для обеспечения полного контроля над средой выполнения. А это для многих клиентов может быть весомым аргументом в пользу использования этого продукта.

Как бы там ни было, Oracle Autonomous Database имеет ряд преимуществ перед обычными системами баз данных. Одно из них – это быстрота развертки. На создание с нуля крупномасштабной базы данных может уйти много времени, а именно – до нескольких недель (если речь идет о закупке и установке нового оборудования в ЦОДе). С использованием Oracle Autonomous Database новые БД любого масштаба создаются очень быстро, буквально за несколько минут.

Настройка и поддержание базы данных в актуальном состоянии – тоже важный вопрос. При работе с обычными БД их конфигурация и оптимизация зачастую осуществляются один раз – при создании и заполнении. Со временем (а это могут быть годы) база растет, меняются запросы к ней, накапливаются ошибки и т. д. В Autonomous Database система подстраивается под нужды пользователей, анализируя их запросы и работу в целом. База обновляется каждый день и всегда предлагает оптимальные настройки системы, в том числе при помощи машинного обучения и адаптивных алгоритмов. Также сервис автоматически применяет исправления и обновления, при этом база данных продолжает работать и оставаться доступной для пользователей. Такой подход не только минимизирует время простоя, но и гарантирует, что БД каждого клиента всегда работает с последними обновлениями.

Автономность – легкое, безграничное, неуязвимое облако данных

Архитектура и механизмы продукта

В основе продукта лежит СУБД Oracle версии 18c и выше. Как уже было сказано ранее, Autonomous Database работает на базе облачных сервисов Oracle и в отрыве от них применяться не может. Единственное исключение – использование Oracle Cloud at Customer. Это облако, которое устанавливается непосредственно в центре обработки данных клиента и администрируется сотрудниками Oracle удаленно. Также в состав продукта входят некоторые фирменные программные решения. Среди них – средства, обеспечивающие гибридное сжатие,

Одно из ключевых преимуществ Oracle Autonomous Database перед обычными системами баз данных – это быстрота развертки, на это требуется буквально несколько минут

Машинное обучение на службе автономности

Машинное обучение – это один из основных элементов обеспечения корректной работы Autonomous Database. Оно применяется при защите БД от внешнего и внутреннего вторжения, в работе служб технической поддержки для определения самых важных и приоритетных для исправления ошибок и т. д. Выявление проблем и неполадок выполняется по такой схеме: продукт автоматически выстраивает базовую модель нормального поведения системы, после чего при работе базы данных определяются отклонения от нее. Модели, используемые для этих целей, генерируются с помощью алгоритмов машинного обучения. Также с их помощью эти модели постоянно обновляются и улучшаются.

При обнаружении отклонений от моделей базового поведения определяются причины таких ситуаций, а также выявляются тенденции ухудшения работы. После этого система в автоматическом режиме может провести коррекцию, чтобы вернуть работу системы в нужное русло.

шифрование данных, разделение и приоритизацию ресурсов ввода/вывода, параллельную обработку запросов и др. Всего же Autonomous Database предлагает пользователям более 50 разнообразных инструментов и механизмов для улучшения работы и производительности. Одних только советчиков (которые дают рекомендации по улучшению работы БД и ее оптимальной настройке) есть более 10.

Сервис Autonomous Transaction Processing равномерно распределяет ресурсы между такими задачами, как проведение транзакций, генерация отчетов, пакетная обработка данных, задачи Интернета вещей и машинное обучение

Администрирование всех элементов автономной базы данных (от оборудования до программного обеспечения) осуществляется специалистами Oracle. Сюда относятся поддержание работоспособности, своевременное обновление, выпуск заплаток и т. д. Все эти процедуры происходят практически без перерывов в работе. По заявлениям разработчиков, уровень надежности сервиса составляет 99,995 %. Это значит, что максимальное время простоя Autonomous Database составляет 2,5 минуты в месяц или 30 минут в год. К этому времени относятся не только сбои и их устранение, но и регламентные работы.

Важным элементом Autonomous Database также является функция самовосстановления. В зависимости от требований пользователей, она умеет создавать защиту от сбоя узла, резервные базы данных, которые используются в случае сбоев, выполнять аварийную перезагрузку и использовать другие подобные механизмы. Также для обеспечения защиты от взлома и хакерских атак платформа шифрует все данные баз данных, в автоматическом режиме устанавливает патчи безопасности, как только они выходят. Механизмы машинного обучения и инструменты аудита позволяют выявлять внешние атаки и злонамеренные действия инсайдеров.

Наподобие большинства других облачных сервисов, Autonomous Database – это эластичный продукт. По мере необходимости клиенты могут увеличивать или уменьшать объем дискового пространства и количество используемых процессоров. Это позволяет существенно экономить средства: оплата работы БД осуществляется только по факту использования ресурсов, а значит, в нерабочее время их количество можно снижать до минимально необходимого уровня. По словам представителей компании, экономия может составлять до 80 %.

Как универсальная СУБД, Autonomous Database может использоваться для создания широкого спектра систем. Это и DSS, и OLTP, и хранилища данных, и множество других вариантов использования. Причем для наиболее эффективной работы можно заказать конкретный специализированный сервис. В таком случае новосозданная БД будет автоматически настроена под выполнение конкретных задач, что обеспечит максимальную продуктивность работы. В Oracle планируют выпустить автономный сервис для OLTP-систем и смешанной нагрузки, а также отдельные сервисы для работы с графами, документами, NoSQL и т. д.

На данный момент пользователям доступен сервис Oracle Autonomous Data Warehouse Cloud Service (ADWS). Его архитектура дает возможность создавать БД для витрины или хранилища данных. Работа с сервисом осуществляется в том числе через SQL Developer, также поддерживается интеграция других систем через фирменные инструменты Oracle или же сторонних производителей. Работать эти сервисы могут как в локальном центре обработки данных, так и в облаке. Для загрузки данных в таблицы созданного хранилища их нужно поместить на облачную систему Oracle (Oracle Object Storage) или Amazon. В базе данных есть процедура для загрузки этих данных или для работы с ними как с внешними таблицами.

Еще один сервис – Oracle Autonomous Transaction Processing – поддерживает комплексное сочетание нагрузок. Он равномерно распределяет ресурсы между такими задачами, как проведение транзакций, генерация отчетов, пакетная обработка данных, задачи Интернета вещей и машинное обучение. И все это в рамках одной базы данных. Такой подход позволяет упростить разработку и развертывание приложений, реализовать аналитику в реальном времени, использовать возможности персонализации и функции обнаружения мошенничества в применении к реальным транзакционным данным.

Администраторы больше не нужны?

Если база данных действительно автономна, а на ее развертку уходят считанные минуты и несколько кликов мышью, то, возможно, администраторы БД в скором времени останутся без работы? Такая мысль действительно может проскочить, когда читаешь про Autonomous Database. Но на самом деле это далеко не так. У администраторов остается множество функций, которые машина выполнить не может. Это, например, загрузка данных или миграция. Важно понимать, что автономная база данных автоматизирует прежде всего рутинные задачи. А высвобождение времени позволит администраторам, во-первых, поддерживать больше баз данных, во-вторых, больше времени уделять инновационным проектам, а в-третьих, осваивать новые инструменты и модели работы с БД. Конечно, роль администраторов со временем изменится. Но говорить об исчезновении их как класса, конечно, не приходится.

По вопросам обращаться: *oracle@muk.ua*.

ОБЛЕГЧАЕМ ЖИЗНЬ:

О НОВЫХ ВАРИАНТАХ ПОДПИСКИ И УДОБНЫХ ИНСТРУМЕНТАХ ДЛЯ ОБЛАЧНЫХ СЕРВИСОВ MICROSOFT

Корпорация Microsoft представила новые сценарии подписок на ряд своих облачных сервисов. О том, как они работают и почему стоит обратить на них внимание, а также о некоторых инструментах, облегчающих работу в целом, читайте далее

Одна из ключевых возможностей новых бизнес-сценариев от редмондской корпорации – это приобретение подписок на один или три года для ключевых продуктов, среди которых – Windows Server, SQL Server, клиентские подключения к удаленным рабочим столам и зарезервированные виртуальные машины Azure. Такие возможности позволяют клиентам существенно экономить, так как подписка обходится намного дешевле, чем другие методы оплаты. Кроме того, у данного подхода есть еще ряд преимуществ. Появляется возможность отменить или изменить вариант подписки, что обеспечивает гибкость использования ресурсов. Управлять зарезервированными экземплярами можно на уровне как всей организации, так и конкретных отделов, что обеспечивает большее удобство в управлении и администрировании. Подписки также помогают финансовым отделам, ведь планировать расходы с учетом разовых платежей за год или три использования сервисов намного легче, чем при оплате по факту.

Если говорить о возможности резервирования подробнее, то в первую очередь такой вариант использования позволяет экономить деньги благодаря внесению предоплаты за использование виртуальных машин, вычислительных мощностей баз данных SQL, пропускной способности Azure Cosmos DB или других ресурсов Azure. Фактически, предоплата дает существенную скидку по сравнению с моделью расчетов по факту. В Microsoft заявляют, что общая экономия может составлять до 72 %. Если говорить более конкретно, то экономия по сравнению с моделью оплаты по мере использования на хранилище данных SQL составляет до 65 %, на базе данных SQL Azure составляет до 80 %, на Azure Cosmos DB – до 65 %, на виртуальных машинах Windows – до 80 %, а Linux – до 60 %.

Приобретение подписок будет наиболее полезно тем компаниям, которые используют виртуализированные мощности, Azure Cosmos DB или баз данных SQL, работающие длительное время. Например, если на предприятии работают сразу пять разных служб, плата идет за все сервисы, исходя из времени работы служб. При резервировании это прекращается, а к ресурсам больше не будет применяться оплата по мере использования. При этом стоит помнить, что резервирование покрывает только конкретные ресурсы (например, виртуальные машины), но не включает оплату дополнительного программного обеспечения, сетей и хранилищ. А при резервировании ядер баз данных SQL покрываются расходы только на вычислительные ресурсы, включенные в подписку, а лицензия оплачивается отдельно.

Работа с подписками предусматривает дальнейшее управление ими: заплатив за конкретную под-

Простая миграция писем, календарей, задач с Exchange Server в Office 365

Для организации миграции, архивирования и создания резервных копий данных в Office 365, а также расширения функциональности подписок Microsoft можно воспользоваться рядом сторонних продуктов

писку, пользователь впоследствии может изменить ее условия, грубо говоря, отредактировать. Например, можно применить резервирование к другой подписке, изменить права на управление резервированием или саму область резервирования. Также можно разделить резервирование на две части для применения некоторых приобретенных экземпляров к другой подписке. Как видим, гибкость довольно большая. То же касается и зарезервированных виртуальных машин Azure. Для них доступно изменение настройки оптимизации резервирования, а скидка может применяться к виртуальным машинам в одной и той же серии. Кроме того, можно зарезервировать ресурсы центра обработки данных для определенного размера виртуальной машины.

Зарезервированные ресурсы могут распределяться между разными пользователями в зависимости от пожеланий администратора. По умолчанию именно заказавший резервирование администратор учетной записи имеет права на распределение заказа и управление подпиской. При этом, когда администратор дает другим пользователям разрешение на управление заказом, они не получают права на управление подпиской. И наоборот, при предоставлении кому-либо прав на управление подпиской, права на управление заказами также не передаются. В целом Microsoft предоставляет очень широкие возможности по настройке и управлению зарезервированными ресурсами, что вместе с выгодной ценой на предоплату делает такую модель работы весьма привлекательной для корпоративных клиентов.

Еще один важный вопрос – это комфортная миграция, архивирование и создание резервных копий данных в Office 365, а также расширение функциональности подписок Microsoft. Для этого можно воспользоваться рядом сторонних продуктов. Расскажем о них вкратце и начнем с архивирования и резервного копирования. Для этой цели можно воспользоваться инструментом Dropsuite. Он позволяет осуществлять безопасное резервное копирование и восстановление почтовых сообщений, вложений, контактов, событий календаря, объектов Exchange Online, SharePoint, OneDrive. Все это происходит в автоматическом режиме незаметно для пользователя – нужно всего лишь один раз настроить программу. При этом инструмент предлагает неограниченный объем и срок хранения данных, а также надежное шифрование резервных копий при помощи 256-битного алгоритма и защиту доступа с использованием протоколов TLS или SSL. Еще одна полезная функция Dropsuite – поддержка резервного копирования и восстановления общих файлов групп и команд Microsoft. Подобная модель работы становится все более популярной во многих предприятиях, так что защита их рабочих данных тоже будет нелишней.

С помощью Dropsuite можно осуществлять и миграцию данных, но для этого также есть отдельные инструменты с большей функциональностью. Один из них называется MigrationWiz. Это облачное решение, работающее по модели SaaS, которое многие эксперты и пользователи *https://g2.com/products/bittitan/reviews* называют одним из лучших подобного рода продуктов. Оно работает не только с сервисами Microsoft и позволяет переносить сообщения электронной почты практически из любого источника в любое место назначения. MigrationWiz очень прост в работе, для этого не нужно проходить специальное обучение или сертификацию. Средство применяется к таким видам данных, как сообщения электронной почты, офисные документы, профили Outlook и разнообразные типы пользовательских файлов, которые нужно перенести на новое место.

Целый ряд полезных инструментов для миграции и повышения уровня безопасности предлагает пользователям компания Quest Software. Например, семейство продуктов для миграции и управления

В ногу со временем

Хороший повод перейти на новую модель подписок появится совсем скоро. Некоторые версии популярных продуктов Microsoft перестанут поддерживаться в ближайшее время, а значит, их использование станет не только нецелесообразным, но и небезопасным. Среди этих продуктов – SQL Server 2008 (в том числе облачный вариант) и Windows Server 2008, R2. Для SQL Server дата окончания поддержки – 9 июля 2019 года, а для Windows Server – 14 января 2020 года. Переход на инструменты Azure (например, SQL Azure, служба приложений Azure и IaaS Azure) при этом поможет модернизировать бизнес-приложения и привести их в соответствие с современными требованиями. И, конечно, оптимизировать расходы – использование новых подписок дает возможность сэкономить до 40 % на виртуальных машинах. Переход осуществляется максимально просто и практически без изменений кода приложений в управляемом экземпляре базы данных SQL Azure. Также можно перейти не только на облачные варианты инструментов, но и на новые версии продуктов, использующихся локально, например, SQL Server 2017. Это также повысит безопасность работы, а переход не потребует много усилий.

Миграция почты с сохранением всех вложений

Инструмент MigrationWiz от Dropsuite – это облачное решение, работающее по модели SaaS, поддерживающее не только сервисы Microsoft, но и продукты других производителей, которое позволяет переносить сообщения электронной почты практически из любого источника в любое место назначения

Quest Change auditor – гибридное решение для обеспечения безопасности в реальном времени и ИТ-аудита инфраструктуры

Quest Microsoft Platform Management с возможностью ZeroIMPACT позволяет проводить миграцию и консолидацию данных для таких продуктов Microsoft, как Active Directory, Exchange, SharePoint, Office 365 и OneDrive for Business. Продукт содержит целый ряд решений для разных задач, которые можно приобретать по отдельности. Для миграции, например, доступны инструменты, которые позволяют существенно сократить время, риски и затраты на данную процедуру. Данные инструменты позволяют скрупулезно планировать процессы, определять необходимый для переноса контент (пользователей, почтовые ящики, общие файловые ресурсы, приложения, другие объекты) и еще на стадии планирования показывают все возможные риски, что в конечном счете помогает предотвратить ошибки в этой сложной процедуре.

Помимо этого присутствуют средства для безопасного копирования и восстановления информации, защиты данных, переноса почтовых архивов и т. д. Также решения платформы ZeroIMPACT оптимизируют повседневные задачи администрирования для Office 365, Active Directory, Exchange, OneDrive for Business, Skype for Business и др., что позволяет сотрудникам ИТ-отделов больше времени уделять решению иных, более важных вопросов работы предприятия.

Отдельное решение под названием Change Auditor отвечает за проведение аудита и обеспечения безопасности в режиме реального времени для среды продуктов Microsoft. Оно проводит всестороннюю экспертизу и комплексный мониторинг безопасности для всех ключевых настроек, изменений, вносимых пользователями и администраторами Microsoft Active Directory, Azure AD, Exchange, Office 365, Exchange Online, файловых серверов и др. Инструмент также отслеживает все действия пользователей и умеет определять их аномальную активность. При этом происходит автоматическое ранжирование учетных записей с разными уровнями рисков, идентифицируются потенциальные угрозы безопасности, исходящие от них, и при этом снижается количество ложных срабатываний систем безопасности. Также Change Auditor работает с Windows Server и SQL Server. Средство умеет в режиме реального времени отслеживать и оповещать обо всех изменениях в этих системах, в том числе действиях пользователей и администраторов. В случае сбоев инструмент предоставляет текущие и исходные параметры состояния системы, что позволяет быстро устранить неполадки. Подобные функции доступны и для VMware vCenter Server, Skype for Business/Lync и других популярных продуктов.

Для улучшения работы базы данных SQL Server можно использовать продукт Toad for SQL Server. Он призван бороться с распространенными проблемами – снижением производительности SQL Server при большом количестве баз данных и сложностью их администрирования. Это средство автоматизирует множество процессов, дает понятные и простые в использовании инструменты, дополняющие арсенал штатных средств Microsoft.

По вопросам обращаться: *microsoft@muk.ua*.

НА ВСЕ СЛУЧАИ ЖИЗНИ:

ОБЗОР НОВЫХ ЛИНЕЕК ИБП ОТ APC

Вопросы качественного энергообеспечения оборудования – одни из самых главных при организации работы предприятия. Использование источников бесперебойного питания играет тут не последнюю роль

Разумеется, сами ИБП бывают разные – от компактных для персонального компьютера до устройств промышленного уровня, используемых в центрах обработки данных. APC by Schneider Electric предлагает ИБП разного уровня. Далее поговорим о новых линейках устройств для использования в офисах компаний малого и среднего бизнеса.

Easy UPS 3S

Еще несколько десятков лет назад трехфазные источники бесперебойного питания использовались только в крупнейших центрах обработки данных и на больших предприятиях. Причина – их громоздкость, дороговизна и сложность в обслуживании. Сейчас же необходимость в подобного рода устройствах могут почувствовать даже предприятия сегмента SMB. Трехфазные ИБП могут понадобиться из-за распространения новых типов устройств. Это, например, 3D-принтеры и станки с числовым программным управлением, которые постепенно вытесняют более привычное оборудование. Таким образом, все большему числу организаций нужны компактные, недорогие и предельно простые в обслуживании трехфазные источники бесперебойного питания.

Линейка продуктов Easy UPS 3S – это трехфазные ИБП мощностью 10–40 кВА. Данные устройства предназначены для использования в компаниях малого и среднего бизнеса, сфере здравоохранения и телекоммуникаций, офисных зданиях, небольших ЦОД и серверных комнатах. Их отличительная черта – высокий КПД (до 96 % в обычном режиме и до 99 % в энергосберегающем режиме), простота установки, настройки и использования, а также возможность параллельного подключения нескольких устройств.

Всего в линейке Easy UPS 3S есть два типа устройств: без встроенных батарей, для использования с аккумуляторами сторонних производителей, и со встроенными

Easy UPS 3S отличаются высоким КПД, простотой установки, настройки и использования, а также возможностью параллельного подключения нескольких устройств

батареями. Максимальная выходная мощность устройств варьируется от 10 до 40 кВА. Работать источники бесперебойного питания могут при температурах от 0 до 40 °С и влажности до 95 % (без образования конденсата). Самые мощные из них, модели «все-в-одном» со встроенными модульными аккумуляторами, обеспечивают до 11 минут автономной работы при 100-процентной нагрузке 40 кВА. Кроме того, из этих ИБП можно формировать группу, параллельно подключая до четырех устройств. Тем самым повышается отказоустойчивость системы либо увеличивается мощность системы ИБП.

Размеры корпуса у разных моделей источников бесперебойного питания отличаются. Например, для ИБП мощностью 10 кВА и с внешними аккумуляторами габариты составляют 53x25x70 см. А вот у устройства мощностью

Easy UPS 3S

Номинальная мощность (кВА / кВт)	10/10	15/15	20/20	30/30	40/40
Номинальное входящее напряжение (В)	380/400/415	380/400/415	380/400/415	380/400/415	380/400/415
Входящая частота, Гц	45 – 65	45 – 65	45 – 65	45 – 65	45 – 65
Номинальное входящее напряжение (В)	304 – 477	304 – 477	304 – 477	304 – 477	304 – 477
Коэффициент напряжения	до 0,99	до 0,99	до 0,99	до 0,99	до 0,99
Номинальное исходящее напряжение (В)	220/230/240 при подключении 3:1	220/230/240 при подключении 3:1	220/230/240 при подключении 3:1	220/230/240 при подключении 3:1	220/230/240 при подключении 3:1
	380/400/415 при подключении 3:3	380/400/415 при подключении 3:3	380/400/415 при подключении 3:3	380/400/415 при подключении 3:3	380/400/415 при подключении 3:3
Энергоэффективность	до 96 % в режиме двойного преобразования	до 96 % в режиме двойного преобразования	до 96 % в режиме двойного преобразования	до 96 % в режиме двойного преобразования	до 96 % в режиме двойного преобразования
	до 99 % в режиме ECO	до 99 % в режиме ECO	до 99 % в режиме ECO	до 99 % в режиме ECO	до 99 % в режиме ECO

40 кВА, работающего по принципу «все-в-одном», они явно посолиднее – 1400x500x969 мм. Все модели линейки обладают надежной защитой от воздействия окружающей среды. У них есть съемные пылезащитные фильтры на магнитных защелках, которые можно снимать для чистки и снова ставить на место без использования специальных инструментов. Это позволяет использовать их даже в местах, где чисто бывает далеко не всегда.

Простота использования этих источников бесперебойного питания обнаруживается уже на начальных этапах работы. Благодаря тому, что они довольно компактны и мало весят, проблем с их размещением возникнуть не должно. Перед подключением оборудование можно протестировать при помощи функции нагрузочного тестирования даже без нагрузочного модуля и необходимости полной зарядки, так что проверить работоспособность конкретного ИБП можно очень быстро.

При установке дополнительной сетевой карты (ее

Easy UPS 1Ph Online Rack Mount Models

Модель	SRV1KRI	SRV2KRI	SRV3KRI	SRV6KRI	SRV10KRI
Номинальное входящее напряжение (В)	220-240	220-240	220-240	220-240	220-240
Входящее соединение	IEC C14	IEC C14	IEC C20	Клеммная колодка	Клеммная колодка
Входящая частота, Гц	50/60	50/60	50/60	50/60	50/60
Диапазон входящего напряжения (В)	110 – 285 @ 50 % нагрузки	110 – 285 @ 50 % нагрузки	110 – 285 @ 50 % нагрузки	110 – 300 +/- 3 % @ 60% нагрузки	110 – 300 +/- 3 % @ 60% нагрузки
Коэффициент напряжения	≥ 0,95	≥ 0,95	≥ 0,95	≥ 0,99	≥ 0,99
Исходящая мощность (Вт)	800	1600	2400	6000	10000
Исходящая мощность (ВА)	1000	2000	3000	6000	10000
Номинальное исходящее напряжение (В)	220/230/240	220/230/240	220/230/240	220/230/240	220/230/240
Диапазон частот, Гц (работа от сети)	50/60 +/- 3	50/60 +/- 3	50/60 +/- 3	50/60 +/- 4	50/60 +/- 4
Регулирование переменного тока	+/- 1 %	+/- 1 %	+/- 1 %	+/- 1 %	+/- 1 %
Диапазон частот, Гц (работа от батареи)	50 +/- 0,5 или 60 +/- 0,5	50 +/- 0,5 или 60 +/- 0,5	50 +/- 0,5 или 60 +/- 0,5	50 +/- 0,1 или 60 +/- 0,1	50 +/- 0,1 или 60 +/- 0,1
Энергоэффективность (переменный ток)	88 %	88 %	88 %	94 %	94 %
Тип батареи	Свинцово-кислотная	Свинцово-кислотная	Свинцово-кислотная	Свинцово-кислотная	Свинцово-кислотная
Пик-фактор	3:1	3:1	3:1	3:1	3:1

APC Easy UPS 1Ph Online

Модель	SRV1KI	SRV2KI	SRV3KI	SRV6KI	SRV10KI
Номинальное входящее напряжение (В)	220/230/240	220/230/240	220/230/240	220/230/240	220/230/240
Входящее соединение	IEC C14	IEC C14	IEC C20	Клеммная колодка	Клеммная колодка
Входящая частота, Гц	40 – 70	40 – 70	40 – 70	40 – 70	40 – 70
Диапазон входящего напряжения (В)	110 – 300 при загрузке 60 %	110 – 300 при загрузке 60 %	110 – 300 при загрузке 60 %	110 – 300 при загрузке 60 %	110 – 300 при загрузке 60 %
Исходящая мощность (Вт)	800	1600	2400	6000	10 000
Исходящая мощность (ВА)	1000	2000	3000	6000	10 000
Номинальное исходящее напряжение (В)	220/230/240	220/230/240	220/230/240	220/230/240	220/230/240
Диапазон частот, Гц (работа от сети)	47 – 53	47 – 53	47 – 53	50 или 60 +/- 0,1	50 или 60 +/- 0,1
Тип батареи	12 V/9 AH X 2	12 V/9 AH X 4	12 V/9 AH X 6	12 V/7 AH X 16	12 V/9 AH X 16

можно приобрести опционально) управление устройствами осуществляется через веб-интерфейс. Отслеживать производительность и другие параметры можно при помощи специальных приложений, в том числе фирменного сервиса EcoStruxure Asset Advisor, который доступен через облако с мобильных устройств – смартфонов и планшетов. Как это работает? При установке фирменной сетевой карты у источников бесперебойного питания серии Easy UPS появляется интеграция с платформой EcoStruxure. Эта служба реализована на основе интернета вещей и применяется в жилых домах, промышленных зданиях, центрах обработки данных, инфраструктуре и различных отраслях промышленности. Если говорить о функциях этой системы в контексте работы с источниками бесперебойного питания, то она позволяет легко мониторить состояние устройств, показывая всю важную информацию о них через Интернет. Также она позволяет удаленно решать некоторые возникающие проблемы и имеет систему умного мониторинга.

Еще одна важная функция данной линейки – возможность холодного старта устройств. Она дает возможность включать ИБП даже при отсутствии напряжения в сети (естественно, для этого должны быть заряжены аккумуляторы). Это позволяет обеспечить питание подключенных устройств в экстренном режиме.

Источники бесперебойниого питания Easy UPS 1 Ph Online поставляются в двух форм-факторах: обычном tower-варианте, а также стоечном (rack) исполнении

APC Easy UPS 1 Ph Online

Однофазные источники бесперебойного питания Easy UPS 1 Ph Online – это устройства мощностью до 10 кВА с топологией двойного преобразования и широким диапазоном поддерживаемых напряжений. Данные ИБП обеспечивают полноценную защиту от перебоев в работе электросети. Они предназначены для использования на предприятиях среднего и малого бизнеса. Устройства поставляются в двух форм-факторах: обычном tower-варианте, а также стоечном (rack) исполнении. Всего в каждой линейке доступно по пять моделей устройств (а также их вариации).

Технические характеристики как обычных, так и стоечных устройств практически не отличаются. Например, самые производительные из них имеют выходную мощность (как уже было сказано выше) в 10 кВА, а зарядка батарей до 90 % после полной разрядки занимает приблизительно 4 ч.

Обе разновидности устройств могут опционально оснащаться сетевой картой Simple Network Management Protocol (SNMP). Это позволит существенно облегчить управление оборудованием и его мониторинг. Например, можно удаленно узнавать заряд и состояние батареи, вольтаж, нагрузку на ИБП и состояние окружающей среды (температуру и влажность). Также поддерживаются простейшие функции управления. Так, при помощи этой карты можно удаленно выключать и перезагружать серверы.

По вопросам обращаться: *apc@muk.ua*.

Smart-UPS On-Line 230 V

Unity output power factor single-phase, double-conversion online UPS with advanced management features

Lean more

A13945

apc.com

Life Is On

APC by Schneider Electric

КОММУНИКАЦИИ ДЛЯ ВСЕХ:

СЕРВЕР ВИДЕОКОНФЕРЕНЦИЙ GRANDSTREAM IPVT10

То, что организация многоточечных видеоконференций в формате Full HD – удел лишь крупных предприятий, сегодня становится все большим и большим заблуждением. Одно из доказательств тому – вышедший на рынок в конце прошлого года сервер видеоконференций IPVT10 от Grandstream Networks

Развитие облачных сервисов делает видеоконференции доступными для всех, позволяя организовывать их без привязки к специализированному оборудованию. Так, в последнее время все большей популярностью пользуется сервис IPVideoTalk от Grandstream. Он представляет собой аудио-, видео- и веб-конференц-сервис, который позволяет участникам присоединяться к встрече из любой точки земного шара. С его помощью можно легко организовать конференции с большим количеством участников – достаточно получить приглашение по электронной почте и в назначенное время войти в конференцию с помощью браузера или установленного на мобильное устройство приложения.

Однако облачные сервисы по тем или иным причинам устраивают далеко не всех. Поэтому компания Grandstream Networks вывела на рынок сервер видеоконференций IPVT10. Это решение делает проведение качественных многоточечных видеоконференций возможным не только для крупных корпораций – в силу привлекательной цены сервер доступен и компаниям небольшого размера. Функциональность IPVT10

Grandstream IPVT10 поддерживает доступ с различных устройств, включая системы ВКС, видеотелефоны, браузеры рабочих станций под управлением Windows и MacOS, мобильные устройства на базе Android и iOS, магистральные линии PSTN и SIP АТС

Технические характеристики сервера Grandstream IPVT10

- MCU на 120 потоков (двунаправленное видео 1080p в формате H.264 со скоростью 30 кадр./мин.);
- способность обслужить до 300 участников одновременно при двунаправленном аудио и однонаправленном видео;
- проведение до 10 конференций одновременно;
- регистрация до 5000 устройств по учетным записям SIP;
- трансляция до 49 картинок на экран;
- поддержка разных расположений картинок на экране с автоматическим увеличением картинки по уровню голоса;
- трансляция конференций в YouTube и Facebook;
- 500 ГБ внутренней памяти для хранения записанных видеоконференций.

не только включает все возможности облачного сервиса IPVideoTalk, но и позволяет интегрировать систему с телефонией компании, а также делает возможным использование любого терминального оборудования ВКС от других производителей. Кроме того, спектр возможностей будет расти с каждым обновлением программного обеспечения сервера.

Новый сервер обладает впечатляющими техническими характеристиками (см. вставку «Технические характеристики сервера Grandstream IPVT10»). Кроме того, эти параметры можно улучшить, поскольку архитектура является масштабируемой и поддерживает балансировки нагрузки и резервирования для больших систем.

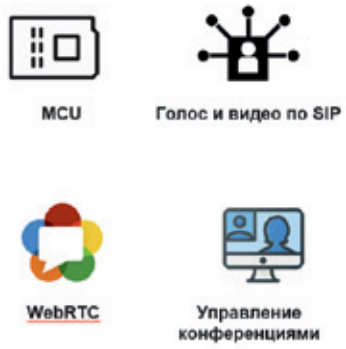
Принцип работы

На всех зарегистрированных на сервере ВКС устройствах есть возможность планировать и проводить видеовстречи и вебинары. Участником такой конференции может стать любой, кто получил приглашение по электронной почте либо знает ID и время ее проведения. Для входа понадобится только веб-браузер или бесплатное мобильное приложение для Android или iOS. Работает все это на базе технологии webRTC, поэтому участники конференций называются webRTC-участниками. У них есть возможность видеть и слышать выступающих, участвовать в текстовом чате, включать и выключать свой микрофон, транслировать в конференцию картинки с камеры ноутбука или мобильного устройства, а также демонстрировать остальным участникам содержимое рабочего стола или окна отдельного приложения – например, при чтении презентации.

Организатор также может зайти в видеоконференцию с помощью браузера для дополнительного контроля и настройки. В этом случае у него будет такой же

IPVT10 не только включает все возможности сервиса IPVideoTalk, но и позволяет интегрировать систему с телефонией компании, а также делает возможным использование терминального оборудования ВКС от других производителей

Веб-интерфейс организатора конференции



Четыре ключевых составляющих функциональности сервера Grandstream IPVT10

Устройства для организации видеоконференций Grandstream GVC32XX наиболее полно интегрированы с сервером IPVT10

Организатор может зайти в видеоконференцию с помощью браузера для дополнительного контроля и настройки. В этом случае у него будет интерфейс, как и у любого из webRTC-участников, но с дополнительными опциями

интерфейс, как и у любого из webRTC-участников, но с дополнительными опциями. Например, есть возможность настроить расположение картинок. Поддерживается размещение плиткой с разным количеством окон – от 9 до 49 на экран, есть возможность автоматически транслировать участников, которые в это время выступают, в окне большего размера по уровню звука, либо выбирать участников вручную.

Участником такой видеоконференции также может стать другой зарегистрированный на сервере терминал ВКС. В этом случае ему поступит вызов во время начала встречи. Также для присоединения с устройства ВКС можно набрать ID конференции.

В итоге, всю функциональность сервера IPVT10 можно разделить на четыре составляющих: MCU, передача голоса и видео по SIP-протоколу, webRTC и управление конференциями. MCU позволяет микшировать все потоки изображений в одну конференцию. SIP-сервер регистрирует все возможные ВКС-терминалы и видеотелефоны для передачи голоса и видео, с возможностью подключать SIP-транки телефонных сетей. Технология WebRTC позволяет пользоваться браузером и мобильными приложениями. Управление конференциями включает их планирование, администрирование и контроль при проведении.

Особенности работы с Grandstream GVC32XX

Наиболее полную интеграцию с сервером IPVT10 получили устройства ВКС серии GVC32XX. Эти модели наиболее удобно использовать как главные терминалы в организации и проведении встреч и вебинаров. Планирование, сбор, контроль во время проведения – все эти функции возможно выполнять не только при помощи веб-портала, но и из меню этих устройств.

Также стоит отметить, что только Grandstream GVC32XX позволяют прямые звонки между собой по номеру IPVideoTalk-сервера без предварительной организации конференций.

В качестве послесловия

Производитель, компания Grandstream, считает свой новый продукт революционным, и в некотором смысле не безосновательно. Какие возможности принесет сервер IPVT10? Организовывать видеоконференции стало легче некуда – участником встречи может стать абсолютно любой пользователь в любой момент времени. Нет никакой необходимости в наличии дорогого терминального видеооборудования или установке какого-либо специализированного программного обеспечения – достаточно ноутбука или современного смартфона. При интеграции сервера с телефонией можно проводить только голосовые конференции.

Установить систему можно как полностью закрытым способом внутри сети организации, так и использовать ее глобально в сети Интернет. Поставщики услуг имеют возможность предоставлять сервис другим компаниям.

Подключение старых систем ВКС к серверу IPVT10 вдохнет в них новую жизнь. Участников становится намного больше, а к видеотрансляции добавились возможности переписки в текстовом чате, обмена содержимым рабочего стола, проведения вебинаров с вопросами и ответами, трансляции происходящего в социальные сети, записи встреч на жесткий диск и многое другое.

По вопросам обращаться: *grandstream@muk.ua*.

GRANDSTREAM
CONNECTING THE WORLD

Семейство беспроводных телефонов

Носимые DECT и WiFi телефоны

Новые DECT трубки DP722 и DP730

- Новый функциональный дизайн
- Функция Push-To-Talk
- Встроенный датчик приближения и акселерометр (в модели DP730)

Портативный WiFi SIP телефон WP820

- Большое время автономной работы
- Поддержка открытого протокола SIP
- Набор всех необходимых корпоративных функций

Dual WiFi

NAS ДЛЯ ВИДЕОНАБЛЮДЕНИЯ:
СИСТЕМА МОНИТОРИНГА QNAP QVR PRO

Зачастую система видеонаблюдения – штука весьма сложная, состоящая из большого числа различных элементов, и процесс ее построения является достаточно затратным. Компания QNAP предлагает более простой подход к созданию решения видеонаблюдения любого масштаба на базе NAS

Реализовать такую систему дает возможность приложение для наблюдения QVR Pro, которое работает вместе с NAS в качестве независимой операционной среды. По умолчанию QVR Pro предоставляет восемь встроенных каналов мониторинга на базе файлового сервера QNAP без необходимости использования какого-либо дополнительного программного обеспечения. Для развертывания крупномасштабной сети можно приобрести лицензию, которая позволит предприятию расширить систему видеонаблюдения до 128 каналов.

Развертывание и управление

QVR Pro поддерживает огромное количество камер от более чем 140 производителей. В сетевую камеру наблюдения можно превратить и обычную недорогую USB-веб-камеру, установив приложение QUSBCam2. Добавлять новые камеры, масштабируя инфраструктуру, достаточно просто – так, при развертывании большого числа элементов модели одного производителя могут добавляться с одинаковыми настройками.

В случае, если инфраструктура видеонаблюдения распределена на территории большой площади (например, по целому кампусу), полезной может оказаться система QVR Center. Она дает возможность управления несколькими QVR Pro, установленными в различных локациях, отслеживая изображение с различных камер, воспроизводя записи и получая уведомления о событиях.

Режимы наблюдения

При развертывании системы видеонаблюдения целесообразнее будет использовать камеры типа Fisheye, или «рыбий глаз». Это позволит существенно сократить общее количество устройств – если раньше требовалось несколько обычных PTZ-камер для наблюдения за каждым углом помещения, то одна камера Fisheye обеспечит одновременный круговой обзор 360°. Это позволит повысить эффективность видеонаблюдения, снизив при этом затраты.

QVR Pro поддерживает большинство моделей камер Fisheye, представленных на рынке. Фирменная технология Qdewarp дает возможность получить изображение

Готов ко всему

Для обеспечения бесперебойного наблюдения и защиты QVR Pro от сбоев системы предусмотрено приложение QVR Guard. Как правило, QVR Guard устанавливается на отдельный резервный сервер и автоматически проверяет сетевое соединение, оставшееся пространство для записи и рабочее состояние сервера QVR Pro. Он работает в режиме ожидания и запускает обычные рабочие процессы NAS, когда контролируемый сервер QVR Pro работает нормально. В случае сбоя системы или оборудования QVR Guard берет на себя задачи записи с сервера QVR Pro. При этом файлы записи сохраняются на NAS-устройстве QVR Guard до тех пор, пока система QVR Pro не перезагрузится и не начнет работать стабильно.

QNAP

MUK
Classics of distribution

Designed for High Performance and Reliability

Server-grade Enterprise NAS

TS-x83XU Series

Reliable performance with ECC memory

The TS-x83XU Series uses DDR4 ECC memory which is capable of correcting single-bit memory errors to ensure the integrity of crucial applications.

Dual 10GbE connectivity optimizes virtualization performance

Two 10GbE SFP+ SmartNIC ports with iSER support accelerate large file sharing, intensive data transfer, and VMware virtualization applications.

Optimized storage efficiency with SSD caching and SSD Over-provisioning

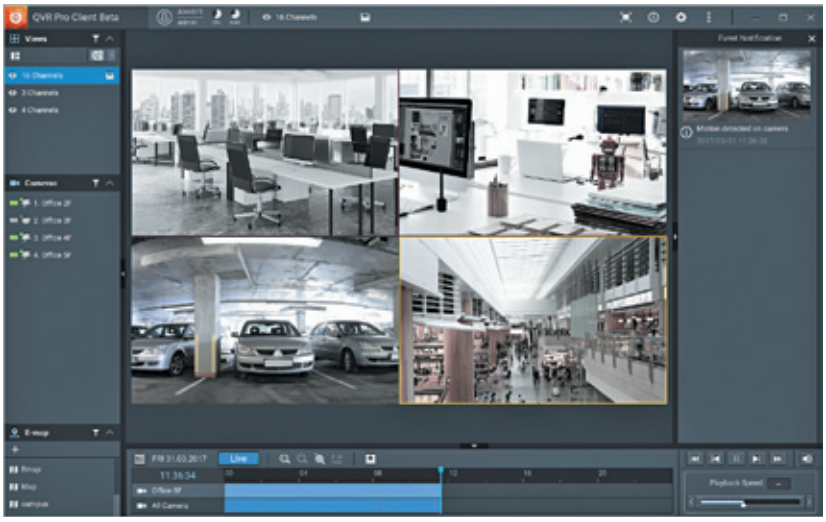
Software-defined SSD extra over-provisioning mitigates write amplification and optimizes SSD random write speeds for IOPS-demanding applications.

Expand NAS functionality with multiple PCIe slots

Install a graphics card or 40GbE/ 25GbE/ 10GbE adapters to increase the application potential of the NAS.

QNAP SYSTEMS, INC.

www.qnap.com



Интересной является возможность выделения так называемых областей интересов – отдельных зон в поле зрения камеры

Есть возможность транслировать изображение с камеры Fisheye на девять каналов под разным углом обзора на одном мониторе

с камер в различных пропорциях – существует целый ряд преднастроенных режимов вывода картинки для большинства сценариев применения. Также есть возможность транслировать изображение с камеры Fisheye на девять каналов под разным углом обзора на одном мониторе, полностью охватывая таким образом сектор обзора. При этому качество сигнала останется прежним, а нагрузка на процессор устройства (NAS) составит не более 25 % (в отличие от примерно 75 % при использовании обычного программного обеспечения для мониторинга).

Еще одной интересной особенностью является возможность выделения так называемых областей интересов – отдельных зон в поле зрения камеры, происходящее в которых интересует вас больше всего. Они могут отображаться в более крупном масштабе, что позволит сфокусироваться на самых важных объектах и исключить ненужные фрагменты.

Стоит отметить, что в QVR Pro также появилась возможность обнаружения движения, причем не только у дорогих моделей со встроенным детектором, а и для бюджетных USB веб-камер, что дает возможность создать более эффективную систему видеонаблюдения для дома и офиса при доступном бюджете. При фиксации какого-либо события оно моментально отображается на специальной электронной карте, позволяя моментально определить местоположение камеры, заснявшей это событие. Помимо этого оповещение включает в себя мигание красным цветом границ зоны с происшествием и звуковой тревожный сигнал.

Хранение записей и просмотр

Запись видео с камер в QVR Pro производится с использованием протоколов RTSP/RTMP. Решение позволяет выделить отдельное дисковое пространство для задач видеонаблюдения и хранения записей. Таким образом, хранилище полностью зарезервировано для QVR Pro, и на производительность системы видеонаблюдения не будут влиять никакие другие приложения NAS. Помимо этого можно выделить пространство для хранения записей каждой камеры, а также распределить между ними другие ресурсы NAS – пропускную способность канала, оперативную память и т. д. При необходимости для каждой камеры можно обозначить дни и время ведения записи.

Кроме того, в рамках NAS можно организовать резервное хранилище для записей на случай сбоя исходного тома. Для увеличения объема хранилища можно подключить к NAS дополнительные модули или использовать VJBOD – технологию расширения емкости за счет добавления свободного пространства из другого NAS.

Для просмотра записей с видеокамер используется QVR Pro Client. Клиент оснащен удобным и гибко настраиваемым интерфейсом, дающим возможность установить соотношение изображения выводимых на экран каналов наблюдения в соответствии с пожеланиями пользователя. В рамках одного интерфейса возможен одновременный просмотр видео с камер в реальном времени и архивных записей. Можно просмотреть записи за определенное время, используя временную шкалу либо выбрав соответствующий временной диапазон.

QVR Pro позволяет установить настройки привилегий, давая возможность определить права доступа для различных пользователей на основе ролей. Помимо стандартных ролей по умолчанию, таких как Администратор или Зритель, есть возможность создавать новые роли с индивидуально настроенными правами доступа к камерам, архивам записей, электронной карте и т. д.

Стоит отметить и мобильное приложение QVR Pro Client, которое дает возможность отслеживать одновременно несколько каналов и, как и стационарная версия, переключаться между режимами реального времени и воспроизведения. Кроме того, мобильная версия позволяет удаленно управлять камерами.

По вопросам обращаться: *qnap@muk.ua*.

АРХИТЕКТУРА В ОБЛАКЕ:
AUTODESK BIM 360

Компания Autodesk предлагает заказчикам широкий портфель решений для автоматизированного 2D- и 3D-проектирования. Как и многие другие производители, особое внимание Autodesk уделяет облачным решениям. Особое место среди них занимает платформа BIM 360

Линейка продуктов Autodesk максимально широко представлена по всем направлениям в индустрии строительства, машиностроения и даже мультимедиа. Для каждого из направлений предназначена своя коллекция. Общий список состоит из более чем сотни продуктов и может закрыть практически все требования современной инженерной, строительной или мультимедийной компании.

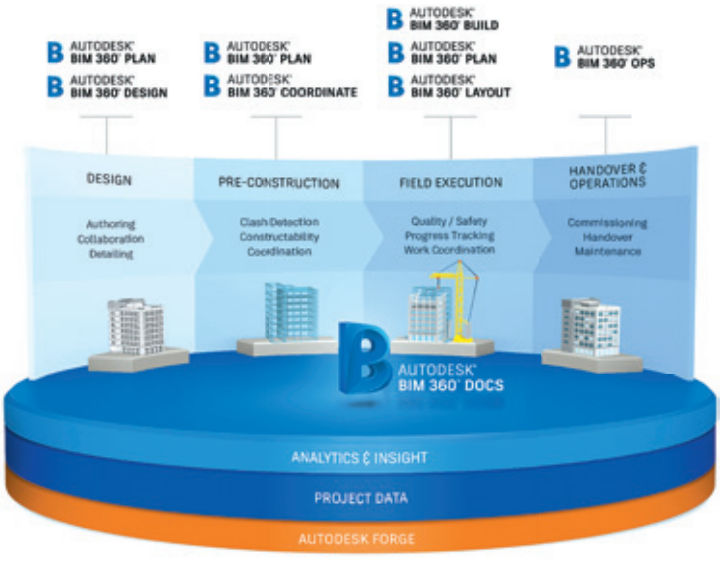
Поскольку облачные решения сегодня в тренде, Autodesk не может игнорировать мировые тенденции. Компания представила рынку свои облачные продукты, такие как Fusion 360 для машиностроительной отрасли, Shotgun для мультимедийной и BIM 360 для строительной индустрии.

Есть несколько причин акцентировать внимание именно на платформе BIM 360. Во-первых, она представляет собой очень популярную и перспективную технологию проектирования и строительства, которая стремительно развивается во всем мире. Во-вторых, BIM 360 очень активно поддерживается и развивается компанией Autodesk. И в-третьих, это уникальное решение, которое не имеет аналогов у конкурентов.

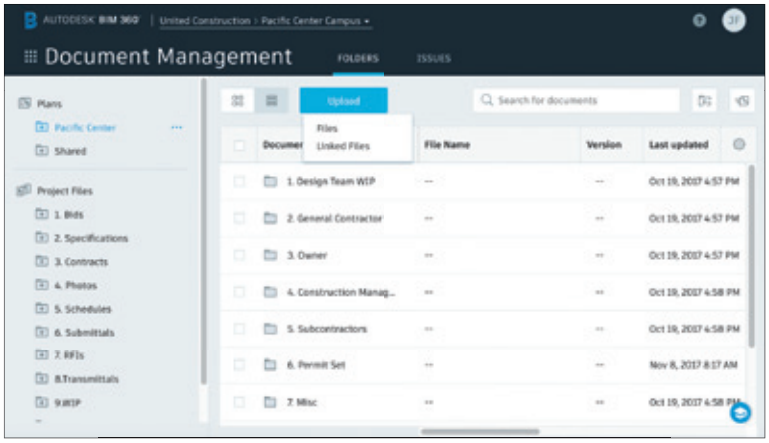
Облачный коворкинг

Что же представляет из себя BIM 360? Это облачное хранилище данных, которое работает по принципу других подобных служб, таких как BOX, OneDrive и т. д. Но уникальным BIM360 делает наличие других сервисов, которые позволяют работать инженерам, строителям и заказчикам в единой среде данных с поддержкой инженерных форматов файлов. Таким образом, можно сказать, что BIM 360 представляет собой подключенную облачную платформу для профессионалов в строительстве, работающих как в офисе, так и на строительной площадке, что приводит к более быстрой реализации проекта и более предсказуемым результатам.

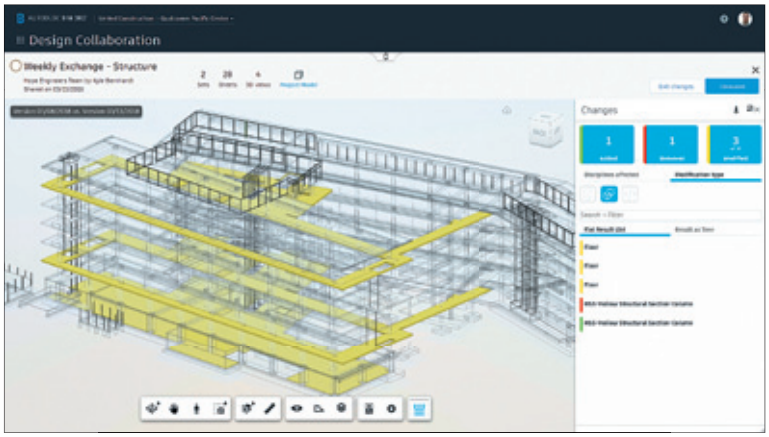
Что это означает на практике? Инженеры могут выполнять взаимодействие внутри системы, используя только веб-браузер и не нуждаясь в дополнительных инструментах. Оперативные обновления и контроль версий позволяют проектным группам тратить меньше времени на борьбу с документооборотом и



Последовательность итераций проекта в BIM 360 и модули, использующиеся на каждом этапе



BIM 360 Docs предназначен для передачи документации на строительную площадку и устранение замечаний



BIM 360 Design позволяет организовать совместную работу над проектами между сотрудниками, находящимися в различных точках мира

больше – на принятие проектных решений и коммуникацию друг с другом.

Платформа Autodesk BIM 360 включает в себя ряд сервисов. Рассмотрим некоторые из них более подробно.

BIM 360 Docs

Платформой для BIM 360 служит BIM 360 Docs. Этот сервис позволяет закрыть до 75 % потребностей проектной команды. Он помогает устанавливать уровни доступа к проектам и папкам внутри проекта, что классифицирует платформу как «работа в командах с низким уровнем доверия».

Версии документов формируются автоматически, можно посмотреть состояние файла в любой период времени – например, в настоящий момент, неделю или месяц назад. А функция сравнения 3D-моделей и 2D-чертежей позволит оценить прогресс, который был достигнут за это время. Особенностью платформы является поддержка рабочих процессов для утверждения выполненной работы, функция пометок, просмотр информации о конкретном элементе в модели и на чертеже, доступность с мобильных устройств – и это далеко не полный перечень возможностей.

BIM 360 Design

Одной из уникальных особенностей платформы BIM 360 является совместная работа в облаке. Все чаще заказчики отказываются от использования традиционных файловых серверов. Особенно это актуально для небольших проектных команд в составе от двух до десяти человек.

Хранение на локальном сервере означает, что командам для работы над различными проектами нужно ездить между разными офисами. А значит, придется терять время на перемещение и настройку рабочих процессов на новом месте. Это достаточно затратно с точки зрения ресурсов даже в пределах одного города, не говоря уже о проектах, реализуемых в пределах всей страны. При этом нескольким инженерам или архитекторам невозможно одновременно работать над моделью, не находясь в одном офисе. BIM 360 Design позволяет реализовать такое сотрудничество независимо от места нахождения участников команды.

BIM 360 Design создает пространство «Work-InProgress», общую среду для проектной команды, в которой используется многоуровневая система утверждения и одобрения для передачи модели между фазами проекта. Автоматизация рутинных задач, таких как пересылка моделей и подготовка их для демонстрации, позволяет высвободить время сотрудников для более качественного проектирования.

BIM 360 Coordinate

Ключевым фактором для успешной реализации проекта является отсутствие в нем пересечений между различными дисциплинами. BIM360 Coordinate – это совершенно инновационный подход к автоматизированной проверке на предмет пересечений. Архитектору, конструктору или инженеру достаточно загрузить свои модели в специальную директорию – и после нескольких минут анализа получить полную картину по неудовлетворительным местам в проекте.

BIM360 Coordinate помогает заказчикам добиться значительной экономии времени благодаря поиску таких пересечений, но еще большая экономия получается за счет своевременного их устранения на этапе проектирования.

BIM 360 Build

Модуль BIM 360 Build помогает контролировать и отслеживать реализацию проекта на строительной площадке. Поскольку вся информация хранится в единой среде общих данных, это позволяет экономить время на коммуникацию и обратную связь с проектировщиками, подрядчиками и менеджментом проекта

С помощью BIM 360 Build есть возможность решать такие задачи, как регистрация и отслеживание запросов на изменения проекта, передачу тендерных пакетов, отчетность о выполнении всех видов работ, а также контроль качества, безопасности и ввода объектов в эксплуатацию. Модуль позволяет фиксировать ежедневные отчеты об активности на

строительной площадке, получать отчеты о выполнении, а также ставить задачи с привязкой к видам работ, срокам и исполнителям.

BIM 360 Cost Management

Новый модуль управления затратами BIM 360 добавляет мощные рабочие процессы контроля расходов и управления изменениями, позволяя рабочим группам минимизировать риски и заведовать всеми процедурами, связанными с затратами, в рамках одной программы.

BIM 360 Cost Management обеспечивает сводный обзор всех статей бюджета и контрактов в режиме реального времени, дающий четкое представление о доходах, расходах, прогнозах и отклонениях, связанных с каждой статьей. Модуль оптимизирует рабочие процессы в восходящем и нисходящем порядке, создавая четкую подотчетность и жесткий контроль финансовых потоков, относящихся к проекту.

Forge API

Система BIM 360 создана с помощью инструментов программирования на базе платформы Forge. Платформа Forge раскрывает всю мощь проектных и инженерных данных, что позволяет объединять команды и рабочие процессы и создавать новые сервисы для удовлетворения потребностей заказчиков.

Инструменты Forge помогают компаниям создавать приложения, которые используют их данные проектирования и разработки – от автоматизированных процессов до оповещений. Платформа также оснащена 3D-браузером для виртуальной реальности. API-интерфейсы Forge можно комбинировать с существующими программными системами для получения большей эффективности от данных заказчика.

На сегодняшний момент реализован BIM 360 API, который позволяет:

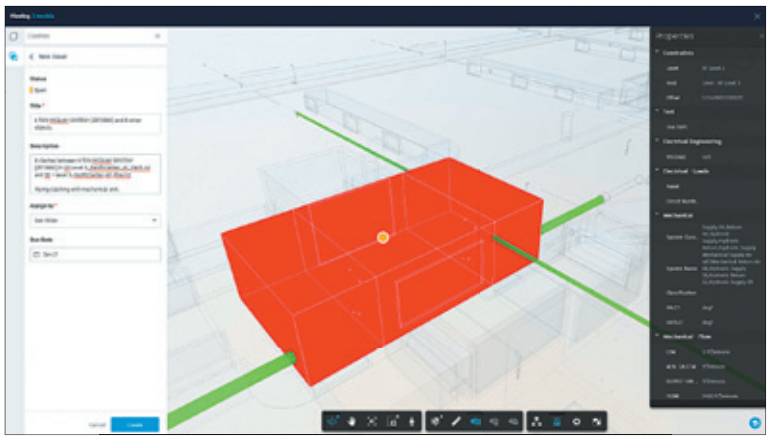
- автоматизировать настройку проектов, назначение администраторов, синхронизацию данных с внешними системами;
- автоматизировать загрузку 3D- и 2D-данных и их совместное использование;
- подготовить модель к просмотру в своем собственном приложении;
- настроить более функциональное управление задачами, управлять обновлением, созданием, отслеживанием статуса;
- гибко управлять контрольными списками на строительной площадке.

Кроме того, доступен целый ряд других возможностей.

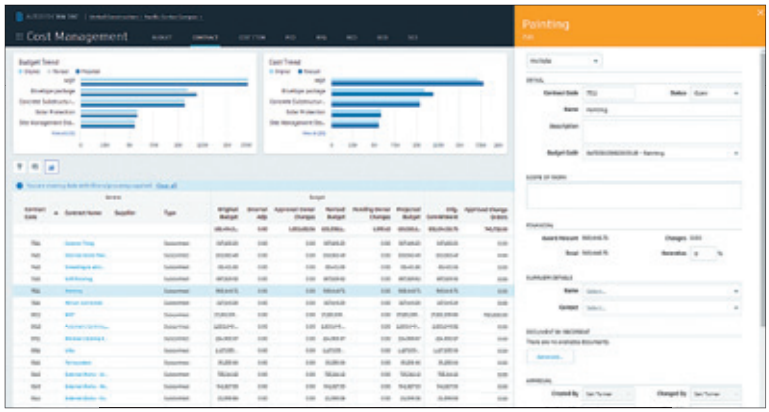
В качестве послесловия

BIM 360 представляет собой унифицированную платформу, соединяющую проектные команды и данные в режиме реального времени на всех этапах – от проектирования до строительства. Это поддержка принятия обоснованных решений и достижение более предсказуемых и прибыльных результатов.

Платформа позволяет предсказать риски проекта, управлять качеством, автоматизировать задачи и сократить объем работ, а также контролировать расходы и не отставать от графика строительства.



BIM 360 Coordinate обеспечивает значительную экономию ресурсов благодаря поиску пересечений между различными дисциплинами проекта



BIM 360 Cost Management позволяет проводить контроль финансовых потоков, относящихся к проекту

Заказчики Autodesk наблюдают увеличение производительности до 25 % в облачных проектах только за счет времени загрузки и синхронизации/

Решение дает возможность централизовать данные проекта и получить доступ к необходимой информации в режиме реального времени в любом месте, чтобы легко отслеживать проект и принимать решения на местах.

Контролируемый совместный доступ позволяет многопрофильным группам совместно создавать и редактировать модели Revit, визуализировать каждое обновление и управлять проектными данными на протяжении всего жизненного цикла проекта.

Использование BIM 360 Design значительно увеличивает производительность Revit и связанной с ней BIM. Теперь заказчики также являются частью процесса. Не нужно устанавливать Revit, необходим лишь веб-браузер. С его помощью можно войти в систему, просмотреть листы, посмотреть, как подрядчики координируют модели, делятся комментариями и обмениваются идеями.

По вопросам обращаться: *autodesk@muk.ua*.

VEEAM AVAILABILITY SUITE 9.5 UPDATE 4:

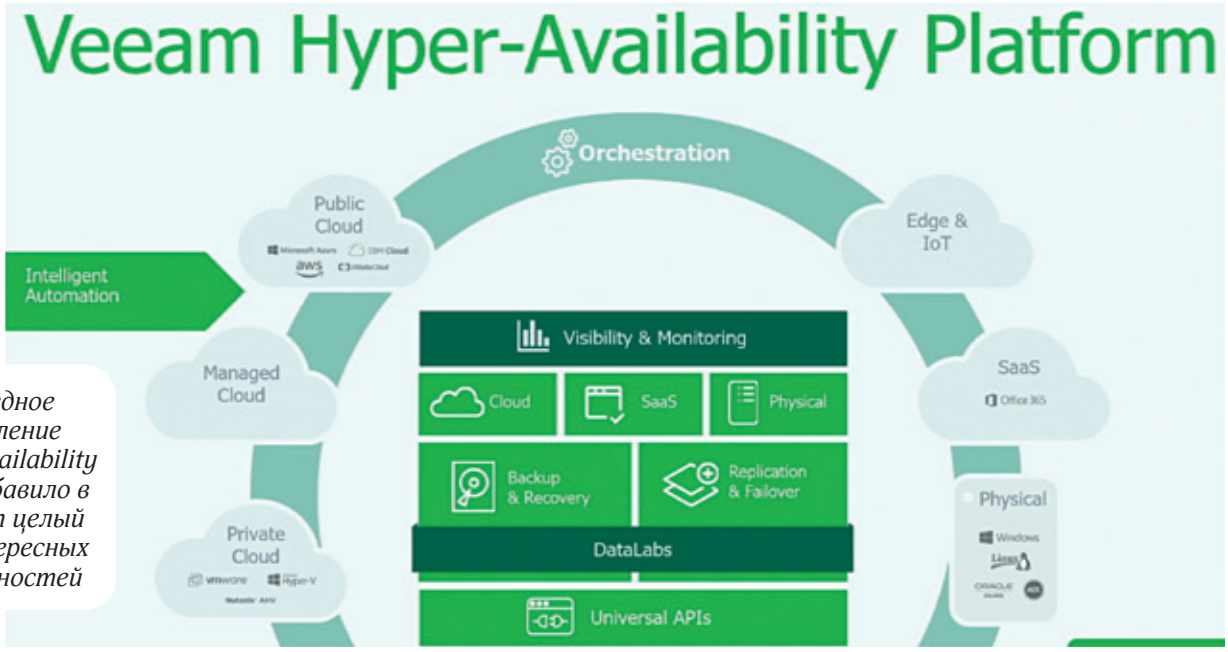
НОВЫЙ УРОВЕНЬ ДОСТУПНОСТИ ДАННЫХ

В начале года компания Veeam выпустила новую версию своего продукта для обеспечения доступности данных Availability Suite 9.5 – Update 4. Наибольшее количество ключевых изменений было реализовано в одном из центральных компонентов системы – Backup & Replication

Veeam Backup & Replication обеспечивает доступность всех виртуальных, физических и облачных ресурсов предприятия, позволяя гибко управлять резервным копированием, восстановлением и репликацией всех приложений и данных в рамках единой консоли. Далее более подробно рассмотрим все новшества, которые появились в свежей версии решения.

Cloud Tier

В первую очередь стоит отметить появление в новом релизе нативной интеграции с облачными объектными хранилищами Veeam Cloud Tier. Cloud Tier представляет собой масштабируемое хранилище резервных копий (SOBR, Scale-Out Backup Repository) с неограниченной емкостью для хранения данных, реализованное посред-



Очередное обновление Veeam Availability Suite добавило в продукт целый ряд интересных возможностей

ством интеграции с Amazon S3, Azure Blob Storage и IBM Cloud Object Storage, а также с различными сервис-провайдерами и локальными хранилищами.

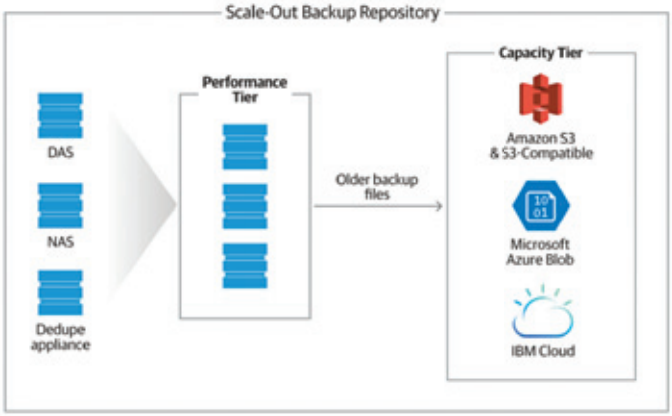
Veeam Cloud Tier реализован как новый уровень хранения внутри SOBR, так называемый уровень емкости (Capacity Tier). Он настраивается с помощью политики, которая автоматически помещает файлы резервных копий в хранилище объектов из окна оперативного восстановления по мере их устаревания, начиная с наиболее ранних версий, до того, как свободное место на дисках локального хранилища начнет исчерпываться. При использовании публичного облачного хранилища объектов данные могут быть защищены с помощью дополнительного шифрования при помощи алгоритма AES 256-bit.

Интеграции хранения объектов Veeam включают в себя ряд существенных преимуществ. Так, например, к резервным копиям, которые были выгружены в хранилище объектов, остается возможным применение всех функций программного обеспечения Veeam. Они также доступны для восстановления непосредственно из SOBR без предварительной подготовки. В дополнение к сжатию на площадке заказчика, резервные копии файлов выгружаются в хранилище объектов инкрементно, что позволяет предотвратить дублирование между несколькими бекапами и обеспечить эффективную дедупликацию. Во время восстановления выходной трафик из хранилища объектов минимизируется путем считывания всех соответствующих блоков из ближайшей резервной копии, доступной локально, вместо извлечения всех блоков из SOBR. Это позволяет снизить стоимость восстановления.

Выгруженные резервные копии являются самодостаточными и не зависят от какого-либо внешнего каталога или метаданных. Это дает возможность импортировать их, даже если локальный сервер резервного копирования недоступен вместе с конфигурацией и базой данных. Архивные бекапы можно импортировать из хранилища объектов и восстанавливать в любой момент, используя бесплатную версию Veeam Backup & Replication Community Edition. Стоит также отметить, что за загрузку данных в SOBR не требуется отдельная плата за единицу объема данных.

Cloud Mobility

Также была расширена функциональность Veeam Cloud Mobility, которая позволяет обеспечить переносимость



Cloud Tier обеспечивает нативную интеграцию с облачными объектными хранилищами, которые можно использовать для долговременного хранения бекапов в рамках концепции Scale-out Backup Repository

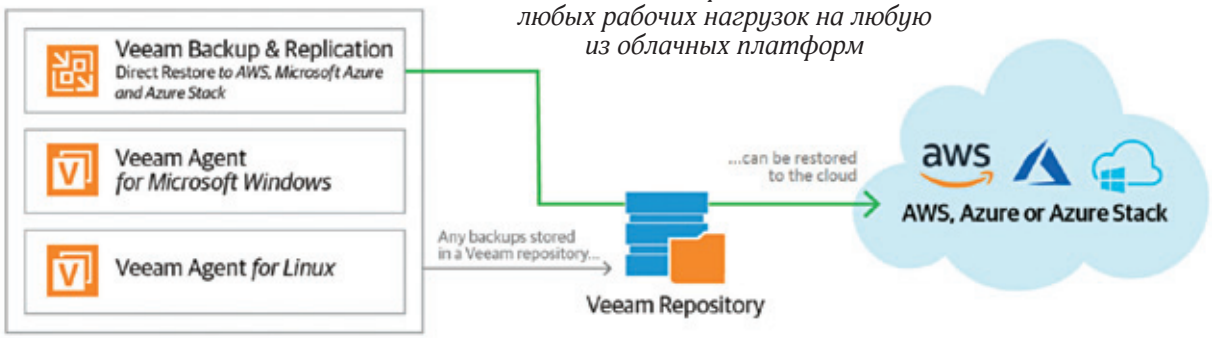
и быстрое восстановление любых рабочих нагрузок из репозиториев Veeam (в том числе Veeam Agent для Windows и Linux) на любую из облачных платформ или в локальное хранилище.

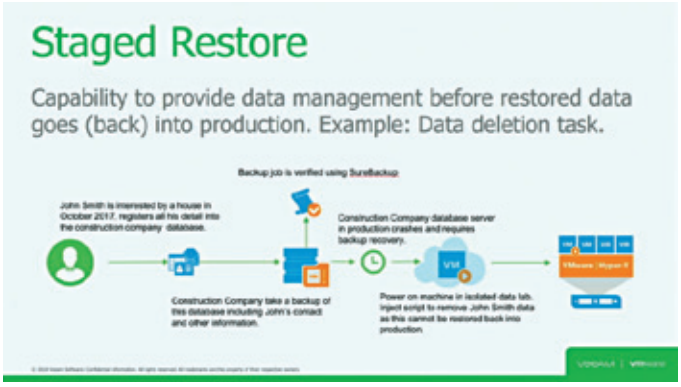
В ранней версии Veeam Backup & Replication было реализовано прямое восстановление резервных копий в Microsoft Azure. Обновление дополнило Cloud Mobility функциями восстановления в Amazon AWS и Microsoft Azure Stack.

Прямое восстановление в Amazon AWS дает возможность восстановления резервных копий непосредственно в облаке и позволяет оптимизировать распределение ресурсов и минимизировать затраты. Бекапы виртуальных машин на базе Windows и Linux, физических серверов и рабочих станций восстанавливаются в виде виртуальной машины AWS EC2, в том числе и в Amazon Government Cloud и Amazon China. Функция включает в себя встроенное преобразование загрузчика UEFI в BIOS – именно оно позволяет восстанавливать современные рабочие станции Windows непосредственно в AWS EC2, не поддерживающие UEFI.

Прямое восстановление в Microsoft Azure Stack основано на проверенном механизме Direct Restore to Microsoft Azure. С его помощью можно восстанавливать резервные копии виртуальных машин на базе Windows и Linux, физических серверов и рабочих станций в Microsoft

Veeam Cloud Mobility позволяет обеспечить быстрое восстановление любых рабочих нагрузок на любую из облачных платформ





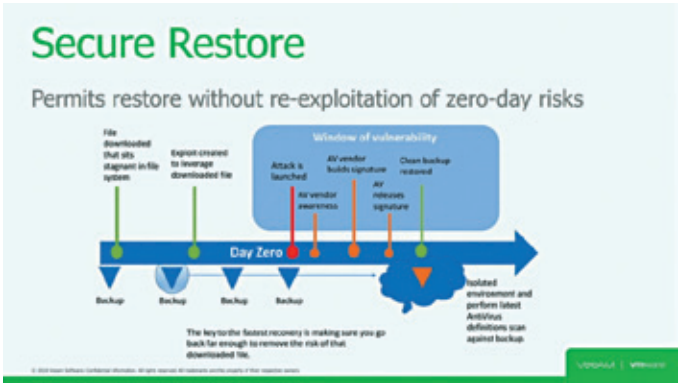
Staged Restore удаляет персональную информацию из резервных копий при восстановлении виртуальных машин

Azure Stack в виде виртуальной инфраструктуры как сервиса (IaaS). Совместно с Veeam Agent эта функция представляет собой полноценное решение резервного копирования для Microsoft Azure Stack IaaS VM.

Лаборатории данных

Еще одна новая функция в Backup & Replication – Veeam DataLabs, ранее известная как Virtual labs, предназначена для повышения безопасности, соответствия требованиям и оптимизации ИТ-процессов. DataLabs представляет собой набор инструментов, которые позволяют ИТ-специалистам и разработчикам тестировать рабочие нагрузки в изолированной среде, проверять обновления, исправления, наличие уязвимостей в системе безопасности, обеспечивать соответствие требованиям и анализировать возможность восстановления резервных копий Veeam.

Одна из наиболее важных функций DataLabs – Staged Restore, которая позволяет изменять данные внутри резервных копий перед их реальным восстановлением в производственную среду. Такой поэтапный процесс восстановления состоит из запуска требуемой точки восстановления в DataLab непосредственно из файлов резервных копий, внедрения настраиваемого сценария



Благодаря Secure Restore появилась возможность проверить резервную копию перед восстановлением, чтобы избежать возможного заражения виртуальной машины

в гостевой ОС с сохранением внесенных изменений и переноса измененных бекапов непосредственно в производственную среду для завершения восстановления.

Staged Restore позволяет соблюсти требования GDPR, позволяя удалить персональную информацию из резервных копий при восстановлении виртуальных машин из старых архивов. Также функция дает возможность оптимизировать рабочие процессы, позволяя администраторам вносить необходимые изменения в настройки ОС (например, IP-адреса, конфигурации DNS или брандмауэра), устанавливать или удалять приложения, а также выполнять любые другие операции, необходимые для обеспечения соответствия восстановленной виртуальной машины целевой среде до ее фактического размещения там. Стоит отметить, что функция Staged Restore доступна только в редакции Enterprise.

Еще одна ключевая функция – Secure Restore. Она обеспечивает возможность сканирования данных внутри восстановленных резервных копий с помощью антивирусного ПО, чтобы устранить угрозы перед вводом бекапов в производственную среду. Это осуществляется путем подключения виртуальных дисков с архивным репозиторием и запуска антивирусной программы, установленной на сервере.

Казалось бы, какой смысл в данной функции, если внутри виртуальной машины есть антивирус? В частности, Secure Restore позволяет выявить «спящие» программы-вымогатели в выбранной точке восстановления и не перенести их в производственную среду. Кроме того, функция повышает шансы обнаружить редкое вредоносное ПО или атаки типа Zero-day, не позволив им попасть в резервную копию и заразить при восстановлении виртуальную машину. В случае обнаружения угрозы виртуальная машина и ее данные помещаются на карантин и после процедуры «лечения» могут быть восстановлены. Также Secure Restore будет полезна для проверки резервных копий из локаций, меньше контролируемых ИТ-отделами, таких как удаленные офисы или филиалы, перед их восстановлением в дата-центре.

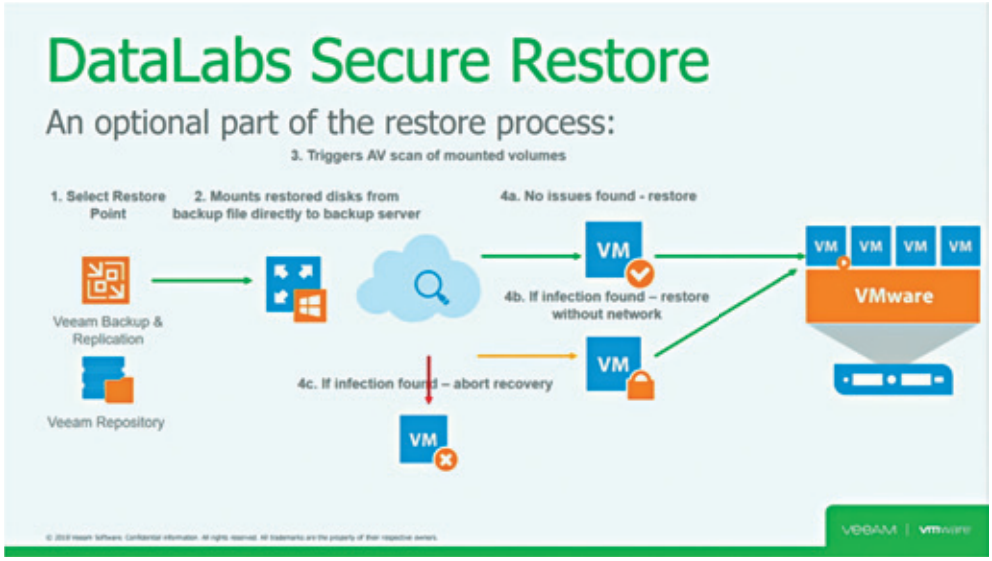
«Из коробки» Secure Restore поддерживает работу с такими антивирусными продуктами, как Microsoft Windows Defender, Symantec Protection Engine и ESET NOD32. При помощи добавления сценариев в файл конфигурации можно расширить эту поддержку на любой антивирус, который поддерживает запуск из командной строки.

Кроме того, стоит отметить в Veeam DataLabs наличие таких инструментов, как SureBackup и SureReplica, которые дают возможность удостовериться в работоспособности восстановления бекапов и реплик, и виртуальной «песочницы» On-Demand Sandbox для тестирования восстановленных резервных копий.

Работа с БД

Администраторы баз данных получат возможность контролировать резервное копирование и восстановление БД с помощью привычных нативных инструментов, при этом помещая все резервные копии в репозиторий Veeam. Это позволяет сделать новые плагины корпоративных приложений для работы с базами данных.

Подключаемый модуль Veeam для SAP HANA сертифицирован SAP и позволяет администраторам баз данных HANA использовать интерфейс BACKINT для резервного



В случае обнаружения антивирусом угрозы виртуальная машина и ее данные помещаются на карантин

копирования и восстановления БД как в, так и из хранилища резервных копий Veeam, включая поддержку развертываний HCI SAP HANA. Плагин Veeam для Oracle RMAN дает администраторам баз данных Oracle возможность использовать диспетчер RMAN для выполнения резервного копирования и восстановления БД в репозиторий Veeam.

Дополнительным преимуществом использования таких подключаемых модулей является поддержка масштабируемого хранилища бекапов. SOBR значительно увеличивает пропускную способность резервного копирования и восстановления благодаря масштабируемой многоузловой серверной части.

Для того чтобы использовать плагины корпоративных приложений для работы с базами данных, требуется версия Enterprise Plus.

Портал самообслуживания

Можно существенно сократить время восстановления бекапов и совокупную стоимость владения решения, дав пользователям возможность самостоятельно управлять резервными копиями своих виртуальных машин с помощью портала самообслуживания резервного копирования и восстановления для VMware vSphere. На портале установлен доступ на основе ролей, привязанный к уже установленной и поддерживаемой системе разрешений vSphere. Это означает, что при каких-либо изменениях инфраструктуры либо появлении новых сотрудников никаких обновлений в ручном режиме от ИТ-отдела организации не понадобится.

В зависимости от прав пользователя в среде виртуализации можно определить правила доступа к операциям резервного копирования и восстановления виртуальных машин. Также есть возможность разграничить доступ к виртуальным машинам на основе тегов vSphere.

Портал самообслуживания базируется на оптимизированном пользовательском интерфейсе Enterprise Manager. Настройка максимально упрощена: пользователю нужно просто выбрать нужную резервную копию виртуальной машины и необходимые параметры. При этом доступ к расширенным настройкам, таким как выбор репозитория или режима резервного копирования, запрещен – такие конфигурации выполняются администратором портала посредством шаблонов правил. И уже непосредственно на этапе восстановления пользователь получает возможность выбрать нужный вариант восстановления виртуальной машины из списка, предоставляемого Enterprise Manager.

Для получения доступа к порталу самообслуживания резервного копирования и восстановления требуется версия Enterprise Plus.

Интеллектуальная диагностика

Повысить надежность и успешность процессов резервного копирования, сократив при этом совокупную стоимость владения, можно благодаря функции интеллектуальной диагностики, позволяющей проактивно решать типовые проблемы и ошибки конфигурации при их возникновении.

Эта новая функция Veeam ONE отслеживает журналы Veeam Backup & Replication на наличие шаблонов известных проблем и сопоставляет их с данными мониторинга виртуальной инфраструктуры. В случаях, если инфраструктура резервного копирования настроена не оптимально, в виртуальной инфраструктуре возникла проблема, которая может повлиять на резервные копии, или конфигурация требует каких-либо важных исправлений, – пользователь получит уведомление. И произойдет это до того, как эти проблемы окажут существенное влияние на резервные копии

Важной особенностью реализации этой функции является то, что анализ журналов выполняется локально с использованием набора «сигнатур» известных проблем, подготовленного и обновляемого службой технической поддержки и управления продуктами Veeam. Такой подход позволит легко разобраться с проблемой самостоятельно, не открывая кейс в службе технической поддержки.

Помимо описанного выше, стоит отметить еще несколько ключевых улучшений новой версии Veeam Backup & Replication: внешний репозиторий для N2WS, улучшение бекапа на ленточные носители, а также усовершенствованный Veeam Explorer.

По вопросам обращаться: *veeam@muk.ua*.

ИГРЫ В «ПЕСОЧНИЦЕ»: ПРЕИМУЩЕСТВА FORTISANDBOX

Рост убытков компаний по всему миру вследствие действий киберпреступников и увеличение числа угроз и вредоносного ПО постепенно приводят к необходимости пересмотреть схему работы существующих систем защиты, а также одного из важных элементов обеспечения безопасности – «песочниц»

Количество видов вредоносного ПО на сегодняшний день превышает 700 млн. Кроме того, для автоматизации атак киберпреступники в последнее время зачастую используют модель «вредоносное ПО как услуга» и искусственный интеллект. Поэтому использование «песочниц» в автоматических системах защиты является важным аспектом обеспечения безопасности инфраструктуры компании.

Помимо роста числа атак и разнообразия угроз, стоит отметить, что сами сети находятся на этапе цифрового преобразования. Тотальное проникновение облачных технологий обуславливает потребность в интегрированных решениях безопасности, которые обмениваются данными об угрозах в распределенных сетях, и пропускной способности по периметру сети. Как итог – рост облачной инфраструктуры приводит к необходимости масштабировать систему безопасности для защиты от новых уязвимостей.

Оба этих фактора, желание ИТ-отделов не просто обнаружить утечку данных, но и предотвратить ее, а также снижение цен на устройства-«песочницы» приводят к росту спроса на подобные решения. Однако далеко не все «песочницы» соответствуют современным требованиям – многие традиционные решения имеют устаревшую функциональность и ограниченную производительность. Далее рассмотрим подробнее четыре основные проблемы, которые необходимо учитывать при обновлении или интеграции «песочницы» в корпоративной сети.

Эффективность

В современных реалиях скорости движения данных и динамики работы сети важной является способность «песочницы» не только обнаружить угрозу, но и обеспечить мгновенную реакцию на любое событие безопасности – своевременно блокировать атаку и сообщить о заражении. Поэтому при выборе решения необходимо учитывать не только эффективность обнаружения угроз, но и показатели времени реакции. Ведь чем быстрее происходит обнаружение угроз и ликвидация заражения, тем ниже затраты на восстановление.

Раньше считалось вполне нормальной ситуацией, когда организациям приходилось выбирать между защитой сети от всех видов атак и обеспечением высокой пропускной способности. Сегодня же оба эти условия необходимы: эффективность функций защиты «песочницы» следует

Защита от продвинутых угроз для интернет-трафика

оценивать в контексте ее производительности и наоборот. Далее приведем еще несколько критериев, которые важно учитывать при выборе.

Интеграция. Не стоит останавливать выбор на продукте, который не поддерживает интеграцию с другими компонентами архитектуры безопасности. Зачастую в таких случаях вредоносное ПО определяет присутствие виртуальной «песочницы» и избегает обнаружения. Одним из вариантов решения проблемы является развертывание нескольких технологий «песочницы», однако это приведет к существенному повышению сложности конфигурации со всеми вытекающими последствиями.

Данные об угрозах. «Песочница» обязательно должна иметь доступ к данным об угрозах из отдела исследования угроз в режиме реального времени для своевременного обновления сигнатур и получения информации о новых зловредах. Она также должна обмениваться данными с другими средствами защиты и компонентами архитектуры для обеспечения скоординированного и автоматизированного реагирования на атаки. В результате такого обмена обеспечивается более эффективная защита, нежели та, которую предоставляют все компоненты системы безопасности по отдельности.

Обнаружение и предотвращение. Важнейшей особенностью «песочницы» является способность превентивно блокировать потенциальные атаки и оповещать о потенциальных угрозах. Как правило, это называется функцией обнаружения и предотвращения вторжений или защитой от продвинутых угроз. Только такой подход позволит не допустить вредоносное ПО в сеть для получения доступа к конфиденциальным данным, а администраторам даст возможность сдержать распространение заражения и минимизировать воздействие на сеть.

Собственные технологии. Рискованным выбором являются «песочницы», в основе которых лежат общие технологии, лицензированные производителями для разных поставщиков. В этом случае задержки с обновлениями продукта по разным причинам могут привести к проблемам с его эффективностью без возможности их решения. Лучше выбрать решения на базе оригинальных технологий от производителя – в этом случае компании, как правило, следят за тем, чтобы их продукты всегда были в актуальном состоянии.

Административные расходы

Одними из главных проблем ИТ-отделов большинства компаний являются ограниченный бюджет и нехватка квалифицированных кадров, в том числе и специалистов по информационной безопасности. И без того высокая нагрузка на последних становится еще большей из-за того, что администрирование многих устаревших «песочниц» приходится осуществлять вручную. Ниже рассмотрим ряд факторов, которые нужно учитывать в разрезе загрузки персонала.

Упрощение управления системой безопасности. Для того чтобы устранить «ручные» процессы администрирования и сэкономить время персонала на управление «песочницей», лучше отдавать предпочтение продуктам, которые обмениваются данными об угрозах со всеми внутренними средствами управления безопасностью. Также это позволит автоматически применить меры защиты при обнаружении зловредного ПО или проникновения в сеть.

Защита от продвинутых угроз для почтовой инфраструктуры

Использование «песочниц» в автоматических системах защиты является важным аспектом обеспечения безопасности инфраструктуры компании

Развертывание и форм-факторы. Вторым по важности критерием при приобретении продуктов безопасности после стоимости является простота интеграции. Форм-фактор для работы в локальном режиме могут ограничивать варианты применения «песочницы». А использование только физических подключений повышает время и стоимость развертывания «песочницы».

Масштабируемость

Важное значение для продуктов практически любого направления имеет возможность масштабирования. Растущий трафик или преобразование инфраструктуры, например, при расширении в облачные среды, – для многих традиционных «песочниц» подобные изменения могут стать проблемой, и для соответствия новым требованиям возникает необходимость в приобретении дополнительных устройств. Что, соответственно, приводит к повышению расходов и сложности масштабирования самой «песочницы». При масштабировании распространенными проблемами являются нехватка производительности, ограничения лицензирования и физические ограничения развертывания.

Лицензирование. Сложные и дорогие модели лицензирования вряд ли станут экономически выгодными, особенно в случае развертывания решения по мере расширения инфраструктуры.

Защита от продвинутых угроз для веб-инфраструктуры

Количество узлов в кластере. Лучше выбрать решение, которое поддерживает большое количество узлов в кластере. Это позволит масштабировать решение при росте сети, увеличении потока трафика и повышении требований к системе безопасности.

Стоимость

На совокупную стоимость развертывания, технического обслуживания и содержания «песочницы» влияет целый ряд факторов. Так, например, для многих решений нужно использовать несколько устройств и/или подписок, что приводит к повышению совокупной стоимости владения (TCO). Далее подробнее остановимся на двух основных критериях стоимости продукта.

Поверхность атаки. При использовании «песочницы» независимо от того, внедряется ли новое решение или обновляется старое, необходимо учитывать все связанные с этим расходы. Для этого нужно оценить, охватывает ли продукт всю поверхность атаки – сеть, конечные точки, Интернет, электронную почту и облако, и нужны ли для этого какие-либо дополнительные лицензии. Кроме того, важна поддержка таких функций, как проверка трафика SSL и TLS.

Автоматизация безопасности для всей сети

Стоимость каждого защищенного Мбит/с. При выборе «песочницы» также следует обратить особое внимание на такой параметр, как стоимость каждой защищенной единицы трафика. Для этого можно воспользоваться результатами тестирований, проводимых независимыми организациями – экспертами в области информационной безопасности, такими, например, как NSS Labs.

FortiSandbox и ее преимущества

Просуммировав вышесказанное, становится ясно, что «песочницы» предыдущего поколения могут не справляться со сложностью и скоростью распространения современных угроз, а также не соответствовать изменениям сетевых инфраструктур, вызванным развитием цифровых технологий. И, тем не менее, «песочница» как инструмент остается необходимым компонентом интегрированной архитектуры безопасности.

В связи с этим компания Fortinet предложила свое решение – «песочницу» FortiSandbox. Продукт постоянно совершенствуется – добавляется новый функционал, который помогает организациям надежно защищать весь спектр сетевых и вычислительных сред. Так, например, из недавних функций – реализация поддержки операционных систем Mac OS и Android, а также анализ зашифрованных и облачных угроз. Fortinet использует смежные технологии безопасности, такие как система предотвращения вторжений (IPS), антивирус и веб-фильтрация, в качестве базовых уровней проверки безопасности в продуктах FortiSandbox.

Функциональная совместимость FortiSandbox с платформой Fortinet Security Fabric помогает обмениваться интеллектуальными данными со всем спектром продуктов безопасности Fortinet, включая FortiGate, FortiMail, FortiProxy, FortiSIEM, FortiCASB и FortiClient. Это, в свою очередь, позволяет обнаруживать подозрительные и неизвестные файлы в различных точках входа, таких как брандмауэры, веб-шлюзы, почтовые шлюзы и конечные точки.

После обнаружения неизвестного вредоносного ПО FortiSandbox генерирует соответствующие индикаторы компрометации (IOC) и в режиме реального времени обменивается ими с другими компонентами обеспечения безопасности и Fabric-Ready Partner для автоматического устранения угрозы.

Кроме того, FortiSandbox интегрируется с брандмауэром веб-приложений FortiWeb (WAF). Стоит отметить, что лишь немногие конкурирующие решения AMS изначально интегрируются с WAF.

FortiSandbox доступен в виде физических или виртуальных устройств, размещенных как в приватных, так и в публичных облаках. Он может быть развернут как самостоятельный продукт или как интегрированное решение, подключенное к продукту безопасности Fortinet или стороннему решению. Помимо гибкости развертывания, использования комбинаций эмуляции и полного динамического анализа на основе изолированной среды, FortiSandbox позволяет обнаруживать неизвестные угрозы и снижает нагрузку на систему безопасности. В целом, его централизованное управление угрозами предоставляет специалистам по информационной безопасности целостное понимание ландшафта угроз для быстрого и точного обнаружения и реагирования.

По вопросам обращаться: *fortinet@muk.ua*.

ТОРГОВЫЕ ПРЕДСТАВИТЕЛИ:

POS-ТЕРМИНАЛЫ HP ENGAGE ONE PRIME

Кассовый терминал – давно уже не роскошь, а необходимый атрибут для любой, даже небольшой торговой точки. Компания HP Inc. представила новые компактные POS-системы для обработки платежей, которые отлично подойдут для магазинов небольших и средних размеров

Небольшие розничные магазины, как и крупные торговые сети, стремятся предложить возможность оплачивать товары и услуги тем способом, который наиболее удобен клиенту. Поэтому они нуждаются в оснащении доступными, надежными и простыми в управлении системами – терминалами безналичной оплаты. Стоит также отметить, что подобные торговые точки имеют небольшие площади и стараются экономить свободное пространство, поэтому им требуются терминалы, являющиеся комплексными решениями, которые включают в себя комплект периферийных устройств. POS-системы HP Engage One Prime, предназначенные для обработки платежей в сфере розничной торговли и гостиничного бизнеса, станут в таких случаях оптимальным вариантом.

Внешний вид

HP Engage One Prime представляет собой стильное многофункциональное устройство, которое отлично впишется в интерьер магазина благодаря элегантному дизайну. Терминал доступен в двух цветах – строгом черном и ослепительном белом. Система оснащена 14-дюймовым сенсорным экраном с разрешением Full HD, который для удобства работы легко наклоняется и переворачивается для взаимодействия с покупателями. Кроме того, есть модели со специальным дополнительным «клиентским» дисплеем.

Функциональность

POS-терминал имеет достаточно широкий набор возможностей и снабжен встроенным считывателем магнитных карт и принимающим NFC-модулем для аутентификации сотрудников, а также сканером

HP Engage One Prime предназначены для обработки платежей

Сенсорный экран POS-терминала можно наклонять и переворачивать

штрих-кодов на основе цифровой камеры для сканирования товаров. Помимо этого функциональность терминала можно существенно расширить за счет опциональных дополнительных модулей. К HP Engage One Prime можно подключить принтер, сканер штрих-кода, считыватель отпечатков пальцев для дополнительной безопасности, кассу для наличных денег, платежное устройство PayPal, принимающее платежи с использованием чипа, а также считыватель iButton. Для подключения большего количества устройств можно дополнительно приобрести специальный концентратор ввода/вывода, который имеет целый ряд слотов: два разъема db9, четыре порта USB 2.0, два порта USB type-C и порт USB A, гигабитный сетевой разъем и разъем для подключения денежного лотка. Терминал также интегрирован с популярным сторонним ПО для торговых точек и платежными системами от партнеров HP Inc.

Производительность

Новая модель работает под управлением операционной системы Android 8.1 и оснащена достаточно мощной аппаратной начинкой, которая конфигурируется согласно пожеланиям заказчика. «Под капотом» терминала – мощный многоядерный гетерогенный процессор Qualcomm APQ8053 с тактовой частотой 1,8 или 2,2 ГГц, 2 или 4 ГБ оперативной памяти, а также внутреннее хранилище объемом 16 или 32 ГБ.

По вопросам обращаться: *hp@muk.ua*.

MUK review

ПУТЬ К СОВРЕМЕННОМУ ЦОД: VMWARE CLOUD FOUNDATION

В условиях колоссального увеличения объемов данных и все возрастающей сложности работы с ними чуть ли не единственным выходом становится внедрение искусственного интеллекта в современные центры обработки данных. Справиться с этой непростой задачей поможет VMware Cloud Foundation

Искусственный интеллект достаточно быстро зарекомендовал себя главной движущей силой всех сегодняшних инноваций благодаря возможностям и конкурентным преимуществам, которые раньше казались невероятными. Экспоненциальный рост информации открывает дорогу к новым достижениям во всех сферах – от транспорта и здравоохранения до энергетики и коммуникаций. Однако похоже, что наибольшие изменения ИИ привнесет именно в корпоративный сектор.

Опираясь на обширный опыт, специалисты компании VMware выделили три ключевых фактора, которые оказали наибольшее влияние на развитие искусственного интеллекта. Разберем каждый из них детально.

1. Вычисления – жажда скорости. За последние годы удалось достичь невероятного прогресса в производительности CPU и GPU. Вычислительные ресурсы FPGA и ASIC помогли сделать процесс обработки данных значительно быстрее и глубже. Кроме того, новые каналы развертывания (такие как GPU или ASIC, используемые в публичных облаках) позволяют заказчикам найти баланс между капитальными и операционными затратами на ИИ-инициативы.
2. Алгоритмы – уравнения сегодняшнего дня. Алгоритмы стали теоретическим фундаментом для ИИ и машинного обучения – от простейших нейронных сетей до более сложных, циклических и сверточных архитектур. Многие алгоритмы имеют многолетнюю историю, однако лишь недавно с их помощью стали производиться невероятные технологические прорывы. Почему? Во-первых, из-за достижений в работе с вычислениями. А во-вторых – из-за фактора номер 3.
3. Информация – новая нефть. Технологии машинного обучения, как известно, не так эффективно воспринимают информацию, как люди. Многие разработки на базе ИИ, такие как AlphaGo, обучаются на огромных базах данных, которые ни один человек не сможет обработать за всю свою жизнь. Без должной работы по развитию технологии машинного обучения не смогут достичь требуемого уровня производительности. А ведь совсем недавно, около 10 лет назад, количество данных, доступных для машинного обучения, составляло ничтожную долю от того, что доступно сегодня: от логов и метрик до протоколов и конфигураций.

Перспективы ИИ – самооптимизирующийся ЦОД

Резкое увеличение количества оперативных данных – это одновременно и хорошо, и плохо. В современном мире, где все зависит от центров обработки данных и облачных операций, компании отчаянно пытаются не отставать от потока информации, но с каждым годом делать это становится все сложнее. Сегодня платформы и инструменты уже не справляются с объемом данных, из-за чего растет нагрузка на людей – операторов и разработчиков.

Действительно, недавний отчет Enterprise Management Associates (*http://blog.enterprisemanagement.com/3-key-lessons-from-dockercon-2018-strategic-analysis-of-the-container-market-place*) говорит о том, что в среднем 30–40 % времени разработчиков тратится на борьбу с проблемами на стадии развертывания, конфигурации, тестирования, отладки и поддержки, а не на разработку новых решений. Такой «налог» неприемлем для организаций, работающих в высококонкурентных отраслях, ведь для них в первую очередь важна скорость.

ИИ позволит компаниям не просто избавиться от этого бремени, но и превратить его в стратегическое преимущество. Он поможет перейти к единой глобальной операционной модели, благодаря которой организации смогут извлекать из информации максимум пользы в режиме реального времени.

Искусственный интеллект заполнит пробел между сложностью в настройке необходимых процессов и операционным потенциалом. При этом некоторые сферы применения искусственного интеллекта позволят улучшить дата-центры: повысить эффективность работы,

Лучшим вариантом для современных ЦОД станет гибридный подход к построению облаков

VMware Cloud Foundation предоставляет удобный способ создания совместимого, масштабируемого и распределенного гибридного облака

сбалансировать затраты и производительность в режиме реального времени, обеспечить безопасность и оптимизировать бизнес-показатели.

Немного прогнозов

Едва ли стоит ожидать упрощения процесса работы с данными в ближайшем будущем: разница между машинными и человеческими возможностями продолжает расти. На фоне этого компании, неспособные расширить потенциал дата-центров, облаков и периферийных вычислений с помощью ИИ, рискуют отстать еще больше. И наоборот, предприятия, которые научатся использовать машинное обучение, получат важнейшие конкурентные преимущества.

Есть предположение, что гибридные центры обработки данных, облака и EDGE станут самовосстанавливающимися и самооптимизирующимися, тем самым значительно сокращая затраты на администрирование и позволяя сосредоточиться на стратегических инновациях и работе с клиентами. ИТ-инфраструктура с элементами ИИ, в свою очередь, раскроет потенциал саморегулирования, выходящий далеко за рамки сегодняшних возможностей, базирующихся на политиках.

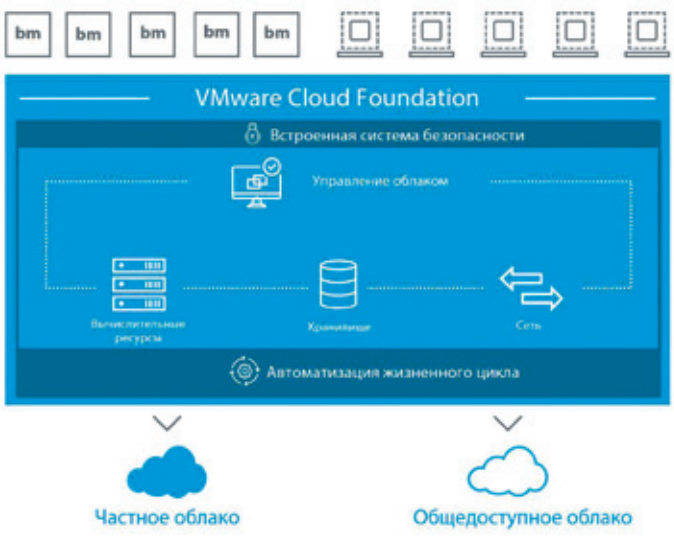
Мультиоблачная стратегия

Подготовка дата-центра к современным реалиям – задача нетривиальная. Начать стоит с подготовки ЦОД к внедрению ИИ-решений, которые в скором времени появятся на рынке. Например, ожидается принятие шаблонов Infrastructure-as-code (IAC), а также интеграция устаревших ручных процессов с API там, где это возможно.

Что касается данных, стоит рассмотреть возможность реализации периферийных вычислений – это позволит собирать информацию и проводить аналитику вблизи источника данных. Также стоит задуматься об инвестировании в программно-определяемую сеть как в ключевой фактор процесса трансформации.

Кроме того, лучшим вариантом станет гибридный подход к построению облаков. Развертывание гибридного облака позволит открыть новые возможности для масштабирования, а также обеспечит необходимую для внедрения прорывных технологий гибкость.

Решение VMware Cloud Foundation предоставляет самый удобный способ создания совместимого, масштабируемого и распределенного гибридного облака за счет использования единой инфраструктуры



и согласованной модели эксплуатации, которая объединяет локальный и внешний ЦОД.

VMware Cloud Foundation упрощает развертывание и использование гибридного облака и предоставляет интегрированную облачную инфраструктуру (вычислительные ресурсы, хранилище, сеть и средства безопасности) и службы управления облаком для выполнения корпоративных приложений в частных и общедоступных средах.

Платформа создана на базе ведущей гиперконвергентной архитектуры VMware (vSAN), которая существенно упрощает управление, обеспечивает высокую производительность систем и предоставляет услуги хранения корпоративного класса. Встроенные инструменты для автоматизации процессов – от приложений до инфраструктуры – обеспечивают эффективное планирование, администрирование и масштабирование программного ЦОД. Пользователям доступны возможности мониторинга и устранения неполадок, а также автоматизированное упреждающее управление, балансировка и исправление рабочих нагрузок.

Cloud Foundation повышает эффективность работы искусственного интеллекта и машинного обучения за счет поддержки графических процессоров в vSphere 6.7. В свою очередь, сочетание высокопроизводительного хранилища vSAN с горизонтально масштабируемым внешним хранилищем большой емкости дает возможность в зависимости от задач использовать подходящий тип хранилища и быстрее выполнять анализ больших данных.

По вопросам обращаться: *vmware@muk.ua*.

ДЕЛО В ШЛЯПЕ:
СЕРТИФИКАЦИЯ RED HAT НА БАЗЕ УЧЕБНОГО ЦЕНТРА МУК

Летом 2017 года Учебный центр МУК и Red Hat Limited заключили партнерское соглашение, согласно которому УЦ МУК получил официальный статус – Red Hat Certified Training Partner для таких стран: Азербайджан, Казахстан и Украина. Следующим шагом стало открытие в марте 2019 года станции тестирования для сдачи индивидуальных экзаменов Red Hat

Программа сертификации Red Hat является последовательной, аутентичной и надежной. Экзамены состоят из практических заданий, что делает их лучшими показателями вашего мастерства. Каждый экзамен проверяет способность выполнять актуальные ИТ-задачи, которые сопряжены с вашими рабочими обязанностями.

Благодаря формату индивидуального тестирования по всему миру экзамены Red Hat помогут вам подтвердить свои навыки и подготовиться к глобальному рынку. Вы можете сдать сертификационные экзамены в качестве индивидуального экзамена на безопасной станции тестирования в офисе партнеров Red Hat или непосредственно в офисе компании.

Индивидуальные экзамены Red Hat можно назначить в удобное для вас время. Это позволит подготовиться к ним за удобный период времени и сдать экзамен на ближайшей испытательной станции. Именно такая станция тестирования для сдачи индивидуальных экзаменов Red Hat открыта на базе Учебного центра.

Последовательность сдачи индивидуальных экзаменов Red Hat

Логистика – как сдавать экзамен?

Индивидуальные экзамены сдаются на отдельной рабочей станции, специально сконфигурированной Red Hat. Это безопасный, предварительно настроенный ноутбук. Станция тестирования гарантирует, что вам предоставлены все функциональные возможности, необходимые для экзамена, и сдача происходит безопасным способом, дистанционно контролируемым тестовым проктором Red Hat. Индивидуальные экзамены Red Hat также предусматривают дополнительное время для обучения – это очень удобно при наличии у вас плотного графика.

Начинаем – зарегистрироваться и сдать индивидуальный экзамен легко

Для регистрации на сдачу экзамена необходимо сделать несколько шагов:

1. Выберите необходимый экзамен и удобный способ обучения, затем заполните форму заказа и оформите платеж. Нет необходимости сразу же указывать место или время экзамена. Вы получите электронное письмо с подтверждением вашей покупки и подробным описанием следующих шагов.
2. Следуйте инструкциям в подтверждении покупки, чтобы войти в приложение планировщика и выбрать время, дату и место проведения экзамена. Вы получите электронное письмо с подтверждением запланированного экзамена и подробными инструкциями о том, что делать в день тестирования.
3. Приходите в выбранные дату и время и сдавайте экзамен.

Перед экзаменом

При сдаче экзамена необходимо следовать определенным инструкциям:

1. В день экзамена явиться в Тестовый Центр за 15 минут до начала экзамена, имея при себе документ, удостоверяющий личность (например, гражданский паспорт, загранпаспорт, водительские права, военный билет).
2. Перерыв в течение первого часа экзамена запрещен.
3. Убедитесь, что вы помните адрес электронной почты и пароль, которые вы использовали при заказе экзамена на сайте redhat.com. Данная информация понадобится вам для начала экзамена
4. Убедитесь, что ваш рабочий стол полностью чист. Проктор экзамена попросит вас переместить или убрать на столе все, что не связано с сдачей экзамена. Проктор может также попросить вас открыть все ящики стола и отсканировать их камерой во время экзамена.

5. Ознакомьтесь с разделом «Во время экзамена» данной статьи непосредственно перед экзаменом. Он содержит информацию об изменениях режима среды экзамена, которая может возникнуть во время сдачи.

Начало экзамена

Для того, чтобы начать экзамен, выполните следующие действия:

1. Нажмите пункт меню «Take an exam».
2. Ознакомьтесь и согласитесь с предоставленными инструкциями, затем нажмите «Continue».
3. Введите адрес электронной почты и пароль, которые вы использовали при заказе экзамена на сайте redhat.com.
4. Необходимо следовать инструкциям удаленного проктора. Ответственный проктор наблюдает за вами во время сдачи экзамена. Прокторы не являются техническими специалистами и, следовательно, не могут оказать помощь по техническим вопросам. При наличии проблемы со средой экзамена сообщите об этом проктору – он свяжется с Red Hat для технической поддержки.

Если у вас возникнут трудности с любым из указанных выше шагов или при подключении к проктору, необходимо обратиться к ответственному сотруднику тестового центра. Если ответственный сотрудник тестового центра недоступен, необходимо связаться с Red Hat по телефону +1-480-726-5818.

Во время экзамена

Вы не должны выключать питание на ноутбуке. Вы будете работать на одной или нескольких виртуальных машинах, поэтому нет никаких причин или необходимости в циклическом отключении питания либо перезагрузке рабочей станции. Это может привести к прерыванию сдачи экзамена и его переносу.

Результаты экзаменов Red Hat высылаются кандидатам в течение трех рабочих дней США.

Сдать выбранный экзамен на индивидуальной станции экзаменов Red Hat можно с понедельника по пятницу с 09:00 до 17:00 при наличии свободных мест.

Получить более подробную информацию об экзаменах и курсах Red Hat, а также узнать их стоимость можно, отправив заявку на *info@muk.training* или позвонив по телефонам:

Алматы: +77 (27) 346 7901;
Тбилиси: +995 (32) 260 1654;
Баку: +994 (12) 464 4350.

Список доступных экзаменов

Название экзамена	Код экзамена
Red Hat Certified Specialist in Ceph Storage Administration exam	EX125
Red Hat Certified Enterprise Application Developer exam	EX183
Red Hat Certified System Administrator (RHCSA) exam	EX200
Red Hat Certified System Administrator in Red Hat OpenStack exam	EX210
Red Hat Certified Specialist in Hybrid Cloud Management exam	EX220
Red Hat Certified Specialist in Gluster Storage Administration exam	EX236
Red Hat Certified Specialist in Enterprise Application Server Administration exam	EX248
Red Hat Certified Specialist in OpenShift Administration exam	EX280
Red Hat Certified Enterprise Microservices Developer exam	EX283
Red Hat Certified Specialist in OpenShift Application Development exam	EX288
Red Hat Certified Engineer (RHCE) exam	EX300
Red Hat Certified Engineer in Red Hat OpenStack exam	EX310
Red Hat Certified Specialist in Virtualization exam	EX318
Red Hat Certified Specialist in Linux Diagnostics and Troubleshooting exam	EX342
Red Hat Certified Specialist in Identity Management exam	EX362
Red Hat Certified Specialist in Deployment and Systems Management exam	EX403
Red Hat Certified Specialist in Configuration Management exam	EX405
Red Hat Certified Specialist in Ansible Automation exam	EX407
Red Hat Certified Specialist in Server Security and Hardening exam	EX413
Red Hat Certified Specialist in Security: Linux exam	EX415
Red Hat Certified Specialist in Camel Development exam	EX421
Red Hat Certified Specialist in Business Process Design exam	EX427
Red Hat Certified Specialist in High Availability Clustering exam	EX436
Red Hat Certified Specialist in Messaging Administration exam	EX440
Red Hat Certified Specialist in Linux Performance Tuning exam	EX442
Red Hat Certified Specialist in Data Virtualization exam	EX450
Red Hat Certified Specialist in Fast-Cache Application Development exam	EX453
Red Hat Certified Specialist in Business Rules exam	EX465

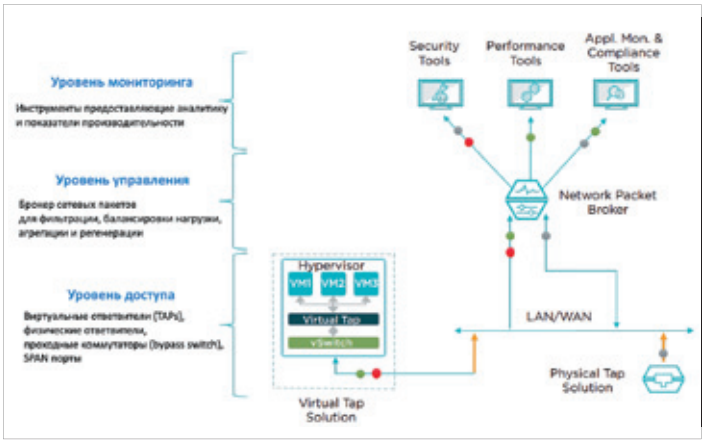
НЕ ПРОПУСТИТЬ НИЧЕГО:

ИСПОЛЬЗОВАНИЕ РЕШЕНИЙ IXIA ДЛЯ ОБЕСПЕЧЕНИЯ ВИДИМОСТИ СЕТИ

Невозможно контролировать то, что нельзя увидеть – этот тезис имеет право на жизнь практически в любой сфере деятельности. Применим он и для построения и управления сетевой инфраструктурой организации. Поэтому одной из главных задач ИТ-отделов является обеспечение так называемой видимости сети (Network Visibility)

Под видимостью сети или приложения подразумевается удаление «слепых зон», которые скрывают способность видеть или количественно определять, что происходит в сети и/или приложениях в этой сети. Она позволяет ИТ-командам быстро изолировать угрозы безопасности и решать проблемы с производительностью, что в конечном итоге обеспечивает наилучшее взаимодействие с пользователями сети.

Еще одна трактовка этого термина – это то, что позволяет ИТ-командам контролировать и оптимизировать сеть наряду с приложениями и ИТ-сервисами. Именно поэтому видимость сети, приложений и безопасности абсолютно необходима для любой организации.



Три основных уровня архитектуры видимости: доступ, управление и мониторинг

Самый простой способ организовать видимость сети – это реализовать архитектуру видимости (Visibility Architecture), которая представляет собой комплексную end-to-end-инфраструктуру и обеспечивает видимость физической и виртуальной сети, приложений и безопасности.

Закладка фундамента

Как только будет создана архитектура видимости, станет доступно множество вариантов ее использования. Как видно из скриншота, архитектура видимости представляет три основных уровня видимости: уровни доступа, управления и мониторинга.

Используя эти элементы, ИТ-специалисты могут решать различные проблемы сети и приложений. Есть две категории вариантов применения:

- основные решения видимости;
- полная видимость сети.

Основные решения видимости ориентированы на безопасность сети, экономию средств и устранение неполадок. Это три критерия, которые влияют на ИТ ежемесячно и даже ежедневно. Полная видимость сети призвана обеспечить более глубокое понимание областей слепых зон, производительности и соответствия нормативным требованиям.

Возникает вопрос: как можно использовать видимость сети? Существует шесть различных вариантов ее применения:

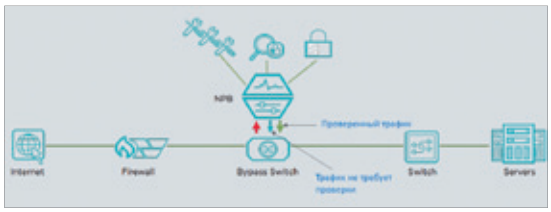
- повышение безопасности сети;
- предоставление возможностей сдерживания и снижения затрат;
- ускорение траблшутинга и повышение надежности сети;
- устранение слепых зон сети;
- оптимизация производительности сети и приложений;
- укрепление соблюдения нормативных требований.

Далее рассмотрим несколько конкретных примеров использования видимости сети.

Пример № 1 – фильтрация данных для решений безопасности, которые стоят в разрыве сети (in-line), повышает эффективность данных решений

Суть этого варианта заключается в использовании брокера сетевых пакетов (NPB – Network Packet Broker) для фильтрации данных с низким риском (например, видео и голос), чтобы исключать их из проверки средствами безопасности (системой предотвращения вторжений (IPS), модулем предотвращения потери данных (DLP), сетевым экраном для веб-приложений (WAF) и т. д.). Этот «неинтересный» трафик может быть определен и передан обратно на обходной коммутатор (by-pass switch) и отправлен далее в сеть. Преимущество этого решения состоит в том, что WAF или IPS не должны тратить ресурсы процессора на анализ ненужных данных. Если сетевой трафик содержит значительный объем данных этого типа, можно реализовать эту функцию и снизить нагрузку на инструменты безопасности.

Бывали случаи, когда до 35 % сетевого трафика с низким уровнем риска было исключено из проверки



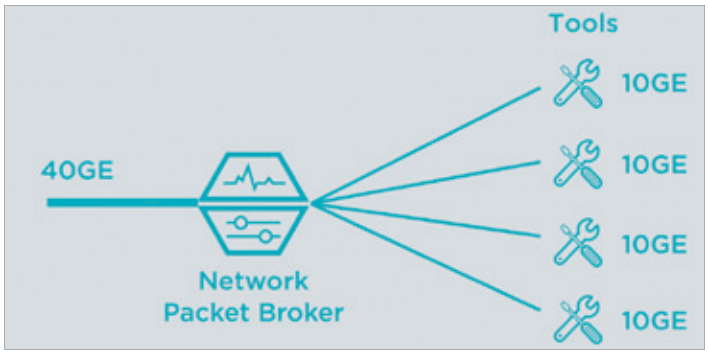
Использование брокера сетевых пакетов дает возможность снизить нагрузку на системы безопасности

IPS. Это автоматически увеличивает эффективную полосу пропускания IPS на 35 % и означает, что можно минимизировать расходы и отложить апгрейд или приобретение дополнительных IPS.

Пример № 2 – балансировка нагрузки продлевает жизнь устройств 1–10 Гбит/с в сети 40 Гбит/с

Второй пример использования предусматривает снижение стоимости сетевого оборудования. Это достигается с помощью пакет-брокеров (NPB) для балансировки трафика на инструменты безопасности и мониторинга. Как балансировка нагрузки может помочь большинству предприятий? Во-первых, увеличение объемов сетевого трафика наряду с ростом скорости является очень распространенным явлением. Но как насчет мониторинга влияния роста пропускной способности? Например, если вы модернизируете ядро сети с 1 Гбит/с до 10 Гбит/с, то вам потребуются решения с пропускной способностью 10 Гбит/с для корректного мониторинга. Если вы повысите скорость до 40 или 100 Гбит/с, то при таких скоростях выбор инструментов мониторинга будет намного меньшим, а их стоимость – очень высокой.

Пакет-брокеры предоставляют необходимые возможности агрегации и балансировки нагрузки. Например, балансировка трафика 40 Гбит/с позволяет распределить трафик монито-



Балансировка трафика со скоростью 40 Гбит/с позволяет распределить трафик мониторинга между несколькими 10-гигабитными инструментами

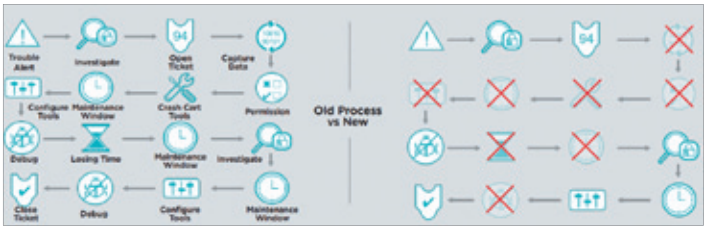
ринга между несколькими 10-гигабитными инструментами. После этого можно продлить срок службы 10-гигабитных устройств, пока не появится достаточно средств для приобретения более дорогих инструментов, способных справляться с более высокими скоростями передачи данных.

Другой вариант – объединить инструменты в одном месте и передать им необходимые данные от брокера пакетов. Иногда используются отдельные решения, распределенные по сети. Данные опроса, проведенного компанией Enterprise Management Associates (EMA) за 2016 год, показывают, что 32 % корпоративных решений недостаточно загружены, то есть менее чем на 50 %. Централизация инструментов и балансировка нагрузки позволяют объединять ресурсы и оптимизировать их использование, применяя меньше устройств. Можно откладывать приобретение дополнительных инструментов до тех пор, пока коэффициент использования не станет достаточно высоким.

Пример № 3 – траблшутинг для уменьшения/устранения потребности в получении разрешений на изменения (Change Board permissions)

После того, как оборудование для видимости (ответвители (TAPs), NPB и т. д.) установлено, вносить изменения в сеть придется достаточно редко. Это позволяет оптимизировать некоторые процессы устранения неполадок, чтобы повысить эффективность работы.

Например, после того, как TAP установлен, он пассивно передает копию всего трафика в NPB. Это дает огромное преимущество, поскольку устраняет большую часть бюрократических проволочек, таких как получение одобрений для внесения изменений в сеть. Также если установить брокер пакетов, будет обеспечиваться мгновенный доступ практически ко всем данным, которые нужны для траблшутинга.



Установка оборудования для видимости сети позволит оптимизировать процессы устранения неполадок

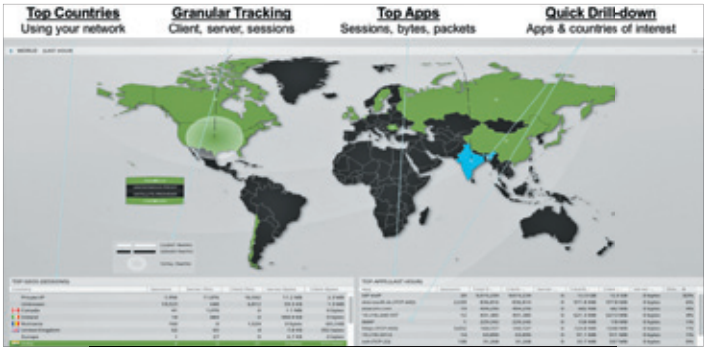
Если потребности во внесении изменений нет, можно пропустить этапы их согласования и перейти непосредственно к отладке. Этот новый процесс оказывает большое влияние на сокращение среднего времени на восстановление (MTTR – Mean Time to Repair). Исследования показывают, что заказчики могут снизить MTTR до 80 %.

Пример № 4 – Application Intelligence, применение фильтрации приложений и маскировки данных для повышения эффективности безопасности

Прежде всего, разберемся, что такое интеллект приложений (Application Intelligence). Это технология, доступная у брокеров пакетов (NPB) IXIA. Она предоставляет расширенную функциональность, позволяющую выйти за пределы фильтрации пакетов уровня 2–4 модели OSI и полностью перейти на уровень 7 (прикладной уровень). Ее преимущество заключается в том, что данные о поведении и местонахождении пользователей и приложений могут создаваться и экспортироваться в любом необходимом формате – необработанные пакеты, отфильтрованные пакеты или информация NetFlow. ИТ-отделы могут выявлять скрытые сетевые приложения, уменьшать угрозы сетевой безопасности, а также снижать простои сети и/или повышать ее производительность. Отличительные подписи для известных и неизвестных приложений могут быть идентифицированы, захвачены и переданы специализированным инструментам мониторинга и безопасности.

Интеллект приложений делает возможным осуществление следующих функций:

- идентификация подозрительных/неизвестных приложений;
- выявление подозрительного поведения по геолокации, например, пользователь из Северной Кореи подключается к FTP-серверу и передает данные;
- расшифровка SSL для проверки и анализа потенциальных угроз;
- анализ неправильной работы приложений;

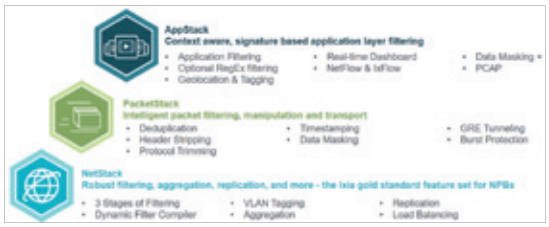


Интеллект приложений дает возможность выявлять и отправлять администраторам сети различную информацию о пользователях и приложениях

- анализ количества и роста трафика для активного управления ресурсами и прогнозирования расширения;
- маскировка конфиденциальных данных (кредитные карты, учетные данные и т. д.) перед отправкой.

Функционал Visibility Intelligence доступен как в физических и виртуальных (Cloud Lens Private) пакет-брокерах IXIA (NPB), так и в публичных облаках – Cloud Lens Public.

Кроме стандартного набора возможностей NetStack, PacketStack и AppStack, за последнее время был добавлен также функционал безопасности SecureStack для оптимизации обработки конфиденциального трафика, MobileStack для операторов мобильной связи и TraeStack для мониторинга и фильтрации данных финансового трейдинга.



Стандартный набор возможностей NetStack, PacketStack и AppStack

Функционал TraeStack для мониторинга и фильтрации данных финансового трейдинга

В сухом остатке

Из всего вышесказанного видно, что решения для видимости сети от IXIA – мощный инструмент, способный оптимизировать архитектуру сетевого мониторинга и безопасности, который позволяет организовать фундаментальный сбор и обмен необходимыми данными.

Варианты использования инструментов для обеспечения видимости сети позволяют:

- давать доступ к нужным специфическим данным по мере необходимости для диагностики и траблшутинга;
- добавлять/удалять решения безопасности и мониторинга как in-line, так и out-of-band;
- уменьшить MTTR;
- обеспечить быстрое реагирование на проблемы;
- проводить расширенный анализ угроз;
- устранить большинство бюрократических согласований;
- снизить финансовые последствия взлома, оперативно подключив нужные решения в сеть и уменьшив MTTR;
- сократить стоимость и трудозатраты по настройке SPAN-порта.

По вопросам обращаться: *ixia@muk.ua*.

ШЕСТОЕ ЧУВСТВО:
AVIGILON PRESENCE DETECTOR

Традиционно камеры являются «глазами» системы видеонаблюдения. Но эти «глаза» не всегда способны заметить на наблюдаемой территории или объекте чье-либо присутствие, особенно если этот кто-то стремится остаться незамеченным. Выявить незваных гостей в таких случаях позволит Avigilon Presence Detector

Avigilon Presence Detector представляет собой радарный датчик малого форм-фактора, который сочетает в себе самообучающуюся аналитику и технологию импульсного радара. Он дает возможность обнаружить присутствие людей на расстоянии до 9 м с точностью до 99 %, даже если они перестали двигаться или спрятались. Датчик не полагается на визуальные данные, поэтому может работать в условиях полного отсутствия освещения.

Это делает Avigilon Presence Detector отличным решением для объектов, где важна конфиденциальность данных. Он предназначен для размещения внутри помещений и отлично подойдет для банкоматов, вестибюлей банков, магазинов, аптек, медицинских учреждений и даже тюрем.

Avigilon Presence Detector позволяет обнаружить присутствие людей, даже если они перестали двигаться или спрятались

Импульсная радиолокация

Presence Detector является радиолокационным устройством, оснащенным функциями анализа радиолокационных данных и самообучения. Оно сканирует окружающую обстановку, при этом постоянно адаптируясь к ее изменениям. Это дает возможность обеспечить высокую точность определения присутствия человека и делает сенсор хорошим решением для помещений, где применение традиционных устройств может быть неэффективно. Сканер позволяет определить присутствие даже в случае, если объект не виден или закрыт препятствием – покрывалом, картоном, гипсокартоном, деревом и т. д.

Решение использует технологию импульсной радиолокации, при которой импульсный радар излучает сигналы с небольшой энергией и на короткие расстояния. Однако спектр частот сигналов при этом гораздо более широкий, нежели у обычных радиолокационных систем (так называемая широкая полоса, или Ultra-Wide Band). Именно это позволяет эффективно обнаруживать неподвижных или прячущихся людей, детектировать незаметное движение и даже дыхание. Также стоит отметить, что радиолокационная технология не снимает и не отображает такие элементы, как клавиатуры банкоматов и лица людей, что позволяет обеспечить полную конфиденциальность.

Установка и интеграция

Детектор Avigilon Presence Detector имеет компактный размер, что позволяет органично и, главное, незаметно вписаться в окружающую обстановку. Устройство может иметь два варианта монтажа – на стене и на горизонтальной поверхности.

Установка решения упрощается тем, что оно использует стандартную IP-инфраструктуру. Стоит также отметить, что Presence Detector интегрирован с программным обеспечением Avigilon Control Center для управления видеоданными. Это дает возможность повысить эффективность системы видеонаблюдения, своевременно информируя операторов о событиях безопасности и необходимости предпринять необходимые действия.

По вопросам обращаться: *avigilon@muk.ua*.

ВЕБ-САЙТ ПОД ЗАЩИТОЙ:
PENTA SECURITY WAPPLES

Сегодня во всем мире частота инцидентов, связанных с нарушением безопасности веб-сайтов, таких как утечка данных и атаки на веб-страницы, достигли беспрецедентного масштаба. Обезопасить веб-ресурсы компании позволит межсетевой экран веб-приложений (Web Application Firewall)

Практически все компании, независимо от масштаба и сферы деятельности, используют веб-сайты и веб-приложения. Интернет-магазины, интернет-банкинг, сайты служб доставки и многие другие ресурсы стали неотъемлемой частью нашей жизни. На веб-интерфейсы переходят системы управления электронным документооборотом, бухгалтерией, почтой и многие другие приложения, без которых современный бизнес уже не возможен.

Penta Security WAPPLES представляет собой третье поколение устройств класса Web Application Firewall, основанное на искусственном интеллекте

Все эти сайты и сервисы обрабатывают личные данные и содержат множество финансовой информации как о клиентах, так и о самих компаниях, становясь в итоге желанной целью для злоумышленников.

По данным компании Verizone, атаки на веб-ресурсы уже сейчас составили более 20 % от общего объема инцидентов безопасности. Потенциальными целями являются практически все отрасли, включая финансовые услуги, информационные технологии, государственный сектор, производство и др. Последствия при достижении цели атаки могут быть серьезными – ущерб репутации компании, нарушение бизнес-процессов и даже юридические тяжбы.

Что такое безопасность веб-приложений?

По своей сути безопасность веб-приложений представляет собой предотвращение и смягчение атак, направленных на них. Общими целями являются системы управления контентом, базы данных и облачные приложения, которые обычно используются для управления видимыми элементами веб-сайтов и онлайн-сервисов.

При этом, согласно прошлогоднему отчету Positive Technologies, почти половина веб-приложений уязвимы для несанкционированного доступа, и во всех протестированных были обнаружены уязвимости среднего уровня. Даже при наличии решений для обеспечения безопасности существует высокая вероятность того, что эти системы неправильно настроены или развернуты, и могут допустить относительно небольшие уязвимости, которые могут привести к масштабным нарушениям.

Для того чтобы понять, что именно и как необходимо обезопасить, нужно пройти три этапа, которые

помогут правильно расставить приоритеты и выбрать подходящую защиту для веб-приложений компании.

Шаг 1. Оцените масштаб. Насколько критичны веб-приложения для вашей организации?

Первым шагом в планировании организации безопасности является понимание объема и типа ценных активов. Для веб-приложений важно учитывать их роль и значение для критически важных бизнес-операций.

Например, если сайт в системе управления контентом сохраняет личную информацию посетителей в серверной базе данных, то состояние веб-приложений может значительно повлиять на бизнес. И наоборот, если на веб-сайте не размещена конфиденциальная информация, самые изощренные меры безопасности не понадобятся. Другими словами, потребности в безопасности определяются тем, насколько бизнес организации чувствителен к таким факторам, как время простоя веб-сайта и кража данных, которые могут напрямую повлиять на доходы компании, бренд и удовлетворенность клиентов. Чем больше эти факторы влияют на успех бизнеса, тем выше будет потребность в развертывании защиты, оптимизированной для конкретной ИТ-среды и обеспечивающей быструю защиту как от распространенных, так и от сложных угроз.

Шаг 2. Рассмотрите затраты – насколько ценны ваши активы?

Еще одно базовое правило в планировании системы безопасности: для предотвращения атак взлом системы должен быть более дорогостоящим, чем ценность данных компании. Это особенно важно, поскольку уязвимые веб-приложения, как правило, являются недорогими объектами атак с потенциально высокой отдачей.

Обычно важность данных определяется такими факторами, как интеллектуальная ценность, стоимость при перепродаже и персональная ценность. Если ваши данные ценны, для повышения финансовых затрат взлома потребуется расширенная защита, которая разумно адаптируется к возникающим угрозам.

Распределение бюджета и внимания также важно при планировании безопасности веб-приложений. При ограниченных ресурсах необходимо отдавать предпочтение безопасности веб-приложений с наиболее важными ролями в бизнесе. Например, веб-сайтам с «тяжелыми» внутренними базами данных потребуется активная защита от SQL-инъекций, когда злоумышленник вводит вредоносный код на уязвимом веб-сайте для получения доступа к внутренним ресурсам. В этом случае целесообразно подобрать брандмауэр веб-приложений (WAF), который протестирован и доказал свою эффективность против SQL-инъекций.

Шаг 3: Определитесь с реализацией – какое решение отвечает вашим потребностям?

Требования безопасности веб-приложений могут быть наиболее эффективно решены путем развертывания брандмауэра веб-приложений (Web Application Firewall, WAF). При выборе WAF необходимо учитывать два ключевых момента:

1. Способ развертывания: локальное, облачное, гибридное или сервисное.
2. Насколько эффективна технология блокирования угроз.

В конечном итоге, любое решение по обеспечению безопасности может оказаться неэффективным, если оно не настроено должным образом. Следовательно, важно выбрать WAF, который подходит для масштаба и среды организации. Для малого и среднего бизнеса может быть удобно развернуть Security-as-a-Service (SaaS) или масштабируемое облачное решение, тогда

Среднее время настройки Penta Security WAPPLES составляет около 15 минут

Даже при наличии решений для обеспечения безопасности существует высокая вероятность того, что эти системы могут быть неправильно настроены или развернуты, и могут допустить относительно небольшие уязвимости, которые могут привести к масштабным нарушениям

как финансовые учреждения или более крупные предприятия могут выбрать невиртуальные решения, соответствующие отраслевым стандартам и правилам соответствия для защита данных.

С технологической точки зрения важно выбрать решение, которое, помимо защиты от известных угроз и OWASP Top 10 (*https://www.owasp.org/images/9/96/OWASP_Top_10-2017-ru.pdf*), также предохраняет от атак нулевого дня и DDoS-атак. В условиях непрерывно развивающегося ландшафта угроз ключ к эффективной защите лежит в интеллектуальных политиках безопасности, которые обеспечивают низкий уровень ложных срабатываний. Наконец, нужно убедиться, что выбрано решение с удобной консолью управления для поддержки регулярного тестирования и обслуживания WAF.

Отдельно стоит остановиться на противодействии уязвимостям OWASP Top 10 со стороны различных средств сетевой безопасности. Рассмотрим это на примере обычного межсетевого экрана (FW или NGFW), системы обнаружения вторжений (IPS/IDS) и WAF (см. таблицу «Уязвимости OWASP Top 10 vs средства сетевой безопасности»).

Как видно из таблицы, обычные средства межсетевых экранов о HTTP-трафике практически ничего не знают. Как максимум – политика откроет порт/протокол и все данные внутри этих запросов и ответов сервера будут проходить без каких-либо преград. С ними же будут проходить и данные, передаваемые атакующим, словно межсетевого экрана и нет совсем. Конечно, сам по себе межсетевой экран нужен хотя бы для ограничения всего остального трафика, который не должен из внешнего мира попадать на сервер, а также для того, чтобы исключить доступ к базе данных, средствам администрирования из консоли или другим портам транспортного уровня. Но на этом его задача по ограничению доступа будет выполнена.

Системы обнаружения вторжений смогут проанализировать структуру протокола передачи данных, если получат расшифрованный трафик, чего сейчас почти не умеет делать практически ни один из межсетевых экранов. Расшифровка трафика SSL/TLS реализована на всех современных межсетевых экранах, но обычно – по направлению от пользователя в Интернет. В обратном же направлении, из Интернета к серверу, в большинстве случаев возможности нет. На некоторых IPS реализованы сигнатуры обнаружения SQL-кода. Есть некоторые технологии встроенных потоковых DLP, что позволяет частично закрыть A3.

Но что делать, если объем трафика исчисляется гигабитами? Расшифровать такое количество данных – задача непростая. Если заниматься таким шифрованием на межсетевом экране, это приведет к существенной нагрузке на процессоры, да и стоимость процесса будет достаточно высокой. Единственный тип уязвимости при отсутствии шифрования, с которым может справится IPS, – это старые сигнатуры атаки на хорошо известные «дыры в приложениях» (Apache).

Стоит еще раз подчеркнуть, что IPS/IDS и прочие средства анализа трафика подействуют, только если они умеют работать со множеством сайтов и имеют ключи для шифрования. С обычным TLS/SSL-трафиком они не могут сделать ничего, кроме проверки порта транспортного уровня (TCP).

В свою очередь, WAF как специализированное средство безопасности принимает на себя все функции по криптографии от веб-сервера. Хорошей практикой считается, если WAF поддерживает шифрование данных к пользователю, но на веб-сервер отправляет чистый HTTP-трафик. В этом случае веб-серверы не хранят атрибуты шифрования, ключи и сертификаты. То есть ключи мигрируют из приложения в отдел безопасности. Теперь, поскольку трафик расшифрован, его можно очистить от любых вредоносных изменений.

WAF: какие они бывают?

Конечно, возникает вопрос: неужели установка WAF станет панацеей от всего? Давайте сперва разберемся, какие существуют типы брандмауэров веб-приложений. Большинство доступных сейчас WAF – первого и второго поколения. Они используют сигнатуры подобно продвинутым IPS-системам и уже

Уязвимости OWASP Top 10 vs средства сетевой безопасности

№ п/п	Название уязвимости OWASP TOP 10	NGFW	IPS/IDS	WAF
1	A1:2017 – Инъекции, они же «Внедрение кода»	нет	частично	да
2	A2:2017 – Некорректная аутентификация	нет	частично	да
3	A3:2017 – Раскрытие чувствительной информации	нет	частично	да
4	A4:2017 – Внедрение внешних XML-сущностей (XXE)	нет	нет	да
5	A5:2017 – Нарушенный контроль доступа	нет	нет	да
6	A6:2017 – Security Misconfiguration – ошибки в конфигурировании	нет	нет	да
7	A7:2017 – Межсайтовый скриптинг (XSS)	нет	нет	да
8	A8:2017 – Небезопасная десериализация	нет	нет	да
9	A9:2017 – Использование компонентов с известными уязвимостями	нет	да	да
10	A10:2017 – Недостаточное журналирование и мониторинг	нет	нет	да

анализируют структуру сайтов и пакеты данных. И все же использование сигнатурного метода обнаружения уязвимостей накладывает свой отпечаток. Для создания сигнатуры необходимо, чтобы о существовании уязвимости как минимум имел представление разработчик системы безопасности. После чего будет создана соответствующая сигнатура, добавлена в обновление, и только через какое-то время администратор сможет загрузить обновленную базу сигнатур для защиты приложения. В среднем это может занимать от нескольких дней до нескольких месяцев. А что же делать уникальным приложениям, которые создаются собственными отделами разработки? Эти приложения никогда не попадут в отдел разработки сигнатур ведущих производителей WAF.

Компания Penta Security Systems создала новый тип WAF, используя современные технологии. Это уже новое, третье поколение подобных устройств, основанное на искусственном интеллекте. Теперь в сигнатурах уязвимостей нет необходимости, процессорной мощности хватает, чтобы проанализировать работу сервера и пользователя в реальном времени. WAPPLES анализирует страницы, передаваемые пользователям от сервера, и строит в базе знаний логические связи о том, как работает то или иное приложение и какие данные ожидает от пользователя. Затем подписывает все атрибуты, передаваемые пользователю, и накапливает информацию о состоянии соединения. Таким образом, присутствует вся необходимая информация для принятия решения о соответствии данных ожиданиям сервера. И когда пользователь сделает следующий шаг по веб-сайту, WAF сможет передать на сервер только безопасные данные. Нет необходимости накапливать данные о работе сайта долго, каждый новый запрос рассматривается как новый, и строится новая база знаний о сервере и пользователе. Это позволяет закрыть вопрос как старых, так и новых, еще не известных, уязвимостей.

Если рассматривать традиционные WAF с точки зрения администрирования информационных систем, необходимо обучаться и сдавать экзамен за экзаменом, чтобы разобраться в огромном количестве настроек и технологий, которые они используют. Большое число настроек приводит к достаточно трудоемкому процессу внедрения и механическим ошибкам в конфигурации. Чем сложнее интерфейс – тем больше поле для ошибок. Penta Security Systems создала по сути гениальный интерфейс для администратора. Всего 28 правил – и то не для каждого сайта необходимо использовать все. Для большинства типичных внедрений есть уже готовые политики, достаточно добавить сайт и поместить его в нужную политику, на этом конфигурация завершена. Среднее время для настройки WAPPLES – 15 минут, и после этого защита уже работает на полную мощность. Простота управления позволяет существенно облегчить внедрение и содержание средств защиты.

Отдельно необходимо остановиться на задержках в обработке пакета: нужно просто сравнить обработку тысячами сигнатур и 28 правилами. В устройстве от Penta Security Systems задержки составляют менее 1/1000 секунды. Что позволяет использовать систему в самых высоконагруженных проектах совершенно без потери качества сервиса. Поскольку анализируются пакеты данных как к серверу, так и от сервера, в полной мере срабатывают правила, позволяющие избежать раскрытия чувствительной информации или утечки данных.

Penta Security Systems предлагает несколько вариантов WAF, чтобы помочь защитить клиентские приложения в локальных центрах обработки данных, облачной инфраструктуре и виртуальных средах. WAPPLES – это комплексное решение WAF, доступное в виде физического или виртуального устройства (WAPPLES-SA). WAPPLES использует запатентованный механизм обнаружения логических операций, известный как «Обработка классификации и оценки содержимого» (COCEP), который использует методы семантического и эвристического анализа для обнаружения и блокировки известных и неизвестных угроз. В решении используется механизм анализа на основе логики для обеспечения низкого уровня ложных срабатываний и предотвращения утечки данных.

Для малого и среднего бизнеса может быть удобно развернуть Security-as-a-Service (SaaS) или масштабируемое облачное решение, тогда как финансовые учреждения или более крупные предприятия могут выбрать невиртуальные решения, соответствующие отраслевым стандартам

Решения Penta Security Systems легко интегрируются с другими средствами обеспечения безопасности, включая Open Source-продукты. Для интеграции можно использовать операторские SNMP- или syslog-протоколы, также есть коннекторы для SIEM-систем. Для крупных проектов имеется специальное решение Cloud WAF с хорошо документированным API для интеграции в облачные контроллеры или системы управления услугами хостинга.

Также стоит отметить, что на базе Учебного центра МУК на регулярной основе осуществляется подготовка специалистов по защите веб-сайтов. В программу входит углубленное изучение веб-технологий, уязвимостей и решений Penta Security Systems. Хороший набор практических работ позволяет получить и закрепить знания о настройке и обслуживанию WAF WAPPLES, эксплуатации уязвимостей и возможностях систем противодействия.

По вопросам обращаться: *penta@muk.ua*.

ОЦИФРОВАТЬ ВСЕ:
КНИЖНЫЕ СКАНЕРЫ QIDENUS

Большинству организаций для управления документооборотом, в частности сканирования различных документов, вполне достаточно традиционных сканеров. Однако в тех случаях, когда задачи оцифровки достигают промышленных масштабов, помогут лишь специализированные решения

Разумеется, когда речь идет о том, чтобы отсканировать десяток-другой документов в день, стандартного сканера или МФУ вполне достаточно. Однако если речь заходит о создании электронной базы данных или библиотеки из различных бумажных носителей (книг, карт, брошюр разного формата и т. д.), привычное оборудование вряд ли окажется эффективным как в плане скорости работы, так и с точки зрения взаимодействия с документами нестандартных форматов. В таких случаях следует применить специализированные решения – например, книжные сканеры Qidenus. Они широко используются по всему миру и прекрасно подойдут для национальных библиотек, музеев, университетов, архивов и других организаций, нуждающихся в оцифровке книг. Далее подробнее рассмотрим линейку сканеров Qidenus – модели разного уровня для организаций различных масштабов: ручной Smart и автоматические Mastered и Robotic.

Полуавтоматический сканер Mastered является наиболее универсальной моделью в портфеле решений Qidenus

Qidenus Smart предназначен для индивидуальной работы в режиме «одна книга – один оператор»

Qidenus Smart

Qidenus Smart Book Scan представляет собой ручной книжный сканер, который обеспечивает высокое качество изображения, при этом сочетая в себе отличные показатели производительности и скорости с простотой обращения. Модель оснащается V-образной колыбелью и V-образным прижимным стеклом толщиной 3 мм с двойным покрытием. Скорость сканирования модели составляет до 1000 страниц в час. Угол раскрытия 100° и регулируемые боковые створки обеспечивают опору для корешка книги. Qidenus Smart позволяет сканировать хрупкие, поврежденные кислотой, разорванные и разрозненные страницы. В устройстве используются новейшие камеры и объективы, обеспечивающие соответствие стандартам FADGI и Metamorfoze. Возможен вывод изображений в форматах JPEG, TIFF, GIF, RAW, PDF, PDF OCR, XML.

Доминик Матон,
коммерческий директор компании iGuana в странах СНГ

Qidenus Technologies, входящая в группу компаний iGuana, является мировым лидером на рынке V-образных и роботизированных книжных сканеров. Сканеры Qidenus пользуются доверием ряда крупных организаций по всему миру, деятельность которых связана с оцифровкой больших объемов информации. Широкий спектр сканеров Qidenus – от ручных до полуавтоматических и автоматических – позволяет удовлетворить любые потребности и бюджеты организаций различных масштабов.

Qidenus Robotic – самая мощная модель линейки книжных сканеров компании

Сканер предназначен для индивидуальной работы в режиме «одна книга – один оператор». При этом оператор вручную контролирует книжную подставку сканера, положение стеклянной панели и скорость работы.

Qidenus Smart Book Scan сканирует практически все типы книг толщиной до 160 мм и доступен в форматах A2 и A1. В первом случае максимальный размер книги составляет 58x44 см (страницы – 29x44 см), а разрешение изображения – 300/400/500 точек на дюйм, во втором – соответственно 82x61 см (страницы – 41x61 см) и 300/400 точек на дюйм.

Qidenus Mastered

Qidenus Mastered Book Scan разработан для масштабной оцифровки книг. Это полуавтоматический книжный сканер, являющийся наиболее универсальной моделью в портфеле Qidenus. Он предлагает самый широкий диапазон размеров области сканирования и разрешения в зависимости от формата. Сканер оснащен самоцентрирующейся подставкой с мягким углом раскрытия 80°. В сочетании с автоматизированной стеклянной панелью это обеспечивает высокую скорость сканирования – до 1500 страниц в час. Кроме того, такая конструкция позволяет избежать кривизны при сканировании и оцифровывать даже самые хрупкие оригиналы, не боясь повредить их. Доступен широкий набор форматов для вывода результата: JPEG, TIFF, GIF, RAW, PDF, PDF OCR, XML.

Модель дает возможность сканировать практически все типы книг толщиной до 160 мм. Есть возможность создания шаблонов с предустановленными настройками для быстрой обработки, а также набор специального программного обеспечения для постобработки и управления технологическим процессом.

Устройство доступно в четырех форматах: A1, A2, A2+ и A3+. Каждый из форматов предусматривает собственные характеристики максимального размера страниц и доступного разрешения изображений:

- формат A1: 76x58 см, 300 точек на дюйм;
- формат A2: 60x44 см, 300/400/500 точек на дюйм;
- формат A2+: 64x48 см, 300/400/500 точек на дюйм;
- формат A3+: 56x37 см, 300/400/600 точек на дюйм, максимальная толщина – 16 см.

Также стоит отметить, что сканер может быть легко модернизирован и переключается в ручной режим работы простым нажатием кнопки – это позволяет тщательно оцифровывать хрупкие книги.

Qidenus Robotic

Самой мощной моделью линейки сканеров является Qidenus Robotic Book Scan. Это полностью автоматизированный сканер, предназначенный для оцифровки книг и документов в масштабах национальных библиотек и способный поддерживать круглосуточный режим работы. Скорость сканирования устройства составляет до 2500 страниц в час. Модель предусматривает три режима работы: полностью автоматический, полуавтоматический и ручной для наиболее ветхих оригиналов. Переключение между режимами работы осуществляется одним нажатием кнопки.

Как и предыдущая модель, Qidenus Robotic оснащен V-образной подставкой для книг и стеклянной панелью, имеет угол раскрытия оригинала 80°. Устройство использует в работе новейшие сенсоры CMOS. Из интересных особенностей сканера – уникальная запатентованная система автоматического перелистывания страниц Bionic Finger. Ее суть заключается в имитации естественного движения пальца, позволяющей в автоматическом режиме разделять, переворачивать и обрабатывать по одной странице. Кроме того, реализована система контроля сдвоенных страниц – специальные датчики автоматически измеряют плотность страниц, благодаря чему за один прогон переворачивается и сканируется только одна страница.

Как и предыдущие модели, Qidenus Robotic работает с книгами, толщина которых не превышает 160 мм. Устройство позволяет сканировать страницы любого качества и текстуры с плотностью бумаги в диапазоне 30–350 г/м^2. Выходные форматы сканера – JPEG, TIFF, GIF, RAW, PDF, PDF OCR, XML.

Модель доступна в двух форматах – A2 и A3+, отличающихся по максимальному размеру книги, разрешению изображения, а также максимальной толщине книги. Для формата A2 эти показатели равны 60x44 см, 300/400/500 точек на дюйм и 16 см, для A3+ – 56x37 см, 300/400/600 точек на дюйм и 12 см соответственно.

По вопросам обращаться: *dsc@muk.ua*.

ПРОИЗВОДИТЕЛЬНОСТЬ ДЛЯ ЦОД:

СЕРВЕРЫ FUJITSU PRIMERGY CX400 M4

По мере роста инфраструктуры компаний, бизнес-процессов и числа приложений организациям требуются определенные ресурсы, позволяющие оптимизировать работу пользователей. В свете растущих потребностей оптимальным выбором для горизонтального масштабирования инфраструктуры станут серверы Fujitsu PRIMERGY CX

Системы Fujitsu PRIMERGY CX позволяют распределить вычислительные мощности в соответствии с бизнес-приоритетами организаций. Линейка включает в себя широкий ассортимент расширяемых напольных серверов для удаленных офисов и филиалов, универсальных стоечных серверов, а также гиперконвергентных модульных систем. Они эффективно интегрируются в существующую среду, позволяя компаниям сосредоточиться на выполнении основных бизнес-функций.

Модульные системы Fujitsu PRIMERGY CX идеально подходят для облачных сред, гиперконвергентных сетей и высокопроизводительных вычислений. Они предоставляют ЦОД и филиалам огромную вычислительную производительность, позволяя увеличивать плотность размещения серверов, сокращать энер-

Шасси дает возможность установить до четырех двухпроцессорных серверных узлов и до 24 накопителей

PRIMERGY CX400 M4 является самым компактным вычислительным решением Fujitsu

гопотребление, тепловыделение и снижать общие операционные затраты.

А что внутри?

Система PRIMERGY CX400 M4 представляет собой масштабируемую ИТ-инфраструктуру, которая обеспечивает гибкий и быстрый отклик на стремительно меняющиеся потребности. Это идеальная платформа для горизонтально масштабируемых рабочих нагрузок, таких как виртуализация, все виды корпоративных приложений, высокопроизводительные вычисления, глубинное обучение или аналитика данных.

Шасси PRIMERGY CX400 M4 является самым компактным вычислительным решением Fujitsu – это модульный корпус форм-фактора 2U, который сочетает в себе плотность и эффективность блейд-серверов с простотой и экономическими преимуществами стоечных систем. Шасси дает возможность установить до четырех двухпроцессорных серверных узлов и до 24 накопителей. Кроме этого система содержит резервные блоки питания с поддержкой горячего подключения, а также вентиляторы, обеспечивая максимальную степень надежности.

В качестве процессоров в CX400 M4 используются Intel Xeon последнего поколения с технологией энергонезависимой памяти Intel Optane DC, оптимизированной для рабочих нагрузок и позволяющей извлекать более значимую аналитическую информацию из данных – от облачных сред и баз данных до аналитики в оперативной памяти и сетей предоставления контента. Кроме того, серверы могут быть оснащены высокопроизводительными платами ускорителя NVIDIA Tesla.

По сравнению с традиционными серверами, PRIMERGY CX400 M4 обеспечивает гораздо большую вычислительную плотность. Это делает его идеальным решением для поставщиков услуг, предприятий автомобильной промышленности, государственных и местных органов власти, а также розничных продавцов.

Возможности охлаждения

Новое шасси может как работать со стандартной системой воздушного охлаждения, так и дополнительно использовать технологию жидкостного охлаждения Cool-Central. Она позволяет отводить тепло от центральных и графических процессоров, а также от серверных модулей памяти при помощи воды, нагретой до 40 °C. Это дает возможность отказаться от остужения этих компонентов. Такое «естественное охлаждение» устраняет 60–80 % нагрева сервера, позволяя экономить более 50 % средств на охлаждение центров обработки данных, а также увеличить плотность размещения серверов в 2,5–5 раз.

Этот подход устраняет традиционные проблемы с электропитанием и охлаждением, а также позволяет значительно снизить объемы инвестиций и эксплуатационные затраты в центрах обработки данных.

Модульные системы Fujitsu PRIMERGY CX идеально подходят для облачных сред, гиперконвергентных сетей и ресурсоемких вычислений, предоставляя ЦОД и филиалам огромную вычислительную производительность

Управление ЦОД

Помимо аппаратного обеспечения, Fujitsu предоставляет заказчикам комплексные решения по управлению инфраструктурой и серверами, обеспечивающие все функции для гибкой и автоматизированной круглосуточной работы ИТ-инфраструктуры. Так, бесплатное ПО Fujitsu ServerView Suite позволяет разворачивать, устанавливать и проводить мониторинг состояния серверов, обновляя BIOS, микропрограммы и нужное программное обеспечение. Fujitsu Infrastructure Manager, доступный в версиях Advanced и Essential, упрощает и автоматизирует ИТ-операции, а также обеспечивает единое конвергентное управление как физической, так и виртуальной средой, охватывая вычислительные и сетевые устройства, а также системы хранения. Это ПО можно интегрировать с другими решениями управления облаком, задействованными в администрировании элементов сервера, СХД, сетей и площадок. Лицензия на ISM Essential предоставляется бесплатно.

По вопросам обращаться: *fujitsu@muk.ua*.

МАСТЕР ТЕХПОДДЕРЖКИ: «МУК-Сервис»

Компания «МУК-Сервис» с 2002 года успешно оказывает услуги по широкому спектру работ, который включает в себя ремонт компьютерной, печатной и сетевой техники, поддержку и ремонт серверных решений различного уровня сложности, мобильных устройств и планшетов.

«МУК-Сервис» на протяжении более чем 17 лет оказывает услуги сервиса ИТ-оборудования корпоративным заказчикам. Высокий профессионализм, опыт и компетенция ИТ-специалистов, сертифицированных инженеров, логистов и координаторов компании позволяют предоставить по-настоящему качественный сервис и обеспечить непрерывную работу бизнес-критического ИТ-оборудования наших клиентов. Портфель «МУК-Сервис» включает в себя авторизации таких брендов, как APC, Check Point, Cisco, Dell EMC, e.HOT, Extreme Networks, Fortinet, Fujitsu, Grandstream Networks, IBM, Hitachi Vantara, HP, Oracle, Tripp Lite.

Главный актив компании – это квалифицированный персонал, состоящий из сертифицированных специалистов высокого класса, что гарантирует заказчикам качественный и профессиональный ремонт оборудования как на модульном, так и на компонентном уровне. Все инженеры проходят регулярное обучение у вендоров и имеют соответствующие подтверждающие документы – сертификаты и дипломы.

Технические возможности сервисного центра МУК позволяют обеспечить качественное обслуживание техники заказчиков как во время действия гарантии, так и после ее окончания. При необходимости можно заключить контракт на сервисное обслуживание. Он позволит избежать прерываний бизнес-процессов вследствие поломки оборудования, которые зачастую ведут к утрате критически важных данных, потере клиентов и подрыву доверия к компании. Контракт гарантирует восстановление работоспособности серверного или сетевого оборудования, или предоставление замены в установленные сроки. Скорость реагирования на проблему обеспечивается наличием в сервисном центре обширнейшего склада запасных частей и подменного оборудования, поэтому не придется длительное время ожидать доставки непосредственно от производителя.

Контрактное обслуживание включает в себя программы по гарантированному восстановлению техники, которые отличаются по времени обслуживания (количество дней поддержки в неделю: рабочие дни недели или все дни недели вне зависимости от праздников и выходных), длительности поддержки в течение дня (рабочее время 8/5, весь день 24/7 или его часть), а также времени восстановления работоспособности системы (четыре, восемь, 24 часа или другое время, необходимое заказчику).

Кроме ремонта оборудования, «МУК-Сервис» предлагает возможность приобретения любых запасных частей, комплектующих и расходных материалов для компьютерной техники, серверного оборудования, ноутбуков, принтеров и сетевого оборудования, а также предоставляет услуги по аренде и аутсорсингу, инсталляции оборудования и информационно-консалтинговую поддержку для корпоративных клиентов.

Преимущества работы с «МУК-Сервис»:

- Высокая квалификация сотрудников
- Оперативность выполнения ремонта
- Контрактное сопровождение техники
- Индивидуальный подход к заказчику
- Наличие собственного склада запчастей
- Собственная служба доставки
- Филиалы в Армении, Беларуси, Грузии, Казахстане
- Сотрудничество с производителями по продаже гарантий

КОНТАКТЫ:
г. Киев, ул. Смелянская, д. 17-А
Тел.: +38 (044) 492-29-09 #460
+38 (044) 594-97-97 #460
e-mail: Stanislav.Vivdenko@muk.ua

«МУК КОМПЬЮТЕРС»,
АЗЕРБАЙДЖАН, БАКУ

Компания «МУК КОМПЬЮТЕРС» начала свою деятельность в Азербайджане в августе 2015 года

Основное направление деятельности компании – дистрибуция компьютерной техники, периферийного и сетевого оборудования, программного обеспечения, решений для построения инфраструктуры и сопутствующих сервисов. Специалисты «МУК КОМПЬЮТЕРС» принимают активное участие в разработке и внедрении проектов, использующих эти решения, предоставляя комплекс дополнительных услуг для своих дилеров и развивая модель Value-Added Distribution. Компания осуществляет продажи исключительно через дилерскую сеть. В настоящее время портфель «МУК КОМПЬЮТЕРС» включает в себя контракты с такими производителями, как 4x, A10 Networks, ACTi, AEG, Altaro, APC, Autodesk, Avigilon, BenQ, Bitdefender, BitTitan, Check Point, Commscope, Conteg, e.HOT, EnGenius, Dell EMC, Delphix, Dropsuite, Extreme Networks, Fortinet, Grandstream Networks, Hitachi Vantara, IBM, Infocus, IXIA, Ivanti, Juniper Networks, Kingston, LearnQuest, Matrix, Microsoft, NetApp, Oracle, Qnap, PacketLight, Proget Software, Radware, RCG Power, Samsung, SaneBox, Shavlik, Shenzhen Max Power, Sopar, StarWind, Stratus, Symantec, Tripp Lite, Veeam, YSoft, Zimbra, Zoom.

Недавно компания получила партнерский статус Microsoft Cloud Service Provider, который дает возможность предложить партнерам облачные решения Microsoft.

Учебный Центр МУК успешно функционирует на территории Азербайджана с 2016 года. За время работы Учебный Центр расширил свои границы, усовершенствовал рабочую площадку и портфель авторизаций. Сейчас УЦ МУК предоставляет своим клиентам комфортные условия для обучения, практику на качественном оборудовании и авторизацию от таких вендоров, как AMP Netconnect, Autodesk, Check Point, Dell EMC, Fortinet, Grandstream, HPE, IBM, ITIL, Juniper Networks, Linux, Microsoft, Oracle, Penta Security, PMI, Red Hat, Veeam, VMware.

В 2018 году в Учебном Центре МУК обучились 280 слушателей из разных компаний. Сильная база сертифицированных тренеров и качество проведенных тренингов усиливают позицию Учебного центра на рынке Азербайджана. Ведется систематическая работа по увеличению и расширению портфеля авторизаций и доступных курсов.

«МУК КОМПЬЮТЕРС» огромное внимание уделяет маркетинговой активности, проводя совместно с вендорами различные мероприятия для партнеров и заказчиков.

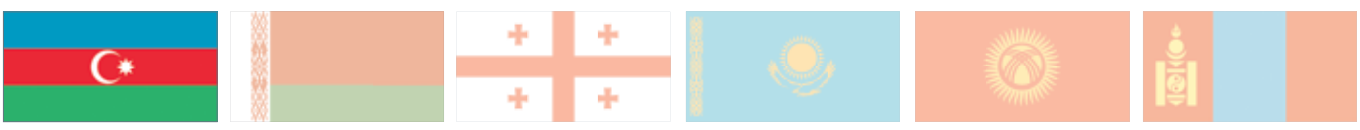
В компании «МУК КОМПЬЮТЕРС» можно разместить заказы или взять на тестирование указанные в статье продукты. Просьба для получения детальной информации об этих решениях и их приобретении, ознакомления с партнерскими программами и предоставляемыми VAD-сервисами, а также с предложениями о проведении совместных мероприятий обращаться по тел. +994 (12) 310-34-43 или электронному адресу office@muk.az.

Оборудование для тестов

На складе компании для партнеров доступен набор демооборудования для тестирования:

- оборудование IBM;
- тонкие клиенты Dell Wyse;
- оборудование Fortinet;
- оборудование Commscope;
- телефония Grandstream;
- серверы, СХД и другое оборудование Dell EMC;
- оборудование CheckPoint;
- оборудование Oracle.

Ассортимент демооборудования постоянно обновляется и пополняется.



MUK COMPUTERS,
AZƏRBAYCAN, BAKI

MUK KOMPYUTERS şirkəti Azərbaycanda öz fəaliyyətinə 2015-ci ilin avqustunda başlamışdır

Şirkətin fəaliyyətinin əsas istiqaməti – kompüter texnikasının, periferiya və şəbəkə avadanlığının, proqram təminatının, infrastrukturun və əlaqəli xidmətlərin qurulması üçün həllərin distribusiyasıdır. MUK KOMPYUTERS mütəxəssisləri öz dilerləri üçün əlavə xidmətlər kompleksini təqdim etməklə və Value-Added Distribution modelini inkişaf etdirməklə bu həlləri istifadə edən layihələrin işlənib hazırlanması və tətbiqində fəal iştirak edirlər. Şirkət satışları yalnız diler şəbəkəsi vasitəsilə həyata keçirir. Hal-hazırda MUK KOMPYUTERS şirkətinin portfelinə 4x, A10 Networks, ACTi, AEG, Altaro, APC, Autodesk, Avigilon, BenQ, Bitdefender, BitTitan, Check Point, Commscope, Conteg, e.HOT, EnGenius, Dell EMC, Delphix, Dropsuite, Extreme Networks, Fortinet, Grandstream Networks, Hitachi Vantara, IBM, Infocus, IXIA, Ivanti, Juniper Networks, Kingston, LearnQuest, Matrix, Microsoft, NetApp, Oracle, Qnap, PacketLight, Proget Software, Radware, RCG Power, Samsung, SaneBox, Shavlik, Shenzhen Max Power, Sopar, StarWind, Stratus, Symantec, Tripp Lite, Veeam, YSoft, Zimbra, Zoom kimi istehsalçılarla bağlanmış müqavilələr daxildir. Yaxınlarda şirkət Microsoft bulud həllərini tərəfdaşlara təklif etmək imkanını verən Microsoft Cloud Service Provider tərəfdaşlıq statusunu almışdır.

Muk Tədris mərkəzi 2016-cı ildən etibarən Azərbaycan Respublikasının ərazisində uğurla fəaliyyət göstərir. Fəaliyyət müddəti ərzində Tədris mərkəzi öz sərhədlərini genişləndirmiş, iş sahəsini və avtorizasiya portfelini təkmilləşdirmişdir. Hal-hazırda MUK tədris mərkəzi öz müştəriləri üçün tədris üçün rahat şərait yaratmış, keyfiyyətli avadanlıqlar vasitəsilə təcrübə keçmək və AMP Netconnect, Autodesk, Check Point, Dell EMC, Fortinet, Grandstream, HPE, IBM, ITIL, Juniper Networks, Linux, Microsoft, Oracle, Penta Security, PMI, Red Hat, Veeam, VMware kimi vendorlardan avtorizasiya imkanını yaratmışdır.

2018-ci ildə MUK-un tədris mərkəzimizdə müxtəlif şirkətlərin 280 əməkdaşına təlim keçirilmişdir. Sertifikatlı təlimçilərin güclü bazası və aparılan təlimlərin keyfiyyəti Tədris mərkəzinin Azərbaycan bazarındakı mövqeyini gücləndirir. Avtorizasiyaların və münasib kursların portfellərinin artırılması və genişləndirilməsi üzrə sistematik iş aparılır.

MUK KOMPYUTERS təchizatçılarla birlikdə tərəfdaşlar və sifarişçilər üçün müxtəlif tədbirləri keçirməklə marketinq aktivliyinə xüsusi önəm verir.

MUK KOMPYUTERS şirkətində sifariş yerləşdirmək və ya məqalədə göstərilən məhsulları sınaq üçün əldə etmək mümkündür. Bu həllər və onların əldə edilməsi barədə daha ətraflı məlumat almaq, tərəfdaşlıq proqramları və təqdim edilmiş VAD-servisləri ilə, həmçinin müştərək tədbirlərin keçirilməsi ilə bağlı təkliflərlə tanış olmaq üçün +994 (12) 310-34-43 telefon nömrəsi və ya office@muk.az elektron poçt ünvanı ilə əlaqə saxlamağınız xahiş olunur.

Sınaqlar üçün avadanlıq

Şirkətin anbarında tərəfdaşlar üçün sınaqlar üçün demo-avadanlıqlar dəsti mövcuddur:

- IBM avadanlığı;
- Dell Wyse müştəriləri;
- Fortinet avadanlığı.
- Commscope avadanlığı
- Grandstream telefoniyası;
- serverlər, MSS və digər Dell EMC avadanlığı;
- CheckPoint avadanlığı
- Oracle avadanlığı

Demo-avadanlığının çeşidi daim yenilənir və artırılır.

M.U.K. COMPUTERS,
АРМЕНИЯ

Компания M.U.K. Computers, локальное представительство группы компаний МУК в Республике Армения, начала свою деятельность в 2014 году

За время работы были подписаны контракты с ведущими производителями мировой ИТ-индустрии – 4x, A10 Networks, ACTi, AEG, Altaro, Autodesk, BenQ, Bitdefender, BitTitan, Conteg, Dell EMC, Delphix, Dropsuite, e.HOT, EnGenius, Extreme Networks, Fortinet, Grandstream Networks, Hitachi Vantara, IBM, InFocus, Ivanti, IXIA, Juniper Networks, Kingston, Lenovo, LearnQuest, Microsoft, NetApp, Oracle, PacketLight, Proget Software, Qnap, Radware, RCG Power, SaneBox, Shavlik, Shenzhen Max Power, Sopar, Stratus, Symantec, Tescom, Tripp Lite, Veeam, Vmware, Ysoft, Zimbra, Zoom. Кроме того, компания активно развивает в Армении партнерскую сеть, осуществляя продажи исключительно через своих партнеров и помогая им в реализации проектов различного масштаба для заказчиков различных сфер деятельности.

Серверы и СХД

При поддержке своих партнеров M.U.K. Computers снабжает серверными решениями государственные органы, финансовые организации, телеком-операторы и другие коммерческие структуры. Партнеры M.U.K. Computers продолжают успешно реализовывать проекты по интеграции ЦОД, серверов, СХД, и гиперконвергентных решений на базе производителей Dell EMC, IBM, Oracle.

Сетевое оборудование и безопасность

Совместно с партнерами, M.U.K. Computers предлагает на рынке Армении сетевые решения Juniper и Extreme Networks, а также широкий спектр решений по безопасности: аналитика, SIEM, «песочница» на базе вендоров A10, IBM, Fortinet, Symantec, Microsoft, Oracle.

Облачные решения

M.U.K. Computers участвует в развитии рынка облачных технологий. Обучая и развивая новым схемам продаж облака, M.U.K. Computers также занимается привлечением новых партнеров, занимающихся исключительно облаком. Эту миссию M.U.K. Computers осуществляет совместно с вендорами: Microsoft, IBM, Oracle, VMware.

Работа с партнерами

Компания M.U.K. Computers при продвижении брендов своего портфеля на рынке уделяет особое внимание обучению партнеров и заказчиков, проводя различные мероприятия: презентации новых продуктов, обучающие семинары и вебинары и т. д.

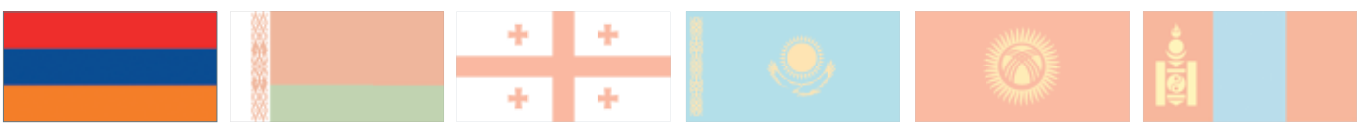
Возможность заказа или тестирования указанных в статье продуктов можно запросить в локальном представительстве группы компаний МУК – M.U.K. Computers. Для получения детальной информации об этих решениях и их приобретении, ознакомления с партнерскими программами и предоставляемыми VAD-сервисами, а также с предложениями о проведении совместных мероприятий обращаться по тел. +374 (94) 655 044, или по электронному адресу armenia@muk.am.

Оборудование для тестов

На складе компании для партнеров доступен набор демооборудования для тестирования:

- фаерволы и программные решения Fortinet;
- системы ВКС Grandstream;
- оборудование от Dell, BenQ, InFocus.

Ассортимент демооборудования постоянно обновляется и пополняется.



M.U.K. COMPUTERS,
ՀԱՅԱՍՏԱՆ

M.U.K. Computers ընկերությունը՝ M.U.K. ընկերությունների խմբի տեղական ներկայացուցչությունը Հայաստանի Հանրապետությունում, իր գործունեությունն է սկսել 2014թ.-ին:

Այդ ընթացքում պայմանագրեր են ստորագրվել համաշխարհային SS ոլորտի առաջատար արտադրողների հետ՝ 4x, A10 Networks, ACTi, AEG, Altaro, Autodesk, BenQ, Bitdefender, BitTitan, Conteg, Dell EMC, Delphix, Dropsuite, e.NOT, EnGenius, Extreme Networks, Fortinet, Grandstream Networks, Hitachi Vantara, IBM, InFocus, Ivanti, IXIA, Juniper Networks, Kingston, Lenovo, LearnQuest, Microsoft, NetApp, Oracle, PacketLight, Proget Software, Qnap, Radware, RCG Power, SaneBox, Shavlik, Shenzhen Max Power, Sopar, Stratus, Symantec, Tescom, Tripp Lite, Veeam, Vmware, Ysoft, Zimbra, Zoom: Բացի այդ, ընկերությունը Հայաստանում ակտիվորեն զարգացնում է գործընկերային ցանց՝ վաճառքներն իրականացնելով բացառապես իր գործընկերների միջոցով, և օգնում է նրանց իրագործել տարբեր չափերի ծրագրեր տարբեր ոլորտներում գործող հաճախորդների համար:

Սերվերներ և ՏՊՀ (տվյալների պահպանման համակարգեր)

Իր գործընկերների աջակցությամբ M.U.K. Computers-ը սերվերի լուծումներ է տրամադրում պետական գերատեսչությունների, ֆինանսական կազմակերպությունների, հեռահաղորդակցման օպերատորների և այլ առևտրային կազմակերպությունների: M.U.K. Computers-ի գործընկերները շարունակում են հաջողությամբ իրականացնել տվյալների մշակման կենտրոնների, սերվերների, ՏՊՀ-երի և հիպերկոնվերգենտ լուծումների ինտեգրման ծրագրեր՝ հիմնված Dell EMC, IBM, Oracle արտադրողների վրա:

Ցանցային սարքավորումներ և անվտանգություն

Գործընկերների հետ միասին, M.U.K. Computers-ը հայաստանյան շուկայում առաջարկում է Juniper և Extreme Networks ցանցային լուծումներ, ինչպես նաև անվտանգության լուծումների լայն շրջանակ՝ վերլուծություն, SIEM, Sandbox՝A10, IBM, Fortinet, Symantec, Microsoft, Oracle ընկերությունների բազայով:

Ամպային լուծումներ

M.U.K. Computers-ը ներգրավված է ամպային տեխնոլոգիաների շուկայի զարգացման մեջ: Ուսուցանելով և զարգացնելով ամպերի վաճառքի նոր ձևեր՝ M.U.K. Computers-ը նաև զբաղվում է բացառապես ամպով զբաղվող նոր գործընկերների ներգրավմամբ: Այս առաքելությունը M.U.K. Computers-ը իրականացնում է Microsoft, IBM, Oracle, VMware վաճառողների հետ:

Աշխատանք գործընկերների հետ

M.U.K. Computers ընկերությունը շուկայում իր պորտֆելի ապրանքանիշերն առաջ տանելիս առանձնահատուկ ուշադրություն է դարձնում գործընկերների և պատվիրատուների ուսուցմանը՝ անցկացնելով տարբեր միջոցառումներ ՝ նոր ապրանքների շնորհանդեսներ, սեմինարներ և վեբինարներ և այլն:

Հոդվածում նշված արտադրանքները պատվիրելու կամ փորձելու համար կարելի է դիմել MUK ընկերությունների խմբի տեղական ներկայացուցչությանը՝ M.U.K. Computers-ին: Այս լուծումների և դրանք ձեռք բերելու վերաբերյալ մանրամասն տեղեկություններ ստանալու, գործընկերային ծրագրերի և տրամադրվող VAD ծառայություններին, ինչպես նաև համատեղ միջոցառումների վերաբերյալ առաջարկություններին ծանոթանալու համար դիմեք՝ +374 (94) 655 044 հեռախոսահամարով կամ armenia@muk.am էլ. փոստի միջոցով:

Թեստային սարքավորումներ

Ընկերության պահեստում գործընկերների համար կան ցուցադրական սարքավորումներ՝
- Ֆայրվոլներ և Fortinet ծրագրային լուծումներ;
- BKC Grandstream համակարգեր;
- Dell- ի, BenQ- ի, InFocus- ի սարքավորումներ:

Ցուցադրական սարքավորումների տեսականին անընդհատ թարմացվում և համալրվում է:

«МУК-КОМПЬЮТЕРС»,
БЕЛАРУСЬ, МИНСК

Компания «МУК-Компьютерс» начала свою деятельность в Республике Беларусь в ноябре 2011 года

За время работы были подписаны контракты с такими производителями в сфере ИТ-индустрии, как 4x, A10 Networks, ACTi, AEG, Altaro, APC, Autodesk, Bitdefender, BitTitan, Conteg, Commscope, Dell EMC, Delphix, Dropsuite, EnGenius, Extreme Networks, Geovision, Grandstream Networks, IBM, InFocus, Ivanti, IXIA, Juniper Networks, Kingston, Matrix, Microsoft, NetApp, Oracle, PacketLight, Proget Software, Radware, RCG Power, SaneBox, Shavlik, StarWind, Stratus, Symantec, Tescom, Tripp Lite, Veeam, VMware, YSoft, Zimbra, Zoom. Помимо этого компания активно развивает партнерскую сеть по всей территории страны, что позволило повысить объемы продаж и принять участие в целом ряде интересных проектов для организаций различных сфер деятельности.

В ассортименте группы компаний МУК представлены:

- серверные решения от Dell EMC, Oracle и IBM;
- системы хранения данных Dell EMC, IBM, NetApp, Oracle;
- сертифицированные решения по безопасности IBM, Juniper Networks, IXIA и Radware;
- тестовое оборудование для IP-сетей от IXIA;
- оборудование для систем видеонаблюдения от Geovision;
- телефония и видеосвязь от Grandstream;
- активное сетевое оборудование для проводных и беспроводных сетей от EnGenius, Extreme Networks, Gigamon, Juniper Networks, IXIA, Oracle, PacketLight;
- ИБП и батареи от AEG, IBM, Tripp Lite, Shenzhen Max Power, Tescom;
- программное обеспечение от Autodesk, Dell EMC, IBM, Ivanti, Oracle, Veeam, VMware и Zimbra;
- телекоммуникационные шкафы и стойки 4x и Tripp Lite;
- проекторы и интерактивные экраны от InFocus;
- компоненты систем гарантированного электропитания от e.HOT;
- решения для управления документооборотом от YSoft.

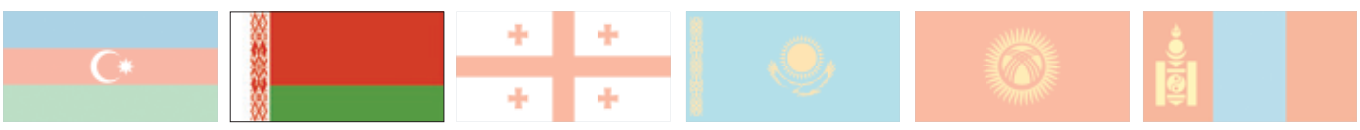
Преимущества работы с МУК:

- разветвленная партнерская сеть;
- наличие собственного склада с постоянно пополняющимся подменным фондом;
- сертифицированные мультивендорные специалисты;
- отсутствие привязки к конкретному продукту/платформе, что дает гибкость в выборе оптимального варианта решения задач;
- гибкая политика ценообразования;
- минимальное время производственного процесса;
- наличие в портфеле компании решений лидирующих производителей отрасли;
- инсталляция оборудования и ПО, обслуживание и консалтинг;
- обучение сервис-партнеров.

Возможность заказа или тестирования указанных в статье продуктов можно запросить в компании «МУК-Компьютерс». Для получения детальной информации об этих решениях и их приобретении, ознакомления с партнерскими программами и предоставляемыми VAD-сервисами, а также с предложениями о проведении совместных мероприятий обращаться по тел. +375 (17) 336-98-97 или электронному адресу office@muk.by.

Оборудование для тестов

На складе компании для партнеров доступен набор демооборудования для тестирования. Перечень оборудования предоставляется по запросу. Ассортимент демооборудования постоянно обновляется и пополняется.



МУК-КОМП'ЮТЭРС,

БЕЛАРУСЬ, МІНСК

Кампанія «МУК-Комп'ютэрс» пачала сваю дзейнасць у Рэспубліцы Беларусь ў лістападзе 2011 года

За час работы былі падпісаны кантракты з такімі вытворцамі ў сферы IT-індустрыі, як 4x, A10 Networks, ACTi, AEG, Altaro, APC, Autodesk, Bitdefender, BitTitan, Conteg, Commscope, Dell EMC, Delphix, Dropsuite, EnGenius, Extreme Networks, Geovision, Grandstream Networks, IBM, InFocus, Ivanti, IXIA, Juniper Networks, Kingston, Matrix, Microsoft, NetApp, Oracle, PacketLight, Proget Software, Radware, RCG Power, SaneBox, Shavlik, StarWind, Stratus, Symantec, Tescom, Tripp Lite, Veeam, Vmware, Ysoft, Zimbra, Zoom. Акрамя гэтага, кампанія актыўна развівае партнёрскую сетку па ўсёй тэрыторыі краіны, што дазволіла павысіць аб'ёмы продажу і прыняць удзел у цэлым шэрагу цікавых праектаў для арганізацый розных сфер дзейнасці.

У асартыменце групы кампаній МУК прадстаўлены:

- серверныя рашэнні ад кампаній Dell EMC, Oracle і IBM;
- сістэмы захоўвання даных кампаній Dell EMC, IBM, NetApp, Oracle;
- сертыфікаваныя рашэнні па бяспецы кампаній IBM, Juniper Networks, IXIA і Radware;
- тэставае абсталяванне для IP-сетак ад кампаніі IXIA;
- абсталяванне для сістэм відэаназірання ад кампаніі Geovision;
- тэлефанія і відэасувязь ад кампаніі Grandstream;
- актыўнае сеткавае абсталяванне для правадных і бесправадных сетак ад кампаній EnGenius, Extreme Networks, Gigamon, Juniper Networks, IXIA, Oracle, PacketLight;
- крыніцы бесперабойнага сілкавання і батарэі ад кампаній AEG, IBM, Tripp Lite, Shenzhen Max Power, Tescom;
- праграмнае забеспячэнне ад кампаній Autodesk, Dell EMC, IBM, Ivanti, Oracle, Veeam, Vmware і Zimbra;
- тэлекамунікацыйныя шафы і стойкі кампаній 4x і Tripp Lite;
- праектары и інтэрактыўныя экраны ад кампаніі InFocus;
- кампаненты сістэм гарантаванага электрасілкавання ад кампаніі e.HOT;
- рашэнні для кіравання абаротам дакументаў ад кампаніі Ysoft.

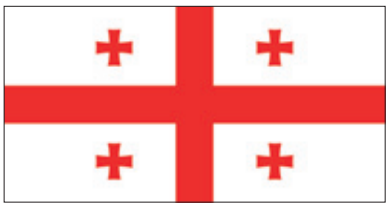
Перавагі работы з МУК:

- разгалінаваная партнёрская сетка;
- наяўнасць уласнага складу з падменным фондам, які папаўняецца ўвесь час;
- сертыфікаваныя мультывендартныя спецыялісты;
- адсутнасць прывязанасці да пэўнага прадукту/платформы, што дае гнуткасць у выбары аптымальнага варыянту рашэння задач;
- гнуткая палітыка цэнаўтварэння;
- мінімальны час вытворчага працэсу;
- наяўнасць у партфелі кампаніі рашэнняў перадавых вытворцаў галіны;
- інсталяцыя абсталявання і праграмнага забеспячэння, абслугоўванне і кансультацыі;
- навучэнне сэрвіс-партнёраў.

Магчымасць заказу або тэставання пададзеных у артыкуле прадуктаў можна запытаць у кампаніі «МУК-Комп'ютэрс». Для атрымання падрабязнай інфармацыі аб гэтых рашэннях і іх набыцці, азнаямлення з партнёрскімі праграмамі і прапанаванымі VAD-сэрвісамі, а таксама з прапановамі аб правядзенні сумесных мерапрыемстваў звяртацца па тэл. +375 (17) 336-98-97 або па электронным адрасе office@muk.by.

Абсталяванне для тэстаў

На складзе кампаніі для партнёраў даступны набор дэма-абсталявання для тэставання. Пералік абсталявання прадастаўляецца па запыце. Асартымент дэма-абсталявання ўвесь час абнаўляецца і папаўняецца.



MUK-TBILISI,
ГРУЗИЯ, ТБИЛИСИ

Компания MUK-Tbilisi начала свою деятельность на территории Грузии в ноябре 2011 года

За это время были подписаны контракты с ведущими компаниями-производителями в сфере информационных технологий: 4X, A10 Networks, ACTi, AEG, Altaro, APC, Autodesk, BenQ, Bitdefender, BitTitan, Check Point, Cisco, Commscope, Conteg, Dell EMC, Delphix, Dropsuite, e.HOT, EnGenius, Extreme Networks, Fortinet, Grandstream Networks, Hitachi Vantara, HPE, HPI, IBM, InFocus, IXIA, Ivanti, Juniper Networks, Lenovo, Kingston, Matrix, Microsoft, NetApp, Oracle, PacketLight, Penta Security, Plustek, Proget Software, Qnap, Radware, RCG Power, Samsung, SaneBox, Shavlik, Shenzhen Max Power, Sopar, StarWind, Stratus, Symantec, Tescom, Tripp Lite, Veeam, VMware, Ysoft, Zimbra, Zoom. Помимо этого компания активно развивает партнерскую сеть по всей территории страны, что позволило повысить объемы продаж и принять участие в целом ряде интересных проектов для организаций различных сфер деятельности.

В ассортименте группы компаний МУК представлены:

- серверы стандартной архитектуры HPE и серверные опции к ним;
- серверные решения от Cisco, Dell EMC, Hitachi Vantara, IBM, Oracle;
- системы хранения данных Dell EMC, Hitachi Vantara, HPE, IBM, Oracle, Qnap, NetApp;
- решения безопасности Bitdefender, Fortinet, IBM, IXIA, HPE, Penta Security, Radware, Symantec;
- тестовое оборудование для IP-сетей от IXIA;
- решения ВКС от Cisco и Grandstream Networks;
- оборудование для систем видеонаблюдения от Geovision;
- ИБП и батареи от AEG Power Solutions, APC, Shenzhen Max Power, Tescom, Tripp Lite;
- активное сетевое оборудование для проводных и беспроводных сетей от Cisco, EnGenius, Fortinet, HPE, Juniper Networks, PacketLight;
- телекоммуникационные шкафы и стойки APC, 4x и Conteg;
- проекторы и интерактивные экраны от InFocus, Plustek, Sopar;
- компоненты систем гарантированного электропитания от e.HOT;
- генераторы RCG Power;
- программное обеспечение от Altaro, Autodesk, BitTitan, IBM, Ivanti, HPE, Microsoft, Oracle, StarWind, Stratus, Veeam, VMware;
- модули памяти Kingston;
- решения управления печатью от YSoft;
- компьютерная техника и электроника от BenQ и HPI.

Преимущества работы с МУК:

- разветвленная партнерская сеть;
- сертифицированные мультивендорные специалисты;
- отсутствие привязки к конкретному продукту/платформе, что дает гибкость в выборе оптимального варианта решения задач;
- гибкая политика ценообразования;
- минимальное время производственного процесса;
- возможность закрепления сделки под конкретный проект;
- наличие в портфеле компании решений лидирующих производителей отрасли;
- инсталляция оборудования и ПО, обслуживание и консалтинг;
- обучение сервис-партнеров.

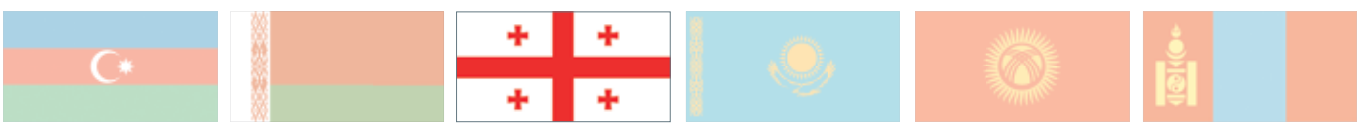
Возможность заказа или тестирования указанных в статье продуктов можно запросить в компании MUK-Tbilisi. Для получения детальной информации об этих решениях и их приобретении, ознакомления с партнерскими программами и предоставляемыми VAD-сервисами, а также с предложениями о проведении совместных мероприятий обращаться по тел. +995 (32) 260-16-54 или электронному адресу office@muk.ge.

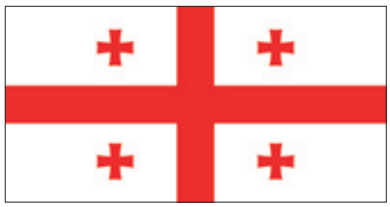
Оборудование для тестов

На складе компании для партнеров доступен набор демооборудования для тестирования:

- беспроводные точки доступа;
- сетевые распределители;
- телефония;
- коммутаторы;
- устройства защиты сети;
- проекторы.

Ассортимент демооборудования постоянно обновляется и пополняется.





MUK- TBILISI,

საქართველო, თბილისი

კომპანიამ MUK-Tbilisi დაიწყო თავისი საქმიანობა საქართველოს ტერიტორიაზე 2011 წლის ნოემბერში

ამ დროის განმავლობაში ხელი მოეწერა კონტრაქტებს წამყვან კომპანია-მწარმოებლებთან საინფორმაციო ტექნოლოგიების სფეროში: 4X, A10 Networks, ACTi, AEG, Altaro, APC, Autodesk, BenQ, Bitdefender, BitTitan, Check Point, Cisco, Commscope, Conteg, Dell EMC, Delphix, Dropsuite, e.HOT, EnGenius, Extreme Networks, Fortinet, Grandstream Networks, Hitachi Vantara, HPE, HPI, IBM, InFocus, IXIA, Ivanti, Juniper Networks, Lenovo, Kingston, Matrix, Microsoft, NetApp, Oracle, PacketLight, Penta Security, Plustek, Proget Software, Qnap, Radware, RCG Power, Samsung, SaneBox, Shavlik, Shenzhen Max Power, Sopar, StarWind, Stratus, Symantec, Tescom, Tripp Lite, Veeam, VMware, Ysoft, Zimbra, Zoom. გარდა ამისა კომპანია აქტიურად განავითარებს პარტნიორულ ქსელს მთელი ქვეყნის ტერიტორიაზე, რამაც მისცა გაყიდვების მოცულობების გაზრდისა და სხვადასხვა სფეროში საქმიანობის განმახორციელებლ კომპანიებისთვის მთელ რიგ საინტერესო პროექტებში მონაწილეობის მიღების შესაძლებლობა.

მუკ-ის კომპანიათა ჯგუფის ასორტიმენტში წარმოდგენილია:

- HPE-ს სტანდარტული არქიტექტურის სერვერები და მათი სერვერული ოფციები;
- Cisco-ს, Dell EMC-ის, Hitachi Vantara-ს, IBM-ის, Oracle-ის სერვერული გადაწყვეტილებები;
- Dell EMC-ის, Hitachi Vantara-ს, HPE-ს, IBM-ის, Oracle-ს, Qnap-ის, NetApp-ის მონაცემთა შენახვის სისტემები;
- Bitdefender-ის, Fortinet-ის, IBM-ის, IXIA-ს, HPE-ს, Penta Security-ს, Radware-ის, Symantec-ის უსაფრთხოების გადაწყვეტილებები;
- IXIA-ს სატესტო მოწყობილობა IP-ქსელებისთვის;
- Cisco-ს და Grandstream Networks-ის ВКС-ს გადაწყვეტილებები;
- Geovision-ის ვიდეოთვალთვალის სისტემების მოწყობილობა;
- AEG Power Solutions-ის, APC-ს, Shenzhen Max Power-ის, Tescom-ის, Tripp Lite-ს უწყვეტი კვების წყაროები და მათი ბატარეები;
- Cisco-ს, EnGenius-ის, Fortinet-ის, HPE, Juniper Networks-ის, PacketLight-ის აქტიური ქსელური მოწყობილობა სადენიანი და უსადენო ქსელებისთვის;
- APC-ს, 4x და Conteg-ის ტელესაკომუნიკაციო კარადები და დანადგარები;
- InFocus-ის, Plustek-ის, Sopar-ის პროექტორები და ინტერაქტიური ეკრანები;
- e.HOT-ის გარანტირებული ელექტროკვების სისტემების კომპონენტები;
- RCG Power-ის გენერატორები;
- Altaro-ს, Autodesk-ის, BitTitan-ის, IBM-ის, Ivanti-ს, HPE-ს, Microsoft-ის, Oracle-ის, StarWind-ის, Stratus-ის, Veeam-ის, VMware-ის პრგრამული უზრუნველყოფა;
- Kingston-ის მეხსირების მოდულები;
- YSoft-ის ბეჭდვის მართვის გადაწყვეტილებები;
- BenQ-ის და HPI-ს კომპიუტერული ტექნიკა და ელექტრონიკა.

მუკ-თან მუშაობის უპირატესობები:

- განშტოებული პარტნიორული ქსელი;
- სერტიფიცირებული მულტივენდორული სპეციალისტები;
- კონკრეტულ პროდუქტზე/პლატფორმაზე მიბმის არარსებობა, რაც მოქნილობას იძლევა ამოცანების გადაწყვეტის ოპტიმალური ვარიანტის შერჩევაში;
- ფასწარმოქმნის მოქნილი პოლიტიკა;
- საწარმოო პროცესის მინიმალური დრო;
- კონკრეტულ პროექტზე გარიგების მიმაგრების შესაძლებლობა;
- კომპანიათა პორტფელში დარგის წამყვან მწარმოებელთა გადაწყვეტების არსებობა;
- მოწყობილობის და პროგრამული უზრუნველყოფის ინსტალაცია, მომსახურება და კონსალტინგი;
- სერვის-პარტნიორების სწავლება.

სტატიაში მითითებული პროდუქტების შეკვეთა ან ტესტირების შესაძლებლობა შეგიძლიათ მოითხოვოთ კომპანიაში MUK-Tbilisi. ამ გადაწყვეტილებების შესახებ, ასევე მათი შეძენის შესახებ დეტალური ინფორმაციის მიღებისთვის, პარტნიორული პროგრამების და VAD-სერვისების, ასევე ერთობლივი ღონისძიებების ჩატარების შესახებ წინადადებების გაცნობისთვის მოგვმართეთ ტელეფონზე +995 (32) 260-16-54 ან ელექტრონულ მისამართზე office@muk.ge.

მოწყობილობა ტესტებისთვის

კომპანიის საწყობში პარტნიორებისთვის ხელმისაწვდომია დემო-მოწყობილობის ნაკრები ტესტირებისთვის:

- უსადენო წვდომის წერტილები;
- კომუტატორები;
- ქსელური გამწაწილებლები;
- ქსელის დაცვის სისტემები;
- ტელეფონია;
- პროექტორები.

მუდმივად ხდება დემო-მოწყობილობის ასორტიმენტის განახლება და შევსება.

MUK COMPUTERS,
КАЗАХСТАН, АЛМАТЫ

Компания MUK Computers начала свою деятельность в Республике Казахстан в мае 2014 года

За период работы компания активно развивала партнерскую сеть, а также заключила дистрибуторские контракты с рядом ведущих компаний-производителей в сфере информационных технологий: 4x, A10 Networks, ACTi, AEG, Altaro, APC, Avigilon, BitTitan, Check Point, Commscope, Conteg, Dell EMC, Delphix, Dropsuite, e.HOT, EnGenius, Geovision, Grandstream Networks, IBM, InFocus, IXIA, Ivanti, Juniper Networks, Kalmo Systems, Kingston, Matrix, Microsoft, NetApp, PacketLight, Penta Security, Proget Software, Radware, RCG Power, SaneBox, Sharp, Shavlik, Shenzhen Max Power, StarWind, Stratus, Symantec, Tescom, Tripp Lite, Ysoft, Zimbra, Zoom. Также компания имеет партнерский статус Microsoft Cloud Service Provider, который дает возможность предлагать партнерам облачные решения Microsoft.

Расширение портфолио

Прошедший год ознаменовался для MUK Computers подписанием ряда контрактов с ведущими производителями мирового рынка информационных технологий. В частности, компания получила статус эксклюзивного дистрибутора NetApp, известного производителя систем хранения данных. Кроме того, стоит отметить и заключение дистрибуторского контракта с компанией Dell EMC, известным брендом в области с широкой продуктовой линейкой, покрывающей все потребности потенциальных заказчиков. В штате MUK Computers присутствуют квалифицированные специалисты, отвечающие за продажи продуктов этих двух производителей. Компетенция сотрудников позволяет им оказывать консультационную поддержку при разработке карты проекта, а также при внедрении решений в инфраструктуру заказчика.

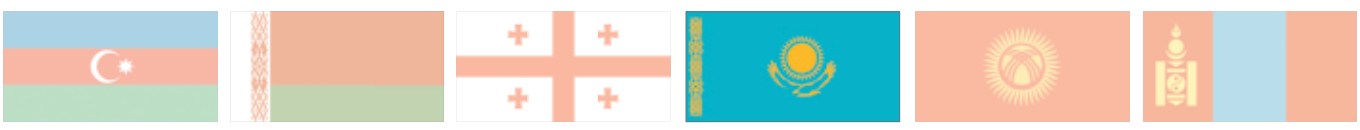
Новые проекты

За прошедший год MUK Computers реализовала целый ряд знаковых проектов. В частности, можно выделить внедрение решения по обеспечению бесперебойного питания для завода на крупном нефтяном месторождении на базе оборудования APC by Schneider Electric.

С 2016 года дистрибуторский портфель компании включает в себя одного из крупнейших в мире производителей и поставщиков аппаратного и программного обеспечения, а также ИТ-сервисов и консалтинговых услуг – корпорацию IBM. За это время было реализовано множество проектов на оборудовании этого вендора. Среди них можно отметить проект модернизации вычислительных мощностей IBM Power system в одной из местных компаний, а также внедрение системы хранения IBM Storwize v5010 в инфраструктуру крупной корпорации – эта модель представляет собой гибкое гибридное решение для хранения данных с повышенной производительностью и поддержкой функциональности систем корпоративного класса.

Помимо аппаратных решений, был реализован и ряд проектов на базе различного программного обеспечения IBM. Крупными заказчиками такого ПО за последнее время стали АО Национальный Холдинг КазАГРО и Государственное Кредитное Бюро. Более того, такие крупные банки Казахстана, как QazaqBank, Halyk Bank и Sberbank, приобрели решения аналитики от этой компании.

Возможность заказа или тестирования указанных в статье продуктов можно запросить в компании MUK Computers. Для получения детальной информации об этих решениях и их приобретении, ознакомления с партнерскими программами и предоставляемыми VAD-сервисами, а также с предложениями о проведении совместных мероприятий обращаться по телефону +7 727 346 79 01 или электронному адресу office@muk.kz.



MUK COMPUTERS,
ҚАЗАҚСТАН, АЛМАТЫ

MUK Computers компаниясы өз қызметін 2014 жылдың мамыр айында Қазақстан Республикасында бастады

Өзінің қызмет ету кезеңінде компания серіктестік желіні белсенді дамытып келеді, сонымен қатар ақпараттық технологиялар саласындағы бірқатар жетекші өндірушілермен: 4x, A10 Networks, ACTi, AEG, Altaro, APC, Avigilon, BitTitan, Check Point, Commscope, Conteg, Dell EMC, Delphix, Dropsuite, e.HOT, EnGenius, Geovision, Grandstream Networks, IBM, InFocus, IXIA, Ivanti, Juniper Networks, Kalmo Systems, Kingston, Matrix, Microsoft, NetApp, PacketLight, Penta Security, Proget Software, Radware, RCG Power, SaneBox, Sharp, Shavlik, Shenzhen Max Power, StarWind, Stratus, Symantec, Tescom,Tripp Lite, Ysoft, Zimbra, Zoom компаниялары-мен дистрибьюторлық келісімшарттар жасады. Компания сонымен қатар Microsoft Cloud Service Provider серіктес мәртебесіне ие, бұл серіктестерге Microsoft оңтайлы шешімдерін ұсынуға мүмкіндік береді.

Портфолионы кеңейту

Өткен жыл MUK Computers үшін әлемдік ақпараттық технологиялар нарығының жетекші өндірушілерімен бірқатар келісімшарттарға қол қоюмен белгіленді. Атап айтқанда, компания деректерді сақтау жүйесінің танымал өндірушісі, NetApp эксклюзивті дистрибьюто-ры мәртебесіне ие болды. Сонымен қатар, әлеуетті клиенттердің барлық қажеттіліктерін қанағаттандыратын кең өнім желісі бар осы салада танымал бренд Dell EMC-пен дистрибьюторлық келісім-шарт жасасуды да атап өткен жөнк. MUK компьютерлерінде осы екі өндірушінің өнімдерін сатуға жауапты білікті мамандар жұмыс істейді. Қызметкерлердің құзіреттілігі оларға жобаның картасын жасауда, сондай-ақ тапсырыс берушінің инфрақұрылымында шешімдерді жүзеге асыруда кеңестік қолдау көрсетуге мүмкіндік береді.

Жаңа жобалар

Өткен жылы MUK Computers бірқатар маңызды жобалар-ды жүзеге асырды. Атап айтқанда, APC by Schneider Electric жабдығы базасында ірі мұнай кен орнындағы зауыт үшін үздіксіз қоректендіруді қамтамасыз ету жөніндегі шешімді енгізуді атап өтуге болады.

2016 жылдан бастап компанияның дистрибьюторлық портфеліне әлемдегі ең ірі өндірушілер мен аппараттық және бағдарламалық қамтамасыз етушілердің бірі, сондай-ақ ИТ -сервистері мен консалтингтік қызметтер – IBM корпорация-сы енеді. Осы уақыт ішінде осы вендордың жабдықтарында көптеген жобалар жүзеге асырылды. Олардың ішінде жергілікті компаниялардың бірінде IBM Power system есептеу қуаттарын жаңғырту жобасын атап өтуге болады, сондай-ақ ірі корпорацияның инфрақұрылымына IBM Storwize v5010 сақтау жүйесін енгізу-бұл модель жоғары өнімділігі бар деректерді сақтау және корпоративтік класс жүйелерінің функционалдығын қолдау үшін икемді гибридті шешім болып табылады.

Аппараттық шешімдерге қосымша, әр түрлі IBM бағдарламалық қамтамасыз ету базасында бірқатар жобалар іске асырылды. Соңғы уақытта мұндай бағдарламалық қамтамасыз етудің ірі ірі тапсырыс берушілер «ҚазАГРО» Ұлттық холдингі» АҚ және Мемлекеттік Кредиттік бюро болды. Сонымен қатар, QazaqBank, Halyk Bank және Сбербанк сияқты Қазақстанның ірі банктері осы компаниядан аналитикалық шешімдерді қабылдады.

Мақалада көрсетілген өнімдерге тапсырыс беру немесе тестілеу мүмкіндігін MUK Computers компаниясынан сұрауға болады. Осы шешімдер және оларды сатып алу туралы толық ақпаратты, серіктестік бағдарламалармен және ұсынылатын VAD-қызметтерімен танысу үшін, сондай-ақ бірлескен іс-шараларды өткізу туралы ұсыныстармен +7 (727) 346-79-01 телефонына немесе office@muk.kz электронды поштасына хабарласуыңызға болады.

MUK COMPUTERS,
КЫРГЫЗСТАН, БИШКЕК

Компания MUK COMPUTERS начала свою деятельность на территории Кыргызстана в 2017 году

Компания активно развивает на территории Кыргызстана модель Value-Added Distribution, осуществляя продажи исключительно через дилерскую сеть. При этом специалисты MUK COMPUTERS активно участвуют в разработке и внедрении проектов в различных сферах деятельности. Продуктовое портфолио компании постоянно расширяется и включает в себя решения таких производителей, как 4x, A10 Networks, ACTi, AEG, Altaro, APC, Avigilon, BenQ, Bitdefender, BitTitan, Commscope, Conteg, Delphix, Dropsuite, e.HOT, EnGenius, IBM, InFocus, IXIA, Ivanti, Juniper Networks, Kingston, Matrix, Metis, Microsoft, NetApp, Oracle, PacketLight, Proget Software, Qnap, Radware, RCG Power, SaneBox, Sharp, Shavlik, Shenzhen Max Power, Stratus, Symantec, Tescom, Veeam, YSoft, Zimbra, Zoom.

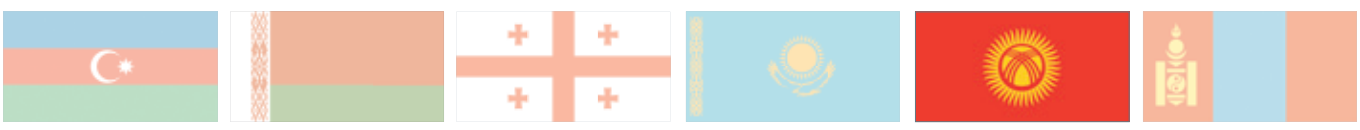
В ассортименте группы компаний МУК представлены:

- серверные решения от IBM и Oracle;
- системы хранения данных IBM, NetApp и Oracle;
- комплексные решения для построения ЦОД от APC;
- решение резервного копирования, восстановления и репликации данных от Veeam;
- полный и полностью интегрированный стек облачных приложений, платформ и инженерных систем от Oracle;
- решения для виртуализации баз данных от Delphix;
- решения безопасности от Bitdefender, IBM, IXIA, Oracle, Symantec;
- тестовое оборудование для IP-сетей от IXIA;
- оборудование для систем видеонаблюдения от Avigilon;
- ИБП и батареи от AEG Power Solutions, APC, Shenzhen Max Power, Tescom;
- активное сетевое оборудование для проводных и беспроводных сетей от EnGenius, IXIA и PacketLight;
- программное обеспечение от Altaro, IBM, Ivanti, Microsoft, Oracle, Stratus и Veeam;
- телекоммуникационные шкафы и стойки 4x и Conteg;
- проекторы и интерактивные экраны от InFocus;
- решения визуализации от Sharp;
- компоненты СКС от Commscope;
- компоненты систем гарантированного электропитания от e.HOT;
- генераторы RCG Power;
- модули памяти Kingston;
- решения для управления документооборотом от YSoft;
- компьютерная техника и электроника от BenQ.

Преимущества работы с МУК:

- разветвленная партнерская сеть;
- сертифицированные мультивендорные специалисты;
- отсутствие привязки к конкретному продукту/платформе, что дает гибкость в выборе оптимального варианта решения задач;
- гибкая политика ценообразования;
- минимальное время производственного процесса;
- автоматизированная схема приема и обработки заявок с веб-интерфейсом;
- возможность закрепления сделки под конкретный проект;
- наличие в портфеле компании решений лидирующих производителей отрасли;
- инсталляция оборудования и ПО, обслуживание и консалтинг;
- обучение сервис-партнеров.

Возможность заказа или тестирования указанных в статье продуктов можно запросить в компании MUK COMPUTERS. Для получения детальной информации об этих решениях и их приобретении, ознакомления с партнерскими программами и предоставляемыми VAD-сервисами, а также с предложениями о проведении совместных мероприятий обращаться по тел. +996 552 585 999 или электронному адресу office@muk.kg.



MUK COMPUTERS,
КЫРГЫЗСТАН, БИШКЕК

MUK COMPUTERS компаниясы өз ишин Кыргызстандын аймагында 2017-жылы баштаган

Компания дилердик тармак аркылуу гана сатуу менен Value-Added Distribution моделин Кыргызстандын аймагында жигердүү өнүктүрүүдө. Ошону менен бирге эле MUK COMPUTERS компаниясынын адистери иштин ар башка иш чөйрөлөрүндө долбоорлорду иштеп чыгууга жана колдонууга киргизүүгө активдүү катышууда. Компаниянын продукттук портфолиосу улам кеңейүүдө жана 4x, A10 Networks, ACTi, AEG, Altaro, APC, Avigilon, BenQ, Bitdefender, BitTitan, Commscope, Conteg, Delphix, Dropsuite, e.HOT, EnGenius, IBM, InFocus, IXIA, Ivanti, Juniper Networks, Kingston, Matrix, Metis, Microsoft, NetApp, Oracle, PacketLight, Proget Software, Qnap, Radware, RCG Power, SaneBox, Sharp, Shavlik, Shenzhen Max Power, Stratus, Symantec, Tescom, Veeam, YSoft, Zimbra, Zoom сыяктуу өндүрүүчүлөрдүн чечимдерин өзүнө камтыйт.

МУК компаниялар тобунун ассортиментинде төмөнкүлөр сунушталат:

- IBM жана Oracleден сервердик чечимдер;
- IBM, NetApp жана Oracle маалыматтарды сактоо системалары;
- APC дан ЦОД түзүлүшү үчүн комплекстүү чечимдер;
- резервдик көчүрмөлөө чечимдери жана Veeamден маалыматтарды калыбына келтирүү жана репликациялар;
- Oracle программасынан булут тиркемелердин, платформалардын жана инженердик системалардын толук жана толугу менен интеграцияланган түзүлүшү;
- Delphix программасынан маалымат базасын виртуалдаштыру үчүн чечимдер;
- Bitdefender, IBM, IXIA, Oracle, Symantec программаларына коопсуздук чечимдери;
- IXIA дан IP-түйүндөрү үчүн тесттик жабдуулар;
- Avigilondон видео байкоо системалары үчүн жабдуулар;
- AEG Power Solutions, APC, Shenzhen Max Power, Tescom программаларынан үзгүлтүксүз камсыз кылуу булактары жана батареялары;
- EnGenius, IXIA жана PacketLight программаларынан өткөрмөлүү жана өткөрмөсүз тармактары үчүн жигердүү тармактык жабдуулар;
- Altaro, IBM, Ivanti, Microsoft, Oracle, Stratus жана Veeamден программалык камсыздоо;
- 4x жана Conteg телекоммуникациялык шкафтар жана тирөөчтөр;
- InFocusда проекторлор жана интерактивдүү экрандар;
- Sharpтан визуалдаштыруу чечимдери;
- Commscopeде СКС компоненттери;
- e.HOTтон кепилденген электр менен камсыздоо системаларынын компоненттери;
- RCG Power генераторлору;
- Kingston эс тутум модулдары;
- Ysofttон документ жүгүртүүнү жөнгө салуу чечимдери;
- BenQдан компьютердик техника жана электроника.

МУК менен иштөө артыкчылыктары:

- ар багыттуу өнөктөштүк тармактары;
- сертификатталган мультивендордук адистер;
- конкреттүү продуктка/платформага байланыштын жоктугу, бул маселелерди чечүүнүн оптималдуу вариантын тандоодо жеңилдик берет;
- баа түзүүнүн ыңгайлуу саясаты;
- өндүрүштүк процесстин минималдуу убактысы;
- веб-интерфейс менен билдирмелерди кабыл алуунун жаа иштеп чыгууну автоматташтырылган схемасы;
- бүтүмдөрдү конкреттүү долбоорго бекитүү мүмкүнчүлүгү;
- компаниянын портфелинде тармактын алдыңкы өндүрүүчүлөрүнүн чечимдеринин болушу;
- жабдууларды жана программалык камсыздоо инсталляциясы, тейлөө жана консалтинг;
- тейлөө-өнөктөштөрүн окутуу.

MUK COMPUTERS компаниясы аркылуу статьяда көрсөтүлгөн продукттарга буйрутма берүү же тесттен өткөрүү мүмкүн болот. Бул чечимдер жана аларды колдонуу тууралуу толук маалымат алуу, өнөктөштүк программалар жана сунушталуучу VAD-сервистер менен таанышуу үчүн, ошондой эле биргелешкен иш – чараларды өткөрүү тууралуу сунуштар менен +996 552 585 999 телефону же office@muk.kg. электрондук дареги боюнча кайрылсаңыздар болот.

MUK DISTRIBUTION,
МОЛДОВА, КИШИНЕВ

Компания MUK Distribution начала свою деятельность в Республике Молдова в марте 2012 года

За время работы были подписаны контракты с ведущими производителями мировой ИТ-индустрии – 4x, A10 Networks, ACTi, AEG, Altaro, Autodesk, BenQ, BitTitan, Check Point, Cisco, CommScope, Conteg, Dell EMC, Delphix, Dropsuite, e.HOT, EnGenius, Extreme Networks, Grandstream Networks, HPI, InFocus, IXIA, Ivanti, Juniper Networks, Kingston, Matrix, Microsoft, NetApp, Oracle, PacketLight, Penta Security, Proget Software, Qnap, Radware, RCG Power, Samsung, SaneBox, Shavlik, Shenzhen Max Power, Stratus, Tescom, Trend Micro, Tripp Lite, Veeam, Ysoft, Zimbra, Zoom. Компания активно развивает партнерскую сеть в Молдове и Приднестровье.

Работа с партнерами

Компания MUK Distribution при продвижении решений вендоров на рынке уделяет особое внимание обучению партнеров и заказчиков, проводя различные мероприятия – презентации новых продуктов, обучающие семинары и вебинары и т. д.

Недавно компания MUK Distribution стала авторизованным дистрибутором в Молдове корпораций Microsoft и HP, Inc.

Совместно с партнером BTS Pro и компаниями Cisco Systems, NetApp и Oracle были организованы семинары для заказчиков. Инженеры MUK Distribution и представители вендоров рассказали о различных семействах продуктов, в частности, о новинках в линейках безопасности.

Уже практически традицией стали демонстрации технологий Cisco Telepresence в формате бизнес-ланча, во время которых показывается работа оборудования бизнес-класса последнего поколения для организации видеоконференций в формате HD. Партнеры Cisco в Молдове и их заказчики общаются в режиме телемостов Кишинев – Киев с инженерами МУК и Cisco.

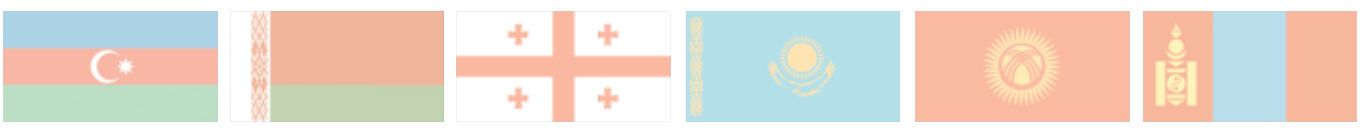
Возможность заказа или тестирования указанных в статье продуктов можно запросить в компании MUK Distribution. Для получения детальной информации об этих решениях и их приобретении, ознакомления с партнерскими программами и предоставляемыми VAD-сервисами, а также с предложениями о проведении совместных мероприятий обращаться по тел. +373 (67) 70-06-11 или по электронному адресу office@muk.md.

Оборудование для тестов

На складе компании для партнеров доступен набор демооборудования для тестирования:

- фаервол Check Point 15400 Next Generation Threat Prevention Appliance;
- системы ВКС и IP-телефонии Grandstream и Cisco.
- оборудование от Audiocodes, Cisco Systems.

Ассортимент демооборудования постоянно обновляется и пополняется.



MUK DISTRIBUTION,
REPUBLICA MOLDOVA, CHIȘINĂU

Compania MUK Distribution și-a început activitatea în Republica Moldova în luna martie 2012

De-a lungul timpului, compania a semnat contracte cu producătorii de top din industria IT din lume – 4x, A10 Networks, ACTi, AEG, Altaro, Autodesk, BenQ, BitTitan, Check Point, Cisco, CommScope, Conteg, Dell EMC, Delphix, Dropsuite, e.HOT, EnGenius, Extreme Networks, Grandstream Networks, HPI, InFocus, IXIA, Ivanti, Juniper Networks, Kingston, Matrix, Microsoft, NetApp, Oracle, PacketLight, Penta Security, Proget Software, Qnap, Radware, RCG Power, Samsung, SaneBox, Shavlik, Shenzhen Max Power, Stratus, Tescom, Trend Micro, Tripp Lite, Veeam, Ysoft, Zimbra, Zoom. Compania își extinde activ rețeaua de parteneri atât în Moldova, cât și în Transnistria.

Colaborarea cu partenerii

Compania MUK Distribution acordă o atenție deosebită instruirii partenerilor și clienților și, ca și parte a măsurilor de promovare a echipamentelor furnizate de producătorii de soluții IT, organizează diverse evenimente – prezentări de produse noi, seminare de instruire și video-conferințe etc.

Anul trecut, compania MUK Distribution a devenit distribuitor autorizat în Republica Moldova a produselor companiilor Microsoft și HP, Inc.

În colaborare cu compania BTS Pro și Cisco Systems, NetApp și Oracle au fost organizate seminare de informare pentru clienți. Inginerii companiei MUK Distribution și reprezentanții producătorilor de soluții IT au prezentat informații despre asortimentul de produse, și, în mod special, au vorbit despre produsele noi din domeniul securității informaționale.

Au devenit practic tradiționale demonstrațiile tehnologiei Cisco Telepresence efectuate în format de business-lunch, în timpul cărora se demonstrează funcționarea echipamentului de ultimă generație de clasă business pentru organizarea video-conferințelor în format HD. Partenerii Cisco din Republica Moldova și clienții acestora comunică în timp real, prin intermediul video-conferințelor ce leagă Chișinăul și Kievul, cu inginerii MUK și Cisco.

Produsele la care se face referire în articol pot fi comandate sau testate de la compania MUK Distribution. Pentru a primi informații suplimentare despre aceste produse și despre cum pot fi ele achiziționate sau pentru a Vă informa cu privire la programele de afiliere și despre serviciile VAD disponibile, precum și cu ofertele de organizare a evenimentelor în parteneriat, vă rugăm să ne apelați la următorul număr de telefon +373 (67) 70-06-11 sau prin email office@muk.md.

Echipament pentru sesiunile de testare

Compania oferă partenerilor spre testare un șir de echipamente, ca de exemplu:

- Sistem firewall Check Point 15400 Next Generation Threat Prevention Appliance;
- Sisteme de video-conferință și IP telefonie Grandstream и Cisco;
- Echipamente Audiocodes, Cisco Systems.

Gama de echipamente de testare se actualizează și se completează permanent.

МУК КОМПЬЮТЕРС,
МОНГОЛИЯ, УЛААНБААТАР

Компания «МУК Компьютерс» начала свою деятельность в Монголии в 2019 году

За время работы были подписаны контракты с такими производителями в сфере ИТ-индустрии, как BitTitan, Dropsuite, EnGenius, Extreme Networks, Microsoft, PacketLight, Proget Software, Oracle, SaneBox, Shenzhen Max Power. Помимо этого компания активно развивает в Монголии партнерскую сеть, осуществляя продажи исключительно через своих партнеров и помогая им в реализации проектов различного масштаба для заказчиков разных сфер деятельности.

В ассортименте «МУК Компьютерс» представлены:

- облачные решения Microsoft;
- сервисы миграции BitTitan;
- решения для резервного копирования, архивирования и восстановления данных Dropsuite;
- сетевое оборудование EnGenius и Extreme Networks;
- CWDM/DWDM- и OTN-решения PacketLight;
- управление электронной почтой SaneBox;
- корпоративная система управления мобильными устройствами от Proget Software.

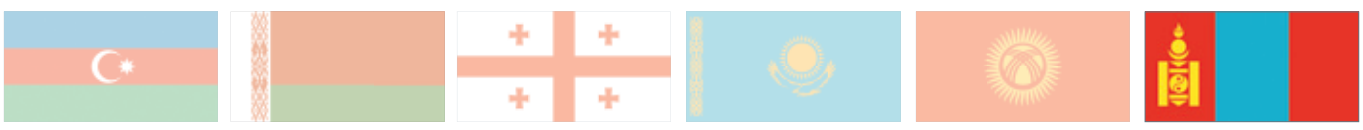
Преимущества работы с МУК:

- разветвленная партнерская сеть;
- сертифицированные мультивендорные специалисты;
- отсутствие привязки к конкретному продукту/платформе, что дает гибкость в выборе оптимального варианта решения задач;
- гибкая политика ценообразования;
- минимальное время производственного процесса;
- наличие в портфеле компании решений лидирующих производителей отрасли;
- инсталляция оборудования и ПО, обслуживание и консалтинг;
- обучение сервис-партнеров.

Возможность заказа или тестирования указанных в статье продуктов можно запросить в компании «МУК Компьютерс». Для получения детальной информации об этих решениях и их приобретении, ознакомления с партнерскими программами и предоставляемыми VAD-сервисами, а также с предложениями о проведении совместных мероприятий обращаться по тел. +976 (75) 05-75-77 или по электронному адресу office@muk.mn.

Оборудование для тестов

На складе компании для партнеров доступен набор демооборудования для тестирования.
Перечень оборудования предоставляется по запросу.
Ассортимент демооборудования постоянно обновляется и пополняется.



MUK DISTRIBUTION,
МОНГОЛ УЛС, УЛААНБААТАР ХОТ

МУК Компьютерс компани нь Монгол улсад 2019 оноос үйл ажиллагаагаа явуулж эхэлсэн.

Өнгөрсөн хугацаанд мэдээлэл технологийн салбарын BitTitan, Dropsuite, EnGenius, Extreme Networks, Microsoft, PacketLight, Proget Software, Oracle, SaneBox, Shenzhen Max Power зэрэг үйлдвэрлэгчидтэй гэрээ байгуулсан билээ. Компани нь мөн Монгол улсад хамтын ажиллагааны сүлжээг идэвхтэй байгуулан зөвхөн өөрийн түнш байгууллагуудаар дамжуулан борлуулалт хийж олон салбарын хэрэглэгчдэд төрөл бүрийн төсөл хэрэгжүүлэхэд туслалцаа үзүүлж байна.

МУК Компьютерсийн бүтээгдэхүүн үйлчилгээний цар хүрээ:

- Microsoft-ын үүлэн шийдлүүд;
- BitTitan-ын шилжүүлгийн үйлчилгээ;
- Dropsuite-ын нөөцлөх хуулбар, архивын сан болон мэдээлэл сэргээх шийдэл;
- EnGenius болон Extreme Networks-ийн сүлжээний төхөөрөмж;
- PacketLight-ийн CWDM / DWDM болон OTN шийдэл;
- SaneBox цахим шуудангийн удирдлага;
- Proget Software-ын зөөврийн төхөөрөмж удирдах нэгдсэн систем.

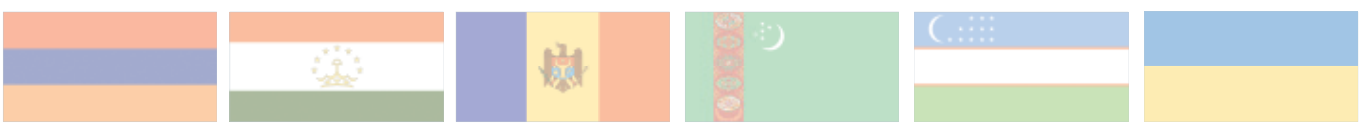
МУК-тэй хамтран ажиллахын давуу талууд:

- Хамтрагчдын өргөн сүлжээ;
- Олон чиглэлийн мэргэшсэн ажилтнууд;
- Тодорхой нэг бүтээгдэхүүн/платформыг заавал ашиглах шаардлага байхгүй учир хамгийн тохиромжтой шийдлийг сонгох боломжтой;
- Үнийн уян хатан бодлого;
- Үйлдвэрлэлийн хугацаа хамгийн бага;
- Компанийн бүтээгдэхүүн үйлчилгээний цар хүрээнд салбарын шилдэг үйлдвэрлэгчдийн шийдэл багтдаг;
- Төхөөрөмж суурилуулалт, үйлчилгээ, зөвлөгөө;
- Үйлчилгээ үзүүлэх түншүүдийг сургах.

МУК Компьютерс компаниас бүтээгдэхүүн үйлчилгээний жагсаалтанд байгаа бүтээгдэхүүнийг захиалах, туршиж үзэх боломжтой. Шийдэл болон тэдгээрийг ашиглах, түншүүдийн программтай танилцах, үзүүлж буй VAD үйлчилгээний талаарх дэлгэрэнгүй мэдээлэл авах болон хамтран арга хэмжээ явуулах тухай саналтай бол +976 (75) 05-75-77 утсаар эсхүл office@muk.mn цахим хаягаар холбогдоно уу.

Туршилтын төхөөрөмж тоноглол

Хамтран ажиллах байгууллагуудад зориулсан компанийн агуулахад туршилт тест хийх үзүүлэнгийн төхөөрөмж байгаа болно. Хүсэлт гаргаж төхөөрөмжийн жагсаалтыг авах боломжтой. Туршилт тестийн үзүүлэнгийн төхөөрөмж тогтмол шинэчлэгдэж нэмэгдэж байдаг болно.



МУК COMPUTERS,
ТАДЖИКИСТАН, ДУШАНБЕ

Группа компаний МУК начала свою деятельность на территории Таджикистана в августе 2014 года

На данный момент портфель компании включает в себя контракты с ведущими компаниями-производителями в сфере информационных технологий: 4x, A10 Networks, ACTi, AEG, Altaro, APC, Avigilon, BenQ, Bitdefender, BitTitan, Commscope, Conteg, Delphix, Dell EMC, Dropsuite, e.HOT, EnGenius, Fortinet, Grandstream Networks, Hikvision, HPE, IBM, InFocus, IXIA, Ivanti, Juniper Networks, Kingston, Matrix, Microsoft, NetApp, Oracle, PacketLight, Proget Software, Qnap, Radware, RCG Power, Samsung, SaneBox, Sharp, Shavlik, Shenzhen Max Power, Stratus, Symantec, Tescom, Veeam, YSoft, Zimbra, Zoom. МУК является активным игроком рынка ИТ, оказывая партнерам помощь в реализации проектов различного масштаба и сложности. Недавно компания получила статус VAD-дистрибьютора IBM, Microsoft Cloud Service Provider, Oracle, что позволяет предложить партнерам и заказчикам большой спектр высокотехнологичных решений.

Благодаря плодотворному сотрудничеству МУК с партнерами в 2017 году специалисты компании приняли активное участие в разработке и внедрении нескольких успешных проектов, внеся свой вклад в развитие страны в области информационных технологий. Среди них – решение по построению безопасной беспроводной инфраструктуры для первой в Душанбе платформы коллективной работы Puzzle Co-working, которое упростило процесс обслуживания и сделало возможным построение интеллектуальных сетей. Также был реализован ряд программ по повышению эффективности деятельности государственных учреждений. Эти проекты облегчают доступность предоставляемых гражданам общественных услуг, контролируя и сокращая эти процедуры.

Прошедший год отметился активным продвижением и внедрением на рынке решений таких производителей, как APC, Hewlett Packard Enterprise и Oracle. При участии и поддержке MUK COMPUTERS был реализован целый ряд крупных проектов на базе продуктов этих производителей для предприятий государственного сектора.

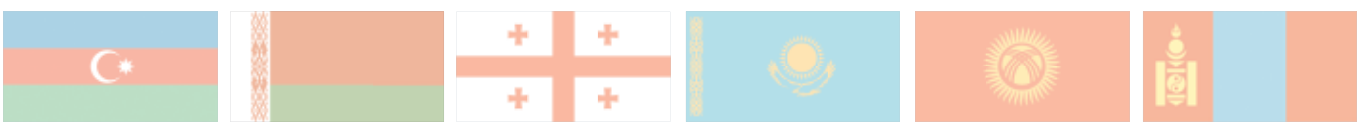
В ассортименте группы компаний МУК представлены:

- серверные решения от DellEMC, IBM, HPE, Oracle;
- системы хранения данных Dell EMC, HPE, IBM, NetApp;
- решения безопасности от Bitdefender, Fortinet, IBM, Juniper Networks, IXIA;
- тестовое оборудование для IP-сетей от IXIA;
- оборудование для систем видеонаблюдения от Avigilon, ACTI и Grandstream;
- телефония и видеосвязь от Alcatel-Lucent, Grandstream и Unify;
- ИБП и батареи от AEG Power Solutions, APC, Tripp Lite, HPE, Matrix, Shenzhen Max Power, Tescom;
- активное сетевое оборудование для проводных и беспроводных сетей от EnGenius, Fortinet, HPE, IXIA и PacketLight;
- программное обеспечение от Altaro, BitTitan, IBM, Ivanti, Microsoft, Oracle, Stratus, Veeam;
- телекоммуникационные шкафы и стойки APC и Commscope;
- проекторы и интерактивные экраны от BenQ и InFocus;
- компоненты СКС от Commscope;
- компоненты систем гарантированного электропитания от e.HOT;
- генераторы RCG Power;
- модули памяти Kingston;
- решения для управления документооборотом от YSoft;
- компьютерная техника и электроника от BenQ.

Преимущества работы с МУК:

- разветвленная партнерская сеть;
- сертифицированные мультивендорные специалисты;
- отсутствие привязки к конкретному продукту/платформе, что дает гибкость в выборе оптимального варианта решения задач;
- гибкая политика ценообразования;
- минимальное время производственного процесса;
- автоматизированная схема приема и обработки заявок с веб-интерфейсом;
- возможность закрепления сделки под конкретный проект;
- наличие в портфеле компании решений лидирующих производителей отрасли;
- инсталляция оборудования и ПО, обслуживание и консалтинг;
- обучение сервис-партнеров.

Возможность заказа или тестирования указанных в статье продуктов можно запросить в группе компаний МУК. Для получения детальной информации об этих решениях и их приобретении, ознакомления с партнерскими программами и предоставляемыми VAD-сервисами, а также с предложениями о проведении совместных мероприятий обращаться по тел. +992 (44) 660 66 99, +992 (44) 640-66-99 или электронному адресу office@muk.tj.



MUK COMPUTERS,
ТОҶИКИСТОН, ДУШАНБЕ

Гуруҳи ширкатҳои МУК фаъолияти худро дар ҳудуди Тоҷикистон моҳи августи соли 2014 шурӯъ кардааст

Айни замон портфолиои ширкат шартномаҳо бо ширкатҳои пешбари истеҳсолкунанда дар соҳаи технология информатсионӣ: 4x, A10 Networks, ACTi, AEG, Altaro, APC, Avigilon, BenQ, Bitdefender, BitTitan, Commscope, Conteg, Delphix, Dell EMC, Dropsuite, e.HOT, EnGenius, Fortinet, Grandstream Networks, Hikvision, HPE, IBM, InFocus, IXIA, Ivanti, Juniper Networks, Kingston, Matrix, Microsoft, NetApp, Oracle, PacketLight, Proget Software, Qnap, Radware, RCG Power, Samsung, SaneBox, Sharp, Shavlik, Shenzhen Max Power, Stratus, Symantec, Tescom, Veeam, YSoft, Zimbra, ва Zoom-ро дар бар мегирад. MUK бозингари фаъоли бозори ТИ буда, ба шарикон дар татбиқи лоиҳаҳои андоза ва мураккабиашон гуногун кумак мекунад. Ба наздикӣ, ширкат мақоми VAD-дистрибютори IBM, Microsoft Cloud Service Provider, Oracle-ро ба даст оварда, ки ин ба шарикон ва мизоҷон пешниҳоди васеъи қарорҳои технологияи олӣро медиҳад.

Соли сипаришуда бо пешбарии фаъол ва татбиқи қарорҳо аз истеҳсолкунандагони APC, Hewlett Packard Enterprise ва Oracle тақдир гашт. Бо иштирок ва дастгирии ширкати MUK COMPUTERS як қатор лоиҳаҳои калонҳаҷм дар асоси маҳсулоти истеҳсолкунандагони зерин барои корхонаҳои бахши давлатӣ, татбиқ карда шуданд.

Ба навъҳои гурӯҳи шаркати МУК дохил мешаванд:

- қарорҳои серверӣ аз Dell EMC, IBM, HPE, Oracle;
- системаҳои нигоҳдории маълумот Dell EMC, HPE, IBM, NetApp;
- қарорҳо оид ба амният аз Bitdefender, Fortinet, IBM, Juniper Networks, IXIA;
- таҷҳизотҳои санҷишӣ барои шабакаҳои IP аз IXIA;
- таҷҳизот барои системаҳои назорати видеоӣ аз Avigilon, ACTI ва Grandstream;
- алоқаи телефонӣ ва видеоӣ аз Alcatel-Lucent, Grandstream ва Unify;
- МББ ва батареяҳо аз AEG Power Solutions, APC, Tripp Lite, HPE, Matrix, Shenzhen Max Power, Tescom;
- таҷҳизоти шабакавии фаъол барои шабакаҳои симдор ва бесим аз EnGenius, Fortinet, HPE, IXIA ва PacketLight;
- нармафзор аз Altaro, BitTitan, IBM, Ivanti, Microsoft, Oracle, Stratus, Veeam;
- чевон ва пояҳои телекоммуникатсионии APC ва Commscope;
- проекторҳо ва экранҳои интерактивии BenQ ва InFocus;
- қисматҳои СКТ аз Commscope;
- ҷузъҳои системаҳои кафолатдори барқӣ аз e.HOT;
- генераторҳо аз RCG Power;
- модулҳои хотиравии Kingston;
- қарор оид ба идоракунии ҳуҷҷатнигорӣ аз YSoft;
- техникаи компютерӣ ва электроника аз BenQ.

Афзалиятҳои кор бо МУК:

- шабакаи васеъи шарикӣ;
- мутахассисон мултивендори дорои сертификат;
- ба аниқ маҳсулот/платформа мутобиқ набудан, ки барои интихоби варианти қарори беҳтарин чандирӣ мебахшад;
- сиёсати нархгузории фасеҳ;
- фосилаи камтарин дар раванди истеҳсолот;
- тарҳи автоматикии қабул ва коркарди дархост тавассути веб-интерфейс;
- имконияти муттаҳид кардани аҳд ба лоиҳаи мушаххас;
- дар портфолиои ширкат мавҷуд будни қарорҳои истеҳсолкунандагони пешбари ин соҳа;
- насби таҷҳизот ва БТ, хизматрасонӣ ва маслиҳатдиҳӣ;
- омӯзонидан шарикони-хидматӣ.

Барои фармоиш ё санҷиши маҳсулотҳои дар мақола зикршуда, ба гурӯҳи ширкати МУК муроҷиат намоед. Барои гирифтани маълумоти муфассал оиди қарорҳо ва дастоварди он, шиносоӣ бо лоиҳаҳои ҳамкорӣ ва VAD-хизматрамонӣ, ва инчунин пешниҳодҳо оиди дар якҷоягӣ гузаронидани чорабиниҳо ба рақами . +992 (44) 660-66-99, +992 (44) 640-66-99 ва ё тавассути почтаи электронӣ office@muk.tj тамос бигиред.

MUK INTERNATIONAL,
ТУРКМЕНИСТАН, АШХАБАД

Группа компаний МУК начала поставки оборудования на территорию Туркменистана в 2015 году

Основное направление деятельности компании – дистрибуция компьютерной техники, периферийного и сетевого оборудования, программного обеспечения, решений для построения инфраструктуры и сопутствующих сервисов. Специалисты МУК принимают активное участие в разработке и внедрении использующих эти решения проектов, предоставляя комплекс дополнительных услуг для своих дилеров и развивая модель Value-Added Distribution. Компания осуществляет продажи исключительно через дилерскую сеть. В настоящее время портфель МУК включает в себя контракты с такими производителями, как 4x, A10 Networks, ACTi, AEG, Altaro, APC, BenQ, Bitdefender, BitTitan, Check Point, Conteg, Delphix, Dropsuite, e.HOT, EnGenius, Extreme Networks, Fortinet, Geovision, HPE, IBM, Infocus, Ivanti, IXIA, Juniper Networks, Kingston, Matrix, Microsoft, NetApp, Oracle, PacketLight, Penta Security, Proget Software, Qnap, Radware, RCG Power, Samsung, SaneBox, Sharp, Shavlik, Shenzhen Max Power, Stratus, Symantec, Tescom, Veeam, YSoft, Zimbra, Zoom.

За минувший год МУК активно развивала на территории Туркменистана актуальное направление кибербезопасности. Была организована поставка деморешений Check Point и Symantec, результатом чего стало заключение договоренностей с партнерами и реализация целого ряда проектов на базе продуктов этих производителей в сфере информационной безопасности. Также компания активно участвует в организации и проведении семинаров и конференций для партнеров и заказчиков.

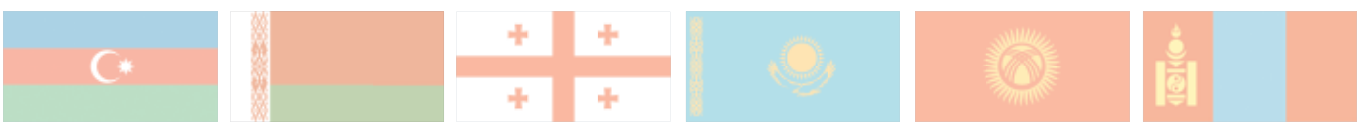
В ассортименте группы компаний МУК представлены:

- серверы стандартной архитектуры HPE и серверные опции к ним;
- серверные решения от IBM;
- блейд-системы от HPE;
- RISC-серверы от HPE;
- системы хранения данных HPE, IBM, NetApp, Oracle;
- решения безопасности Bitdefender, Check Point, Fortinet, IBM, IXIA, HPE, Penta Security, Radware, Symantec;
- тестовое оборудование для IP-сетей от IXIA;
- оборудование для систем видеонаблюдения от Geovision;
- ИБП и батареи от AEG Power Solutions, APC, Shenzhen Max Power, Tescom;
- активное сетевое оборудование для проводных и беспроводных сетей от EnGenius, Fortinet, PacketLight;
- телекоммуникационные шкафы и стойки APC, 4x и Conteg;
- проекторы и интерактивные экраны от InFocus;
- компоненты систем гарантированного электропитания от e.HOT;
- генераторы RCG Power;
- программное обеспечение от Altaro, BitTitan, IBM, Ivanti, HPE, Microsoft, Oracle и Stratus;
- модули памяти Kingston;
- решения управления печатью от YSoft;
- компьютерная техника и электроника от BenQ.

Преимущества работы с МУК:

- разветвленная партнерская сеть;
- сертифицированные мультивендорные специалисты;
- отсутствие привязки к конкретному продукту/платформе, что дает гибкость в выборе оптимального варианта решения задач;
- гибкая политика ценообразования;
- минимальное время производственного процесса;
- автоматизированная схема приема и обработки заявок с веб-интерфейсом;
- возможность закрепления сделки под конкретный проект;
- наличие в портфеле компании решений лидирующих производителей отрасли;
- инсталляция оборудования и ПО, обслуживание и консалтинг;
- обучение сервис-партнеров.

Возможность заказа или тестирования указанных в статье продуктов можно запросить в компании MUK International. Для получения детальной информации об этих решениях и их приобретении, ознакомления с партнерскими программами и предоставляемыми VAD-сервисами, а также с предложениями о проведении совместных мероприятий обращаться по тел. +38 (044) 492-29-29, или по электронному адресам: office@tm.muk.international, turkmenistan@muk.ua.



MUK INTERNATIONAL,
TÜRKMENISTAN, AŞGABAT

MUK Kompaniýalar Topary 2015-nji ýyldan başlap Türkmenistanyň çägine enjamlary getirip başlady.

KoKompaniýanyň esasy iş görnüşi – kompýuter enjamlaryny, goşmaça we set enjamlaryny, programma üpjünçiligini, infrastrukturany we ugurdaş serwisleri gurnamak üçin ulanylýan çözgütleri ýaýratmakdan ybaratdyr. MUK hünärmenleri görkezilen çözgütleri ulanýan taslamalary işläp taýýarlamak we ornaşdyrmak boýunça işlere işjeň gatnaşýar, şeýle hem öz dilerleri üçin goşmaça hyzmatlaryň toplumyny berýär we Value-Added Distribution (“doly taýýar” ulgamyny ornaşdyrýan distribýutor) modelini üpjün edýär. Kompaniýa diňe diler ulgamy arkaly satuwlary ýerine ýetirýär. Häzirki wagtda MUK bukjasyna 4x, A10 Netwoks, ACTI, AEG, Altaro, APC, BenQ, Bitdefender, BitTitan, Chek Point, Conteg, Delphix, Dropsuite, e.HOT, EnGenius, Extreme Networks, Fortnet, Geovision, HPE, IBM, Infocus, Ivanti, IXIA, Juniper Networks, Kingston, Matrix, Microsoft, NetApp, Oracle, PacketLight, Penta Security, Proget Software, Qnap, Radware, RCQ Power, Samsung, SaneBox, Sharp, Shavlik, Shenzhen Max Power, Stratus, Symantec, Tescom, Veeam, YSoft, Zimbra, Zoom ýaly öndürijiler bilen şertnamalar girýär.

Geçen ýylda MUK Türkmenistanyň çäginde kiber howpsuzlygy boýunça derwaýys ugur boýunça işleri durmuşa ornaşdyrdy. Chek Point we Symantec demo-çözgütleri amala aşyryldy, şonuň netijesinde hyzmatdaşlar bilen geleşikler baglaşyldy hem-de şol öndürijiler bilen maglumat howpsuzlygy pudagynda birtopar taslamalar durmuşa geçirildi. Mundan başga-da, kompaniýamyz hyzmatdaşlar we buýrujylar üçin seminarlary we konferensiýalary guramakda we geçirmekde işjeň iş alyp barýar.

MUK kompaniýalar toparynyň iş çygryna şular girizildi:

- HPE standart binagärliginiň serwerleri we olar boýunça serwer mümkinçilikleri;
- IBM-den serwer çözgütleri;
- HPE-den bleýd-ulgamlar;
- HPE-den RISC-serwerler;
- HPE, IBM, NetApp, Oracle maglumatlary ýatda saklamak üçin ulgamlar;
- Bitdefender, Check Point, Fortinet, IBM, IXIA, HPE, Penta Security, Radware, Symantec howpsuzlyk çözgütleri;
- IXIA tarapyndan IP-setler üçin test enjamlary;
- Geovision tarapyndan wideogözegçilik ulgamlary üçin enjamlar;
- AEG Power Solutions, APC, Shenzhen Max Power, Tescom tarapyndan Üznüksiz tok çeşmeleri we batareýalar;
- EnGenius, Fortinet, PacketLight tarapyndan simlik we simsiz setler üçin işjeň set enjamlary;
- APC, 4x we Conteg tarapyndan telekommunikasi şkaflary we söýegleri;
- InFocus tarapyndan proýektorlar we interaktiw ekranlar;
- e.HOT tarapyndan kepillikli elektrik togy ulgamlarynyň komponentleri;
- RCG Power generatorlary;
- Altaro, BitTitan, IBM, Ivanti, HPE, Microsoft, Oracler we Stratus tarapyndan programma üpjünçiligi;
- Kingston ýat modullary;
- Ysoft tarapyndan dolandyryş çözgütleri;
- BenQ tarapyndan kompýuter tehnikasy we elektronika.

MUK bilen işlemegiň artykmaçlyklary:

- köp şahaly hyzmatdaşlyk seti;
- sertifikatlaşdyrylan multiwendor hünärmenleri;
- belli bir önüme/platforma baglylygyň bolmazlygy, munuň özi wezipeleri amala aşyrmakda üstünlige getirýär;
- nyrhy emele getirmekde başarnykly syýasat;
- önümçilik prosesiniň iň bir gysga wagty;
- web-interfeýsli ýüztutmalary kabul etmek we işlemek boýunça awtomatlaşdyrylan çözgüt shemasy;
- belli bir taslama boýunça geleşigi berkitmek mümkinçiligi;
- kompaniýalaryň bukjasynda pudagyň öňdebaryjy öndürijileriniň çözgütleriniň bolmagy;
- enjamlary we programma üpjünçiligini gurnamak, hyzmat we konsalting işleri;
- serwis-hyzmatçylara okuw geçmek.

Şu ýerde görkezilen önümleri sargyt etmek we testden geçirmek üçin MUK International kompaniýasyna ýüz tutmak bolar. Şol çözgütler we olary satyn almak barada giňişleýin maglumatlary almak, hyzmatdaşlyk maksatnamalary we VAD-serwisler bilen tanyşmak üçin, şeýle hem bilelikde çäreleri geçirmek boýunça teklipler bilen aşakdaky telefon we elektron poçta salgylaryna ýüz tutup bilersiňiz: +38 (044) 492-29-29 ýa-da office@tm.muk.international, turkmenistan@muk.ua.

MUK COMPUTERS,
УЗБЕКИСТАН, ТАШКЕНТ

Компания MUK COMPUTERS начала свою деятельность на территории Узбекистана в 2016 году

MUK COMPUTERS активно участвует в разработке проектов и внедрении оборудования и ПО в ИТ-инфраструктуру заказчиков, развивая модель Value-Added Distribution. С первых шагов на рынке компания ориентировалась на лидеров мировой ИТ-индустрии, и в настоящее время является дистрибутором таких брендов, как 4x, A10 Networks, ACTi, AEG, Altaro, APC, BenQ, Bitdefender, BitTitan, Cisco, Commscope, Conteg, Delphix, Dropsuite, e.HOT, EnGenius, IBM, InFocus, IXIA, Ivanti, Juniper Networks, Kingston, Matrix, Microsoft, NetApp, Oracle, PacketLight, Penta Security, Proget Software, Qnap, Radware, RCG Power, SaneBox, Shavlik, Shenzhen Max Power, Stratus, Symantec, Tescom, Veeam, YSoft, Zimbra, Zoom.

Прошедший год отметился активным продвижением и внедрением на рынке решений таких производителей, как Cisco, IBM и Oracle. При участии и поддержке MUK COMPUTERS был реализован целый ряд крупных проектов на базе продуктов этих производителей для предприятий государственного, финансового и телекоммуникационного сектора.

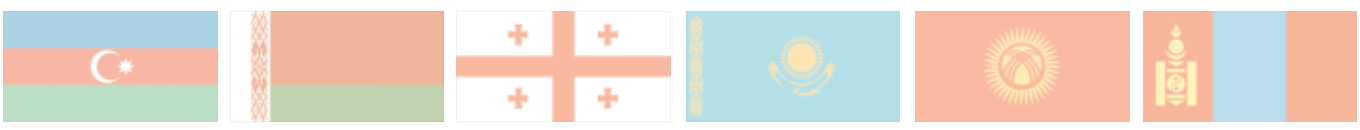
В ассортименте группы компаний МУК представлены:

- серверные решения от IBM;
- системы хранения данных IBM;
- решения безопасности от Bitdefender, Cisco, IBM, IXIA, Symantec;
- тестовое оборудование для IP-сетей от IXIA;
- ИБП и батареи от AEG Power Solutions, APC, IBM, Shenzhen Max Power, Tescom;
- активное сетевое оборудование для проводных и беспроводных сетей от Cisco, EnGenius, Fortinet, IXIA и PacketLight;
- программное обеспечение от Altaro, BitTitan, IBM, Ivanti, Microsoft, Oracle и Stratus;
- телекоммуникационные шкафы и стойки 4x, APC, Conteg;
- проекторы и интерактивные экраны от InFocus;
- компоненты СКС от Commscope;
- компоненты систем гарантированного электропитания от e.HOT;
- генераторы RCG Power;
- модули памяти Kingston;
- решения для управления документооборотом от YSoft;
- компьютерная техника и электроника от BenQ.

Преимущества работы с МУК:

- разветвленная партнерская сеть;
- доступность демооборудования для тестирования;
- сертифицированные мультивендорные специалисты;
- отсутствие привязки к конкретному продукту/платформе, что дает гибкость в выборе оптимального варианта решения задач;
- гибкая политика ценообразования;
- минимальное время производственного процесса;
- автоматизированная схема приема и обработки заявок с веб-интерфейсом;
- возможность закрепления сделки под конкретный проект;
- наличие в портфеле компании решений лидирующих производителей отрасли;
- инсталляция оборудования и ПО, обслуживание и консалтинг;
- обучение сервис-партнеров.

Возможность заказа или тестирования указанных в статье продуктов можно запросить в компании MUK COMPUTERS. Для получения детальной информации об этих решениях и их приобретении, ознакомления с партнерскими программами и предоставляемыми VAD-сервисами, а также с предложениями о проведении совместных мероприятий обращаться по тел. +998 (71) 205-10-12 или электронному адресу office@muk.uz.



MUK COMPUTERS,
ЎЗБЕКИСТОН, ТОШКЕНТ

MUK COMPUTERS компанияси Ўзбекистон ҳудудида ўз фаолиятини 2016 йилда бошлаган.

MUK COMPUTERS компанияси Value-Added Distribution моделини ривожлантирган ҳолда, ускуналар ва дастурий таъминот лойиҳаларини ишлаб чиқишда ва уларни буюртмачилар Инновацион технологиялари (ИТ)-инфратузилмасига татбиқ этишда фаол иштирок қилмоқда. Компания бозордаги дастлабки қадамларидан жаҳон миқёсидаги ИТ-саноат етакчиларига қараб иш тутди ва ҳозирги вақтда 4x, A10 Networks, ACTi, AEG, Altaro, APC, BenQ, Bitdefender, BitTitan, Cisco, Commscope, Conteg, Delphix, Dropsuite, e.HOT, EnGenius, IBM, InFocus, IXIA, Ivanti, Juniper Networks, Kingston, Matrix, Microsoft, NetApp, Oracle, PacketLight, Penta Security, Proget Software, Qnap, Radware, RCG Power, SaneBox, Shavlik, Shenzhen Max Power, Stratus, Symantec, Tescom, Veeam, YSoft, Zimbra, Zoom каби брендларнинг дистрибутори ҳисобланади.

Ўтган йил Cisco, IBM ва Oracle каби ишлаб чиқарувчилар томонидан фаол реклама ва ечимларнинг жорий этилиши билан эсда қолди. MUK COMPUTERSининг иштироки ва қулаб-қувватлаши билан ушбу ишлаб чиқарувчиларнинг маҳсулотлари асосида давлат, молия ва телекоммуникация сохасидаги корхоналар учун қатор йирик лойиҳалар амалга оширилди.

MUK COMPUTERS компанияси гуруҳи ассортиментида қуйидагилар тақдим этилган:

- IBMдан сервер ечимлари;
- IBM маълумотларни сақлаш тизими;
- Bitdefender, Cisco, IBM, Symantec, IXIAдан хавфсизлик ечимлари;
- IXIAдан IP тармоқлар учун тест ускуналари;
- AEG Power Solutions, APC, Shenzhen Max Power, Tescom, IBMдан ИБП ва батареялар;
- Cisco, EnGenius, Fortinet ва IXIAдан симли ва симсиз тармоқлар учун фаол тармоқ ускунаси;
- Altaro, BitTitan, IBM, Ivanti, Microsoft, Oracle ва Stratusдан дастурий таъминот;
- 4x, APC, Conteg телекоммуникация шкафлари ва пештахталари;
- InFocusдан проекторлар ва интерактив экранлар;
- Commscoредан СКС таркибий қисмлари;
- e.HOTдан кафолатланган электр таъминот тизимлари таркибий қисмлари;
- RCG Power генераторлари;
- Kingston хотира модуллари;
- Ysoftдан ҳужжат айланишини бошқариш учун ечимлар;
- BenQдан компьютер техникаси ва электроника.

MUK COMPUTERS компанияси билан ишлаш афзалликлари:

- кенг хамкорлик тармоқи;
- тестдан ўтказиш учун демо-ускуналардан фойдаланиш имконияти;
- сертификатланган мультивендор мутахассислари;
- муайян маҳсулотга/платформага боғлиқлик мавжуд эмаслиги, бу вазифалар ечимининг оптимал вариантини танлашда мослашувчанликни таъминлайди;
- мослашувчан нархни белгилаш сиёсати;
- ишлаб чиқариш жараёни минимал вақти;
- муайян лойиҳа асосида битим тузиш имконияти;
- компаниянинг тармоқдаги етакчи ишлаб чиқарувчилар томонидан эшимлар портфелида мавжудлиги
- ускуналар ва дастурий таъминот инсталляцияси, хизмат кўрсатиш ва консалтинг;
- сервис-ҳамкорларни ўқитиш.

Мақолада қайд этилган маҳсулотларни буюртма қилиш ёки тестдан ўтказиш имкониятини MUK COMPUTERS компаниясидан расмий равишда сўраш мумкин. Ушбу ечимлар ва уларни харид қилиш тўғрисида батафсил ахборот олиш, ҳамкорлик дастурлари ва тақдим қилинадиган VAD-сервислари, шунингдек биргаликда тадбирлар ўтказиш тўғрисидаги таклифлар билан танишиб чиқиш учун +998 (71) 205-10-12 телефон рақамлари ёки office@muk.uz. электрон манзил бўйича мурожаат қилинг.

ГРУППА КОМПАНИЙ МУК,
УКРАИНА, КИЕВ

Группа компаний МУК начала свою деятельность на территории Украины в 1997 году

Основным направлением деятельности компании является дистрибуция комплексных решений и оборудования ведущих мировых производителей в сфере информационных технологий – активного и пассивного сетевого оборудования, серверов, систем хранения данных, бесперебойного питания, телефонии и защиты данных, а также программного обеспечения для построения ИТ-инфраструктуры любого масштаба и сложности. Компания осуществляет продажи через дилерскую сеть и предоставляет комплекс дополнительных услуг для своих дилеров, развивая модель Value Added Distribution (VAD). Группа компаний МУК обладает всеми качествами, характерными для VAD-дистрибутора, и предлагает партнерам базовый «джентльменский набор» сервисов, таких как специальные предложения для реализации проектов, персонализированные кредитные линии, предоставление демооборудования для тестов, проработка проектов, пред- и послепродажный консалтинг и поддержка, тренинги по техникам продаж для торгового персонала, сервисная поддержка и т. д. Кроме того, компания предоставляет различные финансовые сервисы, позволяющие минимизировать риски и повысить стабильность бизнеса. Стоит отметить и отлаженную логистику компании, благодаря которой есть возможность осуществлять оперативную доставку оборудования во все регионы.

В настоящее время у группы компаний МУК подписаны контракты с более чем 50 крупнейшими мировыми A-Brand-производителями: Algosec, APC, ASUS, AudioCodes, Autodesk, Avigilon, Avocent, Check Point, Cisco, Commscope, Dell EMC, Delphix, Dropsuite, EnGenius, ESET, Extreme Networks, Fortinet, Fujitsu, Grandstream Networks, Himoinsa, Hitachi Vantara, HP Inc, IBM, Ivanti, IXIA, Juniper Networks, Kalmo Systems, Keenetic, Kingston, Kofax, LearnQuest, Lenovo, LifeSize, Matrix, Microsoft, NetApp, Oracle, PacketLight, Penta Security, Proget Software, Qnap, Quest Software, Radware, RCG Power, Ricoh, Samsung, SaneBox, Smiddle, StarWind, Stratus, Tescom, TrendMicro, Tripp Lite, Veeam, VMware, YSoft, Zimbra, Zoom.

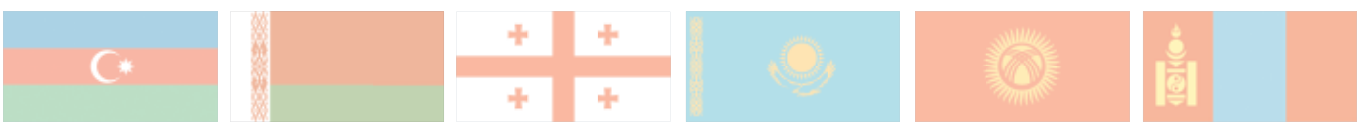
Учебный центр

Много внимания МУК уделяет обучению персонала партнеров и заказчиков. Учебный центр компании предлагает множество авторизированных курсов от ведущих мировых производителей ИТ-индустрии. Портфель УЦ МУК включает в себя более 300 учебных курсов от ведущих ИТ-компаний.

УЦ МУК имеет статусы: HPE Training Partner, Ukraine & CIS, IBM Authorized Training Partner, Microsoft Silver Learning Partner, Oracle Approved Education Provider, Dell EMC Education Partner, Fortinet Authorized Training Partner, Check Point Authorized Training Center, Juniper Authorized Training Partner, Veeam Authorized Education Center, Grandstream Authorized Education Center, Red Hat Certified Training Partner, CommScope Authorized Trainer Assessor, VMware Authorized Training Center, независимый центр тестирования Pearson VUE, а также ITIL Training Partner и Linux Authorized Training – в рамках партнерства с HPE.

Учебный центр МУК предоставляет:

- Индивидуальное консультирование:
  - помощь в выборе курса;
  - составление плана обучения;



- рекомендации по плану сертификации и подготовки к ней.

- Организация тренингов различных форматов:

- обучение в составе группы по общему расписанию;
- корпоративные курсы для ваших специалистов;
- дистанционное обучение под руководством инструктора (ILO, ILT, LVC);
- самостоятельное обучение онлайн (SPVC, TOD, ULS, CLS);
- партнерские мероприятия;
- тренинги, семинары, коучинг, эмуляторы деловых игр.

5 причин для вашего обучения с Учебным центром МУК:

1. Обновление ИТ-навыков по средствам интенсивного обучения – это ваш ключ к успеху.
2. Выбор из более чем 500 углубленных технических тренинговых программ и лабораторий.
3. Получение практического опыта и вовлечение в беспрерывный процесс развития.
4. Обмен идеями и взаимодействие с сообществом единомышленников, передовыми идеологами технологическими гуру, руководителями и экспертами ведущих ИТ-компаний.
5. Проверка и подтверждение своих знаний и навыков в процессе обучения.

Мы создаем базу для будущих успехов наших партнеров и заказчиков.

Сервисный центр

МУК имеет и собственный сервисный центр, более 17 лет оказывающий услуги сервиса ИТ-оборудования корпоративным заказчикам и частным клиентам. «МУК-Сервис» предлагает заказчикам широкий спектр услуг в сфере обслуживания и поддержки оборудования:

- инсталляция и пусконаладочные работы;
- диагностика и ремонт: гарантийный и негарантийный;
- контрактное обслуживание с гарантированным временем восстановления работоспособности;
- настройка оборудования;
- чистка оборудования;
- замена запчастей;
- плановая профилактика оборудования;
- продажа запасных частей;
- аренда и аутсорсинг техники.

Компания осуществляет ремонт оборудования свыше 100 брендов – серверов, систем хранения, сетевого и инфраструктурного оборудования, а также различной периферии.

Ключевыми преимуществами «МУК-Сервис» являются:

- широкий портфель брендов обслуживаемого оборудования: APC, Check Point, Cisco, Dell EMC, e.HOT, Extreme Networks, Fortinet, Fujitsu, Grandstream Networks, IBM, Hitachi Vantara, HPI, Oracle, Tripp Lite;
- покрытие региональной сетью всей Украины;
- гарантированное время восстановления ИТ-оборудования;
- полный спектр техники, подхватываемой на сервис: ноутбуки, серверы, системы хранения данных и сетевое оборудование;
- профессиональная команда сертифицированных инженеров;
- обширный склад запасных частей и подменного оборудования.

Маркетинговая активность

Одним из наиболее важных аспектов развития бизнеса для МУК является маркетинговая поддержка партнеров, а также продвижение брендов на рынке.

Каждый год МУК проводит десятки различных мероприятий для заказчиков и партнеров – встреч, презентаций новых продуктов, обучающих семинаров и т. д. Одним из наиболее масштабных является выставка MUK Expo, ежегодно проходящая в Киеве. Она собирает более 1500 специалистов в области информационных технологий не только из Украины, но и из стран СНГ и Европы, являясь для них своеобразной профессиональной площадкой для общения и обмена опытом. Форум представляет собой сочетание выставки и конференции. С одной стороны, гости имеют возможность посетить экспозиционную зону со стендами компаний-партнеров МУК, на которых представлены новейшие разработки в области ИТ-оборудования и программного обеспечения, предлагающие различные варианты для решения текущих задач для предприятий любого масштаба. Здесь же можно стать свидетелем «живых» демонстраций работы этих решений, которые проводятся прямо на стендах. С другой – можно поучаствовать в работе фокусных сессий и прослушать доклады, посвященные актуальным тенденциям в сфере информационных технологий и содержащие как теоретические сведения, так и прикладные аспекты работы тех или иных решений и технологий.

Возможность заказа или тестирования продуктов брендов, доступных в портфеле МУК, можно запросить в компании. Для получения детальной информации об этих решениях и их приобретении, ознакомления с партнерскими программами и предоставляемыми VAD-сервисами, а также с предложениями о проведении совместных мероприятий обращаться по тел. +38 (044) 492-29-29 или электронному адресу office@muk.com.ua.

ГРУПА КОМПАНІЙ МУК,
УКРАЇНА, КИЇВ

Група компаній МУК розпочала свою діяльність на території України в 1997 році

Основним напрямом діяльності компанії є дистрибуція комплексних рішень та обладнання провідних світових виробників у сфері інформаційних технологій – активного й пасивного мережевого обладнання, серверів, систем зберігання даних, безперебійного живлення, телефонії та захисту даних, а також програмного забезпечення для побудови IT-інфраструктури будь-якого масштабу і складності. Компанія здійснює продажі через дилерську мережу і надає комплекс додаткових послуг для своїх дилерів, розвиваючи модель Value Added Distribution (VAD). Група компаній МУК володіє всіма якостями, характерними для VAD-дистрибутора, і пропонує партнерам базовий «джентльменський набір» сервісів, таких як спеціальні пропозиції для реалізації проектів, персоналізовані кредитні лінії, надання демообладнання для тестів, опрацювання проектів, перед- і післяпродажний консалтинг і підтримка, тренінги з технік продажів для торгового персоналу, сервісна підтримка тощо. Крім того, компанія надає різні фінансові сервіси, що дозволяють мінімізувати ризики та підвищити стабільність бізнесу. Варто зазначити й налагоджену логістику компанії, завдяки якій є можливість здійснювати оперативну доставку обладнання в усі регіони.

Нині в групи компаній МУК підписані контракти з понад 50 найбільшими світовими A-Brand-виробниками: Algosec, APC, ASUS, AudioCodes, Autodesk, Avigilon, Avocent, Check Point, Cisco, Commscope, Dell EMC, Delphix, Dropsuite, EnGenius, ESET, Extreme Networks, Fortinet, Fujitsu, Grandstream Networks, Himoinsa, Hitachi Vantara, HP Inc, IBM, Ivanti, IXIA, Juniper Networks, Kalmo Systems, Keenetic, Kingston, Kofax, LearnQuest, Lenovo, LifeSize, Matrix, Microsoft, NetApp, Oracle, PacketLight, Penta Security, Proget Software, Qnap, Quest Software, Radware, RCG Power, Ricoh, Samsung, SaneBox, Smiddle, StarWind, Stratus, Tescom, TrendMicro, Tripp Lite, Veeam, VMware, YSoft, Zimbra, Zoom.

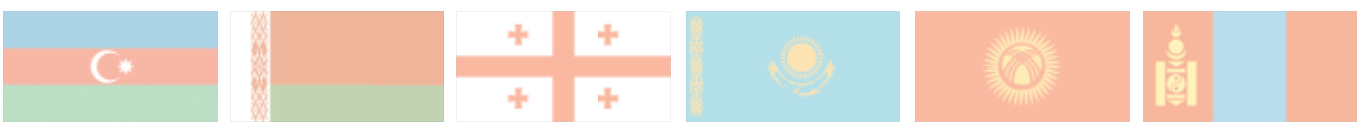
Навчальний центр

Багато уваги МУК приділяє навчанню персоналу партнерів і замовників. Навчальний центр компанії пропонує безліч авторизованих курсів від провідних світових виробників IT-індустрії. Портфель НЦ МУК містить у собі понад 300 навчальних курсів від провідних IT-компаній.

НЦ МУК має статуси: HPE Training Partner, Ukraine & CIS, IBM Authorized Training Partner, Microsoft Silver Learning Partner, Oracle Approved Education Provider, Dell EMC Education Partner, Fortinet Authorized Training Partner, Check Point Authorized Training Center, Juniper Authorized Training Partner, Veeam Authorized Education Center, Grandstream Authorized Education Center, Red Hat Certified Training Partner, CommScope Authorized Trainer Assessor, VMware Authorized Training Center, незалежний центр тестування Pearson VUE, а також ITIL Training Partner та Linux Authorized Training – у рамках партнерства з HPE.

Навчальний центр МУК надає:

- Індивідуальне консультування:
  - допомога у виборі курсу;
  - складання плану навчання;
  - рекомендації щодо плану сертифікації та підготовки до неї.
- Організація тренінгів різних форматів:
  - навчання в складі групи за загальним розкладом;
  - корпоративні курси для ваших фахівців;
  - дистанційне навчання під керівництвом інструктора (ILO, ILT, LVC);
  - самостійне навчання онлайн (SPVC, TOD, ULS, CLS);



- партнерські заходи;
- тренінги, семінари, коучинг, емулятори ділових ігор.

5 причин для вашого навчання у Навчальному центрі МУК:

1. Оновлення IT-навичок за засобами інтенсивного навчання – це ваш ключ до успіху.
2. Вибір з понад 500 поглиблених технічних тренінгових програм і лабораторій.
3. Отримання практичного досвіду й залучення в безперервний процес розвитку.
4. Обмін ідеями та взаємодія зі спільнотою однодумців, передовими ідеологами, технологічними гуру, керівниками та експертами провідних IT-компаній.
5. Перевірка й підтвердження своїх знань і навичок у процесі навчання.

Ми створюємо базу для майбутніх успіхів наших партнерів і замовників.

Сервісний центр

МУК має і власний сервісний центр, понад 17 років надає послуги сервісу IT-обладнання корпоративним замовникам і приватним клієнтам. «МУК-Сервіс» пропонує замовникам широкий спектр послуг у сфері обслуговування та підтримки обладнання:

- інсталяція та пусконалагоджувальні роботи;
- діагностика та ремонт: гарантійний і негарантійний;
- контрактне обслуговування з гарантованим часом відновлення працездатності;
- настройка обладнання;
- чистка обладнання;
- заміна запчастин;
- планова профілактика обладнання;
- продаж запасних частин;
- оренда та аутсорсинг техніки.

Компанія здійснює ремонт обладнання понад 100 брендів – серверів, систем зберігання, мережевого та інфраструктурного обладнання, а також різної периферії.

Ключовими перевагами «МУК-Сервіс» є:

- широкий портфель брендів обладнання, що обслуговується: APC, Check Point, Cisco, Dell EMC, e.HOT, Extreme Networks, Fortinet, Fujitsu, Grandstream Networks, IBM, Hitachi Vantara, HPI, Oracle, Tripp Lite;
- покриття регіональною мережею всієї України;
- гарантований час відновлення IT-обладнання;
- повний спектр техніки, що підхоплюється на сервіс: ноутбуки, сервери, системи зберігання даних і мережеве обладнання;
- професійна команда сертифікованих інженерів;
- великий склад запасних частин і підмінного обладнання.

Маркетингова активність

Одним з найбільш важливих аспектів розвитку бізнесу для МУК є маркетингова підтримка партнерів, а також просування брендів на ринку.

Щороку МУК проводить десятки різних заходів для замовників і партнерів – зустрічей, презентацій нових продуктів, навчальних семінарів тощо. Одним з найбільш масштабних є виставка MUK Expo, яка щорічно проходить у Києві. Вона збирає понад 1500 фахівців в області інформаційних технологій не лише з України, а й із країн СНД та Європи, будучи для них своєрідним професійним майданчиком для спілкування та обміну досвідом. Форум являє собою поєднання виставки та конференції. З одного боку, гості мають можливість відвідати експозиційну зону зі стендами компаній – партнерів МУК, на яких представлені новітні розробки в області IT-обладнання та програмного забезпечення, що пропонують різні варіанти для вирішення поточних завдань для підприємств будь-якого масштабу. Тут же можна стати свідком «живих» демонстрацій роботи цих рішень, які проводяться прямо на стендах. З іншого – можна взяти участь в роботі фокусних сесій та прослухати доповіді, які присвячені актуальним тенденціям у сфері інформаційних технологій та містять як теоретичні відомості, так і прикладні аспекти роботи тих чи інших рішень і технологій.

Можливість замовлення або тестування продуктів брендів, доступних у портфелі МУК, можна запросити в компанії. Для отримання детальної інформації про ці рішення та їх придбання, ознайомлення з партнерськими програмами та VAD-сервісами, що надаються, а також із пропозиціями про проведення спільних заходів звертатися за тел. +38 (044) 492-29-29 або за електронною адресою office@muk.com.ua.

ПОРТФЕЛЬ РЕШЕНИЙ МУК

БОЛЬШИЕ ДАННЫЕ (BIG DATA)

CISCO, DELL EMC, EXTREME NETWORKS, HEWLETT PACKARD ENTERPRISE, IBM, IXIA, MICROSOFT, ORACLE

БЕЗОПАСНОСТЬ

ALGOSEC, BITDEFENDER, CHECK POINT, CISCO, EXTREME NETWORKS, ESET, FORTINET, FS GROUP, IBM, JUNIPER NETWORKS, HEWLETT PACKARD ENTERPRISE, IXIA, ORACLE, RADWARE, SYMANTEC, TRENDMICRO

ВИДЕОНАБЛЮДЕНИЕ

ACTI, AVIGILON, GRANDSTREAM NETWORKS

ОБЛАЧНЫЕ РЕШЕНИЯ

CISCO, DELL EMC, DROPSUITE, EXTREME NETWORKS, FORTINET, HEWLETT PACKARD ENTERPRISE, IBM, IXIA, MICROSOFT, ORACLE, SANEBOX, STRATUS

СЕТЕВОЕ ОБОРУДОВАНИЕ

A10 NETWORKS, CISCO, COMMSCOPE, CONTEG, DELL EMC, ENGENIUS NETWORKS, EXTREME NETWORKS, FORTINET, JUNIPER NETWORKS, HEWLETT PACKARD ENTERPRISE, IXIA, ORACLE, PACKETLIGHT NETWORKS, QNAP

СЕРВЕРЫ

CISCO, DELL EMC, FUJITSU, HITACHI VANTARA, HEWLETT PACKARD ENTERPRISE, IBM, ORACLE, STRATUS

СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ

DELL EMC, FUJITSU, HITACHI VANTARA, HEWLETT PACKARD ENTERPRISE, IBM, NETAPP, ORACLE, QNAP

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

AUTODESK, DELPHIX, DELL EMC, HEWLETT PACKARD ENTERPRISE, IBM, IVANTI, MICROSOFT, ORACLE, PROGET SOFTWARE, QUEST SOFTWARE, STARWIND, STRATUS, VEEAM, VMWARE, ZIMBRA

ПЕЧАТЬ И ОЦИФРОВКА ДОКУМЕНТОВ

FUJITSU, HP INC., IGUANA, PLUSTEK, RICOH, SAMSUNG, YSOFT

РАБОЧИЕ СТАНЦИИ И ПЕРИФЕРИЯ

ASUS, BENQ, DELL EMC, FUJITSU, HP INC., INFOCUS, KINGSTON, LENOVO, SAMSUNG

ИНТЕРНЕТ ВЕЩЕЙ (IOT)

CISCO, EXTREME NETWORKS, HEWLETT PACKARD ENTERPRISE, IBM, IXIA, MICROSOFT, ORACLE

КОНВЕРГЕНТНЫЕ РЕШЕНИЯ

CISCO, DELL EMC, EXTREME NETWORKS, FUJITSU, HEWLETT PACKARD ENTERPRISE, IXIA, ORACLE

РЕШЕНИЯ ДЛЯ ТЕСТИРОВАНИЯ, СБОРА И ФИЛЬТРАЦИИ ТРАФИКА

IXIA, HEWLETT PACKARD ENTERPRISE

ТЕЛЕФОНИЯ И ВИДЕОСВЯЗЬ

AUDIOCODES, CISCO, GRANDSTREAM NETWORKS, LIFESIZE, SMIDDLE

УПРАВЛЕНИЕ ЭЛЕКТРОПИТАНИЕМ

AEG, APC, AVOCENT, E.HOT, HEWLETT PACKARD ENTERPRISE, TESCOM, TRIPP LITE

SD-WAN: НАДЕЖНАЯ СВЯЗЬ С САМЫМИ ОТДАЛЕННЫМИ МЕСТАМИ

Безопасное подключение любого пользователя, любого приложения в любом месте с помощью облачных технологий.

Cisco SD-WAN

- Обеспечение безопасной и гибкой связности
- Обеспечение качества работы приложений
- Для облака и в облаке
- Возможности гибкой эксплуатации

Подбор решений и помощь в проектах cisco@muk.ua