CIS
Современные Информационные Системы
Спецвыпуск (24) / 2023

MONT

ДИСТРИБЬЮТОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Для бизнеса любого масштаба

Информационная безопасность

Сегодня, в связи с ростом количества кибератак на российские предприятия, тема информационной безопасности стала актуальной как никогда. Перед заказчиками стоит нелёгкий вопрос приобретения необходимых и эффективных инструментов защиты.

Если многие ещё продолжают использовать прикладные решения ушедших с рынка западных вендоров, рассчитывая на экспертизу собственных инженеров и системных интеграторов, то продолжать использовать решения по информационной безопасности вендоров, объявивших, что они не будут поддерживать российских заказчиков, по-настоящему рискованно.

К счастью, внутренний рынок решений по информационной безопасности начал формироваться не вчера и сейчас он продолжает активно развиваться.

Мы видим особый интерес со стороны заказчиков к решению таких задач, как:

- защита данных от утечки (DLP);
- защита почты и веб-трафика;
- защита веб-приложений;
- защита от DDoS атак;
- контроль доступа;
- соответствие требованиям регуляторов.

Но всё более и более становится очевидно, что собственные сотрудники являются ключевым звеном защиты информации. Решения, призванные защитить от преднамеренных действий и ошибок также вызывают большой интерес. Это, например:

- оперативный мониторинг действий пользователей;
- защита информации от неправомерных действий пользователей, наделённых особыми полномочиями (PAM, Privileged Access Management);
- обучение сотрудников основам информационной безопасности.

В портфеле MONT представлены все основные вендоры решений по информационной безопасности, чьи продукты доступны для покупки в России.

Главный редактор: Станислав Понарин.
Директор по маркетингу: Валерия Рябинина.
Дизайн и вёрстка: Алексей Дмитриев.
Корректор: Оксана Макаренко.
Отдел рекламы и распространения: magazine@sovinfosystems.ru.
Сайт: www.cis.ru,
интернер-блог: cis.ru/blog.
Регистрация журнала: федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Номер свидетельства: ПИ № ФС 77-69584.
Дата регистрации: 02.05.2017.
Наименование СМИ:
Современные Информационные Системы.
Форма распространения: печатное СМИ, журнал.
Территория распространения:
Российская Федерация.
Адрес редакции: 22-й км Киевского ш., (п. Московский), д. 4, стр. 1, кор. Б, офис 04, блок 904Б, г. Москва, 108811.
Язык: русский.
Периодичность: 4 раза в год (1 раз в квартал).

Тираж 5000 экз. (отпечатанный тираж).
Журнал предназначен для лиц старше 16 лет.


MONT
Group of companies
kaspersky

MONT предлагает своим партнёрам в безвозмездную аренду демо-фонд для проведения пилотов технологических решений «Лаборатории Касперского»:

- Kaspersky Anti Targeted Attack Platform (KATA)
- Kaspersky Endpoint Detection & Response (KERD)
- Kaspersky Industrial CyberSecurity (KICS)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Если вас заинтересовало наше предложение, напишите нам на kaspersky@mont.ru

MONT
Group of companies

positive
technologies

MONT оказывает всестороннее содействие своим партнёрам. Мы всегда готовы прийти на помощь, предоставив свой демо-центр и программно-аппаратные комплексы для реализации самых смелых проектов, а также услуги сертифицированных инженеров.

Мы проводим экспресс-обучение партнёров и заказчиков, решаем задачи интеграции и тестирования, реализуем пилотные проекты. Подтверждённая сертификатами инженерная экспертиза MONT – гарантия успешного освоения и использования решений Positive Technologies.

- PT Application Firewall
- MaxPatrol VM
- PT MultiScanner
- PT NAD
- PT Sandbox
- PT SIEM

Если вас заинтересовало наше предложение, напишите нам на positivetechnologies@mont.ru

MOUNT

Сетевая безопасность

Комплекс мер по организации эшелонированной (многоуровневой) защиты сети организации.

CIS / Спецвыпуск (24) / 2023 / www.cis.ru

Межсетевые экраны: UTM, NGFW-системы

Пока развивалась кибербезопасность, киберугрозы тоже не стояли на месте. Постепенно их количество настолько выросло, что компании оказались завалены массой ИТ-решений для защиты от потенциальных атак.

Среди таких решений были следующие устройства:

- межсетевой экран отслеживал качество соединений и фильтрации всего трафика;
- VPN-системы предоставляли дистанционный доступ к материалам компании для удалённой работы;
- система предотвращения вторжений (IDS/IPS) обеспечивала высокий уровень безопасности сети;
- веб-прокси гарантировал дополнительную защиту, фильтровал трафик и URL-адреса;
- спам-фильтр спасал от рекламных писем и вероятности фишинговых атак.

Отрасль активно защищалась от новых сложных угроз, но их количество постоянно росло. Управлять разрозненной системой защиты становилось всё сложнее, особенно в условиях быстрорастущего бизнеса. Требовался новый спаситель, который объединит в себе все ИТ-решения в одном продукте. И этим супергероем в мире кибербезопасности стали UTM.

Что такое UTM

UTM (Unified Threat Management) – универсальные шлюзы безопасности, которые защищают инфраструктуру от всех видов кибератак. Их отличием является многозадачность, так как UTM объединяет в себе функциональность VPN, межсетевого экрана, антивируса, спам- и контент-фильтра, систем защиты от вторжений. Универсальные шлюзы позволяют заменить десяток разрозненных программ.

Функциональность UTM

Многозадачность UTM позволяет бизнесу упростить управление ИТ-инфраструктурой и повысить общий уровень сетевой безопасности.

UTM могут:

- защищать трафик от разных типов атак и угроз;
- блокировать вирусы, подозрительные программы и рекламные продукты;
- предотвращать вторжения.

Почему появились NGFW-системы

Однажды стало понятно, что многозадачность, которая стала волшебной палочкой, в тот же момент доставила новые проблемы. Чем больше средств защиты было встроено в программу, тем медленнее она работала и даже тормозила.

Межсетевые экраны нового поколения NGFW решили эту проблему с помощью FPGA-чипов. Эти устройства работают параллельно друг другу с одинаковым трафиком, в отличие от UTM, которые закрывают задачи поочерёдно.

NGFW (Next-Generation Firewall) выполняет функции межсетевого экрана, систем защиты от фишинговых атак, глубокого анализа, фильтрации веб-трафика и электронной почты, а также разграничения прав доступа пользователей.

В последних поколениях межсетевых экранов производители постоянно улучшают обмен данных и взаимодействие с внешними ИТ-системами. В новых ИТ-продуктах задействованы машинное обучение, искусственный интеллект и средства автоматизации для быстрого реагирования на угрозы.

Исследователи выделили NGFW в отдельный вид из-за появившихся различий между классическими и новыми устройствами. Они посчитали, что UTM больше подходит для малого и среднего бизнеса, а NGFW – для крупных корпораций.

Функциональность NGFW

NGFW-системы могут:

- обнаруживать и блокировать угрозы на различных сетевых уровнях, а также отслеживать постороннее вмешательство;
- управлять политиками NAT и группами пользователей, фильтровать трафик;
- безопасно открывать заражённые файлы;
- сканировать трафик с помощью систем обнаружения и предотвращения вторжений;
- создавать единую базу данных с помощью удобного реестра.

Вендоры поставляют NGFW в качестве программного обеспечения для различных нужд и задач клиентов. Межсетевые экраны отличаются гибкостью и адаптивностью. Их можно использовать совместно с другими устройствами кибербезопасности. Существует не только программно-аппаратный NGFW, но и виртуальный.

Различия между UTM и NGFW

NGFW являются последствием развития UTM. Эти ИТ-решения различаются алгоритмом работы. В UTM трафик обрабатывается последовательно, тогда как в NGFW – параллельно. Вследствие этого скорость работы межсетевых экранов нового поколения гораздо быстрее, а их пропускная способность выше благодаря выделенной памяти для трафика.

Чтобы не нагружать процессор при выполнении задач NGFW, могут использоваться специальные аппаратные блоки под названием ASIC. Они значительно ускоряют и облегчают функционирование NGFW. При этом для каждой цели компании может быть предусмотрен свой ASIC.

Каждый из инструментов имеет свои достоинства, варианты использования и сферу деятельности. Их стоит использовать совместно друг с другом – это поможет увеличить эффективность киберзащиты.

CHECK POINT

Quantum – высокопроизводительные масштабируемые шлюзы безопасности для дата-центров и крупных корпораций, обеспечивающие наилучшее предотвращение угроз и оптимизацию для гибридных облачных сред. Шлюзы Quantum Security Gateways™ 26000 и 28000 Check Point включают отмеченное наградами решение предотвращения угроз SandBlast Network, обладают высокой надёжностью и имеют высокую скорость предотвращения угроз – до 1,5 Тбит/сек.

Если вас заинтересовало решение, обращайтесь по адресу checkpoint@mont.ru

ИНТЕРНЕТ КОНТРОЛЬ СЕРВЕР

Интернет Контроль Сервер (ИКС) – шлюз безопасности для защиты корпоративной сети и организации безопасного удалённого доступа. Контент-фильтр включает готовый набор правил для школ. Зарегистрирован в едином реестре российских программ для ЭВМ и БД, проходит сертификацию ФСТЭК.

Если вас заинтересовало решение, обращайтесь по адресу product@mont.ru

INFOWATCH

InfoWatch ARMA NGFW – межсетевой экран нового поколения, обладающий всеми основными возможностями, которыми пользовались заказчики западных аналогов, такими как application control, web proxy, SSL inspection, интеграция с Active Directory и др., и совместим с отечественным аппаратным обеспечением и ПО от основных российских разработчиков решений классов «песочницы», антивирусы, DLP, операционные системы. Варианты аппаратных платформ InfoWatch ARMA NGFW предусматривают разные параметры производительности, в т.ч. и подходящие под требования корпоративного сегмента. Система обнаружения и предотвращения вторжений (IPS/IDS) использует собственную базу сигнатур, постоянно пополняемую командой экспертов InfoWatch ARMA.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

SMART-SOFT

Универсальный шлюз безопасности (UTM) и система обнаружения (предотвращения) вторжений. Traffic Inspector Next Generation – программно-аппаратный сетевой шлюз нового поколения, включающий межсетевой экран для организации контролируемого доступа к интернету корпоративных компьютерных сетей и их защиты от внешних угроз. Относится к классу Unified Threat Management (UTM). Сделан на открытом коде проекта OPNsense. Traffic Inspector Next Generation обеспечивает фильтрацию на разных уровнях модели OSI и управление через веб-интерфейс по защищённому HTTPS-подключению, а также по протоколу SSH с использованием терминальной программы. Решение разворачивается в роли шлюза на границе корпоративной сети и позволяет контролировать информационные потоки между локальной сетью и Интернетом.

С вопросами обращайтесь по адресу smart-soft@mont.ru

UserGate

Семейство программно-аппаратных и виртуальных комплексов User Gate обеспечивает безопасность сетей как небольших организаций, так и больших корпоративных сетей и дата-центров, обладая высокой производительностью, возможностью масштабирования, позволяет осуществлять дешифрацию трафика (включая TLS 1.3 и TLS GOST) и его глубокий анализ.

Если вас заинтересовало решение, обращайтесь по адресу usergate@mont.ru

Эшелон
комплексная безопасность

«Рубикон» – программно-аппаратный комплекс выполняет функции маршрутизатора, межсетевого экрана и системы обнаружения вторжений. Предназначен для использования в системах ГИС, ИСПДН и для защиты информации, содержащей сведения, составляющие государственную тайну.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

ideco

«Шлюз Безопасности Ideco UTM» – флагманский продукт компании «Айдеко» российского производителя программных продуктов Ideco для построения сетей и развития сетевых инфраструктур любого уровня сложности. Это современное решение, основанное на ядре Linux и включающее в себя межсетевой экран, VPN-сервер, контроль приложений, контент-фильтрацию, защиту от вторжений.

По вопросам, связанным с решениями Ideco, обращайтесь по адресу infoprotect@mont.ru

SkyDNS

Чуть в стороне от стандартной реализации NGFW стоит решение SkyDNS – интернет-фильтр для мониторинга интернет-активности внутри компании, онлайн-безопасности рабочих станций и серверов, ограничения доступа к интернет-ресурсам, не относящимся к рабочим процессам. Он удобен в управлении и предоставляется в виде облачного сервиса или программно-аппаратного комплекса. Кроме бизнес-редакции, предлагаются варианты продукта для домашнего использования и для образовательных учреждений.

Если вас заинтересовало решение, обращайтесь по адресу product@mont.ru

Ростелеком Солар

Solar webProxy – шлюз веб-безопасности (Secure Web Gateway, SWG) для контроля доступа сотрудников и приложений к веб-ресурсам и защиты веб-трафика от вредоносного ПО и навязчивой рекламы. Гибко разграничивает доступ к веб-ресурсам, приложениям и файлам, защищает от заражённых и фишинговых сайтов, блокирует утечки через веб-канал.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

КОД безопасности

«Континент 4» – многофункциональный межсетевой экран (NGFW/UTM) с поддержкой алгоритмов ГОСТ. Система обнаружения и предотвращения вторжений может работать в «невидимом» для сети режиме, детально настраивается и активируется только для необходимого трафика. Система контроля приложений работает на основе базы более 2600 приложений. Механизм поведенческого анализа трафика не использует сигнатуры, а построен на основе механизмов машинного обучения, он позволяет обнаруживать злоумышленника и предотвращать DoS-атаки.

Модельный ряд «Континент 4» позволяет подобрать решение для защиты как больших корпоративных сетей, так и небольших организаций. Различаясь производительностью, все аппаратные исполнения обладают полным функционалом защитных механизмов, реализованных в «Континент 4».

По вопросам, связанным с решениями «Код Безопасности», обращайтесь по адресу kb@mont.ru

ФАКТОР-ТС

Dionis DPS – линейка отечественных маршрутизаторов и криптомаршрутизаторов, сертифицированная по требованиям ФСТЭК и ФСБ России, и соответствующая самым высоким уровням защищённости. Dionis DPS ориентирована как на коммерческий сектор, так и на государственные ведомства и уже используется для организации безопасного информационного обмена во всех министерствах и ведомствах силового блока России, а также в других государственных учреждениях.

Если вас заинтересовало решение, обращайтесь по адресу factor@mont.ru

CIS / Спецвыпуск (24) / 2023 / www.cis.ru

Межсетевой экран для веб-приложений

С появлением HTML 5 начали активно развиваться веб-приложения. Они привлекли к себе внимание благодаря расширенным возможностям по сравнению с классическим HTML-кодом и разнообразному дизайну.

Кроме того, веб-приложения не нужно устанавливать на компьютер или смартфон пользователя, они подходят под любую операционную систему. 2022 год отличился ростом кибератак на веб-ресурсы. Их доля увеличилась с 13% до 22% от общего количества атак на организации. Один из самых эффективных способов защитить свою ИТ-инфраструктуру от внешних угроз – это Web Application Firewall (WAF).

Что такое WAF

Web Application Firewall (WAF) – межсетевой экран для защиты веб-приложений от потенциальных угроз. Это узкоспециализированное решение, так как устройство отличается от NGFW, обычного файрвола или IPS, которые ориентированы на многопротокольные устройства. WAF же специализируется конкретно на протоколах по типу строения http/https.

Благодаря глубокому анализу этот ИТ-продукт имеет более высокую эффективность в сравнении с другими средствами защиты от кибератак. При этом WAF «знает», какие приложения он защищает. Именно поэтому он выделен в отдельный вид устройств, так как это совершенно новый уровень развития межсетевых экранов.

Сферы применения

Самыми привлекательными сферами для хакеров являются ритейл, ИТ-компании и государственные организации. Все они активно используют веб-приложения и хранят большие объёмы личных данных пользователей. Именно поэтому злоумышленники так любят покушаться на их ИТ-инфраструктуры.

WAF используется в различных форматах: виртуальное или аппаратное устройство, облачный сервис, программное обеспечение. Малые и средние организации предпочитают облачные ИТ-продукты, а крупные корпорации покупают отдельные устройства. Несмотря на узкопрофильность WAF, у каждого производителя отличается подход к цифровой защите. Поэтому от правильности выбора продукта зависит его эффективность. При этом важно учитывать варианты взаимодействия с другими инструментами информационной безопасности.

Что умеет WAF

- защищать веб-приложения, связанные с PCI DSS Requirements;
- оперативно реагировать на самые популярные виды атак;
- сканировать веб-трафик и выявлять потенциальные угрозы;
- анализировать веб-уведомления (SOAP, XML, RPC);
- сканировать SSL- и TSL-трафик.

Преимуществом WAF является способность к самообучению. Устройство создаёт «белый алгоритм» работы пользователя с веб-приложениями. Благодаря этому программе удаётся отсеивать 98% различных атак, с которыми UTM, IDS/IPS и обычные прокси не справляются.

У WAF есть доступ к виртуальному патчингу. Это помогает защитить систему от ещё неизвестных для разработчиков взломов. Для этого используется анализ исходного кода приложения. При этом WAF может быть интегрирован с решениями анализа исходного кода, что позволяет найти ошибки в работе самого приложения. В этом случае, благодаря связке статического и динамического сканеров, WAF может применять виртуальный патчинг, в ручном или автоматическом режиме создавать новые правила в Firewall, которые позволяют предотвращать ошибки «нулевого дня».

Как будет развиваться Web Application Firewall в будущем

Пандемия и карантин сделали онлайн частью нашей жизни, что укрепило популярность WAF. Эксперты считают, что ИТ-рынок расколется на два лагеря: уже готовые продукты и персональные решения для отдельных бизнес-задач.

Коробочное программное обеспечение – перспективное направление, ведь компаниям проще купить готовый продукт, нежели нанимать отдельных специалистов для контроля безопасности веб-приложений. Оставшаяся часть производителей будет ориентироваться на тех потребителей, которые предпочитают дополнительные средства защиты с фокусом на необходимые им функции.

Несложно догадаться, что ИИ и машинное обучение станут частью файрвола веб-приложений и появятся новые методы выявления неизвестных угроз. Также будут развиваться интеграция и активное внедрение Web Application Firewall в облачный бизнес.

Выбор между брандмауэром для приложений и межсетевым экраном

Стандартные межсетевые экраны и WAF защищают от разных типов угроз, поэтому важно выбрать тот, который подходит вашему бизнесу. Один межсетевой экран не защитит предприятие от атак на веб-страницы, которые можно предотвратить только с помощью возможностей WAF. В то же время без брандмауэра для приложений ваша сеть всё ещё находится под угрозой. Но WAF не может защитить от атак на сетевом уровне, поэтому он должен дополнять межсетевой экран, а не заменять его. То есть мы видим, что для эффективной защиты информационной безопасности данные инструменты рекомендуется использовать комплексно. Ведь они работают

на разных уровнях и защищают от разных типов трафика. Они не конкурируют, а лишь дополняют друг друга.

Вместо того, чтобы выбирать одно или другое, лучше сосредоточиться на том, чтобы подобрать подходящую систему WAF, которая будет наилучшим образом отвечать потребностям бизнеса. WAF должен иметь аппаратный ускоритель, контролировать трафик и блокировать вредоносные попытки, быть высокодоступным и масштабируемым для поддержания производительности по мере роста вашего предприятия.

---

positive technologies

PT Application Firewall – межсетевой экран уровня веб-приложений (web application firewall) компании Positive Technologies. Предназначен для защиты веб-ресурсов организации от известных и неизвестных атак, включая OWASP Top 10, автоматизированных атак, атак на стороне клиента и атак «нулевого дня». Решение основано на передовых технологиях и регулярных исследованиях экспертов, чтобы обеспечить высочайший уровень безопасности и непрерывность бизнес-процессов организации.

Если вас заинтересовало решение, обращайтесь по адресу pt@mont.ru

---

КОД безопасности

«Континент WAF» – многоуровневая система проверки трафика, блокирующая широкий спектр атак на веб-приложения и предотвращающая хищение баз данных, размещение на сайте вредоносного ПО и внесение в контент сайта несанкционированных изменений.

По вопросам, связанным с решениями «Код Безопасности», обращайтесь по адресу kb@mont.ru

---

ideco

«Шлюз Безопасности Ideco UTM» – флагманский продукт компании «Айдеко» российского производителя программных продуктов Ideco для построения сетей и развития сетевых инфраструктур любого уровня сложности. Это современное решение, основанное на ядре Linux и включающее в себя межсетевой экран, VPN-сервер, контроль приложений, контент-фильтрацию, защиту от вторжений, а также модуль WAF.

По вопросам, связанным с решениями Ideco, обращайтесь по адресу infoprotect@mont.ru

---

CHECK POINT

Quantum – высокопроизводительные масштабируемые шлюзы безопасности для дата-центров и крупных корпораций, обеспечивающие наилучшее предотвращение угроз и оптимизацию для гибридных облачных сред. Шлюзы Quantum Security Gateways™ 26000 и 28000 Check Point включают отмеченное наградами решение предотвращения угроз SandBlast Network, обладают высокой надёжностью и имеют высокую скорость предотвращения угроз – до 1,5 Тбит/сек.

Если вас заинтересовало решение, обращайтесь по адресу checkpoint@mont.ru

DDoS-атаки – наша новая реальность

Из-за политической напряжённости в мире с конца февраля прошлого года и по нынешний день российские интернет-ресурсы оказались под прицелом сильных и продолжительных DDoS-атак. При этом в зоне риска оказался не только бизнес, но и инфраструктуры государственных учреждений, банков, СМИ, образовательных, медицинских и других организаций.

С 2022 года DDoS-атаки стали самым популярным инструментом информационной войны. Их масштаб и сила влияния вызывают беспокойство у экспертов в области. В связи с этим проблема информационной безопасности в России выходит на первый план и становится приоритетной задачей, на борьбу с которой должны быть брошены все силы.

Что такое DDoS-атака

Главная цель DoS-атаки – нарушить нормальную работоспособность интернет-ресурса. Для этого хакеры пытаются перегрузить сервер искусственным потоком запросов. Например, злоумышленники могут попытаться вывести из строя оперативную память сервера, который отвечает за логику приложения, или ширину канала подключения атакуемой системы к сети и так далее.

DoS-атакам могут подвергаться не только интернет-ресурсы, но даже номера телефонов. Так, из-за спам-звонков обычные пользователи не смогут дозвониться до организации, что может привести к потере клиентов.

DoS-атака бывает как искусственная, так и естественная. Вторая происходит в результате сбоя отдельных узлов или неправильного планирования ресурсов в составе системы. Чаще всего это случается, когда перегружается трафик.

Как распознать, что ваша система атакуется

Атака удалась, если ваш сервер стал недоступен для клиентов. Как же распознать её начало?

- Наблюдаются повторяющиеся сбои в работе серверного программного обеспечения и оперативной системы.
- Резко перегружаются аппаратные мощности сервера.
- Происходит скачок входящего трафика.
- Одинаковые действия пользователей ресурса неоднократно повторяются.
- Увеличивается трафик от пользователей, не входящих в вашу целевую аудиторию.

Как защититься от DDoS-атак

За последние месяцы многие отечественные компании поняли, что больше невозможно работать без эффективной DDoS-защиты. Даже те, кто раньше был неинтересен злоумышленникам, становятся наживкой для мошенников лишь потому, что они являются российскими организациями. К тому же DDoS-атаки активно развиваются, а по стоимости они стали доступны даже школьникам.

Если у вашей компании ещё нет защиты от DDoS-атак, в ваших интересах её подключить. Но даже этого может быть недостаточно для информационной безопасности системы. Нужно добиться того, чтобы ваша ИТ-инфраструктура приобрела «иммунитет» к DDoS-атакам.

Уделите внимание правильному подбору проверенного и профессионального провайдера, который будет решать проблему на своей стороне.

При возможности используйте несколько интернет-провайдеров, где при магистральной атаке на одного, будет возможность переключить трафик на другого поставщика.

Архитектор по кибербезопасности SberCloud:

«У вас может быть установлена самая безопасная информационная система, самые современные и эффективные средства защиты и устранены все уязвимости кода. Несмотря на это, ваша информационная система не будет работать и не будет доступна для пользователей всё то время, пока она находится под атакой. При этом стоимость затрат злоумышленников на проведение такой атаки может быть существенно меньше того репутационного риска и опасности потерять клиентов, доходы, рынок, которые несёт владелец атакуемой системы. Стоимость использования защитных мер для противодействия DDoS-атакам существенно ниже потерь бизнеса от реализации этих атак».

Защита электронной почты

От 85 до 90% кибератак происходит именно через почту, так как через неё можно легко получить доступ к другим учётным записям и устройствам. К тому же важную роль составляет человеческий фактор. Стоит вам перейти не по той ссылке, как ваша корпоративная ИТ-инфраструктура окажется в опытных руках киберпреступников.

Защита электронной почты предотвращает нелегальный доступ со стороны злоумышленников к учётным записям и сообщениям электронной почты, а также помогает избежать утрату корпоративных данных или их использование в корыстных целях.

Почему важно защищать электронную почту

В наше время электронная почта – главный инструмент корпоративной коммуникации. Ежедневно каждый сотрудник получает более сотни писем, и любое из них может стать роковым для информационной безопасности компании. Киберпреступники преследуют одну цель: украсть ценные корпоративные данные с помощью взлома рабочей почты. 95% кибератак начинаются с вредоносного содержания письма. За последние 5 лет в ходе атак на деловые почты было похищено около $43 млрд, по данным Internet Crime Complaint Center и IC3.

Как поможет бизнесу киберзащита электронной почты:

- снижаются риски серьёзных финансовых и репутационных потерь;
- возможность минимизировать простои в работе из-за кибервмешательства и оптимизировать систему реагирования на самые изощрённые атаки;
- соблюдение законов о защите данных, что поможет избежать крупных штрафов, судебных разбирательств и расходов.

Какие методы используют мошенники для взлома электронной почты

Кибермошенники постоянно совершенствуют методы атак. Приведём некоторые из них.

Кража данных – это незаконная передача корпоративной информации за пределы компании. Она происходит вручную или с помощью «заражённых» программ. Утечка конфиденциальных данных может дорого обойтись организации. Избежать отправки этой информации без авторизации помогут шлюзы безопасности электронной почты.

Вредоносные программы

Их основная цель – нарушить нормальную работоспособность ПК и информационных систем компании. Вредоносные программы бывают разных видов: вирусы, черви, шантажисты и шпионы.

Спам

Это нежелательные письма, которые массово рассылаются без согласия получателя. Спам не обязательно распространяется мошенниками. Он может использоваться компаниями в коммерческих целях. Но нередко злоумышленники с помощью спама пытаются заразить ИТ-систему компании, чтобы вымогать деньги или украсть ценную информацию.

Фишинг

При фишинге мошенники от имени бренда, банка или любой другой организации рассылают письма на электронную почту. В письме часто содержится ссылка на сайт, внешне не вызывающая подозрений и похожая на настоящую. Но при переходе по ссылке злоумышленники получают доступ к паролям, логинам и другим конфиденциальным данным жертвы.

Один из методов похитить данные через электронную почту – это притвориться сотрудником компании и вынудить обманным путём у партнёров или коллег необходимую информацию.

Как защитить корпоративную почту

Мы ответили на вопрос, почему важно защищать корпоративную почту, а теперь разберём, как это сделать. Чтобы ваши сотрудники работали в безопасной среде, необходимо предпринять ряд мер:

- Регулярно обучайте персонал основам информационной безопасности, так как спецификой атак на электронную почту выступает человеческая слабость и доверчивость. Вкладывайте средства в обучение персонала, чтобы пользователи умели разоблачать попытки фишинговых атак и других обманных методов взлома.
- Подберите правильное ИТ-решение для защиты корпоративной почты с расширенным функционалом и эффективными возможностями информационной безопасности.
- Используйте многофакторную идентификацию для входа в аккаунт, чтобы избежать кражу важных данных компании.
- Проверьте, насколько ваша защита электронной почты способна предотвратить компрометацию с применением спуфинга.
- Если у вас есть процессы и операции с высоким уровнем риска, переведите их на более высокий уровень проверки подлинности.

Используйте различные средства защиты электронной почты: функции отключения, шифрование данных, средства контроля, спам-фильтры, системы аутентификации. Надёжная система защиты – залог успешной работы вашего бизнеса.

CHECK POINT

Quantum – высокопроизводительные масштабируемые шлюзы безопасности для дата-центров и крупных корпораций, обеспечивающие наилучшее предотвращение угроз и оптимизацию для гибридных облачных сред. Шлюзы Quantum Security Gateways™ 26000 и 28000 Check Point включают отмеченное наградами решение предотвращения угроз SandBlast Network, обладают высокой надёжностью и имеют высокую скорость предотвращения угроз – до 1,5 Тбит/сек.

Harmony Email & Collaboration обеспечивает защиту электронной почты и облачного офиса для совместной работы: Microsoft 365, Google Workspace и всех приложений для сотрудничества и обмена файлами.

Если вас заинтересовало решение, обращайтесь по адресу checkpoint@mont.ru

---

Dr.WEB

Dr. Web Mail Security Suite – высокоинтеллектуальная система антивирусной и антиспам-обработки больших потоков сообщений. Предлагается в редакциях для Unix, MS Exchange, IBM Lotus Domino и Kerio. Сертифицирован ФСТЭК России*.

Если вас заинтересовало решение, обращайтесь по адресу drweb_request@mont.ru

---

kaspersky

Kaspersky Security для почтовых серверов обеспечивает их защиту на платформах Exchange, Linux, осуществляя функции антиспама и почтового антивируса.

Kaspersky Security for Microsoft Office 365 – облачный продукт для защиты почтового компонента Exchange Online решения Microsoft Office 365.

Если вас заинтересовали решения, обращайтесь по адресу lk@mont.ru

---

F.A.C.C.T.

Business Email Protection – единое решение для обнаружения, блокировки и анализа всех распространяемых через почту угроз – от спама и фишинга до ВПО и BEC-атак. Настраиваемый дашборд позволяет быстро отслеживать общий уровень защищённости электронной почты вашей организации, а продвинутые инструменты аналитики дают возможность детально изучать угрозы. Продукт автоматически обнаруживает и блокирует вредоносные письма. Благодаря технологиям ретроспективного анализа решение реклассифицирует объекты и ссылки, которые стали вредоносными спустя какое-то время, и удаляет их из входящей почты.

Если вас заинтересовало решение, обращайтесь по адресу gib@mont.ru

---

UserGate

Семейство программно-аппаратных комплексов User Gate, а также программное решение UserGate Virtual Appliance позволяют обеспечивать безопасность сетей как маленьких организаций, так и больших корпоративных сетей и дата-центров, обеспечивая высокую производительность, возможности масштабирования, осуществлять дешифрацию и глубокий анализ трафика. Дополнительный модуль Mail Security обеспечивает фильтрацию спама и защиту пользователей от угроз, связанных с получением писем вредоносными вложениями, а также от фишинга, фарминга и прочих видов мошенничества.

Если вас заинтересовало решение, обращайтесь по адресу usergate@mont.ru

---

ФАКТОР-ТС

Diopost – почтовый клиент с возможностями шифрования и электронной подписи писем. Имеет в своём составе СКЗИ класса КС3.

Если вас заинтересовало решение, обращайтесь по адресу factor@mont.ru

«Песочница» для вашего бизнеса

Чтобы защитить компанию от целевых и массовых атак с применением вредоносного ПО и угроз «нулевого дня», необходим специальный класс решений – «песочницы».

Sandbox – это решение, которое запускает файл в изолированной виртуальной среде, анализирует, какие действия в системе он совершает, и выдаёт вердикт о том, безопасен этот файл или нет.

Почему «Песочница» так популярна в наши дни

Представьте: вам на почту пришло письмо с вложенным файлом «Отчёты. doc. exe». С вероятностью 80% его содержание окажется вредоносным и нанесёт ущерб системе компании. Дело в том, что многие программы имеют специальные форматы файлов: у Microsoft Office Word – это.doc и.docx и ещё целый ряд дополнительных вариантов расширений, в которых можно сохранить документ. Вы можете и не догадываться, что злоумышленник с помощью такого файла попытается получить доступ к вашему компьютеру. Он может закинуть вирус в картинку или убрать формат файла вовсе. Чтобы обезопасить бизнес от таких неприятных происшествий, вы можете обратиться к Sandbox.

Для чего нужна «Песочница»

«Песочница» изолирует непроверенные изменения в коде или предотвращает последствия запуска стороннего ПО так, что они не угрожают безопасности данных или локальных файлов системы.

Многие браузеры наподобие Chrome, Firefox и Edge по умолчанию имеют встроенную «песочницу». Если вы скачаете вредоносный объект с веб-ресурса, он загрузится в «песочницу браузера». Дальнейшая его судьба проста: после закрытия «песочницы» её содержимое беспощадно стирается, в том числе зловредный код. Sandbox работает по принципу одного источника. Благодаря этому JavaScript может добавлять или изменять элементы на веб-странице с ограниченным доступом к внешнему файлу JSON.

Sandbox помогает специалистам безопасно «взорвать» код, чтобы выяснить, как он работает и насколько безопасен.

При тестировании разработчики опираются на следующие признаки:

- самостоятельно ли реплицируется код;
- пытается ли связаться с командно-контрольным сервером;
- загружает ли дополнительное программное обеспечение;
- шифрует ли конфиденциальные данные и т. д.

Также Sandbox может быть полезна при запуске кода перед массовым развёртыванием. «Песочницы» просто незаменимы для бизнеса, ведь без изолированной и безопасной среды рискованно исследовать кибербезопасность инфраструктуры. Это может привести к серьёзным последствиям, так как вредоносные программы активно сканируют корпоративные сети на открывшиеся уязвимости.

Где можно использовать «песочницу»:

- **для защиты почты;**
- **в файловых хранилищах;**
- **на веб-порталах, где загружаются файлы;**
- **в пользовательском трафике.**

Что можно сделать в среде «песочницы»

1. «Взорвать» код и проанализировать его в работе.
2. Запустить и проверить файлы и другие скрытые заражённые программы.
3. Следить за сетевым трафиком.
4. Безопасно протестировать вредоносный код или операции с диском.
5. Безопасно изменять реестры, систему, конфигурацию и т. п.

positive technologies

PT Sandbox – «песочница», которая позволяет защитить компанию от целевых и массовых атак с применением современного вредоносного ПО. Поддерживает гибкую настройку виртуальных сред для анализа в соответствии с реальными рабочими станциями. Обнаруживает угрозы не только в файлах, но и в трафике, в том числе зашифрованном.

Если вас заинтересовало решение, обращайтесь по адресу pt@mont.ru

kaspersky

Kaspersky Sandbox – автоматически защищает компании (от 250 узлов) от продвинутых угроз, способных обходить базовую защиту серверов и рабочих станций. Решение тесно интегрировано с Kaspersky Security для бизнеса и помогает повышать уровень защищённости рабочих мест и серверов от ранее неизвестного вредоносного ПО, программ-вымогателей, эксплойтов «нулевого дня» и других сложных угроз, без привлечения ИБ-аналитиков и хорошо подготовленного ИБ-отдела. Расширенная функциональность «песочницы» доступна в решении Kaspersky Anti Targeted Attach Platform (KATA).

Если вас заинтересовало решение, обращайтесь по адресу lk@mont.ru

CHECK POINT

SandBlast Network – комплексное решение для предотвращения сетевых угроз. Оно обнаруживает вредоносное ПО и гарантирует, что контент внутри сети вашей организации безопасен для использования, тем самым значительно увеличивая производительность пользователей.

Если вас заинтересовало решение, обращайтесь по адресу checkpoint@mont.ru

F.A.C.C.T.

Managed Extended Detection and Response (Managed XDR) предназначен для нейтрализации постоянно усложняющихся угроз, проактивный поиск недетектируемых угроз в инфраструктуре, противодействие атакам в режиме реального времени и максимально быстрое реагирование в случае инцидента. В состав решения входит компонент MDP (Malware Detonation Platform) – платформа детонации вредоносных программ, которая запускает подозрительные файлы и ссылки в виртуальной среде для углублённого анализа, обнаружения угроз, извлечения индикаторов и атрибуции атак.

Если вас заинтересовало решение, обращайтесь по адресу gib@mont.ru

Dr.WEB

Dr. Web vxCube – интеллектуальная удалённая онлайн-проверка подозрительных объектов на вредоносность путём воспроизведения их поведения в изолированной виртуальной среде. Предлагается в двух вариантах: в виде облачного сервиса на серверах вендора и в виде ПАК для установки в инфраструктуре заказчика.

Если вас заинтересовало решение, обращайтесь по адресу drweb_request@mont.ru

ANY RUN

INTERACTIVE MALWARE ANALYSIS

Interactive malware Hunting service – облачный сервис для анализа вредоносных программ

Если вас заинтересовало решение, обращайтесь по адресу any.run@mont.ru

Что такое network traffic analysis и зачем нужны NTA-системы

К сожалению, злоумышленники могут проникнуть внутрь корпоративной сети и их действия останутся незамеченными для периметровых средств защиты. Они могут действовать внутри организации долгое время.

Специалисты PT Expert Security Center зафиксировали рекорд продолжительности такого проникновения – длиной более 8 лет.

Чтобы не позволить хакеру развивать атаку внутри сети, можно анализировать трафик с помощью NTA-систем.

Что такое network traffic analysis

Системы анализа трафика (network traffic analysis, NTA) исследуют сеть, чтобы выявить в ней угрозы возникновения кибератак. Они помогают обнаружить вторжение на первоначальной стадии, оперативно ликвидировать угрозы и соблюдать регламенты информационной безопасности.

Чем отличается NTA-системы от аналогичных решений

NTA-системы анализируют трафик не только на периметре устройства, но и во всей инфраструктуре. Это позволяет заметить злоумышленника и его действия, в то время как межсетевые экраны могут не распознать опасного вторжения.

NTA-системы функционируют на основе сразу нескольких инструментов: машинное обучение, поведенческий и ретроспективный анализы, правила детектирования, индикаторы компрометации. Синергия этих методов повышает эффективность NTA-систем и помогает им обнаружить атаку на ранних стадиях.

Традиционные средства безопасности бессильны в расследовании инцидентов и в threat hunting, в отличие от NTA. NTA-системы хранят информацию обо всех сетевых действиях, а иногда ещё и записывают сырой трафик. Эти данные будут бесценны при анализе алгоритма атаки и её локализации, а также при проверке гипотез в рамках threat hunting.

Аналитическое агентство Gartner включило NTA вместе с системами SIEM и EDR в топ-3 средств для SOC, которые в синергии значительно снижают шансы атакующих на достижение целей в инфраструктуре жертвы. По версии Института SANS, решения NTA входят в топ технологий для выявления угроз, работой которых довольны в SOC по всему миру.

Варианты использования NTA

Возможности NTA не заканчиваются на выявлении атак. Такие системы позволяют отследить алгоритм атаки, чтобы остановить вторжение в инфраструктуру компании. Например, если вы обнаружили попытку взлома, можно обратиться к истории сетевой активности узла и проверить, не было ли подобных кибератак. Если обнаружатся и другие подозрительные действия, то это будет означать, что кто-то целенаправленно пытается взломать вашу систему.

В рамках threat hunting NTA-инструменты могут проверять гипотезы о компрометации сети. Например, ИБ-специалист подозревает, что хакеры проникли в систему компании. Чтобы проверить догадку, он анализирует сетевую активность доменной инфраструктуры, ведь, чтобы развить атаку, злоумышленник должен провести разведку в AD. Если среди подключений обнаружатся нелегальные запросы, значит, подозрения оправдаются – потребуется детальное расследование.

Ещё одно преимущество NTA – это возможность контролировать, насколько соблюдаются регламенты информационной безопасности. В 90% организаций пароли передаются в открытом виде, происходят ошибки конфигурации сети, используются утилиты для удалённого доступа и инструменты сокрытия активности. Всё это только облегчает задачу киберпреступников.

NTA-системы умеют распознавать более 100 сетевых протоколов, несколько десятков из них разбирает на уровне приложений. Благодаря этому оператор сети видит полную картину происходящего и может отследить все данные, переданные в открытом виде. Таким образом он сможет скорректировать ситуацию, ведь специалист видит адреса узлов-отправителей и получателей, а также конкретные сессии по передаче данных.

На сегодняшний день решения класса NTA постоянно совершенствуются. На российском рынке тоже есть высокотехнологичные решения. NTA-системы имеют растущий спрос среди отечественных компаний.

kaspersky

Kaspersky Anti Targeted Attack – комплексное решение для борьбы с продвинутыми угрозами, такими как атаки «нулевого дня» и целевые атаки Advanced Persistent Threats (APT). Специалисты по ИТ-безопасности получают в едином решении все инструменты, которые позволяют выявлять угрозы на разных уровнях развития целевой атаки, проводить эффективные расследования и проактивный поиск угроз, а также оперативно и централизованно реагировать на инциденты.

Если вас заинтересовало решение, обращайтесь по адресу lk@mont.ru

F.A.C.C.T.

Managed Extended Detection and Response (Managed XDR) – нейтрализация постоянно усложняющихся угроз, проактивный поиск недетектируемых угроз в вашей инфраструктуре, противодействие атакам в режиме реального времени и максимально быстрое реагирование в случае инцидента. Один из компонентов системы предназначен для анализа сетевого трафика (NTA) – выявление вредоносной активности, аномалий и скрытых каналов в сетевом трафике, а также анализ и атрибуция угроз.

Если вас заинтересовало решение, обращайтесь по адресу gib@mont.ru

positive technologies

PT Network Attack Discovery – система глубокого анализа сетевого трафика для выявления атак на периметре и внутри сети. PT NAD знает, что происходит в сети, обнаруживает активность злоумышленников даже в зашифрованном трафике и помогает в расследованиях.

Если вас заинтересовало решение, обращайтесь по адресу pt@mont.ru

CIS / Спецвыпуск (24) / 2023 / www.cis.ru

Латаем дыры: что такое сканер уязвимостей

Чтобы ваш бизнес успешно работал, нужно следить за появлением уязвимостей в ИТ-системе. Искать «дыры» можно вручную, но даже для опытных специалистов, имеющих редкое чутьё, это трудоёмкий и долгий процесс. Чтобы облегчить жизнь ИТ-специалистам, разработчики создали автоматизированные сканеры уязвимостей.

Что такое сканер уязвимостей

Это программное или аппаратное решение для диагностики сети с целью обнаружить и устранить уязвимости и потенциальные риски информационной безопасности.

После того как «дыры» в системе найдены, администратор пытается закрыть их и защитить конфиденциальные данные от атаки хакеров.

Что умеют сканеры:

- искать и анализировать уязвимости и ошибки конфигурации в режиме реального времени;
- проверять на безопасность сетевые ресурсы, операционные системы и подключённые устройства;
- сканировать все активные процессы и запущенные приложения;
- отчитываться о типе уязвимости.

Так как большинство современных сканеров – кроссплатформенные, они могут поддерживать различные операционные системы. К тому же они проверяют не только ОС, но и все информационные ресурсы компании. При анализе уязвимостей сканеры сосредотачиваются на популярных в хакерской среде продуктах и браузерах. Некоторые решения диагностируют несколько портов одновременно, за счёт чего сокращают время на поиск «дыр». Также они экономят время администраторов на анализе каждого узла, проверяя раздробленную сеть.

Вы можете настраивать сканеры под потребности сети. Например, у вас есть возможность выбрать перечень анализируемых устройств и типов уязвимостей, указать разрешённые для автоматического обновления приложения, установить частоту проверок и отчётов.

У некоторых сканеров есть чудо-функция – возможность провести анализ «исторических» данных. Благодаря ей можно оценить, когда именно была нарушена безопасность узла и таким образом индивидуально настроить ПО.

Как работает сканер уязвимостей

У сканера есть два метода функционирования: сканирование или зондирование. Разберём каждый из них.

Зондирование – самый эффективный инструмент, но он занимает больше времени, чем сканирование. При зондировании утилита имитирует хакерскую атаку, чтобы проследить за реакцией сети. В это время администратор проверяет догадки относительно уязвимостей и пытается их устранить.

Сканирование – максимально быстрый способ поиска уязвимостей. Но анализ в этом случае проводится на поверхностном уровне, то есть решение проверяет лишь «очевидные» дефекты инфраструктуры. При этом сканирование не подтверждает наличие «дыры», а лишь предупреждает о ней специалиста. В этом главное отличие одного способа анализа от другого.

Важно понимать, что сканер ищет косвенные признаки уязвимостей. Если он начнёт анализировать API, то определит параметры и будет сравнивать их со значениями, которые задал администратор. Если будут найдены расхождения, то сканер уведомит о потенциальном дефекте в системе.

Российский рынок сканеров уязвимостей

В российских нормативных актах (приказы ФСТЭК России № 17, № 21, № 239, № 31, постановление Правительства РФ № 79 и т.д.) прописано, что заказчики должны обязательно иметь сканер уязвимостей, а сам продукт должен обладать сертификатом по требованиям безопасности ФСТЭК России.

Российские сканеры, в отличие от зарубежных, дополнительно могут искать уязвимости из Банка данных угроз безопасности информации ФСТЭК России, проверять некоторые средства защиты и не могут поставляться в качестве облачного сервиса. Практически все отечественные вендоры продают только коммерческие версии своих продуктов.

Некоторые сканеры уязвимостей позволяют проводить проверки на соответствие требованиям PCI DSS и других иностранных нормативных актов. Российские производители предлагают свои решения в основном в локальном виде (on-premise) для установки в инфраструктуре заказчика.

Если регулярно использовать сканеры уязвимостей, то можно не беспокоиться за безопасность своей инфраструктуры. Эти средства защиты стремительно развиваются и постепенно превратятся в более масштабные системы защиты, решающие большее количество задач.

positive technologies

XSpider – профессиональный сканер уязвимостей, позволяющий оценить реальное состояние защищённости ИТ-инфраструктуры. Решение быстро и точно определяет компоненты сети, сканирует сетевые ресурсы на наличие уязвимостей и выдаёт рекомендации по их устранению.

MaxPatrol VM – система управления уязвимостями нового поколения. Решение позволяет выстроить полноценный процесс vulnerability management и контролировать его как в штатном режиме, так и при экстренных проверках. В его основе лежит уникальная технология управления активами Security Asset Management (SAM), которая позволяет с помощью активного и пассивного сбора данных строить в каждый момент времени актуальную и полную модель наблюдаемой ИТ-инфраструктуры.

PT BlackBox – это сканер безопасности приложений, работающий методом чёрного ящика. Даёт рекомендации по устранению проблем. Упрощает работу специалистов R&D.

Если вас заинтересовало решение, обращайтесь по адресу pt@mont.ru

ALTEX SOFT

RedCheck – комплексный продукт для проведения анализа защищённости и управления информационной безопасностью. Обеспечивает поиск и устранение уязвимостей, вызванных ошибками в коде, неверными настройками параметров безопасности, слабостью парольной защиты, несанкционированной установкой программного и аппаратного обеспечения, несвоевременной установкой критичных обновлений и нарушением принятых политик безопасности.

RedCheck имеет действующий сертификат ФСТЭК, который подтверждает соответствие средствам контроля (анализа) защищённости и требованиям РД по 4-му уровню доверия.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

kaspersky

Kaspersky Security Center упрощает управление безопасностью и ИТ-системами. Сбор информации о программном и аппаратном обеспечении и своевременная установка исправлений уязвимостей отнимают много времени и сил. С Kaspersky Security Center физические, виртуальные и облачные рабочие места, мобильные устройства и встраиваемые системы управляются из единой консоли, доступной в том числе в виде веб-версии, что повышает эффективность, облегчает распределение обязанностей между администраторами и уменьшает совокупную стоимость эксплуатации ИТ-системы.

Если вас заинтересовало решение, обращайтесь по адресу lk@mont.ru

Эшелон
комплексная безопасность

«Сканер-ВС» – универсальный инструмент для решения широкого спектра задач по тестированию, анализу защищённости и контролю эффективности систем и средств защиты информации.

Сертифицированный программный комплекс, включающий систему тестирования защищённости «Сканер-ВС» и средство проведения комплексных проверок «Инспектор», предназначен для анализа уязвимостей в программном обеспечении и в автоматизированных системах, контроля эффективности применения средств защиты информации, формирования и контроля полномочий доступа в автоматизированных системах, а также контроля целостности программ и программных комплексов.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

MONT
Group of companies

С апреля 2022 года работу со всеми текущими и новыми клиентами и партнёрами компании ABBYY в России продолжает новый технологический партнёр, компания

CONTENT AI (ООО «КОНТЕНТ ИИ»)

Content AI – российская компания, разработчик решений в области интеллектуальной обработки информации. Компания лицензирует всемирно признанные технологии распознавания текста, классификации документов и обработки естественного языка.

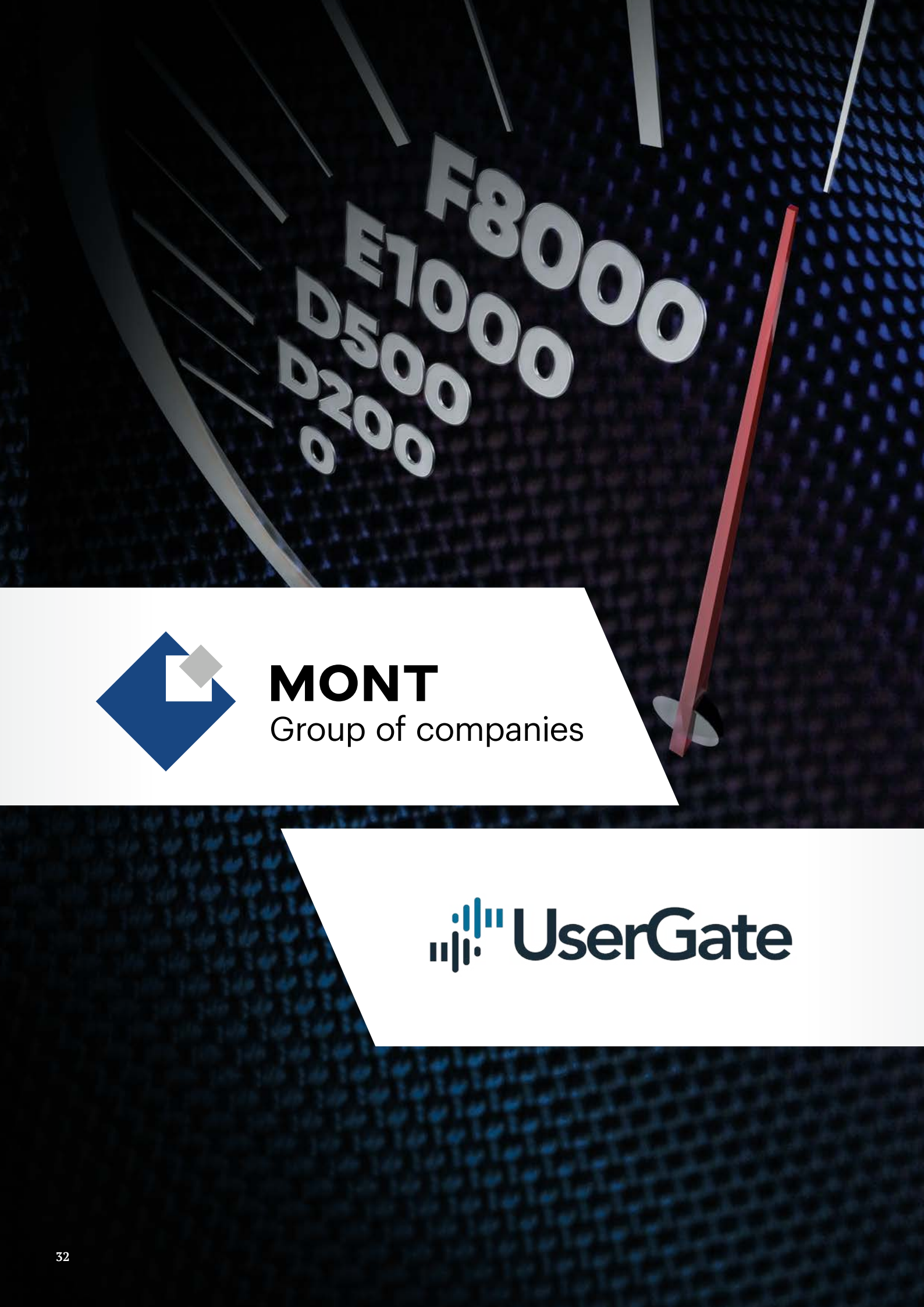
Продукты для всех:

- ContentReader PDF – многофункциональный редактор для решения любых задач с PDF и бумажными документами. Подходит для замены Acrobat и Acrobat Pro.
- Lingvo by Content AI – Электронные словари для работы и учёбы.

Решения для корпоративных пользователей:

- ContentReader Server – корпоративное серверное решение для распознавания, хранения и преобразования файлов в PDF и другие электронные редактируемые форматы.
- ContentCapture – универсальная платформа для интеллектуальной обработки информации из любых типов документов: отсканированных бумаг, фотографий, электронных документов, текстов писем и вложений. Решение распознает, классифицирует документы, извлекает данные, проверяет их корректность и передаёт в корпоративные информационные системы.
- Intelligent Search – это готовое решение для быстрого поиска данных и документов в любых корпоративных источниках.

CONTENT AI



MONT
Group of companies

UserGate

ЗАПИШИСЬ К НАМ НА ТЕСТ-ДРАЙВ USERGATE

Не ждите! Возьмите демооборудование в MONT и протестируйте на своей инфраструктуре.

Уже сейчас в MONT доступны следующие модели: D200, D500, E1000 и F8000.

Не уверены в собственных силах? Наши инженеры помогут настроить и подобрать нужную вам конфигурацию, проконсультируют на любом этапе проекта, помогут провести пилот.

Хотите оставить заявку, пишите нам на usergate@mont.ru

MONT
Group of companies

КОМПАНИЯ MONT ПОМОЖЕТ В ПОДБОРЕ И БЫСТРОЙ МИГРАЦИИ НА НОВОЕ BI-РЕШЕНИЕ

Эксперты MONT проведут анализ инфраструктуры и предложат подходящее BI-решение, которое закроет задачи бизнеса, поможет улучшить качество принятия решений и бесшовно впишется в ИТ-архитектуру.

Мы предлагаем:

- проведение первичной консультации для понимания проблемы и подбора решения;
- проработка коммерческого предложения на поставку ПО;
- проведение демонстраций и пилота для уточнения функциональных требований;
- поставку лицензий на ПО;
- миграцию и внедрение выбранного решения;
- обучение команды пользователей.

MONT РЕКОМЕНДУЕТ:

FanRuan
TRANSFORM DATA INTO VALUE

FineBI – аналог Tableau и MS Power BI от китайского производителя.

VISIOLOGY

Visiology – гибкая система для анализа и подготовки визуализации данных, продукт находится в реестре российского ПО.

ПОЛИМАТИКА
ОТЧЕТНО-АНАЛИТИЧЕСКАЯ ПЛАТФОРМА

Polymatica – современная BI-система для формирования дашбордов, анализа данных. Продукт в реестре российского ПО.

Теперь доступна в виде облачного сервиса в составе решения MONT Office

---

Если вас заинтересовало наше предложение, напишите нам на bi_migration@mont.ru

Оформить подписку на «облачную» Polymatica можно здесь www.oblakoteka.ru/services/mont-office

MONT
Group of companies

ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ДОМА

Навязчивая реклама мешает просмотру фильма или не позволяет насладиться музыкальным произведением? Вам на помощь спешат блокировщики рекламы и нежелательного контента.

ADGUARD	AdGuard Personal (3 устройства) AdGuard Family (9 устройств)
SkyDNS	SKyDNS Домашний (3 устройства) SKyDNS Домашний+ (10 устройств)
UniSafe	UniSafe ALock (1 устройство)

Важная в современном мире категория решений – родительский контроль.

Специальные приложения позволяют дистанционно определять местоположение ребёнка в реальном времени, удалённо контролировать, сколько времени ваш ребёнок проводит со смартфоном, в каких мобильных приложениях и играх, контролировать состояние устройства и др.

Parental Control	Parental Control Kroha
UniSafe	UniSafe Kids

Специализированный продукт, обеспечивающий контроль действий несовершеннолетних детей в интернете на ПК.

UserGate

KinderGate
Родительский контроль

Ещё один аспект — это антивирусная защита, важность которой понимают все.

MONT предлагает своим партнёрам и их заказчикам как узкоспециализированные продукты (NANO Антивирус Pro), так и комплексные решения, включающие, помимо антивирусной защиты, вышеперечисленные функции таких вендоров, как:

kaspersky

Dr.WEB

PRO32

Все продукты можно купить практически моментально в виде электронных ключей – специального кода, активирующего дистрибутив продукта, скачиваемого с сайта вендора.

Технологическая платформа взаимодействия с партнёрами MONT Webstore позволяет доставлять электронные ключи напрямую от поставщиков в режиме онлайн.

Если вас заинтересовали наши предложения, напишите нам по адресу esd@mont.ru

MONT
Group of companies

ГОТОВЫЙ ИНТЕРНЕТ-МАГАЗИН ДЛЯ БЫСТРОГО ЗАПУСКА ОНЛАЙН-БИЗНЕСА

MONT eShop – бесплатный онлайн-сервис, предназначенный для партнёров и позволяющий быстро запустить бизнес по продаже программного обеспечения, доступного в канале электронной дистрибуции MONT.

Сервис включает:

- готовую витрину электронных продуктов с удобным пользовательским интерфейсом, каталогом и живым поиском;
- полное описание всех продуктов, включая картинки, системные требования, инструкции по установке и важные особенности продаж;
- отслеживание и управление заказами покупателей, доступ к данным пользователей магазина;
- две встроенные платёжные системы: ЮKassa и Робокасса – на выбор;
- возможность брендирования (настройки собственного доменного имени интернет-витрины).

Сервис работает круглосуточно без выходных (24/7)

Заказы обрабатываются автоматически

Ключи предоставляются в течение нескольких минут после оплаты покупателем


Корзина ( )
Личный кабинет
КОМПАС-3D v20 Home (Продление на 1 год)
КОМПАС-3D v21 Home
Конструктор тестов
550 ₽
Купить
от 650 ₽
Выбрать версию
от 1 290 ₽
Выбрать версию
Handy Backup Professional
Handy Backup Server Network
Handy Backup Standard
от 2 480 ₽
Выбрать версию
от 58 727 ₽
Выбрать версию
от 1 026 ₽
Выбрать версию


MIO

Безопасность данных

Безопасность данных – это процесс защиты цифровой информации от несанкционированного доступа, повреждения или кражи на протяжении всего её жизненного цикла. Он охватывает всё: оборудование, программное обеспечение, устройства хранения и пользовательские устройства, доступ и административный контроль, а также политики и процедуры организаций.

MONITMON

Предотвращение утечек информации с помощью DLP-систем

Информация правит бизнесом. Вы только вдумайтесь в цифры: 2/3 скомпрометированных компаний закрываются в среднем через полгода или год. В особых случаях утечка персональных данных может закончиться даже уголовной ответственностью. Контролировать потоки корпоративной информации и держать их в безопасности позволяют DLP-системы.

Что такое DLP-система

DLP-система (Data Loss Prevention) переводится как предотвращение потери данных или Data Leakage Prevention – предотвращение утечки данных. Эти технологии предназначены для защиты корпоративной сети от кражи ценной информации. Если вам попадается аббревиатура ILP, ILDP, EPS или CMF, скорее всего, это то же самое, что и DLP-система.

Для каких компаний DLP-технологии жизненно необходимы

Для любого бизнеса, который хочет избежать утечки критически важной информации. Но в первую очередь речь идёт о банках и страховых компаниях, ведь их деятельность находится под контролем регуляторов. Утечка информации для них будет иметь огромные репутационные последствия.

Как работает DLP-система

Программный продукт анализирует поступающие, уходящие данные и их циркулирование по корпоративной системе. DLP-технологии определяют, насколько безопасна информация. Если данные отправляются не туда, то система останавливает их передачу и сообщает об этом специалисту.

DLP-инструменты контролируют все каналы коммуникации: почту, деловые мессенджеры, облачные системы и т.д.

Возможности использования DLP-системы

• Хранилище

Решению можно смело доверить сохранность самой ценной информации компании, ведь в DLP-систему входят все каналы коммуникации специалистов.

• Мотивация

Когда сотрудники понимают, что за ними наблюдают, то они чувствуют повышенную ответственность. Это помогает повысить эффективность всего коллектива.

• Анализ загруженности персонала

Многие DLP-системы умеют делать статистический отчёт по затраченному рабочему времени каждого сотрудника.

• Юридическая поддержка

Если вам всё же не повезло и данные были похищены, то DLP-система предоставит доказательства в суде, что ваша компания стала жертвой мошенников.

Виды DLP-систем

Средства защиты корпоративной информации можно разделить на несколько групп. Разберём каждую из них.

1. **Классические инструменты безопасности**

К стандартному набору безопасности относятся антивирусные программы, встроенные межсетевые экраны, системы выявления несанкционированных вторжений.

2. **Интеллектуальные меры защиты данных**

Сюда входят специальные сервисы и современные алгоритмы определения нелегального доступа к данным, корыстного использования деловой переписки и т.д. Интеллектуальные средства защиты способны проводить детальный анализ информационной безопасности на риски утечки информации разными способами.

3. **Шифрование данных и контроль доступа**

Можно зашифровать ценную информацию и предоставить доступ к ней лишь ограниченному кругу лиц. Это поможет снизить риски кражи персональных данных.

4. **Специализированные DLP-системы безопасности**

Эти решения способны определить и остановить процесс неправомерной передачи данных за пределы компании. Специализированные DLP-системы безопасности позволяют обнаружить мошеннические действия без разрешения на это.

В зависимости от построения на сетевой архитектуре DLP-решения могут быть шлюзовыми и хостовыми. Шлюзовые системы используются на серверах, а хостовые – на рабочих станциях пользователей. Многие современные DLP объединяют в себе оба этих инструмента контроля, что повышает их эффективность.

DLP имеет множество преимуществ: эффективно предотвращает внутренние и внешние угрозы, делает прозрачным процесс обмена данных, применяет процедуры авторизации перед доступом к конфиденциальной информации и машинного обучения для выявления несанкционированных действий пользователя и маркировки конфиденциальных данных. Но даже при том чувстве безопасности, которую вам дают DLP-технологии, не стоит расслабляться. Нужно систематически перепроверять все настройки и конфигурации. Секрет безопасности данных – это синергия вашей бдительности и работы DLP-систем.

CHECK POINT

Quantum – высокопроизводительные масштабируемые шлюзы безопасности для дата-центров и крупных корпораций, обеспечивающие наилучшее предотвращение угроз и оптимизацию для гибридных облачных сред. Шлюзы Quantum Security Gateways™ 26000 и 28000 Check Point включают отмеченное наградами решение предотвращения угроз SandBlast Network, обладают высокой надёжностью и имеют высокую скорость предотвращения угроз – до 1,5 Тбит/сек. Включает модуль DLP.

Если вас заинтересовало решение, обращайтесь по адресу checkpoint@mont.ru

INFOWATCH

DLP-система InfoWatch Traffic Monitor позволяет обнаружить и классифицировать чувствительные данные организации, контролировать их перемещение и предотвращать несанкционированное распространение с использованием машинного обучения для автоматического анализа документов, потоков информации и действий пользователей.

Система впервые была представлена в 2007 году, поддерживает отечественные операционные системы и СУДБ, сертифицирована ФСТЭК России и Министерством Обороны.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

Ростелеком Солар

Solar Dozor – система предотвращения утечек информации (DLP), блокирует передачу конфиденциальных документов, помогает выявлять признаки корпоративного мошенничества, позволяет заниматься профилактикой инцидентов безопасности.

Solar Dozor собирает исходящий, входящий и внутрикорпоративный трафик организации, действия пользователей и другие события с помощью модулей-перехватчиков.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

STAFFCOP

StaffCop Enterprise предназначен для обеспечения информационной безопасности и улучшения эффективности работы организаций и предприятий. Решение позволяет анализировать поведение пользователей, уведомлять об аномалиях и инцидентах, вести учёт рабочего времени и контролировать эффективность труда.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

ZECURION

Zecurion DLP – комплексная DLP-система последнего поколения, признанная «Большой тройкой» мировых аналитических агентств Gartner, IDC, Forrester. Защищает информацию от утечки по локальным и сетевым каналам, выявляет случаи корпоративного мошенничества, помогает расследовать инциденты и оценивать риски информационной безопасности, предоставляя детальную аналитику.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

КИБЕРПРОТЕКТ

«Кибер Протего» обеспечивает комплексную защиту от утечки данных с корпоративных компьютеров, серверов и виртуальных сред. Богатый арсенал методов контроля передаваемых и хранимых данных позволяет эффективно решать задачи предотвращения утечки информации, мониторинга операций передачи конфиденциальных данных и обнаружения нарушений политики их хранения.

Комплекс «Кибер Протего» реализован в модульной архитектуре опционально лицензируемых функциональных компонентов с единым унифицированным управлением, что позволяет клиентам выбрать оптимальную конфигурацию DLP-решения в соответствии со своими требованиями к обеспечению безопасности и бюджетом.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

Средства защиты от несанкционированного доступа к информации

По данным Gartner, 60% людей способны совершить преступление при определённых угнетающих обстоятельствах. Вы можете не подозревать, что ваши сотрудники попали в ловушку и подвергли опасности конфиденциальные сведения компании. Поэтому важно организовать надёжную защиту данных от нелегального доступа. Следить за безопасностью передачи данных необходимо как в случае с бумажными, так и с электронными носителями.

Средства защиты от несанкционированного доступа (СЗИ от НСД) – это программные и/или аппаратные решения, которые блокируют попытки посторонних лиц получить доступ к файлам на компьютере и препятствуют уничтожению конфиденциальной информации.

Как мошенники получают закрытые сведения компании

Несанкционированный доступ к информации не ограничивается взломом операционных систем рабочих компьютеров или прямой кражей документов. Чаще всего мишенью злоумышленников становятся электронные устройства, ведь над ними можно получить удалённое управление.

Киберпреступники обращаются к разным способам получения нелегального доступа:

- подключаются к различным системам связи;
- крадут документы или копируют их в корыстных целях;
- проникают в компьютеры, внешние накопители, чтобы украсть ценную информацию;
- с помощью шпионских программ, вирусов и других вредоносных ПО внедряются в операционную систему компании через Интернет;
- обманным путём используют сотрудников организации, чтобы завладеть необходимыми данными.

Функциональность СЗИ от НСД

Средства защиты от несанкционированного доступа выполняют следующие функции:

- проводят идентификацию и усиленную аутентификацию с помощью доверенных пользователей и устройств;
- разграничивают доступ к важным файлам по уровню их ценности и компетенциям сотрудников. То есть информацию смогут получить только те специалисты, которые ответственны за неё;
- хранят данные о действиях пользователя, что позволяет контролировать информационную безопасность;
- позволяют запускать только выбранный набор программ из легального списка;
- дают возможность контролировать целостность файлов. Если файлы окажутся повреждены, то СЗИ не дадут запустить операционную систему;
- проводят теневое копирование информации при передаче конфиденциальных данных другим устройствам или при печати на принтере;
- разрешают или запрещают (при необходимости) использовать флеш-накопители, DVD-приводы, Wi-Fi-адаптеры и т. д.;
- взаимодействуют со средствами доверенной загрузки.

Как защитить корпоративные сведения от нелегального доступа

Предотвратить постороннее вмешательство в инфраструктуру компании можно с помощью программно-аппаратных и технических средств защиты. Первый вид не позволяет неавторизованным пользователям получить доступ к защищённым файлам, а второй – не даёт чужим лицам физически проникнуть в стены компании.

Чтобы обезопасить бизнес от несанкционированного доступа, можно разбить информацию на группы, которые будут доступны ограниченному кругу пользователей, а также оценить возможности передачи данных между сотрудниками.

В вашей компании должна образоваться иерархия информации в зависимости от её ценности. Доступ к этим данным могут иметь лишь разграниченные группы сотрудников в зависимости от рода их деятельности.

Как компании используют СЗИ

Организации обращаются к СЗИ не только из соображений информационной безопасности, но и из-за необходимости соответствовать требованиям регуляторов. В частности, это касается государственных учреждений и банков. Они используют данные технологии для проведения идентификации и аутентификации, а также чтобы управлять доступом и проводить регистрацию событий.

Разработчики зачастую интегрируют средства защиты от несанкционированного доступа с другими инструментами ИБ, например с программными межсетевыми экранами, антивирусными устройствами и хостовыми средствами обнаружения вторжений.

Надёжность системы защиты информации должна зависеть от ценности конфиденциальных данных в глазах киберпреступников. Важно не перегрузить систему в режиме максимальной защищённости. Адекватно оцените производительность своих рабочих станций и требуемый уровень эффективности СЗИ. Иначе вы только навредите своей инфраструктуре.

STAR FORCE®

StarForce Content Enterprise защищает документы от несанкционированного доступа, копирования, редактирования, распространения и печати. Решение надёжно защищает цифровой корпоративный контент и интеллектуальную собственность компании от перехвата злоумышленниками вне зависимости от того, где находятся файлы относительно ИТ-периметра предприятия.

Зашифрованный файл сможет открыть только человек, имеющий серийный номер документа, а сотрудник службы ИБ будет видеть, когда и сколько раз документ был открыт и были ли неудачные попытки сделать это.

Если вас заинтересовало решение, обращайтесь по адресу starforce@mont.ru

КОД безопасности

Secret Net Studio – защищает данные и инфраструктуру серверов и рабочих станций. Особенностями решения являются:

- проверка имени пользователя, компьютера и исполняемого процесса перед установкой соединения;
- масштабируемая система управления: до десяти тысяч управляемых ПК на один сервер управления; до 1000 зарегистрированных USB-устройств на автономном рабочем месте;
- разграничение доступа как к файлам, так и к NTFS-потокам; до 16 уровней конфиденциальности для мандатной системы разграничения доступа; низкая задержка при распечатке «грифованных» файлов большого размера.

Решение является стандартом для ряда критически важных отраслей российской экономики в области защиты конфиденциальной информации, включая защиту государственной тайны.

По вопросам, связанным с решениями «Код Безопасности», обращайтесь по адресу kb@mont.ru

Аладдин

Семейство продуктов JaCarta позволяет решать следующие задачи:

- организация усиленной или строгой аутентификации в информационных системах и сервисах;
- обеспечение юридической значимости документов и действий пользователей с помощью электронной подписи;
- безопасное хранение контейнеров программных СКЗИ, пользовательских данных, сертификатов, паролей и др.;
- централизованное управление жизненным циклом продуктов семейства JaCarta, средств аутентификации и ЭП, а также других пользовательских данных, которые на них безопасно хранятся. Система сертифицирована ФСТЭК России.

JaCarta Authentication Server (JAS) – высокопроизводительный сервер аутентификации 2ФА с поддержкой как аппаратных OTP- и U2F-токенов, так и программных OTP/PUSH/SMS аутентификаторов для мобильных устройств в составе платформы JaCarta Management System (JMS) 3.7.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

GIS ГАЗИНФОРМ СЕРВИС

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4» является программным средством контроля съёмных машинных носителей информации, предназначенным для защиты от несанкционированного доступа к информации, обеспечения безопасности персональных данных 1 уровня защищённости, значимых объектов КИИ 1 категории на базе персональных компьютеров (ПК) с процессорами, имеющими архитектуру x86 и AMD64. Поддерживаемые ОС: MS Windows/Linux.

Если вас заинтересовало решение, обращайтесь по адресу gis@mont.ru

КРИПТОПРО

«КриптоПро NGate» – это универсальное высокопроизводительное средство криптографической защиты сетевого трафика (TLS- и VPN-сервер). Решения NGate помогут создать комплексную защиту для систем и ресурсов в соответствии с требованиями российского законодательства. Компоненты решения сертифицированы ФСБ России по классам КС1, КС2, КС3 и используют в своём составе сертифицированное ФСБ России СКЗИ «КриптоПро CSP» с российскими криптографическими алгоритмами ГОСТ 28147–89, ГОСТ Р 34.11–94/ГОСТ Р 34.11–2012, ГОСТ Р 34.10–2001/ГОСТ Р 34.10–2012. При этом для классов КС2 и КС3 не требуется выполнение отдельных настроек, приобретение и конфигурирование электронных замков и прочих дополнительных мер защиты, всё необходимое уже включено в аппаратные платформы решения.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

КОМПАНИЯ ИНДИД

Indeed Access Manager позволяет построить систему централизованного управления доступом пользователей к информационным ресурсам компании. Поддерживаются различные технологии усиленной и многофакторной аутентификации. С помощью механизмов интеграции можно подключать разнообразные целевые приложения. Indeed AM помогает сократить расходы на сопровождение инфраструктуры и сделать работу пользователей более эффективной.

Indeed Certificate Manager – это централизованная система управления инфраструктурой открытых ключей, поддерживающая аудит инфраструктуры PKI интеграцию с различными сторонними системами. Продукт позволяет привести процессы использования PKI в соответствие с потребностями всех заинтересованных сторон, снизить затраты на рутинные операции обслуживания PKI и повысить общий уровень информационной безопасности компаний.

Если вас заинтересовали решения, обращайтесь по адресу indeed@mont.ru

Ростелеком Солар

Solar inRights позволяет управлять учётными записями и правами доступа пользователей к корпоративным ресурсам организации любого масштаба и сложности, обеспечивая:

- автоматизацию жизненного цикла пользователей от найма до увольнения;
- полную картину прав доступа к информационным системам;
- ручное и автоматическое предоставление и отзыв доступа;
- создание и редактирование маршрутов согласования заявок;
- лёгкий аудит и контроль доступов сотрудников;
- борьбу с избыточными правами доступа на основе ролевой модели;
- управление SoD-конфликтами;
- настройку парольной политики организации;
- мгновенное выявление расхождений/нарушений;
- управление рисками.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

CHECK POINT

Check Point Capsule представляет собой гибрид систем управления правами доступа к данным и мобильным устройствам, средств взаимодействия с бизнес-приложениями и корпоративным окружением через VPN-шлюз безопасного удалённого доступа, а также механизмов контейнеризации рабочего окружения на мобильных устройствах сотрудников.

Задействованные в «капсуле» технологии позволяют создавать на мобильном устройстве защищённую бизнес-среду и отделять корпоративные данные и приложения от персональных.

Если вас заинтересовало решение, обращайтесь по адресу checkpoint@mont.ru

«Рутокен» – это аппаратные и программные решения в области аутентификации, защиты информации и электронной подписи. Аппаратные устройства, системное и прикладное ПО «Рутокен» сертифицированы ФСТЭК и могут применяться даже для защиты информации с грифом «Секретно» и в автоматизированных системах до класса защищённости 1Г включительно.

В составе технических комплексов, реализующих защиту информации от НСД, продукты «Рутокен» используются как средство двухфакторной аутентификации при доступе к сети. USB-токены и смарт-карты «Рутокен» могут применяться для хранения ключей, сертификатов, «секретов» в различных протоколах и приложениях, обеспечивающих сетевую безопасность:

- Kerberos (доменная аутентификация);
- OpenVPN, IPSEC, SSL VPN и др. (аутентификация в VPN);
- SSL/TLS (аутентификация на web-сайтах, в почте, прикладных сервисах) и др.

Большинство приложений, реализующих сетевую безопасность, позволяют «подключать» токены для проведения строгой криптографической аутентификации через стандартные программные интерфейсы (PKCS#11, Microsoft Crypto API). Продукты «Рутокен» совместимы с сертифицированным ПО российских производителей, ориентированных на сетевую безопасность (VipNet CSP, «VPN Застава», «Крипто-Про IPSec» и др.), что позволяет строить защищённые сети, обеспечивающие высокий уровень безопасности и соответствующие требованиям российского законодательства. В то же время линейка «Рутокен» совместима с решениями западных производителей (Cisco, Stone Gate и др.), а также с продуктами Open Source.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

StarForce Crypto – профессиональное решение, обеспечивающее защиту от анализа и модификации приложений (native-код и managed-код), написанных под ОС Windows, а также сокрытие/защиту от подмены любых неизменяемых файлов данных, оперируемых защищаемым приложением. Решение подходит для любого ПО, распространяемого любым способом.

Если вас заинтересовало решение, обращайтесь по адресу starforce@mont.ru

Программный комплекс «САКУРА» – российская разработка в сфере информационной безопасности. Обеспечивает решение следующих ключевых задач:

- интеграция с VPN-решениями;
- двухфакторная аутентификация;
- контроль доступа к корпоративным ресурсам;
- мониторинг активности сотрудников;
- соответствие удалённых пользователей внутренним политикам безопасности;
- инвентаризация оборудования и ПО.

Совместима как с операционными системами Windows, так и Linux, в том числе Astra Linux, Ред ОС и AlterOS.

Если вас заинтересовало решение, обращайтесь по адресу product@mont.ru

Средства криптографической защиты информации

Если деятельность вашей компании связана с информацией повышенной секретности, то вам нужны соответствующие средства защиты. Криптография считается одним из таких надёжных способов защиты данных. Даже если секретные сведения попадут в руки злоумышленников, они вряд ли смогут их расшифровать. Кодирование данных используют в разных сферах, например, чтобы надёжно хранить документы или передавать информацию по защищённым каналам коммуникации.

Что такое средства криптографической защиты информации

Криптографическое шифрование данных – это процесс кодирования информации при отправлении получателю. Адресат использует тот же алгоритм для расшифровки, что и при кодировании данных. Таким образом информация защищается от перехвата злоумышленниками. Чаще всего СКЗИ применяются для создания и проверки подлинности электронных подписей, шифровки и дешифровки содержимого документа.

Как работают СКЗИ

1. Пользователь создаёт документ, который собирается пересылать.
2. Ключ и специальные программы кодируют подпись, которая затем прикрепляется к основному файлу. После этого весь материал отправляется адресату.
3. Получатель с помощью специального ключа расшифровывает файл. Затем он проверяет, что в декодированный документ не вносились изменения.

Классы криптографической защиты информации

Криптография бывает трёх типов: с секретным ключом, с открытым ключом и с хеш-функциями. Разберём, в чём их отличия.

Симметричная криптография

Криптография с секретным ключом, или симметричная криптография, строится на одинаковом ключе как для шифрования данных, так и для их дешифровки. Именно поэтому эта форма кодирования считается самой простой. Симметричное шифрование данных используется для передачи информации как в сети, так и на носителе. Но ко второму способу компании прибегают чаще, так как он более надёжный.

Асимметричная криптография

Этот тип криптографии использует два разных ключа для кодирования данных. Один из них помогает шифровать информацию, а второй расшифровывает сообщение. У каждого ключа – только одна функция. Использовать ключ для кодирования данных, чтобы декодировать информацию, – нельзя, и наоборот. Один ключ находится только у владельца и называется «закрытым». Вторым может воспользоваться кто угодно – это «открытый ключ».

Хеш-функции

Хеш-функции позволяют защищать информацию без возможности восстановить исходные данные. Хеширование – способ преобразования заданной строки в строку фиксированной длины. Удачный алгоритм хеширования будет выдавать уникальные результаты для каждого заданного входа. Чтобы взломать хеш, злоумышленнику придётся бесконечно подбирать всевозможные варианты входа. Хеш чаще всего используется для шифрования паролей.

Виды средств криптографической защиты информации

Инструменты шифрования для электронной подписи бывают двух видов: программные и аппаратные. Остановимся на каждом из них.

Программное шифрование данных

Программные СКЗИ устанавливаются на ПК и работают в оперативной памяти. Скорее всего, вам придётся купить лицензию. Некоторые разработчики предлагают бесплатный пробный период на несколько месяцев. Если вы работаете с электронной подписью на нескольких компьютерах, то вам потребуется несколько лицензий.

Аппаратное шифрование данных

Такие СКЗИ встраиваются в специальное устройство и считаются более безопасными и простыми в работе. Они функционируют в памяти этого устройства, за счёт чего закрытый ключ сертификата ЭП не остаётся в памяти компьютера. Аппаратные СКЗИ не нужно устанавливать и покупать на них лицензию. Они уже есть в устройстве. После окончания работы с электронной подписью, вы можете удалить её и загрузить новую. Переустанавливать ничего не нужно.

Где нужна электронная подпись

Квалифицированная электронная подпись чаще всего применяется в следующих случаях:

- онлайн-отчётность в различных государственных структурах;
- госзакупки для бюджетных организаций;
- электронный документооборот между компаниями;
- порталы госструктур: РКН, Госуслуги, Единый федеральный реестр сведений о банкротстве, Росимущество и прочие.

Защита криптографической информации в бизнес-процессах

Современные компании управляют большим массивом корпоративной и конфиденциальной информации в облачной системе. Именно поэтому они используют шифрование: это помогает поддерживать информационную безопасность бизнеса. Для этого предприятия используют различные устройства кодирования, приборы защиты телефонии. СКЗИ применяются для защиты офисного оборудования, такого как факсы, телекс или телетайп. Также в коммерческой деятельности к кодированию обращаются, когда работают с электронными подписями.

К работе со средствами криптографической защиты информации нужно относиться со всей серьёзностью, ведь у них есть требования, которые прописаны в специальных ГОСТах и приказах ФСБ. В основном эти нормативы касаются квалифицированной электронной подписи. Любая информационная система согласовывается с ФСБ РФ и ФСТЭК.

GIS ГАЗИНФОРМ СЕРВИС

Криптографическая платформа Litoria Crypto Platform позволяет реализовать в эксплуатируемом или разрабатываемом программном обеспечении весь спектр функциональных возможностей инфраструктуры открытых ключей (от формирования электронной подписи и шифрования данных до функций доверенной третьей стороны и архивного штампа времени).

Если вас заинтересовало решение, обращайтесь по адресу gis@mont.ru

КОД безопасности

Аппаратно-программный комплекс шифрования (АПКШ) «Континент» – централизованный комплекс для защиты сетевой инфраструктуры и создания VPN-сетей с использованием алгоритмов ГОСТ. Комплекс реализует следующие основные функции:

- криптографическая защита данных, передаваемых по каналам связи общих сетей передачи данных между составными частями VPN;
- предоставление доступа удалённым пользователям к ресурсам защищаемой сети;
- межсетевое экранирование;
- автоматическая регистрация событий, связанных с функционированием комплекса;
- централизованное управление компонентами комплекса

По вопросам, связанным с решениями «Код Безопасности», обращайтесь по адресу kb@mont.ru

КРИПТОПРО

«КриптоПро CSP» предоставляет следующие возможности:

- формирование и проверка электронной подписи;
- обеспечение конфиденциальности и контроля целостности информации посредством её шифрования и имитозащиты.
- обеспечение аутентичности, конфиденциальности и имитозащиты соединений по протоколам TLS и IPsec;
- контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений доверенного функционирования.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

ФАКТОР-ТС

Dionis DPS – линейка отечественных маршрутизаторов и криптомаршрутизаторов, сертифицированная по требованиям ФСТЭК и ФСБ России и соответствующая самым высоким уровням защищённости. Dionis DPS ориентирована как на коммерческий сектор, так и на государственные ведомства. На данный момент уже используется для организации безопасного информационного обмена во всех министерствах и ведомствах силового блока России, а также в других государственных учреждениях.

Если вас заинтересовало решение, обращайтесь по адресу factor@mont.ru

КриптоАРМ

«КриптоАРМ VipNet» – кроссплатформенное приложение для создания и проверки электронной подписи файлов, ориентированное на владельцев сертификатов электронной подписи, созданных с использованием СКЗИ VipNet CSP.

«КриптоАРМ Стандарт Плюс» – это удобная программа, позволяющая подписывать и шифровать электронные документы с дополнительной поддержкой использования протокола PKCS#11 (работает с токенами с аппаратной «криптографией на борту») и поддержкой сертификатов DSS.

«КриптоАРМ ГОСТ» – это универсальное приложение с графическим пользовательским интерфейсом для выполнения операций по созданию и проверке электронной подписи файлов, шифрования и расшифрования, управления сертификатами, размещённых в хранилищах криптопровайдера «КриптоПро CSP» версии 5.0.

Если вас заинтересовало решение, обращайтесь по адресу product@mont.ru

С-Терра

«С-Терра Шлюз» – программно-аппаратный комплекс (программный комплекс на аппаратной платформе) для обеспечения безопасности сети связи любой топологии (VPN), с любым количеством туннелей. Обеспечивает криптографическую защиту и фильтрацию как трафика подсетей, проходящего через него, так и защиту трафика самого шлюза безопасности.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

CIS / Спецвыпуск (24) / 2023 / www.cis.ru

Привилегиями нужно управлять

Пандемия COVID-19 стимулировала компании использовать расширенный удалённый доступ к корпоративной сети. Теперь администраторы и пользователи, наделённые особыми полномочиями, могут совершать противоправные действия, оставаясь незамеченными. Это привело к новой волне проблем информационной безопасности.

Вторжение может быть организовано по ошибке или в корыстных целях. Зачастую сбои происходят после работы проверяющих органов, аудиторов, которые были привлечены для управления системой.

В ИТ-сфере под привилегиями понимают полномочия по настройке и выключению системы, загрузке драйверов, настройке учётных записей и т.д. Если не контролировать эти полномочия, то действия их администраторов могут привести к серьёзным последствиям для организации. Именно поэтому существуют специальные системы по управлению привилегированным доступом, которые называются Privileged Access Management.

Что такое Privileged Access Management-системы и как они работают

Privileged Access Management (PAM) – это решение, которое предотвращает нелегальный привилегированный доступ к ценным данным компании. Иными словами, это ещё одно средство для защиты от киберугроз. Оно ограничивает число администраторов ресурса, таким образом лишая киберпреступников возможности украсть учётные данные.

Успех PAM основывается на сумме трёх слагаемых: люди, процессы и технологии. Решение позволяет отследить, кто использует привилегированные полномочия и с какой целью. Оно определяет политику управления привилегированным доступом.

Что могут PAM-системы:

- автоматизировать процесс создания, изменения и удаления учётных записей;
- диагностировать и регистрировать привилегированные учётные записи;
- предоставлять безопасный удалённый доступ и контролировать его со стороны.

PAM-инструменты отслеживают все операции, чтобы вы смогли с помощью отчёта вовремя заметить отклонения и исправить их. Кроме того, это помогает контролировать, насколько соблюдаются требования политики предоставления привилегированного доступа.

Цель злоумышленника – украсть данные для входа в учётную запись пользователя, ведь с помощью них он сможет получить доступ ко всей корпоративной системе. Это позволит ему установить вредоносные программы на рабочие устройства организации или совершить другие противоправные действия со злым умыслом.

Решение PAM минимизирует риск развития такого сценария, так как доступ предоставляется в определённое время с ограниченными привилегиями при условии многофакторной проверки подлинности удостоверений и учётных записей администраторов.

Политика управления привилегированным доступом зависит от стандартов соответствия, которые применяются в вашей организации. Чаще всего компании предоставляют минимальные права для защиты конфиденциальных данных, например платёжной информации или личных медицинских записей.

Как внедрить Privileged Access Management

Мы собрали рабочую методичку, которая поможет повысить безопасность ИТ-инфраструктуры вашего бизнеса и снизить риски при внедрении PAM-системы.

1. Добавьте обязательную многофакторную проверку личности при входе в учётную запись. Это обеспечит дополнительный уровень защиты.
2. Автоматизируйте защиту, чтобы снизить риски ошибки персонала при работе с ценными данными. Если возникнет угроза, вы сможете автоматически ограничить полномочия администратора и остановить небезопасные действия.
3. Вычисляйте и удаляйте ненужных конечных пользователей из группы администраторов на рабочих устройствах. Мошенники могут использовать учётную запись вашего сотрудника для дальнейшего перемещения по сети.
4. Отслеживайте отчёты о деятельности привилегированных пользователей. Нужно знать базовые показатели и сравнивать их с отклонениями. Так вы сможете вовремя обнаружить несанкционированное вмешательство.
5. Ограничивайте права доступа в зависимости от рабочих потребностей пользователей и от вашего уровня доверия к ним.
6. Дозируйте время и привилегии доступа. Открывайте доступ только по веским причинам и на ограниченное время.
7. Предоставляйте привилегии только для ресурсов, которые пользователь реально использует.

Таким образом, PAM-системы позволяют прозрачно и максимально эффективно контролировать все операции, связанные с привилегированными полномочиями в корпоративной структуре. Без этого решения информационная безопасность вашего бизнеса может оказаться под угрозой. PAM поможет обнаружить и расследовать противоправные действия злоумышленников против вашей компании.

КОМПАНИЯ ИНДИД

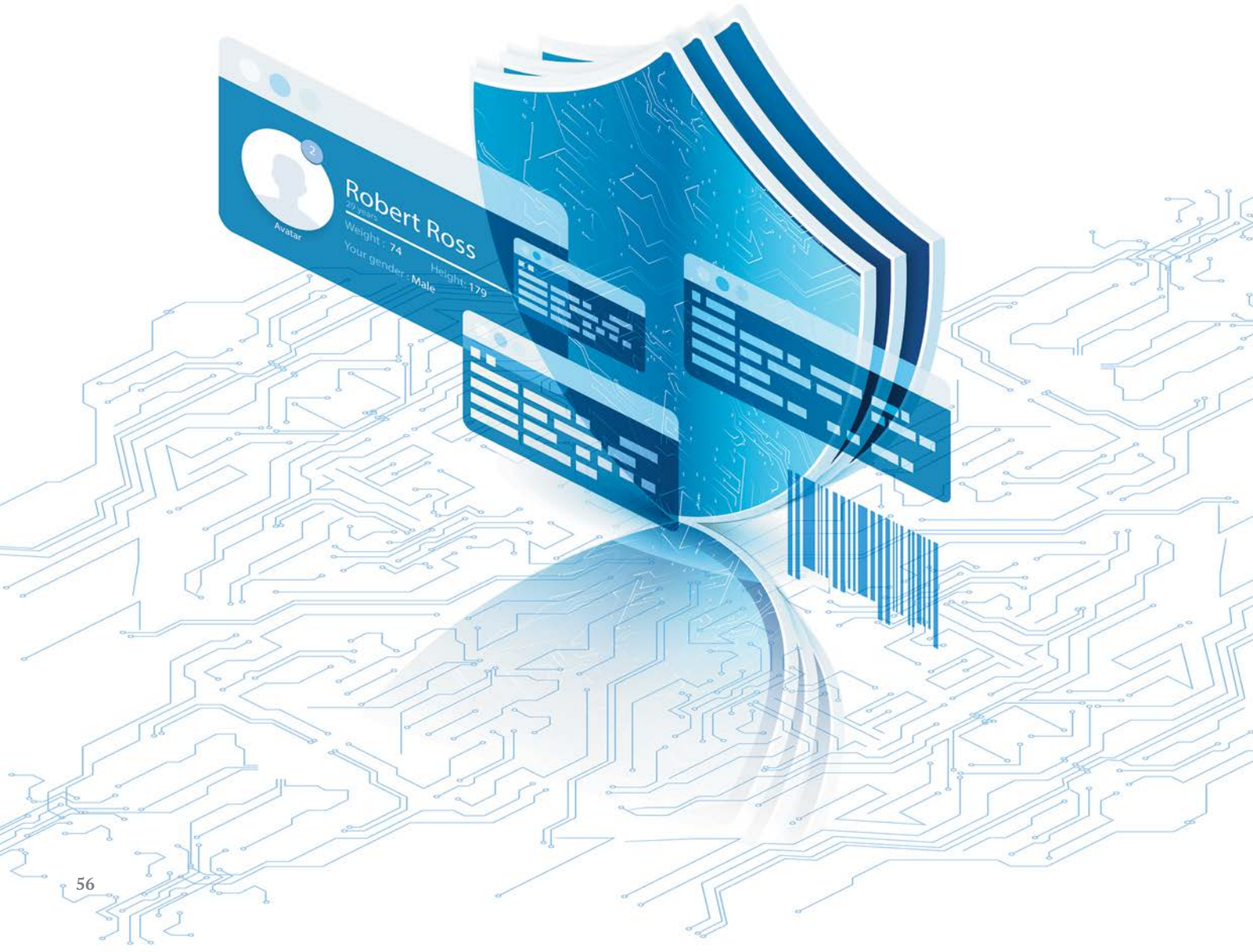
Indeed Privileged Access Manager защищает привилегированный доступ, контролирует привилегированные сессии и предоставляет развитые возможности управления привилегированными учётными записями. Сценарии использования системы включают защиту привилегированных учётных записей, аудит работы администраторов и контроль доступа подрядчиков.

Если вас заинтересовало решение, обращайтесь по адресу indeed@mont.ru

Ростелеком Солар

Solar SafeInspect – полнофункциональная платформа PAM (Privilege Access Management) для эффективного управления привилегированными учётными записями и сессиями в современных информационных системах как классических, так и облачных. Контролирует доступ привилегированных пользователей, проактивно применяет политики безопасности и записывает все действия привилегированных пользователей.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru



Как выбрать анализатор кода приложений

Часто компании не удовлетворены стандартными возможностями программных продуктов и хотят расширить их функциональность под свои запросы. Они обращаются к сторонним модулям, которые закрывают эту потребность. Эти модули представляют собой программный код, который пишется на встроенном языке программирования. Но заказчики не учитывают, что такой встраиваемый код может содержать серьёзные уязвимости, которые могут привести к краже конфиденциальной информации или другим тяжёлым последствиям информационной безопасности.

Здесь на помощь приходит анализатор исходного кода, который работает на основе статистического анализа. Он помогает сделать программу безопасной. Для этого решение анализирует исходный код, чтобы выявить уязвимости. Затем оно формирует отчёт для специалистов, которые отбирают актуальные ошибки и ещё раз их перепроверяют. Только после этого разработчики начинают исправлять код.

Любое автоматизированное решение ИТ-процессов создано, чтобы облегчать работу специалистов. Поэтому очень важно правильно подобрать такой продукт, чтобы он не усложнял вам жизнь. Но как это сделать?

Критерии выбора

Выбрать эффективный анализатор кода не так просто, как кажется на первый взгляд. Многие компании обращают внимание на скорость сканирования или на количество языков программирования. Но на практике выясняется, что специалисты получают бесполезные отчёты, так как неправильно подобрали анализатор кода.

Например, если вы используете только режим поиска по шаблонам (pattern matching, сканирование пройдёт быстро, но недостаточно успешно. Вы получите целую монографию с большим количеством ложных срабатываний. В итоге специалисты потратят много времени на проверку такого неточно отчёта, а код так и не станет безопасным.

При выборе анализатора смотрите не на скорость, а на качество сканирования: его широту, полноту и количество ложных срабатываний. Эффективный анализатор должен искать в первую очередь не уже известные ошибки, а уязвимости, шаблонов которых нет в базе.

Качество сканирования разных анализаторов можно проверить с помощью специального приложения, вручную прогоняя через него код. Но для стандартной организации время – ценный ресурс, а это долгий процесс. Поэтому можно обратиться к результатам исследований независимых организаций, например OWASP – проекта, посвящённого обеспечению безопасности веб-приложений. Команда этого сообщества сформировала ряд эталонных тестов, которые представляют собой код с известным числом уязвимостей. Запуская анализ кода на испытуемых анализаторах, можно понять, как они справляются с поиском уязвимостей.

Что должен уметь хороший анализатор кода

- Вычислять условия дальнейшего использования уязвимостей.

Например, в коде обнаружилась SQL-инъекция, а далее идёт условие, что данный фрагмент кода должен выполняться только 31 февраля. Понятно, что с этой уязвимостью ничего нельзя сделать и не стоит тратить на неё время.

- Формировать тестовые эксплойты, которые позволяют в режиме реального времени проэксплуатировать уязвимость и увидеть реакцию приложения.
- Проверить реальность найденной уязвимости с помощью разных механизмов. Для этого есть функция автопроверки.
- Прогнозировать всевозможные сценарии атак хакеров и их последствия.

Поиск по шаблонам с такой задачей не справляется. Становится популярным инструмент построения диаграммы потоков данных. Он отображает на графике хронологию преобразования данных и пользователей от точки их возникновения в программе до точки выхода подозрительного действия.

Стоит обратить внимание на механизм DFD. Нельзя полностью ему доверять. Этот инструмент показывает перемещения данных по кодам, но не позволяет увидеть их значение. Если не знать эти показатели, то есть риск ложного срабатывания. Чтобы исправить этот недочёт, можно обратиться к символическому анализу.

Приложение становится безопасным только при качественном сканировании, при котором важны не количество поддерживаемых языков, а широта и полнота сканирования, а также малое количество ложных срабатываний. Выбирая анализатор по критерию качества сканирования, можно протестировать один и тот же код анализаторами разных производителей и сравнить результаты или обратиться к исследованиям независимых организаций.

Важно помнить, что главное – не отчёт по результатам сканирования, а исправленное по найденным уязвимостям приложение.

positive technologies

PT Application Inspector – решение для выявления уязвимостей в исходном коде или готовом приложении путём комбинации статических (SAST), динамических (DAST) и инфраструктурных (IAST) методов анализа. По итогам анализа PT Application Inspector не только выдаёт данные о номере строки и типе уязвимости, но и генерирует эксплойты – безопасные, но эффективные тестовые запросы, которые помогают подтвердить или опровергнуть наличие уязвимости. Благодаря модулю динамического анализа эти запросы запускаются на любом тестовом стенде, в том числе в автоматическом режиме, что радикально сокращает трудозатраты экспертов.

Если вас заинтересовало решение, обращайтесь по адресу pt@mont.ru

Ростелеком Солар

Solar appScreener – удобное и простое в использовании комплексное решение, сочетающее возможности статического (SAST) и динамического (DAST) анализа кода, которое помогает обеспечить полноценный контроль безопасности приложений и информационных систем.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

Эшелон комплексная безопасность

Статический анализатор исходных текстов программ «АК-ВС 2» предназначен для проведения сертификационных испытаний на отсутствие недекларированных возможностей (программных закладок), анализа безопасности программного кода.

Анализатор исходных текстов программ «АК-ВС 3» – современное и функциональное средство выявления уязвимостей и недекларированных возможностей в программном обеспечении при помощи SAST и DAST методик.

Продукты включены в единый реестр российского ПО.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

CIS / Спецвыпуск (24) / 2023 / www.cis.ru

Защита баз данных и файловых хранилищ

Системы защиты баз данных

Защита базы данных работает на основе комплексного подхода. Существует множество разных методов. Мы рассмотрим только основные.

Штатный аудит и мониторинг

В штатном аудите можно настраивать и включать триггеры, создавать процедуры, которые срабатывают во время попытки посторонних лиц получить доступ к чувствительной информации. При этом ведётся журнал запросов и подключений к системе управления базами данных в виде таблицы, где указаны время, тип запроса и кем он был сделан. Штатный аудит идеально подходит под все требования регуляторов. Но он не подходит для проведения внутренних расследований событий и решения задач информационной безопасности.

Резервное копирование

Если произошёл сбой в работе системы управления базами данных, информацию можно будет восстановить благодаря резервному копированию, которое дублирует файлы с жёсткого диска на другой носитель.

Шифрование

При этом методе используется устойчивый криптоалгоритм для кодирования информации в базах данных. Мошенник не сможет прочитать зашифрованную информацию, в отличие от пользователей, у которых есть ключ доступа. Но в данном случае нужно учитывать, что ключ доступа может быть намеренно передан постороннему лицу. Кроме того, шифрование не гарантирует безопасность от администратора базы данных.

VPN и двухфакторная аутентификация

Если организовать доступ внутренних пользователей и администраторов к базам данных с помощью VPN и двухфакторной аутентификации, то это значительно увеличит эффективность защиты инфраструктуры от взлома.

Помимо стандартной пары логина и пароля, для доступа к защищённому объекту можно также использовать USB-ключи, смарт-карты, iButton, одноразовый код в виде СМС или email, генератор паролей, биометрические данные и т.д.

Автоматизированные системы защиты

Несмотря на то что практически все современные системы управления базами данных имеют встроенные средства защиты, есть целый сегмент продуктов для обеспечения безопасности различных баз данных.

Эти решения принято делить на две группы в зависимости от их функциональных возможностей: Database Activity Monitoring (DAM) – мониторинг активности баз данных и Database Firewall (DBF) – файрвол уровня баз данных.

DAM отслеживает действия пользователей в системах управления базами данных. При этом вам не нужно менять настройки или конфигурации самих средств управления базами данных. DAM не влияет на бизнес-процессы, так как он обрабатывает копию трафика. Он позволяет классифицировать SQL-запросы, разбирать трафик взаимодействия пользователей с базами данных, вести полный аудит SQL-запросов и ответов на них.

Данные решения позволяют находить среди огромного числа запросов потенциальные инциденты и сохранить полную историю действий пользователей.

DBF выступает в качестве сетевого шлюза, который может внедряться «в разрыв» или работать в пассивном режиме, чтобы обрабатывать копии трафика. Такая система способна блокировать потенциально опасные запросы, но, чтобы это сделать, нужно установить DBF первым способом («в разрыв»).

Перспективы развития средств защиты баз данных

Рынок систем защиты баз данных трудно назвать насыщенным, тем не менее он стремительно развивается и каждый год появляются новые продукты. Большинство заказчиков предпочитают использовать встроенные средства защиты, но это не мешает накладным системам DAM и DBF пользоваться высоким спросом.

Бизнес начинает смотреть в сторону внешних систем безопасности, так как они дают больше возможностей для защиты баз данных, обладают более удобным интерфейсом, средствами мониторинга и подготовки отчётности, а также могут предложить такие функции, как отслеживание нелегальных действий в базах данных. Кроме того, внешние системы безопасности могут успешно интегрировать с другими системами.

ZECURION

Zecurion Storage Security защищает любые типы данных с помощью надёжных алгоритмов шифрования при хранении, использовании, резервного копирования и транспортировке в случае физического доступа. Все данные находятся на носителях в зашифрованном виде: в случае попадания носителей в руки злоумышленников доступ к ним будет невозможен. Шифрование происходит «на лету» и абсолютно прозрачно как для сотрудников, так и для любого прикладного ПО и операционной системы – это обычный диск, сервер, СУБД или магнитная лента. За счёт более чем 20-летнего опыта эксплуатации в крупных и SMB-проектах Storage Security требует минимальных ресурсов и не замедляет скорость работы с данными. Отлично подходит для защиты СУБД, 1С, файловых серверов, СХД, NAS, SAN и любых мест хранения данных.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

kaspersky

Kaspersky Security для систем хранения данных обеспечивает надёжную высокоэффективную масштабируемую защиту в реальном времени ценной и конфиденциальной корпоративной информации, хранящейся в системах EMC™ (Isilon™, Celerra™ и VNX™), NetApp, Dell™, Hitachi HNAS, IBM System Storage N и Oracle® ZFS Storage Appliance.

Если вас заинтересовало решение, обращайтесь по адресу lk@mont.ru

Аладдин

«Крипто БД» – наложенное средство защиты информации, представляющее собой программно-аппаратный комплекс для предотвращения утечек информации из высокопроизводительных СУБД Oracle, Microsoft SQL Server, PostgreSQL, Postgres Pro и Jatoba.

С помощью системы «Крипто БД» можно осуществлять селективное (выборочное) шифрование информации, хранящейся в логической структуре таблиц СУБД, что существенно снижает нагрузку на аппаратные ресурсы по сравнению, например, с шифрованием всех файлов базы данных. Являясь наложенным средством защиты информации, система «Крипто БД» не затрагивает штатных механизмов обработки информации СУБД. При этом обеспечивается дополнительный контроль доступа к защищённым данным, а также регистрация всех операций с ними, независимо от уровня привилегий пользователей СУБД.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

Защита конечных точек

Конечной точкой считается любое устройство, которое может подключаться к центральной сети предприятия. Именно конечные точки зачастую оказываются самым уязвимым местом сетевой безопасности. С развитием мобильных платформ понятие конечных станций тоже расширилось. Теперь в него входят не только компьютеры, но и мобильные и IoT-устройства. В связи с этим увеличилось число атак как на корпоративные, так и на домашние сети.

Какие устройства относятся к конечным точкам

Компьютеры и ноутбуки

Любой компьютер или ноутбук, имеющий выход в сеть, может оказаться мишенью для заражения вредоносными объектами. В целях безопасности обязательно проводите диагностику корпоративных и личных гаджетов, а также внешних ПК, подключённых к офисной сети через VPN.

Мобильные телефоны

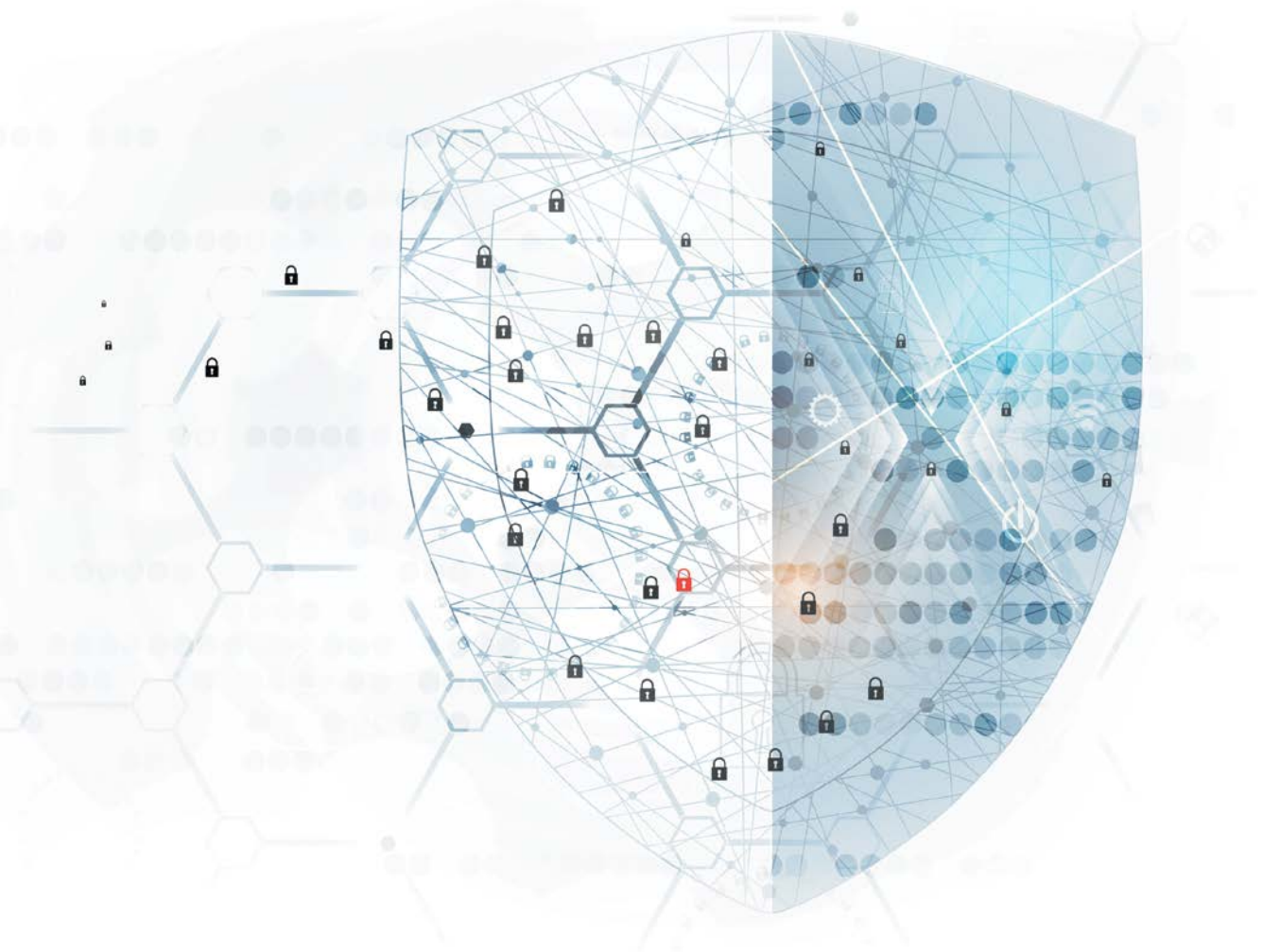
Мобильные телефоны легче всего подхватывают заражённые программы из сети. Чтобы этого избежать, ваши сотрудники должны установить мобильные антивирусы с последними обновлениями программного обеспечения. Кроме того, персонал, использующий личные устройства, должен пройти специальное обучение.

Офисная техника

Принтеры, факсы, умные и другие устройства, которые подключаются к вашей сети, тоже находятся в зоне риска и должны быть защищены.

Серверы

Серверы требуют особого уровня защиты, поскольку на них хранится информация, потенциально интересная для злоумышленников: деловая документация, корпоративная почта и бизнес-данные.



Разница между Endpoint Security и антивирусным ПО

Одним из средств защиты конечных точек считается Endpoint Security. Это решение предназначено для мелких, средних и крупных предприятий, а не для частного и домашнего пользования, как антивирусы.

Endpoint security позволяет:

- обнаруживать уязвимости конечных устройств и реагировать на них;
- создавать отчёты, оповещения о слабых местах информационной безопасности корпоративной сети;
- защищать устройства и данные от потенциальных угроз;
- расследовать подозрительные действия в системе для поиска причин сбоя;
- интегрировать со сторонними средствами безопасности;
- контролировать распространение вредоносных программ;
- централизованно управлять.

К средствам защиты конечных точек также относят антивирус. Это программный продукт, который предотвращает риски информационной безопасности, а также обнаруживает и блокирует вредоносные файлы. К вредоносным программам относятся вирусы, трояны, кейлоггеры, программы-вымогатели, черви, то есть всё, что может нанести вред компьютерной сети или её частям.

Функциональные возможности антивирусов:

- сканировать в режиме реального времени и вручную;
- защищать устройство во время выхода в Интернет;
- идентифицировать различные угрозы;
- удалять или блокировать вредоносные файлы;
- оповещать о периодическом сканировании и обновлении;
- автоматически обновлять свой функционал.

Endpoint Security защищает сеть и все её конечные точки, а антивирус концентрируется лишь на отдельной системе. Первое решение, в отличие от второго, может шифровать данные и предоставлять доступ по уровням значимости пользователей. И в целом функциональность Endpoint security шире, чем антивирусного ПО. Главное отличие этих продуктов в их назначении. Если Endpoint security используется в коммерческих целях, то антивирусы подходят для домашних сетей или очень маленьких организаций.

Но не стоит забывать о человеческом факторе. Без грамотного персонала даже самая эффективная система защиты окажется бесполезной. Противостоять человеческому фактору без ущерба для оперативной работы бизнеса ещё никто не научился. Поэтому проще и гораздо дешевле вовремя обучать людей азам безопасного поведения и использования своих гаджетов.

PRO32

Антивирусы для дома и домашней сети

PRO32 Mobile Security – версия для смартфонов и других мобильных устройств. Защищает от вредоносных программ, кражи и отслеживания устройства. Поддерживает функцию резервного копирования контактов. Обеспечивает безопасное Wi-Fi-соединение. Включает аудит безопасности используемых приложений. И всё это при минимальной нагрузке на систему.

PRO32 Total Security – решение класса Internet Security для ПК и ноутбуков на ОС Windows. Решение обеспечивает:

- родительский контроль: блокировку сайтов и приложений по категориям и времени использования;
- защиту онлайн-платежей;
- защиту от вредоносного ПО;
- блокировку программ вымогателей;
- защиту веб-камеры и Wi-Fi-соединения.

PRO32 Ultimate Security – комплексная защита стационарных и мобильных устройств. Программа поддерживает все функции PRO32 Total Security и PRO32 Mobile Security и обеспечивает возможность лицензирования всех устройств.

Если вас заинтересовало решение, обращайтесь по адресу pro32@mont.ru

CHECK POINT

Harmony Endpoint – это полное решение по обеспечению безопасности конечных точек для защиты организаций и удалённых работников в текущем сложном ландшафте угроз. Решение обеспечивает:

- защиту от программ-вымогателей;
- защиту от фишинга;
- защиту от вредоносных программ и бесфайловых атак;
- предотвращение кражи учётных данных.

Check Point признана ведущим игроком на глобальном рынке современных технологий обеспечения безопасности конечных устройств.

Если вас заинтересовало решение, обращайтесь по адресу checkpoint@mont.ru

---

Dr. Web Enterprise Security Suite – централизованная защита всех узлов корпоративной сети, включающая следующие продукты:

- Dr. Web Desktop Security Suite – защита рабочих станций, клиентов встроенных систем, клиентов терминальных серверов;
- Dr. Web Server Security Suite – защита файловых серверов и серверов приложений (в том числе терминальных и виртуальных серверов);
- Dr. Web Mail Security Suite – фильтрация почты на вирусы и спам;
- Dr. Web Gateway Security Suite – фильтрация интернет-трафика на вирусы и спам;
- Dr. Web Mobile Security Suite – защита мобильных устройств под управлением Android/BlackBerry.

Продукты в составе Dr. Web Enterprise Security Suite имеют сертификаты соответствия ФСТЭК России, ФСБ России и Минобороны России.

Если вас заинтересовало решение, обращайтесь по адресу drweb_request@mont.ru

kaspersky

Kaspersky Small Office Security (KSOS) – решение для обеспечения безопасности рабочих станций и мобильных устройств, а также файловых серверов предприятия малого бизнеса.

Kaspersky Endpoint Security для бизнеса «Стандартный» следит за безопасностью каждого сервера, ноутбука и мобильного устройства в сети. Решение совмещает многоуровневые технологии с гибким управлением в облаке и централизованными средствами контроля программ, веб-контроля и контроля устройств для защиты ваших конфиденциальных данных на всех рабочих местах.

Kaspersky Endpoint Security для бизнеса «Расширенный» включает все функции Kaspersky Endpoint Security для бизнеса «Стандартный», а также дополнительные возможности и технологии защиты: контроль запуска приложений на серверах, адаптивный контроль аномалий, инструменты системного администрирования, встроенное шифрование, патч-менеджмент.

Kaspersky Symphony Security – решение обеспечивает киберзащиту смешанной инфраструктуры организаций, защищает как физические, так и виртуальные среды.

Если вас заинтересовали решения, обращайтесь по адресу lk@mont.ru


INTRO

Построение SOC

SOC (Security Operations Center или Центр операций по обеспечению безопасности) представляет собой внутреннюю или внешнюю команду экспертов по ИТ-безопасности, которая 24/7 365 дней в году контролирует всю ИТ-инфраструктуру организации для обнаружения и эффективного управления инцидентами кибербезопасности в режиме реального времени. Кроме того, SOC играет главную роль в процессах выбора, управления и поддержки технологий кибербезопасности организации, одновременно анализируя данные об угрозах с целью поиска новых вариантов улучшения состояния безопасности.

МОНИТОРИНГ

Системы управления событиями и информацией о безопасности

Чтобы обеспечить кибербезопасность бизнеса, необходимо иметь обзор того, что происходит в вашей ИТ-инфраструктуре в любое время. Для этого рекомендуем внедрить программный продукт для управления информацией и инцидентами безопасности. Такая система называется Security Information and Event Management (SIEM).

Решения класса SIEM могут диагностировать состояние ИБ в режиме реального времени, реагировать на работу сетевых ресурсов и приложений.

Главная миссия этих программных продуктов – помогать компаниям быстро реагировать на кибератаки, события в системах безопасности и структурировать обрабатываемые данные, что значительно снижает разрушительное влияние уязвимостей на бизнес.

Как работает SIEM

Если сотрудник пытается войти в систему с 3-й попытки, а после сбрасывает пароль, то SIEM не отреагирует. Но если пароль вводится десятки или сотню раз, а после наступает успех, то программа берётся за дело. Система отправляет уведомление о попытке взлома корпоративного аккаунта.

Продукт анализирует журнал приложений, активность пользователей, целостность файлов, системы и журнала устройств. SIEM группирует события, чтобы потом их проанализировать.

Сотрудники могут использовать систему управления инцидентами, чтобы легко выявлять потенциальные проблемы и риски. Решение позволяет им быстро и легко анализировать активности и файлы. Благодаря этому специалисты могут дальше работать, не отвлекаясь на проблемы безопасности. Таким образом, системы SIEM могут улучшить процессы отчётности в рамках всего бизнеса.

Важно учитывать, что данные продукты неидеально идентифицируют чувствительные и нечувствительные события. Поэтому может быть трудно отличить безвредное поведение пользователя от реальной кражи конфиденциальной информации.

Возможности SIEM:

- агрегировать данные из технологической инфраструктуры компании и хранить их для проведения расследований инцидентов;
- анализировать угрозы, объединяя внутренние сведения с аналитическими данными;
- оповещать о потенциальных проблемах. Чтобы выявлять отклонения, система использует статистические модели и машинное обучение;
- оперативно реагировать на события нарушения информационной безопасности;
- автоматизировать сбор данных о соответствии и создавать отчёты по различным стандартам таким, как HIPA, HITECH, GDPR и т.д.

Как внедрить SIEM в инфраструктуру компании

Первым делом после покупки системы управления событиями и информацией о безопасности необходимо настроить программное обеспечение под потребности вашего бизнеса. Продукт имеет стандартные настройки, но ваши специалисты при необходимости могут их изменить под запросы компании. Важно следить за соблюдением требований конкретной организации. Программное обеспечение SIEM отлично справляется с этой задачей.

Также обязательно уделите внимание проверке функционирования продукта. Протестируйте, как система реагирует на события информационной безопасности. И конечно же нужно прописать инструкцию для персонала, как ему действовать после оповещения о потенциальных рисках и проблемах.

Плюсы использования SIEM:

- снижаются расходы на обучение сотрудников служб безопасности;
- повышается производительность труда специалистов ИТ/ИБ при увеличении количества наблюдаемых средств защиты;
- автоматизируется анализ уровня безопасности и создания отчётов в соответствии с действующими отраслевыми и международными стандартами и нормативами;
- минимизируются риски возникновения угроз информационной безопасности благодаря оперативному их выявлению и реагированию;
- сокращаются простои рабочих процессов в результате сбоев;
- проводится своевременная и объективная оценка эффективности имеющихся средств защиты за счёт анализа причин возникновения инцидентов ИБ;
- данные о событиях и инцидентах хранятся централизованно в системе ИБ.

Как правильно подобрать решение SIEM

При выборе продукта нужно обращать внимание, насколько он может интегрироваться со сторонними источниками информации о рисках для более точного обнаружения угроз.

Хорошее решение должно уметь быстро и качественно выдавать отчёты и визуальные корреляции. Система управления инцидентами должна контролировать доступ к корпоративным критическим ресурсам и проверять подозрительное поведение пользователя или попытки удалённого входа в систему. От правильности выбора продукта SIEM зависит кибербезопасность всего бизнеса.

positive technologies

MaxPatrol SIEM – система мониторинга событий ИБ и выявления инцидентов в реальном времени. Система обрабатывает до 35 тысяч событий в секунду (EPS) и автоматически выявляет известные и новые виды угроз. Служба ИБ моментально получает уведомления об инцидентах, что помогает оперативно среагировать на атаку и предотвратить репутационный и финансовый ущербы.

Если вас заинтересовало решение, обращайтесь по адресу pt@mont.ru

RUSIEM

RuSIEM – система класса SIEM, включающая корреляцию в режиме реального времени, визуализацию данных и поиск по ним, долгосрочное хранение сырых и нормализованных событий, инцидент-менеджмент и отчёты. Решение обладает высокой производительностью (обработка свыше 90000 событий на одну ноду), оно интегрировано с ГосСОПКА и сертифицировано ФСТЭК РФ.

RuSIEM Analytics – дополнительный модуль с возможностями AI (artificial intelligence), DL (data learning), визуализации данных, управления активами и множеством других, способствующих обнаружению угроз и аномалий, решающих различные кейсы с помощью современных методик.

Если вас заинтересовало решение, обращайтесь по адресу rusiem@mont.ru

kaspersky

Kaspersky Unified Monitoring and Analysis Platform (KUMA) – единая платформа безопасности для обнаружения, анализа, реагирования на современные сложные угрозы, объединяющая как решения ЛК, так и сторонние; единое окно для всех событий всей информационной инфраструктуры от источников, которые подключены к системе.

Если вас заинтересовало решение, обращайтесь по адресу lk@mont.ru

UserGate

UserGate Log Analyzer сочетает в себе функции SIEM и IRP (Incident Response Platform – реагирование на инциденты безопасности). Это предоставляет пользователям возможности сбора логов и событий, поиска инцидентов и реагирования на них. Решение позволяет:

- проводить оценку состояния информационной безопасности компании;
- мониторинг событий безопасности в реальном времени и расследование инцидентов;
- ретроспективный анализ событий безопасности, хранение и резервирование данных.

Если вас заинтересовало решение, обращайтесь по адресу usergate@mont.ru

GIS ГАЗИНФОРМ СЕРВИС

Ankey SIEM – система для централизованного управления безопасностью, событиями и информацией; эффективно и оперативно решает задачу выявления атак и инцидентов, анализирует и управляет событиями информационной безопасности всей ИТ-инфраструктуры. Система анализирует каждый вход в систему и выход из неё, доступ к ресурсам, запросы к базе и транзакции.

Комплексное применение основных и дополнительных компонентов Ankey SIEM обеспечивает эффективное управление событиями и подозрениями на инциденты информационной безопасности, позволяет выполнять расширенный событийный анализ, а также помогает контролировать соблюдение нормативных требований и стандартов в области безопасности информации.

Если вас заинтересовало решение, обращайтесь по адресу gis@mont.ru

Эшелон комплексная безопасность

KOMRAD Enterprise SIEM – гибкая и производительная система централизованного управления событиями информационной безопасности, совместимая с отечественными средствами защиты информации, позволяет осуществлять централизованный сбор событий ИБ, выявлять инциденты ИБ и оперативно на них реагировать. KOMRAD позволяет отправлять данные о событиях и инцидентах ИБ во внешние системы (например, ГосСОПКА).

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

Автоматизированное решение проблем кибербезопасности

Любая уважающая себя компания с серьёзной ИТ-инфраструктурой должна совершенствовать свою информационную безопасность. Особенно это важно, если у организации есть солидная доля цифровых активов. Чтобы их сохранить, нужно не просто отражать атаки хакеров, но и постоянно улучшать систему защиты ИБ. Для этого необходимо расследовать инциденты и грамотно реагировать на потенциальные риски и опасности.

Только проведя качественный анализ действий злоумышленников, можно выбрать правильную стратегию по укреплению безопасности вашей ИТ-инфраструктуры. Концепция Security Orchestration, Automation and Response поможет решить эту задачу. Она предназначена для «оркестровки» эффективности средств защиты ИБ, автоматизации купирования нападений и работы над ошибками после отражённых и пропущенных атак.

В частности, продукты SOAR собирают данные о событиях безопасности из разных источников, анализируют их и автоматизируют генерацию типовых решений по реагированию на возникающие проблемы.

Возможности и функции SOAR-решений

SOAR-системы объединяют в себе несколько защитных продуктов, тем самым они избавляют специалистов от необходимости управлять каждым из них в отдельности и помогают концентрироваться на решении более сложных проблем ИБ.

SOAR могут агрегировать и обрабатывать сведения о потенциальных рисках и угрозах из таких источников, как SIEM-решения, антивирусы, DLP-продукты, платформы для анализа угроз, система для анализа поведения пользователей, межсетевые экраны, службы каталогов оперативной системы.

Данные решения позволяют качественно проанализировать события кибербезопасности благодаря автоматизированным инструментам. Они дополняют сведения об инциденте информацией из сторонних баз, записей об аналогичных проблемах безопасности и других источников. На основании этого SOAR диагностирует состояние программных ресурсов компании, вычисляет подозрительные действия в системе, ранжирует их по степени риска и уведомляет о них специалистов. В определённых случаях программа изолирует вредоносные устройства, чтобы остановить дальнейшее их заражение, или принимает другие ответные решения в зависимости от политики компании.

После анализа инцидента SOAR пытается устранить угрозу или минимизировать её последствия. Для этого система может дать команду другим продуктам информационной безопасности, дистанционно удалить вредоносный объект, восстановить ключ реестра или выполнить другие необходимые для решения проблемы действия.

Для удобства расследования событий кибербезопасности некоторые продукты SOAR могут визуализировать данные в виде таблиц и диаграмм, которые обновляются в режиме реального времени. Эти отчёты содержат информацию о подозрительных действиях по подразделениям компании, конечным точкам, программным продуктам или конкретным сотрудникам.

Разница между SOAR и SIEM

Решения для управления событиями и информацией о безопасности во многом похожи на SOAR-системы. Из-за этого одно понятие иногда подменяется другим. Но между ними есть большая разница: в то время как SIEM-решения нацелены на сбор информации и ручное управление инцидентами, SOAR-системы рассчитаны на автоматизацию и оркестровку работы нескольких различных систем информационной безопасности, в частности на этапе реагирования. В результате SIEM-решения отлично дополняют SOAR в качестве источника информации о событиях.

Перспективы развития SOAR-продуктов

SOAR-системы позволяют специалистам быть на равных условиях с хакерами в борьбе за кибербезопасность. Злоумышленники используют автоматизированные инструменты и действуют благодаря им быстро и чётко. Ручная работа с инцидентами – это всё равно, что сражаться шашкой против танков. Такая защита может отреагировать только на уже совершённую атаку. Пока оператор будет разбираться в произошедшем, мошенник успеет нанести непоправимый ущерб инфраструктуре компании. Именно поэтому SOAR-решения так нужны бизнесу, чтобы эффективно бороться с киберугрозами.

Рынок SOAR достаточно молодой, эти продукты начали пользоваться спросом только в последние несколько лет. Игроков на нём пока немного, хотя уже появляются и российские решения. Тем не менее актуальность инструментов для автоматизации процессов реагирования на события безопасности в ближайшем будущем будет только расти.

R-Vision

R-Vision SOAR – система оркестрации, автоматизации ИБ и реагирования на инциденты, которая агрегирует данные по инцидентам из множества источников, автоматизирует обогащение, реагирование и внедрение защитных мер, обеспечивает единое пространство для совместной работы ИБ-специалистов.

Если вас заинтересовало решение, обращайтесь по адресу rvision@mont.ru

UserGate

Набор продуктов UserGate SUMMA позволяет реализовать комплексное решение SIEM+IRP+SOAR.

UserGate Client – программное обеспечение класса Endpoint Detection & Response (EDR) для конечных устройств. UserGate Client обеспечивает видимость событий безопасности, контроль и сетевой доступ с нулевым доверием (Zero Trust Network Access). Программный продукт централизованно развёртывается на тысячах устройств, осуществляет сбор логов, журналов и отчётов для SIEM-системы UserGate Log Analyzer, позволяет быстро и безопасно подключаться к корпоративным сетям по VPN-туннелям, обеспечивает запись и хранение информации о сетевой активности и действиях пользователей в конечных точках.

UserGate LogAn собирает данные со всех продуктов экосистемы безопасности UserGate SUMMA и сторонних устройств и отправляет уведомления в UserGate Management Center, который, в свою очередь, посылает управляющие команды в UserGate NGFW и UserGate Client для оперативного реагирования на события безопасности (SOAR).

Если вас заинтересовало решение, обращайтесь по адресу usergate@mont.ru

Расширенное обнаружение и нейтрализация угроз

Традиционные антивирусы давно перестали справляться с изощрёнными мошенническими схемами, поэтому компании переходят на продвинутые средства защиты. Такие системы не только гарантируют информационную безопасность инфраструктуры, но и собирают данные из журналов безопасности, логи сетевых устройств, а также получают сведения от антивирусов.

Чтобы обрабатывать эту информацию, крупные организации создают отдельное подразделение – Security Operation Center (SOC). Специалисты SOC анализируют подозрительные действия, выявляют и расследуют инциденты, ищут способы предотвратить и остановить нелегальные вторжения в систему.

Относительно недавно разработчики представили новый перспективный класс решений, который благодаря комплексному подходу позволяет оперативно и легко противостоять сложным кибератакам. Эти решения называли XDR – eXtended Detection and Response, что переводится как расширенное выявление и реагирование.

Что такое XDR

Понятие XDR появилось в итоге эволюции концепции Endpoint Detection and Response. Этот подход означает «выявление и реагирование на конечных точках». EDR при работе концентрировался лишь на конечных точках, таких как ноутбуки и рабочие станции. Но мошенники могут атаковать и другие объекты ИТ-инфраструктуры компании, например серверы, устройства Интернета, облачные системы и т.д. В связи с этим и появился новый модернизированный инструмент XDR, который расширяет функциональность реагирования на инциденты и выходит за пределы конечных точек. Это решение интегрируется с другими средствами защиты ИБ, за счёт чего позволяет реагировать на проблемы безопасности, используя сетевые устройства, электронную почту, системы управления учётными записями и др.

Как подобрать эффективный XDR-продукт

В первую очередь при покупке XDR обратите внимание на способность решения интегрировать с другими программными продуктами ИБ. XDR должен идеально работать в вашем стеке безопасности, используя нативные инструменты с функциональным API. Важна также глубина готового функционала по корреляции событий, предотвращению и реагированию на атаки между разными защитными программами и приложениями. Кроме того, аналитики должны иметь возможность использовать этот движок, чтобы писать собственные межстековые пользовательские правила для обнаружения и реагирования на атаки. Избегайте недоработанных продуктов, которые могут оказаться простым набором старых инструментов с новым названием.

Хороший XDR должен представлять собой единую платформу, которая позволит быстро и легко составить объективную картину обо всём происходящем в вашей ИТ-инфраструктуре.

При выборе XDR важна автоматизация его инструментов. Проверьте, имеет ли ваш поставщик ПО богатый опыт разработки моделей искусственного интеллекта.

Убедитесь, что решение легко внедряется в ваш бизнес. Продукт должен повышать производительность персонала благодаря автоматизации процесса обнаружения и реагирования.

Как внедрить XDR

1. *Определите потребность в хранении данных.*

Прежде чем настраивать XDR-системы под свой бизнес, определите, какая функциональность вам нужна в плане ведения журналов и данных телеметрии. Так вы сможете понять, сколько места потребуется для хранения информации.

2. *Спланируйте поэтапное развёртывание решения.*

Настройте набор служб для интеграции с XDR-системой, и только потом распространите интеграцию на всю технологическую среду.

3. *Проанализируйте базовые данные.*

Чтобы увеличить эффективность XDR-инструментов, оцените их базовые данные. Это позволит добиться точных показателей системы.

Заключение

Борьба между хакерами и защитниками давно вышла за пределы конечных точек. Удалённая работа и облачная инфраструктура только увеличивают пространство для кибератак. Поэтому лишь интегрированная система способна дать информационным ресурсам компаний качественный мониторинг и автоматическую защиту. XDR объединяет телеметрии конечных точек, сети и приложений и создаёт аналитические отчёты о состоянии ИБ. Это позволяет специалистам по безопасности эффективнее и быстрее реагировать на атаки.

F.A.C.C.T.

Managed Extended Detection and Response (Managed XDR) предназначен для нейтрализации постоянно усложняющихся угроз, проактивный поиск недетектируемых угроз в инфраструктуре, противодействие атакам в режиме реального времени и максимально быстрое реагирование в случае инцидента. Решение состоит из нескольких компонентов, основанных на передовых средствах и технологиях защиты.

- Защита конечных станций и реагирование (EDR) – выявление вредоносной активности на хостах с возможностью расширенного реагирования.
- Анализ сетевого трафика (NTA) – выявление вредоносной активности, аномалий и скрытых каналов в сетевом трафике, а также анализ и атрибуция угроз. Защита корпоративной почты (BEP) – защита корпоративной электронной почты, размещённой в облаке или локально. Решение детонирует и анализирует подозрительные вложения и ссылки в изолированной среде, выявляя и блокируя атаки до того, как они достигнут своей цели.
- Детонация вредоносного ПО (MDP) – платформа детонации вредоносных программ запускает подозрительные файлы и ссылки в виртуальной среде для углублённого анализа, обнаружения угроз, извлечения индикаторов и атрибуции атак.

Если вас заинтересовало решение, обращайтесь по адресу gib@mont.ru

CHECK POINT

Horizon XDR/XPR обеспечивает быстрое обнаружение угроз, их исследование и автоматическое реагирование в масштабе всей ИТ-инфраструктуры, включая сеть, облачную среду, рабочие станции, мобильные устройства и электронную почту с единой панели.

Основываясь на применении искусственного интеллекта и кросс-корреляции, XDR/XPR обеспечивает автоматическое предотвращение атак, не допуская их быстрого распространения в вашей среде.

Если вас заинтересовало решение, обращайтесь по адресу checkpoint@mont.ru

kaspersky

Kaspersky Symphony XDR сочетает в себе всё, что нужно команде ИБ. Мощная технология EDR в синергии с базовой защитой конечных точек, а также комплексный мониторинг, анализ сетевого трафика, защита почты, «песочница» и другие технологии помогают противодействовать кибератакам. В решении используется лучшая в мире аналитика об угрозах (Threat Intelligence) это по результатам отчётов Forrester Wave – External Threat Intelligence Services 2021. Решение помогает соответствовать требованиям регуляторов (например, в сфере безопасности объектов КИИ) благодаря встроенному модулю ГосСОПКА и другим компонентам.

Если вас заинтересовало решение, обращайтесь по адресу lk@mont.ru

UserGate

Набор продуктов UserGate SUMMA позволяет реализовать комплексное решение SIEM+IRP+SOAR.

UserGate Client – программное обеспечение класса Endpoint Detection & Response (EDR) для конечных устройств. UserGate Client обеспечивает видимость событий безопасности, контроль и сетевой доступ с нулевым доверием (Zero Trust Network Access). Программный продукт централизованно развёртывается на тысячах устройств, осуществляет сбор логов, журналов и отчётов для SIEM-системы UserGate Log Analyzer, позволяет быстро и безопасно подключаться к корпоративным сетям по VPN-туннелям, обеспечивает запись и хранение информации о сетевой активности и действиях пользователей в конечных точках.

UserGate LogAn собирает данные со всех продуктов экосистемы безопасности UserGate SUMMA и сторонних устройств и отправляет уведомления в UserGate Management Center, который, в свою очередь, посылает управляющие команды в UserGate NGFW и UserGate Client для оперативного реагирования на события безопасности (SOAR).

Если вас заинтересовало решение, обращайтесь по адресу usergate@mont.ru

Защита от кибермошенничества

Сегодня каждое четвёртое преступление в России совершается с применением информационно-коммуникационных технологий, согласно статистике Министерства внутренних дел РФ. Причину повышенной активности кибермошенников можно легко объяснить тем, что онлайн-операции на сайтах и в мобильных приложениях – это как практичная функция для пользователей, так и возможность кросс-канальных атак для мошенников. Но вот вопрос: как и какие ИТ-решения смогут обеспечить защиту от кибермошенничества?

Системы обнаружения мошенничества

Борьбой с преступностью в Интернете сегодня занимаются невидимые борцы за справедливость – системы обнаружения и предотвращения цифрового мошенничества антифрод-системы. Обычно они состоят из систем:

- обнаружения мошенничества *(Fraud Detection)*;
- предотвращения мошенничества *(Fraud Prevention)*;
- анализа *(Fraud Analysis)*.

Кому нужна антифрод-система

Первый ответ, который приходит на ум, – банкам. Ответ верный, но далеко не полный. Антифрод актуален в любой сфере, где происходят транзакции денежных средств, процессы товарообмена онлайн.

Как антифрод защищает бизнес

Антифрод-система оценивает транзакцию, присваивает ей статус и сообщает платёжной системе. Все действия происходят за несколько секунд: обычные покупатели ничего не замечают, а мошенникам приходится изменить свои планы и отказаться от затеи похищения средств.

Что ещё могут антифрод-системы

Анализируют транзакции, истории покупок пользователя, присваивают метку платёжной системе (а далее она решает, что делать с платежом).

Что такое Fraud Prevention и как это работает

Мониторинг, обнаружение и управление уровнем фрода – это то, чем занимается программный комплекс Fraud Perevention. Его главная цель – защита компании от финансовых и репутационных рисков.

Программный комплекс Fraud Prevention устроен так, чтобы его действия были оперативными, последовательными и эффективными. Работа всегда идёт в режиме реального времени с использованием обработки трафика по следующим параметрам: устройство – пользователь – онлайн-пользователь – обработанное событие.

Борьба с кросс-канальными атаками в работе системы проводится в несколько шагов.

Первый шаг – *анализ устройства и окружения пользователя*. Сначала система проводит сбор данных, на основе которых делает вывод, относится ли действие пользователя к мошенничеству. Например, через анализ IP-адреса и данных геопозиции система может определить и отобразить фрод.

Второй шаг – *анализ поведения пользователя и сбор базы ответов на вопросы: как пользователь ведёт себя при входе в личный кабинет и во время всей сессии*. Этот этап является важным, так как включает в себя не только сбор информации, но и составление портрета пользователя в режиме его привычных действий. Так можно выявить подозрительную активность и действия во время сессии, которые не характерны для пользователя.

Третий шаг – *обнаружение угроз и вредоносных программ*. К ним относятся боты, кибератаки, активация вредоносного программного обеспечения. Например, выявив отклонения от поведенческой биометрии пользователя, программный комплекс Fraud Perevention может остановить совершение действий, тем самым предотвратить кибермошенничество.

Как он это будет делать

- с помощью ограничения количества транзакций за определённую единицу времени;
- через ограничение суммы единоразового платежа или перевода;
- с использованием двухфакторной аутентификации и/или биометрии.

Современные системы защиты от кибермошенничества – это не новомодное веяние ИТ-сферы, а эффективный инструмент для защиты денежных средств компаний и их клиентов. Для наглядности можно представить, что любая компания, которая ежедневно проводит денежные транзакции, потенциально подвержена кибератаке. В таком случае тандем компании с антифрод-системой облегчит задачу при совершении денежных переводов, хранении персональных данных, поддержке продаж и увеличении доходов.

F.A.C.C.T.

Fraud Protection – инновационное решение для выявления, предупреждения и устранения мошенничества в режиме реального времени во всех цифровых каналах. Fraud Protection использует Preventive Proxy – патентованную технологию для выявления всех типов бот-атак (скрапинг данных, брут-форс-атаки, нелегитимное использование API и т. д.).

Если вас заинтересовало решение, обращайтесь по адресу gib@mont.ru

kaspersky

Kaspersky Fraud Prevention – защита от мошенничества в мобильном и онлайн-банкинге. Платформа в режиме реального времени анализирует поведение, устройства и окружение пользователя, а также с помощью машинного обучения выявляет продвинутые схемы мошенничества, связанные с хищением данных пользователей и отмыванием денег.

Если вас заинтересовало решение, обращайтесь по адресу lk@mont.ru

MONITORING

Защита виртуальных и облачных сред

Виртуализация и перенос инфраструктуры в облако, полный или частичный, – это реальность компаний, которые стремятся к модернизации процессов и эффективности в работе. Этот подход открывает новые возможности для развития бизнеса, но в то же время он подвергает компании киберрискам. Что нужно сделать, чтобы переход в виртуальные и облачные среды происходил без утечки информации и негативных последствий? В ИТ-сфере есть чёткий ответ: использовать специализированные программные средства для защиты информации.

Возможности систем защиты виртуальных и облачных сред

Цифровая трансформация современного бизнеса требует освоения облачных технологий. Именно эту роль берут на себя системы защиты виртуальных и облачных сред, потому что они выполняют следующие задачи:

- обеспечивают надёжную защиту на всех этапах цифровой миграции;
- учитывают всевозможные сценарии развёртывания и комбинации физических, виртуальных и облачных инфраструктур;
- оказывают минимальное воздействие на скорость работы системы и обеспечивают её надёжную многоуровневую защиту;
- помогают эффективно защищать виртуальные и облачные среды, позволяют управлять ИТ-инфраструктурой и обеспечивают её прозрачность, не мешая работе пользователей.

Системы защиты виртуальных и облачных сред противодействуют широкому спектру киберугроз, в том числе фишингу, шифровальщикам и другому вредоносному ПО. Кроме того, они удобны в использовании и оптимизации процессов с момента развёртывания технологий, ориентированных на бизнес.

Последствия кибератак на облачные хранилища

При атаке на облачные системы, которые не защищены должным образом, последствия могут быть печальными: потеря данных и вред для репутации компании. И, несмотря на то, что поле угроз постоянно меняется, публичное облако должно быть защищено не хуже, чем частное. В ином случае под ударом окажутся самые ценные данные – конфиденциальная информация о сотрудниках, проектах и бизнес-процессах.

Как работает облачная безопасность

Сложное взаимодействие технологий, элементов управления, процессов и стратегий в комплексе формируют и поддерживают надёжное хранение данных. Облачная безопасность достигается и поддерживается с использованием особых инструментов, таких как:

- система управления идентификацией и доступом;
- физическая безопасность – комбинация мер по предотвращению прямого доступа и сбоев в работе оборудования, размещённого в центре обработки данных вашего облачного провайдера;
- анализ угроз, мониторинг и предотвращение вторжений предоставляют функциональные возможности для идентификации злоумышленников, которые в настоящее время нацелены на ваши системы или будут представлять угрозу в будущем;
- шифрование гарантирует, что данные практически невозможно раскодировать без ключа дешифрования. Доступ к нему есть только у пользователя;
- облачные уязвимости и тестирование на проникновение – выявление любых потенциально слабых мест или эксплойтов, а также внедрение решений для исправления этих уязвимостей и улучшения позиции безопасности;
- микросегментация – разделение облачного развёртывания на отдельные сегменты безопасности, вплоть до индивидуального уровня рабочей нагрузки. Изолируя отдельные рабочие нагрузки, можно применять гибкие политики безопасности, чтобы свести к минимуму любой ущерб, который может нанести злоумышленник;
- брандмауэры нового поколения защищают рабочие нагрузки, используя традиционную функциональность и новые расширенные функции.

Если вы всё ещё размышляете о внедрении облачных технологий и виртуальных сред в рабочее пространство, вспомните о растущем объёме киберугроз, и у вас не останется сомнений. Внедрение системы защиты информации виртуальных и облачных сред, как талисман защищает компании и пользователей от репутационных, финансовых и юридических последствий утечек и потери данных. А выбор правильного провайдера повысит безопасность вашей ИТ-инфраструктуры и снизит риски информационной безопасности компании.

CHECK POINT

Check Point CloudGuard обеспечивает унифицированную нативную безопасность облачной среды, для всех ресурсов и рабочих нагрузок в мультиоблачной среде, обеспечивая:

- интеллектуальное предотвращение угроз как на локальном уровне, так и в облачной среде с помощью унифицированной платформы обеспечения защиты Check Point Infinity;
- надёжная защита и предотвращение угроз для AWS, Azure, Google Cloud, Cisco ACI, VMWare NSX, Ali и Oracle;
- централизованную визуализацию всего вашего облачного трафика, оповещения о нарушении безопасности, а также автоматическое устранение нарушений.

Если вас заинтересовало решение, обращайтесь по адресу checkpoint@mont.ru

КОД безопасности

vGate – средство микросегментации и защиты жизненного цикла виртуальных машин в средах VMware, Microsoft Hyper-V и платформе Скала-Р. Корреляция событий vGate и среды виртуализации выявляет несанкционированную активность и позволяет обнаружить инцидент до того, как он приведёт к разрушительным последствиям. Осуществляет контроль жизненного цикла виртуальных машин и целостности «золотых» шаблонов. Защищает хранилища и консоли от доступа администратора среды.

По вопросам, связанным с решениями «Код Безопасности», обращайтесь по адресу kb@mont.ru

Защита автоматизированной системы управления технологическим процессом

Защита АСУ ТП – одна из трендовых тем, которая сегодня вызывает интерес у ИТ-специалистов как в России, так и за рубежом. Почему? Ответ прост: во-первых, на защиту АСУ ТП раньше обращали мало внимания, во-вторых, атаки на промышленные предприятия могут нанести огромный ущерб и экономике, и экологии.

Автоматизированная система управления технологическим процессом (АСУ ТП) – *это совокупность аппаратных и программно-аппаратных средств и систем, которые применяются в промышленности для повышения эффективности и безопасности производственных процессов предприятия, а также улучшения качества его конечного продукта.*

Безопасность АСУ ТП зависит от способности системы обеспечивать непрерывный технологический процесс независимо от влияния внешних факторов. Технологический процесс определяется сферой деятельности объекта, например предприятие занимается металлообработкой, производством удобрений или добычей воды. Учитывая высокую важность непрерывного функционирования объектов, нам становится понятно, почему защита информационной системы является такой значимой задачей. В обеспечении безопасности производства любой отрасли ИТ-специалистами выработаны основные принципы и подходы к построению систем защиты информации. В статье мы собрали ответы на самые популярные вопросы о программно-аппаратных решениях для защиты информации АСУ ТП от кибератак на промышленные предприятия.

Что увеличивает вероятность кибератаки

Наличие подключения промышленной сети к корпоративной может оказать мошенникам добрую услугу для совершения атаки. Чаще всего злоумышленники используют такие недостатки безопасности, как незащищённые каналы администрирования или недостаточно эффективную сегментацию. Также не стоит забывать и о тенденции удалённой работы, которой сопутствует поддержка удалённого доступа к сетевым каналам предприятия. Преимущества удалённой работы видят не только ваши сотрудники, но и киберпреступники, ведь это увеличивает их шансы вывести из строя информационную безопасность инфраструктуры.

Как происходит внедрение системы информационной защиты АСУ ТП

Первым этапом проводится оценка технологического процесса и сбор данных, необходимых для разработки и подбора средств защиты важной информации.

Второй этап – моделирование сценариев негативного воздействия на систему управления, которые учитывают особенности производственного процесса предприятия, а также инновационные технологические возможности, которыми может обладать злоумышленник.

Третий этап – разработка стандартов, которым должны соответствовать системы информационной защиты.

Четвёртый этап – это проектирование эффективной защиты автоматизированных систем управления, которая при этом не будет оказывать неблагоприятное воздействие на ход технологического процесса.

Пятый этап – согласование проекта и тестирование в реальных условиях.

Заключительный и самый важный шестой этап – внедрение системы информационной защиты.

Как работает информационная защита АСУ ТП

Работа защиты АСУ ТП можно представить в форме пирамиды. В её основании лежит *прогнозирование*. Так, исходя из текущих возможностей предприятия оцениваются риски и вырабатывается наиболее подходящая стратегия защиты.

Второй пласт пирамиды – *предотвращение*. В него входит профилактика уже известных угроз путём развёртывания и внедрения защитных решений, переобучения и мотивации персонала объекта, разработки новых и обновления существующих политик безопасности предприятия, сегментирования информационной инфраструктуры.

Третий пласт пирамиды защиты АСУ ТП – *обнаружение*. Данный этап предполагает активный контроль и мониторинг сетевой инфраструктуры и критически важных узлов предприятия с целью обнаружить и сдержать кибератаку.

Вершину пирамиды занимает *реагирование*. Этот процесс можно разделить на пару последовательных действий. Сначала происходит реакция систем безопасности на инцидент и включаются процессы, позволяющие минимизировать тяжесть последствий кибератаки, затем начинается расследование произошедшего.

Какие системы информационной защиты АСУ ТП работают эффективно

Среди множества систем, которые предназначены для промышленных предприятий, мы выбрали несколько функциональных и готовы поделиться с вами подборкой программных комплексов для защиты от киберугроз.

kaspersky

Kaspersky Industrial CyberSecurity (KICS) – комплексный подход к защите индустриальных сетей промышленных объектов от киберугроз, обеспечивающий безопасность производственных процессов и поддержание их непрерывности, оперативное устранение сбоев. Включает несколько продуктов, в частности KICS for Nodes защищает промышленные рабочие места, KICS for Networks следит за безопасностью промышленных сетей, Kaspersky ICS Threat Data Feeds предоставляет вредоносные хэши.

Защитные решения отвечают требованиям государственных и отраслевых регуляторов, проектных организаций и интеграторов. Широкие возможности настройки KICS позволяют сконфигурировать решение в точном соответствии с требованиями конкретного промышленного объекта.

Если вас заинтересовало решение, обращайтесь по адресу lk@mont.ru

positive technologies

PT Industrial Security Incident Manager (PT ISIM) – программно-аппаратный комплекс глубокого анализа технологического трафика. Обеспечивает поиск следов нарушений информационной безопасности в сетях АСУ ТП, помогает на ранней стадии выявлять кибератаки, активность вредоносного ПО, неавторизованные действия персонала (в том числе злоумышленные) и обеспечивает соответствие требованиям законодательства (187-ФЗ, приказы ФСТЭК № 31, 239, ГосСОПКА).

Если вас заинтересовало решение, обращайтесь по адресу pt@mont.ru

CHECK POINT

Quantum – высокопроизводительные масштабируемые шлюзы безопасности для дата-центров и крупных корпораций, обеспечивающие наилучшее предотвращение угроз и оптимизацию для гибридных облачных сред. Шлюзы Quantum Security Gateways™ 26000 и 28000 Check Point включают отмеченное наградами решение предотвращения угроз SandBlast Network, обладают высокой надёжностью и имеют высокую скорость предотвращения угроз – до 1,5 Тбит/сек.

Если вас заинтересовало решение, обращайтесь по адресу checkpoint@mont.ru

INFOWATCH

InfoWatch ARMA Industrial Firewall – промышленный межсетевой экран нового поколения (NGFW). Помимо функции межсетевого экранирования, обладает встроенной системой обнаружения вторжений с базой решающих правил СОВ для АСУ ТП и ГОСТ-VPN. Предоставляет полную информацию о событиях безопасности в промышленной сети и позволяет детально работать с трафиком. Определяет протоколы на основе содержания пакетов промышленного трафика, а не только номера порта. Позволяет фильтровать протоколы по полям до уровня отдельных команд и их значений. Вы можете запрещать или разрешать отдельные команды по протоколам, усиливая защиту специфических АСУ ТП.

Если вас заинтересовало решение, обращайтесь по адресу informprotect@mont.ru

КОД безопасности

«Континент 4» – многофункциональный межсетевой экран (NGFW/UTM) с поддержкой алгоритмов ГОСТ. Система обнаружения и предотвращения вторжений может работать в «невидимом» для сети режиме, детально настраивается и активируется только для необходимого трафика. Система контроля приложений работает на основе базы более 2600 приложений. Механизм поведенческого анализа трафика не использует сигнатуры, а построен на основе механизмов машинного обучения, позволяет обнаруживать злоумышленника и предотвращать DoS-атаки.

Модельный ряд «Континент 4» позволяет подобрать решение для защиты как больших корпоративных сетей, так и небольших организаций. Различаясь производительностью, все аппаратные исполнения обладают полным функционалом защитных механизмов, реализованных в «Континент 4».

По вопросам, связанным с решениями «Код Безопасности», обращайтесь по адресу kb@mont.ru

UserGate

Семейство программно-аппаратных комплексов User Gate позволяет обеспечивать безопасность сетей организаций любого размера, а также безопасное подключение к Интернету многочисленных устройств, управляющие уличной, транспортной, промышленной и другими инфраструктурами.

Если вас заинтересовало решение, обращайтесь по адресу usergate@mont.ru

ФАКТОР-ТС

Dionis DPS – линейка отечественных маршрутизаторов и криптомаршрутизаторов, сертифицированная по требованиям ФСТЭК и ФСБ России и соответствующая самым высоким уровням защищённости. Dionis DPS ориентирована как на коммерческий сектор, так и на государственные ведомства. На данный момент уже используется для организации безопасного информационного обмена во всех министерствах и ведомствах силового блока России, а также в других государственных учреждениях.

Если вас заинтересовало решение, обращайтесь по адресу factor@mont.ru

Зачем нужно обучать сотрудников кибербезопасности

Если сотрудники не знают, как распознать угрозу, то как они смогут её избежать, сообщить о ней или ликвидировать проблему? Логично, что никак. Вы можете вкладывать бесконечные инвестиции в средства защиты, предусмотреть все риски и изучить все уязвимости, но есть одно «НО»: человеческий фактор. Это совсем не значит, что если сотрудники вашей компании попали в ловушку мошенников, то они безответственные. Все мы люди, и можем совершать ошибки: переходить по фишинговым ссылкам, доверять фальшивым лицам, соблазняться наживкой, быть уязвимыми к другим тактикам преступников. Так происходит, потому что сотрудники не знают, как вести себя в подобных ситуациях. Их этому никто не учил.

Чтобы обезопасить компанию от кибератак, начните с обучения персонала. Ознакомив их с угрозами безопасности, порядком действий при обнаружении угрозы, вы укрепляете наиболее уязвимые звенья цепочки своего бизнеса.

Почему важно повышать цифровую грамотность персонала

90% утечек связаны не с мастерством хакеров, а с ошибками персонала. В 2022 году на российские компании было совершено 911 тысяч хакерских атак, что вдвое больше, чем год назад.

Сегодня любимая тактика мошенников – это психологическое манипулирование с целью убедить жертву добровольно или неосознанно выдать конфиденциальные данные. Также киберпреступники чаще всего прибегают к фишингу, а 30% сотрудников даже не знают, что это такое.

Угроза может прийти со стороны вредоносных файлов, которые были случайны скачаны из Интернета. С помощью этих заражённых объектов злоумышленники могут взломать корпоративные устройства и получить доступ к ценным ресурсам компании. Если научить сотрудников распознавать потенциально опасные сайты и обучить азам информационной безопасности, то этого всего можно избежать.

Удалённая работа

Пандемия COVID-19 сделала удалённую работу частью нашей новой реальности. Дистанционный формат настолько распространился, что компании вынуждены выстраивать отдельные политики в отношении сотрудников, работающих на дому. Удалённая работа повысила уровень комфорта, но в то же время добавила новых проблем кибербезопасности. Использование облачных технологий только увеличивает риск вторжений в инфраструктуру организаций. Сотрудники должны использовать офисное оборудование исключительно в корпоративных целях, чтобы не подвергать его киберопасностям. Специальное обучение даст вашему персоналу понимание, как грамотно и безопасно использовать деловые устройства за пределами компании.

Интернет вещей (IoT)

Специалисты нередко используют личные устройства для официальной работы, а также подключают их к корпоративной сети. Это только усугубляет проблемы безопасности. Самая крупная DDoS атака в истории была запущена на провайдера услуг с использованием IoT бот-сети, MIRAI.

Смартфоны чаще всего становятся причиной угроз для информационной безопасности компании, так как у них нет соответствующей защиты. С IoT-атаками можно справиться, если управлять и сводить к минимуму практику «приносимых с собой устройств» (BYOD) на рабочие места. Кроме того, необходимо стимулировать сотрудников соблюдать строгую политику безопасности.

Усиление государственных регуляций

Многие государственные нормативные акты, связанные с политикой безопасности компьютеров и сетей, подчёркивают важность обучения персонала цифровой грамотности. Государственные учреждения и законодатели призывают предприятия защищать свои ИТ-активы и ценную информацию.

Какие сотрудники должны повысить квалификацию в вопросах кибербезопасности

Ваши сотрудники – это первая и основная линия защиты от интернет-преступлений. Любой сотрудник, имеющий доступ к рабочему компьютеру или мобильному устройству, должен пройти обучение по вопросам кибербезопасности. Ведь практически кто угодно может стать мишенью. На персональных телефонах могут храниться данные, которые помогут мошенникам получить доступ к корпоративным сетям. Если сотрудник становится жертвой кражи конфиденциальной информации, эти уникальные сведения могут быть использованы для создания фейковых аккаунтов вашего бренда в корыстных целях.

phishman

PHISHMAN – система автоматизированного управления знаниями, которая, в числе прочего, тренирует сотрудников распознавать кибератаки и противостоять им. Система выявляет потребность в обучении, обучает, тестирует усвоение материала и в дальнейшем поддерживает киберграмотность на заданном уровне.

Если вас заинтересовало решение, обращайтесь по адресу phishman@mont.ru

kaspersky

Kaspersky Automated Security Awareness Platform (ASAP) – автоматизированная платформа для повышения осведомлённости о кибербезопасности – онлайн-инструмент, формирующий и закрепляющий у сотрудников компаний-клиентов навыки безопасной работы в цифровых устройствах. Продукт ориентирован на SMB-сегмент.

Если вас заинтересовало решение, обращайтесь по адресу lk@mont.ru

Антифишинг

Платформа «Антифишинг для сотрудников» помогает компаниям сформировать у сотрудников устойчивые навыки противодействия всем видам цифровых атак: через электронную почту, сайты, соцсети, мессенджеры. Для этого в состав решения входят обучающие курсы по информационной безопасности и система автоматизированной тренировки навыков с помощью имитированных атак. Платформа также позволяет и обнаружить уязвимости на рабочих местах сотрудников.

Если вас заинтересовало решение, обращайтесь по адресу antiphishing@mont.ru

Мы поможем

Российские вендоры имеют зрелые решения, закрывающие весь спектр задач информационной безопасности. Пользователь может выбирать. И это хорошо!

А в выборе подходящих решений для замены иностранного ПО или для решения новых задач по защите информации, помогут специалисты MONT.

Мы можем:

- проанализировать защищённость вашей ИТ-системы;
- порекомендовать набор продуктов для её эффективной защиты;
- провести демонстрацию решений;
- провести пилотный проект для оценки соответствия предлагаемых решений задачам заказчика, включая предоставление оборудования;
- спланировать и реализовать внедрение.

Читайте нас на www.mir.mont.com

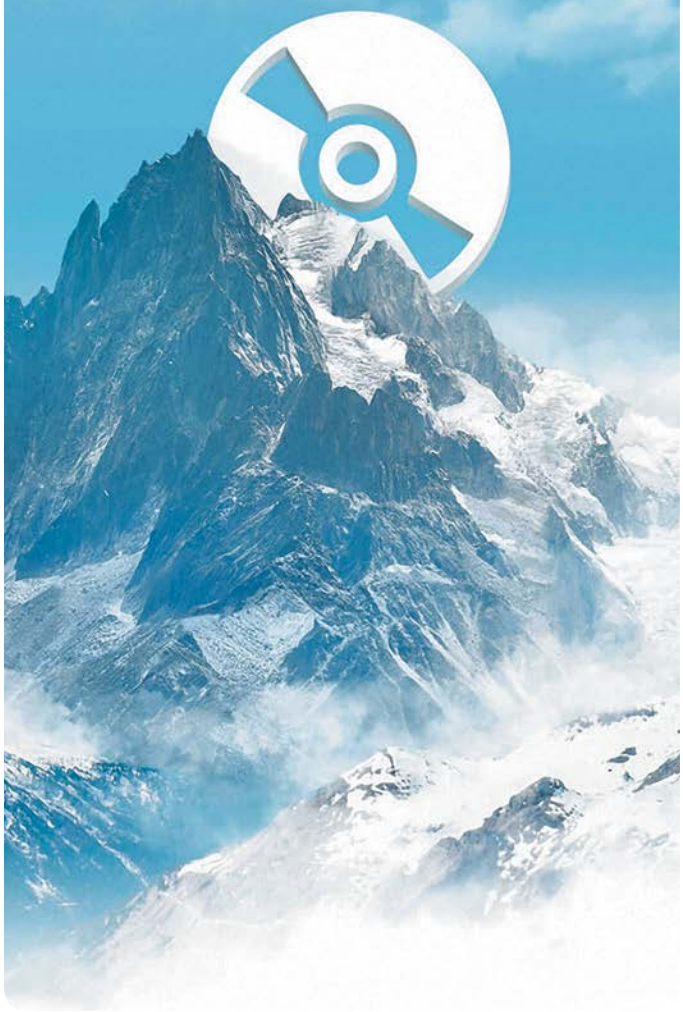
Пишите нам на imz@mont.ru

Дистрибьютор программного обеспечения для бизнеса любого масштаба

Группа компаний MONT начала свою деятельность в 1991 году и в настоящее время является одним из крупнейших в России дистрибьюторов программного обеспечения.

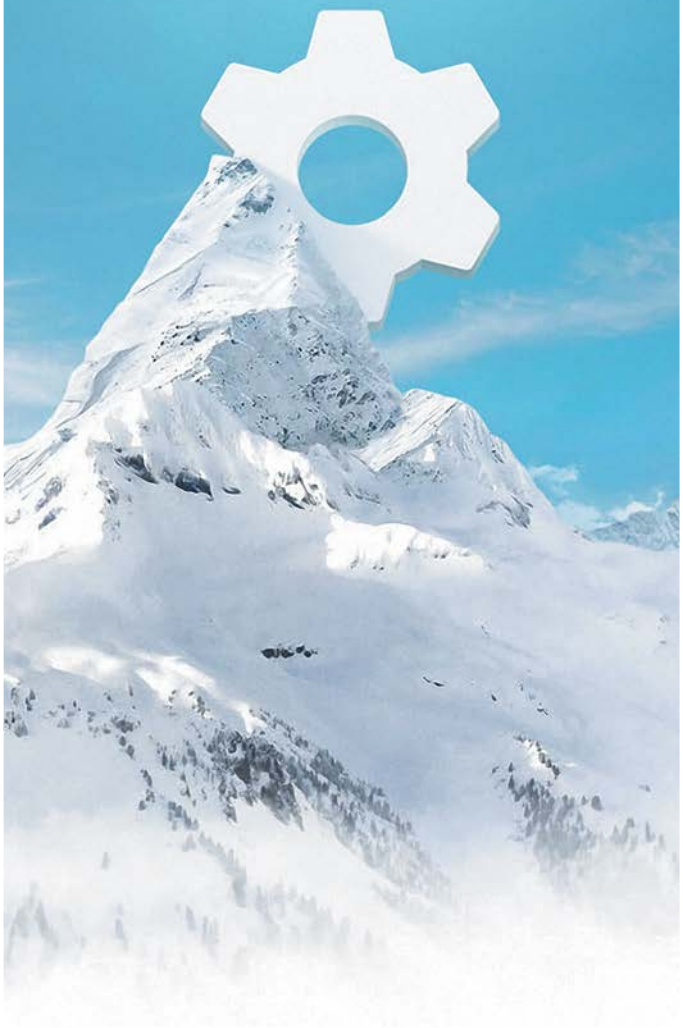
КЛАССИЧЕСКАЯ ДИСТРИБУЦИЯ

Поставка корпоративных лицензий, программно-аппаратных комплексов, «коробочных» продуктов по традиционной схеме: заказ от клиента, размещение заказа у дистрибьютора, отгрузка со склада вендора, доставка партнёру, установка у заказчика.



ЭКСПЕРТНЫЕ РЕШЕНИЯ

Поставка проверенных техническими специалистами MONT комплексных решений, а также пре-сейл, техническая и сервисная поддержка проектов.



Среди наших партнёров есть и ведущие системные интеграторы со штатом в несколько тысяч сотрудников, и небольшие компании, в которых один человек часто выполняет функции и директора, и менеджера по закупкам, и розничного продавца. Мы стремимся обеспечить одинаково высокий уровень сервиса в работе со всеми партнёрами.

MONT предлагает партнёрам:

- Помощь в генерации спроса
- Технологическую экспертизу
- Финансовую и логистическую поддержку
- Информационную поддержку
- Системы автоматизации продаж с технической поддержкой 24x7

Партнёры MONT получают в своё распоряжение:

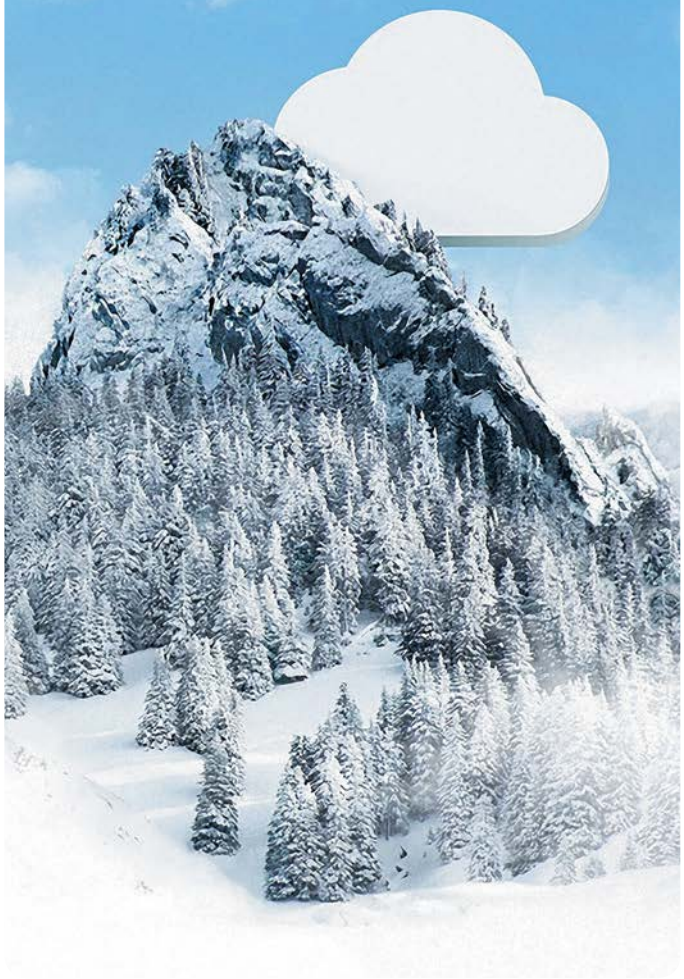
- B2B-портал для самостоятельного размещения заказов на лицензии, коробки, электронные ключи, создание заказов из лицензионных форм, а также получения информации (финансы, документы) **без участия менеджера**
- Автоматизированную платформу MONT Cloud Distribution для продажи облачных сервисов, обеспечивающую **100% контроль и управление подписками заказчиков**
- Технологическую платформу MONT Webstore для **автоматической доставки электронных ключей напрямую от поставщиков в режиме онлайн**

ЭЛЕКТРОННАЯ ДИСТРИБУЦИЯ

MONT ESD – это канал продаж программного обеспечения, позволяющий доставлять электронные ключи напрямую от вендора в режиме онлайн, посредством технологической платформы MONT.

ОБЛАЧНАЯ ДИСТРИБУЦИЯ

MONT Cloud Distribution помогает партнёрам построить и трансформировать бизнес по продаже ИТ-решений, поставляемых в виде облачных и подписных сервисов. Автоматизированная платформа обеспечивает партнёрам 100% контроль и управление подписками заказчиков.



MONT является авторизованным дистрибьютором решений российских и зарубежных поставщиков в сфере информационной безопасности, инфраструктуры, прикладного ПО, САПР и графики, а также имеет в своём портфеле комплексные решения, включающие программное и аппаратное обеспечение.

ПОРТФЕЛЬ ПОСТАВЩИКОВ **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

	КАТЕГОРИЯ	СЕТЕВАЯ БЕЗОПАСНОСТЬ							ЗАЩИТА ДАННЫХ						ПОСТРОЕНИЕ SOC						
ВЕНДОР		Антивирусы	NGFW и UTM	WAF	Защита от DDoS атак	Защита почты	Sandbox	NTA	Сканнер уязвимостей	DLP	СЗИ от НСД и МФА	СКЗИ	Privileged Access Management	Анализ исходного кода на уязвимости	Защита баз данных и файловых хранилищ	SIEM	SOAR	XDR	Защита от кибермошенничества	Защита АСУ ТП	Защита облачных и виртуальных сред	Обучение персонала защите от киберугроз
ANY.RUN							●															
Bifit Mitigator					●																	
Check Point		●	●	●		●	●			●	●							●		●	●	
F.A.C.C.T.						●	●	●										●	●			
InfoWatch			●							●										●		
Phishman																						●
Positive Technologies				●			●	●	●					●		●		●		●		
PR032		●																				
ruSIEM																●						
R-Vision																	●					
SkyDNS			●																			
StaffCop										●												
StarForce											●	●										
UserGate			●			●										●	●	●		●		
Zecurion										●					●							
Айдеко			●	●																		
Актив (Рутокен)											●											
Аладдин Р.Д.											●		●		●							

Узнать больше о портфеле программных решений для импортозамещения вы можете на сайте: mir.mont.com

		СЕТЕВАЯ БЕЗОПАСНОСТЬ							ЗАЩИТА ДАННЫХ						ПОСТРОЕНИЕ SOC						
ВЕНДОР	КАТЕГОРИЯ	Антивирусы	NGFW и UTM	WAF	Защита от DDoS атак	Защита почты	Sandbox	NTA	Сканнер уязвимостей	DLP	СЗИ от НСД и МФА	СКЗИ	Privileged Access Management	Анализ исходного кода на уязвимости	Защита баз данных и файловых хранилищ	SIEM	SOAR	XDR	Защита от кибермошенничества	Защита АСУ ТП	Защита облачных и виртуальных сред	Обучение персонала защите от киберугроз
АЛТЭКС-СОФТ (RedCheck)									●													
Антифишинг																						●
ГазИнформСервис											●	●				●						
Доктор Веб		●				●	●															
Интернет Контроль Сервер			●																			
ИТ-Экспертиза (Сакура)											●											
Киберпротект										●												
Код Безопасности			●	●							●	●								●	●	
Компания Индид											●		●									
КриптоПро											●	●										
Лаборатория Касперского		●				●	●	●	●						●	●		●	●	●	●	●
Ростелеком-Солар			●							●	●		●	●								
Смарт-Софт (Traffic Inspector)			●																			
Стахановец										●												
С-Терра												●										
Фактор-ТС			●			●						●								●		
Цифровые технологии (КриптоАРМ)												●										
Эшелон			●						●					●		●						

ПОРТФЕЛЬ ПОСТАВЩИКОВ **ИНФРАСТРУКТУРНОЕ И ПРИКЛАДНОЕ ПО**

ВЕНДОР	КАТЕГОРИЯ	Офисные ПК,графические станции, серверы	Операционные Системы	Виртуализация, VDI	Контроль и управление инфраструктурой	Контейнеры и разработка ПО	Удаленное управление устройствами	Резервное копирование	Системы хранения данных	Шина данных (ESB)	СУБД	BI системы	Облачные платформы	Офисные приложения	Корпоративные коммуникации
Aquarius		●													
Utinet		●													
Гравитон		●													
Uncome OS			●												
ГК Астра			●	●	●		●	●			●			●	●
АЛМИ			●											●	
Базальт СПО			●	●											
РЕД СОФТ			●	●							●				
РОСА			●	●											
АЭРОДИСК				●					●						
Росплатформа				●					●						
РУСГЭК				●											
Фактор-ТС										●					
Лаборатория Числитель						●									
Sharx DC				●											
Kairos Digital				●	●						●				
ГазИнформСервис					●						●				
PR032							●								
LiteManager							●								
Киберпротект				●				●							
Новософт (Handy Backup)								●							
Postgres Pro											●				
FanRuan												●			
Форсайт												●			
Polymatica												●			
Visiology												●			

ВЕНДОР	КАТЕГОРИЯ	Облачные платформы	Офисные приложения	Корпоративные коммуникации	Графические редакторы	САПР	Графика и дизайн	Работа с PDF	Автоматизация бизнес-процессов
#CloudMTS		●							
VK		●		●					
Облакотека		●							
MONT Office			●	●					
МойОфис			●	●					
Р7			●	●					
Яндекс 360				●					
CommuniGate Systems				●					
eXpress				●					
TrueConf				●					
Vinteo				●					
ТелеМост				●					
VideoMost				●					
livedigital				●					
АСМОграф					●				
ГрафТех					●				
АСКОН						●			
Нанософт						●			
GstarCAD						●			
Renga Software						●			
Zwsoft						●			
Movavi							●		
SoftOrbits							●		
AliveColors							●		
Code Industry								●	
Content AI								●	●
CORRECT								●	●
ROBIN									●
PROMT									

uncom OS

Операционная система для работы, учёбы и отдыха

- Офисный пакет, мессенджеры, браузеры и более 60 000 привычных программ в Магазине приложений
- Десятки тысяч игр и облачный гейминг: GTA V, Red Dead Redemption 2, Fortnite, Counter Strike, Dota 2, World of Tanks Blitz
- Архитектура системы неприступна для вирусов и максимально защищена от хакерских атак

По вопросам приобретения корпоративных лицензий — **uncomos@mont.ru**

По вопросам приобретения электронных ключей для физ. лиц — **esdteam@mont.ru**

Uncom OS поставляется в виде корпоративных лицензий (для бизнеса) и электронных ключей (для дома). Компания MONT является эксклюзивным дистрибьютором Uncom OS.

uncom.tech