Check Point
SOFTWARE TECHNOLOGIES LTD.

РЕШЕНИЯ CHECK POINT ДЛЯ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Развитие информационных технологий всегда имело серьезное влияние на экономическую жизнь общества. Но особенно ярко это влияние заметно в последние десятилетия. Информация из средства обеспечения бизнес-процессов превратилась в сам предмет бизнеса. Это в большей степени является очевидным для компаний и организаций финансового сектора, где связь информации и денег зачастую непосредственна и где информационный ущерб напрямую может выражаться ущербом финансовым. Можно сказать, что информация превратилась в деньги, и ее кража стала практически синонимом кражи денег, а задержки в информационном обмене – потерей конкурентного преимущества.

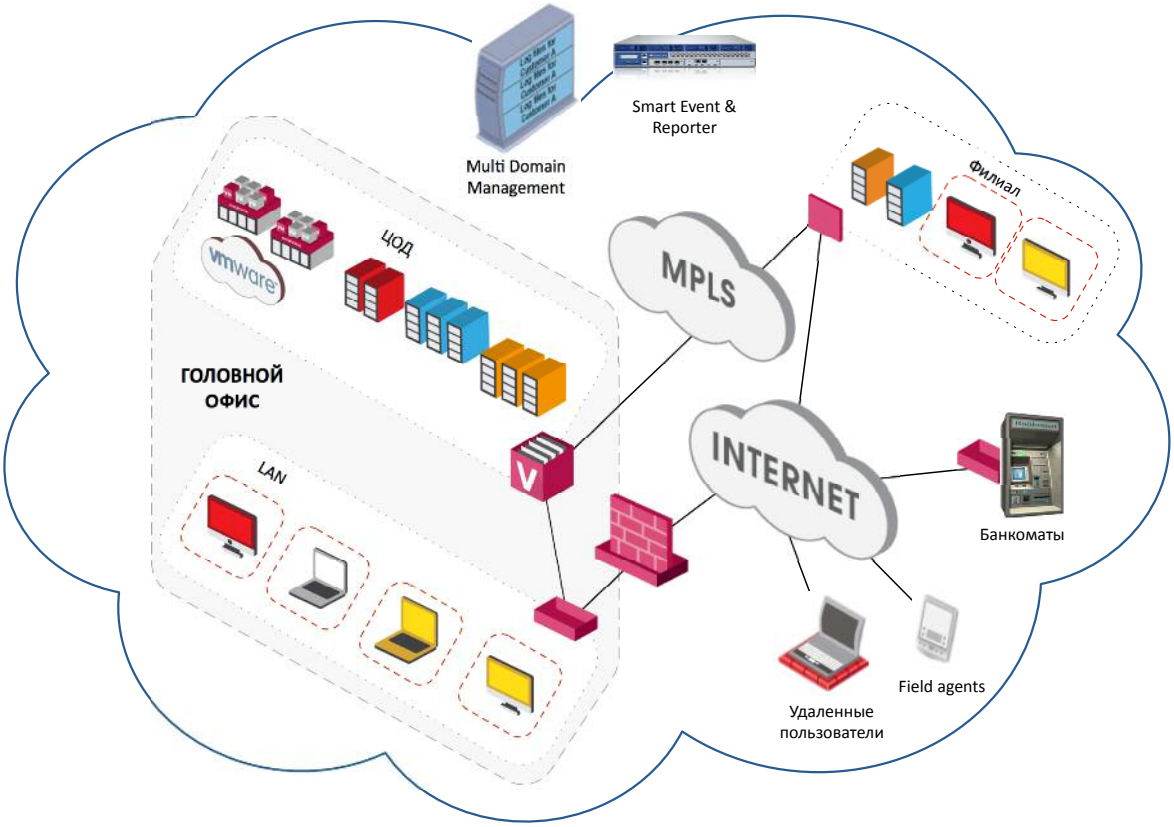
Банки, инвестиционные и страховые компании, биржи всегда были объектом пристального внимания злоумышленников, и неудивительно, что рост значимости информационной компоненты бизнеса приводит к росту угроз, идущих из киберпространства. Но одновременно перед современной финансовой организацией стоят и вызовы другого рода – постоянно меняющийся ландшафт информационного поля требует от компаний адекватного ответа – изменения своих информационных систем. Растущие возможности каналов обмена информацией, увеличение скоростей и объемов передаваемого трафика, мобильность пользователей, лавинообразное распространение персональных устройств, участвующих в бизнес-процессе, высокочастотный трейдинг, майнинг криптовалют, виртуализация и облачные сервисы – вот лишь некоторые отличительные черты того киберпространства, в котором работает современная финансовая компания. Соответственно этому меняется ее информационная инфраструктура и ландшафт угроз.

Появление новых векторов атак, связанных с целенаправленными действиями и расширенными постоянными угрозами (APT), возросший уровень «хактивизма» и кампаний вирусов-«вымогателей», активное использование социальных сетей как инструмента распространения вредоносного ПО, кибервойны, ведущиеся крупными компаниями и правительствами – все это, наряду с традиционными угрозами, требует изменения механизмов и процессов обеспечения информационной безопасности (ИБ) организации.

Говоря о современных проблемах, стоящих перед компаниями финансового сектора, нельзя не упомянуть также и о проблемах, связанных с обеспечением соответствия информационных систем требованиям различных регуляторов. Такие требования могут предъявляться как государственными, так и отраслевыми организациями, а также сертификационными органами. Соответствие таким требованиям рассматривается финансовыми организациями как одна из важнейших компонент управления рисками, и, безусловно, должно оказывать влияние на систему информационной безопасности.

При построении системы защиты неизбежно приходится решать задачу оптимизации с многими ограничениями. Это тем более важно в случае финансовой организации, где экономические параметры такой системы будут напрямую влиять на финансовые показатели компании. Основными факторами, влияющими на решение такой задачи, являются:

- Необходимость обеспечения адаптивности решения с учетом постоянного изменения ландшафта угроз, появления новых векторов атак, а также изменения характера атак от эпизодического к постоянному;



©2017 Check Point Software Technologies Ltd. All rights reserved.

- Необходимость учета динамики информационных систем (например, резкое увеличение использования мобильных устройств, участвующих в бизнес-процессах, возрастающая доля облачных сервисов и т.п.);
- Необходимость соблюдения параметров производительности системы ИБ как части информационной системы организации;
- Ограничения, связанные с недостатком подготовленного персонала, управляющего системой ИБ, в условиях возрастания сложности задач;
- Требование обеспечения сохранности инвестиций и минимизации совокупной стоимости владения системой;
- Возрастание значения требований регуляторов.

Компания Check Point Software Technologies Ltd. предлагает широкий спектр продуктов и решений, позволяющих финансовым организациям построить эффективную систему информационной безопасности, отвечающую современным и перспективным требованиям. Являясь мировым лидером по обеспечению безопасности в сети Интернет, она предлагает своим клиентам надежную защиту против всех типов угроз, уменьшая сложность задачи по обеспечению безопасности и снижая совокупную стоимость владения. Будучи первой компанией, представившей на рынок межсетевой экран FireWall-1 с запатентованной технологией Stateful Inspection, Check Point и сегодня продолжает быть инновационной компанией, предоставляя клиентам простые и гибкие решения, которые могут быть полностью адаптированы для соответствия требованиям безопасности любой организации. Check Point является единственным производителем, который не ограничивается только лишь технологией, но определяет безопасность как бизнес-процесс и предлагает уникальную архитектуру для ее обеспечения. Архитектура Check Point Infinity уникальным образом сочетает политики, человеческий фактор и обеспечение соблюдения требований для создания более эффективной защиты информационных активов и помогает организациям внедрить проект ИБ, соответствующий бизнес-требованиям.

Архитектура Check Point Infinity является первой архитектурой, призванной обеспечить консолидированную безопасность в сетях, облачных и мобильных устройствах и обеспечивающая самый высокий уровень предотвращения угроз как с известными, так и с неизвестными целенаправленными атаками, для защиты вашего бизнеса сейчас и в будущем. Check Point Infinity использует единую аналитическую информацию об угрозах и открытые интерфейсы, позволяя защищать все среды от целенаправленных атак. В отличие от других решений, компания Check Point фокусирует свои усилия на стратегии превентивной борьбы с угрозами, ориентированной прежде всего на предотвращение, а не на обнаружение, чтобы блокировать самые сложные атаки до их возникновения. Архитектура Check Point Infinity консолидирует управление несколькими уровнями безопасности, обеспечивая превосходную эффективность

политик и позволяя управлять безопасностью через единую панель. Единое управление централизованно коррелирует любые типы событий во всех сетевых средах, облачных сервисах и мобильных инфраструктурах.

Ключевыми компонентами, составляющими решение компании Check Point по защите информационной системы финансовой организации, являются:

- Защита корпоративной сети, включающая защиту периметра и региональных офисов, обеспечение устойчивости при атаках класса DDoS, сегментацию сети и защиту центров обработки данных (ЦОД);
- Защита рабочих станций, банкоматов и мобильных пользователей, включая решения по предотвращению расширенных постоянных угроз и обеспечению безопасности данных и документов;
- Система управления с единой консолью для всех компонентов системы ИБ;
- Обеспечение соответствия требованиям регуляторов.

Защита периметра

Определяя безопасность финансовой организации как непрерывный бизнес-процесс, компания Check Point предоставляет решения для защиты всех структурных сегментов корпоративной сети, учитывая их потенциал изменения, а также их взаимосвязь. Решения для защиты периметра Check Point – одной из наиболее традиционных задач информационной безопасности – являются примером системного подхода и находят свое выражение в концепции эшелонированного предотвращения угроз Multi-Layer Threat Prevention, отражающей сложную природу современных вызовов информационной безопасности.

Эта концепция, позволяющая эффективно противостоять широкому спектру как известных, так и неизвестных угроз, включает себя следующие элементы:

Межсетевой экран (МЭ) нового поколения и VPN (Next Generation Firewall and VPN) – запатентованная компанией Check Point технология Stateful Inspection, комбинированная с многочисленными модулями Software Blades, создающая гибкую инфраструктуру для многоуровневых мер безопасности путем предоставления механизмов инспекции сетевого трафика на сетевом и прикладном уровнях, а также уровне данных. Поддержка комплексных политик безопасности, основанных на идентификаторах пользователей, позволяет шлюзам безопасности Check Point и рабочим станциям обмениваться информацией об идентификаторах пользователей и статусе рабочих станций, предоставляя возможности совместного применения политик безопас-

©2017 Check Point Software Technologies Ltd. All rights reserved.

ности во всем предприятии. МЭ нового поколения предоставляет возможности контроля приложений (Application Control) – защиту, основанную на самой большой в индустрии базе веб-приложений, поддерживающей более 6000 приложений и 300000 виджетов. Для обеспечения применения динамических политик Контроль приложений, тесно интегрированный с Фильтрацией URL, поддерживает также механизмы защиты, основанные на репутации и категорировании.

Интегрированную Систему предотвращения вторжений (IPS), блокирующую эксплоит известной и, зачастую, непатченой уязвимости;

Сетевой Антивирус (Anti-Virus), на основе сигнатур блокирующий проникновение и заражение сети вредоносным ПО, вирусами, троянскими программами, а также предотвращающий доступ к вредоносным сайтам;

Систему Анти-бот (Anti-Bot) — решение для периода после заражения, обнаруживающее зараженные машины и предотвращающее дальнейший ущерб путем блокирования коммуникаций ботов с их управляющими центрами;

Программный модуль Check Point Identity Awareness Blade обеспечивает возможность точного и избирательного контроля пользователей, групп и машин, предоставляя непревзойденное управление приложениями и контроль доступа посредством создания точных политик, основанных на идентификации. Централизованная система управления и мониторинга позволяет управлять политиками с единой консоли;

Программный модуль Check Point Anti-Spam & Email Security Blade обеспечивает комплексную защиту инфраструктуры обмена сообщениями. Многомерный подход защищает инфраструктуру электронной почты, обеспечивает высокоточную защиту от спама и защищает организации от широкого спектра угроз, исходящих от вирусов и вредоносных программ, доставляемых по электронной почте;

Программный модуль Check Point URL Filtering Software Blade обеспечивает оптимизированную веб-безопасность посредством полной интеграции в шлюзе безопасности для предотвращения обхода через внешние прокси. Интеграция обеспечения соблюдения правил с помощью контроля приложений дает расширенную защиту Web и Web 2.0, а технология UserCheck позволяет информировать пользователей о политике использования Интернета в режиме реального времени;

Эмулятор угроз (Threat Emulation), предотвращающий заражение от неизвестных эксплоитов, направленных атак и атак «нулевого дня» посредством инспектирования и запуска файлов в виртуальной «песочнице» для вскрытия их вредоносного поведения. Данные такого поведенческого анализа совместно с данными от системы ThreatCloud позволяют надежно защитить информационные ресурсы организации от вновь возникающих и еще неизвестных угроз;

ThreatCloud – уникальная облачная система анализа большого объема информации в целях выявления угроз и создания методов защиты, которая постоянно обновляется, получая информацию о новых угрозах от всемирной сети сенсоров, источников других компаний, исследователей безопасности компании Check Point, исследовательских организаций и шлюзов безопасности Check Point. Согласно последним подсчетам ThreatCloud содержит более 11 миллионов сигнатур вредоносного ПО, 2,7 миллиона адресов зараженных сайтов и свыше 5500 различных схем коммуникации ботнетов. Полученные из ThreatCloud индикаторы могут автоматически применяться для формирования ответных мер по предотвращению возникшей в сети угрозы. При таком взаимодействии, если одна из компаний была атакована вредоносным ПО, соответствующая информация об атаке распространяется через ThreatCloud. Сигнатура атаки добавляется в обширную базу данных и мгновенно используется другими клиентами.

Распределенные атаки типа «отказ в обслуживании» (DDoS) могут быть инициированы кем угодно, даже злоумышленниками с невысоким уровнем технической подготовки, и финансовые организации зачастую оказываются целями таких кампаний. Используя решения Check Point по защите от DDoS, вы легко можете предотвратить сбои ваших сервисов, вызванные атаками этого типа. Check Point DDoS-P (DDoS Protection) использует гибрид выделенных локальных и облачных ресурсов для защиты от DDoS-атак различных типов: объемных, «отражательных», ресурсоемких и атак уровня приложений.

Устройство Check Point DDoS Protector Appliances обладает производительностью до 40 Гбит/с и поддерживает работу с многоуровневыми настраиваемыми профилями, которые автоматически защищают от сетевых «наводнений» и атак уровня приложений с быстрым временем отклика на современные сложные атаки типа «отказ в обслуживании». DDoS Protector Appliances предлагает гибкие возможности развертывания, чтобы легко защитить бизнес любого размера, интегрированное управление безопасностью для анализа трафика в реальном времени, а также управления угрозами для расширенной защиты от атак DDoS. Check Point также обеспечивает выделенную поддержку и ресурсы в режиме 24/7, чтобы предоставить в распоряжение системных администраторов и администраторов сетей самые современные методы защиты для противодействия DDoS-атакам.

©2017 Check Point Software Technologies Ltd. All rights reserved.

Защита ЦОД

Важнейшей частью информационной системы финансовой организации является Центр Обработки Данных (ЦОД), представляющий собой ядро системы информационных активов предприятия. Требования, предъявляемые к архитектуре и оборудованию ЦОД получают свое воплощение в самых передовых технологиях, находящих там свое применение. С ростом объемов данных возрастают и требования к скорости их обработки, передачи и надежности их хранения, а с ростом их значимости для бизнеса возрастают и информационные риски. Применение новых информационных технологий, таких как виртуализация, облачные системы хранения и обработки информации, программно-определяемые сети (Software Defined Networks) выдвигает новые требования к решениям по обеспечению информационной безопасности. Кроме того, такие решения должны обладать необходимым потенциалом расширения, чтобы не стать «узким местом» быстрорастущей системы ЦОД финансовой организации как в смысле мощности, так и в смысле поддерживаемых технологий.

Компания Check Point предлагает широкий спектр решений информационной безопасности, обеспечивающих поддержку всех современных и перспективных технологий, используемых в ЦОД и дающих организации гибкость наращивания потенциала средств защиты.

Компания Check Point предлагает широкий выбор сетевых шлюзов в виде отдельных устройств или программного обеспечения, которое может исполняться на платформах открытой архитектуры, что дает клиентам возможность выбрать решение, соответствующее их специфическим требованиям.

Устройства безопасности Check Point, рекомендуемые к применению в ЦОД и процессинговых центрах, представлены различными моделями, отвечающими потребностям организаций любого масштаба. Продуктовая линейка Check Point для ЦОД начинается с устройств серии 23500, предоставляющей реальную производительность МЭ 34 Гбит/с и IPS до 10 Гбит/с, и идет вплоть до шлюза безопасности серии 64000 — самого быстрого шлюза в индустрии, обеспечивающего беспрецедентную производительность (пропускная способность МЭ на реальном трафике 539 Гбит/с с 228 миллионами одновременных соединений и 9 миллионами новых соединений в секунду, IPS до 142 Гбит/с) и масштабируемость для крупных предприятий.

Построенные на базе GAiA – надежной, безопасной и легко управляемой операционной системы Check Point – устройства компании Check Point сочетают в себе высокую производительность многоядерных систем со скоростными сетевыми технологиями, что позволяет достичь высокого уровня сетевой безопасности.

Все устройства безопасности Check Point могут быть выполнены также в виде виртуальных шлюзов Check Point Virtual Systems (VS). Такие виртуальные шлюзы позволяют организациям оптимизировать и упростить их системы безопасности путем консолидации виртуальной сети с многими маршрутизаторами, коммутаторами и виртуализованными шлюзами безопасности в одной аппаратной платформе.

Использование виртуальных шлюзов безопасности позволяет беспрецедентно увеличить гибкость использования и масштабируемость решений обеспечения информационной безопасности организации. К основным преимуществам такого решения можно отнести:

- Создание Виртуальной системы (ВС) за один клик мыши, используя простой Мастер Создания Виртуальных систем, что позволяет быстро добавлять новые МЭ;
- Наличие отдельной политики на каждую виртуальную систему, позволяющую гибко определять необходимый функционал;
- Простоту эксплуатации, обеспечиваемую возможностью отслеживания использования ресурсов на каждой виртуальной системе, обработкой трафика между ВС с помощью виртуальных маршрутизаторов и коммутаторов, обновлением ПО без времени простоя.

©2017 Check Point Software Technologies Ltd. All rights reserved.

Решение Check Point vSEC Virtual Edition, обладающее возможностью использовать весь спектр модулей Check Pont Software Blades, обеспечивает безопасность систем на уровне гипервизора, предоставляет автоматическую защиту для виртуальных приложений и интегрируется в систему управления с использованием облачных технологий.

Немаловажно отметить, что использование решений компании Check Point, в том числе и виртуализованных, полностью отвечает требованиям стандарта PCI DSS и тем самым упрощает финансовым организациям решение задачи соответствия требованиям регуляторов.

Стремление увеличить эффективность бизнес-процессов и повысить гибкость сети значительно ускоряют внедрение технологий IaaS и SDN. Однако эта новая инфраструктура также имеет свой уникальный набор проблем безопасности, связанный с работой в облачных средах. Check Point vSEC защищает активы в облаке от самых сложных угроз, обладая динамической масштабируемостью, интеллектуальным провижинингом и целостным управлением в физических и виртуальных средах, что гарантирует уверенность при работе с облачными решениями.

Виртуализация сети изменила поведение трафика. Теперь все больше и больше трафика является «горизонтальным» относительно центра обработки данных, создавая новые проблемы безопасности. Учитывая небольшое количество элементов управления для обеспечения безопасности этого «горизонтального» трафика, угрозы могут беспрепятственно перемещаться внутри центра обработки данных. Check Point vSEC плавно обеспечивает расширенную защиту от угроз для предотвращения горизонтального распространения угроз в программно-определяемых центрах обработки данных, а также видимость и контроль для эффективного управления безопасностью как в физической, так и в виртуальной среде - все это из единого унифицированного решения для управления. Решение Check Point vSEC успешно интегрируется с продуктами ведущих производителей решений для частных облачных сред, такими как Cisco ACI, VMWareNSX и решениями на основе OpenStack.

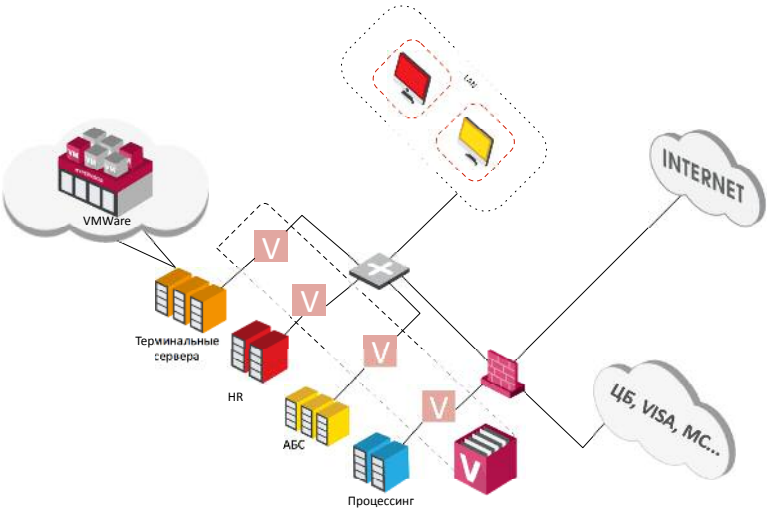
Перемещение вычислительных ресурсов и данных в общедоступные облака означает, что обязанности по обеспечению безопасности распределяются между вами и вашим провайдером облачных вычислений. В то время как защита инфраструктуры предоставляется провайдером, предприятия хотят иметь возможность контролировать свои собственные данные и сохранять их приватность, а также защищать облачные активы, при этом сохраняя соблюдение регулирующих требований. Check Point vSEC обеспечивает надежную связь с публичными облачными активами, защищая приложения и данные с помощью расширенной защиты от угроз в общедоступных и гибридных облачных средах. Решение Check Point vSEC успешно интегрируется с сервисами ведущих провайдеров публичных облачных сред, такими как Amazon Web Services, Google Cloud Platform, Microsoft Azure и VMware vCloud Air.

Построение виртуальных частных сетей

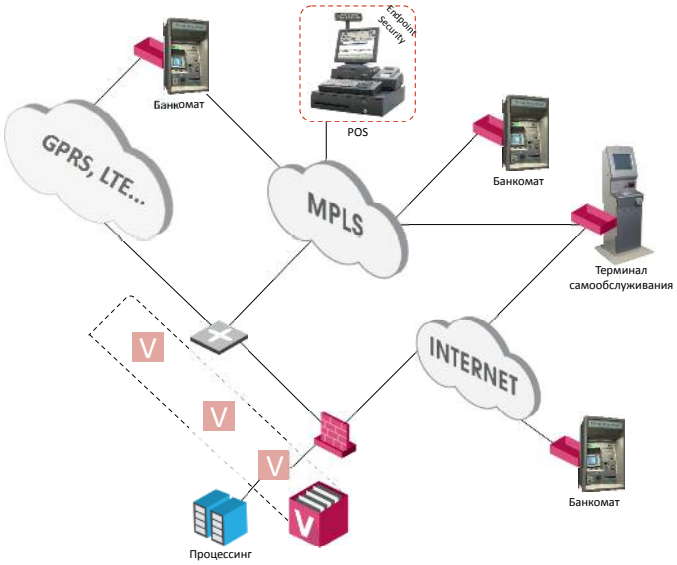
Так как каналы связи с удаленными офисами, банкоматами и мобильными пользователями зачастую проходят по неконтролируемой территории, следует применять шифрование передаваемых данных. Компания Check Point предоставляет в распоряжение своих заказчиков программный модуль Check Point IPSec VPN Software Blade, позволяющий организовать безопасное подключение к корпоративным сетям удаленных и мобильных пользователей, банкоматов, филиальных офисов и бизнес-партнеров. Программный модуль содержит в себе интегрированный контроль доступа, аутентификацию и криптозащиту для гарантии безопасности сетевых соединений поверх интернет.

Отличительными особенностями решения Check Point являются:

- централизованная система управления «site-to-site» VPN и VPN для удаленного доступа;
- повышенная защита IPSec VPN от атак «отказ в обслуживании», в том числе, направленных против механизма обмена ключевой информацией IKE;
- возможность применять политики безопасности в зависимости от уровня шифрования;
- централизованная система управления «site-to-site» VPN и VPN для удаленного доступа;
- поддержка различных режимов создания VPN удаленного доступа для мобильных пользователей, использующих различные типы соединения (включая IPSec VPN, SSL VPN и L2TP);
- поддержка различных методов построения VPN, включая VPN, базирующиеся на маршрутизации и базирующиеся на доменах;
- простая активация и настройка VPN на любом шлюзе Check Point;



©2017 Check Point Software Technologies Ltd. All rights reserved.



- поддержка использования отечественного алгоритма криптозащиты ГОСТ как для протоколов IPSec, так и для SSL;
- централизованное системное журналирование и отчеты в рамках единой консоли.

Защита рабочих станций, банкоматов и мобильных пользователей

Известное высказывание гласит, что эффективность системы защиты определяется эффективностью самого слабого ее звена. Таким звеном в информационных системах зачастую становится человек. Рабочие станции и мобильные устройства используются сотрудниками, контрактерами и клиентами, имеющими недостаточные навыки в соблюдении требований безопасности, что умело используется атакующими для реализации своих планов. Широкое распространение мобильных устройств только усложняет ландшафт угроз. Требования к мобильности, предъявляемые современным бизнесом к сотрудникам финансовых организаций, необходимость работы в неконтролируемых средах, широкое распространение беспроводных технологий, а также лавинообразное увеличение числа персональных мобильных устройств, используемых для бизнес-задач в целях увеличения эффективности работы, приводит к появлению новых векторов атак и требует специальных мер по снижению рисков.

Другой важной задачей, стоящей перед банковскими организациями, является защита банкоматов. Этот участок информационной системы банка традиционно подвержен высоким рискам различного рода, причем доля информационной составляющей риска за последнее время существенно возросла. Это связано как с развитием традиционных методов атак на каналы связи, так и с появлением широкого спектра вредоносного ПО, способного внедриться в программную среду банкомата.

Компания Check Point предоставляет полный набор решений, позволяющих построить эффективную систему защиты рабочих станций, банкоматов и мобильных пользователей.

Широкий спектр модулей Check Point Endpoint Security Software Blades предоставляет беспрецедентную гибкость, контроль и эффективность при управлении и развертывании безопасности конечных устройств. Менеджеры IT могут сделать свой выбор из различных модулей Endpoint Software Blades для развертывания только необходимых механизмов защиты, с последующей возможностью в любое время нарастить решение безопасности. Full Disk Encryption Software Blade прозрачно и в автоматическом режиме защищает всю информацию на жестких дисках конечного устройства. Многофакторная аутентификация перед загрузкой позволяет надежно идентифицировать пользователя. Media Encryption Software Blade предоставляет централизованное управление шифрованием съемных носителей информации с возможностью избирательного шифрования только информации, относящейся к бизнесу, а также возможностью оповещать пользователя и вовлекать его в процесс защиты информации. Remote Access VPN Software Blade дает пользователям возможность удаленного доступа к корпоративным сетям и ресурсам во время путешествий или работая из дома. Anti-Malware and Program Control Software Blade эффективно обнаруживает и уничтожает вредоносное ПО с конечных устройств в рамках одного сканирования и позволяет быть уверенным, что на конечных устройствах исполняются только легитимные и разрешенные программы. Firewall & Compliance Check Software Blade предоставляет проактивную защиту входящего и исходящего трафика для предотвращения заражения конечных устройств вредоносным ПО, блокирования целенаправленных атак и запрета нежелательного трафика. Верификация Соответствия Требованиям Безопасности позволяет убедиться, что ваши конечные устройства будут всегда соответствовать требованиям политики безопасности организации.

Защита данных нового поколения компании Check Point привносит в систему безопасности возможность использования информации о характере данных.

Check Point Capsule представляет собой целостное решение, отвечающее всем вызовам, возникающим перед вашей организацией по мере того, как сотрудники, устройства и данные становятся все более мобильными.

Check Point Capsule позволяет расширить границы безопасности сети и распространить ее на ваши мобильные устройства. Имея единый набор политик, вы можете быть уверены в том, что ваша сеть и мобильные устройства сотрудников применяют одни и те же механизмы защиты против внутренних и внешних угроз.

Используя Check Point Capsule, вы можете получать доступ к корпоративной почте, документам, внутренним

©2017 Check Point Software Technologies Ltd. All rights reserved.

папкам и ресурсам из безопасной бизнес-среды. Персональные данные и приложения будут отделены от корпоративных данных, что позволит безопасно использовать бизнес-ресурсы при одновременной защите персональных данных сотрудников и приложений.

С помощью Check Point Capsule документы будут защищены везде, где бы они ни находились. Свойства безопасности задаются в момент создания документа и следуют всюду, куда бы ни перемещался документ, позволяя быть уверенным в постоянном соблюдении корпоративных политик безопасности.

В современном ландшафте угроз, где бушуют кибервойны и хакеры постоянно меняют свои стратегии и методы, где хакерская экосистема позволяет киберпреступникам делиться кодом эксплойта и вновь выявленными уязвимостями, даже начинающие хакеры могут использовать эти ресурсы для выявления уязвимостей в организациях и легко создавать новые неизвестные атаки «нулевого дня», используя измененные варианты уже существующих вредоносных программ.

Антивирус, межсетевые экраны нового поколения и другие основные решения безопасности сосредоточены только на известных угрозах, у которых есть существующие сигнатуры или профили. Традиционные решения для «песочниц» идентифицируют новые и неизвестные вредоносные программы, но требуют времени на их выявление, рискуя потенциальным воздействием сетевой инфекции до ее обнаружения и блокировки, и, к сожалению, они также уязвимы для методов уклонения, способных обходить традиционную технологию обнаружения «песочниц».

Решение Check Point SandBlast Zero-Day Protection использует возможности технологий Threat Emulation и Threat Extraction для повышения безопасности сети до следующего уровня с помощью защиты от вторжения и от наиболее опасных атак, обеспечивает в то же время быструю доставку безопасного контента для пользователей. Threat Emulation выполняет глубокий контроль на уровне процессора, останавливая даже самые опасные атаки до того, как вредоносное ПО будет иметь возможность развертывания и уклонения от обнаружения. SandBlast Threat Emulation использует проверку уровня ОС для изучения широкого спектра типов файлов, включая исполняемые файлы и файлы данных. Благодаря уникальным возможностям инспекции SandBlast Threat Emulation обеспечивает наилучшую возможную скорость обнаружения угроз и практически не восприимчива к методам уклонения.

SandBlast Threat Extraction дополняет это решение, оперативно доставляя безопасный контент или чистые и восстановленные версии потенциально вредоносных файлов, поддерживая бесперебойный бизнес-процесс. Исключая неприемлемые задержки, создаваемые традиционными «песочницами», Threat Extraction делает возможным реальное развертывание в режиме предотвращения, не только выдает предупреждения, но полностью блокирует доступ вредоносного контента к пользователям.

Check Point SandBlast Zero-Day Protection обеспечивает полное обнаружение, проверку и защиту от наиболее опасных атак «нулевого дня» и таргетированных атак.

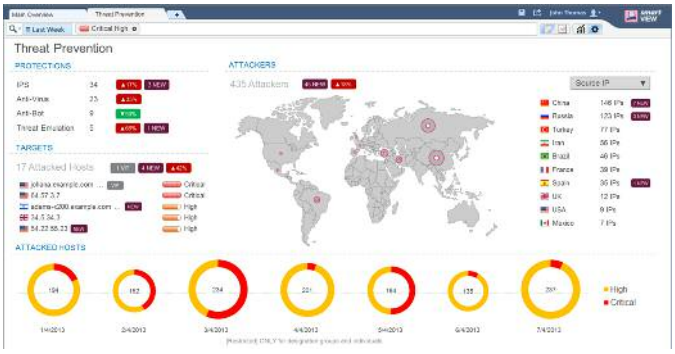
Компания Check Point предлагает своим заказчикам решение SandBlast как в виде облачного сервиса, так и в виде выделенных устройств различной производительности, если компания в силу принятых политик безопасности, требований регуляторов или других причин не могут использовать облачные сервисы.

Компания Check Point также предлагает решение SandBlast Agent, обеспечивающее защиту браузеров и конечных станций от атак «нулевого дня», вымогательского вредоносного ПО и фишинга, сочетающее технологии Threat Extraction, Threat Emulation, Anti–Bot, Antivirus, Zero Phishing, Anti-Ransomware и возможности проведения криминалистического анализа (forensics). Для покрытия задач защиты мобильных устройств на базе операционных систем iOS и Android предлагается решение SandBlast Mobile.

Централизованное управление

Все средства защиты и точки применения политик Check Point управляются с помощью единой унифицированной консоли управления безопасностью, обладающей высокой степенью масштабируемости и дающей возможность управлять десятками миллионов объектов, сохраняя сверхбыстрое время отклика пользовательского интерфейса.

Система управления поддерживает сегментацию предприятия, позволяя администраторам определять политики безопасности для каждого домена безопасности, сохраняя при этом разделение полномочий. В этом случае для предотвращения угроз, управления доступом и защиты данных каждый администратор получает возможность работы с удобным представлением политик безопасности, входящих в зону его ответственности.



©2017 Check Point Software Technologies Ltd. All rights reserved.

Хорошо известно, что политики управления доступом и защиты данных являются специфическими для каждой организации и постоянно изменяются в зависимости от появления новых пользователей, приложений и новых бизнес-процессов. Это особенно верно в отношении финансовых организаций, где изменение в информационной среде происходят постоянно, как то диктует природа рынка.

Для поддержки таких изменений в бизнес-процессах система управления безопасностью Check Point предоставляет программные интерфейсы, позволяющие организациям проводить интеграцию с другими системами, такими как системы управления сетями, CRM, системы сопровождения запросов на поддержку, системы управления идентификационной информацией или системы управления облачными решениями. Открытый интерфейс к внешним системам позволяет системе управления «понимать» изменения в окружении и координировать политики безопасности в соответствии с ними.

Прозрачность является неотъемлемой частью надежной системы безопасности. В этой связи от системы управления требуется обеспечить как полную ситуативную информированность, так и возможности по реагированию на инциденты.

Система Check Point SmartEvent выполняет анализ больших объемов данных и производит корреляцию событий в реальном времени. Это дает возможность получать консолидированную и коррелированную картину инцидента на основе информации из различных источников. Таким образом, создается точная картина события, что помогает ответственным за реагирование на инциденты определить необходимые действия, которые надо предпринять для защиты сети.

Анализ события безопасности представляет результаты в виде индикаторов угроз, которые могут быть переданы в систему ThreatCloud для блокировки угроз в реальном времени. Автоматические механизмы реагирования могут обеспечить сдерживание угрозы, предоставляя возможность предпринять необходимые действия перед возобновлением штатной работы.

Соответствие требованиям регуляторов

Соответствие требованиям регуляторов (compliance) рассматривается финансовыми организациями как одна из важнейших областей управления рисками. Несоответствие корпорации таким требованиям может вылиться в значительные потери, вплоть до отзыва лицензий на деятельность. Поэтому банки и другие компании отрасли прилагают серьезные усилия для обеспечения соответствия требованиям и ищут эффективные решения по управлению этим процессом.

Понимая это, компания Check Point предлагает финансовым организациям решение по контролю за соответствием требованиям регуляторов: модуль Compliance Software Blade — первый встроенный в систему безопасности полностью автоматический сервис такого рода.

Решение позволяет обеспечить всестороннюю проверку настроек всех модулей безопасности относительно заданных требований. Система позволяет легко получить отчет о соответствии требованиям при подготовке к аудиту и применить соответствующие лучшим практикам рекомендации по изменению настроек.

Также решение предоставляет возможность анализа в реальном времени влияния предполагаемых изменений конфигурации всех модулей системы безопасности на соответствие требованиям регуляторов и более чем 300 лучшим практикам.

Проверяя изменения политики и конфигурации в соответствии с лучшими практиками и внутренними политиками в режиме реального времени, модуль Compliance Software Blade позволяет администраторам безопасности выявлять проблемы до внедрения политик. Кроме того, он отвечает требованиям стандартов Basel, Sarbanes Oxley и National Institue of Standards (NIST).

Модуль Compliance Software Blade является критическим компонентом любой архитектуры безопасности Check Point для финансового сектора. Он не только позволяет компаниям проводить аудит политик безопасности в режиме реального времени, но также обеспечивает правильную настройку и функционирование таких элементов управления безопасностью, как межсетевой экран, антивирус, IPS и DLP.

Компания Check Point уделяет особое внимание сертификации своих продуктов и решений в соответствии с требованиями регулирующих органов РФ. Межсетевой экран компании Check Point традиционно сертифицируется по требованиям 3 класса ФСТЭК, также имеются сертификаты на НДВ по 4 уровню контроля, сертифицированы компоненты системы предотвращения вторжений. Система построения виртуальных сетей VPN имеет возможность использования отечественного алгоритма криптозащиты ГОСТ, что подтверждено документами сертифицирующих органов.

©2017 Check Point Software Technologies Ltd. All rights reserved.

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Международная штаб-квартира

Check Point Software Technologies, Ltd.

5 Ha'Solelim Street, Tel Aviv 67897, Israel

Телефон: + 972-3-753-4555 • Факс: + 972-3-575-9256 • Эл. почта: info@checkpoint.com

•

Представительство в России и СНГ

Check Point Software Technologies (Russia) ООО

109544, Москва, бульвар Энтузиастов, 2, Деловой центр «Голден Гейт»

Тел./факс: +7 495 967 7444 • www.checkpoint.com/ru • Эл. почта: Russia@checkpoint.com