CHECK POINT

Software-Defined Protection

Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

SOFTWARE-DEFINED PROTECTION

SOFTWARE-DEFINED PROTECTION

СОВРЕМЕННАЯ АРХИТЕКТУРА БЕЗОПАСНОСТИ

Свободный обмен информацией сегодня является одним из важнейших инструментов развития бизнеса. Корпоративные данные распространяются через облачные сервисы и мобильные устройства, новые идеи ярко вспыхивают в социальных сетях. BYOD, мобильность и облачные вычисления революционно изменили статичную ИТ-среду, предъявив к сетям и инфраструктурам требование динамичности.

Но если Ваша ИТ-среда меняется быстро, то гораздо быстрее меняется спектр угроз. Их изощренность и скорость эволюционирования растут экспоненциально из-за изобретения новых типов атак, зачастую комбинирующих известные и неизвестные угрозы, а также преимуществ уязвимостей «нулевого дня» и использования вредоносного ПО, скрытого в документах, веб-сайтах, хостах и сетях.

В современном мире с его высокопроизводительными ИТ-инфраструктурами и сетями, где уже не существует понятия периметра и угрозы становятся более изощренными, мы должны определить правильное направление защиты предприятий.

Несмотря на широкое распространение узкоспециализированных решений, они остаются по своей природе более реактивными и тактическими, нежели архитектурно-ориентированными. Современные корпорации нуждаются в единой архитектуре, сочетающей в себе высокую производительность сетевых устройств безопасности с проактивными средствами защиты в реальном времени.

Для проактивной защиты организаций требуется новая парадигма безопасности Software Defined Protection[1], которая представляет собой новую методологию и прагматичную архитектуру безопасности. Она предлагает модульную, гибко реагирующую и, что наиболее важно, – БЕЗОПАСНУЮ инфраструктуру.

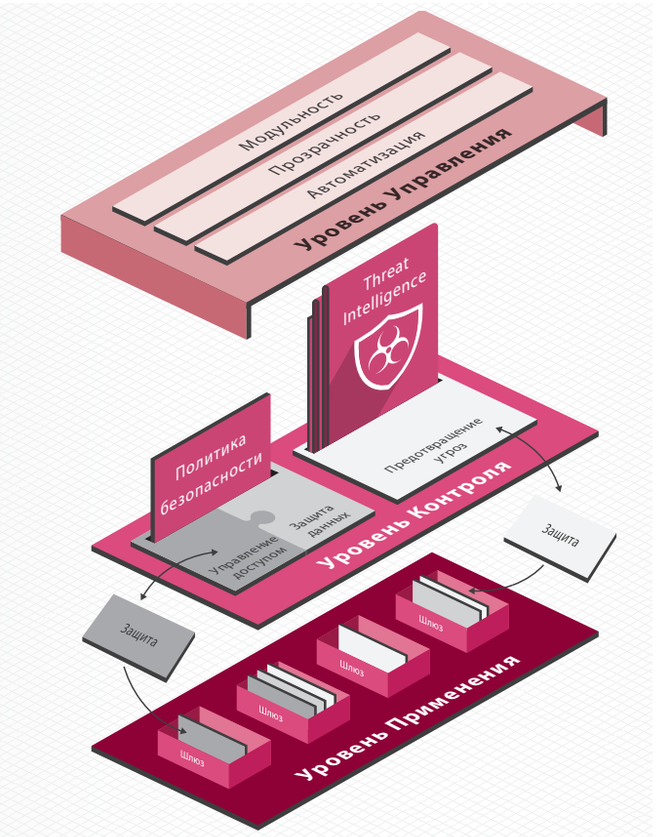
Архитектура такого типа призвана обеспечить защиту организации любого масштаба и местоположения: сети головных офисов и филиалов, смартфонов или мобильных устройств путешествующих сотрудников, или при использовании облачных ресурсов.

Средства защиты должны автоматически адаптироваться к любому спектру угроз без необходимости применения администраторами безопасности многочисленных инструкций и рекомендаций в ручном режиме. Эти средства должны органически интегрироваться в большие ИТ-системы, и их архитектура должна предоставлять оборонительный потенциал, использующий внутренние и внешние источники информации.

Архитектура Software Defined Protection (SDP) делит инфраструктуру безопасности на три взаимосвязанных слоя:

- **Уровень Применения (Enforcement Layer)** основан на физических, виртуальных или хостовых точках применения политик безопасности, осуществляет сегментацию сети и исполнение логики защиты в высокопроизводительных средах.
- **Уровень Контроля (Control Layer**) анализирует различные источники информации об угрозах и создает защитные механизмы и политики, которые будут исполняться на Уровне Применения.
- **Уровень Управления (Management Layer)** управляет инфраструктурой и обеспечивает высокий уровень быстроты реагирования для всей архитектуры.

[1] *Программно-определяемая защита*



Комбинируя высокопроизводительный Уровень Применения с быстро перестраивающимся динамическим программным Уровнем Контроля, архитектура SDP обеспечивает не только надежность в работе, но и возможность проактивно предотвращать инциденты безопасности при быстро меняющемся спектре угроз.

Созданная на перспективу, архитектура SDP поддерживает традиционные требования сетевой безопасности и контроля доступа, равно как и механизмы защиты от угроз, необходимые для современного предприятия, включая такие новые технологии, как: мобильные вычисления и программно-определяемые сети (SDN, Software-defined Network).

УРОВЕНЬ ПРИМЕНЕНИЯ ПОЛИТИК БЕЗОПАСНОСТИ (УРОВЕНЬ ПРИМЕНЕНИЯ)

Уровень Применения архитектуры SDP спроектирован с учетом требований надежности, быстродействия и простоты. Он состоит из сетевых шлюзов безопасности и установленного на хосты программного обеспечения, которые выполняют роль точек применения политик в сети. Эти точки применения могут быть реализованы в виде физических или виртуальных устройств, либо в виде ПО, установленного на рабочих станциях сети (ноутбуках, планшетах, компьютерах и т.д.) и в облачных средах.

Главным принципом, лежащим в основе Уровня Применения, является сегментация. Сегментация критически важна для обеспечения беспрерывного бизнес-процесса организации, так как каждая атака, направленная на определенный сегмент или узел сети, не должна подрывать всю инфраструктуру безопасности корпорации. Таким образом, роль сегментации в архитектуре SDP состоит в предотвращении распространения атаки по всей сети, а также контроле за тем, чтобы в сети передавался только трафик, определенный бизнес-процессами предприятия.

Применение сегментации начинается с выделения «атомарных» сегментов сети. Атомарный сегмент содержит элементы, разделяющие одинаковую политику и одинаковые характеристики защиты. Точки применения будут установлены на границы атомарных сегментов для применения определенных логик защиты. Атомарные элементы могут быть сгруппированы в целях создания модульной защиты. Кроме того, для защиты взаимодействия и обмена информацией между различными сегментами сети устанавливаются доверенные каналы.

Ниже представлены четыре ключевых этапа методологии сегментации:

Шаг 1 — **Атомарные сегменты**
Элементы, разделяющие одинаковые политику и характеристики защиты

Шаг 2 — **Группировка сегментов**
Группировка атомарных сегментов для создания модульной защиты

Шаг 3 — **Консолидация**
Консолидация физических и виртуальных компонентов, таких как сетевые шлюзы безопасности или хостовое ПО

Шаг 4 — **Доверенные каналы**
Каналы для защиты взаимодействия и потоков данных между сегментами

УРОВЕНЬ КОНТРОЛЯ

Уровень Контроля предназначен для развертывания мер защиты в точках применения. Этот уровень включает в себя функционал предотвращения угроз, управления доступом и защиты данных.

Политика предотвращения угроз проста: «Блокировать плохих парней!!!». Такая политика требует минимальной доработки и, скорее, является общим правилом. Защитные средства предотвращения угроз блокируют атакующих и не дают им эксплуатировать уязвимости и доставлять вредоносный контент. Кроме того, они предотвращают попытки ботов и вредоносного ПО связаться с командными серверами управления (Command and Control servers, C&C).

В целях определения корректных решений по применению политик, для выработки правильных инструкций безопасности компонента предотвращения угроз, Уровень Контроля производит корреляцию данных, полученных от разных источников: сигнатурного, репутационного, поведенческого механизмов, механизма эмуляции угроз и результатов проверки данных человеком.

Чтобы меры предотвращения угроз были эффективны, необходим постоянный поток надежной аналитической информации. Аналитическая информация об угрозах может быть получена из внутренних и внешних источников данных об угрозах.

В идеальном случае такие источники должны включать в себя компьютерные группы реагирования на чрезвычайные ситуации (CERTs, Computer Emergency Readiness Teams), инциденты безопасности (CSIRTs, Computer Security Incident Response Teams). Кроме того, необходимо участие аналитиков безопасности, производителей решений по безопасности и других организаций и сообществ по ИБ. В дополнение к указанным внешним источникам аналитика по угрозам создается внутри предприятия путем исследования вредоносного ПО, технологий сэндбоксинга («песочницы») и анализа данных событий безопасности, полученных от точек применения политик.

Анализ угроз позволяет описать агентов угроз, кампании, тактику, технологии и процедуры (TTPs, Tactics, Techniques and Procedures), а также выработать индикаторы угроз в реальном времени.

Управление предотвращением угроз использует аналитику для того, чтобы транслировать большой объем данных по безопасности в готовые к использованию материалы в форме индикаторов и описаний атак. Такие индикаторы представляют собой логику, согласно которой на Уровне Применения будут исполняться решения по защите.

В отличие от предотвращения угроз, механизмы управления доступом и защиты данных представляют собой узкие, специфические для каждого предприятия области.

Управление доступом и защита данных обеспечивает работу бизнес-процессов посредством определения взаимодействия между пользователями и данными в корпоративной сети. Они задают уровень, минимально необходимый для поддержки функционирования бизнеса, и реализуют применение принципа «минимальных привилегий».

Такие защитные механизмы зависят от мест хранения (репозиториев) и описывают специфические для предприятия бизнес-правила, активы, пользователей, роли и приложения, а также определяют политики безопасности как наборы авторизованных видов взаимодействия между активами, пользователями и приложениями.

Анализ и управление трафиком осуществляются адаптивно с учетом контента. Например, в случае интернет-трафика, Уровень Контроля может использовать облачную базу данных для информации о последних приложениях и протоколах, в то время, как для внутреннего трафика могут быть использованы описания специфических приложений или протоколов, используемых в организации. Кроме того, Уровень Контроля должен иметь информацию о всех изменениях и определениях, производимых в других ИТ-системах. Примерами этого могут служить изменения пользовательских репозиториев, автоматическое применение настроек безопасности к виртуальным машинам или разрешения доступа к новому хосту, запись которого появилась в базе данных DNS-сервера.

УРОВЕНЬ УПРАВЛЕНИЯ

Уровень Управления делает архитектуру Software-defined Protection жизнеспособной системой. Активируя каждый компонент архитектуры, уровень действует как интерфейс между администраторами безопасности и остальными двумя уровнями SDP.

Уровень Управления SDP должен быть открытым, модульным и обеспечивать прозрачность состояния безопасности предприятия.

Конфигурации предприятия постоянно эволюционируют, приспосабливая сети, приложения, хосты, пользователей и их роли к динамически изменяющемуся ландшафту бизнеса. Это тем более верно для виртуализованных сред, использующих виртуальные сервера и программно-определяемые сети (SDN), где меры защиты должны изменяться одновременно с изменением функций серверов и их местоположения. Открытая инфраструктура управления предлагает гибкость в интеграции и автоматизации для синхронизации политики безопасности Уровня Контроля с динамической средой предприятия, включающей системы управления облачными ресурсами, базы данных конфигураций, системы инвентаризации активов и инфраструктуру управления идентификационной информацией.

Модульное управление SDP позволяет раздельно определять политики доступа и управления данными и активировать меры предотвращения угроз. Затем политики предотвращения угроз могут быть применены к трафику, разрешенному политиками доступа и управления данными, в автоматическом режиме, либо могут управляться разными людьми или даже могут быть отданы на аутсорсинг.

Модульность также поддерживает уровни и подуровни политик, ассоциированные с различными сегментами сети, таким образом, предоставляя возможность делегировать управление политиками безопасности отдельным администраторам, которые могут работать над ними одновременно.

Прозрачность необходима по двум причинам: во-первых, для ситуационной информированности, во-вторых, для реагирования на инциденты.

Уровень Управления собирает, консолидирует и коррелирует события, поступающие от точек применения политик, развернутых в сети. Лица, ответственные за реагирование на инциденты, в реальном времени получают визуализацию цепочки событий, что позволяет идентифицировать первоначальные векторы атаки и, соответственно, пораженные хосты и скомпрометированные данные. Расследование инцидента позволяет также выработать новые индикаторы угроз для вредоносного ПО, угрожающего поведения и сетевых адресов, ассоциированных с каждой из идентифицированных атак. Эти индикаторы автоматически поступают на Уровень Контроля и отсюда распространяются на Уровень Применения для реализации защиты организации.

ЗАКЛЮЧЕНИЕ

Современные проблемы безопасности требуют свежего взгляда на архитектуру защиты. Они диктуют условия, при которых архитектура должна быстро адаптироваться и соответствовать темпу быстроразвивающихся угроз и постоянно меняющихся требований к развивающимся информационным системам предприятия.

Архитектура Software-defined Protection представляет собой новую парадигму – практический подход к реализации модульной и динамической инфраструктуры безопасности. Она сочетает в себе надежный уровень применения политик безопасности и быстро адаптирующийся, основанный на аналитике уровень контроля для предоставления проактивной защиты корпоративной сети в реальном времени, совместно с мощным интеграционным потенциалом и гибкостью уровня управления.

Это - современная архитектура, которая включает механизмы совместного анализа угроз и создает условия, при которых атаки будут отражены, а внешние угрозы безопасности - выявлены, изолированы и устранены.

CHECK POINT
SOFTWARE-DEFINED PROTECTION

CHECK POINT SOFTWARE-DEFINED PROTECTION

Software-defined Protection (SDP) представляет собой прагматичную архитектуру безопасности, разработанную компанией Check Point для своих клиентов и сообщества в целом. Check Point SDP предлагает инфраструктуру безопасности, которая является модульной, гибко реагирующей и, что наиболее важно, – БЕЗОПАСНОЙ.

Данный документ показывает, как можно построить Архитектуру SDP, используя продукты и услуги безопасности компании Check Point в сетях, на хостах, в мобильных и облачных средах.

Программно-определяемые средства защиты компании Check Point обеспечивают необходимую гибкость для того, чтобы противостоять новым угрозам и соответствовать требованиям новейших технологий. Наши решения создают новые механизмы защиты от известных и неизвестных угроз и проактивно распространяют информацию о них в облаке. Применение решений Check Point, основанных на новой архитектуре безопасности, позволяет предприятиям с уверенностью внедрять новейшие информационные системы.

Software-defined Protection описывает архитектуру безопасности предприятия в контексте трех взаимосвязанных уровней, работающих совместно для обеспечения адаптивной, централизованно управляемой, высокопроизводительной системы безопасности.

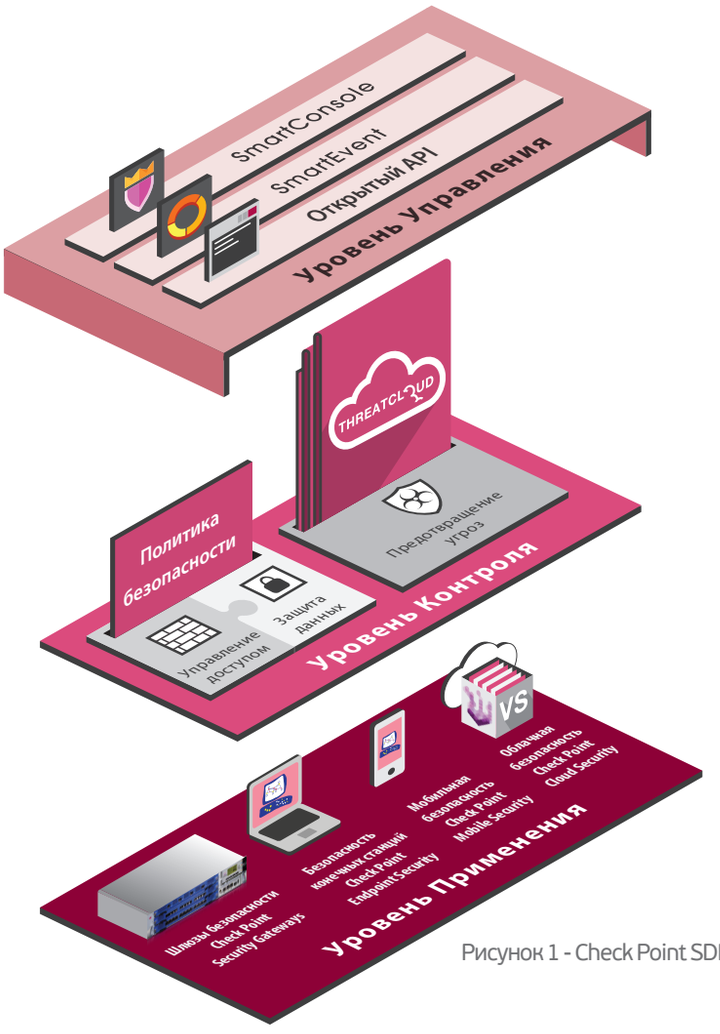


Рисунок 1 - Check Point SDP

УРОВЕНЬ ПРИМЕНЕНИЯ CHECK POINT SDP

Тенденция расширения и размывания границ периметра вынуждает организации сегментировать свои ИТ-системы, включая как внутренние сети, так и облачные и мобильные среды.

Для обеспечения безопасности каждого сегмента компания Check Point предлагает широкий спектр точек применения политик безопасности. Это и высокопроизводительные устройства сетевой безопасности, и виртуальные шлюзы, и программное обеспечение для конечных станций и приложения для мобильных устройств. Компания Check Point предоставляет предприятию все необходимые компоненты для создания сегментированных, консолидированных и безопасных систем и сетей.

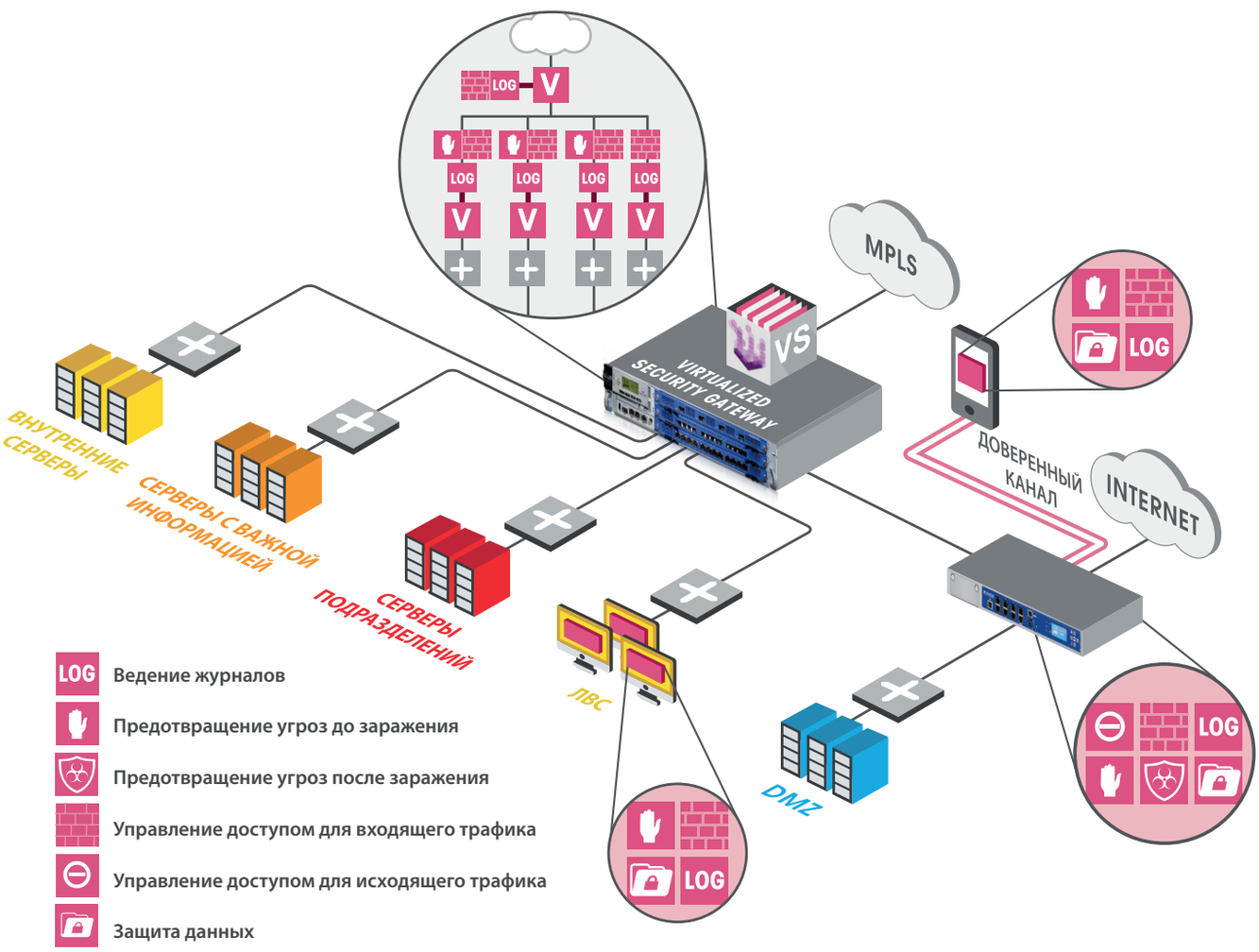


Рисунок 2А – Уровень Применения архитектуры Check Point SDP

Сетевые шлюзы как точки применения политик

Компания Check Point предлагает широкий выбор шлюзов, как в виде отдельных устройств, так и в виде ПО, которое может быть установлено на серверах открытой архитектуры. Это дает клиентам возможность выбрать точки применения политик по своему вкусу.

Устройства безопасности Check Point представлены 19 различными моделями, отвечающими потребностям организаций любого масштаба. Продуктовая линейка Check Point начинается с устройств серий 600 и 1100, предназначенных для защиты малых офисов и филиалов, и заканчивается шлюзом безопасности серии 61000, самым быстрым шлюзом в индустрии, обеспечивающим беспрецедентные производительность и масштабируемость для крупных предприятий и центров обработки данных.

Рисунок 2B – Линейка устройств Check Point 2012 года

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 на хостах. 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.

Хостовые точки применения политик для конечных станций и мобильных устройств

Для эффективной защиты сети границы сегментов должны быть дополнены хостовыми программными агентами, обеспечивающими соблюдение политики безопасности на уровне хоста.

Решения безопасности конечных станций Check Point Endpoint Security для операционных систем Windows и Mas OS позволяют обеспечить точки применения политик на рабочих станциях и мобильных устройствах.

Мобильное приложение Check Point Mobile для платформ iOS и Android обеспечивает криптозащищенный контейнер, позволяющий аутентифицированным пользователям получать доступ в безопасную среду, содержащую корпоративную электронную почту и календари, одновременно обеспечивая разделение с другими личными данными и приложениями, которые могут существовать в среде BYOD.

И, наконец, модуль мобильного доступа Mobile Access Blade от компании Check Point дополняет точки применения политик на конечных станциях и мобильных устройствах доверенным каналом, реализуя VPN доступ с мобильных устройств в интернет и к внутренним корпоративным ресурсам.

Частное и публичное облака

Облачные вычисления все шире используются для достижения экономической эффективности при масштабировании вычислительных и сетевых ресурсов корпорации, а также для систем хранения информации.

В средах типа «частное облако» решение Check Point Virtual Edition (VE) предоставляет возможность применения политик на уровне как гипервизора, так и виртуальных машин, что позволяет пользователям сегментировать трафик между виртуальными машинами. При перемещении виртуальных машин между физическими хостами или создании новых, политики к ним применяются автоматически.

Шлюз безопасности Check Point Amazon Security Gateway позволяет предприятиям применять политики сегментации и межсетевого экранирования на системах внутри публичной облачной среды Amazon Web Services (AWS).

Шлюзы Check Point в облаке

Для мобильных пользователей, перемещающихся вне защищенной корпоративной среды, компания Check Point предлагает шлюзы применения политик в облаке, что дает предприятиям возможность распространить свои политики безопасности на облачную среду. В этом случае весь трафик путешествующих пользователей «туннелируется» через точку применения политик в облаке, поддерживающую технологии Check Point по предотвращению угроз, управлению доступом и защите данных.

УРОВЕНЬ КОНТРОЛЯ CHECK POINT SDP

Уровень Контроля является сердцевиной Архитектуры SDP. Его роль заключается в выработке мер защиты и их развертывании для исполнения на соответствующих точках применения политик. Именно в этой области компания Check Point обеспечивала своих клиентов лучшими в отрасли инновационными средствами защиты последние 20 лет.

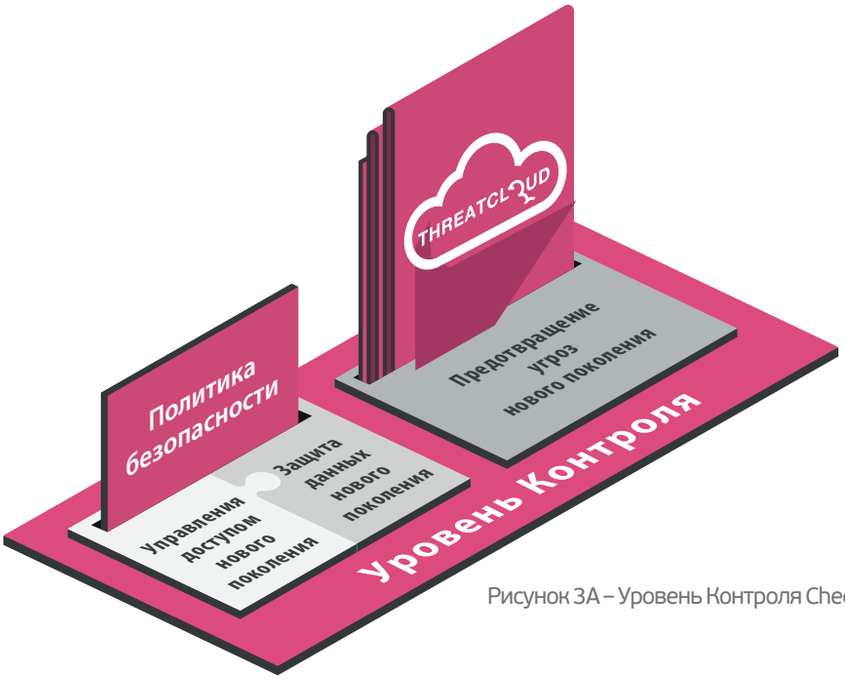


Рисунок 3А – Уровень Контроля Check Point SDP

Модульная архитектура Check Point Software Blade

Уровень Контроля Check Point SDP основан на архитектуре программных модулей Check Point Software Blade Architecture, предоставляющей пользователям гибкие и эффективные решения безопасности, в точности отвечающие их потребностям. Наличие широкого выбора из более 20 программных модулей и модульный характер архитектуры Software Blades дает пользователям возможность выстроить адекватное решение в каждой точке применения политик и расширять инфраструктуру безопасности по мере необходимости.

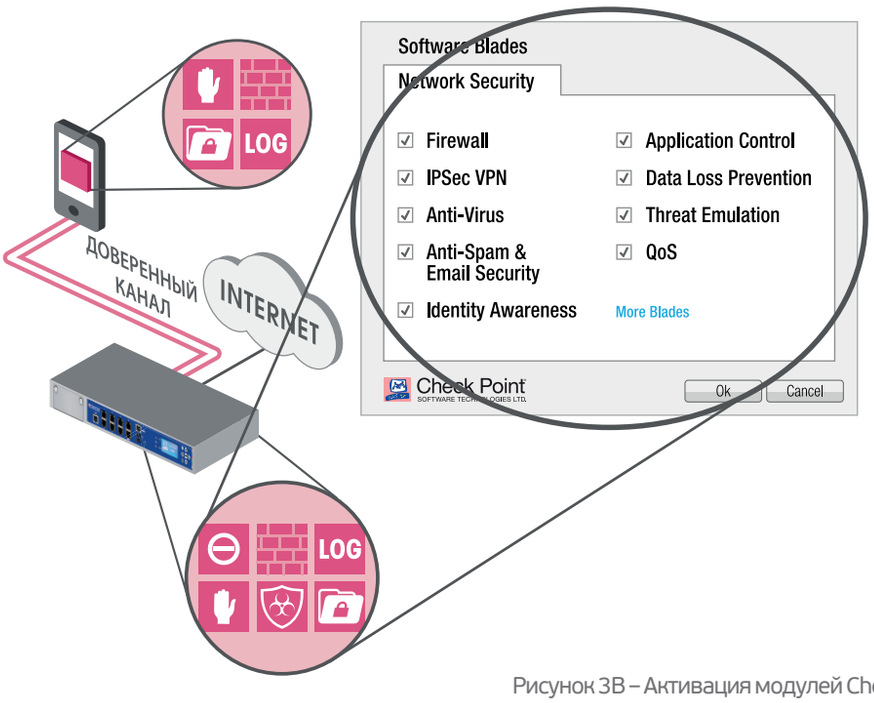


Рисунок 3B – Активация модулей Check Point Software Blades

Предотвращение угроз нового поколения

Компания Check Point позволяет эффективно противостоять широкому спектру известных и неизвестных угроз. Решение Check Point по предотвращению угроз Check Point Threat Prevention включает в себя:

- Интегрированную систему предотвращения вторжений (IPS), блокирующую эксплуатацию известных, зачастую незакрытых уязвимостей;
- Сетевой антивирус (Anti-Virus), на основе сигнатур блокирующий проникновение и заражение сети вредоносным ПО, вирусами, троянскими программами, а также предотвращающий доступ к вредоносным сайтам;
- 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;
- Систему Анти-бот (Anti-Bot), обнаруживающую зараженные машины после проникновения и предотвращающую дальнейший ущерб путем блокирования коммуникаций ботов с их управляющими центрами.

Критически важным является снабжение механизмов предотвращения свежей, постоянно обновляемой аналитической информацией об угрозах. В связи с этим, компания Check Point также создала уникальную облачную систему анализа большого объема информации в целях выявления угроз и создания методов защиты Check Point ThreatCloud ™.

Check Point ThreatCloud создает коллаборативную среду для борьбы с киберпреступностью и проводит анализ угроз в реальном времени с целью выработки индикаторов безопасности для Уровня Контроля.

Согласно последним подсчетам, ThreatCloud содержит более 11 миллионов сигнатур вредоносного ПО, а также 2,7 миллиона адресов зараженных сайтов и свыше 5500 различных схем коммуникации ботнетов.

ThreatCloud постоянно обновляется, получая информацию о новых угрозах от всемирной сети сенсоров, источников других компаний, исследователей безопасности компании Check Point, исследовательских организаций, а также шлюзов безопасности Check Point. Точки применения политик Check Point получают данные о возможных угрозах в режиме реального времени из Threat-Cloud. Если одна из компаний была атакована вредоносным ПО, то соответствующая информация об атаке распространяется через ThreatCloud. Сигнатура атаки добавляется в обширную базу данных и мгновенно используется другими клиентами.

Next Generation Firewall and Data Protection

Управление доступом и защита данных являются важными элементами организации безопасности бизнес-процессов, определяя порядок взаимодействия между пользователями и данными в сети.

Управление доступом компании Check Point базируется на нашем МЭ нового поколения, комбинированном с многочисленными модулями Software Blades. Это позволяет реализовывать унифицированную контекстную политику безопасности, включающую следующие возможности:

МЭ нового поколения и VPN (Next Generation Firewall and VPN) – запатентованная компанией Check Point технология Stateful Inspection, создает гибкую инфраструктуру для многослойных мер безопасности путем предоставления механизмов инспекции сетевого трафика на сетевом и прикладном уровнях, а также на уровне данных;

Использование идентификационной информации пользователей (User Identity Awareness) поддерживает комплексные политики безопасности, основанные на идентификаторах пользователей. Шлюзы безопасности Check Point и конечные станции обмениваются информацией об идентификаторах пользователей и статусе конечных станций, предоставляя возможности совместного применения политик безопасности во всем предприятии;

Контроль приложений (Application Control) предоставляет защиту, основанную на самой большой в индустрии базе веб-приложений, поддерживающей более 5000 приложений и 300000 виджетов. Трафик приложений может просматриваться, выборочно блокироваться и/или ограничиваться по скорости согласно политике безопасности предприятия. Для обеспечения применения динамических политик контроль приложений, тесно интегрированный с фильтрацией URL, поддерживает также механизмы защиты, основанные на репутации и категорировании.

Использование информации о данных или контенте (Data and Content Awareness) основывается на модуле Check Point DLP Software Blade и отличается большим набором автоматических технологий классификации для определения степени важности каждого документа.

Защита данных нового поколения

Защита данных нового поколения от компании Check Point вносит в систему безопасности возможность использования информации о характере данных. Она включает в себя модуль Data Loss Prevention (DLP) Software Blade, выполняющий инспекцию контента и сравнение его с содержимым файлов, хранящихся в репозиториях компании. Check Point DLP поддерживает инспекцию более 800 типов файлов и включает свыше 650 предварительно определенных типов контента. Все это делает Check Point DLP наиболее полным и эффективным решением по предотвращению потери данных на рынке.

Дополнительно компания Check Point предоставляет решение для защиты данных, хранящихся на носителях, с помощью технологии шифрования. Эти технологии могут быть реализованы в любой точке применения политик для защиты важных и конфиденциальных документов от переноса на съемные носители или доступа к ним неавторизованных пользователей.

УРОВЕНЬ УПРАВЛЕНИЯ CHECK POINT SDP

Уровень Управления делает архитектуру Software-defined Protection жизнеспособной системой. Активируя каждый компонент архитектуры, этот уровень действует как интерфейс между администраторами безопасности и остальными двумя уровнями SDP.

Модульная система управления Check Point с многоуровневыми политиками

Все средства защиты и точки применения политик Check Point управляются с помощью единой унифицированной консоли управления безопасностью. Система управления безопасностью Check Point имеет высокую степень масштабируемости и дает возможность управлять десятками миллионов объектов, сохраняя сверхбыстрое время отклика пользовательского интерфейса.

Архитектура SDP требует, чтобы система управления поддерживала сегментацию предприятия, позволяя администраторам определять политики безопасности для каждого сегмента, 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.

Система управления безопасностью Check Point полностью удовлетворяет этим требованиям, реализуя новую концепцию уровней и подуровней (Layers and Sub Layers). Политики могут определяться в каждом сегменте. Политики управления доступом могут быть определены с использованием отдельных уровней, которые могут назначаться разным администраторам. Несколько администраторов имеют возможность работать над одной и той же политикой одновременно.

Policy

Sub-policies

No.	Hits	Name	Source	Destination	Applications	Service	Action
5	21	Web Access	Finance -net Internal-net	Internet	Any Recognized	Any	Drop
5.1	4	Allow Facebook only for HR	HR-Group	Internet	Facebook	Any	Accept
5.2	8	Common Block Categories	Finance-net Internal-net	Internet	Streaming Media Social Networking	Any	Accept
5.3	9	Cleanup	Any	Internet GWs-Group2	Any Recognized	Any	Drop

Рисунок 4A – Под-политики

Автоматизация и интеграция

Согласно архитектуре SDP 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.

Для поддержки таких изменений в бизнес-процессах система управления безопасностью Check Point предоставляет интерфейсы командной строки (CLI) и программный интерфейс веб-сервисов (Web Services API), дающий организациям возможность 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 Уровню Управления «понимать» изменения в окружении и координировать политики безопасности в соответствии с ними. Например, новая виртуальная машина может автоматически получить защиту посредством соответствующей сегментной политики, основанной на классификации данной машины.

Обеспечение прозрачности с помощью системы Check Point SmartEvent

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

Система Check Point SmartEvent выполняет анализ больших объемов данных и проводит 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 предоставляет 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.

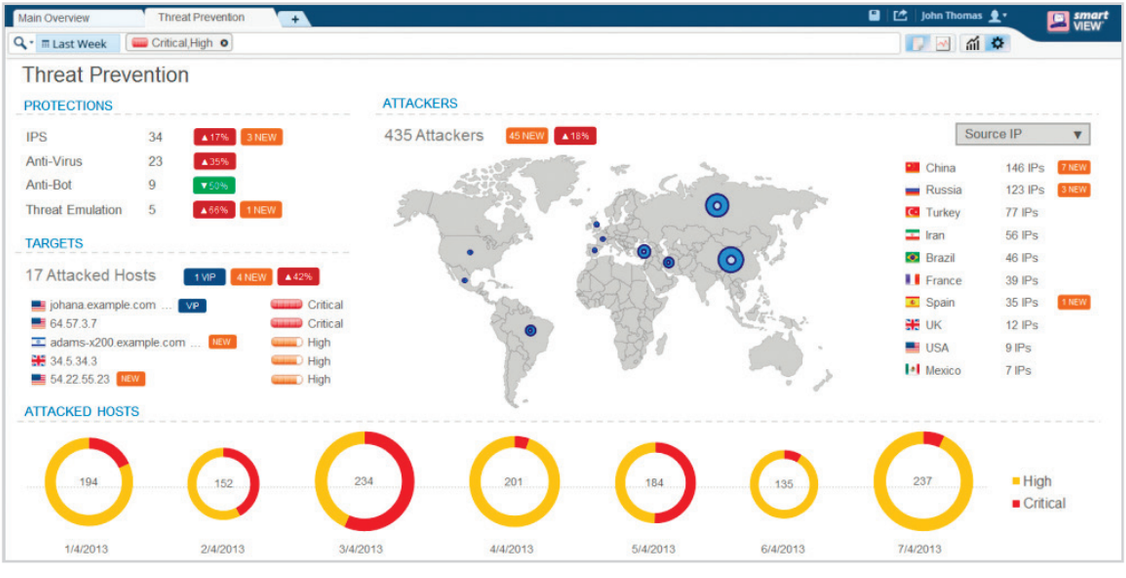


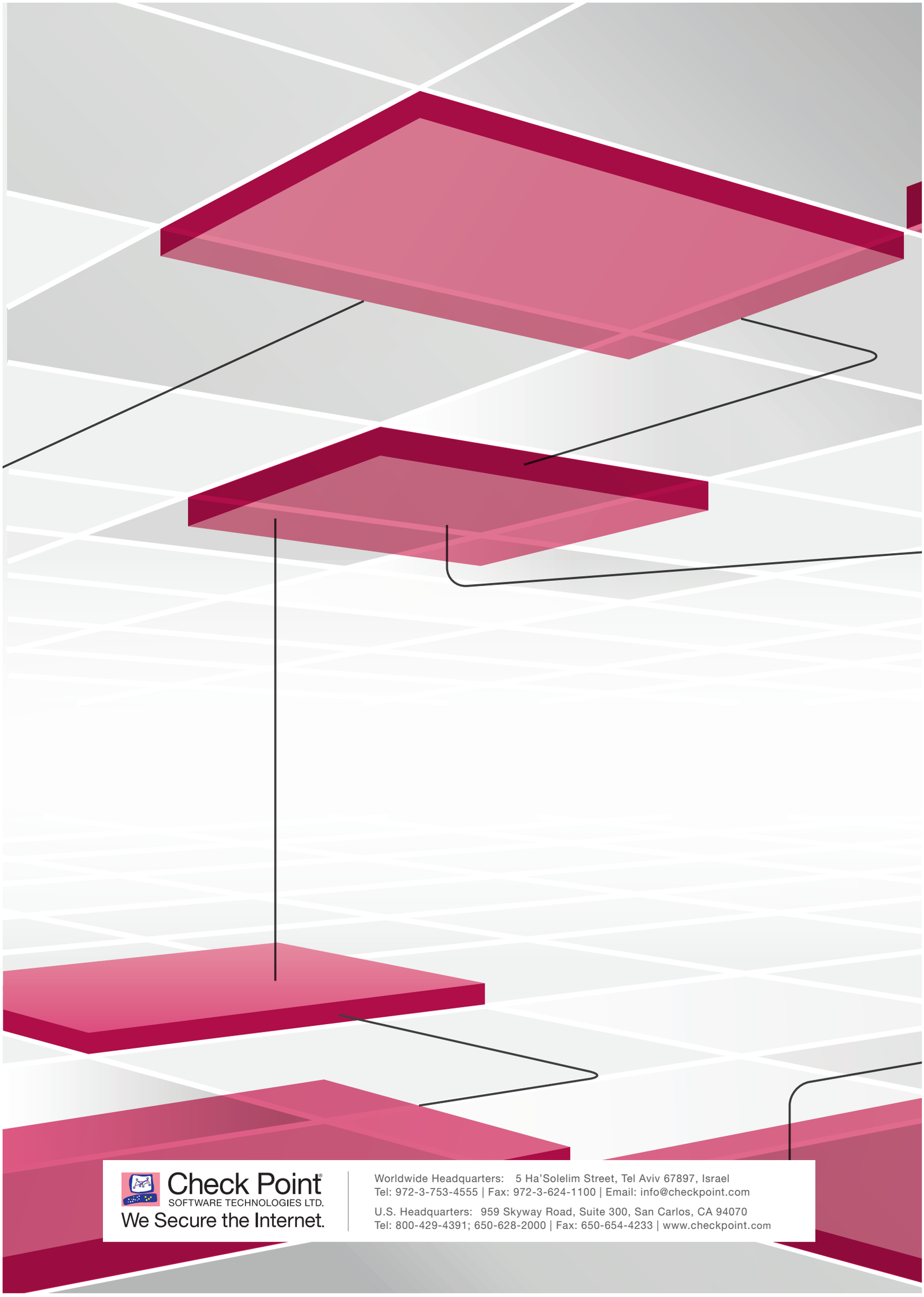
Рисунок 4B – Check Point SmartView

ЗАКЛЮЧЕНИЕ

Для защиты предприятий от постоянно меняющегося спектра угроз необходимо использовать архитектуру, которая позволяет работать в условиях возрастающего объема трафика, при этом является динамичной и обладает механизмами защиты, обновляющимися в реальном времени.

Архитектура Software-defined Protection является лучшим выбором для ответа на текущие и возникающие проблемы информационной безопасности.

Компания Check Point предоставляет все необходимые компоненты для реализации всей архитектуры SDP с наилучшими характеристиками безопасности и управления.



Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Worldwide Headquarters: 5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters: 959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com