

ЦОД: СОЗДАНИЕ СЕРВИСА ЗАЩИТЫ ОТ КИБЕРАТАК (SECURITY-AS-A-SERVICE) ДЛЯ КОРПОРАТИВНЫХ КЛИЕНТОВ

Постоянный рост сложности и мощности атак, направленных на корпоративных клиентов, приводит к повышению спроса на услуги ЦОД по защите серверов, приложений и ресурсов от широкого спектра атак, включая DDoS, атаки на уязвимости и веб-приложения. Система отражения атак Radware AMS обеспечивает безопасность инфраструктуры ЦОД, а также позволяет облачному провайдеру/ЦОД предоставлять настраиваемый под клиента сервис комплексной защиты серверов и приложений от внешних атак для поддержания непрерывной доступности бизнес-ресурсов и работы легитимных пользователей даже во время атаки.

Задача

Важным требованием, предъявляемым на сегодняшний день к коммерческому ЦОД со стороны корпоративных клиентов, является постоянная доступность серверов и приложений для легитимных пользователей. ИТ-системы и веб-сервисы являются ключевым инструментарием современного бизнеса, и кибератаки, направленные на вывод из строя критически значимых бизнес-ресурсов, наносят компаниям существенный финансовый ущерб. Для обнаружения и отражения всех видов мульти-векторных атак, ЦОД должен располагать широким набором средств защиты, включая систему отражения сетевых атак, систему предотвращения вторжений (IPS), систему защиты веб-приложений (WAF) и систему поведенческого анализа (NBA).

Решение

Лучшая в своем классе многоуровневая и, в то же время, простая в управлении система отражения атак Radware позволяет облачным провайдерам/ЦОД предоставлять услугу базовой защиты для всех клиентов ЦОД, а также предлагать дополнительный, настраиваемый под клиента сервис защиты, обеспечивающий создание индивидуального профиля безопасности с учетом конкретных используемых клиентом приложений.

ИБ как услуга ЦОД (Security-as-a-Service):

- Общие сервисы безопасности для всех клиентов ЦОД
- Дополнительные, настраиваемые под клиента услуги защиты на уровне серверов и приложений
- Расширенная услуга защиты веб-сайтов/ веб-приложений, настраиваемая под конкретные реализации веб-приложений

Система отражения атак Radware AMS (Attack Mitigation System)

Система отражения атак Radware AMS является полностью интегрированным программно-аппаратным решением, обеспечивающим защиту на всех уровнях: внешнем, сетевом, системном и уровне приложений. Radware AMS позволяет мгновенно реагировать и отражать атаки всех форм, векторов и масштабов при сохранении функционирования инфраструктуры ЦОД, ИТ-систем корпоративных клиентов и непрерывной работы легитимных пользователей во время атаки.

Создание услуги информационной безопасности из облака (Security-as-a-Service) в коммерческом ЦОД на основе решения Radware AMS

Система отражения атак Radware AMS позволяет ЦОД предлагать клиентам два уровня сервисов безопасности: общие для всех клиентов сервисы защиты, обеспечивающие базовую работоспособность сетевой инфраструктуры ЦОД во время атаки, и дополнительные настраиваемые под клиента услуги защиты от кибератак.

Общие сервисы защиты от атак обеспечивают безопасность и непрерывность работы всего оборудования ЦОД при атаке на клиента или сетевую инфраструктуру ЦОД и подразумевают использование модулей защиты от DDoS и модуля поведенческого анализа. В зависимости от выбранной бизнес-стратегии провайдера/ЦОД, этот сервис может позиционироваться как конкурентное преимущество ЦОД с базовой защитой для всех клиентов или предлагаться как отдельная услуга хостинга в защищенной части ЦОД по более высокой стоимости.

Настраиваемые под клиента сервисы защиты от атак предполагают создание для клиента отдельных политик безопасности с учетом используемых приложений. Система защиты распознает поведенческие модели не только на сетевом уровне, но и на уровне приложений, блокирует нелегитимные HTTP(s) сессии, останавливает медленные атаки и атаки на уязвимости приложений, атаки на исчерпание ресурсов серверов и др. С коммерческой точки зрения такая услуга представляет собой отдельный сервис, так как требует индивидуальной конфигурации под клиента.

Расширенный вариант услуги включает защиту от атак на уязвимости конкретных реализаций веб-сайтов/ веб-приложений за счет разворачивания для клиента виртуальных систем защиты приложений (WAF).

Преимущества решения Radware AMS для ЦОД

- Требуемая мощность (лицензия) системы определяется предполагаемым объемом легитимного трафика ЦОД, не включая трафик атаки
- Время реагирования на атаку измеряется секундами (десятки минут для других решений на рынке)
- Запуск настраиваемого под клиента сервиса защиты не требует дополнительных инвестиций
- Система работает в автоматическом режиме (после короткой первичной конфигурации)
- Решение позволяет увеличить RPU, повысить репутацию ЦОД и лояльность клиентов