Брандмауэр веб-приложений как услуга Barracuda WAF-as-a-Service

Microsoft Azure Certified

ICSA labs CERTIFIED

Member of Microsoft Intelligent Security Association

Защитите любое веб-приложение, где бы оно ни было размещено, всего за несколько минут.

Развертывание и конфигурирование традиционных брандмауэров веб-приложений (WAF) может быть непозволительно сложным и занимать много времени. Действительно, брандмауэр веб-приложений порой просто устанавливают в режиме по умолчанию, чтобы обеспечить соответствие, совсем не заботясь о том, чтобы правильно его настроить – вследствие чего система оказывается уязвимой к угрозам, нацеленным на приложения.

Брандмауэр веб-приложений Barracuda WAF-as-a-Service можно развернуть, сконфигурировать и запустить в работу всего за несколько минут. Предварительно созданные шаблоны мгновенно защитят ваши приложения, а интуитивный интерфейс упростит точную настройку конкретных политик. Всеобъемлющая защита от DDOS-атак обеспечивает постоянную доступность приложений. Встроенная служба устранения уязвимостей Barracuda Vulnerability Remediation Service автоматически сканирует ваши приложения и устраняет уязвимости.

Простое, но гибкое решение

В брандмауэре веб-приложений Barracuda WAF-as-a-Service есть простой в использовании встроенный пятишаговый мастер настройки, с помощью которого вы защитите свои приложения всего за несколько минут. Эффективные предварительно созданные шаблоны полностью защитят наиболее часто используемые приложения. Продвинутые пользователи смогут настроить индивидуальные политики безопасности, выборочно управляя конкретными элементами. Просто добавьте элемент конфигурации, который вы хотите настроить, в список компонентов конфигурации и отрегулируйте его в соответствии с вашими потребностями.

Защита от атак нового поколения

Услуга реализована на основе технологии, уже зарекомендовавшей себя на предприятиях, которая защищает от 10 серьезнейших угроз безопасности по версии OWASP, автоматизированных угроз безопасности веб-приложений из списка OWASP, а также других угроз, включая угрозы нулевого дня. Продвинутая защита от ботов пресекает автоматизированные атаки, такие как веб-скрейпинг, спекуляция, кардинг, спам ботами и атаки, основанные на вводе скомпрометированных идентификационных данных и угоне учетных записей. Неограниченная защита от DDoS предотвращает DDoS-атаки – как нацеленные на приложения, так и объемные. Анализ рисков и интуитивные отчеты помогут вам обеспечить соответствие вашей документации.

Защита приложений нового поколения

Независимо от того, где развернуты ваши приложения – локально, в облаке, в контейнере или бессерверной среде, – к вашим услугам REST API и служба устранения уязвимостей Barracuda Vulnerability Remediation Service, которая сканирует приложения на предмет уязвимостей и позволяет устранить уязвимости одним нажатием кнопки. Это обеспечивает оптимизированную бесперебойную защиту даже при обновлении приложений и развертывании новых приложений с учетом развивающихся потребностей вашего бизнеса, не требуя при этом дополнительных административных расходов.

Решение основано на API и готово к использованию к непрерывной безопасной разработке

Защита от всех нижеперечисленных угроз

• 10 серьезнейших угроз безопасности приложений по версии OWASP
  - Включая внедрение SQL-кода, межсайтовый скриптинг (XSS), межсайтовые подделки запроса (CSRF), атаки внешней сущности XML (XXE) и другие угрозы
• Продвинутые боты
  - Включая автоматизированные угрозы безопасности веб-приложений из списка OWASP
• Атаки, основанные на вводе скомпрометированных идентификационных данных / угоне учетных записей
• Атаки на API, в которых используется XML и JSON
• DDoS-атаки – нацеленные на приложения и объемные
• Атаки нулевого дня
  - С использованием мощной позитивной модели безопасности и технологии интеллектуальной подписи, которая обеспечивает негативную безопасность

Поддерживаемые протоколы

• HTTP/S/0.9/1.0/1.1/2.0
• WebSocket
• IPv4

Другие продвинутые функции безопасности

• Защита репутации IP-адреса
  - Включая определение местонахождения по IP и репутационные каналы на основе данных, полученных от периферийных датчиков и других входных устройств
• Защита при загрузке файлов
  - Включая интеграцию с продвинутой защитой от угроз Barracuda Advanced Threat Protection
• Защита от несанкционированного изменения параметров
• Защита от манипуляций с куки-файлами / формами
• Защита от перечисления файлов и каталогов
• Защита от несанкционированного вмешательства в работу приложения
• Валидация метаданных полей форм
• Маскирование веб-сайта
• Контроль за реакцией
• Детально конфигурируемые политики по элементам HTML
• Проверки ограничений протоколов
• Репутационная база данных IP-адресов Barracuda
• Эвристический анализ отпечатков пальцев
• Задачи, связанные с CAPTCHA
• Защита от атак медленного чтения
• Выходные узлы ToR
• Черный список Barracuda
• Неограниченная защита от DDoS-атак L3-L7

БРОШЮРА • US 1.2 • Авторское право 2019 Barracuda Networks, Inc. • С. Винчестер Бульвар (S. Winchester Blvd.) 3175, Кэмпбелл, штат Калифорния, 95008 • 408-342-5400/888-268-4772 (США и Канада) • barracuda.com