Barracuda Application Security

Комплексная защита веб-приложений и API для ваших приложений в любом месте.

Barracuda Application Protection обеспечивает комплексную и простую в использовании защиту приложений для публично размещенных приложений в любом месте. Благодаря простому трехэтапному процессу регистрации и заранее созданным политикам безопасности вы можете начать защищать свои приложения с помощью машинного обучения уже через несколько минут. Масштабируемая и доступная во всем мире система защиты приложений Barracuda Application Protection способна обеспечить безопасность приложений любого размера. Barracuda Application Protection может быть развернута как SaaS-сервис или как WAF-контейнеры в составе развертываемых приложений, обеспечивая защиту как в направлении «Восток — Запад», так и в направлении «Север — Юг». Barracuda Application Protection работает на более чем 60 PoP по всему миру. Развертывание приложения на ближайшем к вам PoP обеспечивает комплексную защиту без задержек в работе приложения. Приложения могут быть развернуты на нескольких PoP для резервирования и других нужд.

Защитите свои веб-сайты и API с помощью одного комплексного решения.

С помощью одного комплексного решения можно остановить веб-атаки и атаки на API из списка OWASP Top 10, объемные DDoS-атаки и атаки на приложения, а также угрозы «нулевого дня». API — это самый большой вектор угроз для современных приложений, и Barracuda Application Protection защищает API JSON и GraphQL.

Пресечение на корню DDoS-атак и атак с захватом учетных записей.

Barracuda Application Protection содержит полный спектр средств защиты от объемных DDoS-атак и DDoS-атак на приложения без каких-либо ограничений. В тарифный план Advanced также включена защита от атак с перехватом учетных данных (credential stuffing) и распылением учетных данных (credential-spraying). План Premium включает в себя поведенческое обнаружение ATO-атак с помощью функции защиты привилегированных учетных записей.

Barracuda
Your journey, secured.

Адаптивные средства защиты на основе машинного обучения позволяют противостоять новейшим ботам и возникающим атакам.

Barracuda Active Threat Intelligence использует облачные средства машинного обучения для выявления и блокирования возникающих угроз «нулевого дня», автоматизированных атак ботов и угроз практически в режиме реального времени. При этом используются проверенные модели обучения и коллективные данные об угрозах, полученные от всех наших ловушек и инсталляций.

Автоматическое обнаружение и защита скрытых теневых API.

Многие приложения развертывают API для своего бэкенда и не документируют их для администраторов, что приводит к компрометации через эти «теневые API». Barracuda Application Protection использует машинное обучение для обнаружения таких конечных точек API и автоматической настройки защиты для них.

Упрощение защиты с помощью автоматической настройки конфигурации и обновления сигнатур.

Включенный механизм Auto Configuration Engine помогает администраторам настраивать конфигурацию, предоставляя предложения по конфигурации на основе машинного обучения. Обнаружение API на основе схем позволяет администраторам быстро настроить защиту API, а автоматическое обновление сигнатур обеспечивает постоянную защиту от возникающих угроз.

Обеспечьте командам DevSecOps быструю и безопасную работу.

Barracuda Application Protection построена по принципу API. Это означает, что каждый параметр конфигурации может управляться с помощью API и конфигурационного файла на основе JSON, что обеспечивает простоту автоматизации и управления.

Получите глубокую видимость и возможности автоматизированного реагирования.

Barracuda Application Protection обеспечивает подробное протоколирование и отчетность по каждому запросу, позволяя получить беспрецедентное количество информации о приложениях и трафике атак. Кроме того, те же API, которые используются для конфигурирования, могут применяться в системах SIEM/SOAR/XDR, позволяя определять собственные автоматические реакции на различные атаки и события.

Расширьте защиту внутренних приложений с помощью входящего в комплект Barracuda CloudGen Access.

Внутренние приложения нуждаются в более надежной защите при работе в Интернете, чем когда-либо ранее. Возможности ZTNA, включенные в тарифный план Premium, позволяют легко включить ABAC и другие усовершенствованные средства защиты входа в систему для этих внутренних приложений, что еще больше повышает уровень безопасности на границе.

Полная защита «Север — Юг» и «Восток — Запад» для гибридных развертываний с помощью WAF с поддержкой контейнеров.

Традиционные WAF-сервисы могут защищать только трафик от приложения к клиенту и обратно — они не обеспечивают полноценной защиты между различными частями приложений. Компрометация одного микросервиса приложения может позволить злоумышленникам достаточно легко продвигаться вбок. Barracuda Application Protection включает контейнерный режим развертывания, в котором можно развернуть одни и те же средства защиты между микросервисами, защищая их от атак внутри приложения.

Barracuda Application Protection доступна в виде двух планов. Выберите план, который вам подходит.

ВОЗМОЖНОСТИ	ADVANCED	PREMIUM
ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ		
Защита от уязвимостей OWASP Top 10	✓	✓
Интеллектуальные подписи	✓	✓
Защита от атак «нулевого» дня	✓	✓
Аналитика IP-угроз	✓	✓ (Подключение к облаку)
Геолокация по IP-адресу	✓	✓
Защита от утечки данных	✓	✓
Защита цепочки поставок веб-сайта	Только визуализация	✓
Антивирусная защита при загрузке файлов	✓	✓
Защита от сложных угроз при загрузке файлов		✓
Обнаружение атак с учетом рисков		✓
ПОЛНЫЙ СПЕКТР DDOS-ЗАЩИТЫ		
Неограниченные возможности предотвращения объемных DDoS-атак	✓	✓
Предотвращение DDoS-атак на неограниченное количество приложений	✓	✓
Ограничение скорости трафика	✓	✓
DNS Защита		✓
ЗАЩИТА API		
Защита API-интерфейсов JSON и GraphQL	JSON	JSON + GraphQL
Обнаружение API на основе схем	✓	✓
Обнаружение API JSON при помощи машинного обучения		✓
Обнаружение теневых API при помощи машинного обучения		✓
Неограниченные правила ограничения скорости трафика API (Tarpit)		✓
ПРОДВИНУТАЯ ЗАЩИТА ОТ БОТОВ		
Базовая защита от ботов — веб-скрейпинг	✓	✓
Базовая защита от ботов — обнаружение бот-спама	✓	✓
База данных сигнатур ботов	✓	✓
Добавление и испытания CAPTCHA	✓	✓
Предотвращение атак методом грубой силы	✓	✓
Защита от подстановки учетных данных	✓	✓
Облачная аналитика активных угроз		✓
Защита привилегированных учетных записей		✓
Обнаружение ботов при помощи машинного обучения		✓
Идентификация и контроль клиентов		✓
БЕЗОПАСНАЯ ДОСТАВКА ПРИЛОЖЕНИЙ		
Сеть доставки контента	✓	✓
Аутентификация, авторизация и управление доступом	Клиентские сертификаты и JWT	Клиентские сертификаты и JWT
Общий IP-адрес	✓	✓
Доступ к сети с нулевым доверием		✓
Балансировка нагрузки с мониторингом состояния сервера		✓
Маршрутизация содержания		✓
Контейнерное развертывание		✓
IP-адреса приложений		✓

ВОЗМОЖНОСТИ	ADVANCED	PREMIUM
АВТОМАТИЗАЦИЯ, ОТЧЕТНОСТЬ, АНАЛИТИКА И СЕРВИСЫ		
Экспорт журналов в SIEM	Один сервер экспорта	Несколько серверов экспорта
Механизм автоматической конфигурации	✓	✓
Интеграция виртуальных патчей и сканеров	BVM	BVM
Продолжительность хранения журнала	30 дней	60 дней
Доступ к API конфигурации	✓	✓
Снимки конфигурации	✓	✓
Расширенная отчетность и визуализация		✓

Основные функциональные возможности

Защита веб-приложений

- Защита от 10 серьезнейших угроз безопасности веб-приложений по версии OWASP
- Определение местонахождения по IP и репутация IP (включая публичные прокси-сервера и узлы Tor)
- Интеллектуальные подписи
- Защита от кражи исходящих данных (кредитные карты, номера социального страхования и т.д.)
- Эвристика исключений
- Контроль загрузки файлов
- Антивирус для защиты при загрузке файлов
- Защита от сложных угроз при загрузке файлов (требуется подписка на защиту от сложных угроз – ATP)
- Маскирование веб-сайта
- Проверки ограничений протоколов
- Политики, детально конфигурируемые по URL-адресам / параметрам
- Регулирование скорости трафика и тарпиты
- Механизм автоматической конфигурации
- Автоматизированное применение политик обеспечения целостности субресурсов и безопасности контента (защита на стороне клиента)
- Глубокая видимость ресурсов и изменений (защита на стороне клиента)

Полный спектр DDoS-защиты

- Неограниченные возможности предотвращения объемных DDoS-атак
- Предотвращение DDoS-атак на неограниченное количество приложений
- Неограниченные правила управления скоростью трафика

Защита API

- Защита от 10 серьезнейших угроз безопасности API по версии OWASP
- Безопасность JSON
- Безопасность GraphQL
- Обнаружение API на основе схем
- Автоматизированное обнаружение API JSON на основе машинного обучения

Продвинутая защита от ботов

- Защита от веб-скрейпинга
- Усовершенствованная защита от ботов с помощью облачного машинного обучения
- База данных известных ботов
- Защита от спама ботов (спам по реферерам и комментариям)
- Защита от спама через формы
- Защита от вброса и распыления учетных данных
- Защита привилегированных учетных записей
- Защита от атак методом Brute force
- Поддержка CAPTCHA
- Поддержка reCAPTCHAv2/v3
- Интеграция hCAPTCHA

Безопасная доставка приложений

- Разгрузка TLS/SSL
- Глобальное распределение нагрузки сервера
- Маршрутизация содержания
- DNS Защита
- Интеграция сети доставки контента
- Динамическое шифрование URL-адресов
- Поддержка HTTP/1.0, HTTP/1.1 и HTTP/2.0
- Поддержка WebSocket
- Поддержка IPv6
- Управление запросами и ответами (трансляция URL)
- Переводы веб-сайтов
- Кэширование и сжатие

Идентификация и управление доступом

- Сертификаты клиента
- Веб-токены JSON
- Виртуальная установка патчей и контуры обратной связи
- Служба отчетности об уязвимостях Barracuda (бесплатно)

Автоматизация

- API конфигурации
- Примеры кода автоматизации конфигурирования
- Интеграция с Github
- Конфигурирование на основе JSON
- Снимки

Отчетность и аналитика

- Встроенная система регистрации (журналы доступа, журналы Web Firewall и журналы аудита)
- Интерактивные и запланированные отчеты
- Экспорт системных журналов
- Экспорт AMQP/AMQPS

Дополнительные режимы развертывания

- Развертывание в контейнерах для защиты на близком расстоянии

Barracuda®
Your journey, secured.