SOLIDWALL WAF

СЕТЕВОЙ ЭКРАН ДЛЯ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ И API

Специализированное решение для защиты критичных веб-ресурсов от внешних атак. SolidWall WAF контролирует сценарии использования приложений и минимизирует возможность эксплуатации ошибок бизнес-логики.

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

- Защита от атак OWASP Top-10
- Предотвращение логических атак
- Защита от ботов и переборных атак
- Блокировка атак на 0-day и 1-day уязвимости
- Защита API, мобильных приложений
- Блокировка DoS и DDoS-атак
- Предотвращение мошенничества
- Безопасность внутренних ресурсов и UBA

КЛЮЧЕВЫЕ ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ

Эффективный анализ бизнес-логики

SolidWall WAF – единственное решение, полноценно реконструирующее бизнес-логику приложения. Информация о выполняемых пользователем действиях и их параметрах используется для тонкой настройки защиты и может экспортироваться в другие системы.

Эффективное подавление ложных срабатываний

Инструменты раннего подавления на основе сигнатурного анализа и моделей нормальной работы приложений дают возможность максимально быстро вводить WAF в эксплуатацию и снижают вероятность появления ложных срабатываний.

Полнофункциональная защита API

Функционал API Gateway. Создание и корректировка моделей вручную или автоматически, включая определение форматов данных и методов взаимодействия, не поддерживаемых стандартом Open API.

Готовые модели для всех аспектов работы приложения

Универсальные модели работы приложения строятся от его архитектуры, а не от видов атак, что позволяет использовать WAF во множестве сценариев и быстро адаптировать его под новые задачи.

Комплексные алгоритмы защиты от переборных атак и ботов

Многоуровневая защита от переборных и автоматизированных атак включает позитивную модель, рейт-лимитинг, анализ поведения пользователей и иные механизмы, работающие на различных уровнях, в том числе на уровне бизнес-логики. Возможность полнофункционального анализа клиентского окружения.

Интерпретируемое машинное обучение

Интеллектуальные алгоритмы машинного обучения позволяют минимизировать затраты ресурсов на настройку WAF. Результаты обучения могут быть проанализированы и скорректированы оператором.

ООО «СолидСофт», 121205, Россия, Москва, территория Инновационного центра «Сколково», Большой бульвар, д. 42, стр. 1

+ 7(499)705-76-57

info@solidwall.ru

ПРЕИМУЩЕСТВА SOLIDWALL WAF

Быстрое подключение и гибкие настройки под заказчика

Работа в режиме блокировки с минимальным уровнем ложных срабатываний

Масштабируемость и отказоустойчивость уровня Enterprise

Предоставляется в виде облачного решения или размещается на площадке заказчика

ПРОФЕССИОНАЛЬНЫЕ СЕРВИСЫ

Включают в себя полный набор услуг по внедрению и сопровождению:

- проектирование, развертывание и первоначальная настройка WAF,
- мониторинг «здоровья» инсталляции,
- обновление WAF и устранение ошибок в работе решения,
- устранение ложных срабатываний,
- реагирование на инциденты, критичные для заказчика,
- тонкая настройка WAF под изменения приложений заказчика,
- ретроспективный анализ событий, настройка WAF для защиты от переборных атак и ботов,
- расследование инцидентов,
- разработка периодических аналитических отчетов,
- экспертные консультации по вопросам разработки защищенных приложений.

РАСШИРЕННАЯ АНАЛИТИКА И ВНЕШНЯЯ ИНТЕГРАЦИЯ

SolidWall WAF легко интегрировать с SIEM, аналитическими и антивирусными решениями, а также другими внешними системами с использованием механизмов Syslog, SQL, REST API и протокола ICAP.

SolidWall WAF поддерживает интеграцию с корпоративной инфраструктурой доставки приложений: внешними балансировщиками, SSL-концентраторами и др. Существуют готовые схемы для интеграции с IBM Qradar, Splunk, Zabbix.

{...} splunk> ZABBIX {REST : API} Prometheus elastic ICAP ANGIE PRO

О КОМПАНИИ

SolidSoft, российский разработчик решений по защите веб-приложений, выпускает продукты под брендом SolidWall. Компания была основана в 2014 г. на базе независимой лаборатории безопасности SolidLab, которая занимается анализом защищенности информационных ресурсов, настройкой средств защиты, организацией процесса разработки защищенных приложений, мониторингом и реагированием на инциденты.

Сертификат ФСТЭК
№ 4652 о соответствии SolidWall WAF требованиям четвертого класса защиты для межсетевых экранов уровня веб-сервера (тип «Г») и четвертого уровня доверия

SolidWall WAF – в реестре отечественного ПО
в соответствии с Приказом Минцифры России № 799 от 30.12.2020