Sk Участник

solidwall

Почему необходимо защищать веб-приложения?

Веб-технологии получают все более широкое распространение. Они используются повсеместно для создания самых разнообразных приложений и сервисов – от простых сайтов-«визиток» до распределенных систем электронной коммерции, систем управления предприятием или государственных информационных сервисов.

Однако, использование веб-технологий приносит и **значительные риски**. По статистике атаки на веб-приложения являются одними из самых распространенных причин инцидентов информационной безопасности, при этом ущерб от них может быть очень значительным. Поэтому безопасность веб-приложений должна быть зоной повышенного внимания для каждой организации.

Интеллектуальный межсетевой экран уровня веб-приложений **SolidWall WAF** – Решение, которое позволяет обеспечить эффективную защиту критичных веб-ресурсов Заказчика от внешних атак, а также дает возможность осуществлять полный контроль над использованием приложений в разрешенных сценариях.

Ключевые преимущества решения

Высокий уровень защиты

Использование максимально подробных моделей работы защищаемого приложения, наряду с сигнатурными и семантическими методами обнаружения аномалий, обеспечивают высокую степень защиты как от широко распространенных простых видов атак, так и от сложных направленных воздействий.

Эффективная защита от ложных срабатываний

Механизм раннего подавления ложных срабатываний дает возможность минимизировать их влияние на принятие решений и сфокусировать внимание оператора WAF на действительно важных событиях.

Уникальные функции по анализу бизнес-логики

Определение пользователей, их действий в приложении, параметров и данных действий. Эта информация может быть использована для подавления ложных срабатываний, создания позитивной модели работы приложения или экспортирована в другие системы для дальнейшего анализа.

Особые алгоритмы машинного обучения

Дают возможность оптимизировать производительность WAF, выявлять ложные срабатывания, автоматически строить модели работы приложений, эффективно использовать решение в активном цикле разработки (SDLC).

Архитектура решения

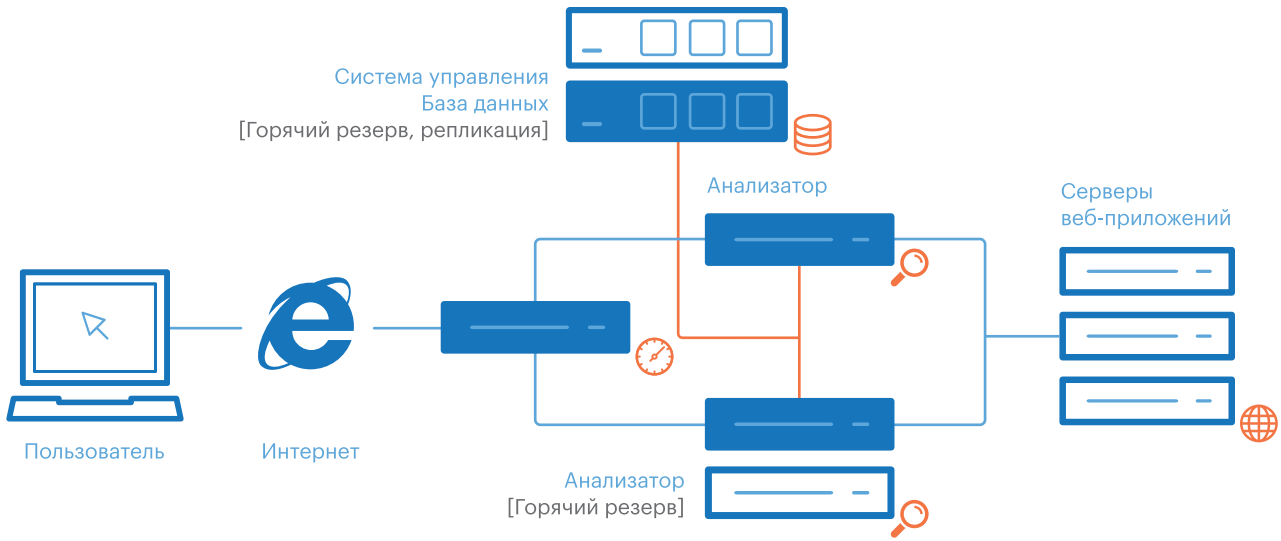
При внедрении на площадке заказчика, архитектура системы дает возможность выбора различных способов установки, а также обеспечивает высокую степень масштабируемости и отказоустойчивости.

База данных и система управления

- Централизованное управление несколькими анализаторами
- Поддерживается неограниченное количество приложений
- Репликация данных
- Интеграция с внешними системами с использованием механизмов Syslog, SQL, SNMP, REST API
- Готовые схемы для интеграции с MicroFocus ArcSight, IBM Qradar, Splunk, Zabbix

Анализатор

- Режимы работы: «в разрыв», «на зеркальном трафике», анализ логов веб-сервера и дампов трафика PCAP
- Поддержка режимов отказоустойчивости Active-Active, Active-Passive
- Терминирование SSL и балансировка нагрузки
- Режим «программный байпасс» обеспечивает доступность сервисов даже в случае сбоев модулей WAF либо существенного превышения нагрузки

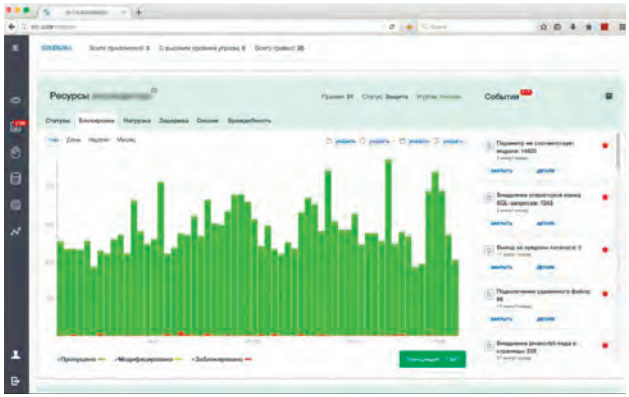


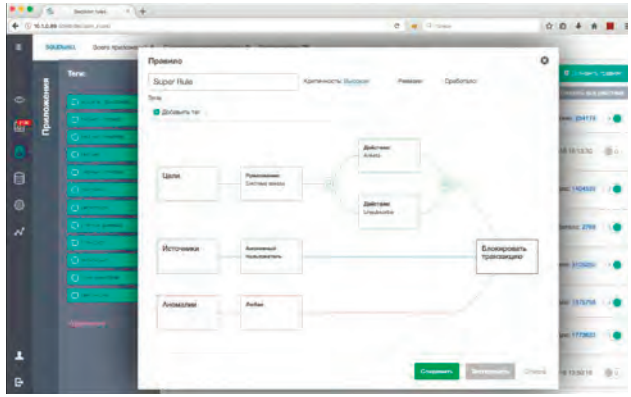
Интерфейс управления

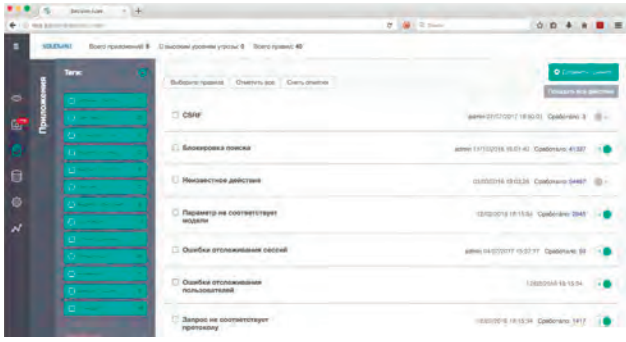
Современный графический интерфейс управления повышает удобство мониторинга и настройки, снижает требования к компетенциям и ресурсам оператора WAF.

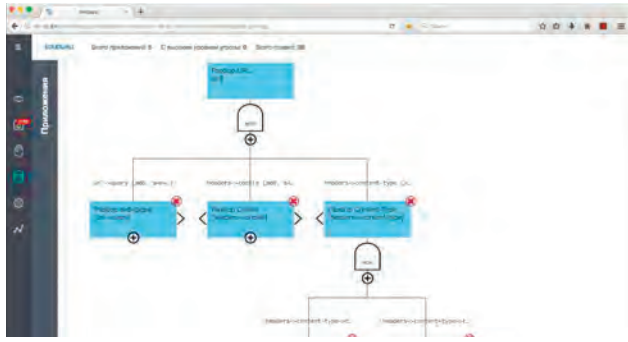
Основные особенности веб-интерфейса:

- Централизованное управление всеми узлами инсталляции из единого интерфейса
- Графическое представление моделей работы защищаемых приложений
- Удобная система мониторинга с набором панелей и группировкой событий ИБ, а также возможностью ограничения объема поступающей информации
- Версионность всех конфигурационных настроек
- Ролевой доступ к функциям интерфейса и подробный аудит действий пользователей
- Поддержка режима Multitenancy (для сервис-провайдеров)









Профессиональные сервисы

Профессиональные сервисы от разработчика по внедрению, настройке системы, мониторингу и реагированию на инциденты позволяют получить максимум эффективности от использования системы.

Услуги включают:

- Анализ защищенности веб-приложений и пилотное тестирование предлагаемого решения для оценки его потенциальной эффективности
- Техническое проектирование, внедрение и тонкую настройку SolidWall WAF, интеграцию со сторонними средствами
- Изменение функциональности WAF по запросу клиента
- Обучение навыкам работы с системой и основам противодействия угрозам в сети Интернет
- Техническую и консультационная поддержку экспертов по вопросам безопасной разработки и защиты веб-приложений
- Мониторинг событий информационной безопасности, реагирование в соответствии с требуемым SLA, помощь в расследовании инцидентов
- Подготовку сводных периодических отчетов по результатам мониторинга

Варианты поставки и схема лицензирования

Решение может поставляться в различных исполнениях для установки на площадке заказчика:

[Программное обеспечение]
[Виртуальное устройство]
[Программно-аппаратный комплекс]

Также решение может предоставляться в виде облачного сервиса совместно с решением AntiDDoS StormWall либо в составе CDN платформы от компании NGENIX.

Сравнение версий системы управления	SolidWall WAF Core	SolidWall WAF Pro	SolidWall WAF Enterprise
Защита от основных видов атак на веб-приложения из перечня OWASP Top 10	●	●	●
Эффективная защита от ложных срабатываний, автоматическое выявление аномалий с высоким уровнем срабатываний	●	●	●
Поддержка предустановленных моделей разбора данных для распространенных фреймворков CMS	●	●	●
Возможность создания собственных моделей разбора данных для веб-приложений собственной разработки	●	●	●
Анализ бизнес-логики и контроль сессий пользователей	●	●	●
Автоматическое определение действий и моделей параметров действий для сложных приложений с активным циклом разработки		●	●
Поддержка интеграции с внешними системами (Syslog, SQL, SNMP, REST API), готовые модули интеграции HPE ArcSight, IBM Qradar, Splunk		●	●
Поддержка отказоустойчивых кластерных конфигураций		●	●
Поддержка распределенных масштабируемых конфигураций с установкой различных компонентов WAF на отдельные узлы			●
Возможность интеграции в SDLC (специальный интерфейс, лицензия для тестовой зоны – бесплатно)			●

О компании SolidSoft

Sk Участник

Разработчик решения, компания **SolidSoft** является дочерней компанией лаборатории безопасности **SolidLab**, специализирующейся на услугах по анализу защищенности, тонкой настройке средств защиты и внедрении процессов безопасной разработки.

Компания основана в 2014 году и является резидентом Фонда «Сколково».

КОНТАКТЫ

ООО «СолидСофт»
121205, Россия, г. Москва,
Территория инновационного центра «Сколково»,
Большой бульвар, д. 42, стр. 1

Т. +7 (499) 705-76-57
Официальный сайт: www.solidwall.ru
E-mail: info@solidwall.ru