SOLAR

СЕРВИС ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ

На базе решения класса
Web Application Firewall (WAF)

МОСКВА, 2024

Оглавление

1. Почему веб-приложениям нужна защита

Веб-приложения играют не последнюю роль в современном бизнесе. С их помощью осуществляется взаимодействие с клиентами, предоставляется доступ к важным бизнес-сервисам, например к CRM-системам, облачным хранилищам, личным банковским кабинетам и т. д. Однако широкое распространение и значимость для бизнеса делают их привлекательной мишенью для киберпреступников – с их помощью можно выкрасть персональные или финансовые данные, заблокировать деятельность компании или получить доступ к внутренней ИТ-инфраструктуре организации.

Отвечая на потребности рынка, компании вынуждены часто обновлять свои корпоративные ресурсы, делать это приходится в сжатые сроки, зачастую пренебрегая анализом на уязвимости.

По данным ГК «Солар»*:

80%

уязвимостей не требуют для эксплуатации специальных условий или технологий

77%

веб-приложений содержат хотя бы одну уязвимость с высоким уровнем критичности

20%

веб-приложений имеют низкий уровень защищенности

Этим и пользуются злоумышленники.

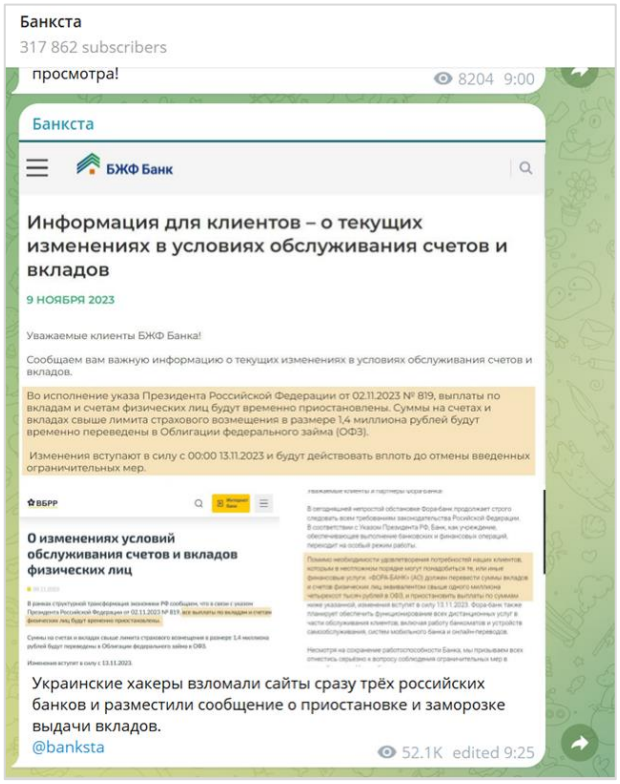
Как показывает практика, средства, используемые злоумышленниками для проведения кибератак, автоматизированы и не требуют особой подготовки. Для поиска уязвимостей в веб-приложениях также используются автоматизированные инструменты – сканеры.

* Отчет об атаках на онлайн-ресурсы российских компаний в 2023 году.

В течение 2023 года доля злонамеренных сканирований существенно выросла. Пиковое значение пришлось на ноябрь и достигало 56% от общего количества угроз. Поэтому можно прямо сказать, что каждая незакрытая уязвимость является общедоступным вектором атаки.

Отказаться компаниям от веб-приложений нельзя – без них бизнес станет неконкурентоспособным или вовсе не сможет работать. Таким образом, от защищенности веб-приложений напрямую зависят:

- Непрерывность бизнес-процессов. Любой сбой в работе, вызванный кибератакой может серьезно повлиять на бизнес-процессы, оперативность принятия решений и обслуживание клиентов.
- Финансовые показатели. Останавливаются продажи, следовательно, уменьшается выручка. Недополученная прибыль в результате простоя, стоимость восстановления данных, штрафы за несоблюдение 152-ФЗ – все это может сильно повлиять на доходность компании.
- Пользовательский опыт (UX). Негативный клиентский опыт посетителей сайта или пользователей веб-приложения напрямую влияет на успешность бизнеса и сказывается на его показателях – от NPS до LTV.
- Репутация. Репутационные потери в случае дефейса или утечки персональных данных могут серьезно повлиять на лояльность текущих клиентов и оттолкнуть потенциальных клиентов, партнеров и сотрудников компании. Особенно если это озвучивается в СМИ и отраслевых каналах, как на примере из Telegram-канала «Банксta».



При этом важность защиты веб-приложений не зависит от размера бизнеса. Киберпреступники угрожают не только крупным компаниям, малый бизнес им тоже интересен. В небольших компаниях реже обновляют ПО, меньше ресурсов для защиты от кибератак, а сотрудники чаще используют личные устройства, что экономит деньги, но повышает вероятность стать жертвой злоумышленников.

По этой причине инвестирование в защиту веб-приложений является важным шагом для любого бизнеса, независимо от его размера и сферы деятельности.

Недостаточная защита веб-приложений может привести к таким серьезным последствиям для бизнеса, как финансовый и репутационный ущерб, утечка или потеря конфиденциальных данных без возможности их восстановления, а также серьезный штраф за нарушение законодательства о защите персональных данных.

Для онлайн-бизнеса важность защиты веб-ресурсов определяется трафиком или количеством пользователей: чем их больше – тем важнее. Но обязательной защита точно становится, если в веб-приложениях есть:

- возможность оплаты или взаиморасчетов с клиентами и контрагентами,
- обмен электронными документами,
- прием заявок от клиентов, маркетинговый трафик,
- сбор данных телеметрии и мониторинга (IoT = Internet of Things, Интернет вещей),
- обмен информацией с контрагентами или разъездными сотрудниками,
- личный кабинет самообслуживания,
- прием обращений в сервисную или техническую поддержку,
- API, остановка которых недопустима и через которые есть доступ к конфиденциальной информации.

Традиционные методы сетевой защиты не спасают от атак на веб-приложения. Межсетевые экраны ориентированы на угрозы сетевого и транспортного уровней, тогда как веб-приложения работают на прикладном уровне. А системы предотвращения вторжений не учитывают логику работы приложений – сессии, cookies и т. д.

Для борьбы с веб-угрозами на уровне приложений используют специализированные решения – WAF, межсетевые экраны уровня приложений. Они позволяют эффективно блокировать атаки из списка OWASP TOP 10 (SQL-инъекции, XSS и т. д.) и DDoS-атаки уровня приложений (L7).

Но недостаточно просто приобрести WAF. Как и другие средства защиты, решение необходимо настроить и постоянно обновлять. Для этого требуется команда специалистов по кибербезопасности, создать которую будет сложно и дорого. Образовательные курсы от вендоров предполагают обучение специалистов только по базовой настройке, а не по адаптации решения под особенности веб-ресурсов компании. Эксплуатацией межсетевого экрана уровня приложений должны заниматься эксперты, которые имеют опыт настройки подобных решений под самые разные веб-приложения и онлайн-ресурсы.

ГК «Солар» предлагает решение этой проблемы – защиту веб-приложений как сервис.

Экспертиза специалистов «Солар» является ключевым компонентом, гарантирующим качество нашего решения. Опыт команды основан на огромном масштабе атак на веб-приложения**:

105 млн
События ИБ в месяц

70%
События ИБ высокого приоритета

80%
Атак сложного уровня

** Вебинар: «Защита веб-приложений: актуальные векторы атак и реализованные кейсы».
Выступление на SOC Forum 2023: «Ключевые боли защиты онлайна. Почему WAF, Anti-DDoS должны быть в SOC».

2. Описание сервиса

2.1. О сервисе

Сервис защиты веб-приложений располагается в георезервированной облачной инфраструктуре ГК «Солар», сертифицированной по PCI DSS и ISO9001, и управляется командой квалифицированных специалистов по кибербезопасности Solar JSOC – первого и крупнейшего в России коммерческого центра противодействия кибератакам. Это позволяет гарантировать высокую производительность и отказоустойчивость сервиса, применение самых актуальных настроек и сигнатур WAF, а также обнаружение и устранение инцидентов кибербезопасности в максимально сжатые сроки.

2.2. Преимущества сервиса

Использование WAF как сервиса от ГК «Солар» имеет ряд преимуществ:

- **Быстрое подключение** благодаря накопленному опыту и выстроенным процессам.
- **Сохранение непрерывности бизнес-процессов** – внедрение сервиса без остановки работы веб-приложений.
- **Реальная защита 24/7 и быстрое реагирование** за счет 6 центров SOC по всей стране и оказания услуг во всех часовых поясах.
- **Минимальный уровень ложных срабатываний** за счет адаптации и профилирования решения под специфику веб-приложения клиента.
- **Опыт и компетенции** ведущей компании на российском рынке ИБ, обеспечивающей безопасность ключевых инфраструктур страны.
- **Высокий уровень клиентского сервиса** – клиентоцентричность и внимательное обслуживание заказчиков.
- **Лучшее по функциональности программное обеспечение** WAF (в таблице 1 представлено сравнение ПО ГК «Солар» с ПО в сервисах конкурентов).
- **Соответствие требованиям регуляторов (98-ФЗ, 152-ФЗ, 149-ФЗ).**
- **Прогнозируемая стоимость сервиса** в перспективе многолетнего планирования.
- **Без затрат на оборудование и обучение персонала** – TCO (совокупная стоимость владения) сервиса почти в 2,5 раза меньше, чем TCO собственного решения On premise. И чем меньше емкость веб-ресурсов компании, тем сервис выгоднее.

Таблица 1. Сравнение ПО WAF

Оценки от 1 до 5, где 5 баллов – полное соответствие, 1 балл – функционал или характеристика отсутствуют.

№	Категория оценки ПО	WAF1	WAF2	WAF3	WAF4
1	Сценарий использования, защита от разных видов атак OWASP, 0-days-уязвимостей, логических и других	4,75	4,75	3,00	2,75
2	Соответствие требованиям: PCI DSS, ФСТЭК и Реестру отечественного ПО	5,00	5,00	1,75	1,75
3	Функционал: разбор передаваемых данных, выявление и реагирование на аномалии	4,67	3,81	2,35	2,33
4	Функции машинного обучения: интерпретируемость и возможность корректировки результатов	5,00	2,33	2,33	1,67
5	Архитектурные особенности, интерфейс управления и интеграция с внешними системами SIEM, BI	5,00	4,71	3,00	2,29
6	Сертификация по требованиям к МЭ 4Г и ОУД4	5,00	5,00	0	1,00
	Итого средний балл	4,90	4,10	2,07	1,96

Сервис удобнее, чем SaaS (Software as a Service) или PaaS (Platform as a Service), т. к. вам не придется самостоятельно осуществлять постоянные настройки профилей защиты под меняющийся ландшафт киберугроз для веб-приложений, тем более что для этого нужен опыт, который невозможно приобрести только на «собственных» нечастых и невариативных веб-атаках.

Дополнительные возможности сервиса WAF от команды «Солар» (в рамках индивидуальных условий под конкретное веб-приложение):

- Сопровождение мероприятий 24x7 аналитиками команды «Солар» с возможностью тюнинга сигнатур «на лету».
- Интеграция сервиса WAF с SIEM для выявления попыток целенаправленных атак на защищаемые веб-ресурсы.
- Возможность оперативного подключения веб-ресурсов под атакой с тюнингом противомер без собранного профиля защиты обучающими механизмами программного обеспечения WAF.
- Создание кастомных правил под особенности бизнес-логики защищаемого веб-приложения в рамках общения с разработчиками веб-приложения.

2.3. Ключевые возможности сервиса

Сервис обеспечивает защиту веб-приложений и поддержку решений кибербезопасности в круглосуточном режиме. Специалисты ГК «Солар» осуществляют техническое обслуживание, аналитику и профилирование модулей защиты.

Использование сервиса помогает клиентам развивать стратегию защиты веб-приложений и отвечать на появление новых угроз и атак. Технологии, лежащие в основе сервиса, позволяют осуществлять:

- **Быстрое и точное выявление основных атак из списка OWASP Top 10:**
  - внедрение кода,
  - некорректная аутентификация и управление сессией,
  - утечка чувствительных данных,
  - внедрение внешних XML-сущностей (XXE),
  - нарушение контроля доступа,
  - небезопасная конфигурация,
  - межсайтовый скриптинг (XSS),
  - небезопасная десериализация.
- **Расширенную защиту от DDoS-атак уровня приложений**
- **Обнаружение автоматизированных атак** (защита от программ-роботов)

Профилирование пользователей позволяет оперативно обнаруживать автоматизированные атаки, осуществляемые с целью кражи уникального контента или размещения несанкционированного контента на защищаемом сайте. При этом не происходит блокирование поисковых ботов и тем самым сохраняется индексация сайта.

- **Маскирование данных**

В рамках оказания сервиса администратор может создавать правила определения чувствительных данных, к примеру паспортных сведений или номеров банковских карт. Эти правила можно применять для маскировки секретной информации от третьих лиц или даже от администраторов решения. Это позволяет добиваться максимального уровня конфиденциальности данных конечных пользователей.

- **Защиту от обхода**

Сервис обрабатывает данные с учетом специфики защищаемого сервера, анализирует XML, JSON и другие форматы данных современных порталов и мобильных приложений. Это позволяет противодействовать большинству методов обхода межсетевого экрана, включая HTTP Parameter Contamination и HTTP Parameter Pollution.

- **Защиту от межсайтовой подделки запроса**

Сервис позволяет блокировать такие атаки, как межсайтовая подделка запроса (CSRF), даже если разработчики не реализовали соответствующие механизмы защиты в самом приложении.

3. Техническая реализация

3.1. Архитектура сервиса

Сервис защиты веб-приложений представляет собой облачное решение ГК «Солар», имеющее инфраструктурную защиту от DDoS-атак уровня L3/L4.

Рисунок 1. Схема подключения сервиса к инфраструктуре клиента

Технологические компоненты инсталлируются в автоматическом режиме в виде отказоустойчивого кластера в режиме active/standby с применением принципов георезервирования.

Подключение происходит путем изменения DNS-A-записи защищаемого веб-приложения на IP-адрес, выделяемый ГК «Солар».

3.2. Модули и механизмы защиты

Сервис использует многоступенчатую схему защиты, позволяющую выявить и заблокировать атаки описанных типов:

- **CSRF**. Защищает от уязвимостей класса «межсайтовая подделка запросов».
- **Инъекции**. Защищает от уязвимостей класса «внедрение операторов SQL», «внедрение произвольных команд операционной системы», «инъекции внешних сущностей XML».
- **XSS**. Защищает от атак класса «межсайтовое выполнение сценариев».
- **Open Redirect**. Отражает атаки класса «открытое перенаправление».
- **Защита XML**. Обрабатывает XML-документы и SOAP-запросы.
- **Защита от DDoS-атак**. Отражает атаки уровня приложений, направленные на ввод серверного программного или аппаратного обеспечения в состояние «отказ в обслуживании».

4. Этапы оказания сервиса

Оказание сервиса состоит из двух этапов:

1. Подключение сервиса.
2. Эксплуатация.

Административный контроль работ, выполняемых на каждом этапе, осуществляется командой сервис-менеджеров.

4.1. Подключение сервиса

Для того чтобы подключить сервис защиты веб-приложений, необходимо выполнить несколько шагов.

Со стороны клиента:

1. Подать заявку на подключение.
2. Получить консультацию специалиста ГК «Солар» и заполнить опросный лист.
3. Подписать договор и оплатить услугу.
4. Совместно со специалистами ГК «Солар» выполнить работы по тестированию и подключению сервиса.

Со стороны ГК «Солар»:

1. Выполнить подготовительные работы по подключению клиента к сервису:
   - проанализировать веб-приложения: нагрузку, частоту и структуру вносимых изменений, процессы релизного цикла;
   - сформировать архитектурное решение в облаке ГК «Солар»;
   - подготовить облачную инфраструктуру исходя из согласованного архитектурного решения;
   - согласовать регламент оказания сервиса (опционально);
   - выполнить первичную настройку WAF для осуществления проксирования трафика исходя из данных в опросном листе;
   - сформировать персональный раздел клиента в личном кабинете информационной безопасности (ЛК ИБ) и предоставить клиенту доступ к нему;
   - настроить мониторинг доступности и работоспособности WAF.
2. Осуществить подключение клиента к сервису:
   - провести тестирование корректности проксирования трафика;
   - после переключения клиентом DNS-A-записи подтвердить успешность проксирования трафика в режиме Detect;
   - осуществить анализ проксируемого трафика веб-приложений и корректировку политик защиты веб-приложений при выявлении ложных срабатываний;
   - перевести политики защиты веб-приложений в режим Block.

4.2. Эксплуатация

Для того чтобы подключить сервис защиты веб-приложений, необходимо совершить следующие шаги.

1. Обеспечение бесперебойного предоставления сервиса полного цикла:
   - круглосуточный мониторинг доступности и работоспособности WAF, а также функциональные проверки и анализ быстродействия;
   - устранение сбоев и недочетов в работе WAF, в том числе взаимодействие и эскалация запросов производителю;
   - выполнение полного спектра регламентных работ с WAF, необходимых для профилактики скрытых дефектов и сбоев, а также поддержания работоспособности;
   - обработка запросов клиента на добавление исключений в политики защиты веб-приложений.
2. Сопровождение релизного процесса защищаемых веб-приложений:
   - предварительная подготовка сигнатурных политик для новой версии ПО на предпродуктивной среде;
   - их корректировка в рамках функционального и нагрузочного тестирования новой версии;
   - обеспечение бесшовного перевода новой версии ПО на новую политику защиты.
3. Проактивное блокирование и доработка политик защиты веб-приложений:
   - обновление и корректировка сигнатур блокирования веб-атак;
   - разработка новых правил защиты, адаптированных под векторы угроз, актуальных для защищаемых веб-приложений;
   - оперативная разработка правил блокирования новых массовых и таргетированных атак на основании исследований, проводимых специалистами ГК «Солар».
4. Выявление, анализ и реагирование на инциденты кибербезопасности, зафиксированные системой (в случае подключения сервисов Solar JSOC).

5. Регламент технической поддержки

SLA на время решения инцидентов и запросов клиента:

- **Низкий приоритет** – обращение по техническим вопросам, связанным с кратковременным прекращением предоставления сервиса без последствий для бизнес-процессов (на момент записи инцидента сервис работает нормально). Возможно минимальное снижение уровня предоставления сервиса. Этот приоритет также используется для информационных запросов от отдельных пользователей, если в них не сообщается о потере качества сервиса или отсутствии необходимых условий для работы с ним.
- **Средний приоритет** – любые возникающие инциденты у одного или нескольких пользователей сервиса, не приводящие к прерыванию его доступности, но заметно влияющие на параметры качества сервиса. Снижение качества обслуживания. Есть риск повышения приоритета со временем.
- **Высокий приоритет** – существенное снижение или прекращение работоспособности оборудования или ПО, не приводящее к потере критичного (основного) функционала информационных систем, но оказывающее существенное влияние на бизнес-процессы. Возможны альтернативные варианты выполнения основных функций информационных систем или восстановления их нормального функционирования с помощью инструкции или плана восстановления.
- **Критический приоритет** – аварийная нештатная ситуация, связанная с полной потерей работоспособности оборудования или сервисов. Доступных обходных решений на момент появления инцидента не существует.

Таблица 2. Регламент технической поддержки

Приоритет инцидента	Время решения (час.) в тарифах емкостью 100, 300, 500 и 700 RPS*	Время решения (час.) в тарифах емкостью 1000 и более RPS*
Критический	12	4
Высокий	24	8
Средний	48	48
Низкий	240	240

Режим работы технической поддержки: 24/7/365

* RPS – Requests Per Second, количество запросов к веб-приложению в секунду.

6. О компании ГК «Солар»

6.1. Компетенции

ГК «Солар» – это архитектор комплексной кибербезопасности. Мы обеспечиваем защиту организаций всех уровней: от малого бизнеса до федеральных органов власти. Ключевые направления деятельности – аутсорсинг ИБ, разработка собственных продуктов, комплексные проекты по кибербезопасности.

Экспертиза, накопленная за годы работы с крупными корпорациями, государственными организациями и объектами критической инфраструктуры, призвана обогащать все наши продукты и поддерживать высокий уровень средств защиты, разработанных с учетом последних видов киберугроз.

№1
на рынке
сервисов ИБ

2000+
экспертов
по кибербезопасности

850+
организаций
под защитой

24/7
обеспечение
кибербезопасности

600+
комплексных и сервисных
проектов в год

200+ млрд
анализируемых
событий ИБ в сутки

Продуктовый портфель компании ГК «Солар» делится на три основных направления: продукты на базе собственных технологий (DLP, SAST, SWG, IGA), сервисы кибербезопасности под брендами Solar MSS и Solar JSOC, а также услуги в области кибербезопасности, в том числе для защиты автоматизированных систем управления технологическими процессами (АСУ ТП) и Промышленного интернета вещей (IIoT).

6.2. Лицензии

- Министерства обороны Российской Федерации – на проведение работ, связанных с созданием средств защиты информации.
- ФСБ России – на проведение работ, связанных с использованием сведений, составляющих государственную тайну.
- ФСБ России – на разработку, производство и распространение шифровальных (криптографических) систем.
- ФСТЭК России – на деятельность по технической защите конфиденциальности информации.
- ФСТЭК России – на деятельность по разработке и производству средств защиты конфиденциальной информации.
- ФСТЭК России – на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны.
- ФСТЭК России – на проведение работ, связанных с созданием средств защиты информации.
- Соглашение с ФСБ России в рамках ГосСОПКА о взаимодействии по предупреждению кибератак.

7. Контактная информация

Телефоны:

+7 (499) 755-07-70 – продажи и общие вопросы

E-mail:

solar@rt-solar.ru – продажи и вопросы по сервису

info@rt-solar.ru – общие вопросы

Адреса:

- Москва, Никитский пер., 7, стр. 1
- Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд
- Санкт-Петербург, ул. Савушкина, 126, БЦ «Атлантик Сити»
- Ижевск, ул. Ленина, 21, БЦ «Форум»
- Нижний Новгород, Казанское ш., 25, корп. 2
- Ростов-на-Дону, Доломановский пер., 70Д
- Самара, Молодогвардейская ул., 204
- Томск, Комсомольский просп., 70/1
- Хабаровск, ул. Серышева, 56