



Памятка

КАК ПОНЯТЬ, ЧТО ВАШЕЙ КОМПАНИИ НУЖЕН WAF

Как понять, что веб-приложениям вашей компании точно нужна защита? Ниже — список причин, которые могут указывать на необходимость ее внедрения:

01

НАЛИЧИЕ ПУБЛИЧНЫХ ВЕБ-ИЛИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Если ваша компания имеет приложения, доступные для широкой аудитории, либо корпоративные ресурсы, доступные для сотрудников, это создает потенциальные уязвимости. Веб-приложения и мобильные приложения часто становятся мишенью для злоумышленников, что может привести к серьезным последствиям, таким как утечка конфиденциальной информации и подрыв репутации



Взлом и утечка данных



Сервис WAF Solar MSS обеспечит защиту веб-ресурсов от кибератак, круглосуточно сканируя и фильтруя вредоносный трафик

02

ПЕРЕГРУЖЕННАЯ СЛУЖБА БЕЗОПАСНОСТИ ИЛИ НЕДОСТАТОК ЭКСПЕРТИЗЫ

Если ваши специалисты по безопасности испытывают трудности с управлением текущими угрозами и задачами, это может привести к недостаточной защите ваших систем и повышенному риску инцидентов. Сложность современных инфраструктур и растущее количество кибератак ставят под угрозу безопасность бизнеса



Недостаточная защита, высокая вероятность инцидентов, большое количество ложных срабатываний и блокировок



Подключение к сервису WAF Solar MSS разгружает ИБ-службу компании, так как провайдер берет подключение, мониторинг и защиту на себя

03

ОБЯЗАННОСТИ ПО СОБЛЮДЕНИЮ НОРМАТИВНЫХ ТРЕБОВАНИЙ

Следование стандартам безопасности, таким как приказы ФСТЭК №17 и №21, является необходимым условием для обеспечения защиты информации и соблюдения нормативных требований. Однако невыполнение этого требования может стать серьезным вызовом для организаций. Несоблюдение стандартов может привести к санкциям от регуляторов и негативно сказаться на репутации компании



Штрафы и репутационные потери



Сервис WAF Solar MSS помогает заказчикам соблюдать требования регуляторов, обеспечивая необходимый уровень защиты

04

ДОСТУПНОСТЬ API В ИНТЕРНЕТЕ

API на основе веб-технологий становятся важной частью современных приложений, однако их использование может повысить риски безопасности. Уязвимости в API могут быть использованы злоумышленниками и привести к утечке данных и нарушению работы приложения



Взломы и неправомерное использование



WAF Solar MSS защищает ваши API от атак и неправомерного использования

05

НЕОБХОДИМОСТЬ ЗАЩИТЫ ОТ ЛОГИЧЕСКИХ АТАК

Логические атаки направлены на использование уязвимостей в бизнес-логике приложений, что может позволить злоумышленникам получить доступ к данным или нарушить функциональность системы. Эти атаки могут оказаться сложными для обнаружения, так как злоумышленники часто используют против него легитимные функции приложения



Нарушение работы приложения, высокая нагрузка на веб-инфраструктуру



Сервис WAF Solar MSS обеспечивает стабильность работы веб-приложения, настраивая защиту под его бизнес-логику

06

ПОВЫШЕНИЕ СЛОЖНОСТИ ИНФРАСТРУКТУРЫ

С повышением уровня сложности инфраструктуры и переходом на децентрализованные многооблачные решения компании сталкиваются с новыми вызовами в области безопасности. Разнообразие технологий, интеграций и архитектур делает защиту приложений более трудоемкой задачей, что увеличивает вероятность атак и уязвимостей



Уязвимости, недостаточная защита, взломы



WAF Solar MSS предоставляет защиту для различных архитектур, включая облачные, контейнерные и традиционные решения, что позволяет эффективно справляться с разнообразными угрозами

07

ПРОБЛЕМЫ С БОТ-ТРАФИКОМ

Возможность применения средств автоматизации позволяет злоумышленникам активно использовать боты для сканирования приложений на уязвимости, атаки на бизнес-логику и атаки типа «отказ в обслуживании» (DoS). Эти действия могут привести к значительным финансовым потерям и нарушению работы приложений



Нарушение работы, искажение аналитики



WAF Solar MSS эффективно фильтрует бот-трафик, защищая ваши приложения от автоматизированных угроз

08

СТАРЫЕ И НОВЫЕ ВЕБ-ПРИЛОЖЕНИЯ

С учетом того что компании часто используют как современные, так и устаревшие приложения, важно понимать, что это требует уникальных мер безопасности. Устаревшие технологии могут содержать известные уязвимости, которые злоумышленники используют для атак, а уязвимые и устаревшие компоненты часто входят в список топ-10 угроз веб-приложениям



Недостаточная защита, высокая вероятность инцидентов



WAF Solar MSS обеспечивает универсальную защиту для всех типов приложений, повышая общую безопасность бизнеса

ЗАЩИТА ВАШЕГО БИЗНЕСА — НАШ ПРИОРИТЕТ

Если вы нашли то, в чем нуждается ваша компания, в одном или нескольких из перечисленных вариантов, это явный сигнал, что вам стоит рассмотреть внедрение сервиса защиты веб-приложений (WAF).

В условиях роста киберугроз WAF Solar MSS становится необходимым инструментом для обеспечения стабильной работы бизнеса. Сервис обеспечивает обнаружение и блокировку атак, которые пропускают традиционные межсетевые экраны, включая атаки из списка OWASP Top 10 и DDoS-атаки уровня приложений (L7).

Также сервис Solar MSS не только помогает предотвратить взломы и утечки данных, но и оптимизирует работу команды безопасности вашей компании, позволяя ей сосредоточиться на стратегических задачах.



Защита от атак из списка OWASP Top 10



Защита от DDoS-атак уровня приложений

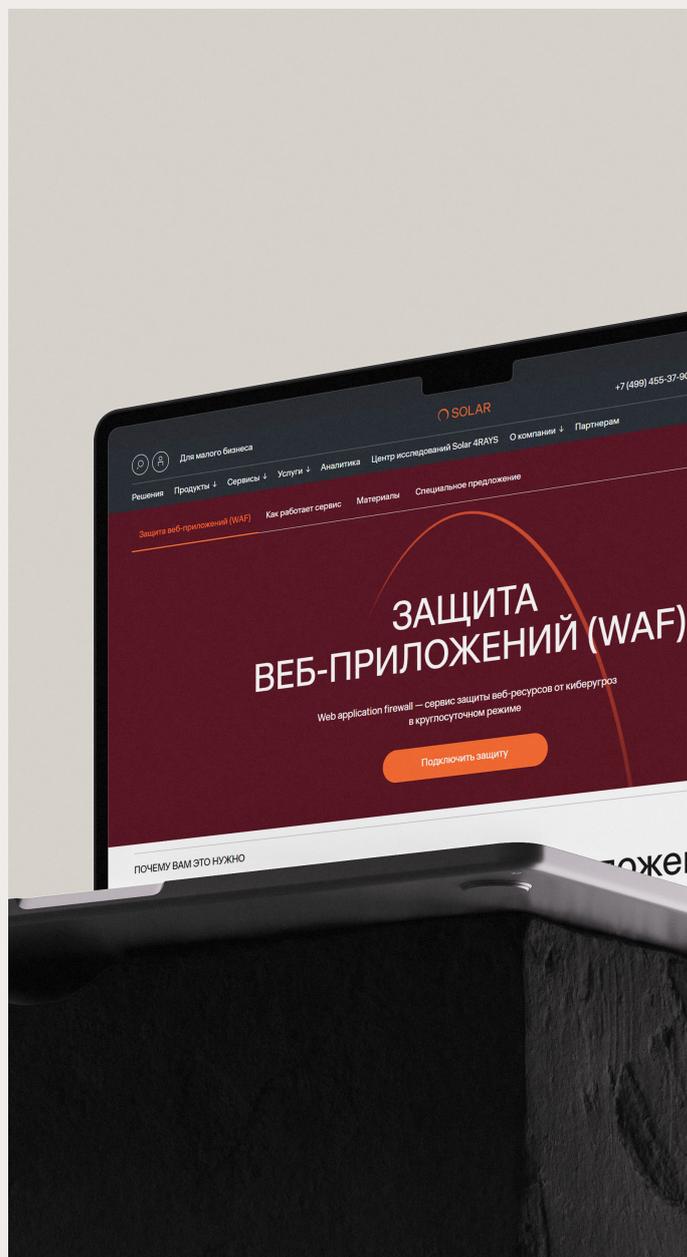


Защита веб-приложений от уязвимостей



Защита от атак в режиме 24/7

[Подробнее о сервисе](#)



О КОМПАНИИ

№1

на рынке сервисов ИБ

Топ-5

европейских MSSP
(Managed Security Service Provider)

2000+

экспертов по кибербезопасности

1000+

организаций под защитой

1,5+^{млрд}

отраженных атак в год