Web Application Firewall: необходимое решение или устаревшая технология

Вячеслав Гордеев

20.09.2018

© Copyright Fortinet Inc. All rights reserved.

Web-приложения – легкая цель

- Уязвимости веб-приложений являются основной причиной утечек и взломов
- Системы предотвращения вторжений (IPS) в одиночку не обеспечивают эффективной защиты веб-приложений, в том числе от атак нулевого дня (zero-day)
- Необходимость соответствия стандарту PCI DSS
- Решения веб-безопасности в первой пятерке приоритетов инвестиций для ИТ лидеров в 2017[4]

verizon

48%

от всех нарушений безопасности вызваны уязвимостями в web-приложениях [1]

acunetix

42%

Из всех web-сайтов имеют хотя одну уязвимость[2]

99,9%↑

критических уязвимостей эксплуатируются через год после публикации

70%

организаций будут использовать решения Web Application Firewalls в 2020 году[2]

Notes/Sources:

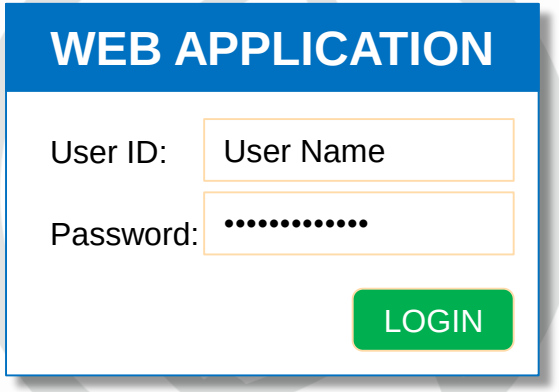
1. Verizon 2018 Data Breach Report.
2. Acunetix Web Application Vulnerability Report 2017
3. Gartner Magic Quadrant for Web Application Firewalls 2016

Устранение уязвимостей может занять месяцы

Злоумышленник использует известные или новые эксплоиты для проведения атаки

На выпуск патча могут уйти недели или даже месяцы

Старые приложения могут не иметь поддержки



КРАЖА ИНФОРМАЦИИ

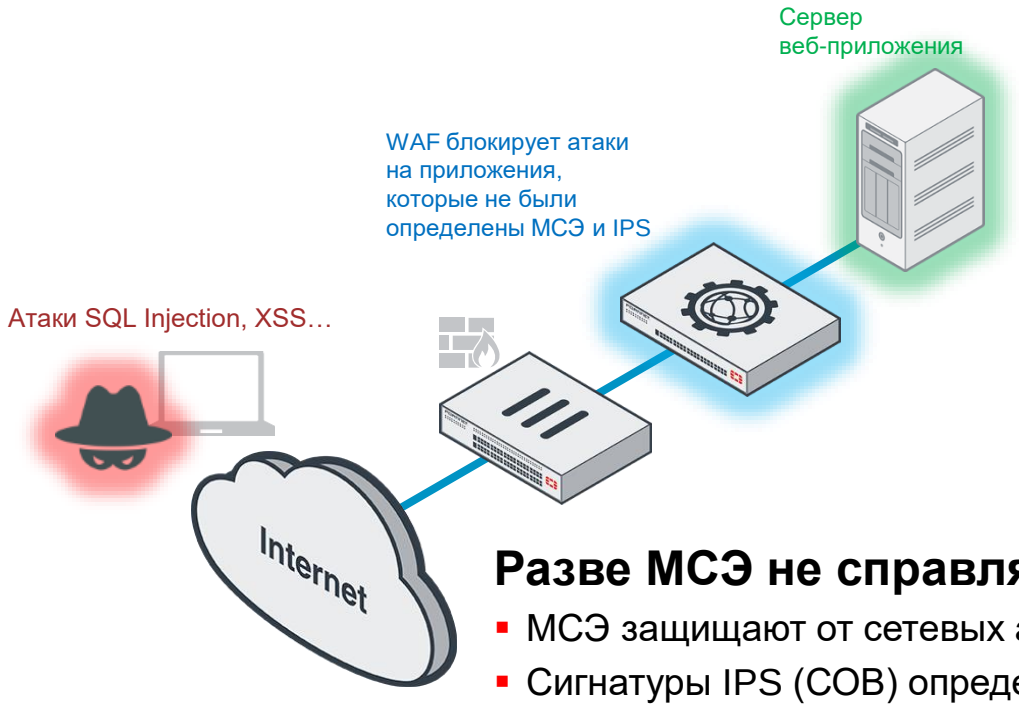
ВЫВОД ИЗ СТРОЯ ПРИЛОЖЕНИЯ

РАСПРОСТРАНЕНИЕ MALWARE

ПОХИЩЕНИЕ УЧЕТНЫХ ДАННЫХ

Применение Web Application Firewall

- Защитить веб-приложения от атак на уязвимостей в коде:
  - » SQL инъекции
  - » Cross Site Scripting…
- Защитить веб-приложения от загрузки вредоносного ПО
- Изучить «нормальное» поведение, детектировать аномалии и заблокировать отклонения
- Публикация приложений, в том числе Microsoft (OWA, SharePoint, ActiveSync)
- Повысить надёжность и доступность



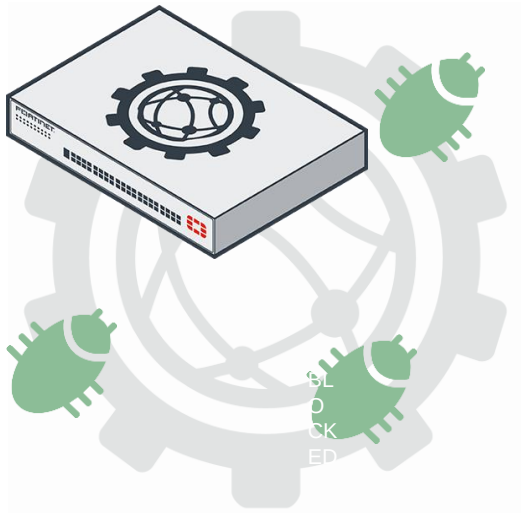
Разве МСЭ не справляются?

- МСЭ защищают от сетевых атак
- Сигнатуры IPS (СОВ) определяют только известные угрозы
  - » Большое количество ложных срабатываний
  - » Нет защиты SSL-трафика
  - » Нет привязки к приложению или пользователю

Многоуровневая защита, корреляция событий

FortiWeb

Web Application Firewall



АТАКИ / УГРОЗЫ

БОТНЕТЫ, ЗАРАЖЁННЫЕ ХОСТЫ, ПРОКСИ ИСТОЧНИКИ DDOS	IP-РЕПУТАЦИЯ
АТАКИ ОТКАЗА В ОБСЛУЖИВАНИИ DDOS НА УРОВНЕ ПРИЛОЖЕНИЙ	ЗАЩИТА ОТ DDOS
ВЫЯВЛЕНИЕ НЕСООТВЕТСТВИЯ HTTP RFC	КОРРЕКТНОСТЬ ПРОТОКОЛА
ИЗВЕСТНЫЕ ТИПЫ АТАК НА ВЕБ-ПРИЛОЖЕНИЯ	СИГНАТУРЫ АТАК
ВИРУСЫ, ЗЛОВРЕДЫ, КРАЖА ДАННЫХ	АНТИВИРУС / DLP
FORTIGATE И FORTISANDBOX ДЕТЕКТИРОВАНИЕ APT	ИНТЕГРАЦИЯ
СКАНЕРЫ, ПАУКИ, ВЫЯВЛЕНИЕ КРАЖИ УЧЁТНЫХ ДАННЫХ	РАСШИРЕННАЯ ЗАЩИТА
НЕИЗВЕСТНЫЕ АТАКИ НА ВЕБ-ПРИЛОЖЕНИЯ	МОНИТОРИНГ ОТКЛОНЕНИЙ

КОРРЕЛЯЦИЯ

ОЦЕНКА УРОВНЯ УГРОЗЫ ПО ПОЛЬЗОВАТЕЛЯМ / УСТРОЙСТВАМ

ПРИЛОЖЕНИЯ

Web Application Firewall следующего поколения

FW/IPS
FortiGate и Конкуренты

100% сигнатурный подход

Сильные стороны
- Одно устройство
- Обнаружение известных атак
- Простое ”1-click” развертывание

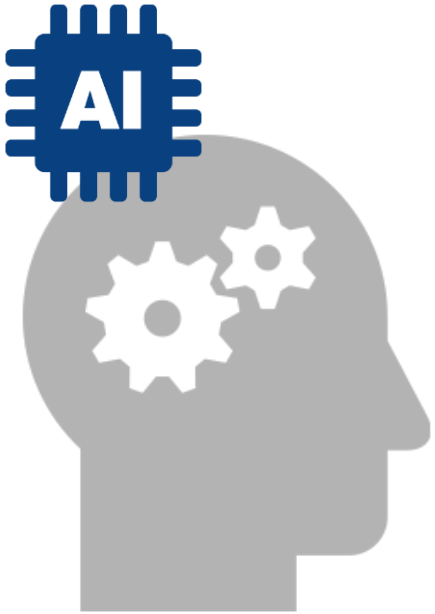
Слабые стороны
- Ограниченная поддержка HTTP
- Отсутствует мониторинг сессий
- Отсутствует анализ веб-приложений
- Отсутствует определение имени пользователя
- Отсутствует гибкий тюнинг
- Ограниченные настройки WAF

WAF
FortiWeb и Конкуренты

Построение модели приложения

Сильные стороны
- Сигнатуры + автоматическое сканирование
- Анализирует веб-приложение
- Понимает паттерны нормального трафика
- Обнаружение аномалий

Слабые стороны
- Частые False-Positive
- Трудоемкость тонкой настройки
- Модель не 100% строится
- Изменения требуют перестроения модели веб-приложения



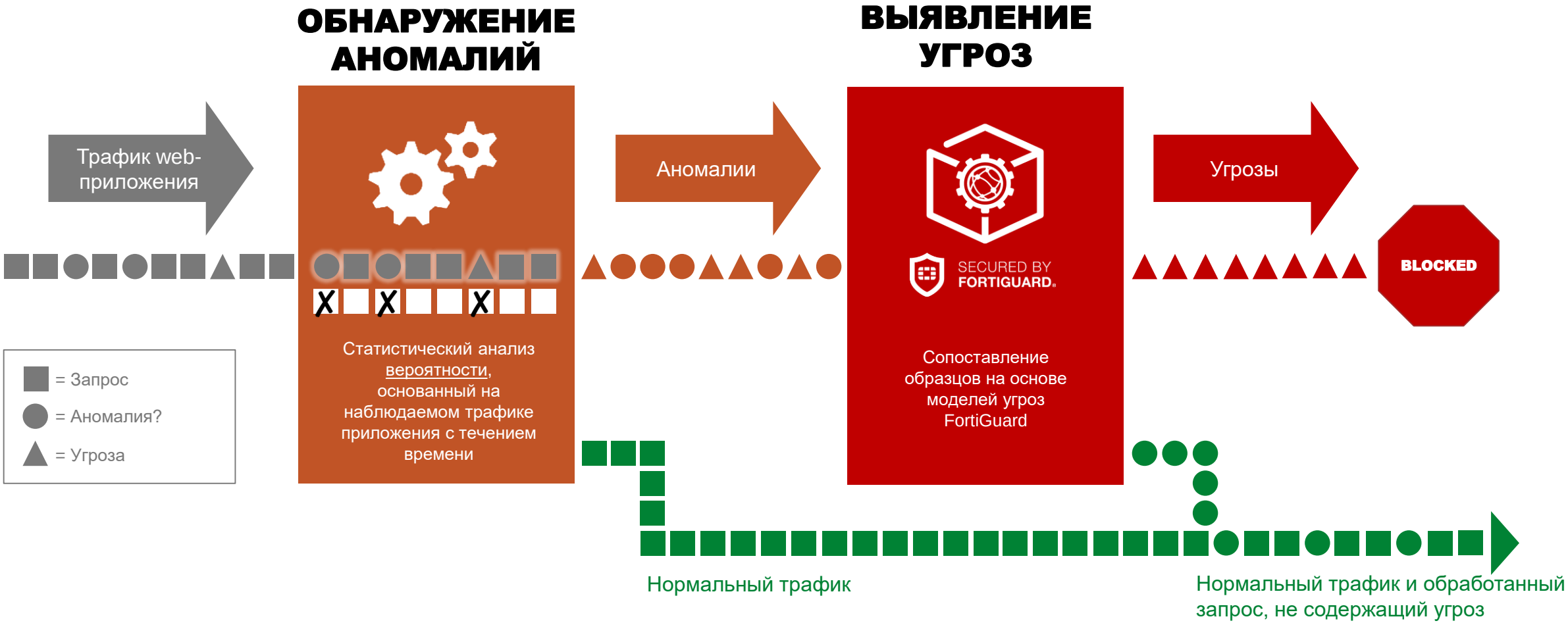
MACHINE LEARNING

Традиционный подход WAF к обучению

Известные проблемы/ограничения

- Блокирование всех аномалий приводит к высоким ложным срабатываниям
- Точность определения угроз требует тонкой настройки и трудоемкой работы
- Ненаблюдаемые вариации вызывают аномалии
- Белый список символов, используемых в атаках, позволяет избежать обнаружения угроз
- Изменения в приложении требуют повторного обучения

FortiWeb использует 2 этапа машинного обучения



Как работает Machine Learning в FortiWeb

https://www.example.com/insert?firstname=Mark&lastname=Smith

Пользователь отправляет "Mark Smith" в поле формы заявки NAME

FortiWeb ML ожидает только буквы в этом поле

FortiWeb ML видит этот трафик как **Нормальный Трафик Web-приложения**

ALLOWED

Normal Application Traffic

FortiWeb ML сопоставляет запрос с символами, ожидаемыми для данного поля и типичной длиной для него

https://www.example.com/insert?firstname=Janette&lastname=Smit&

Пользователь случайно отправляет «Janette Smit &» в поле формы заявки NAME

FortiWeb ML подтверждает АНОМАЛИЮ **как Аномалию с ОЖИДАЕМЫМ полем**

ALLOWED

Anomalies

ATTACKS

SECURED BY FORTIGUARD®

Support Vector Machine (SVM) отделяет угрозы от аномалий с использованием векторных паттернов от FortiGuard Labs

Пользователь отправил "SELECT *.* FROM CUSTOMER" в форме приложения NAME

FortiWeb ML с FortiGuard SVM подтвердил это как **Аномалию и АТАКУ**

BLOCKED

https://www.example.com/insert?firstname="SELECT *.* FROM CUSTOMER"

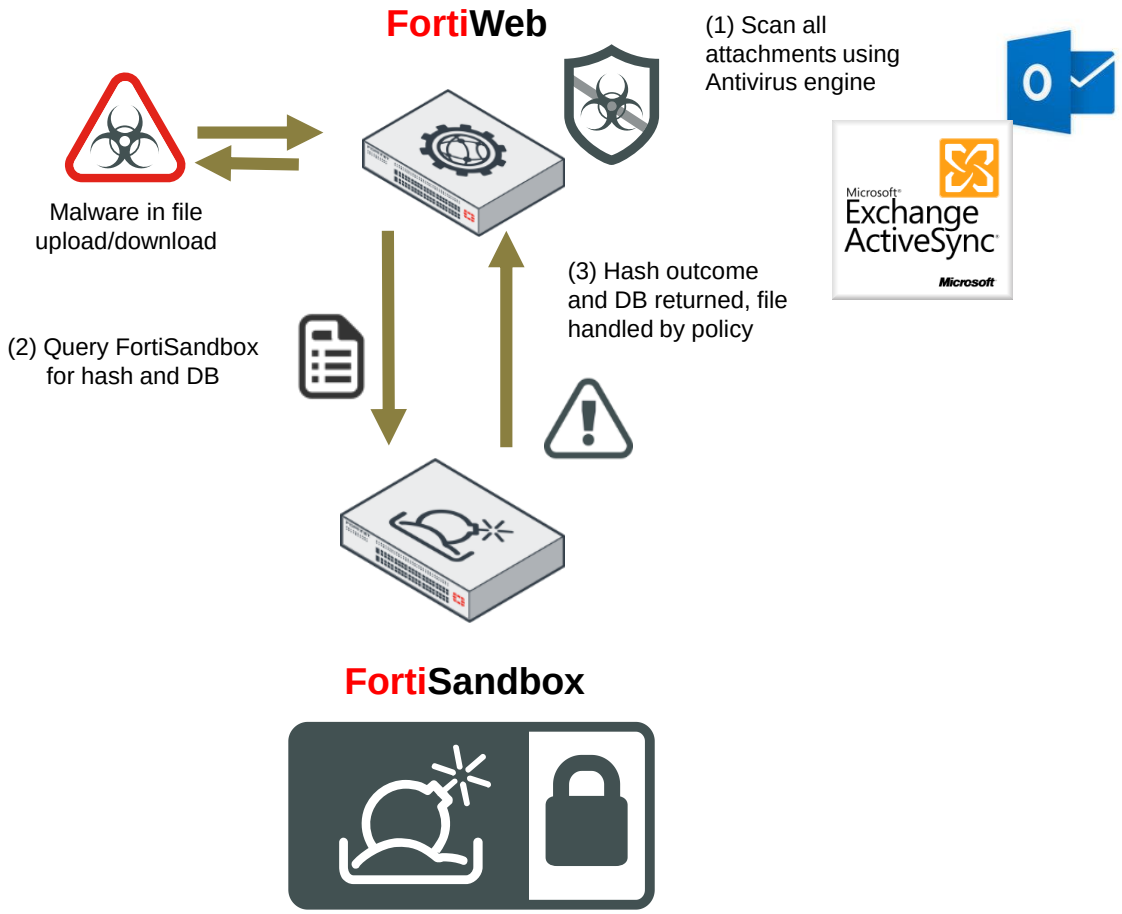
Application Learning vs. Machine Learning

	Application Learning	FortiWeb Machine Learning
Методология	Блокирование на основе отклонения от профиля	Блокирование аномалий которые подтверждены как реальные атаки
Построение профиля	• **Простой** • Добавление элементов HTTP трафика в профиль • Нет различия между «хорошими» и «плохими» символами, которые используются в атаках	• **Сложный** • Обучение, выполненное с использованием алгоритмов машинного обучения • Различный уровень угроз для разных групп символов
Определение атак	Разрешены ли символы в параметре профиля?	Какова вероятность атаки в запросе?
Перевод в режим блокирования	**Вручную**	**Автоматически**
Проверка атак	**Нет**	**Да**, используя второй этап машинного обучения
Лонжноположительные срабатывания	**Высокие** (Каждая аномалия блокируется, которая не соответствует профилю)	**Ограниченные** (Аномалии помечаются, а затем проверяются вторым этапом машинного обучения с целью обнаружения угрозы)
Необходимость тюнинга	**Высокая**	**Минимальная**
Изменения в web-приложениях	**Ограниченная адаптивность** (Разрешенный трафик может быть заблокирован до изменения профиля)	**Автоматически** (Разрешенный трафик не блокируется из-за наличия второго этапа)
Преимущества	• Есть возможность просматривать профиль • Простая концепция	• Легко развернуть и управлять • Не требуется ручное вмешательство • Минимальное количество false-positive

Функции - безопасности ATP

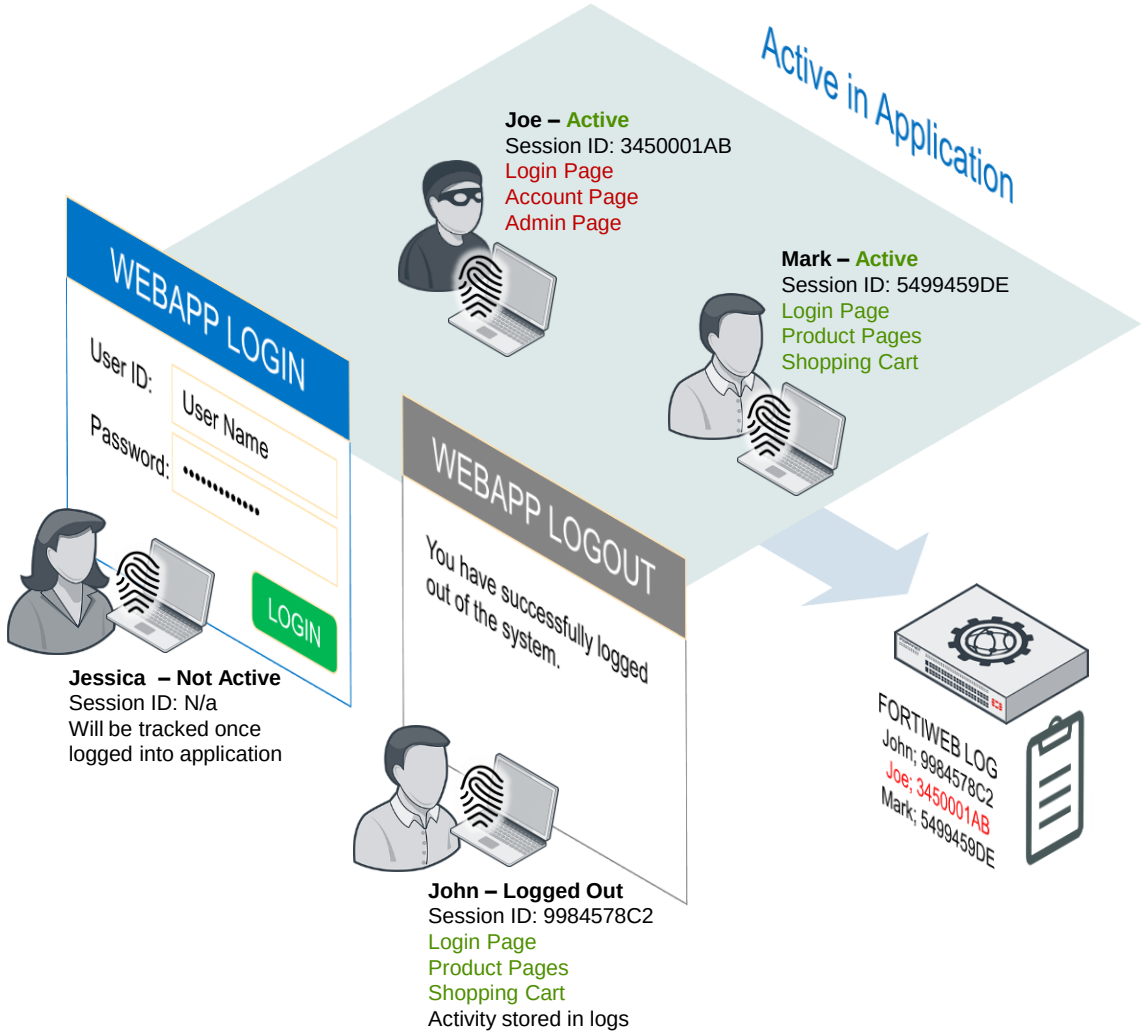
Файловая безопасность

- Сканирование вложений ActiveSync, OWA, MAPI модулем Антивируса, а также отправка в песочницу FortiSandbox
- Существующие решения защиты почты сканируют только SMTP трафик.



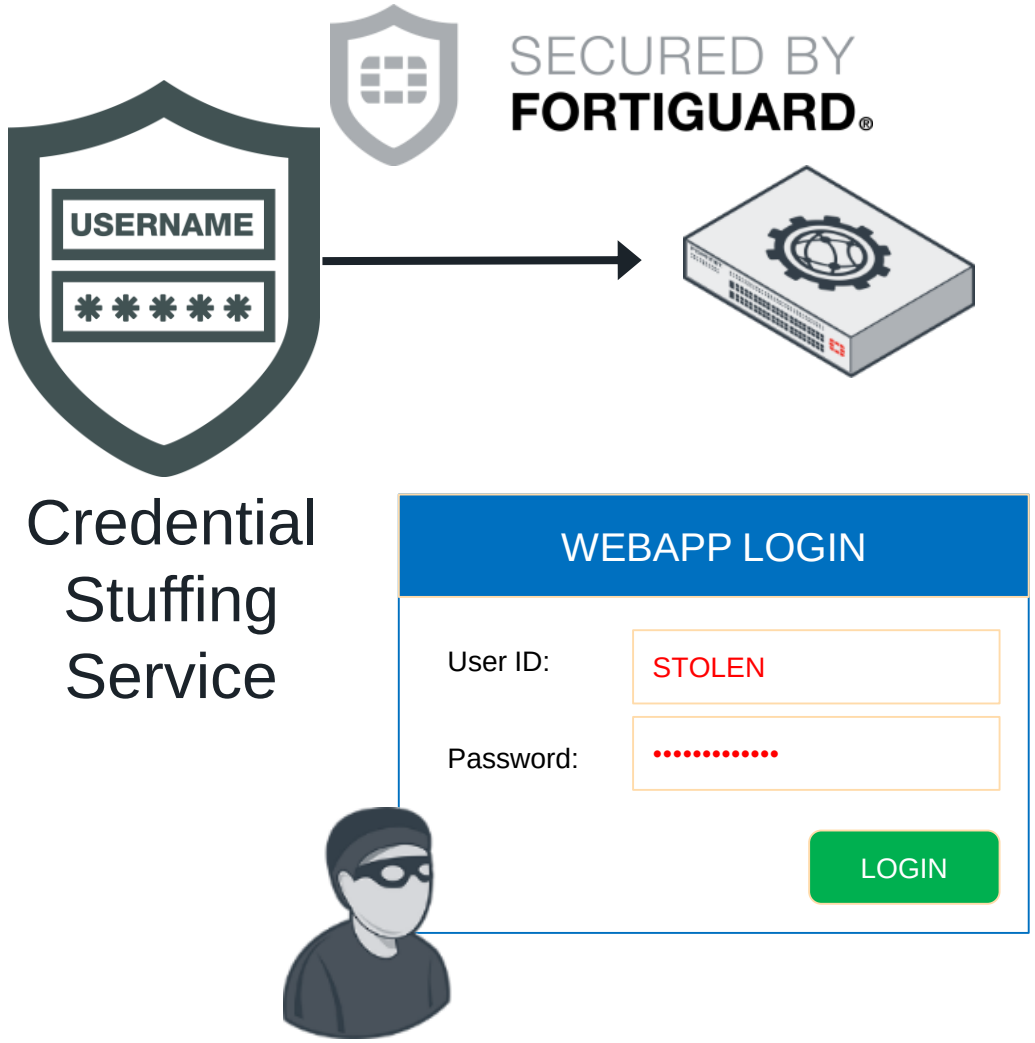
Отслеживание пользователей и устройств

- Для быстрого детектирования подозрительной активности и скомпрометированных пользователей и устройств
- Помогает при расследовании инцидентов
- Защита от существующих и будущих атак
- Как это работает:
  - » Автоматическое определение пользователей
  - » Отслеживание уникальных устройств
  - » Пользователи отслеживаются на протяжении всей сессии
  - » Подозрительная активность прослеживается до конечного пользователя
  - » Сохраняется информация для предотвращений будущих атак



Credential Stuffing Defense – сервис FortiGuard

- Credential Stuffing = использование (часто автоматизированное) скомпромитированных учётных данных для получения доступа
- База данных сервиса содержит скомпрометированные учётные данные крупных сервисов (Home Depot, Yahoo, Dropbox и других)



Основные преимущества WAF FortiWeb

Dynamic Vulnerability Patching	Real time threat protection
Dual Layer AI-based Machine Learning	Near 100% Accuracy
ActiveSync/MAPI Attachment Scanning	Closes email security gap
MS Application Publishing	Inexpensive and secure

FortiWeb Reviews: Gartner and NSS Labs

Gartner WAF MQ 2017:
Challenger

Source: Gartner (August 2017)

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose

NSS Labs 2017 WAF Testing:
Recommended

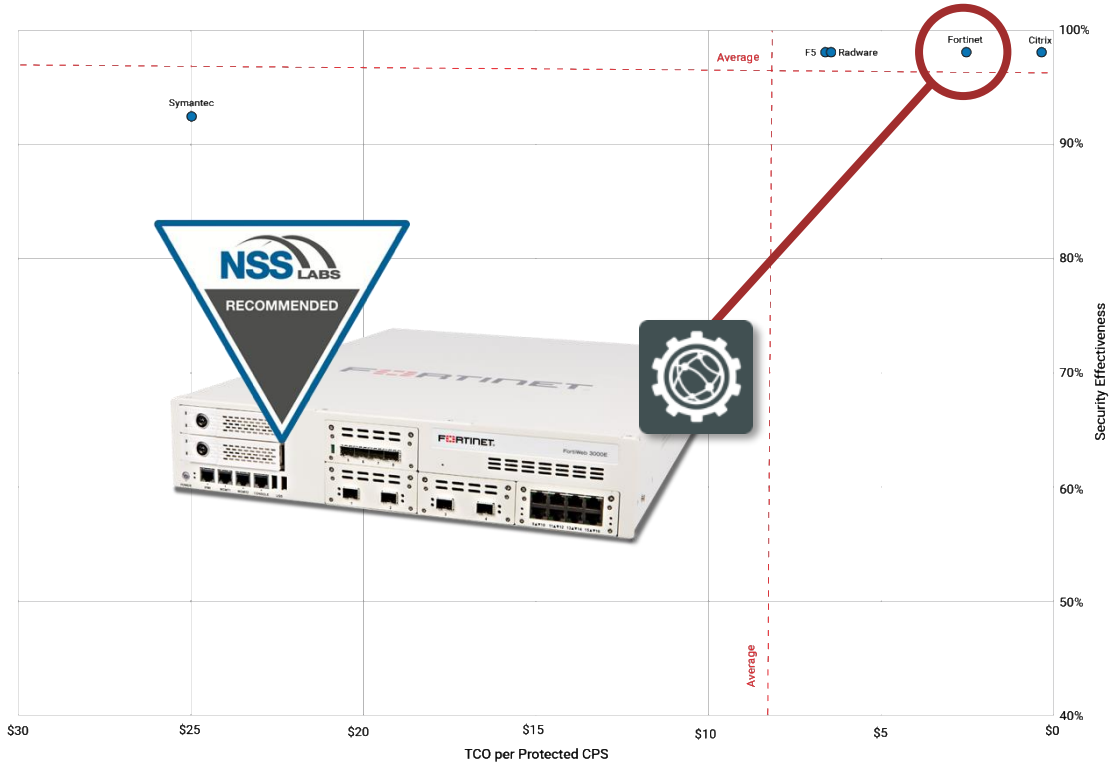


Figure 1 – NSS Labs' 2017 Security Value Map (SVM) for Web Application Firewall (WAF)


FORTINET®