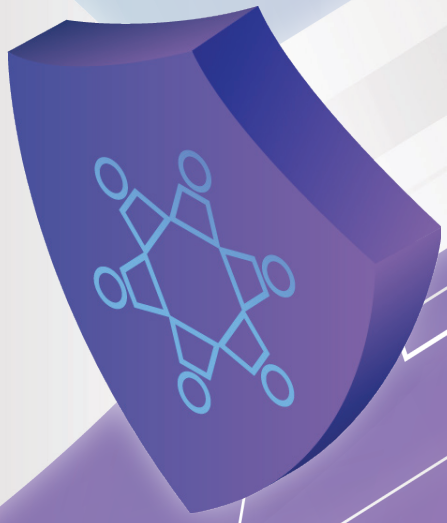
umv

WEB SERVER SECURITY
IN REAL-TIME



автоматическое обнаружение и реагирование на вредоносное ПО на сервере и несанкционированные изменения файлов для обеспечения непрерывности бизнеса и повышения устойчивости

umvwebsecurity.com

ВРЕДОНОСНЫЙ КОД, URL-АДРЕСА И ВЕБ-ОБОЛОЧКИ:
Сетевой безопасности недостаточно

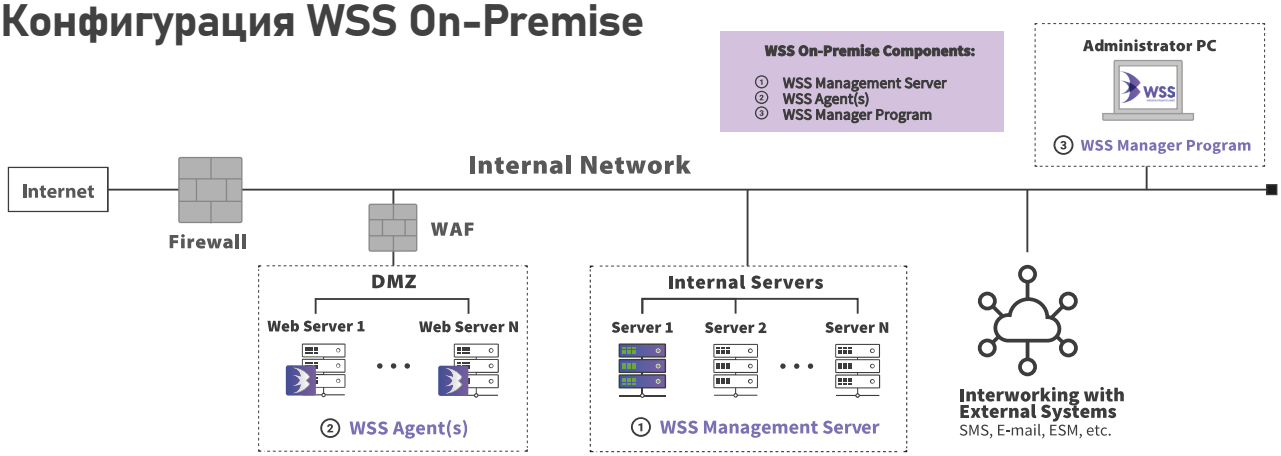
- Постоянное разнообразие методов вторжения делает меры сетевой безопасности на основе правил недостаточными
- Обнаружение сетевой безопасности ограничено (неполное сопоставление/фильтрация шаблонов, низкий уровень обнаружения обфусцированных/скрытых вредоносных программ)
- Ужесточение правил обнаружения сетей приводит к образованию узких мест и перебоям в обслуживании
- Обойдены внутренними субъектами угроз
- Ранее существовавшие инфекции в сетевых устройствах остаются не обнаруженными

ЗАЩИТИТЕ СВОИ ВЕБ-ДАННЫЕ С ПОМОЩЬЮ СИСТЕМЫ БЕЗОПАСНОСТИ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

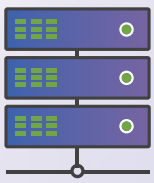
Разработанный компанией UMV Inc. продукт **W**eb **S**erver **S**afeguard (**WSS**) - это решение для повышения безопасности в режиме реального времени, предназначенное для интеграции в существующую инфраструктуру безопасности веб-серверов. Обнаруживая проникшие на сервер вредоносные URL-адреса, код и веб-оболочки, WSS мгновенно реагирует на угрозы, позволяя выявлять, помещать в карантин и управлять вредоносным ПО без задержек.

Благодаря полному набору параметров настройки и управления, а также передовым методам обнаружения, которые обнаруживают даже зашифрованные вредоносные программы, WSS предоставляет вашей команде безопасности возможность оперативно обнаруживать и реагировать на вредоносные веб-программы, не прерывая работу ваших веб-сервисов.

Конфигурация WSS On-Premise

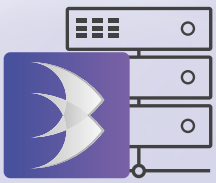


Трехкомпонентная структура WSS

① 

СЕРВЕР УПРАВЛЕНИЯ WSS

- Сохраняет историю обнаружения веб-оболочек
- Поддерживает удаленное управление
- Контролирует и распространяет обновления шаблонов веб-оболочек или изменения настроек для агентов
- Устанавливается на виртуальную машину или оборудование

② 

WSS-АГЕНТ

- Выполняет обнаружение веб-оболочек и вредоносных URL-адресов
- Передает результаты обнаружения и фильтрации на сервер управления
- Совместимо со всеми операционными системами, поддерживающими JDK 1.5+

③

МЕНЕДЖЕР WSS

- Управляет обнаружением, функциями и другими операциями
- Управляет настройками мониторинга, удаленного действия, конфигурации
- Осуществляет управление пользователями, статистику и отчетность
- Устанавливается на ПК администратора

НАШИ ПРОДУКТЫ

WSS On-Premise

- Решение для повышения безопасности веб-сервера
- Обнаруживает, помещает в карантин и сообщает о вредоносном веб-программном обеспечении в режиме реального времени
- Для локальной среды

WSS Cloud

- Предлагает все виды защиты WSS On-Premise с возможностью масштабирования и поддержкой Docker/Container
- Разработано для облачных вычислений (ВМ)

WARSS

- **W**ebsite **A**ttack **R**estoration **S**ecurity **S**olution
- Обнаруживает нежелательные изменения в содержимом веб-сайта и восстанавливает исходное содержимое в режиме реального времени
- Защищает от таких атак, как порча веб-сайта, подделка данных/исходного кода и подделка контента
- Также доступно для облака

ПОЧЕМУ РЕШЕНИЯ UMV?

ЗАЩИЩАЙТЕ
от атак на загрузку веб-оболочки

ПРОТИВОДЕЙСТВУЙТЕ
атакам с загрузкой вредоносного кода/URL

АВТОМАТИЧЕСКОЕ ВОССТАНОВЛЕНИЕ
файлов после несанкционированных изменений

ОСТАНОВИТЕ
вредоносное изменение настроек конфигурации

ЗАЩИЩАЙТЕ
личную информацию ваших клиентов

ПЕРЕХИТРИТЕ
попытки дефейса веб-сайта

УПРАВЛЯЙТЕ
и настраивайте с легкостью

ЗАЩИТИТЕ
свою облачную (ВМ)/ гибридную среду

Улучшите соответствие требованиям безопасности

ISO 27001 · NIST Cybersecurity Framework · AICPA SOC 2 (Formerly SAS 70 Reports) · CIS Critical Security Controls® Version 8.1 · NIS2 Directive

Использование продуктов UMV повышает соответствие различным глобальным стандартам кибербезопасности посредством:

- Автоматический **мониторинг** и **обнаружение** вредоносного ПО на веб-серверах
- Автоматическое **сдерживание** вредоносного ПО с помощью функций автоматического карантина
- Автоматическое обнаружение и **восстановление** непреднамеренных изменений файлов
- Тщательное **ведение журналов** и отчетов по действиям по обнаружению и смягчению последствий для аудитов

THE SECURITY CHAIN IS ONLY AS **STRONG** AS ITS **WEAKEST LINK**

Дополните архитектуру вашей веб-безопасности с помощью UMV

Наши клиенты

Продукты UMV защищают более 30 000 веб-серверов в локальных или облачных вычислительных средах по всему миру. Более 300 наших клиентов охватывают различные отрасли, включая бизнес, медицинские услуги, правительство, телекоммуникации, финансы, поставщиков интернета/данных и многое другое.

AhnLab · amazon web services · Microsoft Azure · SAMSUNG ELECTRONICS · TOYOTA
LOTTECARD · KDB Bank · BC CARD · SAMSUNG CARD · Hyundai Capital
Seoul Metro · HYUNDAI MOTOR GROUP · SEOUL METROPOLITAN GOVERNMENT · CHEONG WA DAE · Ministry of Foreign Affairs Republic of Korea
SAMSUNG SAMSUNG SDS · gabia. · SK securities · SK telecom · Kdata Korea Data Agency
Seoul Design 서울디자인재단 · S-OIL Corporation · Hi Seoul Soul of Asia · SUPREME COURT OF KOREA · cafe24
LOTTE DUTY FREE · ROBOTIS · NH Bank · SK infosec · kt
iMBC · STARBUCKS · Bluewalnut · AMOREPACIFIC · JOSUN HOTELS&RESORTS
BOANNEWS · KORAIL · Prudential · KBS Media · dun & bradstreet
daiso 다이소 · GS · DAEWOO E&C · SHINSEGAE · Hansol
Hanwha · Gmarket · Ministry of National Defense Republic of Korea · CJ CHEILJEDANG · AUCTION.

umv

umvwebsecurity.com
sales@umvglobal.com

ISTANBUL · SEOUL · ALMATY