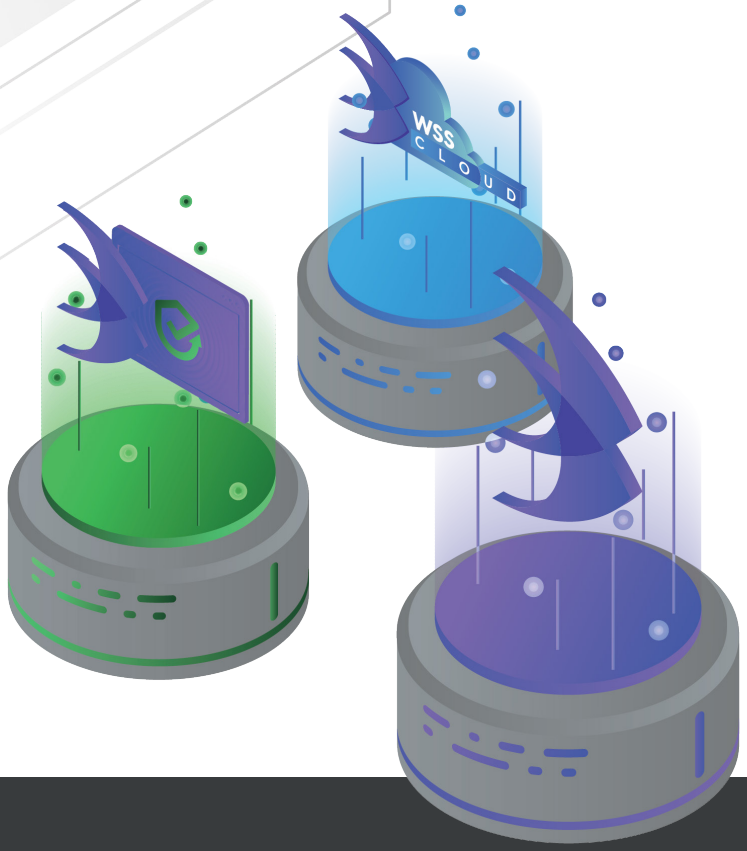
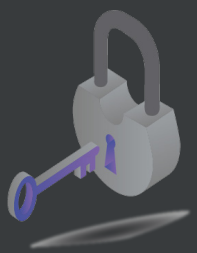
КОМПЛЕКСНЫЕ РЕШЕНИЯ БЕЗОПАСНОСТИ ДЛЯ ВЕБ-СЕРВЕРОВ И ПОЛЬЗОВАТЕЛЕЙ ВИРТУАЛЬНЫХ МАШИН



УКРЕПЛЕНИЕ ВЕБ-БЕЗОПАСНОСТИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕСПЕРЕБОЙНОГО ОБСЛУЖИВАНИЯ И КОМПЛЕКСНОЙ ЗАЩИТЫ



Обнаружение в реальном времени - Уведомление - Карантин - Действия по восстановлению

- ✓ **Защита от APT-атак**
- ✓ **Защита от веб-оболочки и атак установки вредоносных кодов/URL-адресов**
- ✓ **Обнаружение личной информации**
- ✓ **Предотвращение модификации файлов**
- ✓ **Обнаружение и восстановление повреждений веб-сайтов в режиме реального времени**

Важность безопасности веб-сервера реального времени

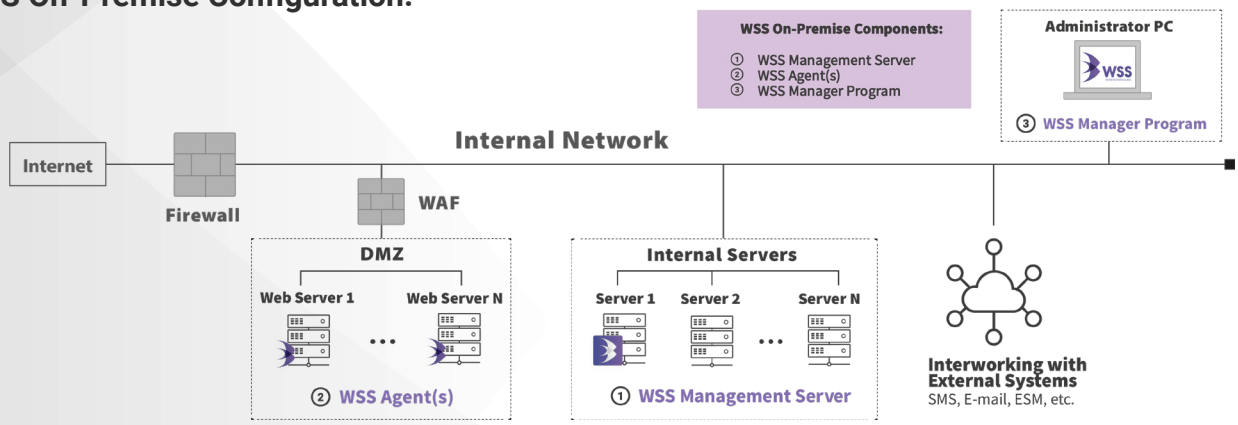
Только решения сетевой безопасности имеют ограничения для защиты от атак, использующих вредоносный код/URL, и установки веб-оболочки, которые могут просочиться через сетевую защиту.

- В связи с диверсификацией методов вторжения, только сетевых мер безопасности недостаточно (веб-оболочки, установленные на веб-сервере внутри системы, создают необходимость обнаружения/карантина вредоносных кодов в режиме реального времени)
- Обнаружение различных и разнообразных форм установки веб-оболочки невозможно с помощью только сетевых устройств безопасности
  - » Ограничения сопоставления шаблонов и фильтрации в сети
  - » Неизвестные/кодированные/зашифрованные/скрытые/трансформированные/фрагментированные веб-оболочки или вредоносный код
- Сложность фильтрации и сопоставления шаблонов, применяемых устройствами сетевой безопасности
- Перегрузка при обновлении и полный контроль
- Риски безопасности, вызванные не только внешними атаками, но и действиями внутренних сотрудников
- Увеличение проникновения с помощью методов обхода сети

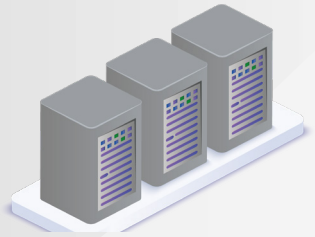
Комплексная защита данных, размещенных в Интернете, с помощью решения для обеспечения безопасности в режиме реального времени

Интегрированное и улучшающее безопасность решение обнаруживает вредоносные URL /коды или веб-оболочки, которым удалось пройти через уязвимости сети и подготовиться к атакам на систему, позволяя вам принять меры еще в момент атаки до того, как произойдет повреждение или кража данных. Таким образом, wss полностью покрывает ваши меры безопасности и не прерывает работу ваших веб-сервисов, защищая при этом ваш веб-сервер и веб-данные.

WSS On-Premise Configuration:



WSS, состоит из трехслойной структуры;



СЕРВЕР WSS S/W

- Хранение информации об обнаружении веб-оболочки
- Удаленный контроль управления
- Обновление шаблона веб-оболочки
- Функции распределения агентов
- Установка на виртуальную машину или оборудование

СРЕДСТВО ОБНАРУЖЕНИЯ WSS

- Обнаружение веб-оболочки и вредоносных URL
- Обнаружение личной информации
- Передача результатов обнаружения и фильтрации на сервер
- Совместимость со всеми операционными системами, поддерживаемыми JDK 1.5

МЕНЕДЖЕР WSS

- Функция обнаружения и работа
- Функции мониторинга, дистанционного действия, настройки среды
- Управление пользователями, статистика и отчетность
- Установка на контрольный и операционный
- компьютер системы безопасности

НАША ПРОДУКЦИЯ

WSS On-Premise

Комплексное решение для защиты веб-серверов, которое обнаруживает атаки в режиме реального времени и мгновенно реагирует на них для защиты информации на веб-серверах для локальных сред

Облако WSS

Комплексное решение безопасности, которое обнаруживает атаки в режиме реального времени и мгновенно реагирует на них для защиты веб-данных пользователей облачных вычислений (VM) и обеспечения бесперебойного предоставления услуг

WARSS

Решение для обеспечения безопасности веб-сайтов, которое обнаруживает атаки до нанесения ущерба веб-сайтам, такие как повреждение, подделка данных/кода источника и контента, заменяет веб-сервер на оригинальные источники в режиме реального времени

WSS КОМПЛЕКСНАЯ ЗАЩИТА ВЕБ-СЕРВЕРА В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Защита от атак на загрузку веб-оболочки

Предоставляет расширенные функции, такие как мониторинг, обнаружение, карантин, исключение, уведомление администратора с полным обнаружением и методами обнаружения в реальном времени, опасных веб-оболочек (ASP, JSP, PHP, CGI, Python script), которые пытаются быть установлены в системе после прохождения уязвимостей безопасности, а затем генерирует статистический отчет.

Защита от атаки загрузки вредоносного кода/URL

Для обнаружения и сообщения о вредоносном коде/URL-адресах используются методы полного обнаружения и обнаружения в реальном времени. Он классифицирует и сообщает об обнаружении в черном / белом / сером списке, обеспечивая при этом функции карантина, частичного карантина, исключения.

Предотвращение несанкционированного изменения файлов

Хакер может создать новую уязвимость в системе путем подмены файлов в настройках веб-сервера, заложив основу для следующей атаки. WSS обнаруживает изменения на веб-сервере в режиме реального времени и обеспечивает комплексную защиту, предотвращая изменения файлов.

Предотвращение изменения параметров конфигурации

Обнаруживает случайные или злонамеренные изменения в конфигурационных файлах веб-сервера и немедленно сообщает об обнаруженном IP-адресе злоумышленника администратору, анализируя журнал веб-сервера/ WAS.

Обнаружение личной информации

Контролируя содержимое файлов на веб-серверах в режиме реального времени, обеспечивает обнаружение личной информации в файлах или в базе данных (PDF , HWP , DOC , PPT , EXCEL , TXT и т.д.) и мгновенно сообщает об этом уполномоченному лицу.

Безопасность облачных вычислительных машин (VM)

Поддерживает контейнеры Docker, WEB/WAS службы Scale IN/OUT, обнаружение/изменение/удаление, авторегистрацию, автоматическое обнаружение домашнего каталога, управление репликацией событий, управление историей, управление безопасностью и многое другое.

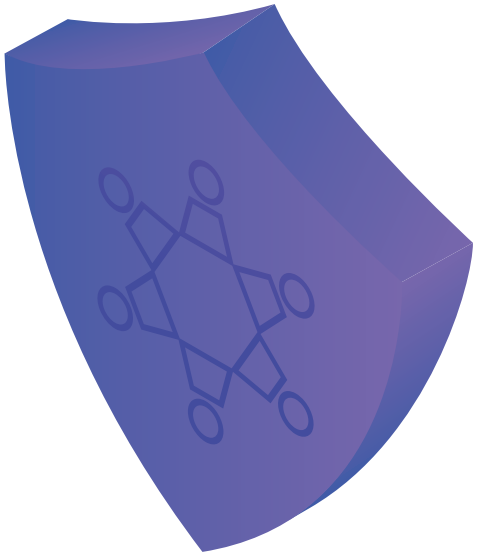
Решение для атаки на повреждение веб-сайта

WARSS (Website Attack Restoration Security Solution) восстанавливает оригинальные ресурсы (исходный код, данные, содержимое) веб-сайта в реальном времени для предотвращения и защиты от атак подделки, таких как атаки на повреждение веб-сайта, атаки подделки исходного кода и данных веб-сервера, атаки изменения файлов цифрового содержимого (видео, изображения).

Особенности управления WSS

Обеспечивает различные функции управления, такие как простое обновление, управление авторизацией, работа с внешними системами (такими как SYSLOG, SMTP, API / ESM /SIEM /SMS /MAIL и т.д.), автоматическое обнаружение и резервное копирование целевого каталога, фильтрация неавторизованных расширений, настройка использования источника (CPU/память), поддержка двунаправленной репликации (активная/активная), удаленная аутентификация и многое другое.

Цепь сильна лишь настолько, насколько сильно ее самое слабое звено



Завершите меры по обеспечению веб-безопасности

Наши рекомендации

Продукты UMV подходят для использования в локальных или облачных вычислительных средах, таких как коммерческие предприятия, медицинские компании, государственные учреждения, телекоммуникации, финансовые учреждения, компании по контролю безопасности, центры обработки данных в Интернете.

AhnLab · STARBUCKS · amazon web services · SAMSUNG ELECTRONICS · TOYOTA

LOTTECARD · KDB Bank · BC CARD · SAMSUNG CARD · Hyundai Capital

Seoul Metro · HYUNDAI MOTOR GROUP · SEOUL METROPOLITAN GOVERNMENT · THE REPUBLIC OF KOREA CHEONG WA DAE · Ministry of Foreign Affairs Republic of Korea

SAMSUNG SAMSUNG SDS · gabia. · SK securities · SK telecom · K data 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 · YTN · PANTECH · AMOREPACIFIC · JOSUN HOTELS&RESORTS

BOANNEWS · KORAIL · Prudential · KBS Media · dun & bradstreet

다이소 daiso · GS · DAEWOO E&C · SHINSEGAE · Hansol

Hanwha · Gmarket · Ministry of National Defense Republic of Korea · CJ CHEILJEDANG · AUCTION.

umv

www.umvwebsecurity.com