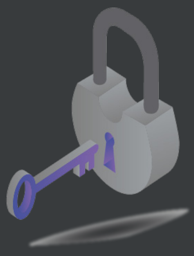
umv

COMPREHENSIVE SECURITY SOLUTIONS FOR WEB SERVERS AND VM USERS

STRENGTHEN YOUR WEB SECURITY AND PROVIDE UNINTERRUPTED SERVICES



Real Time Detection - Notification - Quarantine - Restoration Functions

- ✓ Defense Against APT Attacks
- ✓ Defense Against Web Shell And Malicious Codes/URLs Installation Attacks
- ✓ Personal Information Detection
- ✓ File Modification Prevention
- ✓ Website Defacement Real-Time Detection & Restoration

Equipping you with
Real-Time Web Security

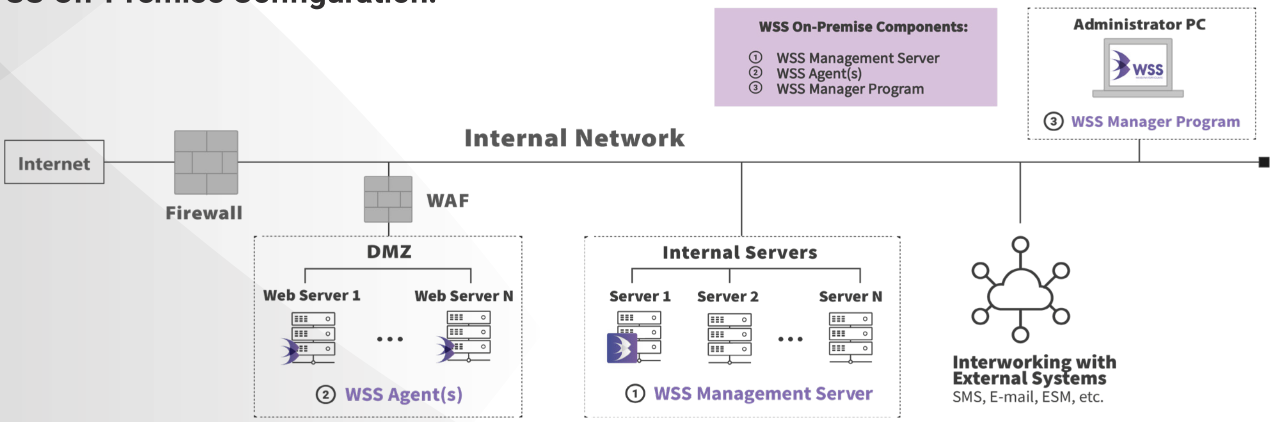
MALICIOUS CODE, URLs, AND WEB SHELLS: Network security isn't enough

- Constant diversification of intrusion methods renders rule-based network security measures insufficient (web shells attacks call for real-time detection and response)
- Network security detection is limited (incomplete pattern matching/filtering, low detection of obfuscated/hidden malware)
- Stricter detection rules cause bottlenecking and service interruptions
- Bypassed by internal threat actors
- Pre-existing infections in network devices go undetected

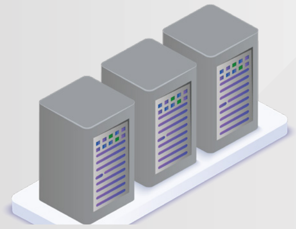
PROTECT YOUR WEB-BASED DATA WITH REAL-TIME SECURITY

Web Server Safeguard (**WSS**), developed by UMV Inc., is a real-time security booster solution designed to **integrate seamlessly** into existing web server security infrastructure. Detecting malicious URLs, code, and web shells that have infiltrated a system, WSS reacts in **real-time** to incoming threats, enabling you to **discover**, **quarantine**, and **manage** malware in an instant. Complete with a full suite of configuration and management options, WSS equips your security team with the agility to respond to and mitigate web-based malware without interrupting your web services.

WSS On-Premise Configuration:



WSS's 3-Component Structure



WSS MANAGEMENT SERVER

- Detection, function, and operation management
- Monitoring, remote action, configuration settings
- User management, statistics and reporting
- Installed on an administrator PC

WSS AGENT

- Web shell and malicious URL detection
- Personal information detection
- Forwards detection and filtering results to server
- Compatible with all operating systems supporting JDK 1.5

WSS MANAGER PROGRAM

- Stores web shell detection history
- Remote management control
- Web shell pattern updates
- Distributes settings changes/ updates to Agents
- Installed on VM or hardware

OUR PRODUCTS

WSS On-Premise

- Web server security booster solution that detects, quarantines, and reports web-based malware in real-time
- For on-premise environments

WSS Cloud

- Enjoy all the protections of WSS On-Premise with scale-in/-out and Docker/Container support
- Tailored for cloud computing (VMs)

WARSS

- Website security solution that detects unwanted changes to website content and restores original content in real-time
- Prevents attacks like website defacement , data/ source code forgery, and content forgery

WSS
INFORMATION SECURITY WITH UNINTERRUPTED SERVICE
Webserver Security Solution
On-Premise
Security booster solution for webservers, protecting information data and providing uninterrupted service
umv
WSS CLOUD
Webserver Security Solution
CLOUD
Security booster solution for cloud computing (VM), protecting information data and providing uninterrupted service
WARSS
Website Attack Restoration & Security Solution
Best software solution for real-time website recovery and restoration solution before hacking attack and damage

WHY UMV'S SOLUTIONS?

DEFEND against web shell upload attacks

WSS allows you to monitor, detect, quarantine, set exceptions, and notify administrators of web shell scripts (.asp, .jsp, .php, .cgi, .py, etc.) in real-time, keeping your system safe even when network security systems have been compromised.

PREVENT unauthorized file modification

WSS detects changes to web server files in real-time, allowing you to stay one step ahead of threat actors tampering with web server settings to lay down groundwork for further attacks.

PROTECT personal information

WSS monitors web server file content in real-time, allowing for the detection of personal information in database files (.pdf, .hwp, .docx, .pptx, .xlsx, .txt, etc.) and instant reporting to an administrator.

MANAGE and customize with ease

WSS, WSS Cloud, and WARSS give you full control with management fuctions such as automated updates, authorization management, linking with external systems (such as syslog, SMTP, APIs, ESMs, SIEMs, SMS, etc.), auto-detection of target directories, automated backups, filtering for unauthorized extensions, resource usage settings (CPU/memory), bidirectional replication support (active/active), remote authentication, and more.

COUNTER malicious code/URL upload attacks

WSS's full detection and real-time detection techniques are applied to detect and report malicious code/URLs. Use diverse management options to categorize and report detected code/URLs via Black/White/Gray-Listing as well as quarantines, partial quarantines, and exceptions.

STOP configuration settings modification

WSS detects malicious changes to web server configuration files and immediately notifies the administrator of the changes, along with a report including attacker IP.

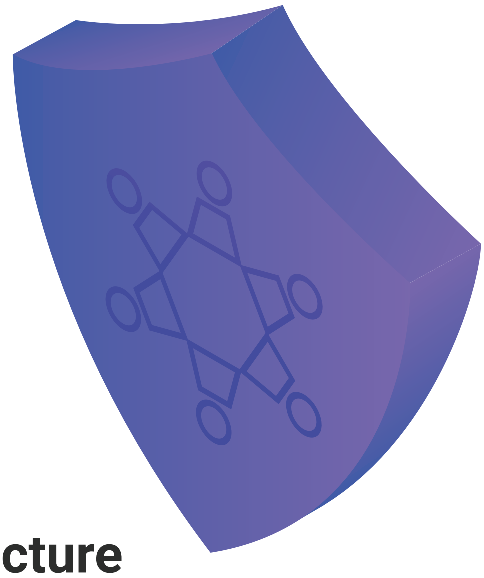
SECURE your cloud servers (VM)

WSS Cloud provides full support for cloud environments, including support for docker containers, web/WAS services, scale-in/-out, detection/change/deletion history preservation, auto-detection of home directories, event replication management, history management, security management and more.

OUTSMART website defacement attempts

WARSS (Website Attack Restoration Security Solution) restores the original resources (source code, data, contents) of a website in real -time to prevent and defend against forgery attacks such as website defacement, web server source code and data forgery, and/or unauthorized digital content (video, image) file modification.

The security chain is only as strong as its weakest link



Complete your web security architectucture

Our References

UMV products are suitable for use in **on-premise** or **cloud computing** environments of **all sectors**, like business enterprises, medical companies, government agencies, telecommunications, financial institutions, security control companies, internet data centers, and more.

AhnLab · amazon web services · STARBUCKS · 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

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

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

umv

www.umvwebsecurity.com
sales@umvglobal.com