umv

WEB SERVER SECURITY
IN REAL-TIME

automated detection & response for
server malware and unauthorized file changes
– for business continuity and improved resilience

umvwebsecurity.com

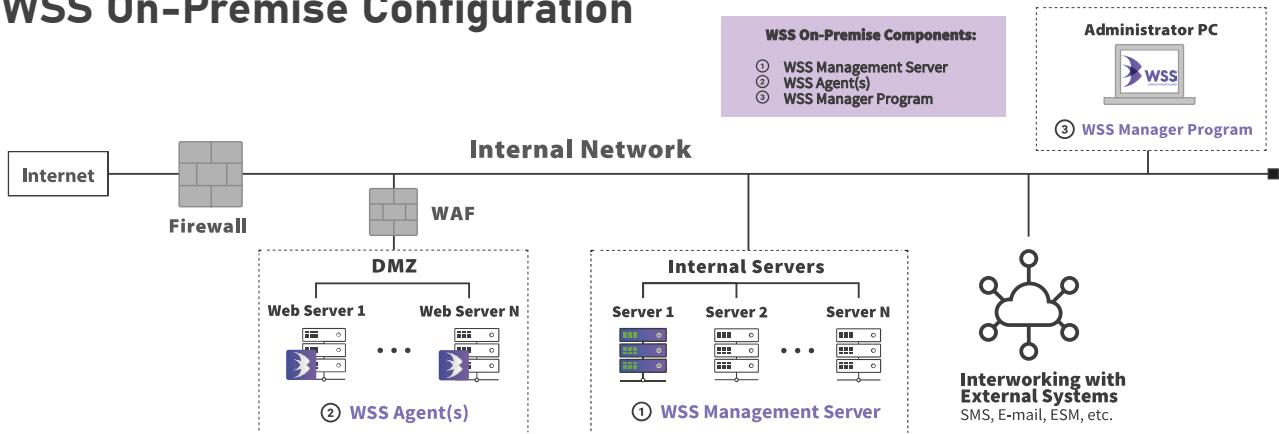# MALICIOUS CODE, URLs, AND WEB SHELLS:
Network security isn't enough

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

SAFEGUARD YOUR WEB-BASED DATA WITH REAL-TIME SECURITY

Developed by UMV Inc., **W**eb **S**erver **S**afeguard (**WSS**) is a real-time security enhancement solution designed to integrate seamlessly into existing web server security infrastructures. By detecting infiltrated malicious URLs, code, and web shells, WSS reacts instantly to threats—allowing you to identify, quarantine, and manage malware without delay.

Complete with a full suite of configuration and management options, as well as state-of-the-art detection methods that catch even encrypted malware, WSS equips your security team with the agility to uncover and respond to web-based malware without interrupting your web services.

WSS On-Premise Configuration

WSS On-Premise Components:
① WSS Management Server
② WSS Agent(s)
③ WSS Manager Program

Administrator PC
③ WSS Manager Program

Internal Network

Internet — Firewall — WAF

DMZ
Web Server 1 ... Web Server N
② WSS Agent(s)

Internal Servers
Server 1   Server 2 ... Server N
① WSS Management Server

Interworking with External Systems
SMS, E-mail, ESM, etc.

WSS's 3-Component Structure

①
WSS MANAGEMENT SERVER
- Stores web shell detection history
- Supports remote management
- Controls and distributes web shell pattern updates or settings changes to Agents
- Installed on VM or hardware
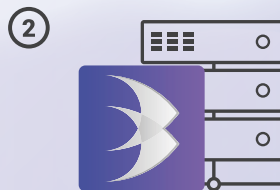
②
WSS AGENT
- Performs web shell, malicious URL, and personal information detection
- Forwards detection and filtering results to Management Server
- Compatible with all operating systems supporting JDK 1.5+

③
WSS MANAGER
- Manages detection and functions
- Controls settings for monitoring, remote action, configuration
- Performs user management, statistics, and reporting
- Installed on administrator PC

OUR PRODUCTS

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

WSS On-Premise
- Web server security booster solution
- Detects, quarantines, and reports web-based malware in real-time
- For on-premise environments

WARSS
- **W**ebsite **A**ttack **R**estoration **S**ecurity **S**olution
- Detects unwanted changes to website content and restores original content in real-time
- Protects against attacks such as website defacement, data/source code forgery, and content forgery
- Also available for cloud

WHY UMV SOLUTIONS?

DEFEND
against web shell upload attacks

COUNTER
malicious code/URL upload attacks

AUTO-RESTORE
files upon unauthorized changes

STOP
malicious configuration settings modification

PROTECT
your clients' personal information

OUTSMART
website defacement attempts

MANAGE
and customize with ease

SECURE
your cloud (VM)/hybrid environment

Improve your security compliance

ISO 27001 · NIST Cybersecurity Framework · AICPA SOC 2 · CIS Critical Security Controls Version 8.1 · NIS2 Directive

Employing UMV products strengthen compliance with various global cybersecurity frameworks via:

- Automatic **monitoring** and **detection** of web-based server malware
- Automated **containment** of malware through auto-quarantine functions
- Automatic detection and **recovery** of unintended file modifications
- Thorough **logging** and reports on detection and mitigations actions for audits

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

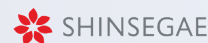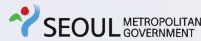## Complete your web security architecture with UMV

Our Customers

UMV products secure 30,000+ web servers in on-premise or cloud computing environments worldwide. Our 300+ customers span diverse industries, including business, medical services, government, telecommunications, finance, internet/data providers, and more.

AhnLab · amazon web services · Microsoft Azure · SAMSUNG ELECTRONICS · TOYOTA

LOTTE CARD · 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 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 · 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