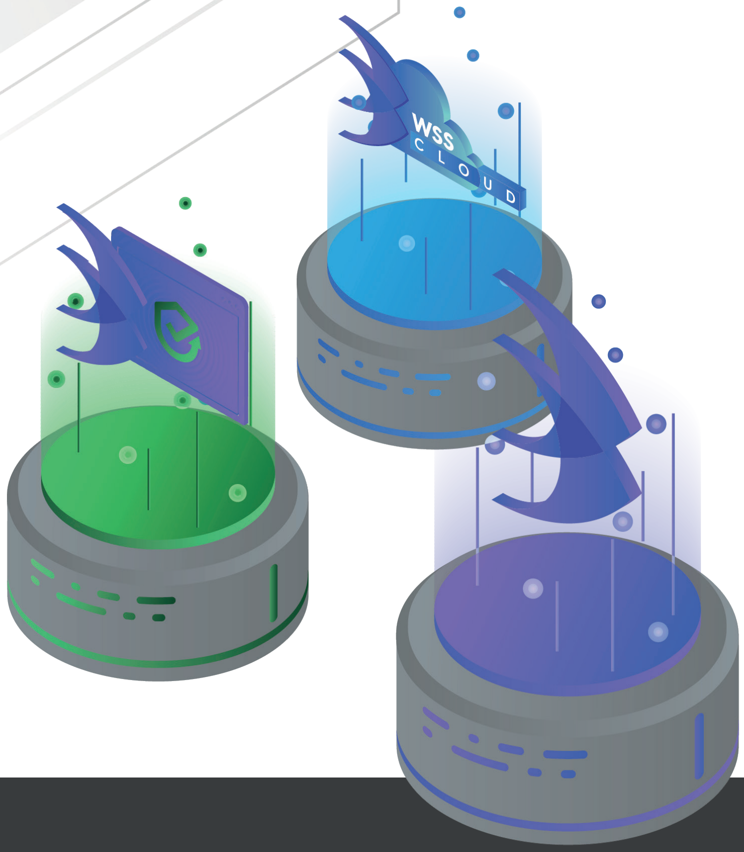
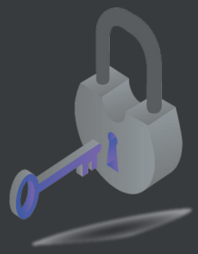
umv

COMPREHENSIVE SECURITY SOLUTIONS FOR WEB SERVERS AND VM USERS



STRENGTHEN YOUR WEB SECURITY FOR UNINTERRUPTED SERVICE AND COMPREHENSIVE SECURITY



Real Time Detection - Notification - Quarantine - Restoration Actions

- ✓ 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

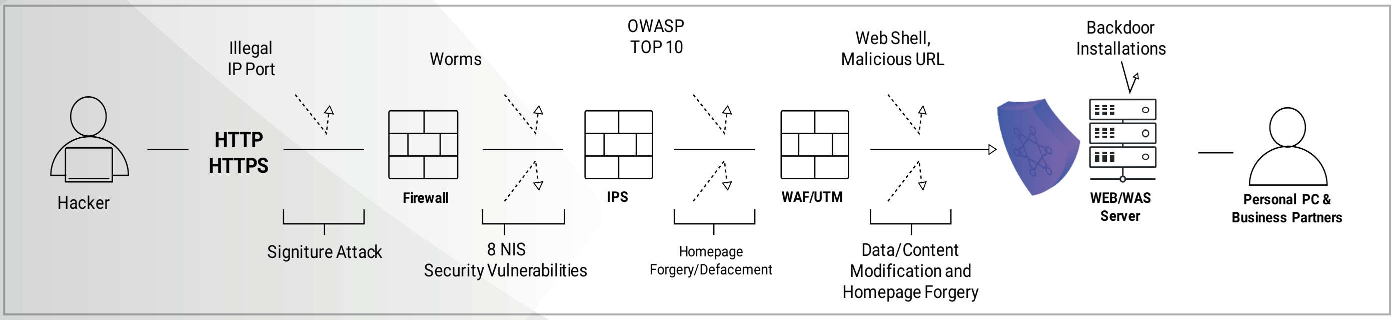
Importance of Real-Time Web Server Security

Only network security solutions has limitations to defend against attacks that use malicious code/URL, and web shell installations that can leak through network security.

- Due to the diversification of intrusion methods, only network security measures are insufficient (web shells installed on the web server within the system create the need to detect/quarantine malicious codes in real time)
- Detection against various and different forms of web shell installation is not possible with only network security devices alone
  - Limitations of pattern matching and filtering in network
  - Unknown/encoded/encrypted/hidden/transformed/fragmented web shells or malicious code
- Difficulty in filtering and pattern matching applied by network security devices
- Overload on update and full control
- Security risks caused not only by external attacks, but also by internal employees
- Increase in penetration with network bypass methods

Protect Your Web-Based Data Comprehensively With Real-Time Security Solution

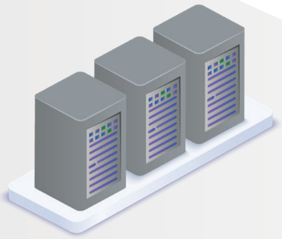
Integrated and enhancing security solution detects malicious URL /codes or web shells that succesed to pass through the vulnerabilities of the network and prepare to cause attacks on the system, allowing you to take action even at the time of attack before any attack damage or data theft occurs. Thus, wss fully covers your security measures and does not interrupt your web services while protecting your web server and web-based data.



WSS, Consists of Three Layer Structure;

WSS DETECTION AGENT

- Web shell and malicious URL detection
- Personal information detection
- Forwarding detection and filtering results to the server
- Compatibility with all operating systems supported by JDK 1.5



WSS SERVER S/W

- Web shell detection information storage
- Remote management control
- Web shell pattern update
- Agent distribution functions
- Installation on VM or hardware

WSS MANAGER

- Detection function and operation
- Monitoring, remote action, environment setting functions
- User management, statistics and reporting
- Installation on security control and operating computer

OUR PRODUCS

WSS On-Premise

Comprehensive web server security solution that detects attacks in real time and responds instantly to protect web-based information on web servers for on-premise environments

WSS Cloud

Comprehensive security solution that detects attacks in real-time and responds instantly to protect web-based data of cloud computing (VM) users and provides uninterrupted services

WARSS

Website security solution that detects attacks before websites are damaged , such as defacement , data/source code and content forgery, replaces web server to the original sources in real time

WSS
WEBSERVERSAFEGUARD
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
URITY WITH UNINTERRUPTED SERVICE
Webserver
Security Solution
CLOUD
Security booster solution for cloud computing (VM), protecting information data and providing uninterrupted service
WARSS
WEBSITE ATTACK RESTORATION & SECURITY SOLUTION
URITY WITH UNINTERRUPTED SERVICE
WARSS
Website Attack Restoration
& Security Solution
Best software solution for real-time website recovery and restoration solution before hacking attack and damage

WSS COMPREHENSIVE REAL-TIME WEB SERVER SECURITY

Web Shell Upload Attack Defense

Provides advanced functions such as monitoring, detection, quarantine, exception , administrator notification with full detection and real-time detection methods, of dangerous web shells (ASP , JSP , PHP , CGI , Python script) that are tried to be installed on the system after passing the security vulnerabilities and then generates a statistical report.

Unauthorized File Modification Prevention

A hacker can create a new vulnerability in the system through file tampering in the web server settings , laying the groundwork for the next attack. WSS detects changes in the web server in real time , provides comprehensive defense by preventing file changes.

Personal Information Detection

By monitoring the file contents on web servers in real-time, provides detection of personal information in files or in the database (PDF , HWP , DOC , PPT , EXCEL , TXT , etc.) and instantly reports it to the authorized person.

Web Site Defacement Attack Solution

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 attacks, web server source code and data forgery attacks , digital content (videos , pictures) file change attacks.

Malicious Code/URL Upload Attack Defense

Full detection and real-time detection techniques are used to detect and report malicious code/URLs. It categorizes and reports detections in black /white / grey list while providing quarantine, partial quarantine, exception functions.

Configuration Settings Modification Prevention

Detects the hacker 's random or malicious changes to the web server configuration files and immediately notifies to and reports the detected attacker IP to the administrator by analyzing the web server/ WAS log.

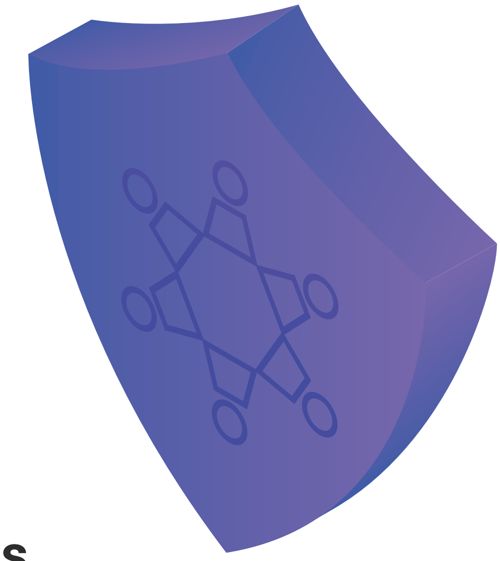
Cloud Computimg (VM) Security

Supports Docker containers, WEB/WAS service Scale IN/OUT, detect/ change/ delete, auto-registers, home directory auto detection, event replication management, history management, security management and more.

WSS Management Features

Provides various management functions such as easy update, authorization management , working with external system (such as SYSLOG , SMTP , API / ESM /SIEM /SMS /MAIL etc.), target directory automatic detection and backup, unauthorized extension filtering, source usage setting (CPU/memory), bidirectional replication support (active/active), remote authentication and more.

A Chain is Only as Strong as it‘s weakest link



Complete Your Web Security Measures

Our References

UMV products are suitable for use in on -premise or cloud computing environments such as business enterprises, medical companies, government agencies, telecommunications, financial institutions, security control companies, internet data centers.

AhnLab	docker	amazon web services	SAMSUNG ELECTRONICS	TOYOTA
LOTTECARD	STARBUCKS	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 Corporatio	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