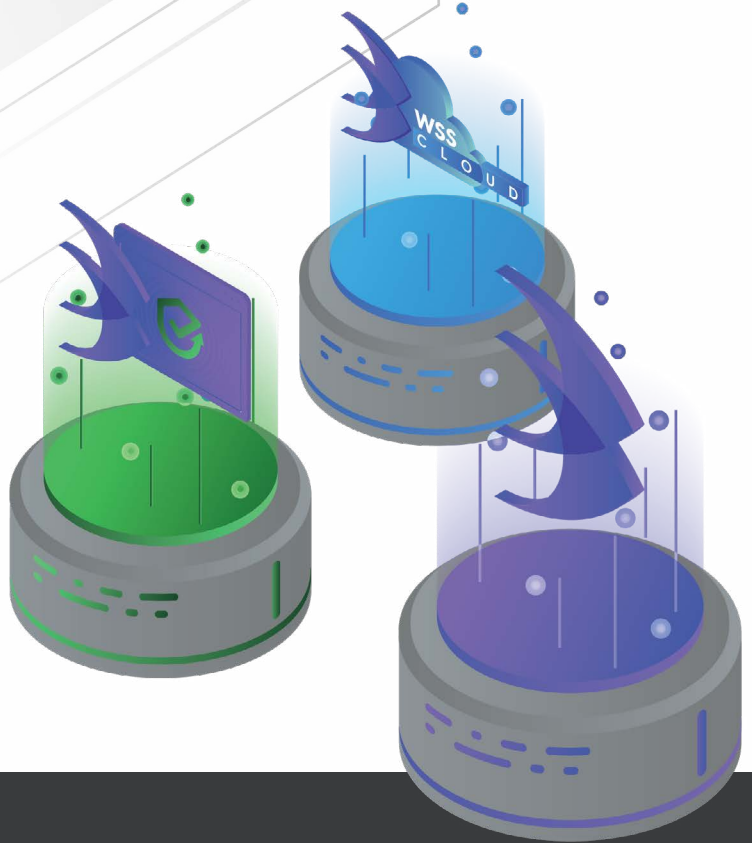
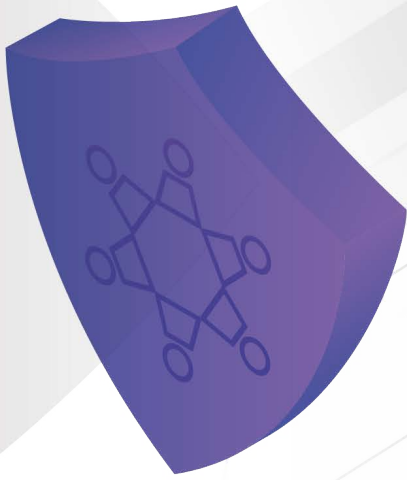
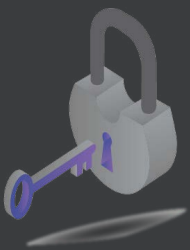




웹 서버 및 클라우드 컴퓨팅 통합 보안 솔루션



**Provides Integrated
Web Security Solutions
With Uninterrupted Service**



실시간 탐지 - 알림 - 검역 - 복원

- ✓ APT 공격 방어
- ✓ 개인 정보 탐지
- ✓ 중요 파일 변경 방지
- ✓ 웹쉘 및 악성코드 업로드 공격 방어
- ✓ 웹사이트 위변조 탐지 및 즉시 복원

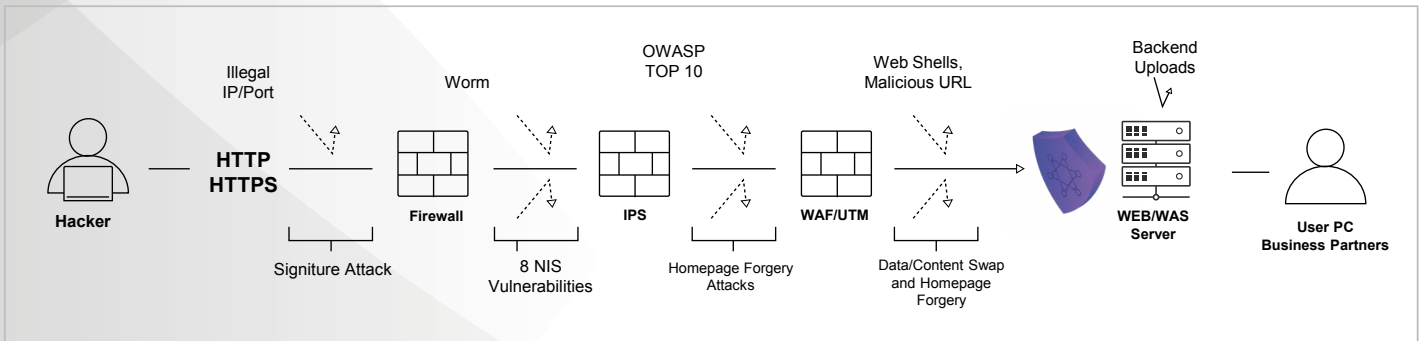


Real-Time 웹 서버 보안 중요성

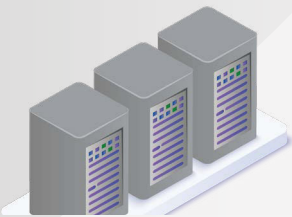
- 다양한 취약점을 이용한 해커의 공격을 방어하기 위해서는 기존의 네트워크 보안 솔루션만으로는 신속한 대응과 완벽한 방어의 어려움이 있습니다. 웹서버 보안은 집요하고 지능적인 해킹에 대하여 능동적이고 즉각적인 대응이 필요합니다
- 해킹의 다양화로 인한 네트워크 방어를 보완하는 시스템 보안 솔루션 필요
- 우회 기술 발달로 시스템에 업로드된 웹셸 및 Malware 등에 대한 탐지/격리 필요
 - 다양한 형태의 웹셸 침투에 대응하는 네트워크 보안장비의 한계
- 신규 패턴의 웹셸 / 여러 번 암호화 된 웹셸 / 짧게 단편화 / 변형된 패턴의 웹셸
 - 네트워크에 영향을 미치는 웹셸 및 Malware 탐지를 위한 패턴 매칭의 어려움
 - 외부 공격뿐만 아니라 악의적인 내부 직원에 의한 인적 보안 위험성에 대처가 필요
- 내부 네트워크에서 시스템에서 업로드된 웹셸 및 Malware에 대한 탐지/격리 필요

실시간 웹 기반 정보 보안 솔루션

WSS는 네트워크 취약점을 이용해 지능적이고 지속적인 공격을 위한 기반을 마련하는 웹셸 및 악성 URL을 실시간 탐지하여 해킹 피해 및 정보 도난 등 기업의 손실을 예방하며, 공격이 발생하더라도 중단 없는 웹a 서비스를 제공하며 기업의 웹 기반 데이터를 안전하게 보호합니다.



WSS 구성 (관리 서버, 에이전트, 매니저 프로그램)



WSS 관리 서버

- 탐지된 이력 및 탐지 정보 저장
- 원격 관리 제어
- 웹셸 패턴 업데이트 및 에이전트 배포 외
- VM 또는 하드웨어에 설치



WSS 탐지 에이전트

- 웹셸 탐지 및 악성 유포지 URL 탐지
- 개인 정보 탐지
- 웹셸 탐지 및 필터링 경과 서버 송 외
- Unix, Linux, NT 지원 (JDK 1.5)



WSS 매니저 프로그램 (PC)

- 웹셸 탐지 실행
- 모니터링, 원격 조치, 환경 설정
- 관리자 권한 관리, 통계 & 리포팅 외
- 관제 및 운영 PC 설치

PRODUCTS

WSS On-Premise (Web Server Safeguard)

온프레미스 환경의 웹 기반/웹 서버 데이터를 보호하고 중단 없는 서비스를 제공하기 위해 실시간으로 공격 탐지, 즉각적인 대응이 가능한 종합 웹 보안 솔루션

WSS Cloud (VM Security Solution)

클라우드 컴퓨팅(VM) 사용자의 웹 기반 데이터 공격을 실시간으로 탐지하고 즉각 대응하여 고객을 보호하고 중단 없는 서비스를 제공하는 클라우드 컴퓨팅 보안 솔루션

WARSS (Website Attack Restoration)

웹사이트의 소스 코드, 데이터, 디지털 콘텐츠 위변조 등으로 기업의 신뢰 및 이미지 실추 전에 공격을 실시간으로 탐지하여 원본으로 즉시 복원하는 보안 솔루션



WSS 실시간 보안기능

웹셸 (Web Shell) 공격 방어

보안 취약점을 이용하여 시스템 침입을 시도하는 위험한 웹셸(ASP, JSP, PHP, CGI, PYTHON 등의 Script)을 전체 및 실시간 탐지, 모니터링, 검역, 예외 처리, 관리자 보고 및 통계 보고서 제공

중요 파일 무단 변경 방지

웹 서버 설정 파일 변조하여 시스템 내에 새로운 취약점을 통해 지속적인 공격에 대하여 웹 서버 설정 파일의 변경 방지 기능 제공

개인 정보 탐지

웹 서버의 파일 내용을 실시간으로 모니터링하여 파일이나 데이터베이스 내의 개인 정보(PDF, HWP, DOC, PPT, EXCEL, TXT 등)를 탐지하여 관리자에게 즉시 보고

Website 공격 / 실시간 위변조 탐지 및 복원

홈페이지 변조 (Defacement) 공격, 웹서버 코드 및 데이터 위변조, 디지털 콘텐츠(동영상, 사진 등) 변조 등 기업의 이미지 및 금전 손실을 입힐 수 있는 공격으로부터 웹사이트를 보호하기 위하여 원본 소스 (코드, 데이터, 콘텐츠 등) 실시간으로 즉시 복원 및 보고

악성 코드/URL 삽입 공격 방어

전체 및 실시간 탐지 기능을 이용하여 악성 코드/URL을 탐지하고, 검역, 부분 검역, 예외 처리 등의 기능을 제공하며 탐지된 악성 URL은 블랙/화이트/그레이 리스트로 분류하여 보고

환경 설정 변경 방지

웹 서버 구성 파일에 대한 해커의 무작위 또는 악의적인 변경을 감지하여 즉시 관리자에게 통보하고 웹서버/WAS 로그를 분석하여 탐지된 공격자 IP를 관리자에게 보고

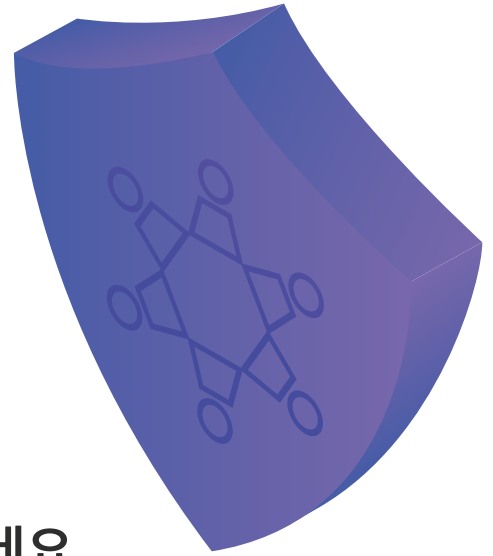
클라우드 컴퓨팅(VM) 환경 지원

WEB/WAS 서비스 Scale IN/OUT, 감지/수정/삭제, 자동 저장, Docker 컨테이너 지원, 홈 디렉토리 자동 감지, 이벤트 복제 관리, 이력 관리, 보안 관리 등을 지원

관리 기능

손쉬운 업데이트, 권한 관리, 외부 시스템(SYSLOG, SMTP, API/ESM/SIEM/SMS/EMAIL 등)과의 연동, 대상 디렉토리 자동 감지 및 백업, 무단 확장 필터링, 리소스 사용 튜닝 (CPU/메모리), 양 방향 지원 (Active/Active), 원격 인증 등 다양한 관리 기능을 제공

A Chain Is Only As Strong As It's Weakest Link



통합 솔루션 "WSS" 로 웹 보안을 완성하세요

주요고객사

UMV 제품은 기업, 공공기관, 통신, 금융, 보안관제, 인터넷, 데이터 센터에서 On-Premise 및 Cloud 컴퓨팅 환경에서 중단없는 웹 서비스를 위해 운용중에 있습니다



umv

www.umv.co.kr

서울특별시 서초구 마방로 2길 84 흥아빌딩 4층
+82 2 448 3435
sales@umv.co.kr