umv

ZYON Platform

Website Attack Restoration Security Solution

WARSS 위변조 실시간 복원솔루션

Contents

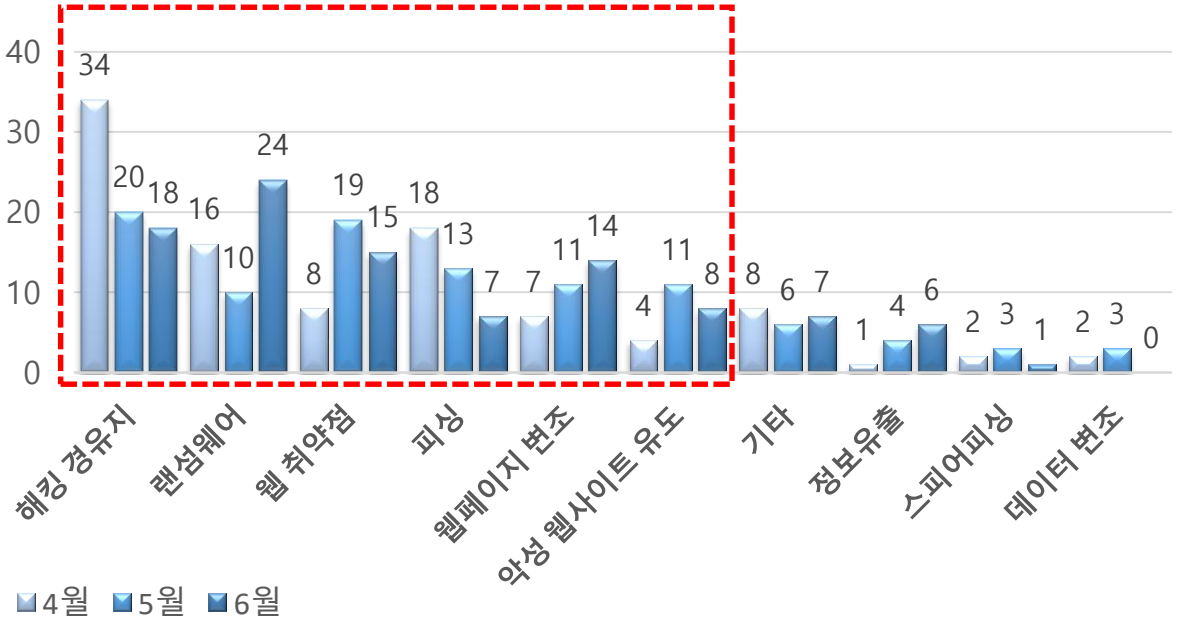
01. 제안배경

사이버 위협 증가와 위변조 복원의 필요성

최근 다양한 유형의 해킹 사고 건수가 증가하고 있습니다.

24년 2분기 침해 사고 통계

"86%+ web shell 해킹"



*출처 : 2024년 2분기 중소기업 침해사고 피해지원서비스 동향 보고서

웹 서버의 취약점

- 사이버 공격의 80% 이상이 웹 서버를 통해 발생
- 최근 웹쉘 기반의 복합적, 지속적(APT) 공격 주류

기존 보안 솔루션 한계

- 네트워크 보안 WAF, IDS/IPS 등 외부 위협에 한정
- 난독화/암호화된 웹쉘 위협 탐지 미흡

끊임없이 진화하는 웹 위협, 당신의 홈페이지는 안전한가요?

출처 : 국가사이버안보센터

최근 해킹사고 동향 보고 사례(1)

교육서비스 플랫폼 런피아, 웹사이트 해킹… 해커, 유튜브에 해킹 과정 공개

입력 : 2024-01-22 15:13

▲런피아 웹사이트의 디페이스 해킹 화면

런피아 웹사이트는 빅데이터·인공지능 기반 학습 콘텐츠 서비스를 제공하는 교육 서비스 플랫폼으로 알려져 있는데, 지난 19일 해커가 웹사이트 메인 페이지를 디페이스 공격한 후, 위·변조된 웹페이지를 추가한 정황이 포착된 것이다.

긴급속보

[긴급] 중국 해커, S2W 보고서에 앙심 품고 한국 여러 사이트 해킹…국방부 공격도 주장

여러 사이트 해킹하며 해킹 증거 올리고 있어 각별히 주의해야 할 상황

▲ 디비리치 사이트를 변조하여 비방한 화면

중국 커뮤니티에서 활동하는 니엔 해커는 웹쉘을 삽입해서 홈페이지 디페이스 공격으로 이어졌습니다.

포스텍 상호작용 연구실 홈페이지 해킹 당했다

포스텍 상호작용 연구실 홈페이지 디페이스 공격 피해
"홈페이지 오래돼 해킹… 중요 정보 유출 피해는 없어"
"워드프레스 플러그인 취약점에 의한 피해로 추정"

입력 2024-12-26 16:13:17

▲ 포항공과대학교 상호작용 연구실 홈페이지의 디페이스 해킹 화면

26일 본지 취재를 종합하면 포스텍 상호작용 연구실(Interaction Laboratory)은 한 해커로부터 최근 디페이스(Deface) 공격을 받았다.

최근 해킹사고 동향 보고 사례(2)

조은날영상기획, 인도네시아 해커가 웹사이트 디페이스 해킹

입력 : 2024-07-22 18:36 (출처 : 보안뉴스)

▲ '조은날영상기획' 디페이스 해킹 정황 화면

조은날영상기획의 웹사이트 화면이 위변조 공격인 디페이스 해킹을 당한 정황이 포착됐다.
지난 20일 한 제보자는 "해당 사이트가 디페이스 해킹을 당했다"며 "그러나 해킹된 사이트가 주말 동안 정상적으로 복구되지 못하고 방치되어 있다"고 설명했다..

키오스크 '오더나인' 해킹 당했다…피싱 사이트도 생겨

'디페이스' 공격에 홈페이지 변조…직접적인 계정정보 탈취 시도

컴퓨팅 | 입력 :2025/08/07 19:46 수정: 2025/08/08 15:21

▲ 키오스크 업체 오더나인 홈페이지에 접속하면 표시되는 해커의 글

더9컴퍼니코리아의 키오스크 브랜드 '오더나인' 홈페이지가 7월 중순부터 해킹으로 접속 불가 상태이며, 디페이스 공격으로 화면이 변조됐다. 해커는 닉네임과 메시지를 남기고, 유사 URL 피싱 사이트까지 만들어 개인정보 탈취를 시도했다. (중략)

쿠르드족 해킹그룹, 한전 자회사 K사 홈페이지 등 해킹공격

발행일 : 2025-05-19 10:04

▲ 한전 자회사 K사 홈페이지의 디페이스 해킹 화면

해킹그룹 TEAM1722가 지난 14일부터 이틀간 국내 홈페이지 4곳을 해킹했다고 주장했다. 이들은 주로 홈페이지 화면을 위변조하는 디페이스 해킹공격을 벌인다. 한국전력 자회사 K사와 영어교육·채용 사이트 등을 대상으로 디페이스 공격과 내부 정보 탈취를 시도했다.

웹 해킹 및 대응방안

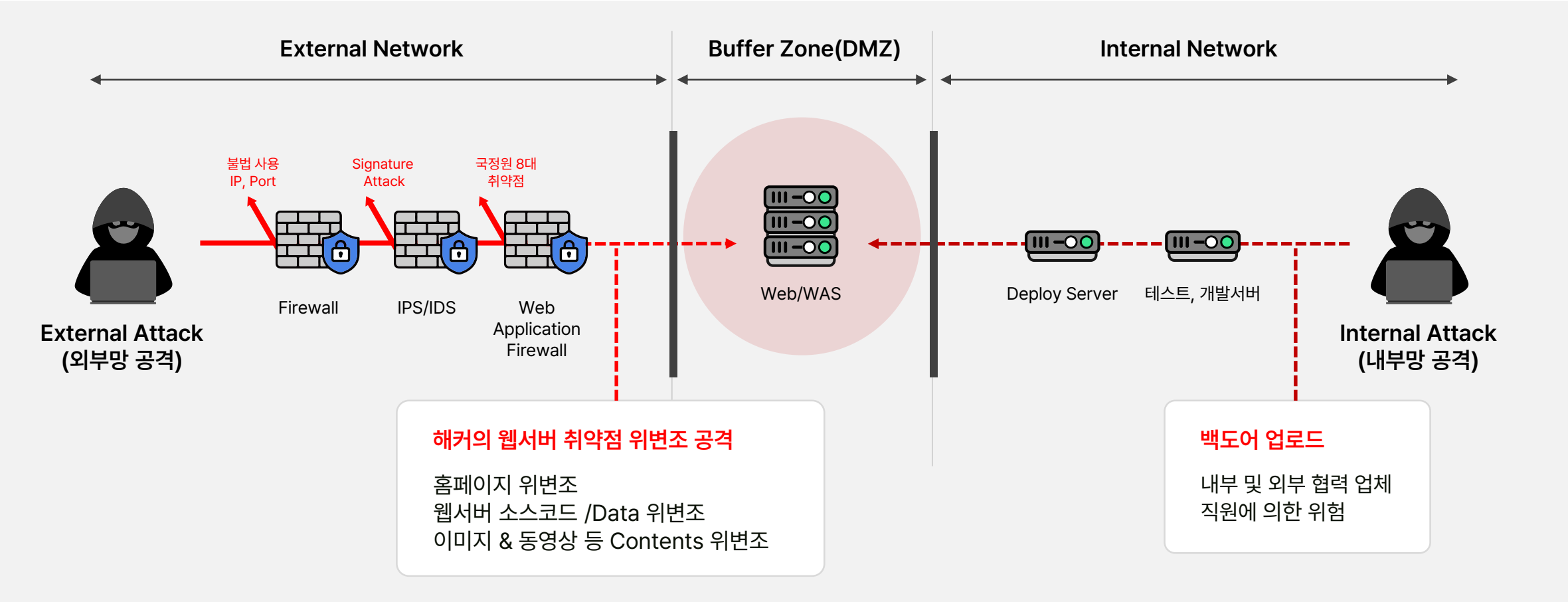
홈페이지 디페이스, 소스코드 및 콘텐츠 위변조 공격

취약점을 이용한 웹공격

- 네트워크 보안 솔루션 약점을 이용한 공격
- 내부 침입 공격
- 게시판 업로드 공격
- 소스코드 취약점을 이용한 업로드 공격
- Operation System Zero Day 취약점 공격

웹쉘(Webshell)이란?

WARSS는 국내외 최초로 개발된 실시간 웹사이트의 원본 리소스(소스코드, DATA, Contents)를 복원하는 솔루션으로
홈페이지 디페이스 공격, 소스코드 및 DATA, 그리고 웹에서 제공하는 Contents에 대한 위변조 공격을 실시간으로 방어하여 중단없는 웹서비스를 제공하는 솔루션



02. 제안 제품

WARSS(Website Attack Restoration & Security Solution)

실시간 웹사이트 위변조 탐지 및 복구 솔루션

(1) 실시간 위변조 탐지 및 복원·복구 기능

기존 솔루션의 '탐지와 보고' 한계를 넘어, 공격 즉시 원본 상태로 복원하는 WARSS
홈페이지 디페이스, 이미지·동영상 위변조, 소스코드 변조 등의 즉각 복구 가능

(2) 클라우드 / 컨테이너 호환

온프레미스 및 클라우드(도커 포함) 환경 지원을 통한 유연한 배포 가능

(3) 리소스 사용량 높은 안정성

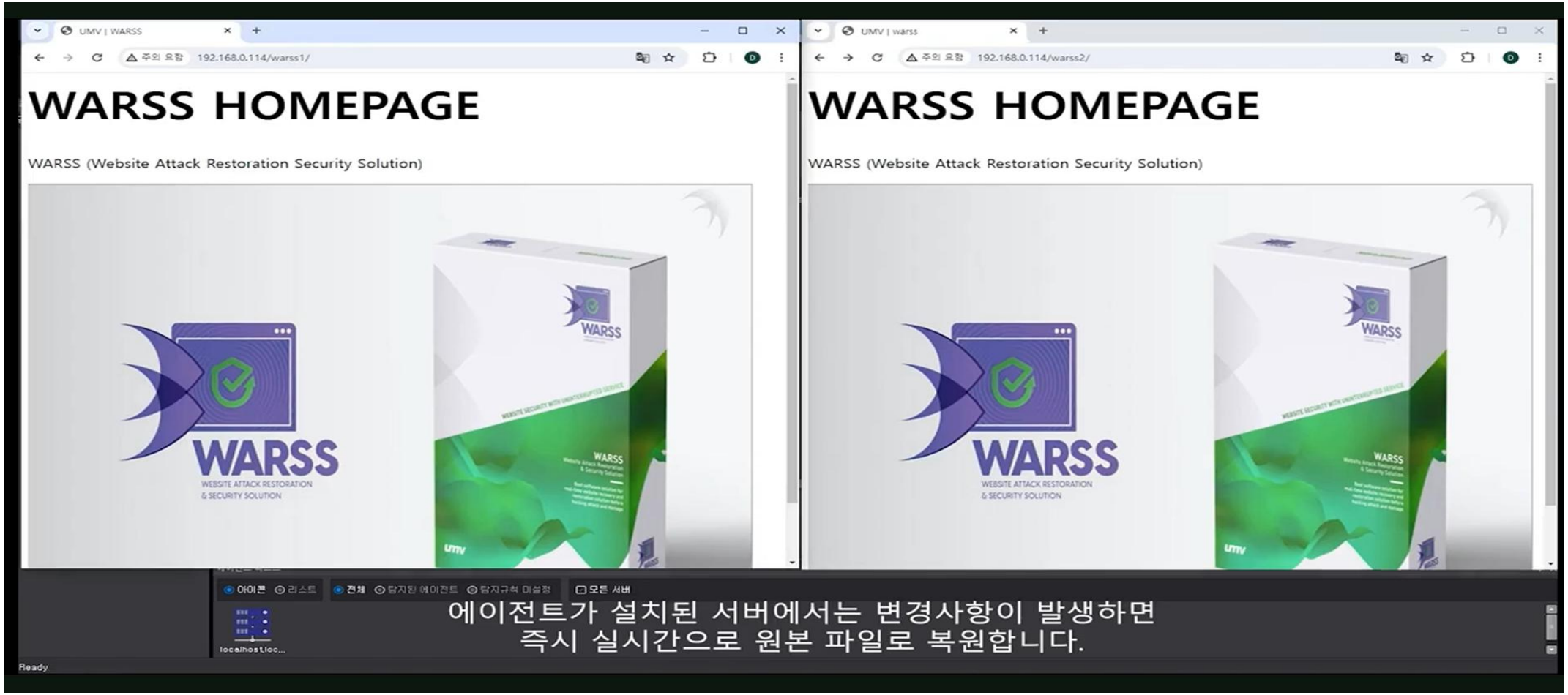
경량화 구조를 통한 CPU 및 메모리 사용량 최적화와 서버 성능 저하 최소화
병행 운영 시에도 안정적인 서비스 성능 유지

(4) 신뢰할 수 있는 운영 실적 및 레퍼런스

장기 신뢰성 : 일부 고객사 대상 17년간의 무중단 운영을 통한 안정성 및 신뢰성 입증
보안 성과 : KOICA 알제리 수출 사업, 주요 정부기관, 금융권(삼성·현대카드·농협은행 등) 성공 도입

WARSS(Website Attack Restoration & Security Solution)

<실제 동작 화면>



WARSS vs CRAWLER 비교

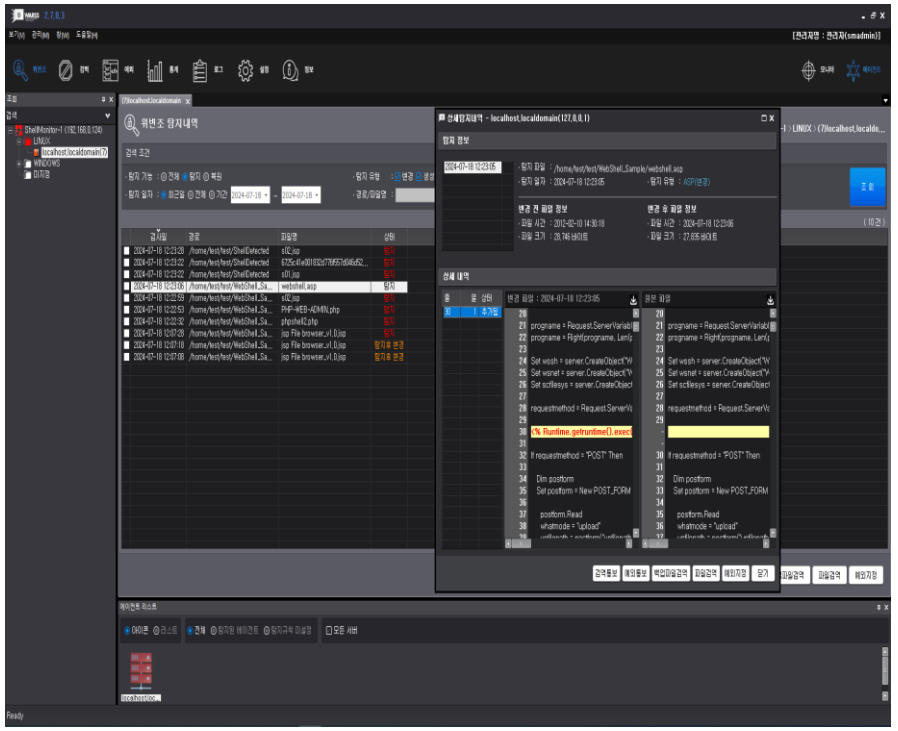
WARSS vs CRAWLER

항목	WARSS	CRAWLER
탐지 방식	실시간 위변조 탐지	주기적인 탐지만 가능(실시간X)
속도	최적화된 리소스 사용(CPU 1% 내외)	URL등록이 많아질 수록 속도감소
URL 등록	디렉토리 설정만으로 하위 전체 탐지	수기 등록 필요, 누락 가능
위변조 대응	탐지 즉시 자동 조치 가능	탐지 후 수동 조치
변조 파일 복원	실시간 자동 복원	복원 기능 없음
서버 부하	이벤트 기반으로 부하 적음	크롤링 시 부하 발생
위험성	실시간 대응으로 사각지대 최소화	탐지 간격 동안 노출 가능
대용량 컨텐츠	모든 파일 및 소스코드 탐지 가능	탐지 불가

WARSS 상세기능

위변조 탐지 및 복원 기능

항목	WARSS 방식
위변조 탐지	• 홈페이지 소스파일 및 데이터 위변조 탐지 및 알림
위변조 복원	• 위변조 탐지 시 실시간 원본파일로 복원
원본 재지정	• 실시간 복원된 파일에 대해 원본으로 재지정하여 복원



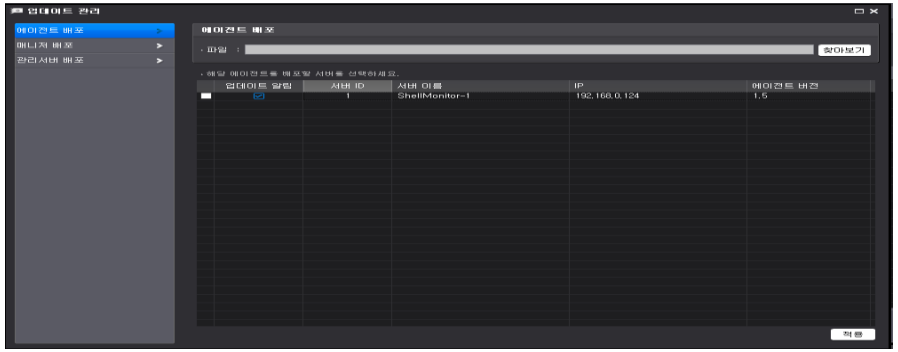
[위변조 탐지 및 실시간 복원 화면]

WARSS 상세기능

관리 기능

항목	WARSS 방식
업데이트관리	• 에이전트, 매니저 업데이트 및 버전 관리
권한 및 보고 관리	• 계정 및 사용자 별 권한 관리 • ESM, SMS, EMAIL 등 외부 시스템 연동 및 인터페이스 제공 • 보고서 및 통계 리포팅
안정성	• 설치된 웹서버/WAS의 자원을 최소화 사용 • 서버 환경에 맞게 조정 관리
공격자 IP 탐지	• 탐지 기능만 활성화하여 사용하는 경우, 위변조된 파일 실행 시 웹서버/WAS 로그를 분석하여 실행IP 보고
환경설정 관리	• WEB/WAS 설정 파일 관리 및 변경 탐지

[관리자 권한 화면]

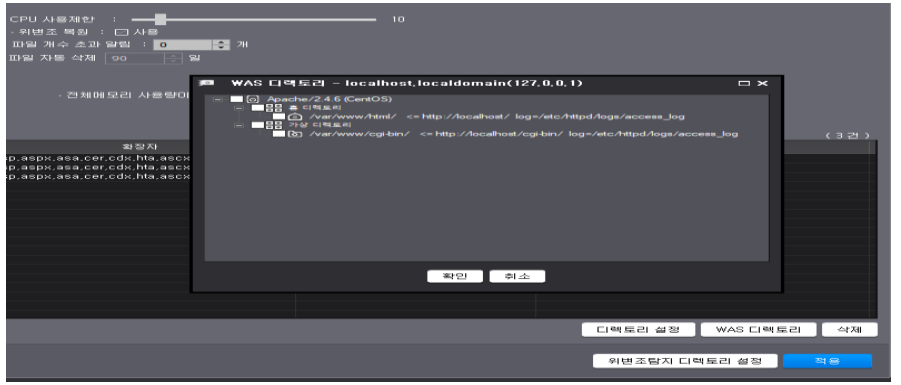


[업데이트 관리 화면]

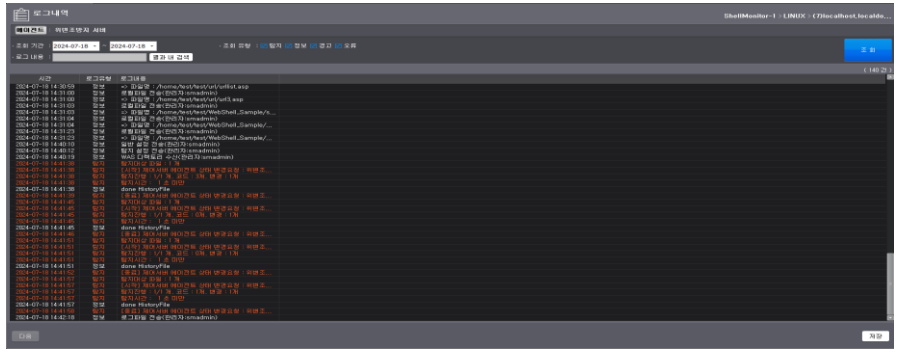
WARSS 상세기능

클라우드 컴퓨팅 지원

항목	WARSS 방식
SCALE IN/OUT	• WEB/WAS Scale Out 시 탐지 대상 자동 등록 후 자동 탐지 • WEB/WAS Scale In 시 삭제 Instance의 탐지/변경/삭제 로그를 관리서버로 자동 저장
홈 디렉토리 찾기	• WEB/WAS 홈 디렉토리 추가/변경 사항에 대한 스케줄링 탐지 • 홈 디렉토리 탐지 추가/변경 내역 확인
이력 관리	• 설치/삭제, 기동/중지 등 에이전트 운영 상태 및 이력 관리
이벤트 중복관리	• 홈 디렉토리가 NAS 영역에 포함되어 있을 경우 이중화 되어 있는 시스템의 중복 탐지 이벤트 발생 방지



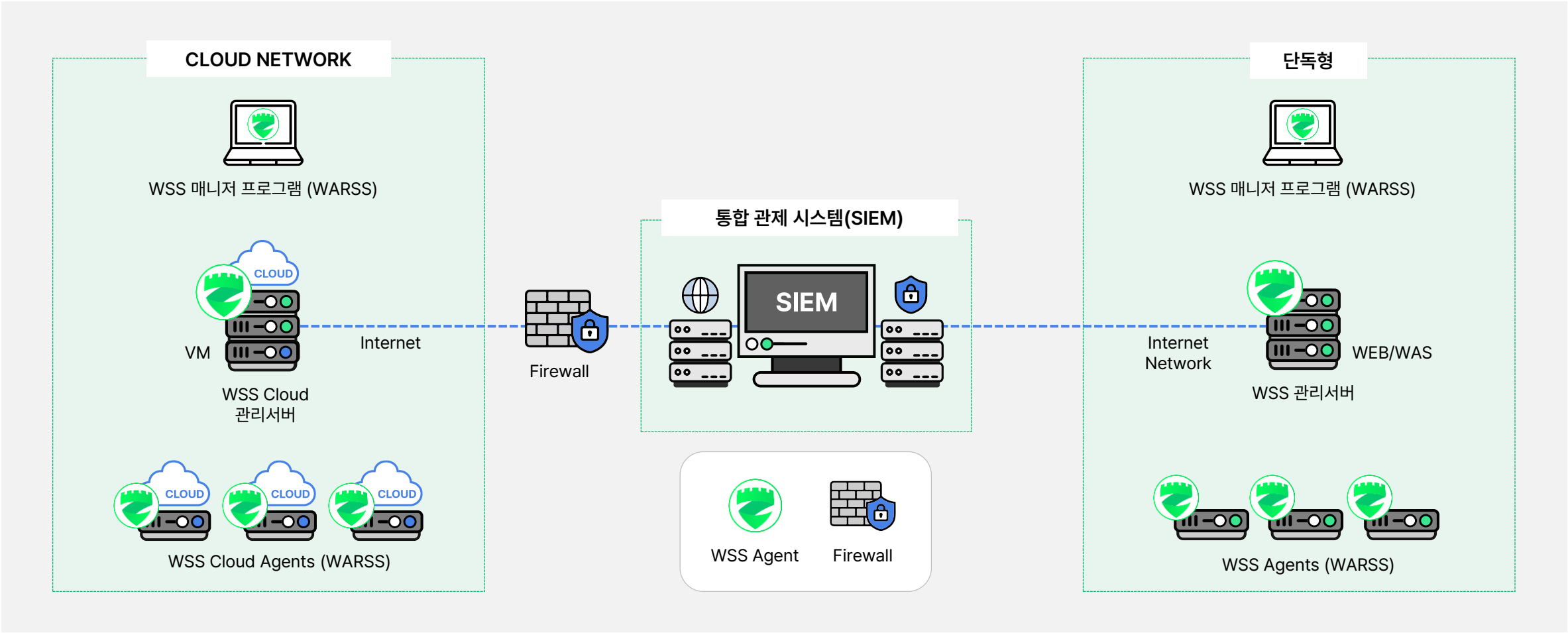
[홈 디렉토리 찾기 화면]



[이력 관리 화면]

WARSS 상세기능

WARSS는 On-Premise, Cloud Computing 및 중앙관제 환경 지원



03. 도입사례

- WARSS를 현재 운용하고 있는 주요 고객사 19

WARSS를 현재 운용하고 있는 주요 고객사

공공기관

청와대, 군부대, 서울시청,국방과학연구소, 한국전자통신연구원, 영남대학교, 지역난방공사, LS그룹, 한국원자력연료, 도로교통공단, 한국도로공사, KDB 생명보험 등

umv

㈜유엠브이기술 I www.umvglobal.com I Tel 02-448-3435