NET 인증 | GS 인증 1등급 | 조달청 디지털 서비스몰

AI 기반 네트워크 위협 탐지 및 대응 솔루션

MNX AI NDR

AI-Powered Network Detection and Response Solution

소개

MNX는 네트워크 상의 모든 트래픽을 AI 기반으로 수집-분석하고, 이상 징후를 탐지해 자동으로 대응하는 NDR 솔루션입니다.
네트워크에서 발생하는 위협의 수집 – 분석 – 탐지 – 대응까지 각 단계 별 특화된 기능과 성능으로 보안 담당자의 '위협 관리 부담'은 최소화 하고 '업무 효율성'을 극대화합니다.

Collect	Analysis	Detect	Respond
100%	AI	4X	365
네트워크 트래픽 무손실 수집	L7 패킷 심층 분석, 트래픽 상세 정보 제공	최신 위협 탐지 룰, AI 탐지 모델 등 다중 위협 탐지	실시간 모니터링 및 시나리오 기반 위협 자동 대응

왜 AI NDR일까요?

MNX는 독자적인 AI 기술로 기존 NDR 제품의 한계를 극복하여 위협 대응에 필요한 다양한 가치와 기준을 제공합니다.
보안 담당자는 MNX로 현재 발생한 위협에 효과적으로 대응하고, 미래 발생 가능한 위협까지 능동적인 대처가 가능합니다.

AI 분석 모델

암호화된 트래픽에서도 어플리케이션 식별

AI 탐지 모델

글로벌 위협 빅데이터를 학습한 AI 모델로 위협 탐지

AI 어시스턴트

네트워크 현황 및 위협 정보, 대응 가이드 상세 설명

도입효과

네트워크 가시성 확보

네트워크 가시성을 확보해
보안 사각지대 해소

네트워크 포렌식

모든 트래픽 수집으로
역추적, 네트워크 포렌식 가능

맞춤형 시나리오

AI 기반의 맞춤형 시나리오로
정교한 탐지 및 대응

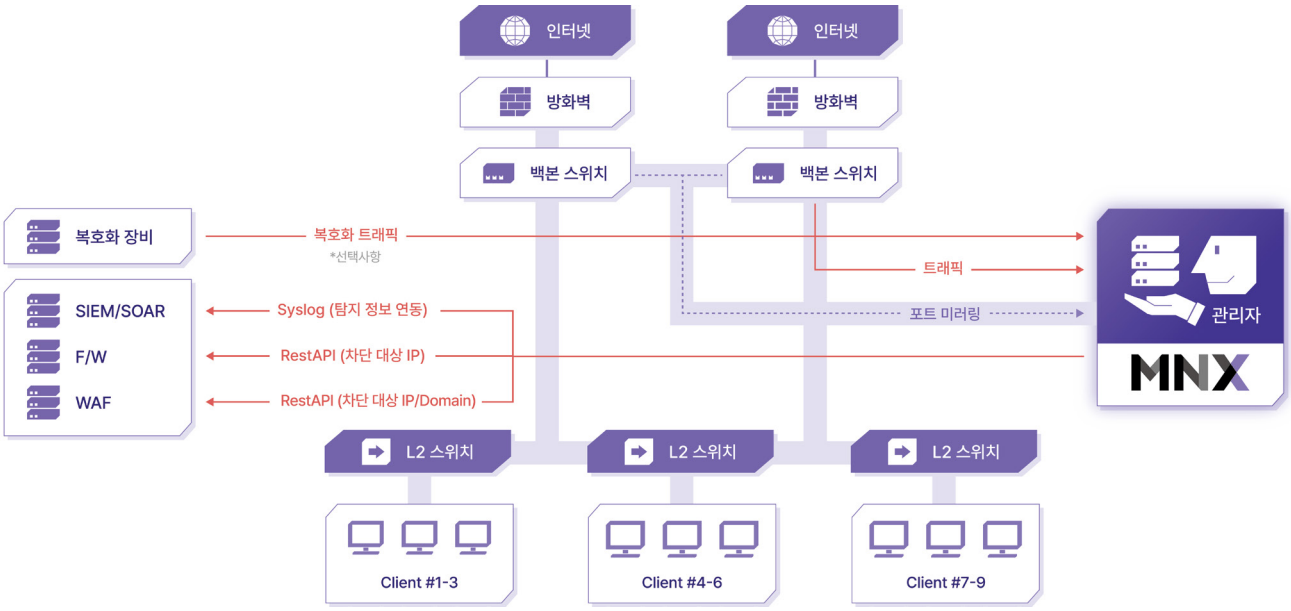
보안 컴플라이언스 강화

내부 자료 유출, 비인가 접속 등
내부 자산 관리

통합 보안 관제

다양한 보안 솔루션과 연동,
통합 보안 관제 환경 구축

구성도

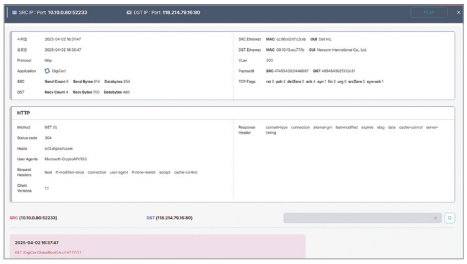


핵심 기술 | **DPDK** | 고성능 패킷 수집 기술 | **DPI 엔진** | 심층 패킷 분석 기술 | **AI** | 이상 징후 탐지, 어시스턴트

- 트래픽 미러링으로 사내 네트워크 망에 영향 없이 안정적 운영
- 네트워크 위협 수집~대응까지 전 과정을 단일 솔루션으로 수행
- 업무망, DMZ망, 특정망 등 고객 니즈에 따라 구성 가능
- 보안 담당자의 관리 효율성과 운영 편의성 향상

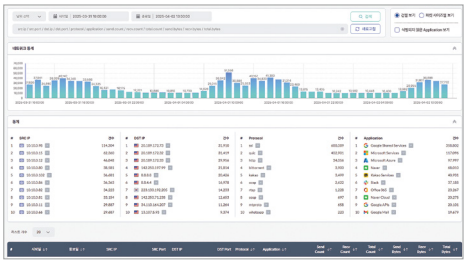
*MNX 장비 1대가 타사 장비 7대의 역할 수행 (10G 기준)

주요 기능



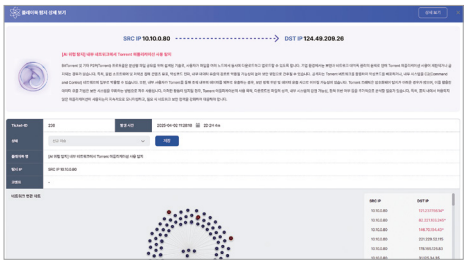
가시성

- 네트워크 트래픽 실시간 모니터링
- 공격 정보 확인 및 역추적 가능
- 상세 Payload 확인 가능



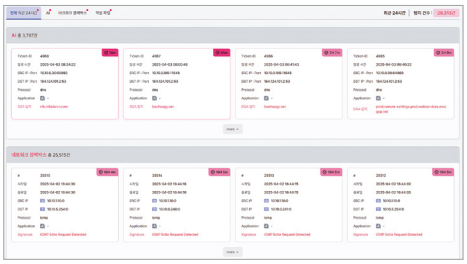
데이터 수집

- 풀 패킷 데이터 무손실 수집
- L7 데이터 인덱싱으로 위협 추적 및 포렌식 분석
- 쿼리 기반 검색 및 조건 필터링 지원



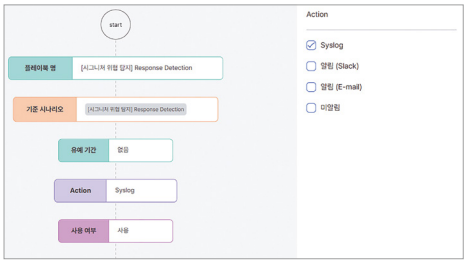
위협 분석

- 프로토콜 500종, 어플리케이션 2,000종 식별
- 복호화/암호화 트래픽 상세 분석
- 탐지된 위협 자연어 기반 설명



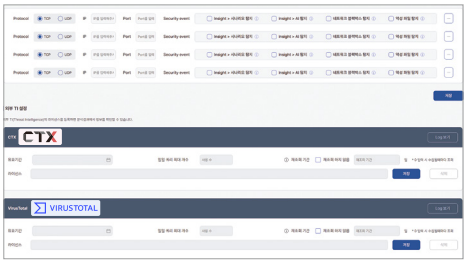
위협 탐지

- AI 기반 네트워크 이상행위 탐지
- AI / AV(Anti Virus) 기반 수집된 파일 탐지
- MITRE ATT&CK T-ID 매핑 공격 기법 식별



자동 대응

- SNS, E-Mail, API, syslog 연동 이벤트 실시간 알림
- 기존 보안 장비 연동, 정책 적용 및 자동 차단 지원
- 대응 시나리오 50여 종 제공



연동

- 다양한 보안 서비스/솔루션 연동 지원

<사이버 위협 인텔리전스> **<보안 관제 솔루션>**

CTX OSINT VirusTotal SIEM SOAR WAF FireWall

라인업

* 운영 정책에 따라 HDD는 별도 협의

구분	MNX V23 **500M**	MNX V23 **1G**	MNX V23 **5G**	MNX V23 **10G**
CPU	2.0Ghz * 2EA (16 Core)	2.0Ghz * 2EA (16 Core)	2.0Ghz * 2EA (32 Core)	2.0Ghz * 2EA (32 Core)
RAM	256GB	256GB	1T	1T
HDD	12TB * 6EA 이상	12TB * 12EA 이상	24TB * 15EA 이상	24TB * 30EA 이상
NIC	1Gb * 4Port	1Gb * 4Port	10Gb * 2Port 이상	10Gb * 2Port 이상

MNX AI NDR

레퍼런스

[주요 도입 사례]

전인 교육기업 D사

#교육 #출판

비즈니스 과제

다양한 외부 사용자의 네트워크 접근에 따른 고객 개인정보 보호 강화

MNX 역할

- 유출입 되는 파일 AI로 교차 검증
- 내부 PC 악성코드 감염 신속 대응
- 비인가 소프트웨어 탐지 및 제어
- 업무망 보안 정책 위배 사항 분석

성과

위협 탐지 속도 향상	대응 시간 단축	업무 효율성
실시간 수준	**12시간→30분**	**150% 향상**

엔터테인먼트 기업 C사

#엔터테인먼트 #미디어

비즈니스 과제

콘텐츠 제작 과정에서 발생하는 데이터 탈취, 비인가 접근 식별

MNX 역할

- 대용량 파일 유출의심 사례 탐지
- 내부 스토리지 비정상 접근 탐지 및 보호
- 어플리케이션 사용 24시간 모니터링
- 외부 인력 네트워크 사용패턴 분석

성과

정책 위반 행위	잠재적 파일 유출 시도	위협 대응 속도
+98% 탐지	**+90% 차단**	**2배 향상**

[고객사 후기]

유통기업 H사

AI 기반 탐지된 정보가 의미가 있다.
업무망 구축 및 DMZ망 구축을 희망한다.

G광역시청

이렇게 **디테일한 검색이 가능한 솔루션**은 처음 경험해 봤다.

철강 제조기업 D사

POC를 진행하면서 내부에 발생하고 있는 **실제 침해 사고를 MNX로 확인했다.**

고용노동부 산하 공공기관

AI 기반 네트워크 **이상 징후 탐지**는 놀라울 정도다.
침해 분석 관련한 **네트워크 포렌식**이 가능하다.

> MNX 도입 후 평균
> 위협 **탐지 속도 5배** 향상, **대응 시간 70% 단축**이라는
> 놀라운 효과를 경험하고 있습니다.

SANDS Lab

KOSDAQ
코스닥상장법인

주식회사 샌즈랩 경기도 과천시 과천대로 7나길 25. 12층 샌즈랩
Tel. 02-704-7502 | **E-Mail.** contact@sandslab.io | https://www.sandslab.io

샌즈랩 바로가기