Trellix Fire Eye

글로벌 No.1

APT 공격 대응 솔루션

Trellix는 웹, 이메일, 파일공유, 엔드포인트 등으로 전개되는 APT 공격 방어 글로벌 No.1 보안 솔루션입니다.
독자 기술로 자체 개발한 MVX 가상머신을 통해 지능형 위협 및 알려지지 않은 위협을 식별하고 대응합니다.
또한 Trellix DTI(다이나믹 위협 인텔리전스)를 통해 전세계에서 발생하는 위협 정보에 대한 실시간 업데이트를 제공합니다.

제품 구성

NX	EX	FX	HX	AX
웹 트래픽을 통한 공격 탐지/차단	이메일을 통한 공격 탐지/차단	파일공유/망연계구간의 악성코드 탐지/차단	엔드포인트 환경의 공격 탐지/차단	전체 공격 라이프사이클 포렌식 분석

CM Central Management

도입 배경

진화하는 APT 공격 대응 필요

제로데이, 랜섬웨어 그리고 다양한 우회 기법을 이용하는 멀티 벡터기반의 고도화된 APT 공격 증가

지능화, 고도화되어 기존의 보안 시스템을 우회하고 알려지지 않은 취약점을 이용하는 공격 대응

도입 효과

탐지 능력 강화

행위 기반 동적 분석을 통해 알려지지 않은 위협까지 탐지
APT공격에 특화된 전용VM을 통한 다양한 우회 기법 대응
장비 간 이벤트 상관 관계 분석을 통한 멀티플로우 위협 분석

기업 내부 환경 보호

알려지지 않은 위협 탐지로 기업의 내부 환경을 보호

시너지 극대화

기운영 보안 솔루션과의 연동을 통해 보안 업무 시너지 극대화

진화하는 APT 공격에 대한 체계적인 대응

Trellix는 [탐지] [차단] [대응] [분석]을 통해 안전한 환경을 지원합니다.

구성도

1 NX
사용자의 웹 트래픽을 분석하여 악성 트래픽을 탐지 및 차단

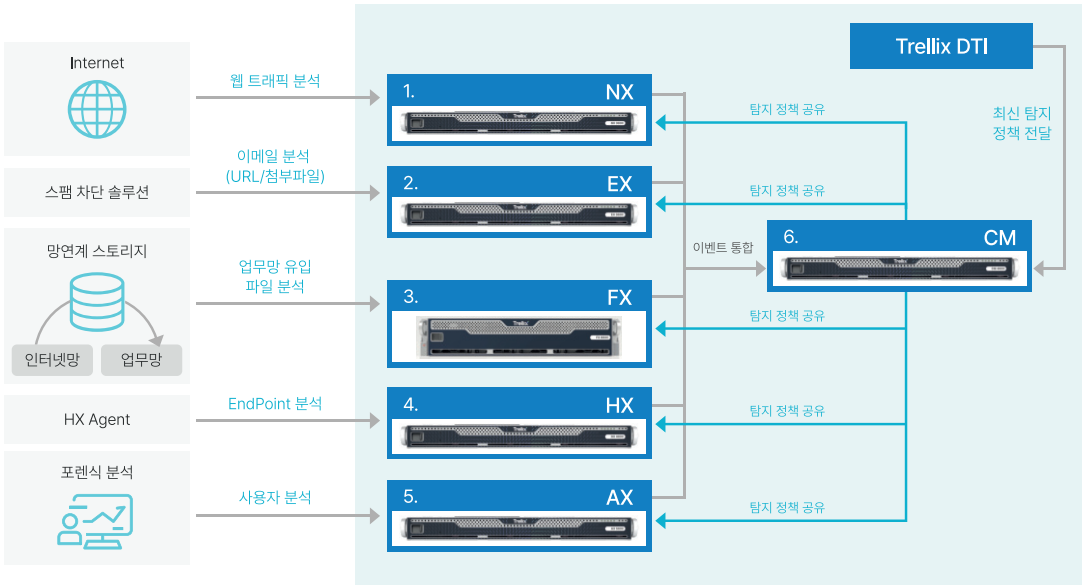
2 EX
내부 메일서버로 유입되는 이메일을 분석하여 악성 이메일을 격리

3 FX
업무망으로 유입되는 파일을 분석하여 악성 파일을 격리

4 HX
Agent를 통해 엔드포인트를 분석하여 감염된 엔드포인트 격리

5 AX
사용자 분석을 통해 포렌식 분석 기능 제공

6 CM
Trellix 전 제품을 통합관리, 모니터링, 장비 간 이벤트 상관관계 분석



주요 기능

탐지 / 차단

NX / EX / FX

- AV Suite, YARA 등 시그니처 기반 정적 분석 및 MVX 가상머신 동적 분석
- 세션 단위의 멀티 플로우 분석을 통해 난독화 파일 등 고도화된 악성코드 탐지
- 파일 내 URL, 리다이렉션 URL, 발신자 사칭 등 이메일 기반 다양한 APT 공격 탐지
- 인라인 또는 미러(SPAN/TAP) 구성을 통한 위협 탐지 및 차단

HX

- 업계 선두 시그니처 엔진을 통해 알려진 악성파일 탐지/치료/격리
- 머신러닝 엔진을 통해 제로데이 신종 공격, 변종 공격 탐지/격리
- 행위 기반 탐지 엔진을 통해 알려지지 않은 위협 탐지/차단
- 인텔리전스 기반 행위 탐지 IOC 룰 및 사용자 정의 IOC 룰을 통한 위협 탐지
- 호스트별 정책 설정 제공, 다양한 모듈 제공

분석

HX

- Triage Summary를 통해 침해 흔적 발견 및 가시성 확보
  Enterprise Search를 통해 엔드포인트 전수 검사

AX

- 포렌식 분석으로 공격에 대한 직관적인 분석 지원

대응

HX

- 감염된 엔드포인트 격리 조치
  분석 결과를 기반으로하여 위협 제거

특장점

행위 기반

행위기반 분석으로
알려지지 않은 공격 탐지 및 차단

샌드박스

특허 받은 자체 개발 가상머신으로
상용 VM 대비 압도적 분석 성능

인텔리전스

실시간으로 위협 인텔리전스 공유
및 90개국 4만여 개 래퍼런스 보유

전문성

수백 건의 침해 조사 경력 및
지속적인 기술 개발 투자

sales@tocsg.co.kr | 02. 320. 5050 | www.tocsg.co.kr
IT EXPERT GROUP ToCSG 고객의 Business를 위한 최고의 IT 솔루션과 서비스를 제공합니다.
TOCSG 투씨에스지