데이터시트

FireEye SmartVision Edition

엔터프라이즈 네트워크 내부의 의심스러운 이동 탐지

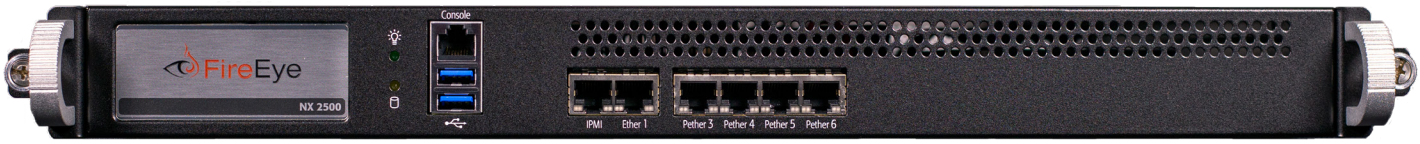

그림 1. NX 2500 SmartVision 하드웨어

이점

- 이전에 감지되지 않았던 의심스러운 내부 트래픽 감지
- 침해 발생 후 활동 탐지에 소요되는 시간 단축
- 전체 네트워크로 확장할 수 있는 유연성 제공
- 네트워크 세그먼트화 이니셔티브에 대한 가시성 지원
- 네트워크 포렌식 및 침해 사고 대응 개선
- 공격 지속 시간 최소화

FireEye SmartVision Edition은 기업 네트워크 내부의 의심스러운 트래픽을 탐지하는 네트워크 트래픽 분석(Network Traffic Analysis, NTA) 솔루션입니다. 유입되는 악성 공격을 막기 위해 경계에 설치되는 다른 네트워크 보안 솔루션과 달리, FireEye SmartVision Edition은 코어, 네트워크 세그먼트 전반, 주요 서버 자산의 전방 등 네트워크 어디에나 배포되어 악의적인 내부 트래픽을 감지할 수 있습니다.

FireEye SmartVision Edition을 사용하면 보안 분석가와 관리자가 방화벽 및 기타 보안 게이트웨이에서 감지되지 않는 의심스러운 내부 트래픽에 대한 새로운 통찰력과 가시성을 확보할 수 있습니다. 업계를 선도하는 FireEye의 Cloud MVX™ 기술과 호환되는 배포가 용이한 경량 센서를 사용하여 고객은 데이터 센터부터 원격의 지사 사이트까지, 전체 네트워크로 SmartVision Edition의 가시성을 확장할 수 있습니다.

SmartVision Edition은 데이터 유출 시도를 탐지하는 고급 상관관계 파악 및 분석 엔진과 머신 러닝 모듈로 이루어진 지능형 위협 탐지 소프트웨어를 기반으로 하며, 취약한 침해 지표를 식별하는 120여 개의 침입 탐지 규칙으로 강화됩니다.

SMARTVISION EDITION의 구성 요소

SmartVision Edition을 사용하려면 세 가지 구성 요소가 필요합니다.

- 2개 이상의 SmartVision 센서(하드웨어 또는 가상 센서)
- FireEye MVX 엔진 연결(온프레미스, 스마트 그리드 또는 Cloud MVX*를 통한 연결)
- SmartVision이 활성화된 FireEye OS 릴리스 8.1.2 이상

표 1. SmartVision Edition의 기능

기능	설명
의심스러운 내부 네트워크 트래픽 탐지	고급 상관관계 파악 및 분석 엔진과 머신 러닝 모듈, 은밀한 내부(East-West) 트래픽을 감지하는 120여 가지 고유 규칙 결합
SMB/SMB2 프로토콜을 통해 객체 파괴	FireEye MVX 기술을 사용하여 SMB 프로토콜을 통해 내부로 이동하는 WannaCry 등의 멀웨어 및 랜섬웨어와 기타 의심스러운 파일 및 객체 파괴
신속하게 이벤트를 분류할 수 있도록 경보 시각화	공격자의 활동을 신속하게 조사하고 포렌식 분석을 수행할 수 있도록 10분(+/- 5분) 분량의 L4 및 L7 경보 상황 분석 제공
폭넓은 메타데이터 프로토콜 지원	다음 프로토콜을 포함하여 포괄적인 분석을 위한 메타데이터 생성: FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS
기존 FireEye Network Security 설치 환경 보완	4세대 및 5세대 네트워크 보안 어플라이언스를 사용하는 FireEye 고객은 기존 인프라에 SmartVision Edition을 손쉽게 통합하여 ROI를 높일 수 있음
FireEye Helix와 통합	팀 간 협업을 위한 추가 위협 인텔리전스 상황 정보 및 통합 경보 분류 기능 제공

FireEye SmartVision Edition은 내부망 내 공격 주기 전반에서 고유한 위협 행위를 식별하여 침해 발생 후 공격 지속 시간과 손실 위험을 줄입니다.

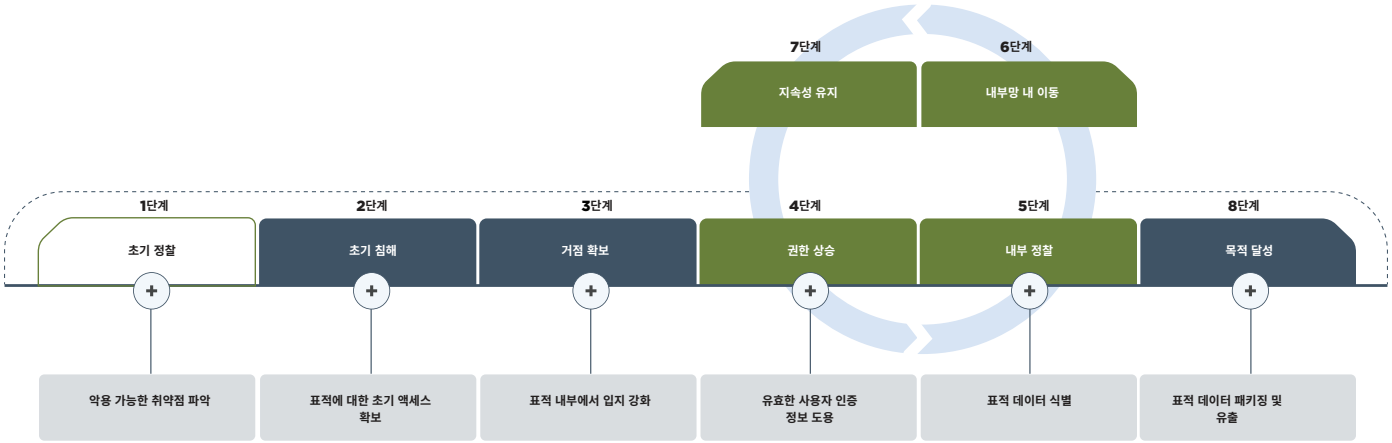

표 2. 하드웨어 모델별 SmartVision Edition 사양

모델	SV-2500-HW	SV-5500-HW	SV-6500-HW
센서 모드 성능**	최대 500Mbps	최대 10Gbps	최대 15Gbps
통합 또는 하이브리드 모드 성능**	최대 200Mbps	최대 5Gbps	최대 10Gbps
네트워크 모니터링 포트	4x 10/100/1000 BASE-T 포트	8x 10GigE SFP+ 4x 1Gig E 우회	8x 1GigE/10GigE SFP+ 2x 40GigE QSFP+
관리 포트	2x 10/100/1000 Base-T 포트 (전면 패널)	2x 10/100/1000 Base-T 포트	4x 1000BaseT 포트
저장 용량	단일 1TB 3.5인치, SATA HDD, 내부, 고정	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU, RAID1	"2x 10TB HDD, 3.5", SAS3, 7.2krpm FRU RAID1"
엔클로저	1RU, 19인치 랙에 적합	2RU, 19인치 랙에 적합	2RU, 19인치 랙에 적합
섀시 크기(WxDxH)	437mm(17.2인치) x 500mm(19.7인치) x 43.2mm(1.7인치)	438mm(17.24인치) x 620mm(24.41인치) x 88.4mm(3.48인치)	438mm(17.24인치) x 620mm(24.41인치) x 88.4mm(3.48인치)
AC 전원 장치	단일 250와트, 90-264VAC, 3.5-1.5A, 50-60Hz, IEC60320-C14, 인렛, 내부, 고정	이중화(1+1) 800와트, 100-240VAC 10.5-4.0A, 50-60Hz IEC60320-C14 인렛, FRU	이중화(1+1) 800와트, 100-240VAC 10.5-4.0A, 50-60Hz IEC60320-C14 인렛, FRU
최대 전력 소비	85와트	658와트	660와트
어플라이언스 중량/발송 중량, kg(lbs)	7.3kg(16.2lbs) 2.95kg(28.2lbs)	19.2kg(42.7lbs) 29.0kg(63.8lbs)	20kg(44lbs) 32.2Kg(71lbs)
작동 온도	0°-40°C 32°-104°F	0-35°C 32-95°F	10-35°C, 추가 차이를 고려하여 0-40°C에서 테스트함
비작동 온도	-20-80°C -4-176°F	-40-70°C -40-158°F	-30-70°C -22-158°F
지원되는 메타데이터 프로토콜	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS

표 3. 가상 모델별 SmartVision Edition 센서 사양

모델	2550v	6500v
성능**	최대 500Mbps	최대 2Gbps
네트워크 모니터링 포트	1-8개	1-8개
관리 포트	1개 또는 2개	1개 또는 2개
CPU 코어	6개	16개
메모리	16GB	64GB
드라이브 용량	384GB	512GB
하이퍼바이저 지원	VMWare ESXi 6.0 이상	VMWare ESXi 6.0 이상
지원되는 메타데이터 프로토콜	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS

* Cloud MVX는 알려진 위협과 알려지지 않은 위협을 실시간으로 간편하게 감지하고 파괴하도록 설계되었습니다. 일반적인 클라우드 기반 샌드박스와 달리, Cloud MVX는 단순히 파일 종류와 객체를 분석하는 것이 아니라 네트워크 트래픽을 재생하여 여러 네트워크 플로우에 걸친 공격을 식별합니다.

** 성능 수치는 개별 네트워크의 조건에 따라 달라집니다.

FireEye에 대한 자세한 정보: **www.FireEye.com**

FireEye Korea
서울특별시 강남구 테헤란로 534 글라스타워 20층
02.2092.6580
korea.info@fireeye.com

FireEye, Inc. 소개
FireEye는 인텔리전스 기반의 보안 솔루션을 제공합니다. FireEye는 혁신적인 보안 기술, 최고의 Threat Intelligence 및 세계적으로 인정받는 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영 플랫폼을 완벽하게 확장하여 보안을 강화시킵니다. 이를 통해 FireEye는 사이버 위협에 대비하고 공격 방어 및 대응하는 조직의 사이버 보안 부담을 줄이고 보안 운영의 복잡성을 간소화합니다.

FIREEYE™