엔드포인트 보안

알려지지 않은 위협 및 익스플로잇에 대한
온-프레미스 또는 원격 엔드포인트 보안

요약

오늘날의 노련한 공격자들은 대부분의 보안 팀에서 수년간 사용해 온 기존의 엔드포인트 보안시스템(방화벽, 안티바이러스 소프트웨어)을 우회합니다. 기존의 방어 체계로 알려진 위협을 방어한다 하더라도 해당 공격자가 무엇을 시도하려고 했는지까지는 알 수 없습니다. 이럴 때, 기업 네트워크 내부 및 외부에 위치한 엔드포인트에 온-프레미스로 FireEye Endpoint Security(HX 시리즈)를 설치할 수 있습니다. 그러면 보안 팀에서 다음과 같은 기능을 사용하여 알려진 위협과 알려지지 않은 위협의 특성 및 목적을 탐지, 통제, 파악할 수 있습니다.

- 위협 지표를 검사하고 분석하기 위한 Triage Viewer 및 Audit Viewer
- 위협을 신속하게 검색하여 발견하고 통제하는 엔터프라이즈 시큐리티 서치 기능
- 심층적인 엔드포인트 검사와 분석을 위한 데이터 수집 기능
- 엔드포인트 익스플로잇 프로세스를 탐지하고 경고하는 익스플로잇 가드 기능

FireEye Endpoint Security를 사용하면 조직에서 모든 엔드포인트의 알려진 위협과 알려지지 않은 위협을 사전에 검사하고 분석하고 통제할 수 있습니다.

모든 엔드포인트로 위협 인텔리전스를 확장

위협 인텔리전스는 공격 당시에 존재해야 그 효력이 있습니다. HX EDR(엔드포인트 탐지 및 대응)은 다른 FireEye 제품의 위협 인텔리전스 기능을 엔드포인트로 쉽게 확장시킵니다. FireEye 제품이 네트워크의 어디에서든 공격을 탐지하면, 엔드포인트에서는 업데이트를 자동으로 진행하며 IOC를 검사할 수 있습니다.

한층 향상된 엔드포인트 가시성 구현

가시성은 경보의 근본 원인을 파악하고 위협에 대해 심층적인 분석을 수행하는 데 있어 매우 중요합니다. Endpoint Security의 캐시 기록 보기 기능을 사용하면 엔드포인트의 현재 및 과거의 경보를 검사하고 분석할 수 있습니다. 또한 Triage Viewer를 통해 포렌식 분석을 위한 이벤트 타임라인을 자동으로 구축할 수 있습니다.

주요 기능

- 엔드포인트 에이전트 소프트웨어와 함께 온-프레미스 장비로 Endpoint Security를 설치하여 사내 및 원격 엔드포인트 모니터링
- FireEye DTI(동적 위협 인텔리전스)와 함께 핵심 네트워크부터 엔드포인트에 이르기까지 지능형 위협에 대한 보안을 확장
- 자세한 엔드포인트 조사 및 IOC를 파악하고 통제하기 위한 타임라인 생성
- 수많은 엔드포인트(연결 여부와 상관없이)의 위협을 몇 분 내에 검색, 탐지, 파악 및 통제
- 단일 인터페이스에서 모든 엔드포인트 활동을 간단히 평가하여 익스플로잇을 파악 및 분석하고, 관련된 통제 또는 대응 결정을 내림
- CC인증과 FIPS 정부 표준을 모두 준수
- 실시간 경보, 시스템 세부 정보 및 수집에 관한 호스트 기반 워크플로우를 중앙으로 집중
- 중요한 상황 정보를 통해 알려진 위협과 알려지지 않은 위협에 신속하게 대응
- 온-프레미스, 오프-프레미스, 네트워크 외부, NAT(Network Address Translation) 뒤 등 위치와 관계없이 모든 엔드포인트 방어
- 원격 조사를 허용하면서 단 한 번의 클릭만으로 위협 및 침해당한 장치 통제
- Audit Viewer로 워크플로우를 향상하여 Endpoint Security 내에서 완벽하게 위협 분석
- 보안 사고의 고유한 특성을 해결할 수 있도록 Endpoint Security 맞춤형 기능 지원
- 다양한 DMZ 설치 지원

FireEye
SECURITY REIMAGINED

완벽한 엔드포인트 커버리지 확보

기업 네트워크 외부에 있는 온사이트 및 원격 엔드포인트들은 공격에 매우 취약합니다. Endpoint Security는 모든 엔드포인트를 커버하며 인터넷 연결 유형에 상관없이 인텔리전스를 모든 엔드포인트까지 확장할 수 있습니다. 이 같은 완벽한 커버리지를 통해 추가 VPN 연결 없이도 세계 전역에 위치한 엔드포인트를 조사하고 통제할 수 있습니다.

침해 당한 엔드포인트 통제 및 내부 확산 방지

단일 엔드포인트에서 시작된 공격은 네트워크를 통해 빠르게 확산될 수 있습니다. 공격을 파악하게 되면, 단 한 번의 클릭만으로 침해 당한 장치를 즉각적으로 격리할 수 있으며, 공격을 막고 내부 확산을 방지할 수 있습니다. 그런 다음, 추가 감염의 위험 없이 해당 침해 사고에 대해 완벽한 포렌식 조사를 수행할 수 있습니다.

엔드포인트의 숨겨진 익스플로잇 프로세스 탐지

익스플로잇 탐지와 관련하여, 기존의 EPP(엔드포인트 방어) 기능은 시그니처와 데이터베이스를 비교하기 때문에 한계가 있습니다. FireEye Endpoint Security는 익스플로잇 가드라고 하는 기능을 통해 유연한 데이터 기반 익스플로잇 인텔리전스를 제공합니다. 이 기능은 EDR(엔드포인트 탐지 및 대응) 기능을 제공하여, 기존 엔드포인트 솔루션에서 감지하지 못하는 영역에 대한 자세한 정보를 수집합니다. 또한 상세한 FireEye 전용 인텔리전스를 사용하여 개별적인 여러 활동의 상호 연관성을 찾아내어 익스플로잇을 파악합니다.

Endpoint Security 작동 방식

Endpoint Security는 수많은 엔드포인트의 알려진 위협과 알려지지 않은 위협을 몇 분 내에 검색하여 조사할 수 있습니다. 또한 동적 위협 인텔리전스를 사용하여 FireEye 엔드포인트 및 네트워크 보안 제품과 로그 관리에서 생성된 경보의 연관성을 찾아냅니다.

위협을 검증한 후에는 다음을 확인할 수 있습니다.

- 공격자가 엔드포인트에 침투하는 데 사용한 경로
- 특정 엔드포인트가 침해를 당했는지(그리고 지속되는지) 여부
- 내부 확산 여부 및 그로 인해 침해된 엔드포인트
- 엔드포인트가 공격자에 노출된 기간
- IP가 유출되었는지 여부
- 추가 침해를 방지하기 위해 통제할 엔드포인트 혹은 시스템

ENDPOINT SECURITY 요구 사항

운영 체제	최소 시스템 메모리(RAM)
Windows XP SP3	512MB
Windows 2003 SP2	512MB
Windows Vista SP1 이상	1GB(32비트), 2GB(64비트)
Windows 2008(R2 포함)	2GB(64비트)
Windows 7	1GB(32비트), 2GB(64비트)
Windows 2012(R2 포함)	2GB(64비트)
Windows 8	1GB(32비트), 2GB(64비트)
Windows 8.1	1GB(32비트), 2GB(64비트)
Windows 10	1GB(32비트), 2GB(64비트)

주: Endpoint Security를 사용하려면 1Ghz 이상의 Pentium 호환 프로세서 및 300MB 이상의 디스크 여유 공간이 필요합니다. 상기 운영 체제에서 작동합니다.

하드웨어 어플라이언스 사양

사양	HX 4402/HX 4400D
저장 용량	4x 1.8TB HDD, RAID 10, 2.5인치, FRU
엔클로저	1RU, 19인치 랙에 맞음
섀시 크기(WxDxH)	17.2" x 27.8" x 1.7"(437 x 706 x 43.2mm)
AC 전원	중복(1+1) 750와트, 100-240 VAC
최대 전력 소비(와트)	313와트
MTBF(h)	35,200h
어플라이언스 단독	32lb. (15kg)

주: Endpoint Security의 하드웨어 설치 옵션은 단일 장비로 최대 100,000개의 엔드포인트에 위협 인텔리전스 및 통신을 지원합니다.

엔드포인트 위협에 네트워크 수준의 경보 연결

FireEye Endpoint Security가 다른 FireEye 제품과 어떻게 함께 작동하는지 알아보십시오. 잠재적인 보안 사고에 대해 보안팀이 더 정확한 판단을 내릴 수 있도록 도와드립니다.

FireEye에 대한 더 자세한 정보를 원하시면 다음의 웹사이트를 방문하십시오.
www.FireEye.com

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

www.FireEye.com

FireEye