엔드포인트 보안

알려지지 않은 위협과 익스플로잇에 대한 온-프레미스 또는 원격 엔드포인트 보안

요약

오늘날의 공격자들은 대부분의 보안 팀이 수년 간 사용해 온 엔드포인트 보안시스템(방화벽, 안티바이러스 소프트웨어)을 우회합니다. 또한 기존 방어 체계로 알려진 위협을 멈춘다 하더라도 해당 위협을 통해 무엇을 시도하려고 했는지까지는 알 수 없습니다. 이럴 때, 기업 네트워크 내부 및 외부의 엔드포인트에 FireEye 엔드포인트 보안(HX 시리즈)를 온-프레미스로 설치할 수 있습니다. 그러면 다음과 같은 기능을 사용하여 알려진 위협과 알려지지 않은 위협의 특성 및 목적을 탐지, 통제, 파악할 수 있습니다:

- 위협 지표를 검사하고 분석하기 위한 트리아쥬 뷰어 및 오딧 뷰어
- 위협을 신속하게 검색하여 발견하고 통제하는 엔터프라이즈 보안 검색
- 심층적인 엔드포인트 검사 및 분석을 위한 데이터 수집
- 엔드포인트 익스플로잇 프로세스를 탐지하고 경고하기 위한 익스플로잇 가드

FireEye 엔드포인트 보안을 사용하면 모든 엔드포인트의 알려진 위협과 알려지지 않은 위협을 사전에 검사하고 분석하여 통제할 수 있습니다.

위협 인텔리전스를 모든 엔드포인트로 확장

위협 인텔리전스는 공격이 일어나는 순간에 존재해야 그 효력이 있습니다. HX EDR(엔드포인트 탐지 및 대응)은 다른 FireEye 제품의 위협 인텔리전스 기능을 엔드포인트로 확장시킵니다. FireEye 제품이 네트워크에서 공격을 탐지하면, 엔드포인트는 자동으로 업데이트되며 IOC 검사를 할 수 있게 됩니다.

한층 향상된 엔드포인트 가시성 확보

가시성은 경보의 근원을 파악하고 위협을 심층적으로 분석하는데 있어 중요한 요인입니다. 엔드포인트 보안의 룩백 캐시 기능을 사용하면 엔드포인트의 현재 및 과거의 경보를 검사하고 분석할 수 있습니다. 또한 트리아쥬 뷰어를 통해 포렌식 분석을 위한 이벤트 타임라인을 자동으로 구축할 수 있습니다.

주요 기능

- 엔드포인트 에이전트 소프트웨어와 함께 온-프레미스 장비로 엔드포인트 보안을 설치하여 사내 및 원격 엔드포인트 모니터링
- 핵심 네트워크부터 엔드포인트에 이르기까지 지능형 위협에 대한 보안을 FireEye DTI(동적 위협 인텔리전스)로 확장
- IOC를 파악하고 통제하기 위한 타임라인 생성 및 상세한 엔드포인트 조사
- 수만 개의 엔드포인트(연결 여부와 상관없이)에서 위협을 몇 분 내에 검색, 탐지, 파악 및 통제
- 모든 엔드포인트 활동을 단일 인터페이스에서 손쉽게 평가하여 익스플로잇을 파악 및 분석하고, 통제 또는 적합한 대응을 결정함
- CC인증과 FIPS 정부 표준을 준수
- 실시간 경보, 시스템 세부 정보 및 수집을 위해 호스트 기반 워크플로우를 중앙으로 집중
- 중요한 상황 정보를 통해 알려진 위협과 알려지지 않은 위협에 신속하게 대응
- 온-프레미스, 오프-프레미스, 네트워크 외부 또는 NAT(Network Address Translation) 뒤 등의 위치와 관계없이 모든 엔드포인트 보호
- 원격 조사를 허용하면서 단 한 번의 클릭만으로 위협 및 침해당한 장치 통제
- 오딧 뷰어로 워크플로우를 향상함으로써 엔드포인트 보안 내에서 위협을 완벽하게 분석
- 침해 사고의 고유한 특성을 해결할 수 있도록 맞춤형 엔드포인트 보안 기능 지원
- 다양한 DMZ 설치 지원

FireEye

완벽한 엔드포인트 커버리지 확보

기업 네트워크 외부에 있는 온사이트 및 원격 엔드포인트는 공격에 취약할 수 있습니다. 하지만 엔드포인트 보안은 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

엔드포인트에서 시작된 공격은 네트워크를 통해 빠르게 확산될 수 있습니다. 엔드포인트 보안은 공격을 파악한 후, 단 한 번의 클릭만으로 침해 당한 장치를 즉시 격리할 수 있으며, 공격을 막아 내부 확산을 방지할 수 있습니다. 그런 다음, 추가 감염의 위험 없이 침해 사고에 대해 완벽한 포렌식 조사를 진행할 수 있습니다.

엔드포인트의 숨겨진 익스플로잇 프로세스 탐지

익스플로잇 탐지와 관련하여, 기존의 EPP(엔드포인트 방어)는 시그니처와 데이터베이스를 비교하기 때문에 그 기능에 한계가 있습니다. FireEye 엔드포인트 보안은 익스플로잇 가드라고 하는 기능을 통해 유연한 데이터 기반 익스플로잇 인텔리전스를 제공합니다. 이 기능은 EDR(엔드포인트 탐지 및 대응) 기능을 제공하여, 기존 엔드포인트 솔루션이 감지하지 못한 영역에 대해 상세히 정보를 수집합니다. 또한 FireEye의 상세한 독점 인텔리전스를 사용하여 개별 활동들의 상호 연관성을 찾아내며 익스플로잇을 파악합니다.

엔트포인트 보안의 작용 방식

엔드포인트 보안은 수만 개의 엔드포인트에서 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.

이를 통해 위협을 검증한 후, 다음을 확인할 수 있습니다:

- 공격자가 엔드포인트에 침투하는 데 사용한 벡터
- 특정 엔드포인트에 공격이 발생했는지(그리고 지속되는지) 여부
- 내부 확산 여부 및 확산된 엔드포인트
- 엔드포인트가 공격자에 노출된 기간
- IP가 유출되었는지 여부
- 추가 침해를 방지하기 위해 통제할 엔드포인트 및 시스템

엔드포인트 보안의 필수 요건

운영 체제	최소한의 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)
Windows Server 2008-2016	2GB
레드햇 엔터프라이즈 리눅스(RHEL) 버전 6.8, 7.2, 7.3	2GB

주: 엔드포인트 보안을 위해서는 1Ghz나 그 이상의 펜티엄 호환 프로세서 및 300MB 이상의 디스크 공간이 필요합니다. 다음 운영 체제에서 작동합니다.

하드웨어 어플라이언스 사양

사양	HX 4402	HX 4400D
저장 용량	4x 1.8TB TB, RAID 10, 2.5인치	4x 600 GB, SAS, 2.5인치, FRU
엔클로저	1RU, 19인치 랙에 적합	
섀시 크기(WxDxH)	17.2" x 27.8" x 1.7"(437 x 706 x 43.2mm)	
AC 전원 장치	중복(1+1) 750와트, 100-240 VAC	
최대 전력 소비(와트)	313와트	
MTBF(h)	35,200h	
단독 어플라이언스	32lb. (15kg)	

주: 엔드포인트 보안은 클라우드, 가상 또는 온프레미스 하드웨어 어플라이언스를 통해 배치될 수 있습니다. 단일 어플라이언스는 엔드포인트를 최대 100,000개까지 지원합니다.

엔드포인트 위협에 네트워크 수준의 경보 연결

FireEye 엔드포인트 보안이 다른 FireEye 제품과 어떻게 함께 작용하는지 확인하십시오. 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, Inc. 소개

FireEye®는 인텔리전스 기반 SaaS(Security-as-a-Service)의 리더입니다. FireEye는 고객 보안 운영의 완벽한 확장을 위해 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 맨디언트 컨설팅을 결합한 단일 플랫폼을 제공합니다. 이를 통해 FireEye는 사이버 공격에 대비, 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 간소화합니다. FireEye는 포브스 글로벌 2000 기업 중 940개 이상의 기업을 포함해 67개국의 5,000여 기업을 고객으로 보유하고 있습니다.

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

www.FireEye.com

FireEye