데이터 시트

FireEye Endpoint Security

일선에서의 위협 대응 경험으로부터 축적된 지식을 바탕으로 공격 예방

주요 기능

- 엔드포인트에 대한 대부분의 사이버 공격 방지
- 침해를 탐지 및 차단하여 침해 피해 감소
- 경보 처리가 아닌 위협을 사전 포착하여 생산성 및 효율성 향상
- 최종 사용자에게 미칠 영향을 최소화하기 위해 소규모 공간의 단일 에이전트 사용
- 다운로드 가능한 모듈을 통한 보호 및 기능 추가
- PCI-DSS 및 HIPAA 등의 규정 준수
- 온사이트 또는 클라우드 배포

새로운 유형의 사이버 공격, 취약성 또는 랜섬웨어 표적은 매일 새롭게 생겨납니다. 보안 담당자는 사용자, 기업 데이터 및 지적 재산을 위협하는 공격에 대처하기가 점점 더 어려워지고 있으며 추가 지원을 기대하기 힘든 상황입니다. 공격에 대응하는 보안 담당자들은 호환성이 낮고 너무 많은 노이즈를 발생시키며 유용성이 떨어지는 수많은 툴로 인해 어려움을 겪습니다. 현재의 시스템으로는 이러한 지능형 위협을 적절히 탐지하고 이에 대응할 수 없을 때도 많습니다.

FireEye Endpoint Security는 FireEye 기술, 전문 지식 및 인텔리전스로 기존의 레거시 보안 제품이 가지는 장점을 극대화함으로써 오늘날의 사이버 공격을 방어합니다. 심층 방어 모델을 사용하는 엔드포인트 보안의 모듈식 아키텍처는 기본 엔진과 다운로드 가능한 모듈을 통합하여 보호, 탐지 및 대응을 수행하고 엔드포인트 보안을 관리합니다.

엔드포인트 보안은 일반적인 멀웨어를 방지하기 위해 시그니처 기반 엔드포인트 보호 플랫폼(Endpoint Protection Platform, EPP) 엔진을 사용합니다. 아직 시그니처가 존재하지 않는 위협을 찾아내기 위해 MalwareGuard는 일선에서 발생하는 사이버 공격으로부터 얻은 지식을 바탕으로 한 머신 러닝 기술을 활용합니다. 일반적인 소프트웨어 및 브라우저에 대한 익스플로잇 공격의 경우, ExploitGuard의 행동 분석 엔진이 익스플로잇 사용 여부를 확인하고, 발견 시에는 실행을 중지합니다. 또한 FireEye는 공격 기술을 탐지하고 새로운 위협에 대한 대응을 가속화하기 위해 지속적으로 모듈을 개발합니다. 예를 들어, Process Guard는 크리덴셜 유출을 방지하기 위해 개발된 모듈입니다.

IT는 학생들을 효과적으로 교육할 수 있게 하는 주요 요소입니다. FireEye Endpoint Security를 통해 IT 자산의 가용성, 고기능성 및 보안성을 확보하고, 조직 환경을 최적화할 수 있었습니다.

— James D. Perry II
University of South Carolina, CISO(최고 정보보안 책임자)

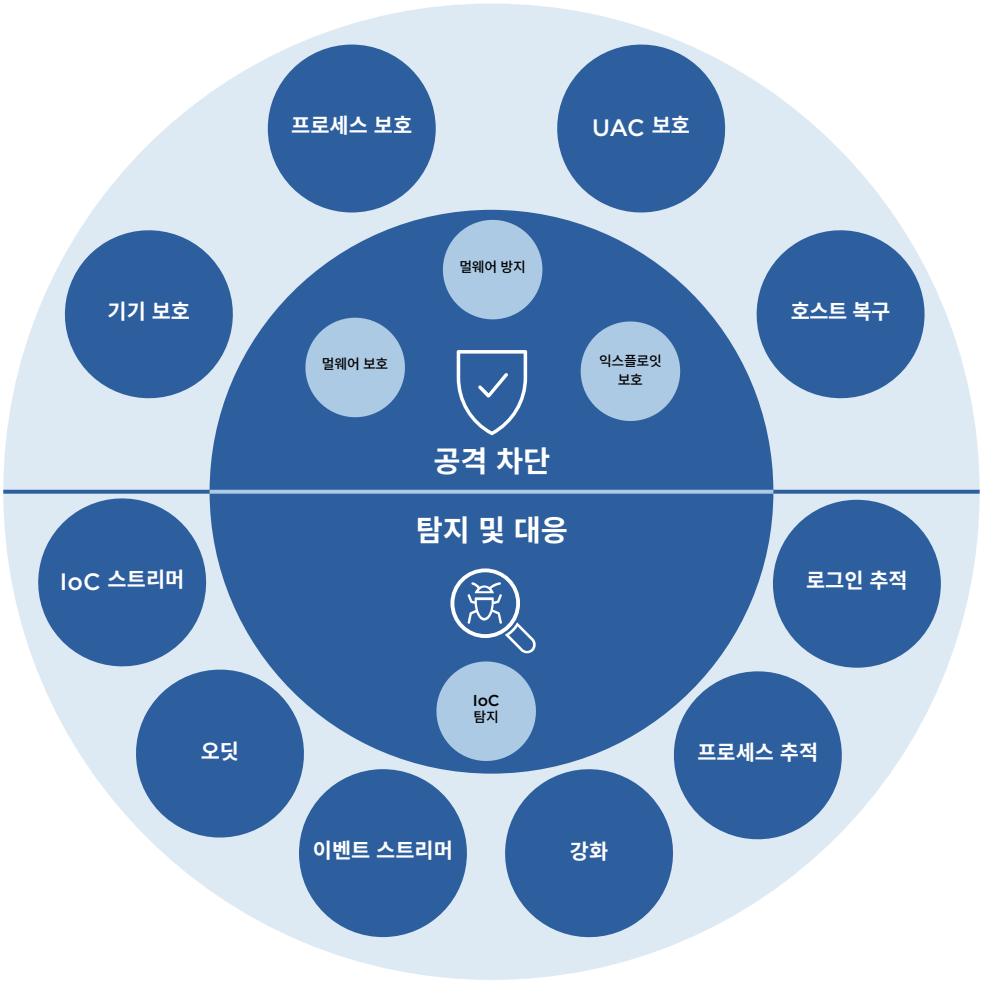
최상의 보호 태세를 갖추고 있더라도 침해는 불가피합니다. 엔드포인트 보안은 일선의 Mandiant 사고 대응팀의 지원으로 개발된 실시간 침해 지표(Indicators of Compromise, IOC)를 기반으로 작동하는 엔드포인트 탐지 및 대응(EDR) 역량을 갖춤으로써 비즈니스가 중단되는 상황을 최소화하는 실질적인 대응을 보장합니다. FireEye 툴의 추가 기능은 다음과 같습니다.

- 수많은 엔드포인트의 알려진 위협과 알려지지 않은 위협을 몇 분 내에 검색 및 조사
- 엔드포인트 침투 시 사용된 공격 경로를 식별하고 상세히 열거
- 특정 엔드포인트에 공격이 발생했는지(그리고 지속되는지) 여부와 확산된 영역 확인
- 엔드포인트 침해의 타임라인 및 기간을 구체화하고 침해 사고를 추적

최근의 위협은 하나의 엔드포인트만을 표적으로 삼지 않으므로, 대부분 침해의 경우 엔드포인트 하나만 복구한다고 해결되지 않습니다. 효과적인 커뮤니케이션으로 위협이 숨어있을 수 있는 모든 디바이스를 식별하고 이 정보를 실시간으로 연관시킬 수 있을 때만 완전한 복구가 가능해집니다. 엔드포인트 보안은 FireEye Helix XDR의 컴포넌트로서, 모든 FireEye 기술과 서비스를 원활하게 연결하여 가장 지능적인 위협까지 탐지 및 대응할 수 있게 해줍니다.

그림 1.

FireEye Endpoint Security
코어 엔진(가운데)과 사용 가능한 모듈(바깥쪽)



대부분의 경영진은 바이러스가 세계의 종말이라고 볼 수 있는 재앙이라고 생각합니다. FireEye를 통해 저는 문제의 본질을 보여주는 실질적인 데이터와 관련 문제를 관리하고 통제할 수 있었는 지에 대한 근거를 제시할 수 있습니다. 이처럼 필요한 정보를 빠르게 파악할 수 있다면 조직 전체가 압박감에서 벗어나게 됩니다.

— Michael Hennessy, Alpha Grainer Manufacturing, Inc
기술 서비스 책임자

주요 기능

- 구성을 최소화하고 탐지 및 차단을 극대화하는 심층 방어를 사용하는 단일 에이전트
- 엔드포인트 보안 내에서 위협을 분석하고 이에 대응할 수 있는 통합 워크플로우
- 안티바이러스(AV) 방어, 머신 러닝, 행동 분석, 침해 지표(IOC) 및 엔드포인트 가시성을 기반으로 멀웨어 차단
- 조직 내 모든 위협으로부터 완전한 복구를 위한 FireEye Helix XDR 컴포넌트

추가 기능

- 기업 보안 검색 - 의심스러운 활동 및 위협을 빠르게 찾아서 인지
- 데이터 수집 - 특정 기간에 걸쳐 상세하고 심층적인 엔드포인트 검사 및 분석을 수행
- 포괄적인 가시성 - 보안 팀이 위협 수준을 빠르게 검색, 확인 및 포착할 수 있음
- 탐지 및 대응 능력 - 엔드포인트를 빠르게 탐지, 조사 및 억제하여 보다 신속하게 대응할 수 있음
- 직관적인 인터페이스 - 의심스러운 모든 엔드포인트 활동에 대한 빠른 정보 확인 및 대응

지원되는 운영 체제 및 환경	
Windows	Windows 7, 8, 8.1, 10 Server 2008R2, 2012R2, 2016, 2019
Mac	10.9-10.15, 11
Linux	RHEL 6.8-6.10, 7.1-7.7, 8-8.2 CentOS 6.9-6.10, 7.1-7.7, 8 SUSE 11.3, 11.4,12.2-12.5, 15 Open SUSE 15.1, 15.2 Ubuntu 12.04, 14.04, 16.04, 18.04, 19.04, 20.04, 20.10 Amazon Linux AMI 2018.3, AM2 Oracle Linux 6.10, 7.6, 8(1 및 2)

배포 옵션: 현장의 물리적 어플라이언스, 현장의 가상 어플라이언스, FireEye Cloud Service

AV-TEST MITRE VirusTotal

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

FireEye Korea
서울특별시 강남구 테헤란로 507
WeWork 빌딩 12층 112호
02-6959-4017
korea.info@fireeye.com

FireEye 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 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 보안 운영의 복잡성을 간소화합니다.

FIREEYE™