데이터 시트

FireEye Network Security

중견기업과 대기업을 위한 효과적인 사이버 침해 보안 솔루션

개요

FireEye Network Security는 인터넷 트래픽을 통한 지능적이고 고도화된 표적 공격을 정확히 탐지하고 즉시 차단시켜 자칫 막대한 금전적인 피해를 입을 수 있는 공격을 최소화시키는 효과적인 사이버 위협 방어 솔루션입니다. 탐지된 보안 사고를 명확한 근거, 활용 가능한 인텔리전스, 그리고 사고 대응 워크플로우 연동을 통해 신속하고 효율적으로 처리할 수 있게 합니다. FireEye Network Security를 사용하면 Microsoft Windows 또는 Apple OS X와 같은 운영 체제나 애플리케이션의 취약점을 이용한 공격과 기업의 본사 또는 지사를 표적으로 하는 위협 또는 실시간 검사가 필요한 대량의 인바운드 인터넷 트래픽을 효과적으로 방어할 수 있습니다.

FireEye Network Security에서는 멀티벡터 가상 실행(Multi-Vector Virtual Execution™, MVX)과 동적 머신 러닝 및 인공 지능(AI) 기술이 중추적인 역할을 합니다.

MVX는 의심스러운 네트워크 트래픽을 검사하여 기존의 시그니처 및 정책 기반 방어 기술을 회피하는 공격을 식별하는 동적 시그니처리스 분석 엔진입니다. 다수의 머신 러닝, AI 및 상관관계 분석 엔진은 머신, 공격자, 피해자에 대한 인텔리전스를 기반으로 악성 활동을 실시간으로 소급 탐지하고 차단하는 컨텍스트 정보 분석을 위한 동적 룰 엔진의 집합체입니다. FireEye Network Security에는 기존의 시그니처 매칭으로 자주 발생하는 공격을 탐지하는 침입 방어 시스템(Intrusion Prevention System, IPS) 기술도 포함되어 있습니다.

FireEye Network Security는 다양한 폼 팩터, 배포 방법 및 성능 관련 옵션을 지원하고, 일반적으로 차세대 방화벽, IPS 및 보안 웹 게이트웨이(Secure Web Gateways, SWG)와 같은 기존 네트워크 보안 어플라이언스의 인터넷 트래픽 경로 내에 배치됩니다. FireEye Network Security는 발생되는 보안 경보에 효율적으로 대응하면서도 오탐이 거의 없는 정확성과 함께 모든 공격을 매우 신속하게 탐지함으로써 이들 솔루션을 보완할 수 있습니다.

그림 1. 일반 구성 - Network Security 솔루션

기능	특장점
위협 탐지	
지능형, 표적 및 기타 우회 사이버 공격을 정확히 탐지	비용이 많이 드는 사이버 침해에 대한 리스크 최소화
확장성이 높은 모듈화된 보안 아키텍처	시스템을 보호하고 비즈니스 성장을 지원
여러 OS 환경과 모든 네트워크 지점에 일관성 있는 수준의 보안 제공	조직 전체에 모든 유형의 디바이스에 대한 강력한 방어 체계 구축
구성 옵션: 통합 또는 분산 설치, 물리적 또는 가상화 구성, 온-프레미스 또는 클라우드 배포 옵션	조직 요구사항과 리소스 구성에 맞는 유연성 높은 기능 선택 옵션
이메일 및 콘텐츠 보안과의 멀티 벡터 상관관계 파악	노출되는 공격 표면 전반에 대한 가시성 확보
공격 차단	
250Mbps~10Gbps의 회선 속도로 공격을 즉시 차단	회피 공격에 대한 실시간 보호 제공
암호화된 트래픽에 대한 가시성	라이선스 비용의 추가 없이 기본 제공 TLS 1.3 복호화 과정을 어플라이언스상에서 지원
대응	
낮은 비율의 거짓 경보, 리스크웨어 범주화 및 MITRE ATT&CK 프레임워크 매핑	신뢰할 수 없는 경보 분류에 드는 불필요한 비용 절감
사고 조사 및 경보 검증, 엔드포인트 격리 및 침해 사고 대응	보안 워크플로우 자동화 및 간소화
정확한 상황 정보 및 활용 가능한 위협 인텔리전스	탐지된 보안 침해 사고의 우선순위 지정 및 해결 가속화

기술적 이점

정확하고 실행 가능한 위협 탐지 및 인사이트

FireEye Network Security는 다양한 분석 기술을 사용하여 공격 탐지의 정확도를 높이고 오탐률을 낮춥니다.

- **멀티벡터 가상 실행(Multi-Vector Virtual Execution™, MVX)** 엔진은 안전한 가상 환경에서 동적 시그니처리스 분석으로 제로데이, 다중 플로우 및 여러 우회 공격을 탐지합니다. 또한 전에 관찰된 적이 없는 익스플로잇과 멀웨어를 식별하여 사이버 공격 킬 체인의 감염 및 침해 단계에서 차단시킵니다.
- **복수의 동적 머신 러닝, AI 및 상관관계 엔진**은 수천 시간에 달하는 최일선에서의 침해 사고 대응 경험을 통해 축적된 실시간 인사이트로 상황에 맞는 룰 기반으로 분석 정보를 제공하는 한편, 난독화 공격, 표적 공격 및 기타 맞춤형 공격을 탐지하고 차단합니다. 또한 악성 익스플로잇, 멀웨어, 피싱 공격 및 커맨드 및 제어(Command and Control, CnC) 콜백을 식별하여 사이버 공격 킬 체인의 감염, 침해 및 침입 단계에서 차단합니다. 의심스러운 네트워크 트래픽을 추출하여 명확한 결과 분석을 위해 MVX 엔진에 전달하기도 합니다. 이러한 엔진은 클라이언트 측 보호 외에도 서버 측 탐지, 내부망 내 이동(lateral movement) 탐지 및 추속 공격 탐지 기능을 지원합니다.
- FireEye Network Security로 발생되는 경보는 새롭게 발견된 표적 공격 사례에 신속하게 대응하고 우선순위를 지정하며 이를 방어하기 위해 구체적인 실시간 근거 데이터를 함께 제공합니다. 상황별 근거 데이터 확보를 위해 탐지된 위협을 MITRE ATT&CK 프레임워크상에 매핑할 수도 있습니다.

신속하고 회복력이 높은 방어

FireEye Network Security는 다음과 같은 유연한 배포 모드를 제공합니다.

- TAP/SPAN을 통한 대역 외 모니터링, 인라인 모니터링 또는 능동적인 인라인 차단. 인라인 차단 모드는 인바운드 익스플로잇 및 멀웨어와 아웃바운드 다중 프로토콜 콜백을 자동으로 차단합니다. 인라인 모니터링 모드에서는 경보가 생성되고 조직에서 경보 대응 방법을 결정합니다. 대역 외 방어 모드에서는 FireEye Network Security가 TCP를 재설정하여 TCP 또는 HTTP 연결을 대역 외에서 차단합니다.
- 몇몇 모드에서 네트워크 또는 장치 장애 발생 시 회복력을 제공하는 능동적인 고가용성(High Availability, HA) 옵션을 제공합니다.

광범위한 공격 표면 보호

FireEye Network Security는 오늘날의 다양한 네트워크 환경에 일관성 있는 수준의 보호를 제공합니다.

- 가장 일반적인 Microsoft Windows 및 Apple Mac OS X 운영 체제 지원.
- 이식 가능한 실행 파일(Portable Executables, PE), 활성 웹 콘텐츠, 아카이브, 이미지, Java, Microsoft 및 Adobe 애플리케이션, 멀티미디어를 포함한 160여 개의 파일 형식 분석.
- 수천 개의 운영 체제, 서비스 팩, IoT 애플리케이션 유형 및 애플리케이션 버전에 대한 의심스러운 네트워크 트래픽 실행.
- 시그니처를 통해 탐지하기 어려운 지능형 공격 및 멀웨어 유형으로부터 보호: 웹 셸 업로드, 기존 웹 셸, 랜섬웨어, 크립토마이너.

검증되고 우선순위가 지정된 경보

FireEye MVX 기술은 실제 공격을 탐지할 뿐만 아니라 기존의 시그니처 매칭 방법으로 탐지된 경보를 검증하며 중요한 위협을 식별하고 우선순위를 결정하는 데 사용됩니다.

- MVX 엔진 검증이 포함된 침입 방지 시스템(Intrusion Prevention System, IPS)은 허위 경보 가능성이 큰 시그니처 기반 탐지를 선별하는 데 소요되는 시간을 줄입니다.
- 리스크웨어 분류는 정상적이진 않지만 비교적 덜 악성인 활동(애드웨어, 스파이웨어 등)과 실제 침해 시도를 구분하여 경보 대응의 우선순위를 지정합니다.

대응 워크플로우 연동

FireEye Network Security는 경보 대응 워크플로우를 자동화하는 몇 가지 방법으로 보안성을 더욱 강화합니다.

- **FireEye Central Management**는 공격을 더 광범위하게 파악하고 더 확산되는 것을 막기 위한 차단 규칙을 설정하기 위해 FireEye Network Security와 FireEye Email Security에서 발생되는 경보를 상호 연결합니다.
- **FireEye Network Forensics**는 FireEye Network Security와 연동되어 경보와 관련된 상세 패킷을 캡처하고 심층 조사를 수행할 수 있게 도와줍니다.
- **FireEye Endpoint Security**는 FireEye Network Security에서 탐지된 위협을 식별, 검증 및 차단하여 영향권에 있는 엔드포인트를 보호하고 복구 절차를 간소화합니다.

유연한 설치 옵션

FireEye Network Security는 조직의 요구사항과 정해진 예산에 따라 다양한 설치 옵션을 제공합니다.

- **통합 네트워크 보안:** 통합된 MVX 서비스를 사용하여 단일 사이트의 네트워크를 보호하는 독립형 올인원 하드웨어 어플라이언스. FireEye Network Security는 규칙, 정책 또는 조정 없이도 빠른 배포가 가능하며 관리하기도 쉬운 클라이언트리스 플랫폼입니다.
- **분산 네트워크 보안:** 중앙의 공유 MVX 서비스를 사용하여 기업의 여러 지역 및 구간에 대한 네트워크 보호를 가능하게 하는 확장형 어플라이언스.
  - **네트워크 스마트 노드:** 인터넷 트래픽을 분석하여 악성 트래픽을 탐지 및 차단하고 정확한 결과 분석을 위해 암호화된 연결로 MVX 서비스에 의심스러운 활동을 알리는 물리적 또는 가상 어플라이언스.
  - **MVX 스마트 그리드:** 온프레미스에서 중앙 관리되는 유연한 MVX 서비스로서, 우수한 확장성, 내장된 N+1 내결함성과 자동 로드 밸런싱 기능 제공.
  - **FireEye Cloud MVX:** 네트워크 스마트 노드에서 트래픽을 분석하여 개인 정보 보호를 보장하여 FireEye에서 호스팅되는 MVX 서비스 구독입니다. 의심스러운 객체만 암호화된 연결을 통해 MVX 서비스에 전송되며, 여기에서 양성으로 밝혀지는 객체는 폐기됩니다.
  - **온프레미스 또는 클라우드에서 보호:** 독립형 어플라이언스와 가상 어플라이언스 외에, FireEye는 Amazon 및 Azure와 같은 퍼블릭 클라우드에서의 네트워크 보안 역시 제공합니다.

그림 2. NX 2550, NX 3500, NX 5500, NX 10550을 포함한 통합 네트워크 보안 예시

그림 3.

네트워크 보안을 위한 분산형 배포 모델

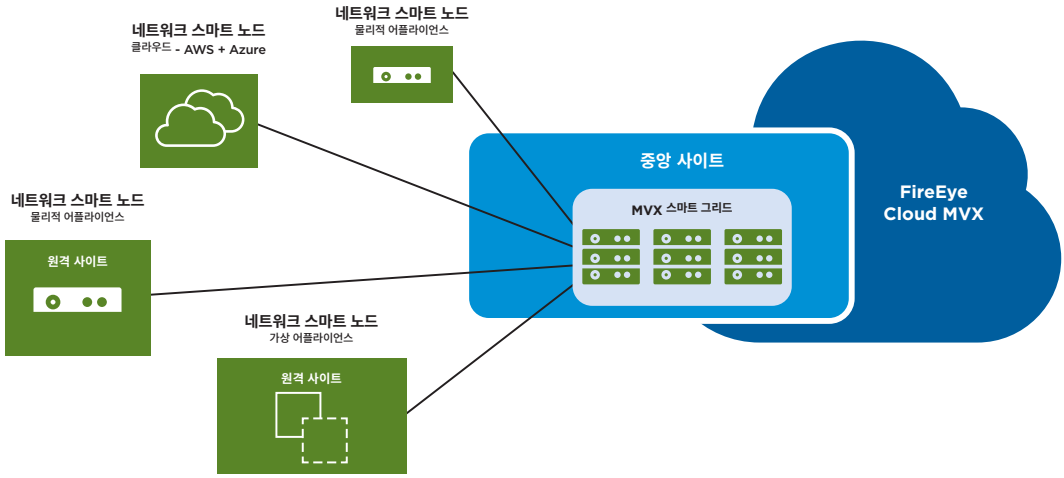
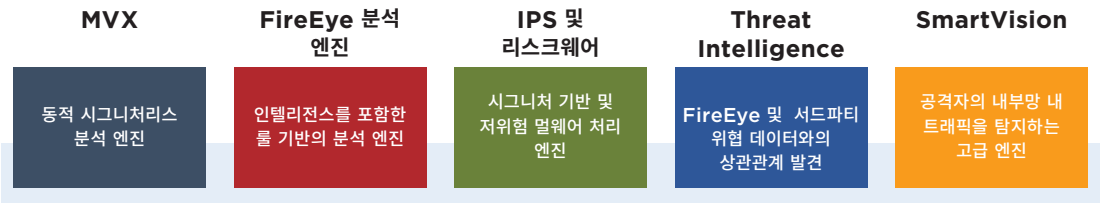


그림 4.

FireEye Network Security의 모듈화된 컴포넌트



뛰어난 성능 및 확장성

FireEye Network Security는 다양한 규모의 조직을 위한 성능 옵션을 제공하여 네트워크를 보호합니다.

MVX 스마트 그리드와 FireEye Cloud MVX의 확장 가능한 아키텍처를 통해 MVX 서비스가 한 개에서 수천 개의 네트워크 스마트 노드를 지원하고 필요에 따라 탄력적으로 확장할 수 있습니다.

폼 팩터	성능
통합 네트워크 보안	50Mbps-5Gbps
물리적 네트워크 스마트 노드	50Mbps-10Gbps
가상 및 퍼블릭 클라우드 네트워크 스마트 노드	50Mbps-8Gbps

비즈니스 상의 특장점

단일 사이트나 여러 사이트로 분산되어 있는 조직에 맞춰 설계된 FireEye Network Security는 다양한 이점을 제공합니다.

사이버 침해로 인한 리스크 최소화

FireEye Network Security는 다음과 같은 기능을 제공하는 매우 효과적인 사이버 방어 솔루션입니다.

- 고도화된 표적 공격 및 기타 다양한 우회 공격을 차단함으로써 공격자가 조직 네트워크에 침입하여 주요 자산을 훔치거나 비즈니스 혼란을 일으킬 수 없게 합니다.
- 구체적인 정보, 실행 가능한 인텔리전스, 인라인 차단 및 대응 워크플로우 자동화로 보다 빠르게 공격과 침입을 차단합니다.
- 다양한 운영 체제, 애플리케이션 유형, 지사 및 중앙 사이트에 대한 일관성 있는 보호로 조직의 사이버 방어의 취약점을 없앱니다.

짧은 투자 회수 기간

Forrester Consulting의 조사[1]에 따르면 FireEye Network Security 고객은 3년간 ROI를 152% 절약하고 단 9.7개월 만에 초기 투자금을 회수한 것으로 알려졌습니다. FireEye Network Security:

- 보안팀 리소스로 하여금 실제 공격에 집중하도록 하여 운영 비용을 줄입니다.
- 조직의 요구 사항에 맞는 다양한 규모로 설치가 가능하고 다양한 성과 점수와 공유 MVX 서비스로 비용을 최적화합니다.
- 기업의 지사 수나 인터넷 트래픽 양이 증가할 경우 유연하게 확장시켜 보안 투자의 효과를 보장합니다.
- 통합 설치에서 분산 설치로 무상 마이그레이션을 지원하여 기존에 투자된 시스템을 보호합니다.
- 확장 가능한 모듈식 아키텍처로 투자 비용을 감소시킵니다.

1 Forrester(2016년 5월). FireEye의 전반적인 경제적 효과

수상 내역 및 인증

FireEye Network Security의 제품 포트폴리오는 업계 및 정부로부터 다수의 수상 및 인증을 받았습니다.

- FireEye는 2020년 해군 정보전 시스템 사령부(Naval Information Warfare Systems Command, NAVWAR) 인공지능 사이버보안 챌린지에서 1위를 차지했습니다.[2]
- KuppingerCole은 2020년 네트워크 탐지 및 대응의 리더십 부문에서 FireEye에 상을 수여했습니다.[3]
- Forrester는 2020년 FireEye를 네트워크 분석 및 가시성 분야의 주요 공급업체로 선정했습니다[4]
- Frost & Sullivan은 2018년 FireEye를 보안 산업의 리더로 선정했습니다. FireEye의 시장 점유율은 46%로, 다음 10개 경쟁업체의 시장 점유율을 합친 것보다 높습니다.[5]
- FireEye Network Security는 Common Criteria, FIPS 140-2 및 SOC 2를 비롯한 여러 인증을 획득했습니다.
- FireEye Network Security는 SANS Institute, SC Magazine, CRN 등으로부터 수많은 상을 받았습니다.
- FireEye Network Security는 미국 국토안보부 안전법 인증(US Department of Homeland Security SAFETY Act Certification)을 받은 업계 최초의 보안 솔루션입니다.

2 FireEye(2021년 1월 6일). 해군 정보전 시스템 사령부(NAVWAR)가 FireEye를 네트워크 위협 탐지 챌린지의 우승자로 선정
3 KuppingerCole(2020년 1월 10일). 네트워크 탐지 및 대응의 리더십 부문
4 Forrester(2020년 6월 23일). Now Tech: 네트워크 분석 및 가시성 부문, 2020년 2분기.
5 Frost & Sullivan(2018년 7월 5일). 2022년까지의 글로벌 지능형 멀웨어 샌드박스(AMS) 솔루션 시장 예측

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™