FIREEYE™

진화하는 네트워크 위협의 과제 해결

다른 조직에서 탐지하지 못하는 공격에 대비하세요

오늘날의 보안 과제

지능형 표적 공격과 기타 우회 공격으로 사이버 침해를 효과적으로 예방하는 것이 극히 어려워지고 있습니다.

- 사이버 범죄자는 지능형 공격을 사용하여 차세대 방화벽, IPS 및 안티바이러스 솔루션을 우회하고, 수 개월간 조직 내부에 잠복합니다(외부로부터 알려진 경우를 추산했을 때 2015년에는 평균 320일의 잠복기간).[1]
- 악성코드의 68% 이상이 한 조직에 맞춰 설계되었고 해당 악성코드의 80%는 단 한 번만 사용됩니다.[2] 이에 따라 시그니처 기반의 방어는 표적 공격에 효과가 없습니다.
- 시그니처 기반 및 정책 기반 보안에서 생성된 경보의 80% 이상은 신뢰할 수 없습니다.[3] 이로 인해 중요한 경보에 리소스를 집중하지 못합니다.

오늘날 비즈니스가 IT에 더욱 의존하게 되면서, 조직을 공격할 수 있는 접점이 더욱 확대되고 있습니다.

- 2020년까지, 공용 클라우드 애플리케이션이 기업 지출의 3분의 2를 넘을 것으로 예상됩니다.[4] 클라우드 기반 운영으로 조직의 인바운드 및 아웃바운드 인터넷 트래픽(그리고 이에 따른 잠재적 위협)이 40%까지 증가합니다.[5] 그리고 이러한 트래픽을 모두 검사해야 합니다.
- 현재 조직의 96%에서 지원하는 비 Windows 디바이스는 일반적으로 제대로 보호되지 않고 있습니다.
- 지사의 40%에서 사용하는 인터넷 직접 연결 링크는 강력한 보호 체계를 갖춘 본사가 외부의 공격에 노출될 가능성을 높입니다.

사이버 침해 방어의 네 가지 요구 사항

경제적으로 막대한 손실을 끼치는 사이버 침해 위험을 최소화하기 위해 공격을 효과적으로 방어하는 솔루션이 모든 규모의 조직에 필요합니다. 요건:

1. 기존의 보안 제품이 감지하지 못하는 위협 탐지 및 방어
2. 침해 사고에 대한 신속한 대응 및 저지
3. 진화하는 위협 환경에 지속적으로 적응
4. 조직 성장 또는 IT 서비스 제공 모드 변화에 따라 확장 및 유연성 유지

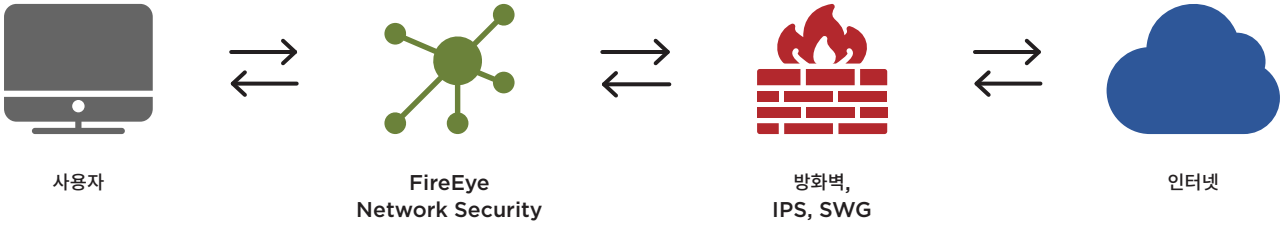
FireEye Network Security

모든 규모의 조직은 FireEye Network Security를 통해 인터넷 트래픽에 숨겨진 지능형 표적 공격과 기타 우회 공격을 정확히 탐지하고 즉시 차단하여 침해에 따른 경제적 손실을 최소화할 수 있습니다. FireEye Network Security의 핵심에는 MVX(Multi-Vector Virtual Execution™ 및 IDA(Intelligence-Driven Analysis) 기술이 있습니다. MVX는 의심스러운 객체를 검사하여 표적 및 우회 위협과 알려지지 않은 위협을 파악하는 시그니처리스 동적 분석 엔진입니다. IDA 엔진은 머신 인텔리전스, 공격자 인텔리전스 및 희생자 인텔리전스를 기반으로 하여 악성 객체를 탐지하고 차단합니다.

FireEye Network Security는 다양한 폼 팩터 및 설치 모델에서 사용할 수 있으며, 대개 차세대 방화벽, IPS 및 SWG(보안 웹 게이트웨이)와 같은 기존 네트워크 보안 어플라이언스 뒤의 인터넷 트래픽 경로에 배치됩니다.

1 FireEye(2016년 2월). M-Trends 2016.
2 Joshua Goldfarb(2016년 9월 19일). “Detection Innovations(탐지 혁신).”
3 Ponemon Institute LLC(2015년 1월). “The Cost of Malware Containment(악성코드 억제 비용).”
4 Forrester(2016년 9월). “The Public Cloud Services Market Will Grow Rapidly to $236 Billion in 2020(공용 클라우드 서비스 시장은 2020년에 2,360억 달러까지 급속히 성장할 것 입니다).”
5 IDC(2016년 2월). “Communication Service Provider Adoption of SD-WAN Technology and Its Impact to MPLS VPN Services(통신 서비스 제공자의 SD-WAN 기술 채택 및 MPLS VPN 서비스에 대한 영향).”
6 JAMF Software(2015년). 2015 Survey: Managing Apple Devices in the Enterprise(2015년 설문조사: 기업의 Apple 장치 관리)

그림 1. 일반 구성 - 네트워크 보안 솔루션.



사이버 침해로부터 모든 규모의 조직을 효과적으로 방어하기 위해서 FireEye Network Security는 다음을 제공합니다.

- **정확한 탐지 기능:** MVX 및 IDA 기술은 허위 경보 생성 비율을 최소화하면서 높은 정확도로 공격을 탐지합니다. 또한 이러한 기술은 다중 흐름의 이벤트와 위협 경로의 연관성을 통해 다른 솔루션이 탐지하거나 막을 수 없는 단계적인 공격을 방어합니다.
- **즉각적이고 탄력적인 방어:** 인바운드 익스플로잇 및 악성코드와 아웃바운드 다중 프로토콜 콜백에 대한 인라인 차단을 통해 공격을 즉시 저지합니다. 네트워크 링크 또는 디바이스에 장애가 발생한 경우 고가용성 옵션을 통해 추가적인 회복력과 방어를 제공합니다.
- **실행 가능한 통찰력:** 경보에는 최일선에서 수집한 상황 인텔리전스와 구체적인 증거가 포함되는데, 이를 통해 위협에 신속하게 대응하고, 우선순위를 정하며, 위협을 격리할 수 있습니다.
- **지표 수집:** STIX(Structured Threat Intelligence eXpression) 형식을 사용하여 IDA 엔진에 맞춤형 인텔리전스를 주입할 수 있습니다.
- 신규 **확장 가능한 아키텍처:** 소프트웨어 및 시스템 설계를 통해 다중 위협 방어 기술을 소프트웨어 모듈로 제공할 수 있습니다.

- **포괄적인 방어 기능:** 광범위한 공격에 모두 대처하기 위해 가장 일반적인 Microsoft Windows 및 Apple OS X 운영 체제, 140가지 이상의 다양한 파일 형식 및 수많은 운영 체제, 서비스 팩 및 애플리케이션 조합을 비롯하여 다양한 환경을 지원합니다.
- **대응 워크플로우 통합:** 심층 조사를 위한 경보 검증, 리스크웨어 분류 및 패킷 캡처로의 전환을 통해 경보 대응 워크플로우를 자동화하고 가속화합니다.

모든 조직에 이상적

FireEye Network Security는 중간 규모와 대규모 조직의 요구와 예산에 맞게 최대 8Gbps까지 유연하고 확장 가능한 설치 옵션을 제공합니다.

- **통합 네트워크 보안:** MVX 서비스를 사용하여 단일 인터넷 접근 지점을 보호하는 스탠드얼론, 올인원 하드웨어 어플라이언스입니다.
- 신규 **분산 네트워크 보안:** 네트워크 스마트 노드 및 공유 MVX 서비스를 통해 전체 조직으로 보안을 확장합니다.
  - **네트워크 스마트 노드:** 의심스러운 활동을 식별하고 방어하기 위해 인터넷 접근 지점에 배치되는 물리적 또는 가상 어플라이언스입니다.
  - **MVX 스마트 그리드 또는 FireEye 클라우드 MVX:** 지능형 공격을 탐지하고 보안팀을 더 효율적으로 운영하기 위해 추가 분석을 수행하는 온-프레미스 또는 클라우드 기반 MVX 서비스입니다.

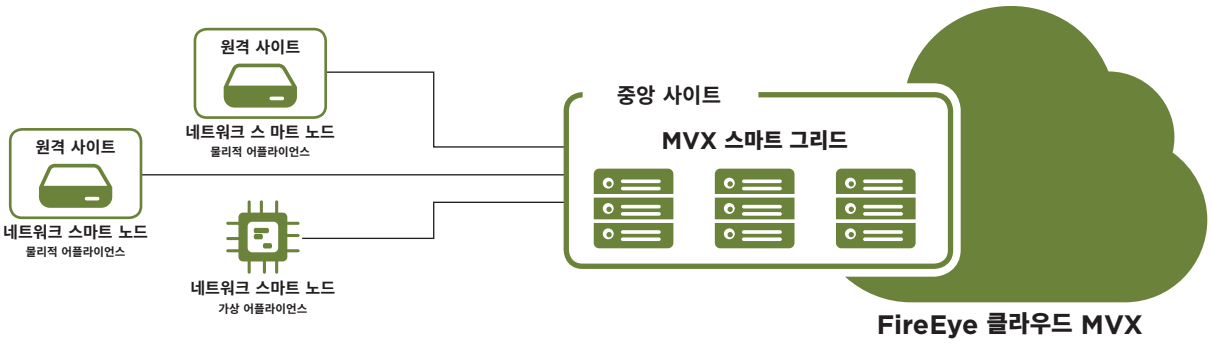


그림 2. 분산 네트워크 보안.

FireEye Network Security 에센셜은 중소규모 조직을 위해 10Mbps~2Gbps 범위의 비용 효율적인 통합형 및 분산형 설치 옵션을 제공합니다.

표 1. FireEye Network Security 설치 옵션.

	통합 어플라이언스	네트워크 스마트 노드	MVX 스마트 그리드 네트워크 스마트 노드 필요	FireEye 클라우드 MVX 네트워크 스마트 노드 필요
중견 및 대규모 조직용 FireEye Network Security	온-프레미스	물리적 또는 가상	온-프레미스 및 분산	클라우드 기반 및 분산
중소 규모 조직용 FireEye Network Security 에센셜	온-프레미스	물리적 또는 가상	해당 없음	클라우드 기반 및 분산

짧은 투자 회수 기간

단일 사이트와 분산된 다중 사이트 조직 모두의 필요에 맞게 설계된 FireEye Network Security는 사이버 침해 위험을 최소화하고 투자 회수 기간을 단축시킵니다.

Forrester Consulting의 최근 조사에 따르면[7] FireEye Network Security 고객은 3년간 비용 절감을 통해 152%의 ROI를 예상하고 단 9.7개월 만에 초기 투자 회수를 기대할 수 있습니다. 비용 절감은 다음을 통해 달성할 수 있습니다.

- 보안 팀 리소스를 실제 공격에 집중하여 운영 비용을 줄입니다.
- 설치 규모를 적절히 조정할 수 있도록 MVX 용량과 다양한 성능을 나누어 사용하는 옵션을 이용할 수 있으며, 이를 통해 자본 지출을 최적화합니다.
- 지사의 수 또는 인터넷 트래픽 양이 증가할 경우 용량 확장을 허용하여 투자의 미래를 보장합니다.
- 통합 설치에서 분산 설치로 무상 마이그레이션을 지원하여 기존 투자를 보호합니다.
- 확장 가능한 모듈식 아키텍처로 향후 자본 지출을 줄입니다.

왜 FireEye Network Security를 선택해야 하는가?

FireEye MVX 엔진은 다음과 같이 지능형[8] 위협에 대해 시장에서 가장 독창적이며 성공적인 방어 솔루션입니다.

- FireEye는 2013년부터 현장에서 많이 악용되는 제로데이 공격을 다른 모든 솔루션을 합한 것보다 더 많이 발견했습니다.
- 2016년 Frost & Sullivan에서 FireEye를 독보적인 시장 리더로 선정했습니다. FireEye의 시장 점유율은 56%로 다음 10개 경쟁업체의 시장 점유율을 합친 것보다 높습니다.[9]
- 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 시장 최초의 보안 솔루션입니다.

7 Forrester(2016년 5월). "The Total Economic Impact Of FireEye(FireEye가 전체 경제에 미친 영향)."
8 IDC(2015년). Worldwide Specialized Threat Analysis and Protection Market Shares(전 세계적 전문 위협 분석 및 방어 시장점유율).
9 Frost & Sullivan(2016년 9월). "Network Security Sandbox Market Analysis(네트워크 보안 샌드박스 시장 분석)."

표 2. FireEye Network Security의 이점

기능	이점
기존의 보안 제품이 감지하지 못하는 위협 탐지 및 방어	
시그니처리스 위협 탐지(MVX)	다중 흐름, 다단계 공격, 제로데이, 다형, 랜섬웨어 및 기타 우회 공격 탐지
실시간 및 소급 탐지	과거 위협 탐지도 지원하는 동시에 알려진 위협과 알려지지 않은 위협을 실시간으로 탐지
다중 경로 상관관계	이메일, 엔드포인트 및 파일 경로의 공격 검증 및 차단 자동화
다중 OS, 다중 파일 및 다중 애플리케이션 지원	광범위한 애플리케이션과 다양한 엔드포인트 환경 지원
강화된 하이퍼바이저	회피 방지 기능 제공
침해 사고에 대한 신속한 대응 및 저지	
실시간 인라인 차단	공격 즉시 저지
통합된 보안 워크플로우	탐지에서 조사 및 대응으로 전환
HA(고가용성)	복구 탄력성 방어
노이즈 감소를 통한 시그니처 기반 IPS 탐지	기존의 번거로운 경보 선별을 자동화하고 가속화하여 수동 오버헤드 제거
리스크웨어 탐지 및 분류	중요한 악성코드와 중요하지 않은 악성코드를 분류하여 대응 리소스의 우선순위 지정
적용 가능한 상황 인텔리전스	공격 및 공격자에 대한 심층적인 정보를 사용하여 지능형 위협 억제를 가속화
진화하는 위협 환경에 지속적으로 적응	
실시간 위협 인텔리전스 공유	실제 증거를 전 세계와 공유하여 이전에 알려지지 않은 공격 즉시 차단 및 대응 가속화
신규 **맞춤형 및 타사 위협 인텔리전스(STIX)**	STIX에서 이용 가능한 IDA 엔진에 FireEye 및 타사 지표 수집
전략적 위협 인텔리전스	위협 환경 변화에 대한 선제적 평가 지원 및 린포워드 보안 태세 강화
조직 성장 또는 IT 서비스 제공 모드 변화에 따라 확장 및 유연성 유지	
지원되는 대역폭	10Mbps-8Gbps
지원되는 규모	분산 설치의 경우 단일 사이트에서 수천 개의 사이트까지 지원
지원되는 폼 팩터	물리적, 가상, 클라우드
설치 모델	통합 네트워크 보안 및 분산 네트워크 보안 (네트워크 스마트 노드 및 MVX 서비스 아키텍처 사용)

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

FireEye, Inc.
서울특별시 강남구테헤란로 534 글라스타워 20층
02.2092.6580
korea.info@FireEye.com

FireEye, Inc. 소개

FireEye는 인텔리전스 기반의 보안 회사입니다. FireEye는 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영의 완벽한 확장을 지원합니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 간소화합니다. FireEye는 포브스 글로벌 2000 기업 중 45% 이상의 기업을 포함해 67개국의 6,600여 기업을 고객으로 보유하고 있습니다.

FIREEYE™