FireEye

공격 체인을 저지하여 비즈니스 위험 최소화

FireEye Security Suite 활용

91%의 사이버 공격이 스피어 피싱 이메일로부터 시작됩니다.[1]

사이버 공격 체인 문제

위협 범죄자들은 그 유형마다 동기가 서로 다르지만 결국 노리는 것은 하나입니다. 바로 여러분의 데이터에 액세스하는 것입니다. 데이터는 21세기의 화폐라고 할 수 있습니다. 데이터는 모든 공격 임무의 중심이 되며, 그러한 임무는 표준 공격 체인에 따라 실행됩니다. 보안 전문가들은 체인의 모든 지점에서 공격을 저지하기 위해 애쓰고 있습니다. 여기에는 사일로로 구축된 포인트 제품이 아니라 종합적인 통합 분석을 통해 단서를 취합하고 비즈니스에 미치는 심각한 영향을 방지할 수 있는 솔루션이 필요합니다.

이메일은 표적화/맞춤화를 통해 성공적으로 악용하기 쉽기 때문에 지능형 공격이나 랜섬웨어 공격의 수단으로 꾸준히 이용되고 있습니다. 기존의 안티스팸 필터 및 안티바이러스 소프트웨어는 알려진 악성 첨부 파일, 링크 및 콘텐츠를 이용하는 전통적인 대규모 피싱 위협을 포착하는 데에는 효과적이지만, 이러한 솔루션을 우회하도록 고안된 정교하게 표적화된 스피어 피싱 공격과 사칭 공격은 포착하지 못합니다.

기존의 엔드포인트 보안은 최신 위협에 효과적이지 않으며, 정교한 지능형 지속 위협(APT) 공격을 해결하기 위한 적절한 솔루션이 아닙니다. 엔드포인트의 보안을 유지하려면 솔루션이 그러한 위협을 빠르게 분석하고 그에 따라 대응해야 합니다.

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. 기존 및 차세대 방화벽, 침입 방법 시스템(IPS), 보안 웹 게이트웨이(SWG)는 공격자의 수단과 수법을 알 때 효과가 있습니다. 지능형, 표적 및 기타 우회 사이버 공격을 탐지하고 방어하는 데에는 효과적이지 않습니다. 오늘날의 흔한

1 PhishMe(2016년). "Enterprise Phishing Susceptibility and Resiliency Report."
2 Joshua Goldfarb(2016년 9월 19일). "Detection Innovations(탐지 혁신)."

사이버 범죄자들은 기존의 네트워크 보안 기술을 우회하는 지능화된 기법을 활용할 수 있습니다. 데이터를 빼내는 것은 물론이고, 때로는 수개월 또는 수년까지 발견되지 않은 채 네트워크에 상주하기도 합니다.

공격 체인 저지

일반적으로 공격은 악성 이메일로 시작되지만 엔드포인트 장치에서 최초로 나타나거나 의심스러운 아웃바운드 네트워크 트래픽에서 시작되기도 합니다. 이 같은 체인의 모든 지점에서 공격을 저지하려면 통합된 가시성을 확보해야 합니다. FireEye Security Suite는 모든 규모의 조직에 네트워크, 이메일 및 엔드포인트를 보호하는 엔터프라이즈급 보안 솔루션을 제공합니다. FireEye Email Security, FireEye Endpoint Security 및 FireEye Network Security의 모든 기능을 통해 지능형 공격을 방어하고 사고 대응을 가속화하며 핵심 비즈니스를 보호합니다.

이메일 보호

FireEye Email Security는 지능화된 스피어 피싱 및 사칭 공격, 알려지지 않은 악성코드에 대한 지능형 위협 방어 기능을 제공하여 무단 액세스와 데이터 손실 및 보안 침해를 방지합니다.

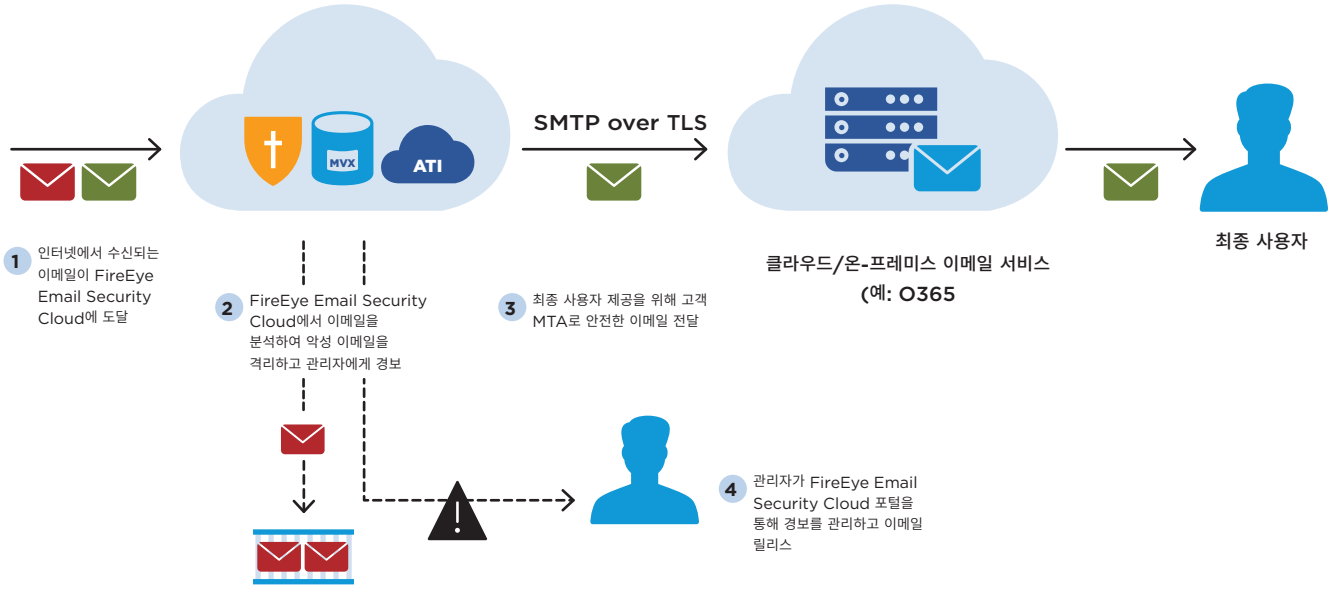

그림 1. FireEye Email Security를 사용한 인라인 차단.

엔드포인트 보호

FireEye Endpoint Security는 고객 환경의 모든 엔트리 포인트를 일반적인 위협과 지능형 위협으로부터 방어합니다. 시그니처 엔진, EDR(엔드포인트 탐지 및 대응) 기능 및 위협 인텔리전스를 결합한 Endpoint Security는 단순 공격과 지능형 공격을 탐지하고 차단합니다.

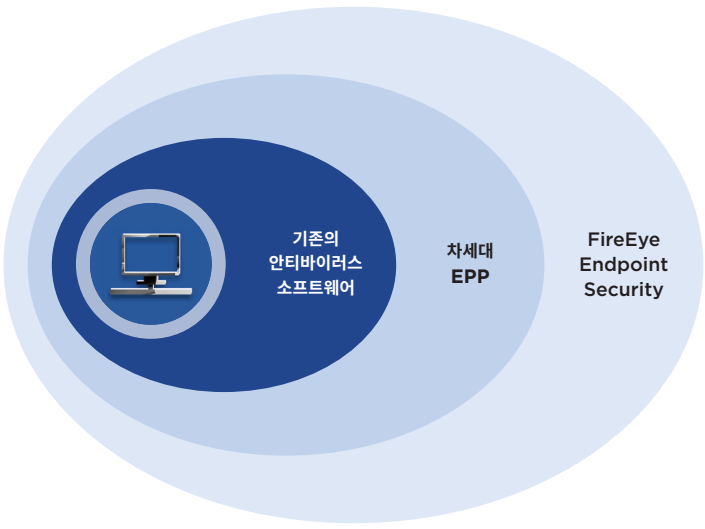

그림 2. FireEye Endpoint Security를 사용한 보호 범위 확대.

네트워크 보호

FireEye Network Security는 지능형 공격을 차단하고 세계에서 가장 지능화된 공격에 대한 가시성을 제공합니다. 특허받은 Multi-Vector Virtual Execution(MVX) 엔진을 기반으로 한 Network Security는 여타 어떤 회사도 제공하지 못하는 독보적인 방식으로 트래픽을 분석할 수 있습니다.

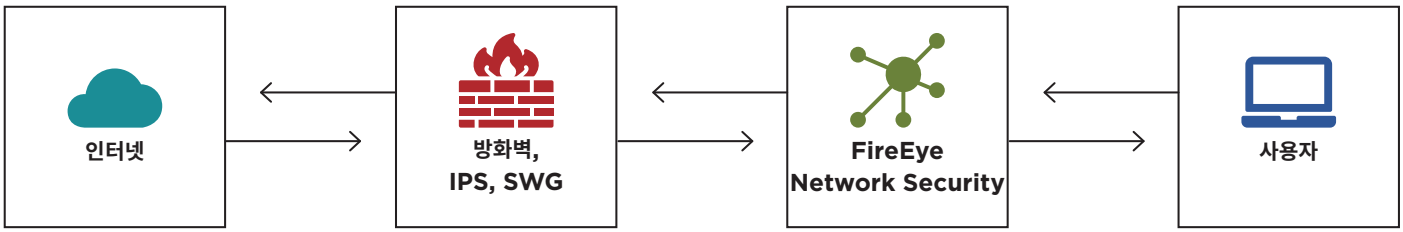

그림 3. FireEye Network Security의 강화된 방어 계층.

FireEye Security Suite의 작동 방식

효과적인 보안 기능의 제공 이외에도 FireEye Security Suite는 보안 운영을 간소화하고 자동화합니다. 이를 위해 이메일, 엔드포인트 및 네트워크에 대한 FireEye 보안 솔루션의 경보를 FireEye Helix라는 단일 클라우드 기반 플랫폼으로 통합합니다.

1. FireEye 이메일, 엔드포인트 및 네트워크 보안 솔루션은 각각 다양한 지능형 공격을 탐지하도록 전문화되어 있지만 경보 통합을 통해 정보를 중앙 집중화하여 완전한 위협 내러티브를 구축합니다.
2. FireEye의 일선 전문가들이 개발한 상관관계 분석 및 상황 위협 인텔리전스는 중요하고 위험을 포착할 수 있는 경보를 찾아내는 프로세스를 효율화하는 데 도움이 됩니다.
3. FireEye 보안 솔루션은 각각의 주요 공격 경로에서 발견하는 가장 중요한 위협을 차단할 수 있습니다.
4. 포함된 툴로 위협을 억제할 수 있지만 어떤 데이터가 어떻게 도용되었는지도 확인해야 합니다. 강력한 탐지 및 대응 툴을 사용하여 보안 침해의 원인이 된 공격 체인을 재현하고 침해 조사에서 알아보고자 하는 주요 항목에 대한 답을 찾을 수 있습니다. 구체적인 경보가 없는 상황에서도 이 동일한 툴과 인텔리전스를 사용하여 위협을 사전에 포착할 수 있습니다.

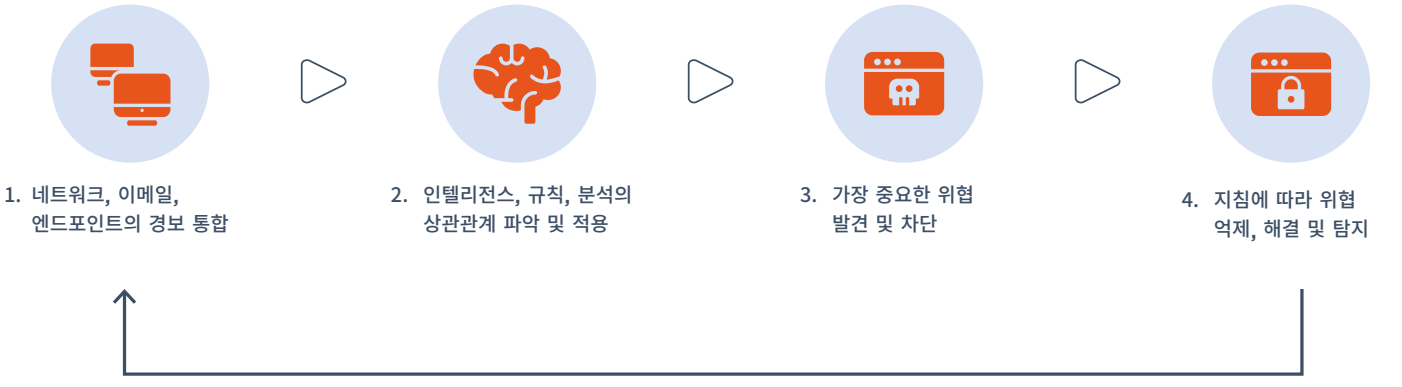

그림 4. FireEye Helix를 사용한 운영 간소화 및 자동화.

가치 실현

사용자 규모가 100~2,000명인 조직에 최적화된 FireEye Security Suite는 데이터 비밀 유지, 무결성 및 가용성과 관련한 비즈니스 위험을 최소화하도록 설계되었습니다. 벤더 통합과 사용자별 요금으로 구매가 간소화됩니다. 또한 지능형 사이버 보안 기능을 신속하게 추가하고 채택할 수 있습니다.

비용 관리

사용자별 요금으로
구매 간소화

효율성 개선

벤더 통합으로
여러 위협 경로 방어

비즈니스 위험 최소화

실제 위협을 신속하게 포착

사례연구

사용자 규모가 200명 미만인 말레이시아의 한 알루미늄 압연 제품 공급업체는 피싱 공격으로 인한 피해를 입고 있던 중 FireEye Security Suite에 대해 알게 되었습니다. 이 회사는 독일, 오스트레일리아 및 일본을 비롯한 전 세계의 대규모 기업 고객을 지원하므로 높은 수준의 사이버 보안 숙련도와 실사 결과를 제시해야 했습니다. FireEye의 평판과 Security Suite의 합리적인 가격대가 구매 결정을 좌우한 주된 요인이었습니다.

천연 유기농 식품 및 건강 보조 제품을 판매하는 필리핀의 한 소매 조직은 사용자가 약 350명으로, 고객 보상 프로그램에서 고객 개인 데이터의 기밀성이 얼마나 중요한지를 인식하게 되었습니다. 이에 FireEye가 데이터와 브랜드 평판을 보호할 파트너로 제시됐습니다. 주 공격 경로를 광범위하게 방어하는 FireEye Security Suite의 기능은 구매 결정을 내리는 데 크게 작용했습니다.

싱가포르 국내의 한 통합 대중교통 서비스 회사는 철도 차량의 설계, 조립 및 유지보수를 비롯한 원스톱 솔루션과 재무 및 운영 관리 서비스를 제공합니다. 랜섬웨어 공격으로 회사가 큰 피해를 입으면서 향후 보안 사고를 예방해야 할 필요성이 대두되었습니다. FireEye Email Security로 기존 이메일 게이트웨이에서 탐지되지 않던 위협을 탐지할 수 있었기 때문에, 이들은 FireEye Security Suite를 도입하여 엔드포인트와 네트워크까지 보호함으로써 전체 보안 프레임워크의 미래 가치를 확보하기로 결정했습니다.

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

FireEye Korea
서울 특별시 강남구 테헤란로 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.

FireEye®