데이터 시트

FireEye Email Security Cloud Edition

이메일 공격을 식별 , 분석 및 차단하는 클라우드 기반 보호 솔루션

요약

- 포괄적인 인바운드 및 아웃바운드 이메일 보안 제공
- 이메일 보안 스택을 포괄적인 단일 벤더 솔루션과 통합
- 위협 탐지 효율을 높일 수 있도록 맞춤형 YARA 규칙 지원
- 경보 우선순위를 지정하여 대응 가속화
- 모든 타사 이메일 제공자와 통합
- 일선의 조사와 공격자 관찰을 통해 얻은 공격 및 공격자에 대한 심층적인 지식 제공
- FedRAMP 보안 요건 준수

"이메일은 모든 협업 환경의 토대가 되는 만큼, FireEye Email Security를 구축함으로써, 많이 악용되는 이메일 채널이 침해당할 위험을 단일 솔루션으로 해결할 수 있게 된 것은 저희에게 큰 의미가 있습니다."

Nils Göldner
매니징 파트너 겸 클라우드 자문가
Blackboat GmbH

개요

이메일은 데이터가 가장 많이 들어오는 지점이기 때문에 사이버 공격에 무엇보다 취약합니다. 조직들은 이메일 기반의 스팸, 악성코드 및 지능형 위협의 숫자가 계속 증가하는 위험에 직면해 있습니다. 이메일을 통해 침투하는 지능형 위협은 대부분 인증 피싱 사이트에 연결된 URL, 사기 송금 요청, 무기화된 첨부 파일의 형태를 띱니다. 고도로 타겟팅되고 사용자 정의가 가능한 이메일의 특성을 사이버 범죄자들이 성공적으로 이용하므로, 사이버 범죄의 주요 수단이 됩니다.

FireEye Email Security는 지능형 이메일 공격으로 인한 고비용 침해 위험을 최소화하는 단일 이메일 보안 솔루션을 통해 비용을 절감하고 직원의 생산성을 높입니다. 클라우드에 구축된 FireEye Email Security는 완벽한 기능을 갖춘 이메일 게이트웨이로, URL, 사칭 및 첨부 파일 기반 공격을 식별, 격리 및 즉시 중지하는 데 있어 업계를 선도하고 있습니다. 또한 FireEye Email Security는 이메일 트래픽을 검사하여 지능형 위협, 스팸 및 바이러스를 찾아냅니다.

인텔리전스 기반 컨텍스트와 탐지 플러그인의 결합을 이용하여, 악성 URL을 진정한 빅 데이터, 확장 가능한 플랫폼에서 찾아냅니다. 발신인 이름 및 이메일 주소에 대한 신뢰성을 확인하고 CEO 사기 및 기타 악성 프로그램 공격을 차단하기 위한 가장 전술이 있는지 내용을 검토합니다. 시그니처리스 Multi-Vector Virtual Execution™(MVX) 엔진은 이메일 첨부 파일 및 URL을 운영 체제, 애플리케이션 및 웹 브라우저의 포괄적인 크로스 매트릭스와 대조하여 분석합니다. 그리고 최소한의 노이즈로 위협을 식별하며, 오탐률은 0에 가깝습니다.

FireEye는 수백만 개의 센서를 통해 공격자 및 직접 침입 조사와 관련한 광범위한 위협 인텔리전스를 수집합니다. Email Security는 공격 및 공격자에 대한 이와 같은 실제 증거와 상황 인텔리전스를 활용하여 경보의 우선순위를 정하고 위협을 실시간으로 차단합니다.

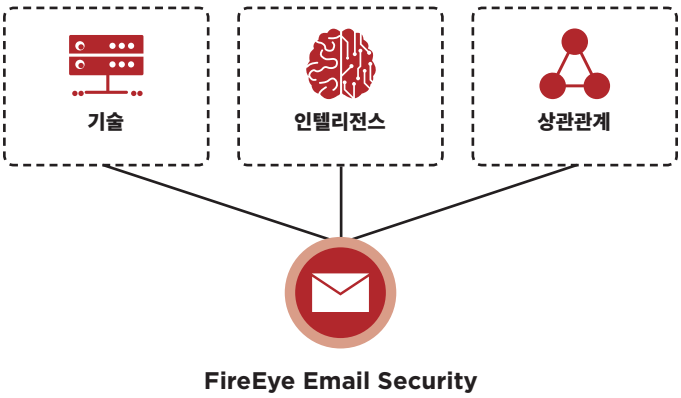

그림 1. 보안 이메일 게이트웨이.

ETP는 FireEye Network Security와 통합하여 보다 광범위한 가시성을 제공함으로써 다중 경로 및 혼합 공격을 실시간으로 방어합니다.

이메일 기반 위협에 대한 방어 시스템

온라인으로 개인 정보를 손쉽게 수집할 수 있기 때문에, 사이버 공격자는 사회 공학을 이용하여 거의 모든 사용자로 하여금 URL을 클릭하거나 첨부 파일을 열도록 유도할 수 있습니다.

Email Security는 기존의 이메일 보안 시스템을 회피하는 자격 증명 수집, 사칭 및 스피어 피싱 공격에 대한 실시간 탐지 및 방어를 제공합니다. 알 수 없는 지능적 위협이 다음에 숨겨진 경우 전자 메일을 분석하고 검역(차단됨):

- EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 및 ZIP/RAR/TNEF 아카이브를 비롯한 모든 첨부 파일 유형
- 암호로 보호되며 암호화된 첨부 파일
- 이메일, PDF 및 Microsoft Office 문서에 포함된 URL
- 인증 피싱 및 타이포스쿼팅 URL
- 알려지지 않은 OS, 브라우저 및 애플리케이션 취약점
- 스피어 피싱 이메일에 내장된 악성 코드

랜섬웨어 공격은 이메일로 시작되지만 데이터를 암호화하려면 명령 및 제어 서버로 콜백해야 합니다. Email Security는 이와 같은 다단계 악성코드 캠페인을 식별하고 저지합니다.

뛰어난 위협 탐지

Email Security는 정상 트래픽으로 위장된 고급, 대상 및 기타 회피 공격을 식별하고 격리함으로써 비용이 많이 드는 위반 위험을 완화하는 데 도움이 됩니다. 일단 탐지되면, 이러한 공격은 즉시 중지되고, 분석되고, 식별자를 찍어 미래의 위협을 더 빨리 식별하도록 활용됩니다.

Email Security의 핵심에는 고급 URL 방어, MVX 엔진 및 MalwareGuard가 있습니다. 이러한 기술은 기계 학습과 분석을 사용하여 전통적인 서명과 정책 기반 방어를 회피하는 공격을 식별합니다.

고급 URL Defense의 핵심인 PhishVision은 딥러닝을 사용하여 신뢰할 수 있고 일반적으로 타겟팅된 브랜드의 스크린샷을 전자 메일의 URL에서 참조하는 웹페이지 및 로그인 페이지와 컴파일하고 비교하는 이미지 분류 엔진입니다. Kraken은 PhishVision과 협력하여 도메인 및 페이지 콘텐츠 분석을 적용하여 기계 학습을 강화하는 피싱 탐지 플러그인입니다. URL 감지의 또 다른 발전인 Skyfeed는 특별히 제작된 완전히 자동화된 맬웨어 인텔리전스 수집 시스템입니다. 소셜 미디어 계정, 블로그, 포럼 및 위협 피드는 거짓 부정 행위를 발견하기 위해 수집됩니다. 고급 URL Defense의 다면적인 특성은 Email Security에 의해 보호받는 조직이 자격 증명 수집 및 스피어 피싱 공격으로부터 비할 데 없는 방어 수단을 제공합니다.

MVX 엔진은 안전한 가상 환경에서 동적 시그니처리스 분석 기능을 사용하여 제로데이, 다중 트래픽 및 기타 우회 공격을 탐지합니다. 또한 전에 관찰된 적이 없는 익스플로잇과 악성코드를 식별하여 사이버 공격 킬 체인의 감염 및 침해 단계를 저지합니다.

향상된 AVAS 보호

Email Security – Cloud Edition을 안티스팸 및 안티바이러스 보호 솔루션과 함께 사용하면 기존의 시그니처 매칭 수법을 이용하는 일반적인 수법을 탐지할 수 있습니다.

CEO 사기(비즈니스 이메일 침해라고도 함)와 같은 사칭 공격은 기업에 지속적으로 재정적 영향을 미치고 있습니다. 이는 공격에 악성코드를 사용하지 않고 사회 공학 기법만 사용하므로 부분적으로 악의적인 첨부파일이나 링크와 같은 전통적인 위협 지표가 부족하기 때문입니다. 이러한 공격에 맞서 싸우고 고객을 보호하기 위해 FireEye는 사칭 감지와 방어에 특화된 혁신적인 알고리즘, 시스템 및 도구를 개발했습니다.

이메일 공격의 일반적인 지표는 발신인 도메인의 경과 시간입니다. 사칭 캠페인을 만들 때, 사이버 범죄자들은 그들이 가장하고 있는 사람 또는 회사의 그것과 유사한 도메인으로부터 공격 이메일을 보내는데, 대개 그 도메인이 만들어진 지 몇 시간 안에 이루어집니다.

Email Security는 자체 개발한 새로운 기존 도메인(NED) 및 새로 발견된 도메인(NOD) 도구를 사용하여 도메인의 수명과 성숙도를 정확히 결정할 수 있습니다. 새로 생성하기로 결정한 도메인은 오포자 및 발신자 표시 또는 사용자 이름 스푸핑과 같은 다른 공격 지표가 있는지 의심하여 광범위하게 검사됩니다.

수신자의 도메인과 유사하거나 비슷하게 들리는 도메인을 구매하고 등록하는 과정을 거칠 필요 없이, 간단히 표시 이름/사용자 이름을 변경하기만 하면 되기 때문입니다. Email Security는 친근한 이름 식별을 활용하여 표시장치 이름 및 사용자 이름의 신뢰성을 결정함으로써 이 발송인의 스푸핑에 대해 방어합니다.

아웃바운드 검사

Email Security는 아웃바운드 이메일 메시지를 통해 전달되는 악성 첨부 파일과 피싱 URL을 비롯한, 알려지지 않은 지능형 위협을 탐지합니다. 발신 이메일 트래픽에서도 악성코드와 스팸을 검사하여 조직의 도메인이 블랙리스트에 등록되지 않도록 보호합니다.

통합으로 알림 처리 효율성 향상

Email Security는 모든 첨부 파일과 URL을 분석하여 오늘날의 지능형 공격을 정확하게 식별합니다. 알려진 위협 공격자에 대한 경보의 특성과 결합된 전체 FireEye 보안 에코시스템에서 제공하는 실시간 업데이트를 통해 중요한 경보의 우선순위를 정하고 그에 대한 조치를 취하며 스피어 피싱 이메일을 차단하는데 필요한 상황 정보를 제공합니다. 최소한의 노이즈와 오탐률로 알려진 위협, 알려지지 않은 위협, 악성코드를 기반으로 하지 않은 위협을 식별하므로 실제 공격에 리소스를 집중하여 운영 비용을 절감할 수 있습니다.

진화하는 위협 환경에 신속하게 적응

Email Security는 조직의 이메일 기반 위협에 대한 선제적 방어 시스템을 지속적으로 조정하도록 지원합니다. Email Security는 느려지는 타사 피드에 의존하지 않고 자체적인 위협 인텔리전스를 생성합니다. 사내 전자 메일별 위협 인텔리전스(또는 스마트 DNS), 데이터 수집 기능, 전자 메일 보안 전문가 및 위협 분석가가 강화된 안티스팸 기술 및 사칭 감지를 위한 기반 인프라를 제공합니다. 위협, 공격자, 시스템 및 피해자 심층 인텔리전스를 결합하여 다음을 수행합니다.

- 위협에 대한 보다 광범위한 가시성을 적시에 제공
- 탐지된 악성코드와 악성 첨부 파일의 역할 및 특징을 식별
- 우선 순위를 정해 신속하게 대응할 수 있도록 상황에 대한 통찰력 제공
- 공격자의 신원과 동기를 파악하고 조직 내에서 그들의 악성 활동 추적
- 스피어 피싱 공격을 소급 식별하고 악성 URL을 재작성하여 피싱 사이트 액세스 차단

조직들은 Email Security 포털에 접근하여 실시간 경보를 확인하고, 사용자 지정 규칙을 생성하며, 보고서를 생성할 수 있습니다. 스마트 사용자 지정 규칙을 통해 조직은 세분화된 여러 조건을 기반으로 정책 및 규칙을 만들 수 있습니다.

대응 워크플로우 통합

Email Security는 다른 여러 FireEye 솔루션과 함께 작동하면서 경보 대응 워크플로우를 자동화하는 데 도움을 줍니다.

FireEye Central Management는 Email Security 및 Network Security에서 생성되는 경보의 상관관계를 분석하여 공격을 거시적으로 파악한 후 공격의 확산을 방지하는 차단 규칙을 설정합니다.

FireEye Helix 플랫폼은 Email Security와 원활하게 작동하며 보안 작업을 간소화, 통합 및 자동화하도록 특별히 설계되었습니다.

손쉬운 설치 및 기업 간 보안

Email Security – Cloud Edition은 하드웨어 또는 소프트웨어를 설치할 필요가 없는 클라우드 기반 솔루션입니다. 따라서 이메일 인프라를 클라우드로 마이그레이션하는 조직에 적합합니다. 이렇게 이동시키면 물리적 인프라를 구매, 설치, 관리하는 복잡성이 제거됩니다.

Email Security – Cloud Edition은 Exchange Online Protection이 포함된 Microsoft Office 365 및 G Suite와 같은 클라우드 기반 이메일 시스템과 완벽하게 통합됩니다.

악성 및 사기 이메일을 방어하기 위해, 조직들은 단순히 메시지를 Email Security로 전송하기만 하면 됩니다. Email Security는 먼저 이메일에 스팸과 알려진 악성코드, 사칭 전술이 있는지 분석합니다. 그 다음에 시그니처리스 폭발실이라고 할 수 있는 MVX 엔진과 URL 방어 기술을 사용하여 모든 첨부 파일과 URL을 분석함으로써 실시간으로 위협을 탐지하고 지능형 공격을 저지합니다.

추가 기능

맞춤화할 수 있는 YARA 기반의 룰

Email Security는 분석가가 맞춤형 YARA 규칙을 사용하여 탐지를 관리 및 개선하고, 최신 위협을 저지하며, 지속적인 캠페인을 파악하도록 지원합니다.

능동적 방어 모드 또는 모니터 전용 모드

Email Security는 능동적인 방어를 위해 이메일을 분석하고 위협을 격리할 수 있습니다. 조직들은 MX 레코드를 업데이트하기만 하면 메시지를 FireEye로 전송할 수 있습니다. 모니터 전용으로 설치하는 경우, 조직들은 BCC 룰을 명확하게 설정하기만 하면 이메일의 사본들을 FireEye로 보내어 MVX 분석을 할 수 있습니다.

규정 준수 인증

ISO 27001

Email Security - Cloud Edition은 데이터 센터를 안전하게 관리하는 ISO 27001 정보 보안 표준을 준수합니다.

FedRAMP

Email Security – Cloud Edition은 정부 및 공공 교육 기관에서 운영하는 클라우드 서비스에 대한 FedRAMP 보안 요건을 준수합니다.

SOC 2 Type 2

Email Security – Cloud Edition은 American Institute of Certified Public Accountants(AICPA) Service Organization Controls(SOC 2) Type 2 보안 및 비밀 유지 인증에 부합합니다.

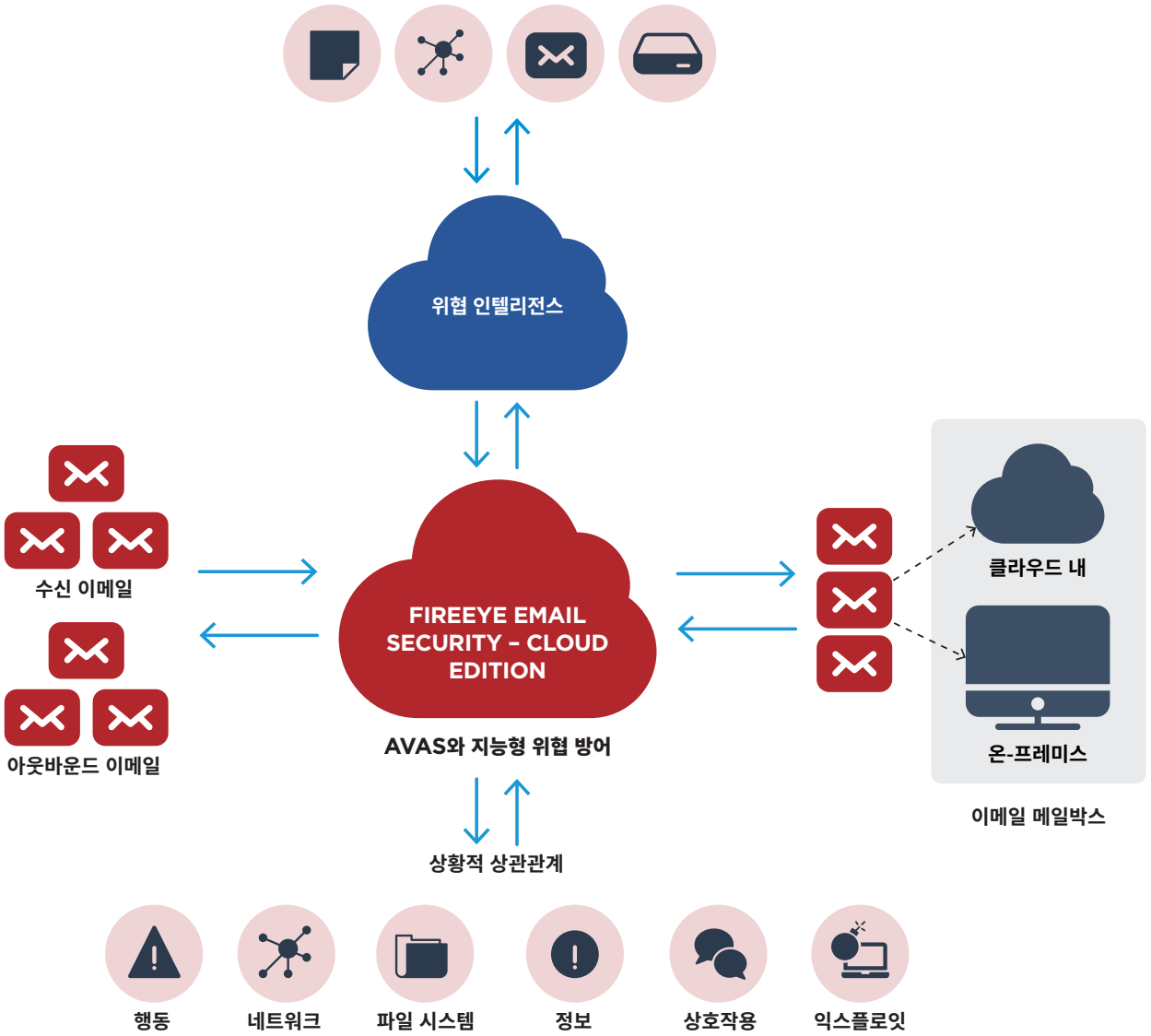

그림 2. FireEye Email Security – Cloud Edition.

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.