FireEye
SECURITY REIMAGINED

이메일 위협 방어(ETP) 클라우드

이메일 공격을 식별, 분석 및 차단하는 클라우드 기반의 플랫폼

데 이 터 시 트

주요 기능

- 안티스팸, 안티바이러스 뿐 아니라 지능형 (APT) 공격을 방어하는 완벽한 이메일 보안 솔루션
- 하드웨어 또는 소프트웨어가 필요 없는 클라우드 기반 솔루션
- 검증된 경보와 상황에 맞는 인텔리전스 제공
- 통합된 보안으로 운영 효율성 증가
- FireEye 네트워크 포함(NX) 플랫폼과 통합하여 다중 위협 경로에 대한 혼합 공격을 차단
- 제로데이 익스플로잇, ZIP/RAR/TNEF 아카이브에 숨겨진 공격, 악성 URL 같은 위협 이메일 분석
- EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX,PPT/PPTX, JPG, PNG, MP3, MP4를 포함하는 모든 파일 첨부 종류에 대해 정확한 파일 분석 제공
- 메일 익스체인저 (MX)에서의 능동적 방어 모드, 또는 모니터 모드(BCC 이용)로 설치 가능
- 능동적 방어 모드에서 사용자 통지 옵션을 사용하여 악성 이메일 격리
- 보안 및 비밀 유지를 위한 SOC 2 Type II 인증 특성을 제공

요약

조직들은 이메일 기반의 스팸, 바이러스 및 지능형 위협의 숫자가 계속 증가하는 위험에 직면해 있습니다. 이메일 기반의 공격, 특히 스피어 피싱은 탐지와 관련된 복잡성 때문에 지능형 지속적 위협(APT) 공격을 시작하기 위해 사용하는 주요 방법 중 하나로 남아 있습니다.

FireEye® 이메일 위협 방어(ETP) 클라우드는 오늘날의 지능형 이메일 공격을 방어하고 안티스팸, 안티바이러스 기능을 제공하는 클라우드 솔루션입니다. 이 솔루션은 클라우드 방식 메일함에 대해서도 완벽한 이메일 보안을 제공합니다.

악성 이메일을 방어하기 위해, 조직들은 단순히 메시지를 ETP 클라우드로 전송하기만 하면 됩니다. ETP 클라우드는 먼저 이메일에 스팸과 알려진 바이러스가 있는지 분석합니다. 그 다음에 행위기반의 FireEye 다중 경로 가상 실행™ (MVX) 엔진을 사용하여 모든 첨부 파일과 URL을 분석한 후에 실시간으로 위협을 탐지하고 APT 공격을 저지합니다.

손쉬운 설치 및 기업 간 보안

하드웨어나 소프트웨어를 설치할 필요가 없는 ETP 클라우드는 인프라를 클라우드로 이동시키려고 하는 조직들에게 적합합니다. 이렇게 이동시키면 물리적 인프라를 구매, 설치, 관리하는 복잡성이 제거됩니다.

지능형 위협 인텔리전스(ATI)를 사용하는 이메일 위협 방어 (ETP) 클라우드는 설치된 전체 FireEye 시스템에서 작동하여 실시간 위협 인텔리전스를 공유합니다. 이 클라우드는 풍부한 상황 인텔리전스를 상호 연결시켜 아래와 같은 역할을 수행합니다.

- 탐지된 악성코드와 악성 첨부 파일의 역할 및 특징을 식별
- 공격자의 신원과 동기를 파악하여 시스템 내에서 악성 활동을 추적
- 스피어 피싱 이메일의 이전 표적 식별
- 표적의 인박스에 들어 있는 악성 이메일 사본의 위치 확인
- 메시지가 새로운 표적으로 전송되었는지 확인
- 메시지를 배달한 후에 악성이 되는 URL에 강조 표시

운영 효율성

ETP 클라우드는 기존의 보안을 통합하여 지출 최적화, 오탐 감소, 운영 효율성을 증대시키는 지능형 위협 방어 솔루션 입니다.

클라우드 내에서 다중 경로 가상 실행

ETP 클라우드는 MVX를 사용하여 운영체제와 어플리케이션(다수의 웹 브라우저 및 어도비 리더와 플래시 같은 플러그인 포함)에서 모두 첨부 파일을 실행합니다. 온프레미스 FireEye 이메일

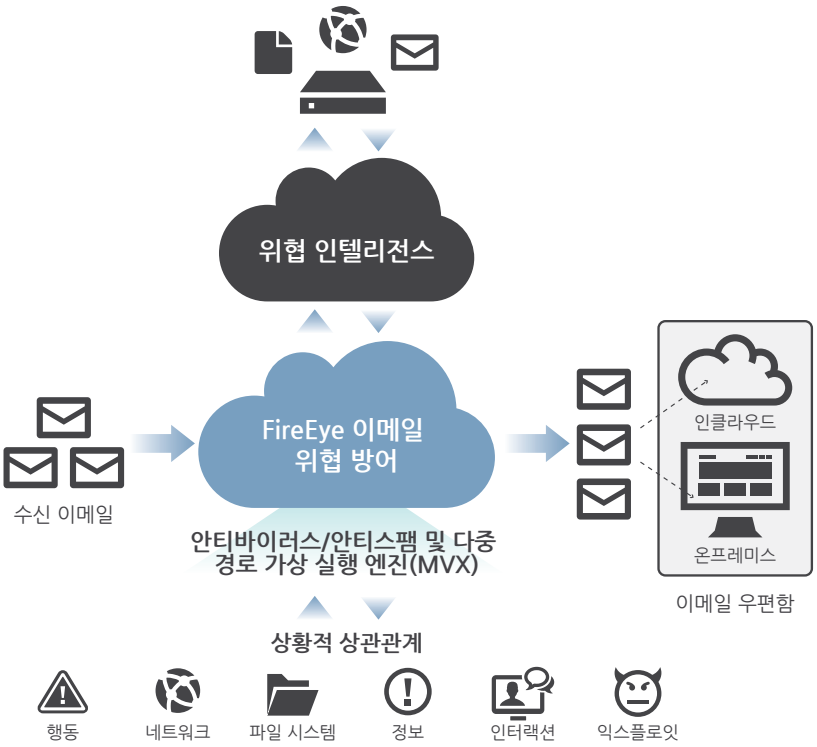
보안(EX 시리즈)과 함께 사용하는 MVX 엔진은 시그니처를 사용하지 않으므로, 알려지지 않은 OS, 브라우저, 애플리케이션 취약점, 그리고 파일과 멀티미디어 콘텐츠에 내장된 악성코드를 악용하는 지능형 공격을 저지할 수 있습니다.

악성 이메일의 실시간 격리
ETP 클라우드는 MVX 엔진을 사용하여 스피어 피싱 이메일을 차단하고 모든 첨부 파일을 분석함으로써 오늘날의 지능형 공격을 정확하게 식별합니다. 공격이 확인되는 경우, ETP 클라우드는 악성 이메일을 격리시켜 추가 분석을 하거나 관리자가 삭제합니다.

사용하기 쉬운 관리 포털
조직들은 ETP 포털에 접근하여 실시간 경보를 확인하고 보고서를 생성할 수 있습니다.

이메일 및 웹 위협 경로에 대한 보안
어떤 공격들은 악성코드가 내장된 첨부 파일을 사용하지만, 또한 사이버 공격자들은 악성 링크를 흔히 사용하여, 오늘날의 기존 방어 사일로를 우회하기를 희망하면서 공격 전술을 혼합합니다. ETP 클라우드는 온프레미스 FireEye NX 플랫폼과 통합하여 다중 경로 및 혼합 공격을 실시간으로 방어합니다.

능동적 방어 모드 또는 모니터 전용 모드로 설치할 수 있습니다
ETP 클라우드는 능동적 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.



더 자세히 알아보십시오

FireEye는 종합적인 서비스 포트폴리오를 제공합니다. 전체적인 세부 내용을 원하시면 Korea.info@FireEye.com 또는 +82-2-2092-6580 으로 연락해 주십시오.

FireEye Korea | 서울 특별시 강남구 테헤란로 534 글라스타워 20층 | 02.2092.6580 | korea.info@fireeye.com | www.fireeye.kr

© 2016 FireEye, Inc. 저작권 소유. FireEye는 FireEye, Inc의 등록상표입니다.
다른 모든 브랜드, 제품 또는 서비스 명칭은 각 소유자의 상표 또는 서비스 마크입니다.
DS.ETPC.KO-KR.102015