FireEye™

데이터시트

AX 시리즈

사이버 공격에 대한 종합적인 정보를 제공하는 포렌식 분석 플랫폼

주요 기능

- FireEye MVX 엔진을 사용하여 전체 공격 라이프사이클에 대해 심층적인 포렌식 분석을 수행
- 의심스러운 웹 코드, 실행 파일, 일반 파일에 대한 분석을 능률화하고 일괄 처리
- 시스템 수준의 OS와 애플리케이션 변경에 대한 심층 보고서를 제공
- 제로데이 익스플로잇을 확인하기 위해 라이브 모드 또는 샌드박스 분석을 제공
- FireEye CM 플랫폼과 통합을 통해서 즉각적인 로컬 보호를 위한 위협 인텔리전스를 동적으로 생성
- 악성 URL 세션과 코드 실행에 대한 분석을 가능하게 하는 패킷 캡쳐
- 사고 대응의 우선 순위 결정을 능률화하기 위해 FireEye AV 제품군을 포함

FireEye® AX 시리즈는 보안 분석가들에게 웹페이지, 이메일 첨부 파일, 일반 파일에 내장된 지능형 악성코드, 제로데이 및 지능형 지속적 위협(APT) 공격을 안전하게 실행하고 검사할 수 있는 강력한 자동 설정 테스트 환경에 대한 실제적인 통제권을 제공하는 포렌식 분석 플랫폼입니다.

사이버 범죄자들은 특정한 기업, 사용자 계정 또는 시스템에 침투하기 위해 공격을 맞춤화하므로, 분석가들에게는 표적 악성 활동에 신속하게 대처하기 위해 사용이 용이한 포렌식 툴이 필요합니다.

OS, 브라우저, 애플리케이션에 대한 공격을 평가

FireEye AX 시리즈는 FireEye Multi-Vector Virtual Execution™ (다중 벡터 가상 실행, MVX) 엔진을 활용하여 최초 익스플로잇에서 콜백 목적지와 후속 바이너리 다운로드 시도에 이르기까지 공격에 대한 전체적이고 종합적인 정보를 제공합니다. FireEye MVX 엔진은 사전 설정되고 기능화된 Windows 가상 분석 환경을 통해서 의심스러운 악성코드를 전체적으로 실행하여 일반적으로 사용하는 웹 객체, 이메일 첨부 파일, 일반 파일에 대한 심층 검사를 수행합니다. FireEye AX 플랫폼은 FireEye MVX 엔진을 사용하여 단일 파일 또는 배치 파일에 악성코드가 있는지 검사하고 다중 프로토콜에 대한 아웃바운드 연결 시도를 추적합니다.

관리가 아닌 분석에 시간을 사용

FireEye AX 시리즈는 관리자가 설정, 베이스라이닝(기본 백업), 그리고 수동 악성코드 분석에 사용되는 가상 머신 환경을 복구하는 시간을 덜어줍니다. 내장된 맞춤화와 페이로드 작동에 대한 튜닝을 제공하는 FireEye AX 시리즈를 사용하면 포렌식 분석가가 악성코드 공격을 종합적으로 이해하여 기업의 방어 요구를 충족시킬 수 있습니다.

AX 5400과 AX 8400

"FireEye 솔루션의 한 가지 큰 매력은 가상 실행 환경에서 분석을 수행하여 의심스러운 코드가 실제로 위협인지 판단할 수 있는 것입니다. 가상 실행을 통해서 생성된 상세한 정보를 활용하면 문제를 해결하는 데 가장 적합한 옵션을 선택할 수 있습니다. 따라서 공격에 대응하는 방법을 정확하게 알 수 있습니다."

— 사이버 보안 디렉터, 에너지 부문

라이브 분석 모드 또는 샌드박스 모드를 선택

FireEye AX 시리즈는 사용자에게 라이브 모드와 샌드박스 모드의 2가지 분석 모드를 제공하는 능력이 있습니다. 악성코드 분석가들은 네트워크 상의 라이브 모드를 사용하여 전체 악성코드 라이프사이클을 분석하고, 외부에 대한 연결을 허용합니다. 따라서 FireEye AX 시리즈는 다양한 다단계 벡터를 통해서 지능형 공격을 추적하는 능력을 제공합니다. 샌드박스 모드에서는 가상 환경에서 특정한 악성코드 샘플의 실행 경로가 완전히 파악되는 것을 볼 수 있습니다.

이 두 모드에서, 사용자는 FireEye CM 플랫폼을 통해서 다른 FireEye 제품들과 공유할 수 있는 동적 및 익명화된 공격 프로파일을 생성할 수 있습니다. FireEye AX 플랫폼이 생성하는 악성코드 공격 프로파일에는 악성코드, 익스플로잇 URL, 그리고 감염 및 공격을 유발하는 다른 출처가 포함됩니다. 또한 악성코드 통신 프로토콜의 특성을 공유하는 FireEye Dynamic Threat Intelligence™ (동적 위협 인텔리전스, DTI) 엔터프라이즈를 통해서 조직에 설치된 전체 FireEye 시스템에 대한 데이터 유출 시도를 동적으로 차단합니다.

맞춤화할 수 있는 YARA 기반의 룰

FireEye AX 시리즈는 맞춤화된 YARA 룰을 전송하는 것을 지원하여 바이트 수준의 룰을 지정하고, 조직에 특정한 위협들에 대한 의심스러운 객체를 신속하게 분석합니다.

글로벌 악성코드 방어 네트워크

FireEye AX 시리즈는 전체 FireEye 위협 방어 포트폴리오와 쉽게 통합할 수 있도록 설계되었습니다. FireEye AX 시리즈는 악성코드 포렌식 데이터를 FireEye CM을 통해서 다른 FireEye 플랫폼과 공유하고, 아웃바운드 데이터 유출을 차단하고, 알려진 인바운드 공격을 방지할 수 있습니다. 또한 FireEye AX 시리즈의 위협 데이터는 FireEye DTI 클라우드를 통해서 공유하여 새로 출현하는 공격을 방어할 수 있습니다.

FireEye AX 시리즈는 휴리스틱을 튜닝할 필요가 없는 사전 설정된 MVX 엔진을 사용하여 관리자의 설정 시간을 절약하고 설정과 관련된 문제를 해결합니다. 또한, FireEye AX 시리즈는 위협 연구자가 네트워크와 보안을 관리하는 경비를 증가시키지 않고 지능형 표적 공격을 분석하는 데 도움을 줍니다.

기술 사양

	AX 5400	AX 8400
폼 팩터	1U 랙 마운트	2U 랙 마운트
무게	30lbs (13.6Kg)	50lbs (22.7Kg)
크기(WxDxH)	17.2" x 25.6" x 1.7" (43.7 x 65.0 x 4.3cm)	17.2" x 27.9" x 3.5" (43.7 x 70.9 x 8.9cm)
엔클로저	19인치 랙에 맞음	19인치 랙에 맞음
관리 포트	(2) 10/100/1000 BASE-T 포트	(2) 10/100/1000 BASE-T 포트
성능	최대 8,200건/일 분석	최대 16,000건/일 분석
AC 입력 전압	자동 전환 100 ~ 240VAC 전범위	자동 전환 100 ~ 240VAC 전범위
AC 입력 전류	8.5-6.0A	9.5-7.2A
전원 공급 장치/RAID	이중화 700W / 2 SAS HDD (HW RAID1 내)	이중화 1400W / 2 SAS HDD (HW RAID1 내)
전력 소비(최대)	1484BTU/시간	1586BTU/시간
주파수	50-60Hz	50-60Hz
작동 온도	10° C에서 35° C	10° C에서 35° C

주: 성능 수치는 FireEye AX 플랫폼을 사용할 때의 기본 분석 횟수에 근거하나, 시스템 설정과 처리 중인 트래픽 프로파일에 따라 달라집니다.

FireEye Korea I 서울특별시 강남구 테헤란로 440, 포스코센터 빌딩 서관 11층 I 02-559-0730 I korea.info@FireEye.com I www.FireEye.com