FireEye
SECURITY REIMAGINED

FX 시리즈

파일 공유와 컨텐츠 저장소에 상주하는 악성코드를 탐지 및 제거하기 위한 컨텐츠 위협 방어 플랫폼

데 이 터 시 트

SECURITY REIMAGINED

주요 기능

- 기존의 AV 엔진이 탐지하지 못하는 잠복 악성코드를 발견
- 격리(보호 모드) 또는 분석 전용(모니터 모드)으로 설치
- CIFS 및 NFS와 호환성이 있는 파일 공유에 대해 반복적이고 예정된 온디맨드 스캔을 제공
- WebDAV 프로토콜을 활용하여 선제적인 Sharepoint 보호를 제공
- PDF, 마이크로소프트 오피스 문서, 멀티미디어 파일과 같은 광범위한 파일 형태에 대한 분석을 포함
- FireEye AV 제품군과 통합하여 사고 대응의 우선 순위 결정 및 명명 규칙 능률화
- FireEye CM과 FireEye DTI를 통해서 FireEye 플랫폼과 위협 데이터를 공유

FX 5400과 FX 8400

요약

FireEye® FX 시리즈는 광범위한 파일 형태에서 발생하는 공격으로부터 컨텐츠를 보호하는 위협 방어 플랫폼 그룹입니다. 웹 메일, 온라인 파일 전송 툴, 클라우드, 이동식 파일 저장 장치는 파일 공유와 컨텐츠 리포지터리로 확산되는 악성코드를 초래할 수 있습니다. FireEye FX 플랫폼은 네트워크 파일 공유와 기업 컨텐츠 관리 저장소를 분석하여 직원과 다른 사람들이 불러들인 차세대 방화벽, IPS, AV, 게이트웨이를 우회하는 악성코드를 탐지하고 격리시킵니다.

파일 공유에 상주하는 악성코드에 대한 문제

오늘날의 지능형 사이버 공격은 정교한 악성코드와 지능형 지속적 위협(APT) 기법을 사용하여 방어 시스템에 침투하고 파일 공유를 통해서 내부로 확산됩니다. 따라서 악성코드는 네트워크에 장기적인 거점을 구축하고 다수의 시스템(오프라인 시스템 포함)을 감염시킬 수 있습니다. 많은 기업 데이터 센터는 특히 지능형, 컨텐츠 기반의 악성코드에 취약하며, 그 이유는 기존의 방어 시스템이 종종 합법적인 수단을 통해서 네트워크로 침입하는 이러한 공격을 방어하는 데 비효과적이기 때문입니다. 사이버 범죄자들은 이러한 취약점을 악용하여 악성코드를 네트워크 파일 공유로 확산시키고 악성코드를 방대한 데이터 저장소에 내장하여, 시스템을 복구한 후에도 위협이 지속됩니다.

지능형 공격 라이프사이클을 중단시키는 데 중요한 컨텐츠 보호

컨텐츠에 잠복해 있는 악성코드를 탐지할 방법이 없으면, 이러한 APT는 네트워크 자산을 악용하여 독점 정보를 추출하고 중대한 피해를 입힐 수 있습니다. FireEye FX 시리즈는 특허를 받은 FireEye Multi-Vector Virtual ExecutionTM (다중 벡터 가상 실행, MVX) 엔진을 사용하여 파일 공유와 기업 컨텐츠 리포지터리를 분석하며, 이 엔진은 일반적으로 사용하는 파일 형식(PDF, MS Office, vCards, ZIP/RAR/TNEF 등)과 멀티미디어 컨텐츠(QuickTime, MP3, Real Player, JPG, PNG 등)에 내장된 제로데이 악성코드를 탐지합니다. FireEye FX 시리즈는 접근 가능한 네트워크 파일 공유에 대해 반복적이고 예정된 온디맨드 스캔을 수행하여, 상주하는 악성코드를 식별하고 격리시킵니다. 이 플랫폼은 지능형 공격 라이프사이클의 주요 단계를 중단시킵니다.

알려지지 않은 제로데이 위협을 탐지하는 FireEye MVX

FX 시리즈는 특별한 목적으로 설계된 FireEye MVX 엔진을 사용하여 각 파일을 검사하고, 제로데이 익스플로잇이나 악성코드가 존재하는지 확인합니다. FireEye MVX 엔진은 광범위한 브라우저, 플러그인, 애플리케이션, 운영체제에 대해 작동시켜 악성 활동을 탐지합니다.

선제적인 SharePoint 컨텐츠 스캔과 격리

FireEye FX 시리즈는 컨텐츠를 지속적으로 스캔하여 Sharepoint 리포지터리에서 발견된 악성코드에 대해 경보를 발하고 영구적으로 격리시킵니다. 이 플랫폼은 WebDAV 프로토콜을 활용하여, Sharepoint 리포지터리를 사용하는 기업 비즈니스 워크플로우를 보호하기 위한 Sharepoint 서비스와 안전하게 통합합니다.

맞춤화할 수 있는 YARA 기반의 룰

FireEye FX 시리즈는 맞춤화된 YARA 룰을 지원하여 조직에 특정한 대량의 파일에 대한 위협을 분석합니다.

사고에 대한 우선 순위 결정을 능률화

안티바이러스 벤더들이 FireEye FX 플랫폼이 중단시킨 악성코드를 탐지할 수 있는지 확인하기 위해 FireEye AV 제품군을 사용하여 각 악성 객체를 분석합니다. 따라서 조직들은 사고 대응 후속 조치의 우선 순위를 효과적으로 결정하고, 알려진 악성코드에 대해 일반적으로 사용하는 명명 규칙을 활용할 수 있습니다.

악성코드 인텔리전스 공유

분석 결과에 따라 동적으로 생성하는 실시간 위협 인텔리전스는 모든 FireEye 제품이 FireEye CM 플랫폼과의 통합을 통해서 로컬 네트워크를 보호하는 데 도움이 될 수 있습니다. 이 인텔리전스는 동적 위협 인텔리전스™ (DTI) 클라우드를 통해서 전세계에서 공유하여 모든 가입자에게 새로 출현한 위협에 대해 통지할 수 있습니다.

룰에 대한 튜닝이 필요 없고 0에 가까운 오탐률

FX 시리즈는 60분 이내에 설치되고 튜닝이 절대로 필요 없는 관리가 용이한 클라이언트리스 플랫폼 그룹입니다. 유연한 설치 모드에는 분석 전용 모니터와 활성 격리가 포함됩니다. 따라서 기업들이 얼마나 많은 악성코드가 파일 공유에 상주하는지 알아보고, 악성코드의 내부 확산을 적극적으로 중단시킬 수 있습니다.

기술 사양

	FX 5400	FX 8400
성능 *	최대 80,000건/일의 파일	최대 160,000건/일의 파일
네트워크 인터페이스 포트	2x10/100/1000BASE-T 포트	2x10/100/1000BASE-T 포트
IPMI 포트(후면 패널)	포함	포함
전면 패널 LCD 및 키패드	포함	포함
PS/2 키보드 및 마우스, DB15 VGA 포트(후면 패널)	포함	포함
USB 포트(후면 패널)	2x타입 A USB 포트	2x타입 A USB 포트
시리얼 포트(후면 패널)	115,200bps, 패리티 없음, 8 비트, 1 정지 비트	115,200bps, 패리티 없음, 8 비트, 1 정지 비트
저장 능력	2x600GB HDD, RAID 1, 2.5인치, FRU	2x600GB HDD, RAID 1, 2.5인치, FRU
엔클로저	1RU, 19인치 랙에 맞음	2RU, 19인치 랙에 맞음
섀시 크기 (WxDxH)	17.2"x27.8"x1.70"(437x706x43.2mm)	17.2"x28.0"x3.41"(437x711x86.6mm)
AC 전원	중복 (1+1) 750와트, 100~240 VAC 9 - 4.5A, 50~60Hz, IEC60320-C14 인렛, FRU	중복 (1+1) 750와트, 100~240 VAC 9 - 4.5A, 50~60Hz, IEC60320-C14 인렛, FRU
DC 전원	해당없음	해당없음
최대 전력 소비(와트)	463와트	506와트
최대 열 방산(BTU/h)	1580BTU/h	1726BTU/h
MTBF(h)	40,700h	68,900h
어플라이언스만/발송 중량(lb.) (kg)	32lb. (15kg)/47lb. (21kg)	42lb. (19kg)/58lb. (26kg)
안전 인증	IEC 60950, EN 60950, CSA 60950-00, CE 마킹	IEC 60950, EN 60950, CSA 60950-00, CE 마킹
EMC/EMI 인증	FCC (파트 15 클래스-A), CE (클래스-A), CNS, AS/NZS, VCCI(클래스 A)	FCC (파트 15 클래스-A), CE (클래스-A), CNS, AS/NZS, VCCI(클래스 A)
보안 인증	CC NDPP v1.1	CC NDPP v1.1
규제 준수	RoHS, REACH, WEEE	RoHS, REACH, WEEE
작동 온도	10°C~35°C	10°C~35°C
작동 상대 습도	10%~85% (비응축)	10%~85% (비응축)
작동 고도	5,000ft	5,000ft

주: 모든 성능 수치는 시스템 설정과 처리 중인 트래픽 프로파일에 따라 달라집니다. 성능 수치는 일반적인 기업 환경에서 관찰된 파일들에 근거합니다.

더 자세히 알아보십시오

FireEye는 종합적인 서비스 포트폴리오를 제공합니다. 전체적인 세부 내용을 원하시면 services@FireEye.com 또는 +1 855.692.2052로 저희에게 연락해 주십시오.

Accumuli Security로 연락하시려면 info@accumuli.com으로 이메일을 보내거나 +44 (0) 1256 303 700으로 전화하십시오.

왜 FIREEYE를 선택해야 합니까?

전문성. 기술. 인텔리전스.

FireEye는 보안 업계에서 가장 뛰어난 전문성, 기술, 그리고 방어 대상이 명확하고 방어와 관련성이 있는 인텔리전스를 결합하여 위협을 차단합니다. FireEye 보안 전문가들은 각 고객과 제휴하여 구체적인 보안 문제점을 파악 및 해결하고, 이 분야의 최고 전문가가 신속한 대응을 제공합니다. FireEye 위협 방어 플랫폼은 FireEye에 수많은 지능형 지속적 위협, 표적 공격, 사이버 범죄에 대한 독특한 통찰력을 제공하고, FireEye는 이 플랫폼을 통해서 각 산업에 속한 고객들에게 동적 위협 인텔리전스를 제공합니다. FireEye는 조직들에게 오늘날의 위협으로부터 비즈니스를 방어하기 위해 필요한 전문성과 인텔리전스를 제공합니다.

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