



CM 시리즈

동적 위협 인텔리전스의 실시간 공유와 기업에
설치된 시스템의 통합 관리

SECURITY
REIMAGINED

주요 기능

- 설치된 다수의 플랫폼에 대해 통합된 제어를 제공
- 다중 벡터 상관 관계를 통해서 혼합된 위협 방어를 활성화
- 60분 이내에 설치할 수 있는 특정한 목격의 플랫폼 제공
- 지능형 표적 공격 방어 상태를 제공하는 한 눈에 볼 수 있는 보안 대시보드를 표시
- 통합 보안 이벤트 저장소를 통해서 보고와 감사를 가속화
- 다수의 FireEye 플랫폼의 관리를 능률화하고, 설정, 위협 업데이트, 소프트웨어 업그레이드 관리에 소비하는 시간을 절약

FireEye® CM 시리즈는 FireEye NX, EX, FX, AX에 대한 관리, 보고 및 데이터 공유를 설치하기 쉬운 네트워크 기반의 플랫폼으로 통합하는 관리 플랫폼입니다.

FireEye CM은 설치된 FireEye 시스템 내에서 자동으로 생성되는 위협인텔리전스를 실시간으로 공유하여 조직을 목표로 하는 지능형 표적 공격을 식별 및 차단할 수 있습니다. 또한 FireEye 플랫폼들에 대한 설정, 관리 및 보고를 중앙집중화할 수 있습니다.

로컬 위협 인텔리전스의 실시간 공유

FireEye 플랫폼은 FireEye Multi-Vector Virtual Execution(다중 벡터 가상실행)™ 엔진을 사용하여 위협 인텔리전스를 실시간으로 생성합니다. FireEye CM은 설치된 전체 FireEye 시스템에 위협 인텔리전스를 배포하여, 각 플랫폼이 진행 중인 지능형 공격에 대해 동일한 동적 방어를 수행하고 있는지 확인합니다. 또한, FireEye Dynamic Threat Intelligence™(동적 위협 인텔리전스, DTI) 클라우드 가입자들은 FireEye CM을 사용하여 전세계의 고객, 기술 파트너, 서비스제공자 내부에 설치된 FireEye 플랫폼에 대해 익명화된 위협 인텔리전스를 송신 및 수신하는 것을 중앙 집중화할 수 있습니다.

한 눈에 볼 수 있는 보안 대시보드와 드릴다운

FireEye CM은 통합된 보안 대시보드를 사용하여 다양한 방어 활동들을 수행하고 상황에 대한 인식을 개선합니다. 대시보드는 관리자에게 감염된 시스템의 숫자를 확인하고 감염 세부사항을 직접 드릴다운하여 다음 단계를 결정하는 실시간 뷰를 제공합니다.

지능형 표적 공격에 대한 통합 분석

FireEye NX, EX, FX, AX 시리즈를 FireEye CM 시리즈와 함께 설치함으로써, 악성 URL을 배포하기 위해 사용하는 스팍어 피싱 이메일을 정확하게 찾아내는 것과 같은 혼합된 위협에 대한 분석이 가능해졌습니다. 보안 분석가들은 이제 산재된 혼합 공격을 통합 분석하는 능력을 갖추어, 지능형 표적 공격으로부터 조직을 방어하기 위해 필요하고 사용 가능한 인텔리전스를 제공합니다.

엔터프라이즈 등급의 콘솔과 경보

FireEye CM 시리즈는 이벤트를 확인, 검색, 필터링할 수 있고, SMTP, SNMP, syslog 또는 HTTP POST를 통해서 실시간으로 경보 통지를 전송할 수 있는 웹 GUI 콘솔을 제공합니다. 관리자는 이벤트, 날짜 또는 IP 범위별로 필터링할 수 있고, 관리자의 IT 운영 역할에 따라 정해진 데이터에 대해서만 결과를 표시합니다. 또한 통지는 다른 회사의 SIEM 툴로 전송할 수도 있습니다. 그리고 관리자는 이벤트 링크를 클릭하여 특정한 FireEye 플랫폼에 접속하여 해당 장비의 이벤트를 확인 할 수 있습니다.



CM 4400과 CM 9400
(CM 7400은 사진이 없음)

중앙 설정 및 플랫폼 업그레이드

FireEye CM 시리즈는 기업에 효율적으로 설치하기 위한 동적 설정 기능이 있습니다. 설정은 중앙에서 결정한 후에 그 결정에 따라 조직에 배포할 수 있습니다. 관리자는 단일 또는 다수의 플랫폼을 원격으로 설정하고 세부 사항을 볼 수 있습니다. 또한, 모든 업그레이드는 모든 관리 플랫폼에 동시에 배포하여, 모든 제품이 최신의 보안 능력을 갖출 수 있습니다.

통합 저장소와 상세 보고

체계화된 대규모의 조직들은 FireEye CM 시리즈의 중앙

보안데이터를 효과적으로 저장하여 능률적이고 통합된 보고를 할 수 있습니다. FireEye CM 시리즈는 감사와 관련된 보안이벤트를 수집 및 저장하는 수단을 제공하여 장기적인 데이터 유지 요건을 충족시킵니다.

FireEye CM 시리즈는 특정한 종류의 위협을 이름 또는 종류에 의해 검색하고 보고하는 편리한 방법을 제공합니다. 또한 조직들은 가장 많이 감염된 호스트, 악성코드, 콜백 이벤트 (지리적 위치에 대한 세부 사항 포함)에 대한 요약을 볼 수 있습니다. 그리고 추세 뷰는 침해된 시스템의 숫자가 감소하는 진척도를 보여줄 수 있습니다.

기술 사양

	CM 4400	CM 7400	CM 9400
품 팩터	1U 랙 마운트	2U 랙 마운트	2U 랙 마운트
무게	30lbs (13.6Kg)	50lbs (22.7Kg)	50lbs (22.7Kg)
크기(WxDxH)	17.2" x 25.6" x 1.7" (43.7 x 65.0 x 4.3cm)	17.2" x 25.6" x 3.4" (43.7 x 65.0 x 8.9cm)	17.2" x 25.6" x 3.4" (43.7 x 65.0 x 8.9cm)
엔클로저	19인치 랙에 맞음	19인치 랙에 맞음	19인치 랙에 맞음
관리 포트	(2) 10/100/1000 BASE-T 포트	(2) 10/100/1000 BASE-T 포트	(2) 10/100/1000 BASE-T 포트
AC 입력 전압	자동 전환 100 ~ 240VAC 전범위	자동 전환 100 ~ 240VAC 전범위	자동 전환 100 ~ 240VAC 전범위
AC 입력 전류	8.5-6.0A	8.5-6.0A	8.5-6.0A
전원 공급 장치/RAID	이중화 700W / 4 SAS HDD (HW RAID10 내)	이중화 700W / 4 SAS HDD (HW RAID10 내)	이중화 700W / 4 SAS HDD (HW RAID10 내)
전력 소비(최대)	1057BTU/시간	1143BTU/시간	1876BTU/시간
주파수	50-60Hz	50-60Hz	50-60Hz
작동 온도	10° C에서 35° C	10° C에서 35° C	10° C에서 35° C

주: 모든 성능 수치는 시스템 설정과 처리 중인 트래픽 프로파일에 따라 달라집니다.