데이터 시트

# FireEye Central Management

## 장비와 인텔리전스 관리를 중앙 집중화하여 공격 경로 간 데이터 상호 연결

### 요약

- 여러 플랫폼 설치를 통합 제어하는 기능 제공
- 다중 경로 상관관계를 통해 혼합 위협 방어 지원
- 60 분 이내에 설치 가능한 특별히 개발된 플랫폼 제공
- 지능형 표적 공격 보호 상태를 한눈에 보여주는 보안 대시보드 표시
- 통합 보안 이벤트 저장소를 통해 보고 및 감사 기간 단축
- 여러 FireEye 솔루션의 관리 능률화 및 구성 , 위협 업데이트 및 소프트웨어 업그레이드를 관리하는데 소요되는 시간 단축

그림 1. CM 4500 및 CM 9500(CM 7500은 사진이 없음)

**개요**

FireEye® Central Management(CM 시리즈 ) 는 FireEye 제품의 관리 , 보고 및 데이터 공유 기능을 설치가 간편한 하나의 네트워크 기반 솔루션으로 통합한 관리 플랫폼 그룹입니다 . Central Management 는 자동으로 생성된 위협 인텔리전스를 실시간으로 공유하여 표적화 지능형 공격을 식별하고 차단합니다 . 또한 FireEye 솔루션에 대한 중앙 집중식 구성 , 관리 및 보고를 지원합니다 .

**로컬 위협 인텔리전스의 실시간 공유**

FireEye 솔루션은 FireEye Multi-Vector Virtual Execution™(MVX) 엔진을 사용하여 실시간 위협 인텔리전스를 생성합니다 . Central Management 는 시스템 전체의 여러 FireEye 설치에 위협 인텔리전스를 배포하여 각 솔루션에서 지능형 공격에 대해 동일한 동적 방어 체계로 대응하게 합니다 . FireEye Dynamic Threat Intelligence™(DTI) 클라우드 가입자는 Central Management 를 사용하여 전 세계의 고객 , 기술 파트너 및 서비스 업체에 설치된 FireEye 솔루션에서 익명화된 위협 인텔리전스의 발신과 수신을 중앙 집중화할 수 있습니다 .

**한눈에 볼 수 있는 보안 대시보드와 드릴다운 기능**

Central Management 는 통합 보안 대시보드를 통해 활동을 통합하고 상황 인식을 개선합니다 . 이 대시보드가 제공하는 실시간 뷰를 통해 관리자는 감염된 시스템 수를 확인하고 감염 세부 정보로 직접 파고들어 다음 단계를 결정할 수 있습니다 .

**지능형 표적 공격의 통합 분석**
악성 URL 을 배포하는데 사용되는 스피어 피싱 이메일을 정확하게 찾아내고 경계 경보와 엔드포인트의 상관관계를 밝히는 등의 혼합 위협의 분석이 가능해집니다 . 보안 분석가는 혼합 공격의 연관성을 파악함으로써 지능형 표적 공격으로부터 조직 보호를 위해 활용 가능한 인텔리전스를 확보할 수 있습니다 .

**기업 수준의 콘솔 및 경보 기능**
Central Management 는 이벤트를 확인 , 검색 및 필터링할 수 있는 웹 GUI 콘솔을 제공하며 , SMTP, SNMP, syslog 또는 HTTP POST 를 통해 전송되는 실시간 경보 알림을 제공합니다 . 관리자는 이벤트 , 날짜 또는 IP 범위에 따라 필터링할 수 있으며 , 관리자의 IT 운영 역할 기반의 데이터만 결과로 표시됩니다 . 타사 SIEM 툴로도 알림을 보낼 수 있습니다 . 관리자는 이벤트 링크를 클릭하고 특정 FireEye 솔루션에 빈틈없이 연결하여 보호 중인 네트워크 세그먼트를 볼 수 있습니다 .

**중심 구성 및 플랫폼 업그레이드**
기업 환경에 효율적으로 설치할 수 있도록 Central Management 는 동적 구성 기능을 제공합니다 . 중앙에서 설정을 결정한 후 그에 따라 조직 전체에 배포할 수 있습니다 . 관리자는 하나 이상의 FireEye 보안 솔루션의 설정을 원격으로 구성하고 볼 수 있습니다 . 또한 모든 업그레이드는 모든 관리 솔루션에 동시에 설치되어 모든 솔루션에 최신 보안 기능이 적용되도록 보장합니다 .

**통합 저장소 및 세부 보고**
엄격한 규제를 받는 대규모 조직에서는 Central Management 를 활용하여 보안 데이터의 효율적인 통합 보고 기능을 구현할 수 있습니다 . Central Management 는 장기적인 데이터 보존 요건을 충족할 수 있도록 감사 관련 보안 이벤트를 수집하고 저장하는 기능을 제공합니다 .

Central Management 는 위협을 이름 또는 유형을 기준으로 간편하게 검색하고 보고하는 기능을 제공합니다 . 감염된 주요 호스트와 악성코드 및 콜백 이벤트와 같은 요약 정보를 지리적 위치 정보와 함께 확인할 수도 있습니다 . 추세 보기 (Trending views) 를 통해 침해 당한 시스템의 수를 줄이는 작업의 프로그레스를 표시할 수 있습니다 .

**표 1.** 어플라이언스 사양.

| | CM 4500 | CM 7500 | CM 9500 |
|---|---|---|---|
| **네트워크 인터페이스 포트** | 2x 1GigE BaseT | 2x 1GigE BaseT | 2x 1GigE BaseT |
| **관리 포트(후면 패널)** | 2x 1GigE BaseT | 2x 1GigE BaseT | 2x 1GigE BaseT |
| **IPMI 포트(후면 패널)** | 포함 | 포함 | 포함 |
| **전면 패널 LCD 및 키패드** | 포함 | 포함 | 포함 |
| **PS/2 키보드 및 마우스, DB15 VGA 포트 (후면 패널)** | 포함 | 포함 | 포함 |
| **USB 포트(후면 패널)** | 2x 타입 A USB 포트 | 2x 타입 A USB 포트 | 2x 타입 A USB 포트 |
| **시리얼 포트(후면 패널)** | 115,200bps, 패리티 없음, 8비트, 정지 비트 | 115,200bps, 패리티 없음, 8비트, 1 정지 비트 | 115,200bps, 패리티 없음, 8비트, 1 정지 비트 |
| **저장 용량** | 4x 4TB HDD, RAID 10 사용 가능, 8TB | 4x 4TB HDD, RAID 10 사용 가능, 8TB | 4x 4TB HDD, RAID 10 사용 가능, 8TB |
| **엔클로저** | 1RU, 19인치 랙에 적합 | 2RU, 19인치 랙에 적합 | 2RU, 19인치 랙에 적합 |
| **섀시 크기(WxDxH)** | 437 x 650 x 43.2mm (17.2 x 25.6 x 1.7인치) | 438 x 620 x 88.4mm (17.24 x 24.41 x 3.48인치) | 438 x 620 x 88.4mm (17.24 x 24.41 x 3.48인치) |
| **AC 전원 장치** | 중복(1+1) 750와트 AC PSU | 중복(1+1) 800와트 AC PSU | 중복(1+1) 800와트 AC PSU |
| **최대 전력 소비(와트)** | 245와트 | 456와트 | 612와트 |
| **최대 열 방산(BTU/h)** | 836BTU/h | 1556BTU/h | 2088BTU/h |
| **MTBF(h)** | 35,200h | 60,700h | 60,700h |
| **어플라이언스 전용/발송 중량 lb. (kg)** | 30.0lbs(13.6kg)/41.0(18.6kg) | 20.0kg(44.1lbs)/29.6kg(65.3lbs) | 50.4lbs(22.9kg)/71.6lbs(32.5kg) |

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

**표 1.** 어플라이언스 사양.

| | CM 4500 | CM 7500 | CM 9500 |
|---|---|---|---|
| **안전 인증** | IEC 60950, EN 60950, CSA 60950-00, CE 마킹 | IEC 60950, EN 60950, CSA 60950-00, CE 마킹 | IEC 60950, EN 60950, CSA 60950-00, CE 마킹 |
| **EMC/EMI 인증** | FCC 파트 15 서브파트 B 클래스 A, ICES-003 클래스 A, EN 61000-3-2 클래스 A, EN 61000-3-3, CISPR22 클래스 A | FCC 파트 15 서브파트 B 클래스 A, ICES-003 클래스 A, EN 61000-3-2 클래스 A, EN 61000-3-3, CISPR22 클래스 A | FCC 파트 15 서브파트 B 클래스 A, ICES-003 클래스 A, EN 61000-3-2 클래스 A, EN 61000-3-3, CISPR22 클래스 A |
| **규제 준수** | RoHS, REACH, WEEE | RoHS, REACH, WEEE | RoHS, REACH, WEEE |
| **작동 온도** | 0-35°C | 0-35°C | 0-35°C |
| **작동 상대 습도** | 40°C에서 10-95%, 비응결 | 40°C에서 10-95%, 비응결 | 40°C에서 10-95%, 비응결 |
| **작동 고도** | 5,000ft | 5,000ft | 5,000ft |

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

**표 2.** 가상 어플라이언스 사양.

| 모델 | CPU 코어 | RAM | 가상 NIC 수 | 하드 디스크 공간 |
|---|---|---|---|---|
| **CM2500V** | 4 | 32GB | 4(전체):<br>1(관리)<br>1-3(향후 사용) | 512GB |
| **CM7500V** | 16개 | 128GB | 4(전체):<br>1(관리)<br>1-3(향후 사용) | 1200GB |

**주 :** 각 가상 어플라이언스는 다음 사양에 부합해야 합니다 .

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.

FIREEYE™