Cisco FireSIGHT Management Center

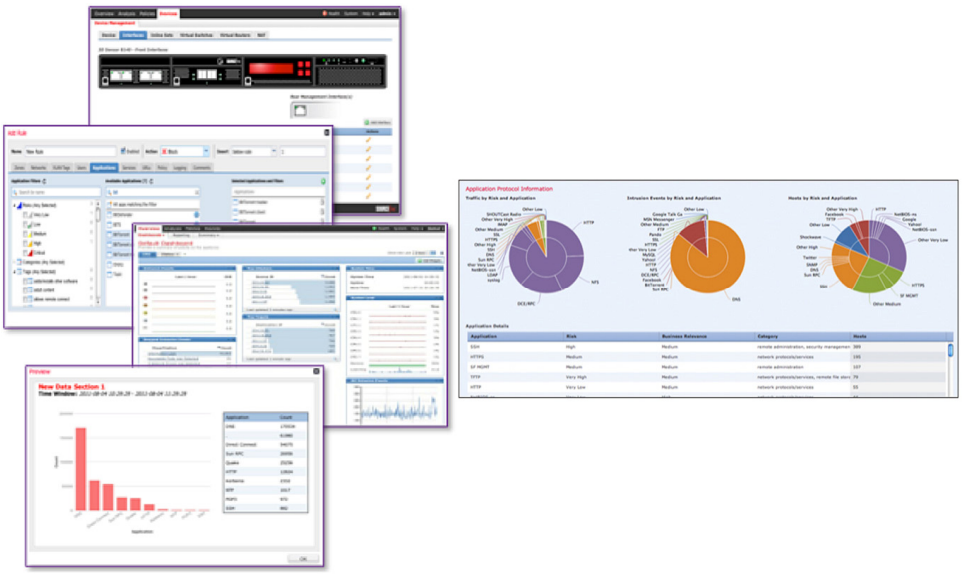
효과적으로 위협을 방어하려면 네트워크에 대한 가시성과 통찰력이 무엇보다 중요합니다. Cisco FireSIGHT™ Management Center가 그 요구 사항을 해결합니다.

제품 개요

Cisco FireSIGHT Management Center에서 네트워크의 모든 것, 즉 물리적 및 가상 호스트, 운영 체제, 애플리케이션, 서비스, 프로토콜, 사용자, 지오로케이션 정보, 콘텐츠, 네트워크 동작, 네트워크 공격, 악성코드 등에 대한 완전한 가시성을 확보하십시오. 이 보안 관리 콘솔(그림 1)은 중앙에서 침입 방어 보안 운영을 위한 이벤트 및 정책 관리를 담당합니다. 여기에서 Cisco의 차세대 방화벽인 Cisco® ASA with FirePOWER™ Services와 Cisco의 NGIPS(next-generation Intrusion Prevention System)인 Cisco FirePOWER NGIPS에서 생성하는 정보를 자동으로 취합하고 상관성을 분석할 수 있습니다. Cisco FireSIGHT Management Center는 이벤트 모니터링, 분석, 보안사고 우선순위 지정, 리포팅을 비롯한 네트워크 보안 및 운영 기능을 중앙에서 관리하여 비즈니스 보호를 용이하게 합니다. 또한, 운영을 효율화하고 일반적으로 반복되는 보안 분석 및 관리 작업을 자동화하여 비용을 절감합니다.

엔터프라이즈급 관리

그림 1. Cisco FireSIGHT Management Center: 중앙 집중식 정책, 이벤트 및 기기 관리



Cisco FireSIGHT Management Center에서 변화하는 네트워크 리소스 및 운영에 대한 실시간 정보를 검색하므로 완전한 컨텍스트를 토대로 현명한 결정을 내릴 수 있습니다(표 1 참조). Cisco FireSIGHT Management Center는 광범위한 인텔리전스뿐 아니라 다음과 같이 정밀한 수준의 세부 정보도 제공합니다.

- **추이 및 요약 통계:** 관리자와 경영진이 특정 시점의 보안 상태는 물론 개선 또는 악화의 변화 동향까지 파악할 수 있습니다.

- **이벤트 세부사항, 규정준수, 포렌식(forensics):** 보안 이벤트 과정에 발생한 상황을 이해하여 더 효과적으로 방어하고 보안 침해 억제 활동을 뒷받침하며 법 집행 활동을 지원합니다.
- **워크플로:** 손쉬운 데이터 내보내기 기능으로 이벤트에 대한 대응을 지원하면서 대응 관리의 수준을 높입니다.

최고의 가시성 및 인사이트

표 1에서는 기존의 보안 기술에서 탐지하지 못하는 공격 벡터에 대해 Cisco FireSIGHT Management Center가 제공하는 컨텍스트 정보의 범위를 보여줍니다.

표 1. Cisco FireSIGHT Management Center: 풀스택 가시성

카테고리	FireSIGHT Management Center	일반 IPS	일반 차세대 방화벽
위협	예	예	예
사용자	예	예	예
웹 애플리케이션	예	아니요	예
애플리케이션 프로토콜	예	아니요	예
파일 전송	예	아니요	예
악성코드	예	아니요	아니요
C&C 서버	예	아니요	아니요
클라이언트 애플리케이션	예	아니요	아니요
네트워크 서버	예	아니요	아니요
OS(Operating Systems)	예	아니요	아니요
라우터 및 스위치	예	아니요	아니요
모바일 디바이스	예	아니요	아니요
프린터	예	아니요	아니요
VoIP 폰	예	아니요	아니요
가상 머신	예	아니요	아니요

Cisco FireSIGHT Management Center는 다양한 모델이 있습니다. 모니터링할 센서 어플라이언스 수(물리적 및 가상), 해당 환경의 호스트 수, 예상 보안 이벤트 발생률을 기준으로 귀사에 적합한 모델을 선택하십시오(표 2 참조). 모든 모델이 다음과 같은 관리 기능을 공통으로 제공합니다.

- 중앙에서 디바이스, 라이센스, 이벤트, 정책 관리
- 역할 기반 관리(관리자 역할 또는 그룹을 기반으로 세분화되고 격리된 보기 및 임무)
- 맞춤 보고서 및 템플릿 기반 보고서가 제공되는 맞춤형 대시보드
- 일반 정보와 집중식 정보 모두에 대한 포괄적인 보고 및 경고
- 하이퍼링크 테이블, 그래프 및 차트로 볼 수 있는 이벤트 및 상황별 정보
- 네트워크 활동 및 성능 모니터링
- 단일 장애 지점을 허용하지 않는 강력한 고가용성 옵션
- 실시간으로 위협을 대응할 수 있는 상관관계 및 복원 기능
- 방화벽, 네트워크 인프라, 로그 관리, SIEM(Security Information and Event Management), 트러블 티켓팅(trouble ticketing), 패치 관리 등의 서드파티 솔루션 및 고객 워크 스트림과 통합하는 개방형 API

동적 방어를 위한 보안 자동화

Cisco FireSIGHT Management Center는 시간의 경과에 따른 네트워크의 변화 추이를 지속적으로 모니터링합니다. 새로운 위협이 발생하면 자동으로 기존 네트워크 취약성과의 상관성을 분석하여 비즈니스에 영향을 미칠지 여부를 판단합니다. 따라서 각종 불필요한 정보를 걸러내고 가장 큰 영향을 미칠 이벤트에 대응하는 데 주력할 수 있습니다. 정책 튜닝과 같은 중요한 보안 활동도 자동화되므로 시간과 수고를 줄이면서 환경의 변화에 발맞춰 네트워크 방어 체계를 조정할 수 있습니다. 그 결과, 해당 네트워크 및 직면한 위협에 맞게 최적화된 보안 정책이 마련됩니다.

구축 모드 선택

Cisco FireSIGHT Management Center는 물리적 또는 가상 어플라이언스로 구축 가능하므로 해당 환경에 가장 적합한 옵션을 선택할 수 있습니다. 물리적 어플라이언스 형태의 Cisco FireSIGHT Management Center는 대개 가상 어플라이언스보다 많은 수의 센서를 관리하고 더 강력한 이벤트 스토리지 기능을 제공합니다. 가상 어플라이언스 형태의 Cisco FireSIGHT Management Center에서는 편리하게 기존 VM 인프라를 사용할 수 있습니다. VMware vSphere 프로비저닝을 사용하여 편리하게 구축할 수 있으며 물리적 네트워크의 자산을 보호하는 데 활용할 수 있습니다. 버전 5.x 가상 어플라이언스는 VMware ESX 및 ESXi 하이퍼바이저에서 호스팅할 수 있으며 최대 25개의 물리적 또는 가상 센서를 관리합니다.

제품 사양

표 2에서는 Cisco FireSIGHT Management Center 물리적 및 가상 어플라이언스의 용량과 처리량을 비교합니다.

표 2. Cisco FireSIGHT Management Center 모델

기능	FireSIGHT FS750	FireSIGHT FS1500	FireSIGHT FS2000	FireSIGHT FS3500	FireSIGHT FS4000	FireSIGHT FS-VMW-SW
관리하는 센서의 최대 개수	10	35	70	150	300	25 10 2
IPS 이벤트 최대 개수	2,000만	3,000만	6,000만	1억 5,000만	3억	1,000만
이벤트 스토리지	100GB	125GB	1.8TB	400GB	4.8TB	250GB
최대 네트워크 맵(호스트/사용자)	2,000/2,000	50,000/50,000	150,000/150,000	300,000/300,000	600,000/600,000	50,000/50,000
최대 플로우 속도 (초당 플로우 수)	2,000fps	6,000fps	12,000fps	10,000fps	20,000fps	가변적*
네트워크 인터페이스	2 x 1Gbps	2 x 1Gbps	2 x 1Gbps 2 x 10Gbps (CCW를 통해 SFP 옵션 사용 가능)	2 x 1Gbps	2 x 1Gbps 2 x 10Gbps (CCW를 통해 SFP 옵션 사용 가능)	1 x 1Gbps
고가용성	LOM(Lights-out management)	RAID 1, LOM, 고가용성 페어링	RAID 5, LOM, 고가용성 페어링	RAID 5, LOM, 고가용성 페어링	RAID 5, LOM, 고가용성 페어링	아니요

참고: 센서를 작동하려면 Cisco FireSIGHT Management Center 어플라이언스가 있어야 합니다. 모든 센서 라이센싱 및 관리는 Management Center에서 처리됩니다. 또한 모든 Cisco FireSIGHT Management Center는 Cisco ASA with FirePOWER Services 구축에서 FirePOWER 영역만 관리합니다.

* 가상 Cisco FireSIGHT Management Center의 성능은 선택된 가상 환경, 즉 CPU, 메모리, 스토리지 등의 요소에 크게 좌우됩니다.

주문 정보

가상 및 물리적 Cisco FireSIGHT Management Center 어플라이언스와 추가 스페어 하드웨어에 대한 주문 정보는 표 3을 참조하십시오.

표 3. Cisco FireSIGHT Management Center 주문 정보

Cisco FireSIGHT Management Center(하드웨어) 어플라이언스	
부품 번호	**제품 설명**
FS750-K9	Cisco FireSIGHT Management Center 750 Chassis, 1RU
FS1500-K9	Cisco FireSIGHT Management Center 1500 Chassis, 1RU
FS2000-K9	Cisco FireSIGHT Management Center 2000 Chassis, 1RU
FS3500-K9	Cisco FireSIGHT Management Center 3500 Chassis, 1RU
FS4000-K9	Cisco FireSIGHT Management Center 4000 Chassis, 1RU
Cisco FireSIGHT Management Center(하드웨어) 스페어	
FS-PWR-AC-650W=	Cisco FireSIGHT 650W AC Power Supply
Cisco FireSIGHT Management Center(소프트웨어) 가상 어플라이언스	
FS-VMW-SW-K9	Cisco FireSIGHT Management Center, Virtual(VMware) FireSIGHT 라이센스
FS-VMW-10-SW-K9	Cisco FireSIGHT Management Center, Virtual(VMware) FireSIGHT 라이센스 - 디바이스 10개
FS-VMW-2-SW-K9	Cisco FireSIGHT Management Center, Virtual(VMware) FireSIGHT 라이센스 - 디바이스 2개

제품을 주문하려면 Cisco 주문 홈 페이지를 방문하십시오.

자세한 정보

자세한 내용은 다음 링크를 참조하십시오.

- Cisco ASA with FirePOWER Services
- Cisco FirePOWER Appliances
- Cisco FireSIGHT Management Center
- Cisco Security Services

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C78-732251-03 05/15