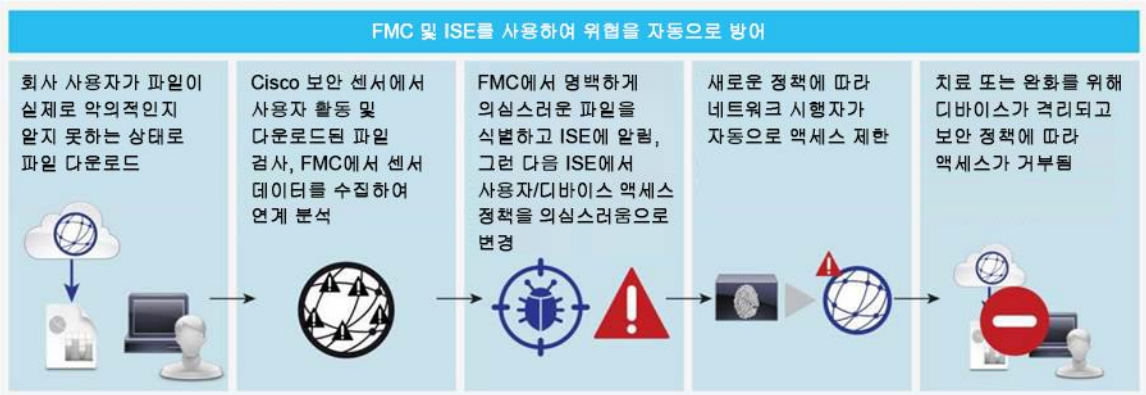
Cisco FireSIGHT Management Center 및 Cisco Identity Services Engine이 포함된 Cisco Rapid Threat Containment

Cisco® Rapid Threat Containment를 사용하면 네트워크에서 악성 위협이 탐지되는 즉시 차단할 수 있습니다.

위협이 탐지되지 않는 시간이 길어질수록 피해 가능성이 커집니다. 현재 업계의 평균 탐지 시간은 200일로, 이는 너무 긴 시간입니다. 보안 침해가 발견되더라도 피해가 이미 발생한 뒤입니다. 화재에 자동으로 반응하는 화재 스프링클러와 같이 작동하는 솔루션이 필요합니다. 명백한 악성 위협에 따른 피해를 억제하려면 이러한 솔루션이 자동으로 활성화되어야 합니다.

Cisco FMC(FireSIGHT Management Center) 및 Cisco ISE(Identity Services Engine)가 포함된 Cisco Rapid Threat Containment 솔루션을 사용하면 중요한 사항의 핵심을 파악할 수 있습니다. 즉, 치명적인 위협을 빠르게 탐지하고 억제하여 보안 위험을 완화할 수 있습니다. 그림 1에서는 이 솔루션이 작동하는 방식을 보여줍니다.



기능 및 혜택

기능	혜택
Cisco ISE(Identity Services Engine) 네트워크 리소스에 상황 인식 보안 액세스를 자동화하고 적용합니다. 엔터프라이즈 환경을 지원하고 액세스를 제어할 수 있는 탁월한 사용자 및 디바이스 가시성을 제공합니다. 통합된 파트너 솔루션과 데이터를 공유하여 더욱 빠르게 위협을 식별하고 완화하며 복원합니다.	권한 있는 안전한 디바이스만 회사 리소스에 액세스할 수 있도록 합니다. 조직은 네트워크에 존재하는 대상, 자세한 디바이스 정보, 디바이스가 연결된 시기 및 위치, 디바이스 연결 방법에 대한 자세한 정보를 얻습니다. 통합 파트너와의 자동화된 통신으로 빠르고 다양한 정책 관리 활용 사례를 사용할 수 있습니다.
Cisco FireSIGHT Management Center 5.4 Cisco ASA with FirePOWER™ Services 및 Cisco FirePOWER 네트워크 보안 어플라이언스에 대한 네트워크 보안 및 운영 기능을 중앙 집중식으로 관리합니다. 자동화된 상황 분석 및 위협 자격 부여를 통해 실행 가능한 인텔리전스를 제공합니다. Cisco 센서에 대한 지속적인 위협 인텔리전스 업데이트로 엔드포인트 인텔리전스를 강화합니다.	IT 보안 팀이 엔드포인트 보안 환경을 파악하고 모니터링하도록 지원합니다. 일반적으로 반복되는 보안 분석 및 관리 작업을 자동화하여 운영을 간소화합니다. 상관성 분석 및 복원 기능이 실시간 위협 대응을 제공합니다. 정책 조정을 자동화하여 새로운 위협으로부터 보호합니다.

기능	혜택
Cisco pxGrid(Platform Exchange) Adaptive Network Control을 통해 점점 더 증가하는 Cisco 제품 및 파트너 플랫폼 목록과의 양방향 통신 지원	다양한 벤더 보안 기술 간에 데이터를 공유하여 위협을 더욱 명확히 하고 네트워크를 시행자로 사용하여 위협을 억제하는 즉각적인 조치를 수행하도록 합니다.
위협 센서	업계 최고의 지능형 위협 탐지를 위해 지능형 악성코드와 보안 침해 지표(IoC)를 탐지합니다.
네트워크 위협 적용	여러 적용 옵션을 통해 보안 범위를 엔터프라이즈 전체로 확장합니다.

위협 가시성 및 탐지 효과 향상

IT 보안 팀에서는 네트워크 전체에 잠복해 있는 새로운 위협을 탐지하고 빠르고 자동화된 의사 결정을 내리는 데 필요한 정보를 수신할 수 있습니다. FireSIGHT Management Center는 자동화된 상황 분석 및 위협 자격 부여를 통해 실행 가능한 인텔리전스를 제공합니다. Cisco ASA with FirePOWER Services, NGIPS(Next Generation Intrusion Prevention System) 및 Cisco AMP(Advanced Malware Protection)를 포함한 Cisco 위협 세션의 조합에서 정보를 수집합니다. 이러한 센서는 사전 대응적이지 않은 방어를 피할 수 있는 위협을 탐지할 수 있도록 실시간 위협 인텔리전스로 계속 업데이트됩니다.

억제 시간 단축

감염된 엔드포인트를 위협으로 간주하여 자동으로 신속하게 제거합니다. 위협 또는 보안 침해 지표(IoC)의 심각도에 따라 FireSIGHT Management Center가 Cisco ISE에 감염된 엔드포인트를 억제하도록 지시합니다. 그런 다음, Cisco ISE가 라우터, 스위치, 방화벽 또는 무선 컨트롤러에 적용 지침을 자동으로 전달합니다. 적용 옵션에는 Cisco TrustSec 소프트웨어 정의 세그멘테이션, dACL(downloadable Access Control List) 또는 VLAN 격리가 포함됩니다. 그런 다음, 엔드포인트를 치료하거나 네트워크에 액세스하지 못하도록 완벽하게 차단할 수 있습니다.

비용 절감

운영 오버헤드, 악성코드 관련 비용 및 자본 비용이 감소됩니다. 설정한 정책을 기반으로 자동화된 응답이 응답을 가속화하므로 공격의 피해 및 재정적인 영향을 완화하는 동시에 IT 보안 담당자의 개입을 줄일 수 있습니다. 이미 적용을 위해 구축된 Cisco 네트워크 디바이스를 사용할 수 있기 때문에 자본 비용이 감소됩니다.

플랫폼 지원/호환성

제품군	지원되는 플랫폼
FireSIGHT Management Center	**5.4**
FireSIGHT pxGrid Remediation Module	**1.0**
FireSIGHT pxGrid Agent	**1.0**
Identity Services Engine	**1.3, 1.4, 2.0**
네트워크 위협 적용	• Cisco TrustSec® 기술: 소프트웨어 정의 세그멘테이션은 감염된 엔드포인트를 억제하는 가장 유연한 지능형 방식을 제공합니다. 감염된 엔드포인트가 연결된 네트워크 액세스 스위치 또는 컨트롤러에서 적용이 발생하거나 Cisco ASA(Adaptive Security Appliance), Cisco Web Security Appliance 또는 Cisco ISR과 같은 다운스트림 디바이스에서 적용이 발생할 수 있습니다. • **dACL(downloadable Access Control List):** Cisco ISE는 dACL 또는 명명된 ACL을 스위치 또는 컨트롤러에 전달하여 스위치 또는 무선 컨트롤러에서 디바이스를 차단하거나 억제할 수 있습니다. • **VLAN:** ISE는 감염된 디바이스를 격리된 VLAN으로 이동할 수 있습니다.

제품군	지원되는 플랫폼
위협 센서	• 라이센스가 부여된 NGIPS(Next-Generation Intrusion Prevention System)와 Cisco AMP(Advanced Malware Protection)를 포함하는 Cisco ASA with FirePOWER Services NGFW(Next-Generation Firewall) • Cisco FirePOWER NGIPS 어플라이언스 • Cisco AMP for Networks 어플라이언스 • Cisco FirePOWER NGIPSv(virtual NGIPS) • Cisco FirePOWER Threat Defense for Cisco ISR(Integrated Services Router)

시스코 캐피탈

목표 달성을 지원하는 파이낸싱

Cisco Capital이 목표 달성과 경쟁력 유지에 필요한 기술 도입을 도와드리겠습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI를 최적화하십시오. 시스코 캐피탈 파이낸싱은 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 도입에 유연성을 제공합니다. 또한 예측 가능한 비용 결제가 단 한 번뿐입니다. 시스코 캐피탈은 100여 개 국가에서 이용할 수 있습니다. 자세히 보기

추가 정보

자세한 내용은 http://www.cisco.com/go/rtc를 참조하거나 Cisco 영업 담당자 또는 Cisco 공인 채널 파트너에 문의하십시오.

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.

인쇄지: 미국 C78-736242-00 12/16