



Cisco FirePOWER Threat Defense for ISR

지사 및 원격 사무실 보호

오늘날 지사에서 발생하는 엔터프라이즈급 위험을 해결하려면 엔터프라이즈급 보안 솔루션이 필요합니다. 분산된 사이트에서 BYOD, 규정 준수 요구 사항 및 날로 늘어나는 DIA(Direct Internet Access) 사용을 지원하는 동시에 끊임없이 발생하는 지능형 위협으로부터 보호해야 합니다.

Cisco ISR(Integrated Services Router)이라는 추가 플랫폼에서 실행되는 업계 최고의 Cisco 위협 차단 기능을 사용하면 이러한 목표를 실현할 수 있습니다. Cisco FirePOWER Threat Defense for ISR은 엔터프라이즈급 위협 차단 기능의 적용 범위를 기존의 네트워크 에지 및 데이터 센터 구축 환경에서 확장하여 DIA 트래픽까지 보호합니다.

이제 지사 DIA의 비용 절감 이점과 향상된 사용자 경험을 활용하는 동시에, 지사, 파트너 위치, 기타 원격 사이트 등 상주하는 위치와 관계없이 디바이스와 호스트를 지능형 위협으로부터 보호할 수 있습니다.

혜택

- 지사에서 연결을 안전하게 보호하면서 DIA(Direct Internet Access)의 이점을 활용합니다.
- 지사, 파트너 및 원격 사무소에 다계층 위협 차단 기능을 제공합니다.
- 라우터와 보안 기술을 하나의 통합된 설치 공간에 구축함으로써 귀중한 공간을 확보해 줍니다.
- 중앙 집중식 관리 콘솔을 사용하여 역할과 책임을 명확하게 나눕니다.

“FirePOWER 8350은 환경에 맞게 튜닝된 정책을 사용하여 익스플로잇 공격을 99.5% 차단했습니다. 이 디바이스는 테스트한 모든 우회 수법에 대해서 효과가 입증되었습니다. 또한 안정성 및 신뢰성 테스트를 모두 통과했습니다.”

NSS Labs 2015 NGIPS(Next Generation Intrusion Prevention System) 테스트 보고서

‘Security Everywhere’ 지향

Cisco FirePOWER Threat Defense for ISR은 Cisco “Security Everywhere” 전략의 구성 요소 중 하나입니다. 이 전략은 환경 전반에서 지능형 위협을 무력화시키는 데 필요한 지속적인 가시성과 제어 기능을 제공하는 것을 목표로 합니다. 통합된 보안 기능 세트가 유기적으로 작동하여 원격 운영을 안전하게 지켜 줍니다.

- **FirePOWER NGIPS(Next-Generation Intrusion Prevention System)**는 실시간 상황 인식 기능, 지능형 보안 자동화 기능 및 업계 최고의 위협 방지 기능을 통합하여 지능형 위협 차단의 표준을 정립합니다.
- **Application Visibility and Control**은 수천 개의 애플리케이션을 정밀하게 제어하고 모바일 앱 정책, 소셜 미디어 앱 정책 및 제한적 사용 정책을 적용하여 잠재적인 공격 표면을 최소화합니다.
- **AMP(Advanced Malware Protection) for Networks**는 고도로 지능화되고 특정 표적을 노리는 제로 데이 공격과 지속적인 지능형 악성코드 위협을 차단합니다.
- **평판 기반 URL 필터링**은 80개 이상의 카테고리에서 2억8천만 개가 넘는 URL에 대한 액세스를 제어하여, 의심스럽고 허용되지 않는 도메인과 관련한 위협을 최소화하여 정교한 클라이언트 쪽 공격을 완화시킵니다.
- **FireSIGHT Management Center**는 중앙 집중식 이벤트 및 정책 관리 기능과 네트워크에서 실행 중인 디바이스, 운영 체제, 애플리케이션 및 사용자에 대한 가시성을 제공합니다.

다음 단계

데모 일정을 예약하고 가격 정보를 요청하려면 현지 세일즈 담당자에게 문의하여 주십시오. 자세한 내용은 [Cisco FirePOWER Threat Defense for ISR](#) 웹 페이지를 참조하여 주십시오.