한눈에 보기

Cisco Firepower Next-Generation Firewall

장점

- **더 많은 위협을 차단:** 업계에서 가장 효과적인 위협 차단 기능을 통해 알려진 위협 및 알려지지 않은 위협을 모두 차단
- **더 정확한 인사이트 확보:** 네트워크의 사용자, 애플리케이션, 디바이스, 위협 및 취약점에 대한 가시성과 제어력 향상
- **조기에 탐지하여 더 신속하게 조치:** 악성코드 탐지 소요 시간을 몇 개월에서 몇 시간으로 단축하고 신속하게 치료
- **복잡성 감소:** 모든 보안 기능을 단일 관리 인터페이스로 통합하여 복잡성을 줄이고 운영을 간소화
- **네트워크를 더욱 활용:** 다른 Cisco 보안 및 네트워크 솔루션과 통합

업계 최초의 완전 통합형 위협 중심 차세대 방화벽

대부분의 NGFW(Next-Generation Firewall, 차세대 방화벽)는 애플리케이션 제어에만 집중하므로 위협 방어 기능에는 거의 관심을 두지 않습니다. 일부 NGFW는 이를 보완하기 위해 일련의 통합되지 않은 추가 제품으로 1세대 침입 방지 솔루션을 보완하려고 합니다. 그러나 이러한 접근 방식은 정교한 공격자와 지능형 악성코드의 위험에서 비즈니스를 보호하지 못합니다. 뿐만 아니라, 감염되었을 때 감염을 조사하여 억제하고 신속하게 치료하는 데 도움이 되지 않습니다.

따라서 완전히 통합된 위협 중심의 차세대 방화벽이 필요합니다. 세밀한 애플리케이션 제어를 제공할 뿐만 아니라 정교하고 우회 능력이 뛰어난 악성코드 공격의 위협에 대해 효과적인 보안을 제공하는 방화벽이 필요합니다.

Cisco Firepower™ NGFW(Next-Generation Firewall)는 업계 최초의 완전 통합형 위협 중심 NGFW입니다. 네트워크에서 엔드포인트에 이르기까지 방화벽 기능, 애플리케이션 제어, 위협 차단, 지능형 악성코드 차단에 대한 종합적인 통합 정책 관리를 제공합니다.

인터넷 에지 및 기타 고성능 환경을 위한 고성능 및 고집적도 플랫폼은 여기에 최적화된 NGFW 보안 플랫폼인 Cisco Firepower 4100 및 9300 어플라이언스의 구축으로 구현할 수 있습니다.

공격 전, 중, 후의 전 단계에서 조직 네트워크를 보호

Cisco Firepower NGFW는 업계에서 가장 널리 구축된 스테이트풀 방화벽을 포함하며 4,000개 이상의 상용 애플리케이션에 대한 세밀한 제어를 제공합니다. 단일 관리 인터페이스를 통해 네트워크에서 엔드포인트까지 통합된 가시성을 제공합니다. Firepower NGFW를 사용하면 액세스를 제어하고, 공격을 차단하며, 악성코드로부터 방어하고, 통합형 툴을 제공하는 종합적인 정책 관리를 통해 공격을 추적 및 억제하고 공격으로부터 복구할 수 있습니다.

Cisco Firepower NGFW는 다음과 같은 이점을 제공하는 업계 유일의 차세대 방화벽입니다.

- 업계 최고의 위협 차단 기능을 지원하기 위해 NGIPS(Next-Generation Intrusion Prevention System)를 제공합니다.
- 통합형 샌드박스와 함께 알려진 위협 및 알려지지 않은 위협을 모두 처리하는 완전 통합형 AMP(Advanced Malware Protection)를 포함합니다.
- 악성코드 감염을 추적하고 억제하는 기능을 제공합니다.
- 위협 이벤트와 네트워크 취약점의 상관관계를 자동으로 분석하여 가장 문제가 되는 위협에 리소스를 집중할 수 있습니다.
- 네트워크의 약점을 분석하고 적용할 수 있는 최선의 보안 정책을 추천합니다.
- 여러 Cisco® 네트워크 보안 제품과 통합되어 이전에 구축되어 있는 제품을 활용하여 더 강력한 보안을 제공합니다.

다음 단계

자세한 내용은 www.cisco.com/go/ngfw를 참조하십시오.

C45-736624-01 02/16