정부 기관이 방화벽을 선택할 때 고려해야 할 5가지 팁

목차

하이브리드 및 분산형 환경의 새로운 세상을 위한 유연하고 신뢰할 수 있는 보안 기반으로 방화벽을 재고해 보세요.

1. 틀을 벗어나 생각하기

최신 방화벽은 어떤 모습인가요? 네트워크 인프라와 완전히 통합되었지만, 아마 가장 중요한 것은 단일 창에서 모든 것에 정책을 시행할 수 있다는 점입니다. 차세대 방화벽은 플랫폼, 모바일 디바이스의 정보, 컨텍스트 및 위협 정보 전체에 걸쳐 통합된 정책을 제공합니다. 이는 취약한 모바일 앱과 엔드포인트 전체를 통해 네트워크에 대한 연결을 처리하는 데 필요한 가시성입니다.

2. 암호화된 트래픽 내에 있는 것 보기

암호화된 트래픽 내에서 무슨 일이 일어나는지 실제로 보는 데 방해가 되는 것은 항상 완전한 해독이었습니다. 이는 법적 수준 및 운영 수준에서 모두 비현실적인 값비싼 프로세스로, 네트워크와 인프라를 데이터 유출(보안 침해)부터 랜섬웨어 공격에 이르기까지 모든 것에 아주 취약한 상태로 있게 만듭니다.

실제 당면 과제는 암호화된 트래픽 내의 악의적인 활동을 탐지하는 방법을 찾는 것이었습니다. 새로운 방화벽은 최소한의 복호화 양력과 비용으로 최대 가시성을 제공하는 것을 목적으로 이 기능을 우선시해야 합니다.

3. 위협 정보 즉시 요구

네트워크와 취약하고 구식인 인프라에 대한 점점 더 정교해지는 위협과 함께 공격 표면이 확장됨에 따라 모든 인텔리전스 프레임워크는 사이버 범죄자보다 한발 앞서야 합니다. 받는 위협이 정확히 무엇인지, 즉 스팸, 악성코드 또는 기타 유형의 위협인지 식별해야 합니다.

이러한 정보는 방화벽이 수행해야 하는 일에 관한 기본적인 지식의 역할을 합니다. 즉, 디바이스, 위치, 네트워크의 사용자에 대한 동적인 컨텍스트를 제공합니다.

4. 보안 탄력성 구축

종종 취약한 디바이스와 앱을 통해 네트워크에 일상적으로 액세스하는 사용자로 구성된 하이브리드 환경은 해커에게 네트워크에 잠입할 여러 가지 유혹적인 방법을 제공해 구식인 인프라를 특히 취약하고 관심이 가도록 만듭니다. 이에 대한 대응은 보안 탄력성을 구축하는 것입니다.

보안 탄력성은 가용성이 높은 보안 인프라의 핵심, 즉 방화벽을 보호하여 위험에 따른 알림과 작업의 우선순위를 지정하고, 다음 단계를 예측하고, 시간별로 보안 업데이트 사항과 예측하지 못한 위협에 대한 대응을 업데이트하여 궁극적으로 시간을 절약하고 불만과 비용을 줄이는 것을 의미합니다.

5. 전체론적인 접근 방식 취하기

트래픽과 인텔리전스 관리를 위해 더 많은 가시성, 더 많은 컨텍스트, 통합 방식을 제공하는 여러 툴을 활용할 수 있는데 왜 방화벽으로 멈추나요? 방화벽 성능을 강화하는 툴 제품군을 사용하면 비용을 더 지불하지 않고도 더 많은 정보를 확인하고 컨텍스트를 더 잘 이해할 수 있습니다.

서비스, 여러 대시보드, 아키텍처 간 연결이 끊기면 위협 관리가 상당히 복잡해집니다. 의사 결정 속도를 높이고, 체류 시간을 줄이고, 유의미하고 실행 가능한 지표를 제공하도록 지원하는 방화벽과 개선 사항을 찾아내세요.

Cisco Secure Firewall이 보안 태세를 강화하고 점점 정교해지는 위협에 맞서 정부 기관을 보호하는 방법에 대해 확인하세요.

Cisco Secure Firewall에 대해 자세히 알아보세요.

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. 주소, 전화 번호 및 팩스 번호는 Cisco 웹사이트**www.cisco.com/go/offices**에서 확인하십시오.

미국에서 인쇄 C22-3937554-00 11/23