한눈에 보기

이점

- 일관된 보안 정책 시행
- 보안 정책 관리 간소화
- 차세대 방화벽 기능 활용
- 보안 유지를 위한 자본 및 리소스 부담 완화

Cisco Defense Orchestrator

간소화된 정책 관리로 보안 상태 강화

포괄적인 방어를 위해서는 멀티레이어 보안이 필요합니다. 하지만 보안 툴을 추가하면 네트워크 운영 팀이 보안 정책을 파악하는 것이 어려워지며 특히 지리적으로 흩어져 있는 조직의 경우 더욱 그렇습니다.

분산된 보안 디바이스의 정책을 관리하는 일은 복잡하고 시간이 소요되는 작업이며 정책 불일치와 불균형이 발생합니다. 이는 엄청난 위험을 초래합니다. 보안 침해의 가장 일반적인 원인 중 하나는 보안 디바이스에 대한 잘못된 컨피그레이션입니다.

이에 대처하려면 Cisco® Defense Orchestrator가 필요합니다. Cisco® Defense Orchestrator는 Cisco Adaptive Security Appliance(ASA), Cisco Adaptive Security Virtual Appliance, Cisco ASA with FirePOWER™ Services, Firepower Next-Generation Firewalls(NGFW), Cisco Web Security Appliance, Cisco Umbrella를 비롯한 Cisco 보안 디바이스 전반에서 번거로운 정책 관리 업무를 없앤 클라우드 기반 관리 애플리케이션입니다.

비즈니스 크리티컬 정보를 보호하는 쉬운 방법

Cisco Defense Orchestrator는 네트워크 운영 팀에 관리의 복잡성은 줄이고 비용을 절감하면서 보안 정책을 생성 및 유지하는 간단하고 일관된 방법을 제공합니다. 설정이 쉽고 빠를 뿐만 아니라 원활하며, Defense Orchestrator는 클라우드 솔루션이기 때문에 새로운 자본 지출이나 공간, 애플리케이션 관리가 필요 없습니다.

Defense Orchestrator의 주요 기능은 다음과 같습니다.

일관된 보안 시행

디바이스 전반에 걸쳐 정책 감사를 실시해 엔드 투 엔드 분석으로 정책 이상 징후를 감지하며 문제를 빠르게 해결합니다. 정책을 정리하고 일관된 정책 적용이 가능한 템플릿으로 새로운 디바이스에 올바른 정책을 쉽게 배포합니다. OOB(Out-of-Band) 변경이 발생하면 자동 알림을 받아 정책 변경을 모니터링합니다.

보안 정책 관리 간소화

계획되거나 계획되지 않은 변경 사항 모두에 대하여 진행 중인 정책 변경 관리를 스트리밍하며, 단일 장소에서 서로 다른 디바이스의 규칙을 설정, 적용 및 관리합니다. 또한 정책을 더 쉽게 최적화합니다. 위협에 빠르게 대응하고 배포하기 전 변경 사항의 효과를 모델링하여 위험을 줄입니다. 보안 정책을 확실하게 클라우드로 확장할 수 있습니다.

애플리케이션 레이어 기능 활용

관리되는 개별 제품에 대한 심층적인 지식 없이도 NGFW(Next-Generation Firewall), FirePOWER Services 및 Firepower Threat Defense의 애플리케이션 보호 기능을 활용하여 강화된 보안을 구현합니다. 광범위한 공격에 맞서 구내 또는 원격에서 일하는 직원을 모두 보호합니다.

Defense Orchestrator의 기능은 다음과 같습니다.

- **분석:** 디바이스 전반에 대해 단일의 창으로 엔드 투 엔드 보안 정책 컨피그레이션을 운영할 수 있습니다. 보안 컨피그레이션을 분석하여 잘못된 컨피그레이션을 찾아내고 보안 정책과 객체에 대해 계획되거나 계획되지 않은 변경을 관리할 수 있습니다. 디바이스별 보안 컨피그레이션의 전문가의 지원 없이도 엔드 투 엔드 정책 분석을 활용할 수 있습니다.
- **모델링:** 비즈니스 성장에 맞춰 일관된 보안 컨피그레이션을 쉽게 시행하도록 지원하는 표준화된 정책 템플릿을 생성할 수 있습니다. 디바이스에 배포하기 전에 변경 사항의 영향을 모델링할 수 있습니다.
- **치료:** 올바른 변경 사항이 디바이스에 적용되었는지 확인할 수 있습니다. 변경 관리 프로세스에 따라 적절한 변경 사항이 실시간 또는 오프라인으로 배포되었음을 확신할 수 있습니다. Defense Orchestrator에서 관리하는 모든 보안 제품에 대해 일관된 보안 상태를 시행하고 유지할 수 있습니다.
- **시각화:** 주요 애플리케이션, 대상, 범주, 공격 및 위험에 대한 정보를 종합적으로 보며 웹 정책 시행의 효과를 확인할 수 있습니다.

자세히 보기

Cisco는 보안 기술과 업계 최대의 보안 데이터베이스 분야에서 10년이 넘는 경험을 갖고 있습니다. 이 솔루션은 Cisco ASA, ASA with FirePOWER Services, Cisco Web Security Appliance, Firepower NGFW, WSA, Cisco Umbrella를 포함하여 여러 플랫폼의 포트폴리오를 통합하는 Cisco의 노력을 잘 보여줍니다.

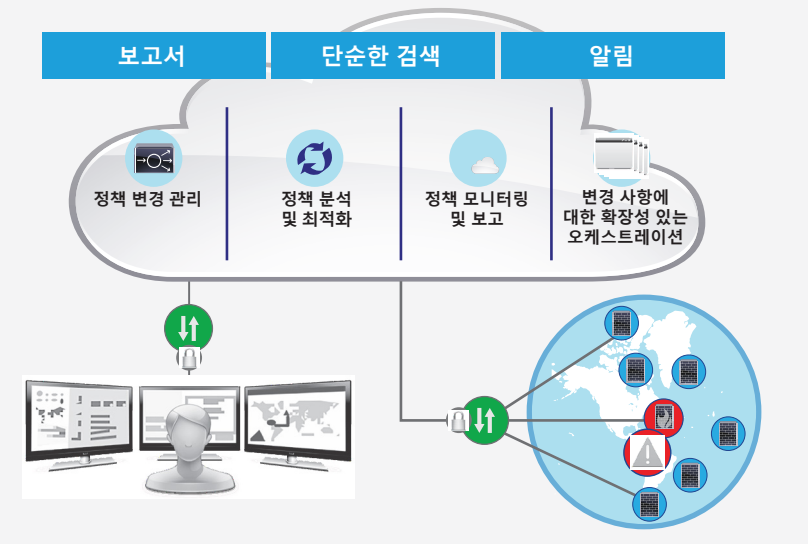
Cisco Defense Orchestrator에 대한 자세한 내용은 cisco.com/go/cdo에서 확인하십시오.

Defense Orchestrator의 이점을 직접 경험하고 싶다면 cdosales@cisco.com으로 문의하여 시작하십시오.

보안 유지를 위한 자본 및 리소스 절감

고도의 보안성, 높은 신뢰성, 지속적 가용성, 확장성을 갖춘 다중 테넌트 클라우드 솔루션을 이용하여 어디에서든 관리할 수 있습니다. 더 적은 리소스와 시간을 투자하여 보안 상태를 강화하고 유지함으로써 다른 우선순위를 처리할 여유를 확보합니다.

그림 1. Cisco Defense Orchestrator의 주요 기능



기능	설명
디바이스 온보딩	온라인과 오프라인에서 관리되는 디바이스에 연결하는 매우 안전한 방법을 다양하게 사용
객체 및 정책 분석	디바이스 전반에 걸쳐 정책 및 객체 레벨에서 중복 또는 사용하지 않은 정책, 일관되지 않은 규칙 또는 일관되지 않은 네트워크 객체 등의 문제 탐지 및 치료
애플리케이션, URL, 악성코드 및 위협 정책 분석	애플리케이션 또는 대상 호스트 이름별로 트래픽을 차단하여 레이어 7 보호 관리
보안 템플릿	새로운 디바이스에 손쉽게 배포하기 위한 템플릿을 설계 및 관리
단순한 검색	모든 객체 이름, ACL 이름, 네트워크 또는 애플리케이션 정책 요소를 검색하여 어떻게 디바이스 유형 전반에 정책이 시행되는지 확인
영향 변경 모델링	비프로덕션 환경에 변경 사항을 적용하여 배포하기 전 정책 변경의 영향 파악
OOB(Out-of-Band) 알림	정책 변경 시 자동 알림 수신
보고서	주요 애플리케이션, 대상, 범주, 공격 및 위험에 대한 보고서를 이용하여 정책 효과 추적

Cisco Defense Orchestrator 사용 사례

한 국내 소매 기업은 기업 운영 부서 간의 백홀링 없이 전 세계에 펼쳐져 있는 수천 개의 리테일 지사에 일관된 정책 구조를 적용하기 위한 방법의 개선이 필요했습니다.

이 기업은 엔드 투 엔드 가시성 및 제어 기능을 강화하기 위해 차세대 기능으로 전환하기를 원했습니다. 이에 따라 간단한 관리 프로세스를 통해 네트워크 전반의 포트 및 애플리케이션을 지원하는 템플릿을 만들었습니다.