Cisco Defense Orchestrator

Cisco ® Defense Orchestrator는 네트워크 운영 부서가 Cisco 보안 디바이스 전반의 보안 정책을 관리하여 보안 상태를 설정하고 유지할 수 있도록 지원하는 클라우드 기반 보안 정책 관리 제품입니다. 지속적 가용성, 높은 안정성, 뛰어난 확장성을 제공하는 다중 테넌트 클라우드 플랫폼입니다.

제품 개요

Defense Orchestrator는 Cisco ASA(Adaptive Security Appliances), Cisco Adaptive Security Virtual Appliance, Cisco ASA with FirePOWER™ Services, NGFW(Cisco Firepower™ Next-Generation Firewalls) 및 OpenDNS의 보안 정책 컨피그레이션을 분석합니다. Defense Orchestrator는 정책 불일치를 식별 및 해결하고, 정책 변경을 모델링하여 변경으로 인한 영향을 확인하고, 정책 변경을 오케스트레이션하여 정책 일관성을 달성하고 보안 상태의 명확성을 유지합니다.

Defense Orchestrator는 클라우드 기반 플랫폼입니다. Defense Orchestrator는 설정 시간을 줄이고, 자본 지출을 운영 비용으로 전환하고, 일상 운영 문제를 줄여줍니다. 간편하고 일관성 있고 매우 안전한 방식으로 보안 정책을 적용하여, 비용을 절감하고 가치를 빠르게 전달합니다.

그림 1은 Defense Orchestrator의 이해하기 쉬운 인터페이스를 보여줍니다.

그림 1. Top-N 보고서에서 애플리케이션 보호 정책, 객체 및 가시성을 보여주는 화면

보안 상태(Security Posture) 일관성

보안 관리 작업은 복잡합니다. 위협 대응 능력은 개별 제품 및 서비스의 뛰어난 설계 및 훌륭하게 수립된 방어 기능을 기반으로 합니다. 최근 위협은 네트워크 보안 분석이 보안 정책을 비롯하여 다양한 요인을 포함해야 함을 보여줍니다. 지속적 분석, 설계 및 구현을 지원하는 프로그램은 적절한 보안 상태를 유지하는 데 있어 필수입니다.

Defense Orchestrator는 보안 컨피그레이션을 분석하여 보안 정책 및 객체의 잘못된 컨피그레이션을 찾아냅니다. 또한 네트워크 운영 부서가 계획되거나 계획되지 않은 변경을 관리하고, 변경 사항을 배포하기 전 변경의 영향을 모델링하고, 올바른 변경 사항이 디바이스에 적용되었는지 확인하도록 지원합니다. 게다가 보안 정책을 분석하여 여러 디바이스의 보안 정책 컨피그레이션에서 이상 징후를 식별합니다. 이러한 분석을 통해 교정이 필요할 수도 있는 일관되지 않은 규칙을 강조하여 표시합니다. 고객은 정책 및 객체 차원에서 문제를 해결할 수 있습니다. Gold 정책 컨피그레이션을 이용하면 여러 위치(예: 매장, 호텔 또는 사무실)를 보유한 고객은 올바른 정책 컨피그레이션이 보안 디바이스 및 서비스에 적용되고 있다고 안심할 수 있습니다.

엔드 투 엔드 정책 관리

Defense Orchestrator는 디바이스와 디바이스 유형 전반에 대해 보안 정책 컨피그레이션을 위한 단일창 방식을 제공합니다. 또한 네트워크 객체, 애플리케이션, 애플리케이션 범주, URL, URL 범주 및 작업을 요약하여 서로 다른 디바이스의 정책을 일관되고 쉽게 관리할 수 있습니다. 관리자는 구내 또는 원격에서 일하는 직원의 일관된 글로벌 보안 상태를 설계하고 시행할 수 있으며 위협에 빠르게 대응할 수 있습니다. 이러한 기능 덕분에 각 보안 제품 및 해당 컨피그레이션에 대해 심층적인 지식이 필요하지 않습니다.

빠른 가치 실현 시간

Defense Orchestrator는 설정이 쉽고 구성이 빠른 클라우드 기반 플랫폼입니다. 추가 자본 지출, 공간 또는 애플리케이션 관리가 필요하지 않습니다. Defense Orchestrator는 컨피그레이션의 직접 연결 또는 오프라인 업로드를 통해 온프레미스 또는 클라우드 서비스 Cisco 보안 제품을 즉각적으로 관리합니다. 보안 정책을 간단하고 일관되고 안전하게 시행하여, 일상 운영 문제를 줄입니다. 고객은 보안 정책 시행에 대한 가치를 빠르게 얻습니다.

기능 및 이점

Defense Orchestrator를 통해 보안 정책을 관리하면 여러 이점을 얻을 수 있습니다.

쉬운 온보딩: Defense Orchestrator로 온프레미스 또는 클라우드 서비스 Cisco 보안 제품을 즉시 온보딩할 수 있습니다. 디바이스에 직접 연결하거나 컨피그레이션을 오프라인으로 업로드하십시오. 디바이스 및 Orchestrator 간의 통신은 매우 안전합니다.

엔드 투 엔드 정책 분석: Defense Orchestrator는 디바이스와 심지어 물리적 인프라 및 클라우드 인프라 전반에 대해 보안 정책 컨피그레이션을 위한 단일창 방식을 제공합니다. 보안 정책 및 객체에 대한 잘못된 컨피그레이션을 찾아내고 계획되거나 계획되지 않은 변경을 관리합니다. 엔드 투 엔드 정책 분석으로 디바이스별 보안 컨피그레이션의 전문가가 필요하지 않습니다.

모델링: Defense Orchestrator를 통해 고객은 안전한 "Gold" 정책 템플릿을 생성할 수 있습니다. 비즈니스 성장에 맞게 일관된 보안 컨피그레이션을 쉽게 시행할 수 있습니다. 디바이스에 컨피그레이션을 배포하기 전에 변경 사항의 영향을 모델링할 수 있습니다.

치료: 컨피그레이션 변경이 모델링되면 고객은 올바른 변경 사항이 디바이스에 적용되었는지 확인할 수 있습니다. 해당 변경 사항이 변경 관리 프로세스에 따라 실시간 또는 오프라인으로 배포되었는지 확실히 알 수 있습니다. Defense Orchestrator에서 관리하는 모든 보안 제품에 대해 일관된 보안 상태를 시행하고 유지할 수 있습니다.

가상화: Defense Orchestrator는 웹 정책 시행의 효과를 판단하기 위해 주요 애플리케이션, 상위 대상, 상위 범주, 상위 공격 및 상위 위험에 대한 집계 정보를 시각화할 수 있습니다.

표 1에서 동급 최고인 Defense Orchestrator의 기능과 이점을 살펴볼 수 있습니다.

표 1. 기능 및 이점

기능	이점
Cisco 보안 제품 관리	다음과 같은 Cisco 보안 환경에 대한 중앙 집중식 보안 정책 관리가 이루어집니다. • Cisco ASA 5500 Series 및 5500-X Series Adaptive Security Appliances • Cisco ASA with FirePOWER Services • Cisco Firepower NGFW • OpenDNS Umbrella
클라우드 플랫폼	손쉬운 설정 및 빠른 컨피그레이션. 추가 자본 지출, 공간 또는 애플리케이션 관리가 필요 없음.
신속한 온보딩	간소화된 컨피그레이션 및 간단한 초기 보안 관리 설정. 디바이스 정보를 컨피그레이션 파일에서 가져오거나 디바이스 자체에서 검색할 수 있습니다.
매우 안전한 연결	디바이스 및 Defense Orchestrator 간의 안전한 통신을 통해 모든 데이터 트랜잭션에 지속적인 보호 제공.
객체 및 정책 분석	여러 디바이스에서 잘못된 컨피그레이션을 찾아내어 계획되거나 계획되지 않은 변경을 관리할 수 있는 기능. 단일창은 엔드 투 엔드 정책 컨피그레이션에 사용됩니다.
템플릿	안전한 "Gold" 정책 컨피그레이션으로 일관된 보안 시행. 여러 분산된 위치(예: 매장, 호텔 또는 사무실)를 보유한 고객은 올바른 정책 컨피그레이션이 보안 디바이스 및 서비스에 적용되고 있다고 안심할 수 있습니다.
설정된 프로세스에 따라 변경 사항 배포	변경 사항을 모델링하고, 해당 변경의 영향을 확인하고, 변경 관리 프로세스마다 디바이스에 대한 변경을 내보내거나 작성할 수 있습니다.
FirePOWER Services와 FTD(Firepower Threat Defense)를 쉽게 지원	차세대 방화벽 및 애플리케이션 보호에 대한 간단한 경로.
OOB(Out of Band) 탐지 및 알림	OOB(Out of Band) 변경이 발생하면 알림을 받아 일관된 보안 상태를 유지할 수 있는 기능.
단순한 검색	정책이 디바이스와 디바이스 유형에 대해 어떻게 시행되는지 찾기 위해 모든 객체 이름, ACL 이름, 네트워크 또는 애플리케이션 정책 요소를 검색할 수 있는 기능.
애플리케이션 보안의 글로벌 시행	구내 또는 원격에서 일하는 직원의 일관된 글로벌 보안 상태를 설계하고 시행할 수 있는 기능. 위협에 빠르게 대응할 수 잇는 기능. Google 같은 검색 기능을 통해 디바이스와 디바이스 유형에 대한 애플리케이션 보호 시행 상태를 빠르게 표시할 수 있습니다.
보고서	웹 정책 시행의 효과를 판단하기 위해 주요 애플리케이션, 상위 대상, 상위 범주, 상위 공격 및 상위 위험에 대한 집계 정보의 쉬운 시각화.

플랫폼 지원 매트릭스

Defense Orchestrator는 ASA, ASA with FirePOWER Services, Firepower NGFW 및 OpenDNS에 대한 보안 정책을 관리합니다.

ASA with FirePOWER Services와 Firepower NGFW 정책 관리에는 ASA 방화벽, 애플리케이션 시각화 및 제어, URL 필터링, NGIPS(Next-Generation Intrusion Prevention System) 및 Cisco AMP(Advanced Malware Protection)가 포함됩니다. 아래의 표 2에서는 Cisco ASA, Cisco ASA with FirePOWER Services 및 Cisco FirePOWER Threat Defense 소프트웨어 지원 매트릭스가 자세히 나와 있습니다.

표 2. Defense Orchestrator에 대한 Cisco ASA, ASA with FirePOWER Service 및 FTD(Firepower Threat Defense) 지원

제품	ASA 소프트웨어 버전	ASA 소프트웨어 버전의 FirePOWER Services	Firepower Threat Defense 소프트웨어 버전
ASA 5505, 5510, 5520, 5540, 5550	8.4 이상	해당 없음	해당 없음
ASA 5506-X, ASA 5508-X, ASA5585-X	9.2.2 이상	5.4.1 이상	6.1.x 이상
ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X	9.2.2 이상	6.0.0 이상	6.1.x 이상
ASA 5585-10, 5585-20, 5585-40, 5585-60	9.2.2 이상	해당 없음	해당 없음
Firepower 4110, Firepower 4120, Firepower 4140, Firepower 4150	9.6.x 이상	해당 없음	6.1.x 이상
Firepower 9300	9.6.x 이상	해당 없음	6.1.x 이상

주문 정보

제품을 주문하려면 Cisco 주문 홈 페이지를 방문하십시오.

추가 정보

Defense Orchestrator에 대한 추가 정보는 http://www.cisco.com/go/cdo를 참조하시기 바랍니다.

Defense Orchestrator 데모의 경우, cdosales@cisco.com으로 문의하십시오.

미주 지역 본부
Cisco Systems, Inc.
캘리포니아 주 산호세

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

Printed in USA C78-736847-00 06/16