소개

Security Cloud Control Firewall Management (이전 Cisco Defense Orchestrator)는 시스코 방화벽 및 기타 디바이스에서 정책을 간소화하고 통합하는 클라우드 기반 보안 정책 플랫폼입니다. 정책 일관성을 간소화하고 직관적이면서도 고급 인터페이스를 제공하며, 여러 디바이스 관리자 간 구성 변경 사항을 조정합니다.

Security Cloud Control Firewall Management 정보

Security Cloud Control Firewall Management (이전 Cisco Defense Orchestrator)는 Cisco 방화벽 및 기타 디바이스에서 정책을 간소화하고 통합하는 클라우드 기반 보안 정책 관리자입니다. 방화벽 및 디바이스는 Security Cloud Control의 제품 아래에 나열된 방화벽에서 관리됩니다.

불일치 사항을 식별하고 이를 수정할 수 있는 툴을 제공하여 보안 정책을 최적화할 수 있도록 지원합니다. 개체 및 정책을 공유하고 설정 템플릿을 만드는 방법을 제공하여 디바이스 전반에 걸쳐 정책 일관성을 유지합니다.

Security Cloud Control이 ASDM(Adaptive Security Device Manager)와 같은 로컬 디바이스 관리자와 공존하기 때문에, Security Cloud Control 및 다른 관리자에 의해 수행된 구성 변경 사항을 추적한 후 관리자 간 차이를 조정합니다.

Security Cloud Control은 다양한 디바이스를 한 곳에서 관리할 수 있는 직관적인 사용자 인터페이스를 제공합니다. 기존 CLI 인터페이스에 몇 가지 개선 사항이 추가되어 고급 사용자가 관리 효율성을 더욱 높일 수도 있습니다.

또한 온프레미스 또는 클라우드 제공 Firewall Management Center에 위협 방어 디바이스를 신속하게 온보딩할 수 있도록 안내하는 "Day 0" 경험을 제공합니다. 또한 여러분이 활용할 수 있는 다른 주요 기능들을 제시하고, 이를 활성화하고 구성하는 데 도움을 줍니다.

디바이스 온보딩

디바이스를 온보딩하기 전에 설치 마법사를 성공적으로 완료하고 디바이스에 라이선스를 부여했는지 확인합니다. 그런 다음 Security Cloud Control의 온보딩 마법사를 사용하여 디바이스를 온보딩합니다. Security Cloud Control는 대규모 구축을 손쉽게 관리할 수 있습니다.

디바이스 및 서비스 온보딩을 참조하십시오.

참고 디바이스를 Security Cloud Control 테넌트에 온보딩하면 한 Security Cloud Control 테넌트 간에 디바이스를 마이그레이션할 수 없습니다. 디바이스를 새 테넌트로 이동하려면 해당 디바이스를 새 테넌트에 다시 등록해야 합니다.

Security Cloud Control이 지원하는 디바이스의 전체 목록은 지원되는 디바이스, 소프트웨어 및 하드웨어를 참조하십시오.

Cisco 온라인 개인정보 보호정책

Cisco Systems, Inc. 및 자회사("Cisco"로 통칭)에서는 개인 정보를 보호하고 사용자가 Cisco 웹사이트에서 그리고 시스코 제품 및 서비스("솔루션")의 사용에서 유익한 경험을 할 수 있도록 최선을 다하고 있습니다. Cisco 온라인 개인정보 보호정책을 주의 깊게 읽고 Cisco에서 개인 정보를 수집, 사용, 공유 및 보호하는 방법을 명확하게 이해하십시오.

Security Cloud Control을 사용하여 SSH 디바이스 관리

일반 SSH 인터페이스를 통해 관리되며 Cisco IOS를 실행하지 않는 기타 SSH 지원 디바이스. SSH를 통해 접근 가능한 Linux 서버, Unix 기반 시스템 또는 서드파티 네트워크 어플라이언스와 같은 디바이스. 일반적인 SSH는 네트워크 디바이스를 원격으로 안전하게 접근하고 관리하기 위한 표준 방법으로 보안 셸(SSH) 프로토콜을 사용하는 것을 의미합니다. 이 디바이스는 SSH를 통해 액세스 가능하며, 디바이스의 IP 또는 FQDN, SSH 포트, 로그인 자격 증명을 지정하여 Security Cloud Control을 통해 온보딩 및 관리할 수 있습니다.

이러한 디바이스에 대해 지원되는 기능은 다음과 같습니다.

- SSH 디바이스를 온보딩합니다. SSH 디바이스에 저장된 높은 권한을 가진 사용자의 사용자 이름과 암호를 사용하여 디바이스를 온보딩할 수 있습니다.
- 디바이스의 구성 파일 보기. 디바이스 구성 파일을 볼 수 있습니다.
- 디바이스에서 정책 및 구성 변경 사항을 검토합니다. SSH 디바이스에서 구성 파일을 읽으면 해당 파일이 Security Cloud Control의 데이터베이스에 저장됩니다.
- 대역 외 변경 탐지. 충돌 탐지를 활성화한 경우 Security Cloud Control는 10분마다 디바이스의 구성 변경 사항을 확인합니다. 변경 사항이 있는 경우 디바이스의 상태가 Conflict Detected(충돌 탐지됨)로 변경되며, 변경 충돌을 해결할 수 있습니다.
- Security Cloud Control 명령줄 인터페이스 툴 사용. Security Cloud Control의 명령줄 인터페이스를 통해 디바이스에 모든 SSH 디바이스 명령을 실행할 수 있습니다.

- 개별 CLI 명령 및 명령 그룹을 편집 및 재사용 가능한 "매크로"로 전환할 수 있습니다. Security Cloud Control에서 제공하는 시스템 정의 매크로를 사용하거나 자주 수행하는 작업에 대해 자신만의 매크로를 만들 수 있습니다.
- SSH 핑거프린트 변경 사항 탐지 및 관리. 디바이스의 자격 증명 또는 속성이 변경되어 SSH 핑거프린트가 변경되는 경우 해당 Security Cloud Control는 변경 사항을 감지하고 새 핑거프린트를 검토하고 수락할 수 있는 기회를 제공합니다.
- 변경 로그. 변경 로그는 사용자가 SSH 디바이스에 실행하는 모든 명령을 캡처합니다.

Security Cloud Control 대시보드

Security Cloud Control 대시보드는 다양한 범주에 걸쳐 조직 수준의 세부 정보을 모니터링하고 관리하기 위한 중앙 허브입니다. 로그인하면 중요한 인사이트와 보안 및 운영 효율성 최적화하기 위한 작업을 제공하는 맞춤형 대시보드에 액세스할 수 있습니다.

대시보드 사용자 맞춤화

표시되는 위젯을 맞춤 설정하여 대시보드를 특정 요구 사항에 맞게 조정합니다.

1. **Home** 페이지에서 **Customize(**맞춤화**)**를 클릭합니다.
2. 대시보드에 표시할 위젯을 선택하거나 선택을 해제합니다.
3. 위젯을 끌어다 놓아 원하는 대로 정렬할 수 있습니다.

상위 정보

이 섹션에서는 다양한 테넌트 수준 메트릭에 대한 상세한 인사이트를 제공합니다. 활성화된 경우 다음 위젯을 볼 수 있습니다.

- **Configuration States(**구성 상태**)**: 사용자의 디바이스에 설정된 구성과 Security Cloud Control에서 유지 관리하는 구성 간의 불일치를 나타냅니다. 이 비교를 통해 존재할 수 있는 불일치나 충돌을 식별하는 데 도움이 됩니다.

  자세한 내용은 디바이스 관리를 참조하십시오.

- **Change Log Management(**변경 로그 관리**)**: 정확한 운영 제어를 위해 변경 로그를 관리하는 데 도움이 됩니다. 위젯에 **Completed(**완료됨**)** 및 **Pending(**보류 중**)** 변경 로그가 표시됩니다.

  자세한 내용은 Change Logs(변경 로그)를 참조하십시오.

- **RA VPN Sessions(RA VPN** 세션**)**: 원격 액세스 VPN 세션을 모니터링할 수 있습니다.

  자세한 내용은 RA VPN 세션을 참조하십시오.

- **Overall Inventory(**전체 재고 목록**)**: 모든 디바이스의 상태를 모니터링할 수 있습니다. **Issues(**문제**)**, **Pending Actions(**보류 중인 작업**)**, **Other(**기타**)**, **Online(**온라인**)**으로 분류된 총 디바이스 수와 하드웨어 지원 기간이 가까워지거나 만료된 위젯의 총 수가 표시됩니다.

  자세한 내용은 모든 디바이스를 참조하십시오.

- **Site-to-Site VPN(**사이트 간 **VPN)**: 사이트 간 VPN 연결을 관리하고 평가하는 데 도움이 됩니다. 위젯에 총 VPN 터널 수와 **Active(**활성**)** 및 **Idle(**유휴**)**의 비율이 표시됩니다.

  자세한 내용은 사이트 간 VPN을 참조하십시오.

- 어카운트 및 자산:
  - 멀티 클라우드 어카운트 및 리소스를 효과적으로 추적하고 관리할 수 있습니다. 여기에서 Multicloud Defense 컨트롤러를 실행할 수 있습니다.
  - **+Add Account(+**어카운트 추가**)**를 클릭하여 새 어카운트을 추가합니다.

  자세한 내용은 Multicloud Defense Controller를 참조하십시오.

- **Top Risky Destinations(**상위 위험한 대상**)**: 액세스 권한이 부여된 상위 위험한 대상을 식별하고 모니터링하는 데 도움이 됩니다. 위젯은 애플리케이션 및 URL 범주를 나열하며, 지난 90일, 60일 또는 30일 동안의 데이터를 필터링할 수 있습니다. 허용된 트래픽(기본값)과 차단된 트래픽 사이에서 필터링할 수 있습니다.

- **Top Intrusion and Malware Events(**상위 침입 및 멀웨어 이벤트**)**: 상위 침입 및 멀웨어 이벤트를 모니터링하고 대응할 수 있습니다. 위젯은 침입 이벤트와 멀웨어이벤트를 표시하며, 지난 90일, 60일, 30일 동안의 데이터를 필터링할 수 있습니다. 허용된 이벤트(기본값)와 차단된 이벤트 사이에서 필터링할 수 있습니다.

발표

최신 Security Cloud Control 기능 및 업데이트를 보려면 알림 아이콘 클릭합니다. 목록에 있는 항목에 대한 추가 정보가 필요할 경우 관련 문서 링크가 제공됩니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.