2021의 주요 기능

이 문서에서는 2021년에 Cisco Defense Orchestrator에 추가된 몇 가지 기능에 대해 설명합니다.

2021년 12월

2021년 12월 9일

Firepower Threat Defense, 버전 **7.1**에 대한 **CDO** 지원

CDO는 이제 FTD(Firepower Threat Defense) 버전 7.1 디바이스를 지원합니다. 다음은 CDO가 제공하는 지원 측면입니다.

- Firepower Threat Defense 버전 7.1을 실행하는 지원되는 물리적 또는 가상 디바이스를 온보딩합니다.
- Firepower Threat Defense 버전 6.4 이상에서 버전 7.1로 업그레이드합니다.
- 기존 Firepower Threat Defense 기능을 지원합니다.

다음 주의 사항은 Firepower Threat Defense, 버전 7.1 지원에 적용됩니다.

- CDO는 현재 버전 7.1을 실행하는 Firepower Threat Defense 디바이스 백업을 지원하지 않습니다. 이 기능에 대한 지원은 Firepower Threat Defense, 버전 7.1의 첫 번째 유지 보수 릴리스에서 제공될 예정입니다.
- CDO는 Firepower Threat Defense, 버전 7.1 릴리스에 도입된 기능을 지원하지 않습니다.

CDO가 현재 지원하는 FTD 기능에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리를 참조하십시오.

새 **CDO** 문서 플랫폼

온라인 도움말

- 모든 디바이스를 설명하는 콘텐츠를 한 곳에서 확인할 수 있습니다.
- 상황별 도움말.
- 검색하는 동안 콘텐츠 일치 항목이 발견되었습니다.
- 목차에서 강조 표시된 검색 결과는 더 큰 컨텍스트로 정보를 제공합니다.

Cisco.com에서 유지 관리되는 콘텐츠

- Cisco.com의 가용성은 모든 Cisco 설명서를 하나의 사이트에 배치합니다.
- 디바이스별 구성 가이드를 사용하면 정보를 더 쉽게 찾을 수 있습니다.
- Cisco Defense Orchestrator의 새로운 기능에서는 CDO에서 사용 가능한 최신 기능에 대해 계속 설명합니다.

2021년 11월

2021년 11월 11일

새로운 **SASE** 터널 기능

이제 CDO UI에서 읽혔거나 CDO UI를 통해 생성된 SASE 터널을 편집할 수 있습니다. 이 기능은 Umbrella 조직과 이미 CDO에 온보딩된 ASA 피어 디바이스 간의 터널만 지원합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "SASE 터널 편집"을 참조하십시오.

2021년 10월

2021년 10월 21일

향상된 **SecureX** 통합

아직 CDO 테넌트와 SecureX를 연결하지 않은 사용자를 위해 CDO는 이제 SecureX와의 간소화된 통합을 제공합니다. 이 프로세스를 통해 CDO 테넌트를 SecureX 조직에 빠르고 안전하게 연결하고 클릭 한 번으로 CDO 모듈을 SecureX 대시보드에 추가할 수 있습니다. SecureX 조직이 없는 경우 이 프로세스 중에 조직을 생성할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "SecureX와 CDO 통합"을 참조하십시오.

CDO 저장소에서 **AnyConnect** 패키지 업로드

이제 CDO는 CDO 저장소에서 ASA 및 FTD 디바이스로의 AnyConnect 패키지 업로드를 지원합니다.

Remote Access VPN Configuration(원격 액세스 VPN 구성) 마법사는 운영 체제별로 AnyConnect 패키지를 제공하며, 이러한 패키지를 선택하여 디바이스에 업로드할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "CDO 저장소에서 AnyConnect 패키지 업로드" 및 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 디바이스에서 AnyConnect 소프트웨어 패키지 관리"를 참조하십시오.

2021년 9월

2021년 9월 16일

서비스 통합을 통한 **CDO** 알림

이제 CDO 알림이 Webhook과 통합됩니다. Notification Settings(알림 설정) 페이지에서 선택한 알림은 선택한 애플리케이션 또는 서비스 통합으로 전송됩니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "CDO 알림에 대한 서비스 통합 활성화"를 참조하십시오.

Cisco Security Analytics and Logging을 위한 **Cisco Secure Firewall Cloud Native** 지원

Cisco Security Analytics and Logging이 Cisco Security Analytics and Logging에서 이벤트 로깅을 지원하도록 크게 확장되었습니다.

Secure Firewall Cloud Native 로깅: Security Analytics and Logging(SAL SaaS)은 이제 모든 Secure Firewall Cloud Native 디바이스에서의 로깅을 지원합니다. 사용자는 Secure Firewall Cloud Native 이벤

트를 시스템 로그 형식, NetFlow NSEL(Security Event Logs) 형식 또는 둘 다로 Cisco Cloud에 저장하고 Cisco Secure Cloud Analytics를 사용하여 분석할 수 있습니다. 로깅 분석을 활성화하려는 고객은 상위 계층 SAL 라이선스에 필요한 텔레메트리를 제공하기 위해 NSEL 로그를 활성화해야 합니다.

- 트래픽 분석 - SAL의 트래픽 분석을 통해 Secure Firewall Cloud Native 로그를 실행할 수 있으며 CDO에서 Cisco Secure Cloud Analytics를 교차 실행하여 관찰 및 알림을 검토할 수 있습니다. 시스템 로그 이벤트를 로깅하는 Cloud Native 고객만 트래픽 분석을 활성화하려면 NSEL 로그로 전환해야 합니다.
- Logging Analytics and Detection 및 Total Network Analytics Detection - Logging Analytics and Detection 및 Total Network Analytics Detection 라이선스를 취득한 고객은 분석을 위해 Secure Cloud Analytics 포털을 프로비저닝하고 사용할 수 있습니다. Secure Cloud Analytics 탐지 항목에는 SAL 사용자가 Secure Cloud Analytics 핵심 기능의 일부로 사용할 수 있는 기타 탐지 항목 외에도 방화벽 로깅 데이터를 사용하여 특별히 활성화된 관찰 및 알림이 포함됩니다. 기존 기록 및 트러블슈팅 라이선스 보유자는 30일 동안 약정 없이 상위 라이선스의 탐지 기능을 테스트할 수 있습니다.
- 무료 평가판: 이 양식을 작성하여 모든 라이선스에 대해 약정 없는 30일 SAL 평가판을 시작할 수 있습니다. 이 평가판에는 클라우드로 데이터를 내보내는 데 필요한 최소 온프레미스 커넥터 집합만 필요합니다. 이 평가판을 사용하여 SAL 기능을 평가하고 프로덕션 환경을 지원하는 데 필요한 데이터 볼륨을 예측할 수 있습니다. 이는 SAL 라이선스에 대한 적절한 일일 볼륨을 구매하기 위한 선행 단계입니다. 이를 위해 SAL 평가판은 대부분의 사용자 볼륨에 대한 데이터를 조절하지 않습니다. 또한 예상 툴을 사용하면 SAL 일일 볼륨을 예측할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 "Cisco Security Analytics 및 로깅"을 참조하십시오.

2021년 8월

2021년 8월 26일

CDO 및 Umbrella 통합

이제 CDO에서 Umbrella 통합을 지원합니다. Umbrella 조직을 온보딩하고 Umbrella와 ASA 디바이스 간에 존재하는 SASE 터널을 보고 관리하고 생성할 수 있습니다. ASA 디바이스는 사용하기 쉬운 보안을 위해 중앙 집중식 관리를 제공하는 Umbrella의 SIG 터널 및 검사를 활용합니다.

Umbrella 조직을 온보딩할 때는 해당 조직과 연결된 ASA 디바이스도 온보딩하는 것이 좋습니다.

Umbrella란 무엇이며 CDO와 Umbrella와 통신하는 방법에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리를 참조하십시오.

2021년 8월 13일

FTD RA VPN에 **LDAP**를 사용하는 **Duo** 구성 지원

이제 FTD 원격 액세스 VPN 연결에 LDAP를 사용하여 Duo 2단계 인증을 구성할 수 있습니다.

기본 인증 소스로 Microsoft AD(Microsoft Active Directory) 또는 RADIUS 서버를 함께 사용하여 Duo LDAP 서버를 보조 인증 소스로 사용합니다. Duo LDAP를 사용하는 경우 보조 인증에서는 Duo 암호, 푸시 알림, 전화 통화 또는 SMS를 사용하여 기본 인증을 검증합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "LDAP를 사용한 Duo 이중 인증"을 참조하십시오.

2021년 7월

2021년 7월 8일

ASA용 디지털 인증서 관리 지원

이제 CDO가 ASA 디바이스에서 디지털 인증서를 관리합니다. ID 인증서 및 신뢰할 수 있는 CA 인증서와 같은 디지털 인증서를 신뢰 지점 개체로 추가하고 하나 이상의 매니지드 ASA 디바이스에 설치할 수 있습니다. 설치된 ID 인증서를 내보내 다른 ASA에서 신뢰 지점 구성을 수동으로 복제할 수도 있습니다.

다음 형식으로 ID 인증서를 업로드하거나 생성할 수 있습니다.

- 암호가 있는 PKCS12 파일
- 자체 서명 인증서
- 인증 기관이 서명한 CSR(Certificate Signing Request)

원격 액세스 VPN은 디지털 인증서를 사용하여 ASA 및 AnyConnect 클라이언트를 인증하여 보안 VPN 연결을 설정합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 인증서 관리"를 참조하십시오.

RA VPN ASA 및 **FTD**에 대한 **AnyConnect** 모듈 지원

이제 CDO는 ASA 및 FTD 디바이스에서 AnyConnect 모듈 관리를 지원합니다.

참고 이 기능은 소프트웨어 버전 6.7 이상을 실행하는 FTD에서 지원됩니다.

RA VPN 그룹 정책 생성의 일부로 이제 사용자가 Cisco AnyConnect VPN Client를 다운로드할 때 다운로드 및 설치할 다양한 선택적 모듈을 구성할 수 있습니다. 이러한 모듈은 웹 보안, 악성코드 방지, 네트워크 외부 로밍 방지 등의 서비스를 제공할 수 있습니다.

AnyConnect 프로파일 편집기에서 생성되고 AnyConnect 파일 개체로 CDO에 업로드된 맞춤형 구성이 포함된 프로파일과 각 모듈을 연결할 수 있습니다.

프로파일을 업로드하고 그룹 정책에 할당하는 방법에 대한 자세한 내용은 *Cisco Defense Orchestrator를 사용하여 FTD 관리*의 "RA VPN AnyConnect 클라이언트 프로파일 업로드" 및 "새 FTD RA VPN 그룹 정책 생성"을 참조하십시오.

2021년 7월 1일

Snort 3 지원

이제 CDO는 버전 6.7 이상을 실행하는 FTD 디바이스에 대해 Snort 3 처리 엔진을 지원합니다. Snort 엔진은 새 Snort 규칙을 자동으로 업데이트하여 디바이스가 최신 취약점을 준수하도록 합니다. Snort 2에서 Snort 3으로 독립형 업그레이드를 수행하거나 디바이스 시스템과 Snort 엔진을 동시에 업그레이드하여 업그레이드 경험을 간소화할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator를 사용하여 FTD 관리*의 "Snort 3.0으로 업그레이드"를 참조하십시오.

맞춤형 침입 방지 시스템 정책

CDO는 이제 버전 6.7 이상을 실행하는 FTD 디바이스에 대해 Snort 3 및 맞춤형 IPS(Intrusion Prevention System) 정책을 지원합니다. 개선된 Snort 3 처리 엔진을 사용하면 Cisco Talos Intelligence Group(Talos)에서 제공하는 규칙을 사용하여 IPS 정책을 생성하고 사용자 지정할 수 있습니다. 모범 사례는 제공된 Talos 정책 템플릿을 기반으로 고유한 정책을 생성하고 규칙 작업을 조정해야 하는 경우 변경하는 것입니다.

참고 업그레이드에 따라 규칙이 구성되는 방식이 변경될 수 있으므로 Snort 3으로 또는 Snort 3에서 업그레이드할 때 차이점과 제한 사항에 유의해야 합니다.

자세한 내용은 *Cisco Defense Orchestrator로 FTD 관리*의 "맞춤형 Firepower 침입 방지 시스템 정책"을 참조하십시오.

2021년 6월

2021년 6월 17일

Firepower Threat Defense, 버전 **7.0**에 대한 **CDO** 지원

이제 CDO에서 FTD(Firepower Threat Defense), 7.0을 지원합니다. FTD 7.0을 실행하는 FTD 디바이스를 온보딩하거나 CDO를 사용하여 해당 버전으로 디바이스를 업그레이드할 수 있습니다. CDO는 DNS 트래픽에 대한 새로운 평판 적용 기능 외에도 기존 FTD 기능을 계속 지원합니다. 이 기능은 액세스 제어 정책 설정입니다. URL 필터링 범주 및 평판 규칙을 DNS 조회 요청에 적용하려면 이 옵션을 활성화합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "액세스 정책 설정 구성"을 참조하십시오.

CDO는 다음 기능을 제한적으로 지원합니다.

- FTDv 계층형 라이선스 지원 - 버전 7.0은 처리량 요구 사항 및 RA VPN 세션 제한을 기반으로 FTDv 장치에 대한 성능 계층형 스마트 라이선스를 지원합니다. 현재 CDO는 계층형 스마트 라이선싱을 완전히 지원하지 않습니다. 계층형 라이선스를 사용하는 FTDv 디바이스를 온보딩할 수 있지만 CDO를 사용하여 라이선스를 업데이트할 수는 없습니다. 디바이스의 Firepower Device Manager를 사용하여 FTDv에서 라이선스를 설치하고 관리합니다.

  자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 라이선싱"을 참조하십시오.

- Scan Interface Support(스캔 인터페이스 지원) - Firepower 4100 Series 또는 9300 Series 디바이스에서 FXOS(Firepower eXtensible Operating System) Chassis Manager를 사용하여 인터페이스를 Firepower 디바이스에 추가하는 경우 FDM에서 해당 인터페이스를 구성한 다음 CDO " 변경 사항 확인"을 클릭하여 구성에서 읽을 수 있습니다.

  자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FXOS를 사용하여 Firepower 디바이스에 추가된 인터페이스 동기화"를 참조하십시오.

- 가상 라우터 지원 - VRF 경로가 CDO에 표시되지 않습니다. 가상 경로를 지원하는 디바이스를 온보딩할 수는 있지만 CDO의 정적 라우팅 페이지에서 가상 경로를 볼 수는 없습니다.

  자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "가상 라우팅 및 포워딩 정보"를 참조하십시오.

- ECMP(Equal Cost Multi Path Routing) - CDO는 ECMP를 사용하는 디바이스를 온보딩하고 구성을 읽을 수 있지만 사용자가 이를 수정할 수는 없습니다. FDM을 통해 ECMP 구성을 생성하고 변경한 다음 CDO로 읽을 수 있습니다.

- 규칙 집합 - FTD 7.0 디바이스에는 규칙 집합을 적용할 수 없습니다.

참고 CDO가 현재 지원하는 FTD 기능에 대한 자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리를 참조하십시오.

2021년 6월 10일

Cisco Secure Firewall Cloud Native 지원

CDO는 이제 Cisco Secure Firewall Cloud Native를 지원합니다. Cisco Secure Firewall Cloud Native는 확장성과 관리성을 위해 Kubernetes(K8s) 오케스트레이션을 사용하여 Cisco의 업계 최고의 보안을 CNFW(클라우드 네이티브 폼 팩터)로 원활하게 확장합니다. Amazon Elastic Kubernetes Service(Amazon EKS)는 AWS 클라우드에서 Kubernetes 애플리케이션을 시작, 실행 및 확장할 수 있는 유연성을 제공합니다. Amazon EKS는 고가용성 및 보안 클러스터를 제공하고 패치, 노드 프로비저닝, 업데이트 등의 주요 작업을 자동화합니다.

CDO는 이 방화벽의 온보딩을 허용하고 완전한 방화벽 관리를 제공합니다.

- AnyConnect RA VPN 세션에서 실시간 및 기록 데이터를 확인합니다.
- 개체를 생성 및 관리하고 네트워크에서 인그레스 및 이그레스 트래픽을 처리하는 다양한 정책에서 사용합니다.
- Kubernetes 명령줄 툴을 사용하여 CDO 외부에서 방화벽에 대한 변경 사항을 인식하고 조정합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리를 참조하십시오.

자세한 내용은 *Cisco Secure Firewall Cloud Native* 개요를 참조하십시오.

향상된 원격 액세스 **VPN** 모니터링

라이브 AnyConnect Remote Access VPN 세션을 모니터링하는 것 외에도 CDO는 이제 지난 3개월 동안 기록된 AnyConnect Remote Access VPN 세션의 기록 데이터를 모니터링할 수 있습니다.

테넌트의 모든 ASA(Adaptive Security Appliance), FTD(Firepower Threat Defense) 및 Cisco SFCN(Secure Firewall Cloud Native) VPN 헤드엔드 전반에서 VPN 세션을 모니터링할 수 있습니다.

다음은 현재 릴리스의 주요 개선 사항입니다.

- CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 볼 수 있도록 직관적인 그래픽 시각적 개체를 표시합니다.
- 라이브 세션 화면에는 CDO 테넌트에서 가장 많이 사용되는 운영 체제 및 VPN 연결 프로파일이 표시됩니다. 또한 평균 세션 기간과 업로드 및 다운로드한 데이터도 표시됩니다.
- 과거 세션 화면에는 지난 24시간, 7일, 30일 동안의 모든 디바이스에 대해 기록된 데이터가 표시되는 막대 그래프가 표시됩니다.

- 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위 등의 기준에 따라 검색 범위를 좁힐 수 있는 새로운 필터링 기능을 제공합니다.

VPN > **Remote Access VPN Monitoring(**원격 액세스 **VPN** 모니터링**)**을 클릭하여 탐색 모음에서 Remote Access VPN Monitoring(원격 액세스 VPN 모니터링) 화면을 엽니다.

새 사용자 역할

이제 CDO는 특정 사용자가 테넌트별로 VPN 세션을 종료할 수 있는 새로운 사용자 역할인 VPN Sessions Manager(VPN 세션 관리자) 사용자 역할을 제공합니다. 이 역할은 VPN 세션을 종료하는 작업만 허용합니다. 이 역할로 지정된 사용자는 읽기 전용 기능으로 제한됩니다.

2021년 5월

2021년 5월 27일

CDO의 향상된 디바이스 알림

이제 CDO 이메일 알림을 구독하고 CDO UI 내에서 최근 알림을 볼 수 있습니다.

테넌트와 연결된 디바이스에서 워크플로우 또는 이벤트 변경이 발생하는 경우 이메일 알림을 수신합니다. 워크플로우 변경 사항에는 구축, 업그레이드 또는 백업이 포함됩니다. 이벤트 변경에는 온라인 또는 오프라인 상태가 되는 디바이스, 충돌 탐지, HA 또는 페일오버 상태, 사이트 간 VPN 연결 상태가 포함됩니다.

참고 이러한 맞춤형 알림은 테넌트와 연결된 모든 디바이스에 적용되며 디바이스별로 적용되지 않습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "알림 설정"을 참조하십시오.

2021년 3월

2021년 3월 25일

APJC에서 **Cisco Security Analytics and Logging** 가용성

이제 새로 가동된 도쿄 데이터 저장소를 통해 아시아(APJC) 지역에서 Cisco Security Analytics and Logging을 사용할 수 있습니다. Security Analytics가 활성화된 계정은 보안 관련 알림을 위해 호주 시드니의 Cisco Secure Cloud Analytics 서비스에 액세스할 수 있습니다. 이를 통해 아시아 지역은 미주 및 EU 지역에서 사용할 수 있는 기능과 동일하게 유지되었습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Cisco Secure Firewall Cloud Native* 관리의 "Cisco Security Analytics and Logging"을 참조하십시오.

2021년 3월 18일

EtherChannel 인터페이스 지원

이제 CDO는 Firepower 버전 6.5 이상을 실행하는 지원되는 모델(예: Firepower 1010, 1120, 1140, 1150, 2110, 2120, 2130, 2140)에서 EtherChannel 인터페이스 구성을 지원합니다. EtherChannel은 포트 링크 집계 기술 또는 포트 채널 아키텍처로, 여러 물리적 이더넷 링크를 그룹화하여 스위치, 라우터 및 서버 간의 링크를 제공하기 위해 하나의 논리적 이더넷 링크를 생성할 수 있습니다.

물리적 포트에 적용하는 구성은 구성을 적용하는 LAN 포트에만 영향을 미칩니다.

디바이스 지원 및 구성 제한 사항에 대한 자세한 내용은 *Cisco Defense Orchestrator*로 *FTD* 관리의 "Firepower 인터페이스 구성에 대한 지침 및 제한 사항"을 참조하십시오.

2021년 3월 15일

ASA 원격 액세스 **VPN** 지원

이제 CDO를 사용하면 ASA(Adaptive Security Appliance) 디바이스에서 RA VPN(Remote Access Virtual Private Network) 구성을 생성하여 원격 사용자가 ASA에 연결하고 원격 네트워크에 안전하게 액세스할 수 있습니다. 또한 ASDM(Adaptive Security Defense Manager) 또는 CSM(Cisco Security Manager)과 같은 다른 ASA 관리 툴을 사용하여 이미 구성된 RA VPN 설정을 관리할 수 있습니다.

AnyConnect는 RA VPN 연결을 제공하는 엔드포인트 디바이스에서만 지원되는 클라이언트입니다.

CDO는 ASA 디바이스에서 RA VPN 기능의 다음 측면을 지원합니다.

- SSL 클라이언트 기반 원격 액세스
- IPv4 및 IPv6 주소 지정
- 여러 ASA 디바이스에서 공유 RA VPN 구성

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA에 대한 원격 액세스 VPN 구성"을 참조하십시오.

ASA 파일 관리 지원

CDO는 ASA 디바이스의 플래시(disk0) 공간에 있는 파일 보기, 업로드 또는 삭제와 같은 기본 파일 관리 작업을 수행하기 위한 파일 관리 툴을 제공합니다. 이 툴을 사용하면 원격 서버에서 URL 기반 파일 업로드를 사용하여 AnyConnect 소프트웨어 이미지, DAP.xml, data.xml, 호스트 스캔 이미지 파일 등의 파일을 단일 또는 여러 ASA 디바이스에 업로드할 수 있습니다.

이 툴을 사용하면 새로 릴리스된 AnyConnect 이미지를 여러 ASA 디바이스에 동시에 업로드할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 파일 관리"를 참조하십시오.

2021년 2월

2021년 2월 11일

다중 보안 디바이스 커넥터 지원

이제 테넌트에 대해 둘 이상의 온프레미스 SDC(Secure Device Connector)를 구축할 수 있습니다. 이를 통해 CDO를 사용하여 더 많은 디바이스를 관리하고 CDO, SDC 및 매니지드 디바이스 간의 통신 성능을 유지할 수 있습니다.

매니지드 ASA, AWS VPC 및 Meraki MX 디바이스를 SDC 간에 이동할 수 있습니다.

SDC가 여러 개 있으면 하나의 CDO 테넌트를 사용하여 격리된 네트워크 세그먼트의 디바이스를 관리할 수도 있습니다. 격리된 네트워크 세그먼트의 모든 매니지드 디바이스를 단일 SDC에 할당하여 이 작업을 수행합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "단일 CDO 테넌트에서 여러 SDC 사용"을 참조하십시오.

2021년 1월

2021년 1월 21일

FMC 개체 읽기

이제 FMC를 CDO에 온보딩하면 CDO가 FMC 매니지드 FTD 디바이스에서 개체를 가져옵니다. CDO로 가져온 개체는 읽기 전용이 됩니다. FMC 개체는 읽기 전용이지만 CDO를 사용하면 FMC에서 관리하지 않는 테넌트의 다른 디바이스에 개체의 복사본을 적용할 수 있습니다. 복사본은 원본 개체에서 연결 해제되므로 FMC에서 가져온 개체의 값을 변경하지 않고 복사본을 편집할 수 있습니다. FMC 개체는 해당 개체 유형을 지원하는 관리하는 모든 디바이스에서 사용할 수 있습니다.

자세한 내용은 Cisco Defense Orchestrator를 사용하여 FMC 관리의 "FMC 개체"를 참조하십시오.

2021년 1월 14일

CLI 명령 결과 내보내기

독립형 디바이스 또는 여러 디바이스에 실행된 CLI 명령의 결과를 쉼표로 구분된 값(.csv) 파일로 내보내 원하는 대로 정보를 필터링하고 정렬할 수 있습니다. 단일 디바이스 또는 여러 디바이스의 CLI 결과를 한 번에 내보낼 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "CLI 명령 결과 내보내기"를 참조하십시오.

FTD 디바이스에 대한 클라우드 서비스 구성

Cisco Success Network에 연결하고 Cisco Cloud로 전송되는 이벤트를 구성하는 것은 소프트웨어 버전 6.6 이상을 실행하는 FTD 디바이스에서 구성할 수 있는 기능입니다.

Cisco Success Network

Cisco Success Network를 활성화하면 FTD를 개선하고 네트워크에서 Cisco 제품의 가치를 극대화하는 데 도움이 되는 미사용 또는 추가 기능을 알리기 위해 Cisco에 사용 정보 및 통계를 제공하게 됩니다. Cisco Success Network를 활성화하면 디바이스는 Cisco Cloud에 대한 보안 연결을 설정하고 항상 이 보안 연결을 유지합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Cisco Success Network에 연결"을 참조하십시오.

이벤트를 **Cisco Cloud**에 직접 전송

이제 FTD에서 Cisco Cloud로 직접 전송할 이벤트 유형을 지정할 수 있습니다. 일단 Cisco Cloud에 저장되면 클라우드 애플리케이션(예: Cisco Threat Response)을 사용하여 이벤트를 분석하고 디바이스에 발생했을 가능성이 있는 위협을 평가할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Cisco Cloud에 이벤트 전송"을 참조하십시오.

웹 분석

웹 분석을 활성화하면 페이지 조회 수를 기반으로 하는 익명 제품 사용 정보가 Cisco에 제공됩니다. 이 정보에는 확인한 페이지, 특정 페이지를 사용한 시간, 브라우저 버전, 제품 버전, 디바이스 호스트 이름 등이 포함됩니다. Cisco는 이 정보를 활용해 기능 사용 패턴을 확인하고 제품을 개선할 수 있습니다. 모든 사용량 데이터는 익명으로 전송되며 민감한 데이터는 전송되지 않습니다. CDO를 사용하여 모든 버전의 FTD에서 이 기능을 구성할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "웹 분석 활성화 또는 비활성화"를 참조하십시오.

2021년 1월 7일

FTD HA 쌍 온보딩

CDO는 FTD HA 쌍의 온보딩 프로세스를 개선했습니다. 등록 토큰 방법 또는 로그인 자격 증명 방법을 사용하여 HA 피어 중 하나를 온보딩하면 CDO는 해당 피어가 아직 온보딩되지 않았음을 자동으로 탐지하고 작업을 수행하라는 메시지를 표시합니다. 이 개선 사항은 두 디바이스를 온보딩하는 데 필요한 노력을 최소화하고, 피어 디바이스를 온보딩하는 데 걸리는 시간을 단축하며, 첫 번째 디바이스를 온보딩하는 데 사용한 등록 키 또는 스마트 라이선스 토큰을 재사용합니다.

액티브 또는 스탠바이 디바이스를 온보딩할 수 있으며, 일단 동기화되면 CDO는 해당 디바이스가 HA 쌍의 일부임을 항상 탐지합니다.

Note 등록 키 방법을 사용하여 FTD 디바이스를 온보딩하는 것이 좋습니다.

FTD HA 쌍 온보딩에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "등록 키로 FTD HA 쌍 온보딩" 또는 "사용자 이름 비밀번호 및 IP 주소를 사용하여 FTD HA 쌍 온보딩"을 참조하십시오.

2021년 1월 7일