클라우드 사용 **Firewall Management Center**를 사용하여 **Cisco Secure Firewall Threat Defense** 디바이스 관리

클라우드 사용 Firewall Management Center는 SaaS(Software-as-a-Service) 제품으로, Secure Firewall Threat Defense 디바이스를 관리하며 CDO(Cisco Defense Orchestrator)를 통해 제공됩니다. 클라우드 사용 Firewall Management Center는 온프레미스 Secure Firewall Management Center와 동일한 여러 기능을 제공합니다.

클라우드 사용 Firewall Management Center는 온프레미스 Secure Firewall Management Center와 모양과 동작이 동일하며 동일한 FMC API를 사용합니다.

CDO(Cisco Defense Orchestrator) 운영 팀은 SaaS 제품으로서 클라우드 사용 Firewall Management Center 소프트웨어 구축 및 유지 관리를 담당합니다. 새로운 기능이 도입되면 CDO 운영 팀이 CDO 테넌트의 클라우드 사용 Firewall Management Center를 업데이트합니다.

마이그레이션 마법사를 사용하여 Secure Firewall Threat Defense 디바이스를 온프레미스 Secure Firewall Management Center에서 클라우드 사용 Firewall Management Center로 마이그레이션할 수 있습니다. 마이그레이션하려면 디바이스에 Threat Defense 소프트웨어 버전 7.0.3 이상 7.0.x 릴리스 또는 버전 7.2 이상이 설치되어 있어야 합니다. Threat Defense 7.1 릴리스는 지원되지 않습니다.

Secure Firewall Threat Defense 디바이스 온보딩은 일련 번호를 사용하여 디바이스를 온보딩하거나 등록 키가 포함된 CLI 명령을 사용하는 등 친숙한 프로세스를 사용하여 CDO에서 수행됩니다. 디바이스가 온보딩되면 CDO 및 클라우드 사용 Firewall Management Center에 모두 표시되지만 클라우드 사용 Firewall Management Center에서 디바이스를 구성합니다.

CDO는 데이터 인터페이스를 통해 관리하는 위협 방어 디바이스에서 고가용성 지원을 제공합니다. 이 기능은 소프트웨어 버전 7.2 이상에서 실행되는 디바이스에서 지원됩니다.

Security Analytics and Logging(SaaS) 또는 Security Analytics and Logging(온프레미스)을 사용하여 온보딩된 위협 방어 디바이스에서 생성된 시스템 로그 이벤트를 분석할 수 있습니다. SaaS 버전은 클라우드에 이벤트를 저장하며 CDO에서 이벤트를 볼 수 있습니다. 온프레미스 버전은 온프레미스 Secure Network Analytics 어플라이언스에 이벤트를 저장하며, 분석은 온프레미스 Secure Firewall Management Center에서 수행됩니다. 두 경우 모두 오늘날의 온프레미스 FMC와 마찬가지로 센서에서 직접 선택한 로그 컬렉터로 로그를 전송할 수 있습니다.

클라우드 사용 Firewall Management Center의 라이선스는 디바이스별 매니지드 라이선스이며 클라우드 사용 Firewall Management Center 자체에는 라이선스가 필요하지 않습니다. 기존 보안 방화벽 위협 방어 디바이스는 기존 스마트 라이선스를 재사용하며, 새 보안 방화벽 위협 방어 디바이스는 FTD에서 구현된 각 기능에 대해 새 스마트 라이선스를 프로비저닝합니다.

기존 고객은 CDO를 계속 사용하여 보안 방화벽 ASA, Meraki, Cisco IOS 디바이스, Secure Firewall Cloud Native, Umbrella 및 AWS 가상 프라이빗 클라우드와 같은 다른 디바이스 유형을 관리할 수 있습니다. Firepower Device Manager에서 로컬 관리용으로 구성된 Secure Firewall Threat Defense 디바이스를 CDO를 사용하여 관리하는 경우 CDO로도 계속 관리할 수 있습니다.

테넌트에서 클라우드 사용 Firewall Management Center를 프로비저닝하는 방법에 대한 자세한 내용은 CDO 테넌트에 대한 클라우드 사용 Firewall Management Center 요청, 2 페이지 섹션을 참조하십시오.

CDO 테넌트에 대한 클라우드 사용 Firewall Management Center 요청

클라우드 사용 Firewall Management Center를 사용하여 Secure Firewall Threat Defense 디바이스를 관리하려는 경우 테넌트에서 클라우드 사용 Firewall Management Center 프로비저닝을 요청할 수 있습니다.

Procedure

단계 **1** CDO 메뉴 바에서 **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center**를 클릭합니다.

단계 **2** **Request FMC(FMC** 요청**)**를 클릭합니다.

단계 **3** **Send Request(**요청 보내기**)**를 클릭하여 클라우드 사용 Firewall Management Center 요청을 확인합니다.

확인 시 클라우드 사용 Firewall Management Center 프로비저닝을 위해 CDO 팀에 요청이 전송됩니다. 프로비저닝이 완료되면 *cdo-alert@cisco.com*에서 등록된 이메일로 이메일을 받게 됩니다. 또한 수신 webhook을 구성한 애플리케이션 및 CDO 알림 패널에서 클라우드 사용 **Firewall Management Center is Ready(**준비됨**)** 알림을 받게 됩니다. 자세한 내용은 알림 설정을 참조하십시오.

그런 다음 위협 방어 디바이스를 클라우드 사용 Firewall Management Center에 온보딩하고 관리할 수 있습니다.

하드웨어 및 소프트웨어 지원

클라우드 사용 Firewall Management Center에서는 Secure Firewall Threat Defense 버전 7.0.3 및 7.0.x 버전을 지원하며, 7.0.3 이후 버전과 7.2 이상 버전은 다양한 Firepower 지원 하드웨어 디바이스 또는 가상 시스템에 설치할 수 있습니다.

클라우드 사용 Firewall Management Center는 Secure Firewall Threat Defense 버전 7.1을 지원하지 않습니다.

자세한 내용은 Firepower Threat Defense 지원 사양을 참조하십시오.

Cisco Defense Orchestrator 플랫폼 유지 보수 일정

Cisco Defense Orchestrator 유지 보수 일정

CDO는 매주 새로운 기능 및 품질 개선을 통해 플랫폼을 업데이트합니다. 이 일정에 따라 업데이트가 3시간 동안 이루어질 수 있습니다.

대부분의 경우 업데이트는 목요일에 완료되지만, 필요한 경우 금요일 및 일요일에도 유지 보수가 진행됩니다.

표 ***1: CDO*** 유지 보수 일정

요일	시간 **(24**시간**)**
목요일	09:00 UTC ~ 12:00 UTC
금요일	09:00 UTC ~ 12:00 UTC
일요일	09:00 UTC ~ 12:00 UTC

이 유지 보수 기간 동안 테넌트에 계속 액세스할 수 있으며, 클라우드 사용 Firewall Management Center가 있는 경우 해당 플랫폼에도 액세스할 수 있습니다. 또한 CDO에 온보딩한 디바이스가 보안 정책을 계속 적용합니다.

참고 유지 관리 기간 동안 관리하는 디바이스에 구성 변경 사항을 배포하는 데 CDO을 사용하지 않는 것이 좋습니다.

CDO 또는 클라우드 사용 Firewall Management Center의 통신이 멈추는 장애가 발생하는 경우, 해당 장애는 유지 보수 기간이 아니더라도 영향을 받는 모든 테넌트에서 최대한 신속하게 해결됩니다.

클라우드 제공 **Firewall Management Center** 유지 관리 일정

테넌트에 클라우드 사용 Firewall Management Center를 구축한 고객은 CDO에서 클라우드 사용 Firewall Management Center 환경을 업데이트하기 약 1주일 전에 알림을 받습니다. 테넌트의 슈퍼 관리자 및 관리 사용자는 이메일로 알림을 받습니다. CDO는 또한 모든 사용자에게 예정된 업데이트를 알리는 배너를 홈페이지에 표시합니다.

테넌트에 대한 업데이트는 최대 1시간이 걸릴 수 있으며, 테넌트 지역에 할당된 유지 관리 날짜의 3시간 유지 관리 시간 내에 이루어집니다. 테넌트가 업데이트되는 동안에는 클라우드 사용 Firewall Management Center 환경에 액세스할 수 없지만, CDO의 나머지 부분에 계속 액세스할 수 있습니다.

표 ***2:*** 클라우드 제공 ***Firewall Management Center*** 유지 관리 일정

요일	시간 **(24**시간**)**	지역
수요일	04:00 UTC ~ 07:00 UTC	유럽, 중동 또는 아프리카 (EMEA)
수요일	17:00 UTC ~ 20:00 UTC	아시아-태평양-일본-중국(APJC)
목요일	09:00 UTC ~ 12:00 UTC	미국(US)