AI Defense

AI Defense와의 통합을 활성화하면 승인되지 않은 모델에 접근하는 관련 활동, 연결 유형 및 ID 수를 포함한 AI 에셋을 보호할 수 있습니다. Multicloud Defense 테넌트와 함께 이 기능을 활용하면 환경에서 모델을 검색하고 AI Defense 실행 시간 보호를 적용할 수 있습니다. 검색된 모델은 AI Defense 검증을 사용하여 안전 및 보안을 테스트할 수도 있습니다. AI Defense에 대한 자세한 내용과 AI를 사용하여 안전과 보안을 개선하기 위해 수행할 수 있는 작업은 AI Defense 설명서를 참조하십시오.

AI Defense를 Multicloud Defense와 통합

지원 및 제한 사항

Multicloud Defense 테넌트와 AI Defense를 얼마나 통합할지에 따른 요구 사항 및 제한 사항은 다음과 같습니다.

- AI Defense 또는 Multicloud Defense에 액세스하려면 먼저 Security Cloud Control 어카운트가 있어야 합니다.
- 현재 이그레스 Multicloud Defense 게이트웨이만 AI Defense와 호환됩니다.
- LLM 프롬프트 및 응답의 AI 실행 시간 모니터링을 사용하여 전체 AI Defense 경험을 원하는 경우 "어카운트를 안전하게 보호"하고 게이트웨이에 서비스 VPC 또는 VNet을 추가 해야 합니다.
- AI Defense 통합을 지원하도록 지정된 Multicloud Defense에서 생성된 프로파일 및 규칙 집합은 Multicloud Defense 컨트롤러에서 수정 해야 합니다. AI Defense 대시보드에서 Multicloud Defense 정책 또는 규칙 집합을 삭제하거나 수정할 수 없습니다.
- AI Defense 라이선스가 있어야 합니다. AI Defense 라이선스에 대한 자세한 내용은 관리를 참조하십시오.
- 에셋의 AI 검색은 AWS 및 Azure에 대해 수행됩니다.

개요

목록은 보안 통합을 허용하기 위해 이러한 제품의 두 가지 측면을 모두 활성화하는 절차의 개요입니다.

1. Multicloud Defense 테넌트에 로그인합니다.
2. Multicloud Defense 대시보드를 사용하여API 키를 생성합니다.
3. Multicloud Defense 테넌트를 AI Defense에 연결합니다.
4. Multicloud Defense에 클라우드 통신 사업자를 온보딩합니다. 액세스 및 통신을 허용하려면 AWS 어카운트에 올바른 권한을 추가 해야 합니다.
5. 트래픽 가시성을 활성화합니다.
6. 어카운트를 보호합니다.
7. AI 가드레일 프로파일
8. 이그레스 게이트웨이의 정책 규칙 집합에 프로파일을 연결합니다.

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.