클라우드 악성코드 및 SaaS API DLP가 포함된 Dropbox 이해

목차

소개

이 문서에서는 Umbrella 및 Secure Access 제품의 Cloud Malware 및 SaaS API DLP 개선 사항에 대한 제품 릴리스 정보를 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella 및 Secure Access를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

Umbrella 및 Secure Access 제품이 새롭게 개선되었습니다. 클라우드 악성코드 및 SaaS API DLP는 이제 Dropbox Teams 폴더에 대한 검사 기능을 제공합니다. 이러한 기능 향상으로 더욱 강력한 데이터 보안 솔루션이 제공됩니다.

Dropbox는 클라우드 악성코드 및 DLP에서 이미 지원되었습니다. 그러나 검색 기능은 개인 Dropbox 폴더에 저장된 파일에 한정되었습니다.

원격 협업이 널리 보급된 이 시대에 협업 활용 사례를 지원하기 위해 중요한 조직 데이터를

Dropbox Team 폴더에 상당량 저장하고 편집하고 있습니다.

개선 사항 사용

개선 사항을 활성화하는 데 필요한 작업은 없습니다. Dropbox를 SaaS API DLP 또는 클라우드 악성코드에 온보딩한 모든 Umbrella 또는 Secure Access 조직은 활성화 또는 추가 컨피그레이션이 필요 없이 자동으로 이러한 개선 기능을 활용할 수 있습니다.

개선 요금

이 개선 사항은 추가 비용 없이 모든 DLP 고객에게 제공됩니다.

클라우드 악성코드 및 SaaS API DLP의 Dropbox 테넌트 온보딩 설명서

클라우드 악성코드 및 SaaS API DLP에서 Dropbox 테넌트를 온보딩하는 방법에 대한 지침은 다음 문서를 참조하십시오.

- Dropbox용 DLP 보호 사용
- Dropbox용 클라우드 악성코드 차단 활성화

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.