

프라이빗 채팅 구성GPT 및 다른 생성 AI 앱에 대한 액세스 제한

목차

[소개](#)

[개요](#)

[1단계: 개인 채팅을 허용하는 웹 규칙 만들기GPT](#)

[2단계: 다른 모든 생성 AI 앱 차단](#)

[DNS 정책](#)

[웹 정책](#)

소개

이 문서에서는 프라이빗 ChatGPT를 구성하고 다른 생성 AI 앱에 대한 액세스를 제한하는 방법에 대해 설명합니다.

개요

인공지능의 풍경은 빠르게 진화하고 있으며, 주목할 만한 진전 중 하나는 '제너레이티브 AI'의 발전이었다. 이 중 ChatGPT가 큰 영향을 미쳤습니다.

조직이 이러한 강력한 툴을 워크플로우에 통합하고자 함에 따라 Generative AI 애플리케이션에 대한 액세스를 제어할 필요성이 점점 더 분명해지고 있습니다. 자체 프라이빗 ChatGPT 인스턴스를 개발한 기업의 경우, 이 툴이 팀이 액세스할 수 있는 유일한 AI 툴임을 보장하면서 다른 Generative AI 앱을 제한하는 것은 중요한 보안 조치입니다.

다행히도 Umbrella 대시보드를 사용하여 이를 달성할 수 있는 간단한 방법이 있습니다. 이 문서에서는 조직이 다른 AI 애플리케이션의 사용을 엄격하게 통제하면서 프라이빗 ChatGPT를 활용할 수 있도록 하기 위해 수행해야 할 단계를 안내합니다.

1단계: 개인 채팅을 허용하는 웹 규칙 만들기GPT

먼저 Umbrella 대시보드에 로그인해야 합니다. DNS 규칙 또는 웹 규칙을 만들 수 있습니다.

이 규칙에는 개인 ChatGPT의 특정 URL이 포함된 "Allow(허용)" 작업과 Destination List(대상 목록) 작업이 있어야 합니다.

이 단계에서는 조직 내 사용자가 제한 없이 개인 ChatGPT에 액세스할 수 있습니다.

2단계: 다른 모든 생성 AI 앱 차단

'Allow' 규칙이 생성된 직후 두 번째 규칙을 생성해야 합니다.

이 규칙에는 '차단' 조치가 있어야 하고, '생성 인공지능' 카테고리를 아우르는 '애플리케이션 목록'을 포함해야 한다.

이를 통해 ChatGPT의 공개 버전을 포함하여 널리 사용되는 다양한 Generative AI 애플리케이션에 액세스하는 것을 방지할 수 있습니다.

DNS 정책

웹 정책이 아닌 DNS 정책을 사용할 때 이러한 규칙이 효과적으로 적용되도록 합니다. 원활한 환경을 위해 지능형 프록시와 SSL 해독을 활성화하는 것이 중요합니다. 또한 SSL 암호 해독이 제대로 작동하려면 Cisco Umbrella 루트 인증서를 설치해야 합니다.

DNS 정책 설정에 대한 포괄적인 지침은 [여기서](#) 공식 문서를 참조하십시오. 또한 DNS 정책의 효과를 최적화하려면 [여기서](#) 모범 사례를 확인하십시오.

웹 정책

조직의 요구 사항에 맞게 웹 정책을 관리하고 조정하는 방법에 대한 자세한 내용은 [여기를](#) 참조하십시오.

이러한 조치를 구현하면 조직이 프라이빗 ChatGPT를 최대한 활용하는 동시에 다른 Generative AI 앱 사용으로 발생할 수 있는 데이터 유출 또는 주의 산만 위험을 완화할 수 있습니다. 보안과 접근성의 적절한 균형은 Generative AI의 잠재력을 활용하면서 조직의 데이터 및 리소스가 잘 보호되도록 하는 핵심입니다.

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.