CLOUDFLARE

솔루션 개요

직원들의 섀도우 AI 및 IT 사용 실태 살펴보기

Cloudflare의 트래픽 검사를 통해 비승인 AI 및 SaaS 도구에 대한 가시성 확장

보이지 않는 것을 파헤치다

섀도우 IT는 새로운 문제가 아니지만, 승인되지 않은 AI 도구의 빠른 도입이 현대적인 위기를 주도하고 있습니다.

- **20%**의 조직이 2025년에 섀도우 AI로 인한 보안 사고로 인해 유출을 경험했습니다[1]
- IT 리더의 **85%**가 직원들이 IT 팀에서 AI 도구를 평가하기 전에 AI 도구를 도입하고 있다고 이야기합니다[2]

Cloudflare는 조직이 이처럼 확장되는 공격면을 관리할 수 있도록 가시성을 회복합니다.

- **애플리케이션 상태 검토:** AI 및 SaaS 애플리케이션을 승인, 미승인, 아직 검토 중으로 분류
- **애플리케이션 상태에 따라 정책 시행:** 허용, 차단, 격리, 상호 작용에 DLP 감지 적용, 파일 업로드 제한 등
- **애플리케이션 사용량 분석:** 종합 동향 모니터링 및 세부 조사 수행
- **애플리케이션 위험 평가:** 신뢰성 평가를 위한 애플리케이션 신뢰도 점수

섀도우 AI의 고유한 위험

섀도우 AI는 기존의 섀도우 IT와 다릅니다. SaaS 애플리케이션은 주로 파일을 저장하거나 공유하는 반면, AI 도구는 모든 직원 입력으로부터 혁신하고 학습합니다.

즉, 중요한 지적 재산(IP), 고객 데이터, 또는 소스 코드가 모델 학습에 되돌릴 수 없이 흡수될 수 있으며, 이후 삭제할 방법이 없습니다.

작동 방식

Cloudflare의 SASE 플랫폼은 직원과 리소스 사이에 위치하여 가시성과 제어를 통합합니다.

또한, API를 통해 Cloudflare의 CASB를 통합하여 잘못된 구성, 사용자 활동 및 중요한 데이터를 검사합니다.
AI 애플리케이션(ChatGPT, Claude, Google Gemini) 및 기타 SaaS 애플리케이션 전반에 걸쳐 보안 상태를 관리합니다.
ID 공급자와 함께 CASB를 사용하여 사용자가 승인되지 않은 타사 애플리케이션에 로그인할 때 이를 확인합니다.

대시보드 예시

이 포괄적인 애플리케이션 사용량 개요는 다음을 기준으로 필터링할 수 있습니다.

- 애플리케이션 및 애플리케이션 유형
- 승인 상태
- ZTNA로 보호되는지 여부
- 사용자 수

AI 애플리케이션에 대한 특정 사용자 또는 그룹, 사용 빈도, 위치, 전송된 데이터 양 등에 대한 자세한 정보를 확인할 수 있습니다.

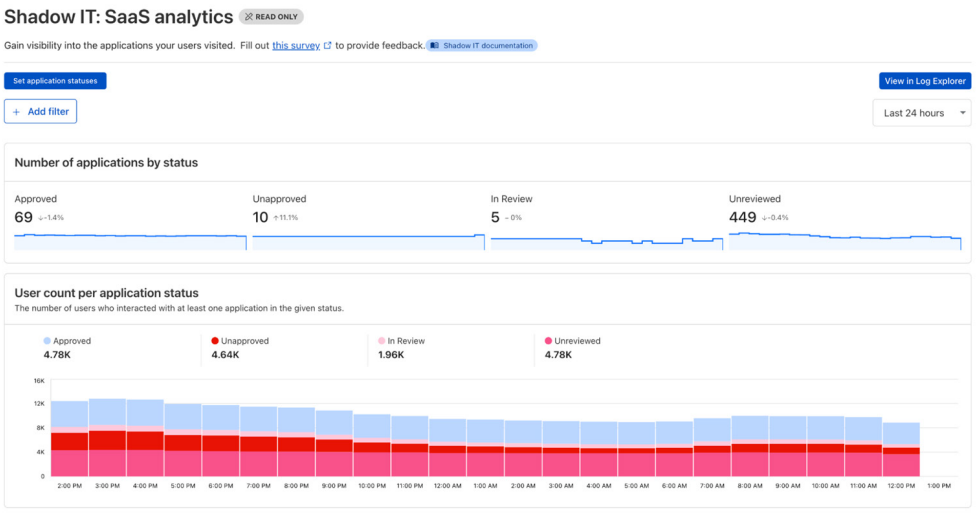

그림 1: 섀도우 IT 분석 대시보드

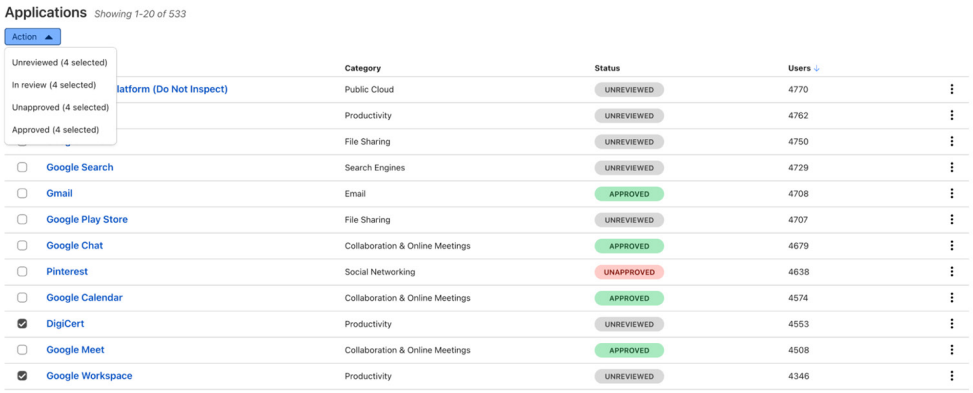

그림 2: 애플리케이션 상태 표시

애플리케이션을 구성하고, 다음과 같은 승인 상태에 따라 액세스 정책을 설정합니다.

- 승인(승인됨)
- 미승인(비승인)
- 검토 중
- 미검토

기술적인 안내를 더 받고 싶으신가요? 이 학습 경로로 정책을 구축하는 방법을 알아보세요.

AI 도입을 보호하는 방법에 대해 자세히 알아보고 싶으신가요?

사용 사례 더 살펴보기

워크숍 요청하기

1. 2025 IBM, 데이터 유출 비용 보고서: 출처
2. 2025 Manage Engine 연구: 출처

