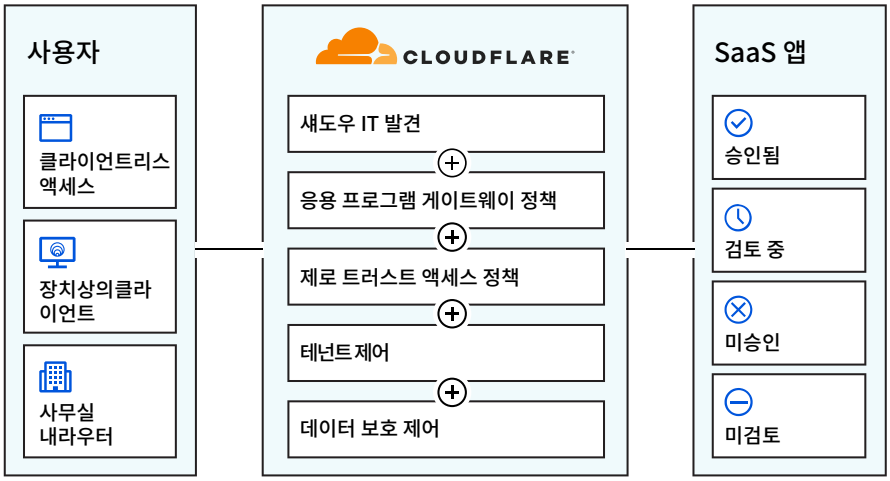
솔루션 요약

Zero Trust 가시성 및 모든 SaaS 응용 프로그램 제어

SaaS 응용 프로그램은 팀이 이전보다 더 많은 업무를 수행할 수 있도록 지원하지만, 이러한 응용 프로그램이 직원에게 제공하는 유연성과 자유로 인해 조직에 보안 위험, 가시성 문제 및 액세스 제어 등의 장애물이 발생합니다.

Cloudflare는 데이터와 직원 보호에 필요한 도구를 제공하는 동시에 직원이 업무를 수행하는 데 도움이 되는 도구를 사용하도록 허용합니다.



섀도우 IT 파악 및 제어

직원이 사용 중인 응용 프로그램에 대한 가시성이 없으면 중요한 데이터의 저장, 공유 또는 제3자 노출 방식을 제어할 수 없습니다. Cloudflare는 조직 내에서 승인되거나 승인되지 않은 모든 응용 프로그램을 검색, 분류 및 제어하는 동시에 중앙화된 하나의 위치에 모든 연결과 요청을 기록하도록 지원합니다.

Zero Trust 액세스 정책 적용

SaaS 응용 프로그램은 기업 네트워크 외부에서 호스팅되기 때문에 보안 팀은 사용자가 해당 애플리케이션에 액세스하고 그러한 응용 프로그램 안팎으로 데이터를 이동하는 방법을 제어하는 능력이 제한됩니다. Cloudflare는 SaaS 응용 프로그램 앞에서 Zero Trust 보안 조치를 계층화하여 합법적인 사용자를 인증하고 권한이 없는 사용자나 위험한 장치가 파일 및 데이터에 액세스하는 것을 방지합니다.

테넌트 및 데이터 보호 제어 적용

직원이 잘못된 응용 프로그램 인스턴스에 액세스하면 데이터를 잘못된 장소에 저장하고 공유할 수 있기 때문에 잠재적인 데이터 유출과 기타 보안 위험이 발생할 수 있습니다. Cloudflare는 데이터가 네트워크에서 이동 중이든 원격 브라우저 내에서 사용 중이든 관계없이 데이터 공유와 저장을 제어하도록 돕습니다. 이제 모든 SaaS 테넌트 내의 데이터를 보호하고 직원이 잘못된 응용 프로그램이나 승인된 응용 프로그램의 잘못된 테넌트에 액세스하지 않도록 Zero Trust 브라우징 정책을 구축 및 배포할 수 있습니다.

섀도우 IT 파악 및 제어

직원이 사용하는 응용 프로그램 평가

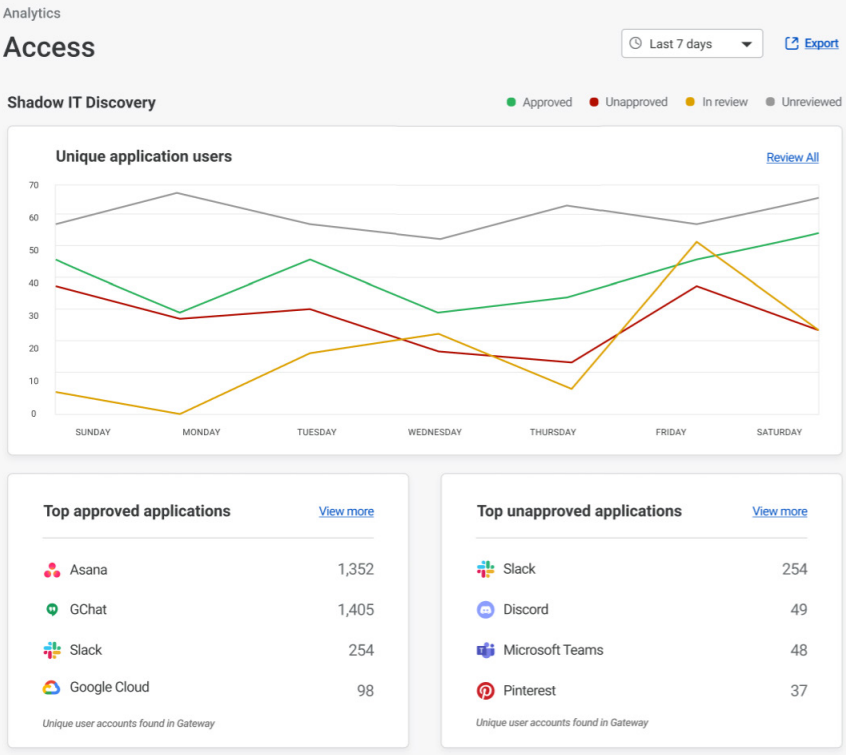
IT 팀에서 직원이 사용하는 응용 프로그램을 볼 수 없으면 그러한 응용 프로그램 내의 데이터에 대한 작업을 제어할 수 없습니다. Cloudflare는 활동 로그의 모든 HTTP 요청을 응용 프로그램 유형별로 종합하고 자동으로 분류합니다. 여기에서 상태를 설정하고 조직 전체에 걸쳐 승인 및 미승인 응용 프로그램의 사용을 추적할 수 있습니다.

모든 연결 및 요청 기록

Cloudflare는 직원이 승인되지 않은 응용 프로그램에 액세스하거나 관리되지 않는 장치를 사용하여 중요한 정보에 액세스할 때 조직에 초래할 수 있는 위험을 완화하도록 돕습니다. 모든 연결과 요청은 중앙화된 하나의 위치에 기록되므로 사용 중인 응용 프로그램과 해당 응용 프로그램 내에서 사용자가 수행하는 활동을 확인할 수 있습니다. 또한, 관리자는 SaaS 응용 프로그램에 대한 요청을 차단 및 허용하여 사용자가 중요한 보안 제어를 우회하고 조직 내의 응용 프로그램, 리소스 및 데이터에 무단으로 액세스하는 것을 방지할 수 있습니다.

주요 기능

- Cloudflare에 의해 이미 보호된 응용 프로그램 자동 추적
- Cloudflare 네트워크에 최대 6개월간 로그 유지
- 하나 이상의 클라우드 로그 스토리지 및 SIEM 서비스에 로그 푸시



SaaS 응용 프로그램에 Zero Trust 액세스 정책 적용

Cloudflare의 ID 프록시를 통해 안전한 SaaS 액세스 제공

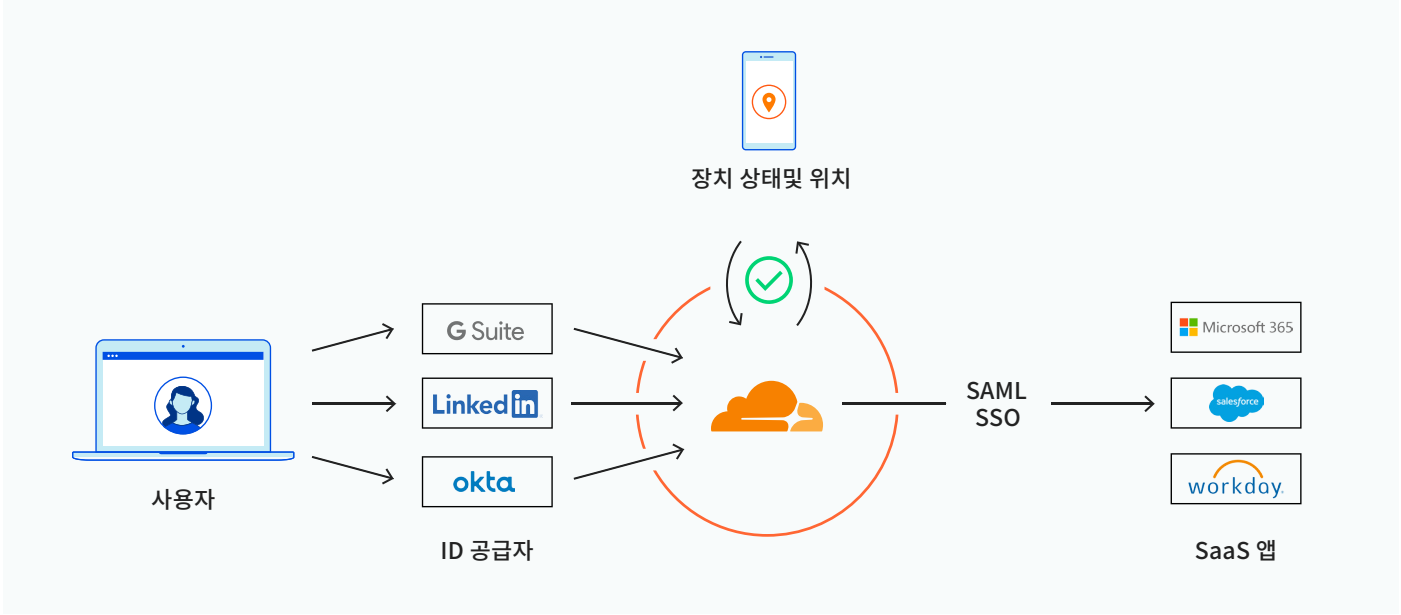
SaaS 응용 프로그램은 제3자가 호스팅하며, 사업부에서 관리하는 경우가 많습니다. 이는 IT 팀에서는 사용자가 그러한 응용 프로그램에 액세스하는 방식을 거의 관리할 수 없다는 것을 의미합니다. Cloudflare는 ID 공급자와 SaaS 응용 프로그램 사이에서 최종 사용자 경험을 방해하지 않고 로그인 프로세스에 ID 인식 컨텍스트 기반 Zero Trust 규칙을 구축하고 적용할 수 있도록 지원합니다.

사용자 장치에 대한 응용 프로그램 권한 결정

IT 부서는 기업에서 관리하는 장치가 SaaS 응용 프로그램에 로그인하는 방식을 세부적으로 제어해야 합니다. Cloudflare는 SAML 인증을 지원하는 모든 응용 프로그램의 SSO(single sign-on) 프로세스에 Zero Trust 규칙을 삽입합니다. 사용자가 먼저 ID 공급자를 통해 인증하면, Cloudflare가 SaaS 응용 프로그램에 대한 액세스를 승인하기 전에 지속적인 확인을 위해 유연한 세션 관리를 통해 장치 상태 및 위치에 대한 요청을 확인합니다. 또한, 보안 관리자는 장치별로 정책을 생성할 수 있기 때문에 사용자는 mTLS 인증서를 포함하여 사전에 설정된 보안 요구 사항을 충족하는 장치를 통해서만 응용 프로그램에 액세스할 수 있습니다.

주요 기능

- 여러 ID 공급자 또는 동일 공급자의 여러 인스턴스 통합
- 응용 프로그램별 규칙(예: MFA는 하드 키 필요)으로 사용자 ID 확인
- 응용 프로그램별규칙(예: SWG 정책 시행, EPP 설치, mTLS 인증서, 디스크 암호화 사용) 및 위치로 장치 상태 확인
- Cloudflare의 앱 런처 포털에서 사용자가 승인된 모든 SaaS 응용 프로그램 확인 및 액세스 가능



모든 SaaS 응용 프로그램에 테넌트 및 데이터 보호 제어 적용

기업 외 응용 프로그램 인스턴스에 대한 액세스 제한

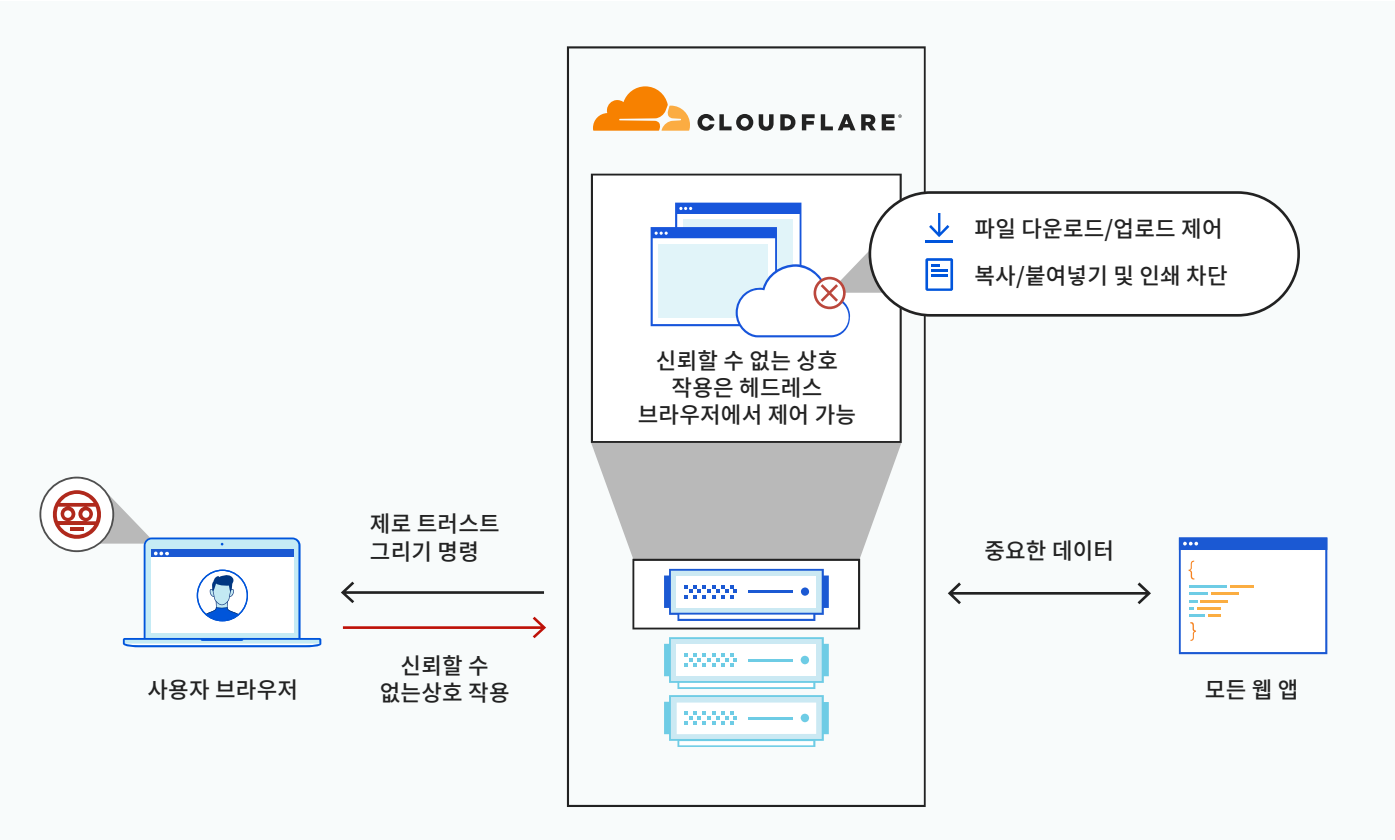
Cloudflare는 사용자가 응용 프로그램의 소비자 버전에 액세스하지 못하도록 구성할 수 있는 HTTP 게이트웨이 정책을 통해 테넌트를 제어할 수 있게 해줍니다. 기업 VPN을 통해 온프레미스 프록시 서버를 사용하여 이러한 정책을 시행하는 대신, Cloudflare는 방대한 데이터 센터 전역 네트워크를 통해 모든 트래픽과 요청을 필터링 및 점검하기 때문에 사용자가 대기 시간 증가나 성능 저하를 결코 겪지 않습니다.

기업 데이터의 테넌트 이탈 방지

Cloudflare는 Zero Trust 브라우징 정책을 손쉽게 구축하고 배포하여 웹 기반 응용 프로그램 내에 있는 데이터를 제어하고 보호할 수 있게 해줍니다. 모든 응용 프로그램 코드는 엔드포인트 장치보다는 대규모 전역 네트워크 전체에서 원격으로 운영되는 안전한 헤드리스 브라우저에서 실행되므로, 손상되거나 신뢰할 수 없는 장치 및 제로데이 위협으로부터 중요한 데이터를 보호할 수 있습니다. 또한, 관리자는 사용자가 해당 데이터에 액세스하고 공유하는 방식을 제어할 수 있으므로 우발적인 데이터 손실이나 더 심각한 데이터 유출의 위험을 최소화할 수 있습니다.

주요 기능

- 응용 프로그램, 응용 프로그램 유형, 호스트 이름, 사용자 ID 및 보안 위험을 포함한 다양한 기준을 기반으로 브라우저 동작 허용 또는 차단
- 다운로드, 업로드, 복사 및 붙여넣기, 키보드 입력, 프린트 기능 등 브라우저 내 사용자 작업 제어



Cloudflare의 차별성

플랫폼 범위

Cloudflare는 IT 팀이 전용 CASB 제품을 구성 및 운영할 필요 없이 SaaS 응용 프로그램 앞에 Zero Trust 액세스(ZTNA), 게이트웨이(SWG) 및 브라우저(RBI) 제어를 배치합니다.

처음부터 새롭게 구축

Cloudflare의 CASB 기능은 모든 것이 처음부터 새롭게 구축되기 때문에 응용 프로그램과 팀을 보호하기 위해 여러 개의 point products를 복잡하게 구성할 필요 없이 ZTNA, SWG 및 RBI 서비스와 원활하게 연동됩니다.

단일 제어판

Cloudflare는 조직에서 단일 대시보드에서 정책을 설정하고 응용 프로그램 액세스와 사용을 관리하도록 허용하기 때문에 모든 요청과 권한을 한눈에 모니터링 할 수 있습니다.

Cloudflare는 기본적으로 통합된 Zero Trust 보안 기능 제품군을 통해 SaaS 응용 프로그램을 여러 팀이 모니터링, 보호 및 제어할 수 있도록 지원합니다.

지금 자세히 알아보세요