CLOUDFLARE

솔루션 요약

중요한 데이터 보호

더 효과적이고, 더 생산적이며, 더 민첩한 데이터 보호를 위한 더 나은 네트워크 아키텍처.

장소에 구애받지 않는 통합 데이터 보호

데이터 보호는 새로운 필수 사항이 아니지만, 하이브리드 클라우드 아키텍처로의 전환이 이루어지고 AI가 빠르게 채택되면서 다음과 같은 새로운 과제가 생겨났습니다.

- **직원의 93%**가 승인을 받지 않고서 AI 도구에 정보를 입력했다고 인정합니다 [1]
- **모든 국가 중 79%**에서 데이터 보호법을 갖추고 있습니다 [2]

Cloudflare에서는 데이터 수명주기 전반에 걸쳐 다음과 같이 일관된 제어를 시행합니다.

- **모든 곳에서 보호:** 웹, SaaS, 이메일, 클라우드 트래픽 전반에 걸쳐 일관된 제어를 시행합니다.
- **AI 유출 차단:** 생성형 AI 프롬프트를 분석하여 중요한 데이터를 차단하고 AI 사용을 관리합니다.
- **데이터 위험 관리:** 섀도우 IT/AI를 발견하고 관리하며, CASB를 사용하여 SaaS/클라우드 애플리케이션을 스캔합니다.

"승인되지 않은 AI 도구의 증가로 인해 보안 접근 방식을 재고하게 되었습니다. 현재 SASE를 살펴보고 있습니다."
- ***AllSaints** 정보 보안 책임자*

엔터프라이즈 DLP 대신 SASE를 사용해야 하는 이유는?

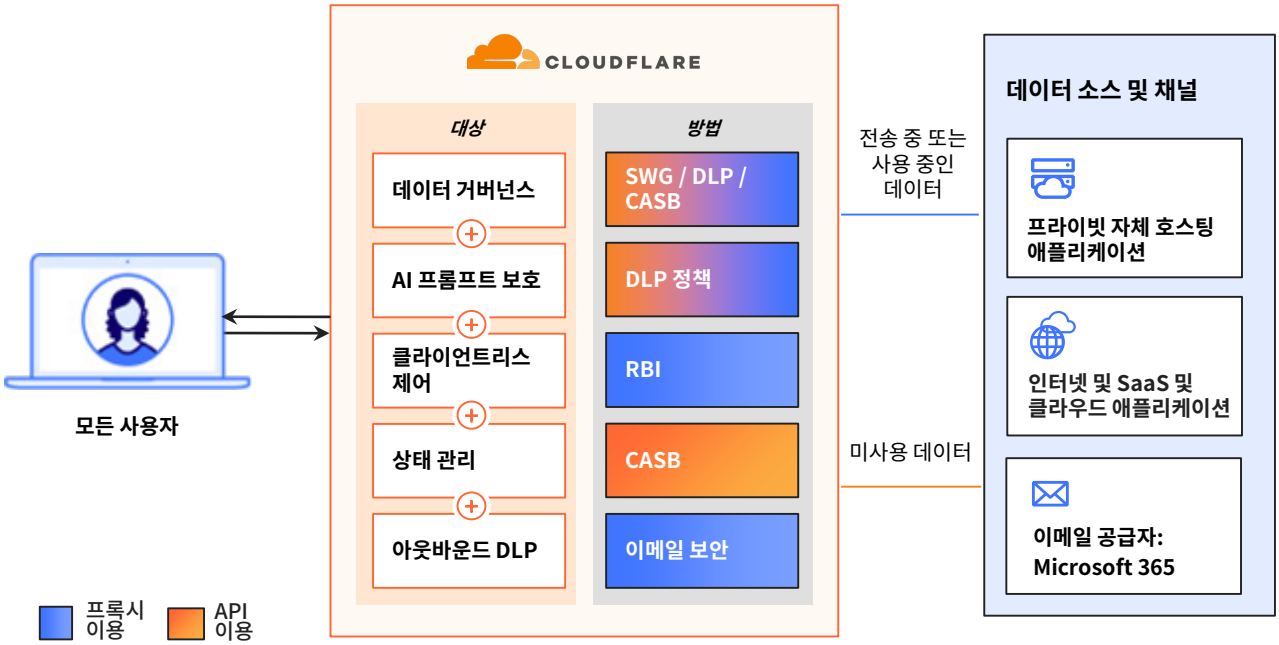
Cloudflare의 보안 액세스 서비스 에지(SASE) 플랫폼은 직원과 모든 애플리케이션 및 데이터 소스 사이에 위치하도록 설계되었습니다. 따라서 SASE는 많은 사람이 데이터를 안전하게 보호하기 시작하는 데 이상적인 출발점이 됩니다.

직원이 SaaS 애플리케이션으로 데이터에 액세스하든, 중요한 파일을 다운로드하든, GenAI 도구와 채팅하든, Cloudflare의 SASE 플랫폼에서는 모든 데이터 상호 작용에 걸쳐 일관된 보안 제어를 시행합니다.

작동 방식

Cloudflare의 SASE 플랫폼은 직원과 리소스 사이에 위치하여 데이터 가시성과 제어를 통합합니다.

웹, SaaS, 이메일, 클라우드 트래픽 전반에 걸쳐 **Cloudflare의 SASE 플랫폼을 통한 AI 기반 데이터 보호**



실시간 인라인 데이터 보호

- **세분화된 DLP:** 개인 식별 정보, 소스 코드, 고객 데이터 등을 위한 컨텍스트 인식 감지를 통해 중요한 데이터 노출을 방지합니다.
- **아웃바운드 이메일 DLP:** 발신 이메일의 중요한 데이터를 자동으로 표시하여 우발적인 데이터 유출을 방지합니다.
- **프롬프트 보호:** 의도에 따라 위험한 AI 프롬프트와 응답을 감지하고 차단합니다(예: 탈옥 시도, 코드 남용, 개인 식별 정보 요청).

섀도우 IT 및 대비 태세 위험

- **섀도우 IT 및 AI 탐색:** 환경 전반에서 섀도우 IT/AI를 발견하고 관리합니다. 애플리케이션 신뢰 점수와 데이터 전송 지표를 사용하여 위험을 수치화하고 노출을 신속히 완화합니다.
- **상태 관리:** 상태 위험에 대해 SaaS 애플리케이션 및 클라우드 환경을 스캔합니다. 보안 결과를 개선하기 위한 규범 조치를 취합니다.
- **테넌트 제어:** SaaS 애플리케이션의 개인 테넌트를 차단하여 데이터 유출을 방지합니다.

안전한 접근 및 클라이언트 제어

- **애플리케이션 액세스 보호:** 에이전틱 AI 연결에 대한 세분화된 DLP 스캐닝과 같은 Zero Trust 네트워크 액세스(ZTNA) 규칙을 모든 기업 애플리케이션에 걸쳐 적용합니다.
- **장치 상태 확인:** 디스크 암호화 및 활성화된 엔드포인트 DLP와 같은 세분화된 상태 검사를 기반으로 액세스를 제어합니다.
- **클라이언트리스 제어:** 브라우저 기반 데이터 제어를 적용하여 타사 액세스 및 직원 BYOD 정책을 보호합니다.

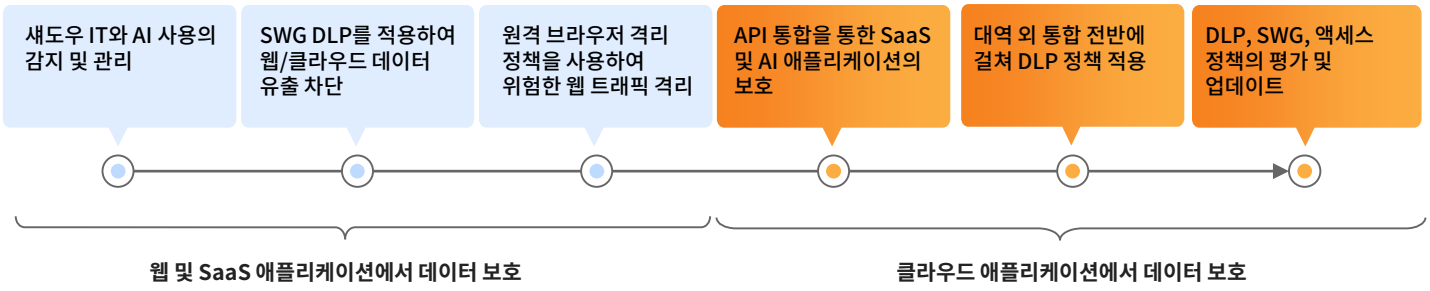
통합 및 보고

- **CASB 통합:** API 기반 CASB 스캔을 위해 주요 SaaS 및 AI 플랫폼(Microsoft 365, Google Workspace, ChatGPT 포함)과 원활하게 통합됩니다.
- **Microsoft MIP 통합:** Microsoft 정보 보호(MIP) 레이블과 지속해서 동기화하여 일관된 DLP 정책을 유지합니다.
- **Observability 및 포렌식:** 감사를 위해 원하는 SIEM에 데이터를 안전하게 기록하거나 대시보드 또는 API를 통해 즉시 로그를 분석합니다.

데이터 보호 여정 예시

공격면 가시성을 확보하기 위해 섀도우 IT와 AI 사용을 파악하는 것부터 시작합니다. SWG에서 기본 DLP 정책을 구성하여 관리되지 않는 클라우드 애플리케이션으로 인한 고위험 데이터 유출을 방지하고, 승인되지 않은 웹 트래픽에 대해 원격 브라우저 격리(RBI)를 배포합니다.

그런 다음, 잘못된 구성을 해결하고 내부 공유 정책을 준수하도록 하여 승인된 SaaS 및 AI 애플리케이션을 보호하기 위해 CASB를 배포합니다. SWG, 이메일, CASB 전반에 걸쳐 세분화된 DLP 및 액세스 정책을 개선하고 통합하여 모든 주요 데이터 벡터를 대상으로 자동화된 통합 예방을 달성합니다.



시작하기 좋은 사용 사례 예시

- 모든 비승인 통신 및 저장 채널에서 **개인 식별 정보/PHI의 실시간 유출을 차단합니다**.
- 내부자 도난 및 무단 배포로부터 **소스 코드 및 지식 재산(IP)을 보호**합니다.
- 생성형 AI 애플리케이션에 **프롬프트 보호 정책을 적용**하여 중요한 데이터 노출과 모델 오염을 방지합니다.
- 모든 SaaS 및 AI 애플리케이션에 걸쳐 **잘못된 구성을 방지**하고 세분화된 액세스 제어를 시행합니다.

고객 성과

EESTI RAUDTEE

인프라 공급자
사례 연구 보기

데이터 손실 및 SaaS 취약점 완화

데이터 유출 및 잘못된 구성 식별을 통해.

APPLIED

보험 기술
사례 연구 보기

ChatGPT와 같은 공개 생성형 AI 도구를 격리하여

중요 데이터 복사-붙여넣기 차단.

Flo

선도적인 건강 애플리케이션
사례 연구 읽기

환자 데이터 보호

규제 준수를 이메일 보안과 Zero Trust로 달성.

CREDIT SAISON INDIA

비은행 금융 기관
사례 연구 보기

PII를 보호하고 규제 준수를 달성하여

원치 않는 데이터 송신을 방지.

귀사의 데이터 보호 관련 필요 사항에 대해 상담할 준비가 되셨나요?

워크숍 요청하기

1. 2025 Manage Engine 연구: 출처
2. 2025 무역 및 개발에 관한 유엔 회의: 출처

