CLOUDFLARE

솔루션 요약

데이터 보호를 위한 Cloudflare One

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

장소에 구애받지 않는 통합 데이터 보호

최신 데이터 위험에는 최신 보안이 필요합니다
데이터는 양, 다양성, 속도 면에서 오늘날 폭있으며 조직에서는 다음으로 인하여 늘어나는 위험에 직면합니다.

발적으로 증가하고 무분별하게 확장되는 클라우드 및 SaaS 환경
↳ ChatGPT와 같은 새로운 불투명한 AI 도구 포함
↳ 귀중한 소스 코드 노출 초래

Cloudflare One의 데이터 보호 제품군은 이렇게 확연한 최신 데이터 위험의 최전선을 맡도록 구축되었습니다.

Cloudflare에서는 포인트 솔루션을 단일 플랫폼과 네트워크에 통합하여 다음과 같은 특징을 가진 데이터 보호를 제공합니다.

- 연결 및 정책 관리 간소화로 **더 효과적임**
- 모든 장소에서 빠르고 안정적이며 일관된 사용자 경험을 보장하므로 **더 생산적임**
- 변화하는 보안 요구 사항을 충족하기 위해 빠르게 혁신하므로 **더 민첩함**

웹, SaaS, 비공개 앱에 걸쳐 데이터를 보호하는 단일 보안 서비스 에지(SSE)

계속해서 다음을 위한 SSE 여정에서 Cloudflare를 채택하세요.

1. Zero Trust를 통해 데이터에 대한 액세스 보호
2. 피싱, 랜섬웨어 등의 위협 차단
3. 가장 중요한 정보 감지 및 잠금

늘어나는 데이터 위험 알아보기…

무분별하게 확장되는 SaaS 풋프린트

82%

클라우드 환경에 저장된 데이터와 관련된 유출의 비율입니다.[1]

당연히 데이터 유출 비용은 늘어나고 – 있으며 지난 3년간 15%가 늘었습니다.[1]

새롭고 다양한 규제

71%

데이터 및 개인정보를 보호하기 위한 법률을 보유하고 있는 국가의 비율입니다.[2]

미국 **11개 주** 에서는 이제 포괄적인 데이터 보호 법률을 보유하고 있습니다. 2021년의 3개 주에서 늘어난 것입니다.[3]

디지털 변환

89%

디지털 변환 이니셔티브를 통한 빠른 변화로 회사 데이터 보호에 예상할 수 없는 위험이 초래될 것이라고 이야기하는 CISO의 비율입니다[4]

사용 사례 #1: 개발 코드 보호

문제
코드는 공개 리포지토리와 같이 눈에 잘 띄는 위치를 포함하여 수많은 개발자 도구에서 노출되거나 도난의 표적이 될 수 있습니다.

솔루션
코드 유출의 위험이 있는 GitHub와 같은 잘못 구성된 공개 리포지토리를 스캔하고 수정합니다. 업로드 및 다운로드 시 소스 코드를 감지하고 제어를 적용합니다.

→ GitHub
→ GitLab
→ Bitbucket

사용 사례 #2: 데이터 노출 가시성 및 위험 관리

→ OpenAI
→ Bard
→ GitHub Copilot

문제
데이터는 다양한 SaaS 및 클라우드 환경, 비승인 섀도우 IT, ChatGPT와 같은 새로운 AI 도구 등에 걸쳐 존재하며, 그에 따라 유출 위험이 높아집니다.

솔루션
중요한 데이터를 위한 통합 DLP 감지를 통해 잘못된 구성을 위해 SaaS 제품군을 스캔합니다. 비승인 앱 사용량에 대한 가시성을 얻고 이에 액세스하기 위해 Zero Trust 제어를 허용, 차단, 격리, 적용합니다.

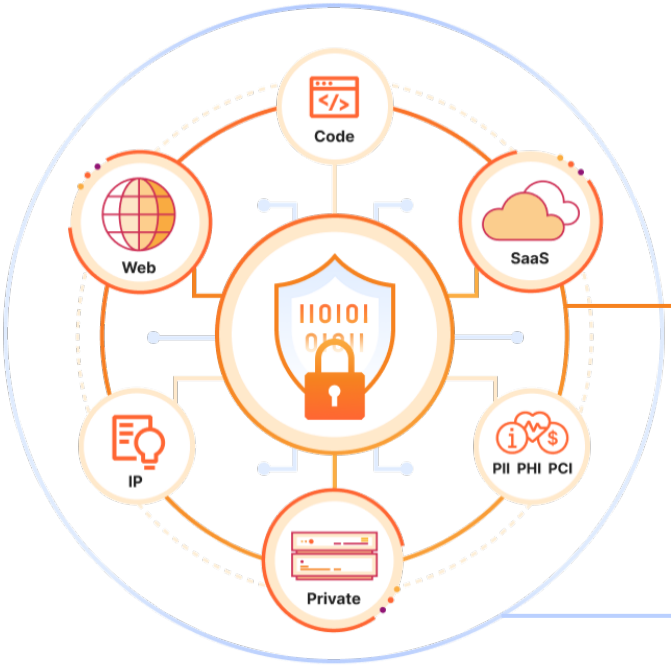
사용 사례 #3: 규제 준수

문제
규제 미준수로 인한 벌금이 늘어나고 있으며 데이터를 안전하고 비공개 상태로 유지하기 위한 회사의 법적 요구 사항이 더 엄격해지고 더 많은 비용이 들게 되었습니다.

솔루션
규제 대상 데이터 클래스(PII, 건강, 금융)에 대한 제어를 식별하고 적용합니다. 로그와 추가 SIEM 분석을 통해 상세한 감사 추적을 유지합니다. 포괄적인 Zero Trust 보안 상태로 공격 표면을 줄입니다.

- ✓ GDPR
- ✓ DPDP
- ✓ CCPA
- ✓ CPRA
- ✓ GLBA
- ✓ PCI DSS
- ✓ HIPAA
- ✓ ISO
- ✓ 기타 등등!

작동 방식



단일 통합 플랫폼
Cloudflare에서는 더 단순한 관리를 위해 DLP, CASB, ZTNA, SWG, RBI, 이메일 보안 서비스에 걸쳐 가시성과 제어를 단일 플랫폼으로 모읍니다.

프로그래밍 가능한 단일 네트워크
우리의 개발자 플랫폼에 구축된 서비스를 갖춘 하나의 제어판으로 웹, SaaS, 비공개 앱 환경 등 모든 적용 지점에서 전송 중, 사용 중, 미사용 중인 데이터에 대한 제어를 시행합니다.

구성 가능한 서비스를 통한 제어의 예시

전송되고 있는 데이터에 DLP 적용 및 액세스 보호

- 트래픽에 있는 중요한 데이터 및 파일을 스캔하고 DLP를 통해 차단 정책을 구성합니다.
- CASB를 통해 섀도우 IT를 파악하고 관리합니다.
- ZTNA를 통해 앱이 보유한 데이터에 대한 액세스를 보호합니다.
- SaaS 앱의 개인 테넌트를 차단하여 데이터 유출을 방지합니다.

사용되는 데이터를 보호하기 위해 앱 격리

- 장치 클라이언트 없이 복사/붙여넣기, 업로드/다운로드, 프린트, 키보드 입력을 차단합니다.
- 클라이언트리스 배포는 비관리형 장치, 타사 사용자, ChatGPT와 같은 AI 도구 등에 이상적입니다.
- 격리된 앱 내에서 DLP 정책을 적용합니다.

SaaS 앱에서 사용되지 않는 데이터 보호

- 의심스러운 활동, 잘못된 구성, 중요한 데이터에 대하여 SaaS 앱을 스캔합니다.
- SWG 정책을 통해 위험을 완화하기 위한 규범 조치를 취합니다.

규제 준수와 제어를 간소화하기 위해 통합

- 상관 관계와 감사를 위해 선호하는 SIEM으로 로그를 푸시합니다.
- API 기반 CASB 스캔을 위해 가장 인기 있는 SaaS 제품군 중 18개와 통합합니다.
- DLP 정책을 위해 Microsoft Information Protection(MIP) 레이블을 통해 지속해서 동기화합니다.

Cloudflare를 통한 더 나은 데이터 보호

더 효과적,
복잡성 절감

다양하고 유연한 옵션으로 연결을 단순화하여 시행을 위해 트래픽을 Cloudflare로 전송합니다.

ZTNA 및 RBI를 위해 SaaS 제품군 또는 클라이언트리스 모드에 API 기반 스캔을 사용하여 앱에 대한 액세스를 보호합니다. 프록시 트래픽을 전달하기 위해 여러 보안 서비스에 걸쳐 단일 장치 클라이언트 또는 광역 네트워크 온램프를 사용합니다.

사용자 경험 개선
으로 더 생산적임

Cloudflare 네트워크는 모든 곳에 존재하며 최종 사용자와 데이터가 어디에 있든 이들에게 가까운 단일 경로 검사를 통해 제어가 시행되는 것이 보장됩니다.

신뢰할 수 있고 성능을 떨어뜨리지 않는 최종 사용자 경험은 데이터 제어 시행이 작업을 절대 방해하지 않음을 의미합니다. 유사한 SSE 제품보다 빠른 속도가 입증되었습니다.

빠른 속도로 혁신하므로
더 민첩함

Cloudflare의 프로그래밍 가능한 네트워크 아키텍처를 통해 새로운 위험에 신속하게 대응할 수 있도록 기능을 빠르게 구축할 수 있습니다.

우리는 데이터 보호가 최신 상태를 유지할 수 있도록 새로운 보안 표준 및 프로토콜(예: IPv6 전용 연결 또는 HTTP/3 암호화)을 빠르게 채택합니다.

고객이 하는 이야기

"오늘날 Cloudflare One은 우리 사용자가 중요한 데이터와 도구를 ChatGPT, Bard 등의 도구와 공유할 수 없도록 해주므로 우리는 AI의 이점을 안전하게 누릴 수 있습니다... 앞으로 특히나 DLP 및 CASB와 같은 서비스를 위한 비전과 로드맵 방면에서 데이터를 보호하기 위한 Cloudflare의 지속적인 혁신이 기대됩니다."

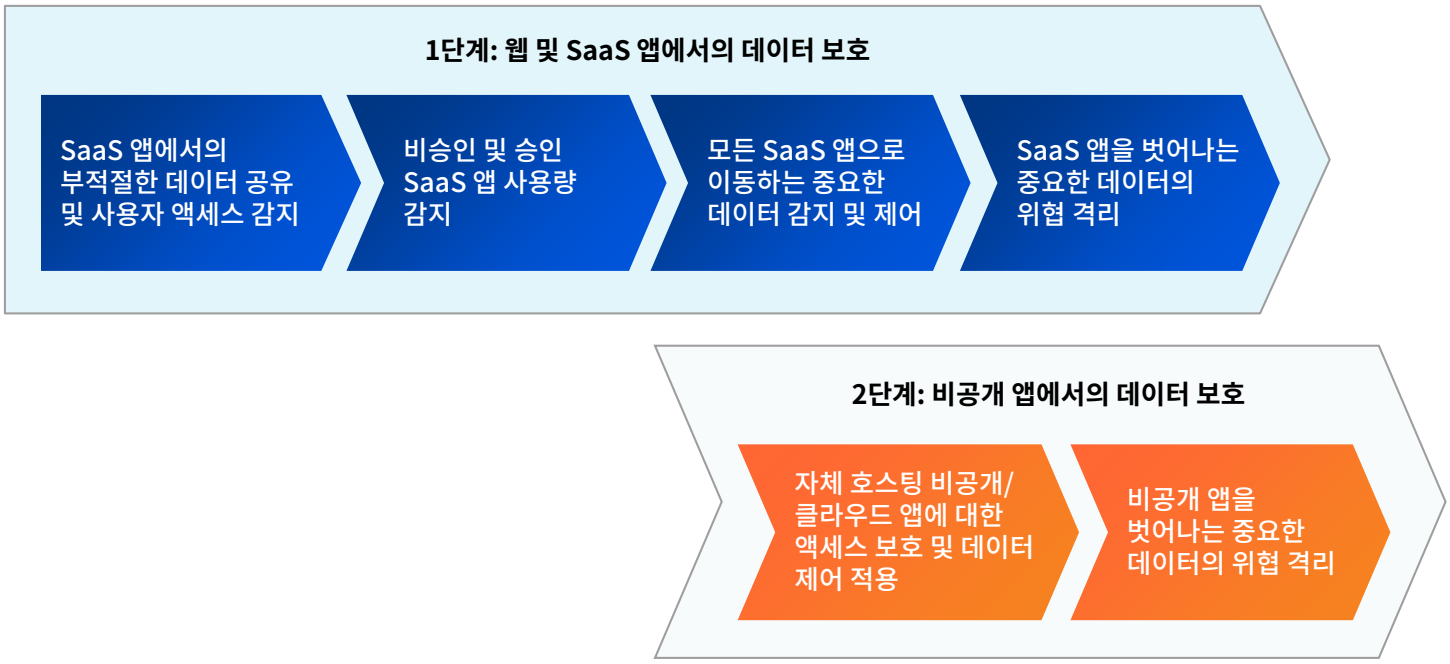
Tanner Randolph
최고 정보 보안 책임자(CISO)

Applied Systems
사례 연구 읽어보기

기타 사용 사례

- **Fortune 500 천연 가스 회사**, 계약업체의 데이터에 대한 액세스 보호
- **대규모 미국 구인구직 사이트**, 코드 및 개인 정보 보호
- **미국 지방 항공사**, 고객 데이터 노출의 위험 완화
- **호주 의료 회사**, 규제 대상 의료 데이터 보호
- **미국 의료기기 제조업체**, HIPAA 규정 준수 간소화

일반적인 채택 경로



시작하기

알아보기…

이 인포그래픽에서의 **늘어나는 데이터 위험**

참여하기…

이 데모에서의 플랫폼 작동 방식

입증하기…

자문 워크숍을 요청하는 것의 가치

1. 데이터 유출 비용 보고서 2023, IBM
2. 무역 및 개발에 관한 유엔 회의
3. International Association of Privacy Professionals(IAPP)
4. 2023 “CISO 현황” 보고서