통합 DLP 및 CASB

Cloudflare One은 데이터 가시성을 개선하고 모든 웹, SaaS, 셀프 호스팅/프라이빗 앱에 걸쳐 데이터가 이동하며 발생하는 유출 위험을 줄입니다.

어디서든 데이터 보호

최대 81%의 침해가 클라우드 환경에 저장된 데이터와 관련이 있습니다.

요즘 조직에서는 그 어느 때보다 더 많은 데이터를 처리하고 있습니다. 고객은 자신의 개인정보를 기업에 믿고 맡깁니다. 요즘의 지식 노동자는 작업을 수행하기 위해 클라우드 및 SaaS 환경에 걸쳐 데이터를 활용하고 공유해야 합니다. 또한, 코드는 회사에서 가장 중요한 자산이며 코드의 양은 매일 빠르게 늘어나고 있습니다. 기본적으로 어디에서든 중요한 데이터가 존재합니다.

통합 Data Loss Prevention(DLP) 및 멀티 모드 클라우드 액세스 보안 브로커(CASB)

하나의 구성 가능한 SSE 플랫폼에 구축된 Cloudflare DLP 및 CASB는 가시성을 쉽게 확장하고 모든 앱, 사용자, 장치에 걸쳐 데이터 보호 제어 기능을 통합합니다. 관리자를 위하여 단순하고 유연하게 배포할 수 있으므로 정책이 셀프웨어가 아니며 제대로 기능을 발휘합니다.

75% 여러 포인트 솔루션 사용과 관련하여 비용을 절감(또는 그 이하)한 비율 [1]

69% 가치가 낮은 작업에 사용하는 시간을 최소화한 비율(예: 위협 방어 정책 설정 및 구성) [1]

20% 데이터 유출 발생 가능성 및 관련 비용을 줄인 비율 [2]

안전하게 SaaS 앱 및 클라우드 수용

규제로 인한 벌금 방지

규제 대상 데이터에 대한 더 간소화된 정책 시행으로 데이터 규제 준수 위반으로 인한 재정적 손해와 평판 손해를 완화합니다.

SaaS 보안 간소화

기업에서 안전하고 자신 있게 새로운 SaaS 앱을 채택할 수 있도록 합니다. 지속적인 감지와 SaaS 위험에 대한 제어로 사각지대를 없앱니다.

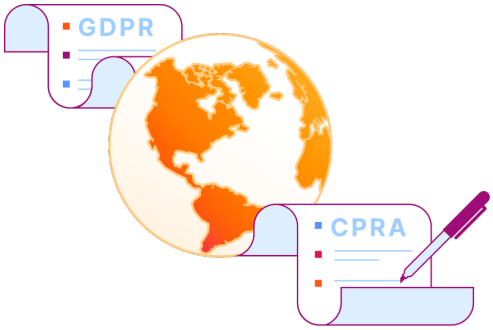
원하는 진행 속도로 확장

일상적인 운영을 방해하지 않고 데이터 보안을 도입합니다. 간단하게 구성할 수 있고 최종 사용자 경험이 원활합니다.

DLP 및 CASB 상위 사용 사례

규제 준수 간소화

포괄적인 Zero Trust 보안 상태로 데이터 유출로 인한 규제 준수 위반의 위험을 줄입니다. DLP는 규제를 받는 데이터 클래스(PII, 건강, 금융)에 대한 제어를 식별하고 적용합니다. 또한, 쉽게 규제를 준수할 수 있도록 로그와 추가 SIEM 분석을 통해 상세한 데이터 감사 추적을 유지합니다.

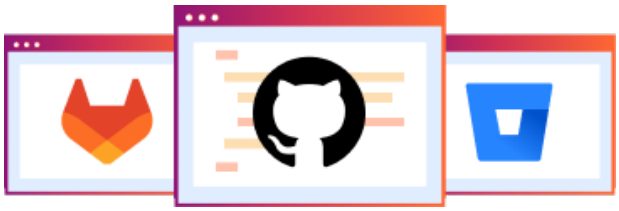


데이터 및 잘못된 구성의 위험에 대한 가시성 향상

알지 못하는 것은 보호할 수 없습니다. Cloudflare CASB는 중요한 데이터를 위한 통합 DLP 감지를 통해 잘못된 구성과 데이터 위협에 대해 SaaS 제품군을 스캔합니다. ChatGPT, Bard 등 새롭게 등장하는 AI 도구를 비롯한 비승인 앱 사용량에 대한 가시성을 빠르게 확보하세요. 그런 다음 허용하거나, 차단하거나, 액세스할 수 있도록 Zero Trust 제어를 적용하여 위험을 줄여보세요.

귀중한 IP 및 개발자 코드 보호

CASB는 코드 유출의 위험이 있는 GitHub와 같은 잘못 구성된 공개 리포지터리를 감지하고 수정합니다. 전송 중인 소스 코드에는 상세한 DLP 제어를 적용하여 사용자가 앱이나 장치에서 업로드/다운로드할 수 없게 만듭니다.



통합 데이터 보호 시작하기

Zero Trust 접근 방식으로 데이터를 더 적극적으로 보호하세요. 기업 사용자가 SaaS, 웹, 프라이빗 앱을 사용하는 방법을 확인하고 사용하는 종류를 세밀하게 파악하세요. 그런 다음 파악한 정보에 따라 데이터 제어와 ID/장치 기반 정책을 적용하여 공격면을 줄이세요.

데이터 이동에 관한 가시성 확보

- SaaS 앱에서 부적절하게 공유되는 중요한 데이터 감지
- 비승인 및 승인된 SaaS 앱 감지
- 감사를 위해 SIEM 공급자와 로그를 통합*

데이터 유출 위험 감소

- 모든 앱을 대상으로 유입되는 데이터의 종류/위치에 대해 DLP 제어 기능 적용
- SaaS 및 프라이빗 앱을 벗어나는 중요한 데이터에 대한 위협 격리*
- SaaS 및 셀프 호스팅 프라이빗/클라우드 앱에 대한 액세스 보호*

** SSE 및 SASE 플랫폼에서 ZTNA, SWG 및/또는 RBI 기능 사용*

DLP 작동 방식

클라우드로 마이그레이션하면서 중요한 정보를 추적하고 제어하기가 그 어느 때보다 더 어려워졌습니다. 직원들은 계속 늘어나는 다양한 도구를 사용하여 방대한 양의 데이터를 처리합니다. 한편 IT 및 보안 관리자는 중요한 데이터에 대한 액세스 권한이 필요한 사람, 데이터가 저장되는 방식, 데이터를 전송할 수 있는 위치를 파악하는 데 어려움을 겪습니다.

Data Loss Prevention을 사용하면 키워드, 패턴 등의 특성을 기반으로 데이터를 보호할 수 있습니다. 트래픽은 기업 인프라에 들어오고 나가면서 중요한 정보의 지표에 대해 검사를 받습니다. 지표가 발견되면 트래픽은 고객의 규칙에 따라 허용되거나 차단됩니다.

규제를 받는 데이터 클래스에 대한 쉽고 빠른 제어

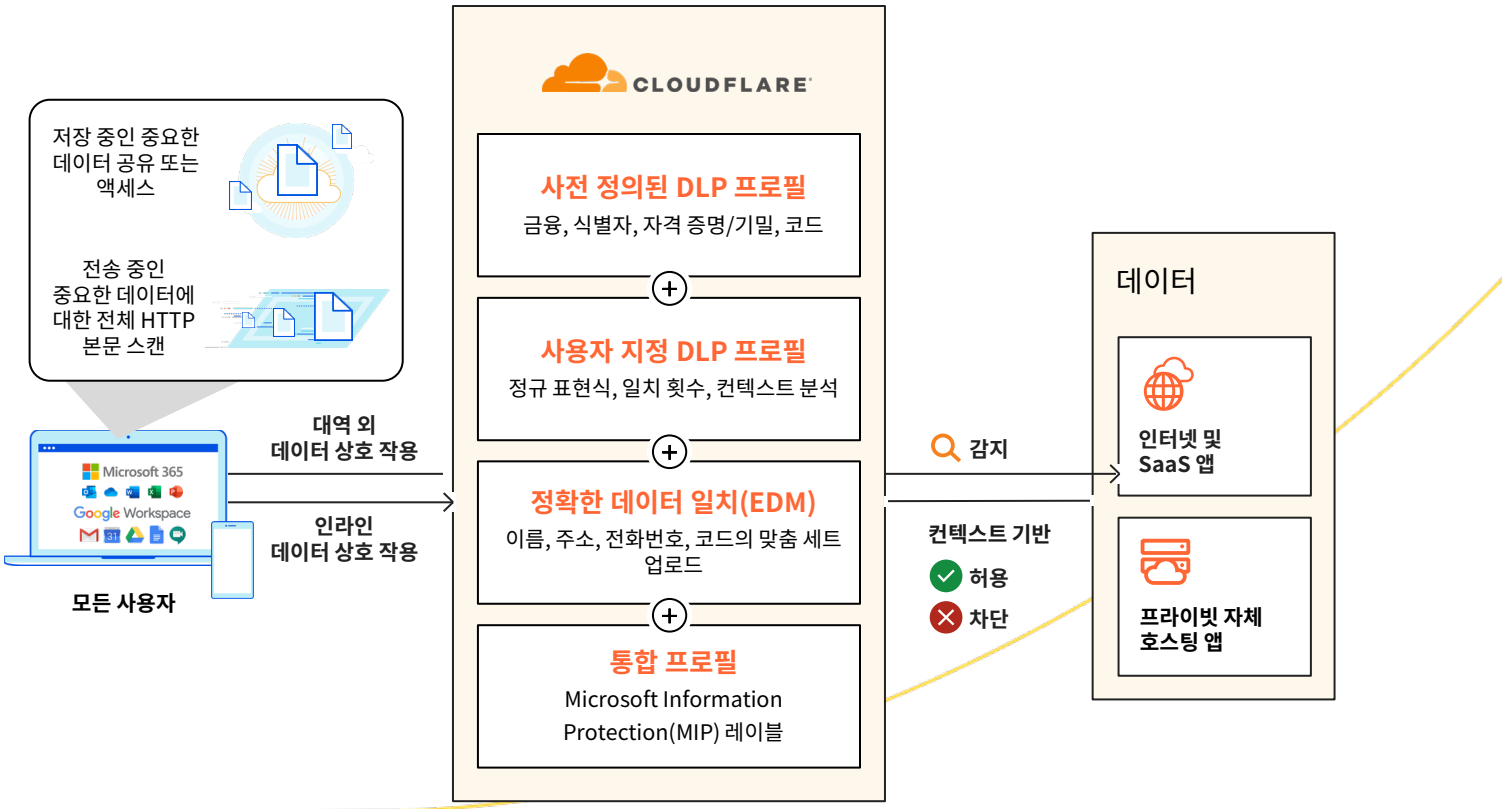
규제 준수 요건은 더 엄격해지고 있으며 범위가 넓어지고 있습니다. 사전 정의된 DLP 프로필을 빠르게 활성화하여 직원 네트워크 트래픽을 분석하고 PII, PHI, 기타 금융 정보(예: 계좌/신용 카드 번호)와 같은 규제를 받는 데이터의 공유를 차단하세요.

계속해서 변화하는 데이터 요구 사항을 위한 고급 사용자 정의

중요한 데이터의 정의는 산업과 운영 위치에 따라 여러 조직에 걸쳐 아주 다양할 수 있습니다. 컨텍스트 분석 및 정확한 데이터 일치를 포함한 사용자 지정 DLP 프로필을 생성하여 기밀, 코드, 자격 증명, IP 등의 다른 데이터 유형에 세부 제어를 적용하세요.

기존의 데이터 분류 도구로 원활한 통합

중요한 데이터에 대한 목록을 꼼꼼하게 유지하는 것은 보안 팀에 큰 부담이 됩니다. 그러므로 MIP와 같은 데이터 분류 도구가 필요합니다. 자동으로 중요한 레이블을 가져와 이를 사용하여 DLP 프로필을 채우는 Cloudflare 통합으로 복잡성을 늘리지 않으면서 민첩성을 개선하세요.



CASB 작동 방식

모든 앱 및 장치에 걸친 일관된 데이터 제어를 위해 인라인 CASB를 제공하는 기본적으로 구축된 SSE

각각의 SaaS 앱은 고려해야 할 보안 요건이 서로 다르며 전통적인 보안 경계의 보호 장치 밖에서 작동합니다. 조직에서 수십 가지 SaaS 앱을 도입하면서 일관된 보안, 가시성, 성능을 유지하기가 점점 더 어려워지고 있습니다.

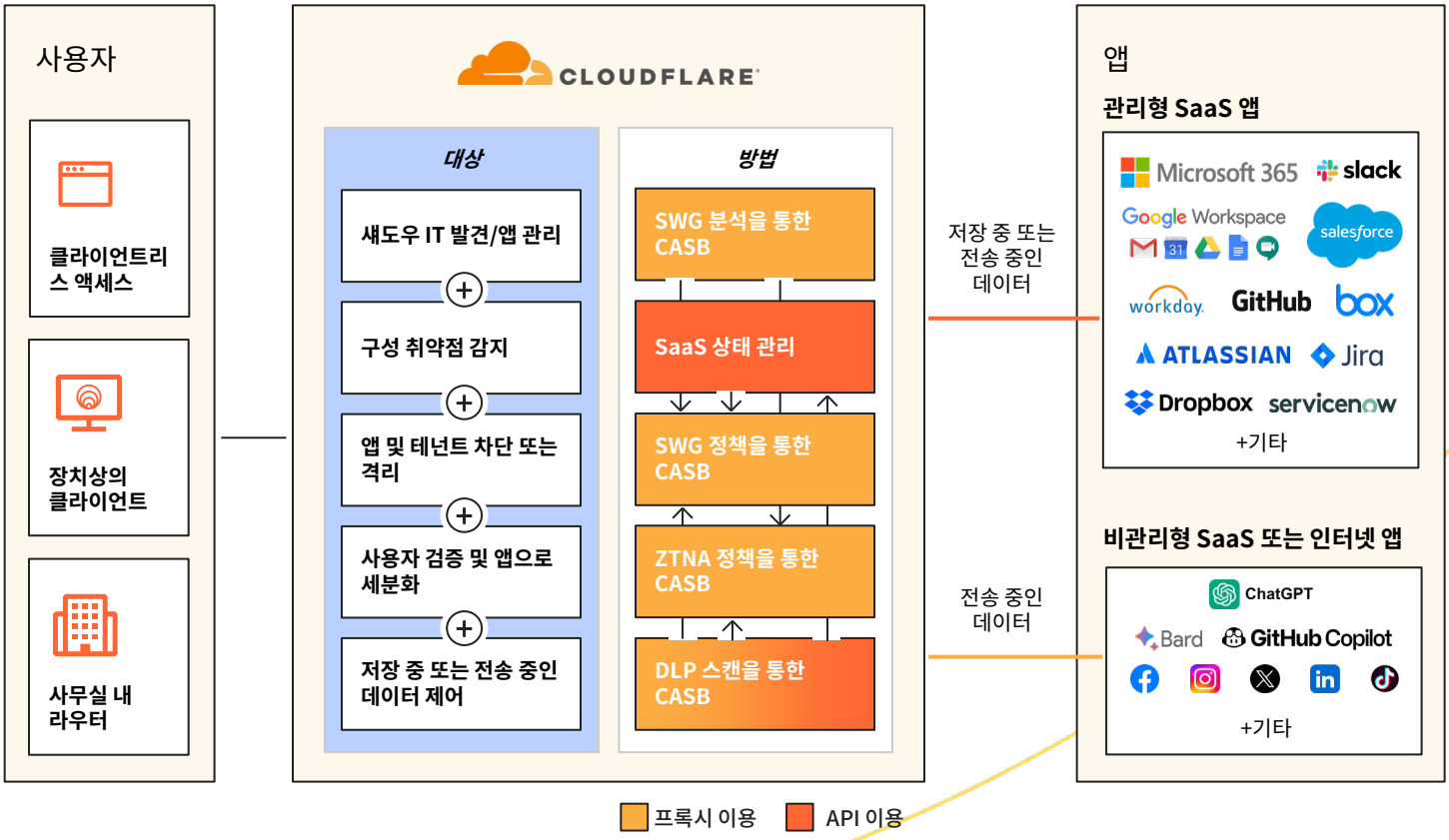
Cloudflare 인라인 CASB는 전송 중인 데이터를 보호하기 위해 앱에 ZTNA, SWG, RBI 제어를 적용합니다.

- 모든 HTTP 요청을 기록하여 섀도우 IT를 밝혀냄
- 위협 및 위험한 데이터 공유 차단/격리
- 모든 SaaS 앱에 대한 액세스 보호

관리형 SaaS 앱에 걸쳐 빠른 위험 가시성을 제공하는 쉬운 API CASB 통합

빠른 API 읽기 전용 통합을 통해 몇 분 만에 인기 SaaS 앱(Google Workspace, Microsoft 365 등)과 연결하세요.

사용 권한, 잘못된 구성, 부적절한 액세스, 제어 문제 등 데이터와 직원을 위험에 빠뜨릴 수 있는 문제에 대한 가시성을 제공하여 강력한 SaaS 보안 상태를 유지하고 IT 및 보안 팀을 지원하세요. 그런 다음 간단히 클릭하여 적용할 수 있는 SWG 정책 및 통합 DLP 스캐닝으로 CASB에서 드러난 위협을 빠르게 수정하세요.



고객이 하는 이야기

"지금 Cloudflare One은 우리 사용자가 중요한 데이터와 도구를 ChatGPT, Bard 등의 도구와 공유할 수 없도록 해주므로 우리는 AI의 이점을 안전하게 누릴 수 있습니다...

앞으로 데이터 보호 부문에서 Cloudflare의 지속적인 혁신을 기대합니다. 특히 DLP, CASB 등의 서비스에서의 비전과 로드맵을 주목하고 있습니다."

— **Applied Systems** CISO Tanner Randolph

APPLIED

Cloudflare는 포인트 솔루션인 Zscaler ZIA와 Cisco AnyConnect VPN을 대체했습니다.

좀 더 폭넓게 살펴보면, Cloudflare에서는 Applied Systems에서 직원, 애플리케이션, 네트워크 전반에 걸쳐 보안을 강화하도록 지원했습니다.

사례 연구 읽어보기

분석가의 견해

FORRESTER

Cloudflare, 2023년 3분기 The Forrester Wave™ Zero Trust 플랫폼 부문에서 우수 성과 기업으로 선정

SSE 시장에서 연이어 엄청난 모멘텀을 지녔다는 평가를 받은 Cloudflare는 혁신, 로드맵, 가격 유연성 및 투명성, 하이브리드 인력 지원 및 보호 부문에서 만점인 5점을 받았습니다.

보고서에 따르면 *"Cloudflare의 다양한 네트워크, DLP, 액세스 제어 정책은 단일 콘솔에서 관리되므로, 고객이 빠르게 배포하고 인터넷으로 인한 위협을 차단할 수 있습니다."*

전체 보고서 읽어보기

Gartner®

Cloudflare는 2023년 Gartner® Magic Quadrant™ SSE 부문의 유일한 신규 벤더입니다

Cloudflare는 2023년 Gartner® Magic Quadrant™ 보안 서비스 에지(SSE) 부문 보고서에서 인정받았습니다. 이번 선정은 하이브리드 근무 보안을 위해 Zero Trust 플랫폼을 지속해서 발전시키겠다는 우리의 노력이 인정받은 결과라고 생각합니다.

전체 보고서 읽어보기

통합 DLP 기능

DLP 프로필	감지할 데이터 패턴을 정의하세요. • **사전 정의된 DLP 프로필:** 금융 정보(예: 신용 카드 번호), 국가 식별자(PII), 건강 정보(PHI), 자격 증명 및 비밀(예: GCP/AWS 키), 소스 코드 • **사용자 지정 프로필**: 사용자 지정 감지를 구축하여 중요한 데이터의 고유한 유형 식별(예: 내부 프로젝트 이름, 출시되지 않은 제품 이름)
데이터 분류	타사 데이터 분류 공급자(예: Microsoft Information Protection(MIP) 중요도 레이블)과 DLP를 통합하세요. 공급자로부터 분류 정보를 가져오고, 이를 사용하여 Cloudflare DLP 프로필을 채우며, 일치하는 데이터를 허용하거나 차단할 정책을 활성화하세요.
일치 횟수	차단 또는 로깅과 같은 작업이 트리거되기 전에 프로필에서 활성화된 항목이 감지될 수 있는 횟수에 대해 사용자 지정 일치 횟수를 설정합니다.
컨텍스트 분석	컨텍스트 분석은 근접 키워드에 따라 DLP 감지를 제한합니다(최대 1,000바이트 거리).
사용자 지정 데이터세트	사용자 지정 데이터세트에 정의된 특정 데이터에 대해 웹 트래픽과 SaaS 앱을 분석합니다. 중요도를 위해 로그에 있는 데이터를 삭제/해시할 수 있습니다. • **정확한 데이터 일치:** 고객 이름, 주소, 전화번호, 신용 카드 번호 등 가장 중요한 PII 세트를 지정합니다. 모든 데이터는 Cloudflare에 도달하기 전에 암호화됩니다. • **사용자 지정 단어 목록:** IP, SKU 번호 등 중요하지 않은 데이터를 보호합니다.

멀티 모드 CASB 기능

위험 가시성 및 규제 준수	
API 기반 스캐닝	타사 SaaS 앱을 통합하여 사용자가 성공적으로 로그인한 후 발생할 수 있는 잘못된 구성, 무단 사용자 활동, 섀도우 IT, 데이터 보안 문제 등의 보안 결과에 대해 사용되고 있지 않은 데이터를 스캔하세요. 18가지 이상의 통합(예: Microsoft 365, Google Workspace)이 제공됩니다.
섀도우 IT 발견	최종 사용자가 방문하는 SaaS 앱 및 프라이빗 네트워크 원본에 대한 섀도우 IT 가시성입니다. 발견된 앱을 검토하고 승인 상태(승인, 미승인, 검토 중, 미검토)를 조정하세요. 그에 따라 상세한 ID 및 장치 기반 정책*을 설정하세요.
감사 로깅	모든 요청, 사용자, 장치를 위한 포괄적인 로깅*입니다. logpush* 또는 API를 사용하여 규제 준수 감사를 위해 기존 타사 스토리지 또는 SIEM 도구와 통합합니다.
데이터 보호 및 위협 방지	
Zero Trust 액세스*	사용자의 데이터에 대한 액세스를 제한하기 위해 ZTNA를 통해 앱별로 최소 권한 정책을 설정하세요
파일 공유 제어*	HTTP SWG 정책을 통해 MIME 유형에 따라 파일 업로드/다운로드를 허용하거나 차단하세요
앱 제어*	HTTP SWG 정책을 통해 앱 유형 또는 특정 앱에 대한 트래픽을 허용하거나 차단하세요
테넌트 제어*	데이터 손실을 방지하기 위해 SWG를 통해 트래픽 SaaS 앱 테넌트를 제어하세요
브라우저 제어*	RBI를 통해 격리된 웹 페이지 및 애플리케이션 내에서 다운로드, 업로드, 복사/붙여넣기, 키보드 입력, 인쇄 작업을 제한하여 브라우저에서 사용 중인 데이터를 보호하세요. 로컬 장치로의 데이터 유출을 차단하고 의심스러운 웹 사이트에서 사용자 입력을 제어하세요.
DLP 스캐닝*	SWG를 통해 HTTP 트래픽을 스캔하세요. DLP 프로필 구성에 명시된 키워드 또는 정규 표현식과 일치하는 문자열로 중요한 데이터를 찾을 수 있습니다. CASB 통합에서 DLP 프로필을 활성화하고 SaaS 앱에 저장된 파일에 중요한 데이터가 포함되어 있는지 확인하세요. 모든 HTTP 기반 정책이 유지되는 클라이언트리스 RBI를 통해 프라이빗 앱에 대한 DLP를 확장하세요.

** SSE 및 SASE 플랫폼에서 ZTNA, SWG 및/또는 RBI 기능 사용*

왜 Cloudflare를 사용해야 할까요?

단일 통합 플랫폼

안전한 액세스
모든 사용자를 검증하고 모든 리소스로 세분화

위협 방어
네트워크 기반 AI/ML 및 위협 인텔리전스로 모든 채널을 커버

데이터 보호
(전송 중, 저장 중, 사용 중인 데이터의 가시성과 제어 능력 강화)

프로그래밍 가능한 단일 네트워크

더 효과적
연결 및 정책 관리 간소화

더 생산적
모든 장소에서 빠르고, 안정적이며, 일관된 사용자 경험 보장

변화하는 보안 요구 사항을 충족하기 위해 빠르게 혁신하므로 **더 민첩함**

귀사의 데이터 보호 관련 필요 사항에 대해 상담할 준비가 되셨나요?

워크숍 요청하기

아직 실시간 대화를 할 준비가 되지 않으셨나요?

Cloudflare의 SSE 및 SASE 플랫폼
자세히 알아보기

1. 2023년 설문조사: techvalidate.com/product-research/cloudflare/charts
2. IBM 유출 비용 보고서: https://www.ibm.com/reports/data-breach