CLOUDFLARE

KURZDARSTELLUNG

Schützen Sie Sensible Daten

Bessere Netzwerkarchitektur für effektiveren, produktiveren und flexibleren Datenschutz.

Einheitlicher Datenschutz an jedem Ort

Datenschutz ist kein neues Gebot, aber die Umstellung auf hybride Cloud-Architekturen in Verbindung mit der schnellen Einführung von KI bringt neue Herausforderungen mit sich:

- **93 % der Mitarbeitenden** geben zu, dass sie ohne vorherige Genehmigung Informationen in KI-Tools eingeben[1]
- **79 % aller Länder** haben Datenschutzgesetze[2]

Cloudflare setzt einheitliche Kontrollen über den gesamten Lebenszyklus Ihrer Daten durch:

- **Überall sichern:** Setzen Sie einheitliche Kontrollen für Web-, SaaS-, E-Mail- und Cloud-Datenverkehr durch.
- **KI-Exfiltration blockieren:** Analysieren Sie GenAI-Prompts, um sensible Daten zu blockieren und die KI-Nutzung zu regeln.
- **Datenrisiken verwalten:** Entdecken und verwalten Sie Schatten-IT/KI und scannen Sie SaaS-/Cloud-Anwendungen mit CASB.

„Die Zunahme all dieser nicht autorisierten KI-Tools veranlasst uns, unseren Sicherheitsansatz zu überdenken. Wir befassen uns jetzt mit SASE." – *Leiter der Informationssicherheit,* ***AllSaints***

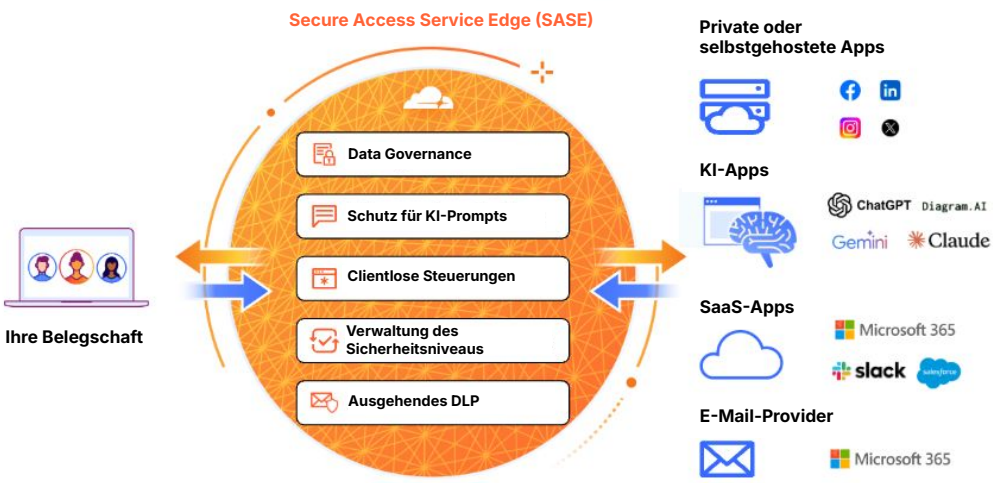
Warum SASE anstelle von Enterprise DLP?

Die Secure Access Service Edge (SASE)-Plattform von Cloudflare ist so konzipiert, dass sie zwischen Ihren Mitarbeitenden und jeder Anwendung sowie Datenquelle sitzt. SASE bietet damit einen optimalen Startpunkt für den Schutz sensibler Daten.

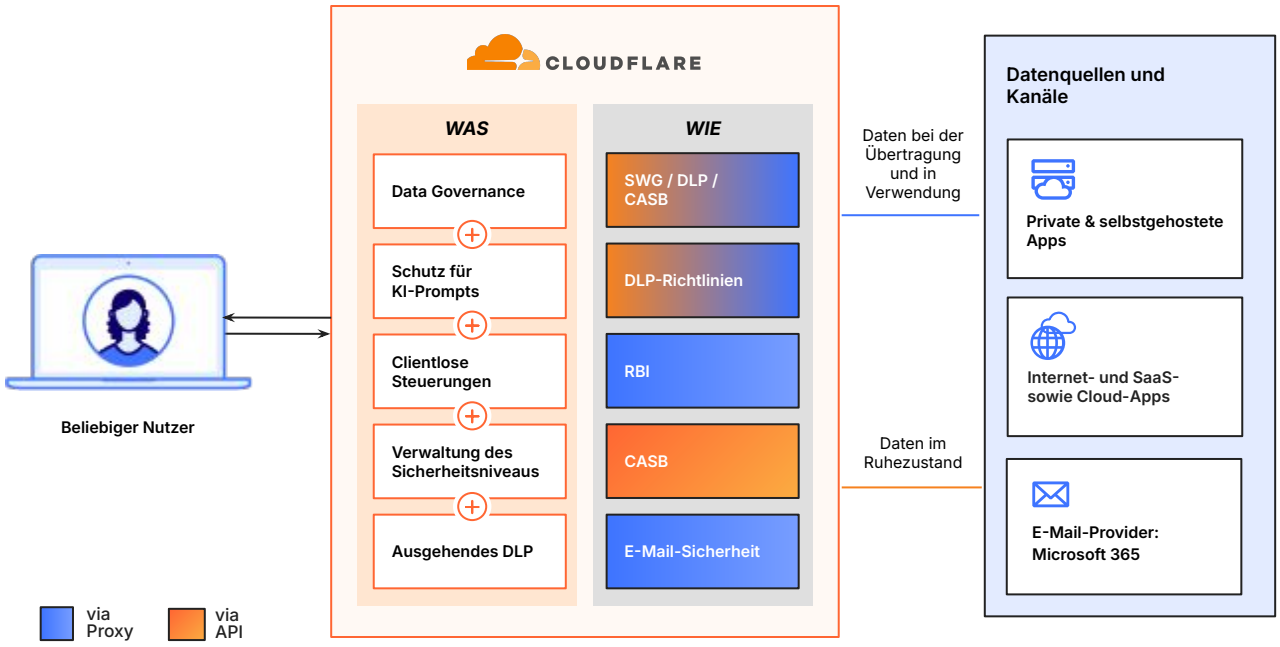
Ob Mitarbeitende in SaaS-Anwendungen auf Daten zugreifen, vertrauliche Dateien herunterladen oder mit GenAI-Tools chatten: Die SASE-Plattform von Cloudflare setzt einheitliche Sicherheitskontrollen für alle Dateninteraktionen durch.

So funktioniert's

Die SASE-Plattform von Cloudflare sitzt inline zwischen Ihrer Belegschaft und Ihren Ressourcen, um Transparenz und Kontrolle zu vereinen.



KI-gestützter Datenschutz mit der SASE-Plattform von Cloudflare
im Web, in SaaS, E-Mails und im Cloud-Traffic



Inline-Datenschutz in Echtzeit

- **Präzise DLP:** Stoppen Sie die Offenlegung sensibler Daten mit kontextbewussten Erkennungen für PII, Quellcode, Kundendaten und mehr.
- **DLP für ausgehende E-Mails:** Sensible Daten in ausgehenden E-Mails automatisch kennzeichnen, um versehentliche Datenlecks zu verhindern.
- **Prompt-Schutz:** Erkennen und Blockieren riskanter KI-Prompts und -Antworten basierend auf der Absicht (z. B. Jailbreak-Versuche, Code-Missbrauch, PII-Anfragen).

Schatten-IT und weitere Sicherheitsrisiken

- **Erkennung von Schatten-IT und KI:** Entdecken und Verwaltung von Schatten-IT/KI in Ihrer Umgebung. Quantifizieren Sie das Risiko mit Zuverlässigkeitswerten für Apps und Datenübertragungsmetriken, um die Gefährdung schnell zu mindern.
- **Verwaltung des Sicherheitsstatus:** Durchsuchen Sie SaaS-Anwendungen und Cloud-Umgebungen nach Sicherheitsrisiken. Ergreifen Sie präskriptive Schritte, um Sicherheitsergebnisse zu beheben.
- **Mandantensteuerung:** Persönliche Mandanten von SaaS-Anwendungen sperren, um Datenexfiltration zu verhindern.

Sichere Zugriffs- und Client-Kontrollen

- **Sicherer Anwendungszugriff:** Setzen Sie Zero Trust-Netzwerkzugang (ZTNA)-Regeln – wie z. B. das fein abgestimmte DLP-Scannen für agentenbasierte KI-Verbindungen – bei allen Firmenanwendungen durch.
- **Gerätestatusprüfungen:** Kontrollieren Sie den Zugriff auf Grundlage von fein abstimmbaren Gerätestatusprüfungen wie Festplattenverschlüsselung und aktivierter Endpunkt-DLP.
- **Clientlose Kontrollen:** Wenden Sie browserbasierte Datenkontrollen an, um den Zugriff von Drittanbietern und die BYOD-Richtlinien der Mitarbeitenden zu schützen.

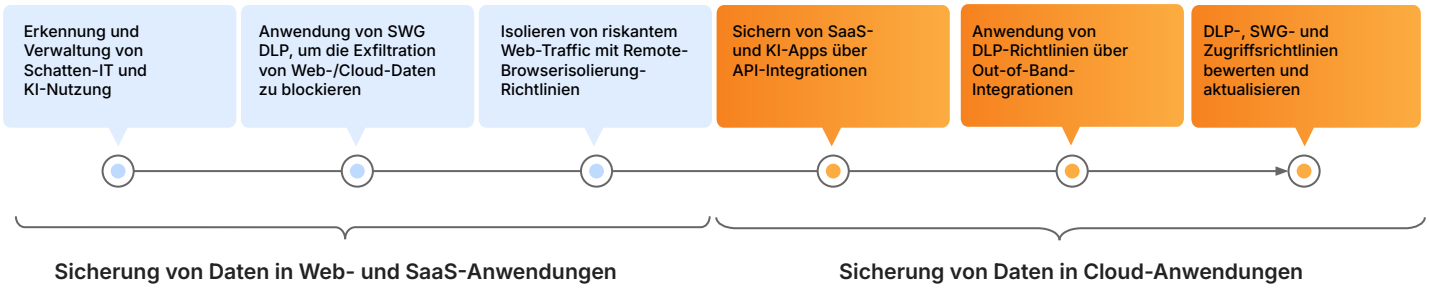
Integrationen und Berichte

- **CASB-Integrationen:** Nahtlose Integration mit führenden SaaS- und KI-Plattformen (einschließlich Microsoft 365, Google Workspace und ChatGPT) für API-basierte CASB-Scans.
- **Microsoft MIP-Integration:** Kontinuierliche Synchronisierung mit Microsoft Information Protection (MIP)-Labels für konsistente DLP-Richtlinien.
- **Observability & Forensics**: Protokollieren Sie Daten sicher in Ihrem bevorzugten SIEM für Audits, oder analysieren Sie Protokolle sofort über Dashboard oder API.

Beispiel für eine Implementierung im Bereich Datenschutz

Beginnen Sie damit, die Nutzung von Schatten-IT und KI zu ermitteln, um die Angriffsfläche sichtbar zu machen. Konfigurieren Sie grundlegende DLP-Richtlinien für SWG, um risikoreiche Datenlecks aus nicht verwalteten Cloud-Anwendungen zu blockieren, und setzen Sie Remote-Browserisolierung für nicht genehmigten Web-Traffic ein.

Setzen Sie dann CASB ein, um sanktionierte SaaS- und KI-Anwendungen zu sichern, indem Sie Fehlkonfigurationen beheben und interne Freigaberichtlinien durchsetzen. Verfeinern und integrieren Sie präzise DLP- und Zugriffsrichtlinien für SWG, E-Mail und CASB, um eine automatisierte, einheitliche Prävention über alle wichtigen Datenvektoren hinweg zu erreichen.



Beispiele für Anwendungsfälle zum Einstieg

- **Blockieren Sie die Exfiltration von PII/PHI in Echtzeit** über alle nicht genehmigten Kommunikations- und Speicherkanäle.
- **Schützen Sie Quellcode und geistiges Eigentum (IP)** vor Insider-Diebstahl und unbefugter Verbreitung.
- **Setzen Sie Prompt-Schutzrichtlinien** für GenAI-Anwendungen durch, um die Offenlegung sensibler Daten und die Modellkontamination zu verhindern.
- **Verhindern Sie Fehlkonfigurationen** und setzen Sie präzise Zugriffskontrollen für alle SaaS- und KI-Anwendungen durch.

Ergebnisse für Kunden

EESTI RAUDTEE

Infrastrukturanbieter
Kundenreferenz lesen

Eindämmung von Datenverlust und SaaS-Schwachstellen

durch die Identifizierung von Datenlecks und Fehlkonfigurationen.

APPLIED

Versicherungstechnologie
Kundenreferenz lesen

Isolierung öffentlicher GenAI-Tools wie ChatGPT,

um das Kopieren und Einfügen von sensiblen Daten zu verhindern

Führende Gesundheits-App
Kundenreferenz lesen

Schutz von Patientendaten

und eine wirksame Einhaltung von E-Mail-Sicherheit und Zero-Trust-Prinzipien.

CREDIT SAISON INDIA

NBFC-Kreditgeber
Kundenreferenz lesen

Schutz von persönlich identifizierbaren Informationen und wirksame Compliance,

um unerwünschten Datenabfluss zu verhindern.

Möchten Sie Ihre Anforderungen im Bereich Datenschutz besprechen?

Für Workshop anmelden

1. 2025 Manage Engine-Studie: Quelle
2. 2025 United Nations Conference on Trade & Development: Quelle