CLOUDFLARE

KURZDARSTELLUNG

Datenschutz mit Cloudflare One

Bessere Netzwerkarchitektur für effektiveren, produktiveren und flexibleren Datenschutz.

Einheitlicher Datenschutz an jedem Ort

Moderne Datenrisiken erfordern moderne Sicherheit
Die Menge, die Vielfalt und die Geschwindigkeit von Daten explodieren heutzutage. Dadurch sind Unternehmen mit zunehmenden Risiken konfrontiert:

Wildwuchs bei Cloud- und SaaS-Umgebungen
↳ einschließlich undurchsichtiger neuer KI-Tools wie ChatGPT
↳ dies führt zur Offenlegung von wertvollem Quellcode

Die Datenschutz-Suite von Cloudflare One wurde entwickelt, um diesen modernen Risiken einen Schritt voraus zu sein.

Indem Cloudflare einzelne Lösungen auf einer einzigen Plattform und in einem einzigen Netzwerk vereint, bietet Cloudflare zuverlässigen, wirksamen Datenschutz:

- **Mehr Effektivität** durch vereinfachte Konnektivität und Richtlinienverwaltung
- **Mehr Produktivität** durch schnelle, zuverlässige und einheitliche Nutzererlebnisse - überall
- **Mehr Flexibilität** durch schnelle Innovation, damit Sie Ihre sich wandelnden Sicherheitsanforderungen erfüllen können

Eine Security Services Edge (SSE) zum Schutz von Daten im Web, bei SaaS und privaten Anwendungen

Führen Sie Cloudflare schrittweise in Ihrer Umstellung auf SSE ein und profitieren Sie von diesen Vorteilen:

1. Sichern des Datenzugriffs mit Zero Trust
2. Stoppen von Bedrohungen wie Phishing und Ransomware
3. Erkennen und Sperren Ihrer sensibelsten Daten

Bewältigen Sie zunehmende Datenrisiken...

Ausufernde SaaS-Angriffsfläche

82 %

der Verstöße betrafen Daten, die in Cloud-Umgebungen gespeichert waren.[1]

Und natürlich steigen die Kosten für Datenverstöße weiter an – in den letzten 3 Jahren um 15 %. [1]

Neue, vielfältige Vorschriften

71 %

aller Länder haben Gesetze zum Schutz von Daten und Privatsphäre.[2]

In den USA haben inzwischen **11 Bundesstaaten** umfassende Datenschutzgesetze – im Jahr 2021 waren es erst 3.[3]

Digitale Transformation

89 %

der CISOs geben an, dass die schnelle Umsetzung von Initiativen zur digitalen Transformation unvorhergesehene Risiken bei der Sicherung von Unternehmensdaten mit sich bringt[4]

1. Anwendungsfall: Schutz von Entwicklercode

Problem
Code kann über viele Entwicklertools offengelegt oder gestohlen werden, auch an gut sichtbaren Orten wie öffentlichen Repositories.

Lösung
Suchen Sie nach falsch konfigurierten öffentlichen Repositories wie GitHub, bei denen die Gefahr von Codelecks besteht, und beheben Sie diese. Erkennen Sie Quellcode in Up-/Downloads und wenden Sie Kontrollen an.

→ GitHub
→ GitLab
→ Bitbucket

2. Anwendungsfall: Sichtbarkeit der Datenoffenlegung und Risikomanagement

→ OpenAI
→ Bard
→ GitHub Copilot

Problem
Die Daten erstrecken sich über verschiedene SaaS- und Cloud-Umgebungen, nicht genehmigte Schatten-IT und aufkommende KI-Tools wie ChatGPT, was das Risiko von Datenlecks erhöht.

Lösung
Scannen Sie SaaS-Suites auf Fehlkonfigurationen mit integrierter DLP-Erkennung für sensible Daten. Sorgen Sie für Transparenz bei der Nutzung nicht genehmigter Apps und erlauben, blockieren, isolieren oder wenden Sie Zero Trust-Kontrollen an, um den Zugriff darauf zu ermöglichen.

3. Anwendungsfall: Einhaltung von Vorschriften

Problem
Strengere und umfassendere gesetzliche Anforderungen an Unternehmen, Daten sicher und geheim zu halten, mit immer höheren Geldstrafen bei Nichteinhaltung.

Lösung
Identifikation und Anwendung von Kontrollen für regulierte Datenklassen (personenbezogene Daten, Gesundheit, Finanzen). Pflege von detaillierten Prüfpfaden über Protokolle und weitere SIEM-Analysen. Reduzierung der Angriffsfläche durch eine umfassende Zero Trust-Sicherheitsarchitektur.

✓ DSGVO ✓ DPDP
✓ CCPA ✓ CPRA
✓ GLBA ✓ PCI DSS
✓ HIPAA ✓ ISO
✓ Und viele mehr!

So funktioniert's

Eine einheitliche Plattform
Cloudflare bündelt die Sichtbarkeit und Steuerung von DLP-, CASB-, ZTNA-, SWG-, RBI- und E-Mail-Sicherheitsservices auf einer einzigen Plattform, um die Verwaltung zu vereinfachen.

Ein programmierbares Netzwerk
Eine Kontrollebene mit Diensten, die auf unserer eigenen Entwicklerplattform basieren, um Kontrollen für Daten bei der Übertragung, bei der Verwendung und im Ruhezustand über alle Durchsetzungspunkte hinweg durchzusetzen – Web, SaaS oder private Anwendungsumgebungen.

Beispiel für Kontrollen mit zusammensetzbaren Diensten

Anwendung von DLP für Daten bei der Übertragung und sicheren Zugriff

- Scannen nach sensiblen Daten im Traffic und in Dateien und Konfigurieren von Sperrrichtlinien mit DLP.
- Entdecken und verwalten von Schatten-IT mit CASB.
- Sicherer Zugriff auf Daten in Anwendungen mit ZTNA.
- Sperren persönlicher Mandanten von SaaS-Anwendungen, um Datenexfiltration zu verhindern.

Isolieren von Anwendungen, um die verwendeten Daten zu sichern

- Blockieren von Kopieren/Einfügen, Hoch-/Herunterladen, Drucken, Tastatureingaben – alles ohne Geräte-Client.
- Die clientlose Bereitstellung ist ideal für nicht verwaltete Geräte, Nutzer von Drittanbietern und KI-Tools wie ChatGPT.
- Anwendung von DLP-Richtlinien innerhalb isolierter Anwendungen.

Schutz von Daten im Ruhezustand in SaaS-Anwendungen

- Scannen von SaaS-Anwendungen auf verdächtige Aktivitäten, Fehlkonfigurationen und sensible Daten.
- Ergreifen vordefinierter Schritte zur Behebung von Risiken mittels SWG-Richtlinien.

Integration zur Optimierung von Compliance und Kontrollen

- Logpush an Ihr bevorzugtes SIEM für Korrelation und Audit.
- Integration mit 18 der beliebtesten SaaS-Suiten für API-basierte CASB-Scans.
- Kontinuierliche Synchronisierung mit Microsoft Information Protection (MIP)-Labels für Ihre DLP-Richtlinien.

Besserer Datenschutz mit Cloudflare

Mehr Effektivität ***durch weniger Komplexität***

Vereinfachen Sie die Konnektivität mit vielen flexiblen Optionen, um Traffic zur Durchsetzung an Cloudflare zu senden.

Verwenden Sie API-basierte Scans für SaaS-Suites oder clientlose Modi für ZTNA und RBI, um den App-Zugriff zu sichern. Verwenden Sie zur Weiterleitung von Proxy-Traffic einen Geräte-Client oder Wide-Area-Network-On-Ramps über Sicherheitsdienste.

Mehr Produktivität ***durch eine verbesserte Nutzererfahrung***

Unser Netzwerk ist überall präsent und stellt sicher, dass die Kontrollen mit Single-Pass-Überprüfung in der Nähe der Nutzer und Daten durchgesetzt werden, egal wo sie sich befinden.

Zuverlässig und unaufdringlich – der Endnutzer wird durch die Durchsetzung von Datenkontrollen nicht in seiner Arbeit unterbrochen. Bewiesenermaßen schneller als SSE-Mitbewerber.

Mehr Flexibilität ***durch raschere Innovation***

Dank unserer programmierbaren Netzwerkarchitektur können wir schnell Kapazitäten aufbauen, so dass Sie sich flexibel an neue Risiken anpassen können.

Wir übernehmen rasch neue Sicherheitsstandards und -protokolle (z. B. reine IPv6-Verbindungen oder HTTP/3-Verschlüsselung), damit der Datenschutz auf dem neuesten Stand bleibt.

Was unsere Kunden sagen

„Cloudflare One verhindert, dass unsere Nutzerinnen und Nutzer in Tools wie ChatGPT und Bard sensible Daten und Quellcode offenlegen…Für die Zukunft freuen wir uns auf weitere Cloudflare-Innovationen im Bereich des Datenschutzes und insbesondere auf ihre Vision und Roadmap für Dienste wie DLP und CASB.“

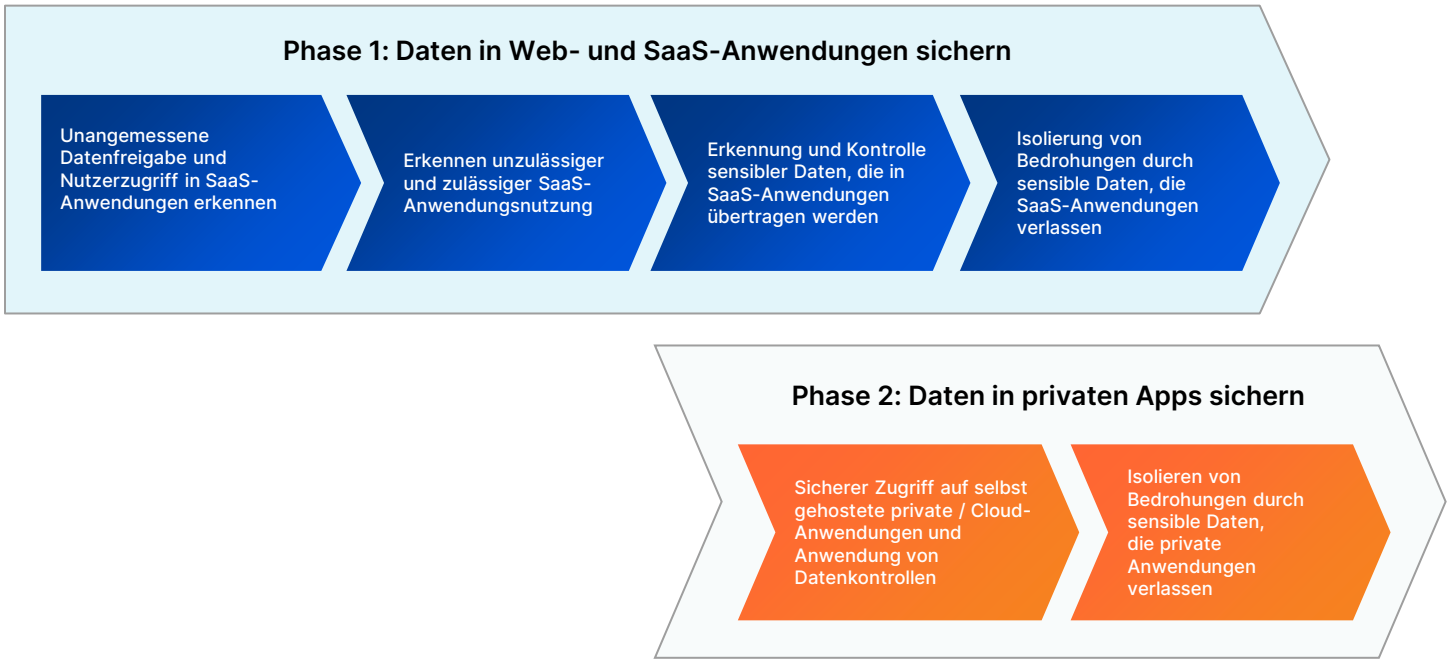
Tanner Randolph
Chief Information Security Officer (CISO)

Applied Systems
Kundenreferenz lesen

Andere Anwendungsfälle

- **Fortune-500-Erdgasunternehmen** schützt Zugang zu Daten von Auftragnehmern
- **Große US-Jobbörse** schützt Code und persönliche Daten
- **Regionale US-Fluggesellschaft** mindert das Risiko der Offenlegung von Kundendaten
- **Australischer Gesundheitsdienstleister** schützt regulierte medizinische Daten
- **US-Hersteller von Medizingeräten** optimiert die Einhaltung des HIPAA

Gängige Pfade zur Einführung



Erste Schritte

ERFAHREN...

Sie mehr über eskalierende Datenrisiken in dieser Infografik

VERTIEFEN...

Sie sich in die Funktionsweise der Plattform – mit dieser Demo

ÜBERZEUGEN...

Sie sich vom Mehrwert, indem Sie einen beratenden Workshop anfordern

1. Cost of a Data Breach Report 2023, IBM
2. United Nations Conference on Trade & Development
3. International Association of Privacy Professionals (IAPP)
4. „State of the CISO 2023"-Bericht