CLOUDFLARE

KURZDARSTELLUNG

Cloud Access Security Broker

Durch umfassende Übersicht und Kontrolle über SaaS-, KI- und Cloud-Umgebungen werden Daten geschützt, ohne Innovationen zu behindern.

SaaS-Sicherheit für das KI-Zeitalter

SaaS-, KI- und Cloud-Umgebungen werden ohne Produktivitätseinbußen geschützt. Der CASB von Cloudflare zeigt Fehlkonfigurationen, Schatten-IT und Datenrisiken für die gesamte hybrid arbeitende Belegschaft auf.

- **Compliance automatisieren:** Sicherheitslücken – wie nicht genehmigte Dateifreigaben oder eine unzureichende MFA – innerhalb von Microsoft 365, Google Workspace und GitHub werden sofort erkannt und behoben.
- **Schatten-KI/-IT stoppen:** Nicht autorisierte Anwendungen werden aufgespürt und der Zugang zu nicht genehmigten Cloud-Speicher- oder File-Sharing-Websites wird gesperrt.
- **KI-Nutzung absichern:** Durch den Überblick über die Einführung von KI-Tools und die Durchsetzung von Mandantenbeschränkungen auf Plattformen wie ChatGPT und Gemini wird sichergestellt, dass nur auf Systeme zugegriffen wird, die vom Unternehmen gebilligt werden.
- **Drittanbieter-Risiko eindämmen:** Risikobehaftete Integrationen von Drittanbietern, die Zugriff auf Firmendaten haben, werden ermittelt und rückgängig gemacht.

Der API-orientierte und interne Schutz des Cloudflare-CASB stützt sich auf unser globales Netzwerk und gewährleistet schnelle, kosteneffiziente und maßstabsgerechte Sicherheit.

EESTI RAUDTEE

Infrastruktur-anbieter

Kenntnis bekannter SaaS-Schwachstellen – wie eine weitreichende Verbreitung sensibler SharePoint-Dateien – trägt zur Eindämmung von Datenverlusten bei

Zur Fallstudie

APPLIED

Anbieter von Versicherungs software

Abgesicherte Einführung generativer KI durch Blockieren der Eingabe sensibler Daten bei Tools wie ChatGPT ohne Beeinträchtigung der Mitarbeiterproduktivität

Zur Fallstudie

Telemedizin-Anbieter

Schutz sensibler Patientendaten (PHI/HIPAA) und schnellerer Zugriff für eine rasch wachsende Zahl von Remote-Mitarbeitenden mittels DLP und CASB

Cloudflare macht den Unterschied

Sofortige Clientless-Bereitstellung

Per API lässt sich in wenigen Minuten eine Verbindung zu SaaS- und KI-Anwendungen wie Microsoft 365, GitHub, Slack und ChatGPT herstellen. Es müssen keine Clients installiert werden, um Systeme sofort nach bereits bekannten Risiken, Fehlkonfigurationen und Datenlecks zu durchsuchen.

Kontinuierliche Verwaltung der Sicherheit von SaaS- und Cloud-Daten

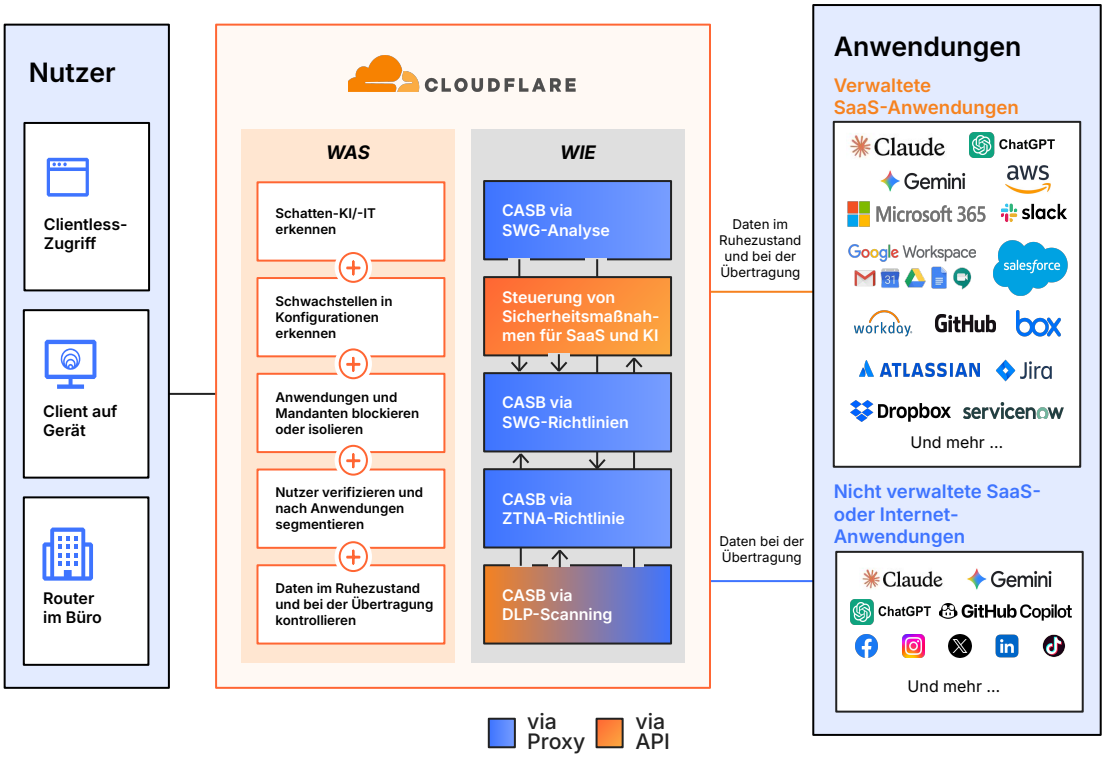
Ein Abdriften der Sicherheit und unsichere Einstellungen bei SaaS- und Cloud-Speichern werden zutage gefördert. Schwerwiegende Fehlkonfigurationen – wie öffentlich zugängliche S3-Buckets oder allgemeine Zugriffsrechte für Projekte – lassen sich feststellen und rückgängig machen, bevor es zu Datenlecks kommt.

Gebündelte Kontrolle von Schatten-IT

Das Hin- und Herwechseln zwischen verschiedenen Konsolen ist nicht mehr erforderlich. Mit CASB-Informationen lassen sich nicht zugelassene Anwendungen ermitteln und dann sofort Zero Trust-Richtlinien zur Blockierung oder Isolierung des zugehörigen Traffics durch Cloudflare Gateway anwenden. Gesteuert wird das Ganze über ein einziges Dashboard.

Sie möchten noch mehr über dieses Produkt erfahren? Dann werfen Sie einen Blick auf unsere Referenzarchitektur oder lassen Sie sich von uns kompetent beraten.

Umfassende Sicherheit für SaaS, KI und Schatten-IT



So funktioniert's

Der Multimode-CASB von Cloudflare trägt zur Gewährleistung einer übergreifenden Cloud-Sicherheit für SaaS-Anwendungen bei. Zum Schutz von Daten im Ruhezustand werden Anwendungen durch einfache API-Integrationen kontinuierlich nach Schwachstellen und potenziellen Risiken durchsucht.

Unsere Steuerungsmechanismen für Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG) und Remote-Browserisolierung (RBI) werden nahtlos als interner CASB eingesetzt, der eine bedienungsfreundliche Konfiguration und robuste Sicherheit in sich vereint.

Externe Absicherung von Daten und Steuerung des SaaS-Sicherheitsniveaus (via API)	
SaaS Security Posture Management (SSPM)	SaaS-Anwendungen und Cloud-Speicher werden via API auf Fehlkonfigurationen und risikobehaftete Drittanbieterintegrationen (wie öffentlich zugängliche S3-Buckets, nicht autorisierte OAuth-Anwendungen oder MFA-Verstöße) durchsucht.
Absicherung von SaaS-Daten (per DLP)	Das Durchsuchen von gespeicherten Daten fördert sensible Dateien (mit personenbezogenen Daten, Finanzdaten und Secrets) zutage. Zur Gewährleistung der Compliance werden Verstöße automatisch behoben (z. B. durch das Entfernen öffentlich zugänglicher Dateien).
Interne Absicherung von Daten (via Proxy)	
Aufspüren von Schatten-KI und -IT	Die Nutzung nicht genehmigter Anwendungen ist sofort erkennbar. Risikobehaftete Anwendungen (wie nicht genehmigte PDF-Konverter oder KI-Tools) werden anhand von Vertrauenswürdigkeits-Scores automatisch kategorisiert und blockiert/isoliert.
Interner DLP und interne Texterkennung	Sensible Daten im Traffic werden mithilfe von Exact Date Match (EDM) und fortschrittlichen Klassifikatoren aufgespürt. Mittels Texterkennung kann dieser Schutz auf Bilder ausgeweitet werden, sodass Datenlecks verhindert werden.
Schutz für Prompts bei generativer KI	HTTPS-Anfragen an Tools wie ChatGPT oder Gemini werden überprüft, damit sensible Informationen (Quellcode, personenbezogene Kundendaten) nicht in öffentliche LLM gelangen und eine sichere KI-Nutzung gewährleistet werden kann.
Mandantenkontrolle	Um eine Anmeldung mit persönlichen Konten auf Firmengeräten zu verhindern, kann durchgesetzt werden, dass nur Firmenkonten Zugriff auf Applikationen wie Microsoft 365, Google Workspace und Slack haben.
Übergreifende Verwaltung	
Ein einziger Client	Ein separater CASB-Client ist nicht erforderlich. ZTNA, SWG und CASB werden mit Single Pass-Überprüfung von einem einzigen Client aus gesteuert.
Nutzerbezogener Risiko-Score	Durch den Abgleich von CASB-Ergebnissen mit Verhaltensanomalien erfolgt eine dynamische Risikobewertung zur Erkennung kompromittierter Nutzer.
Logpush	Eine umfassende Protokollierung erfasst alle Anfragen, Nutzer und Geräte. CASB-Protokolle können zur SIEM-Analyse direkt zu Splunk, Datadog oder S3 exportiert werden.

