CLOUDFLARE

KURZDARSTELLUNG

Schutz vor Datenverlust

Sensible Daten absichern und die Einhaltung gesetzlicher Vorschriften für Web-, Privat-, SaaS-, Cloud-, KI- und E-Mail-Anwendungen gewährleisten

Die am stärksten integrierte Data Loss Prevention (DLP)-Lösung für das Zeitalter der KI-Agenten

Mit Cloudflare DLP kann die Ausschleusung sensibler Daten aus dem gesamten Netzwerk und sämtlichen (SaaS-, KI-, Cloud-, Privat- und E-Mail-)Anwendungen erkannt und unterbunden werden, ohne die Produktivität der Nutzer zu beeinträchtigen.

Die Abschirmung von urheberrechtlich geschütztem Material, Quellcode, personenbezogenen Kundendaten und anderen Informationen ermöglicht:

- **Einhaltung rechtlicher Vorgaben** für Finanzdaten, Krankenakten und Sozialversicherungsnummern mit vorerstellten Profilen
- **Schutz von Firmendaten** durch Blockieren des Uploads sensibler Daten auf nicht autorisierte Cloud-Speicher- oder File-Sharing-Plattformen
- **Absicherung von KI-Prompts** durch das Durchsuchen und von Eingaben bei Tools wie ChatGPT und GitHub auf sensible Daten oder Quellcode und das Unkenntlichmachen dieser Informationen
- **Übersicht über sämtliche Bewegungen von Daten** der gesamten, hybrid arbeitenden Belegschaft

Die Überprüfung nutzt die globale Edge von Cloudflare, erfolgt nur Millisekunden vom Nutzer entfernt und gewährleistet schnellen, kosteneffizienten und maßstabsgerechten Schutz.

Infrastruktur-anbieter

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

Zur Fallstudie

Führende Onlinebank

Zentrale Steuerung der Sicherheit in einem einzigen Dashboard gewährleistet strikte Einhaltung gesetzlicher Vorgaben bezüglich Daten und Schutz vor Ransomware für die Mobile-First-Banking-Plattform

Telemedizin-Anbieter

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

Cloudflare macht den Unterschied

Vereinfachte SaaS- und KI-Sicherheit

Die Verwendung von KI durch Mitarbeitende lässt sich kontrollieren, indem verdächtige Inhalte blockiert werden und das Risiko von Datenausschleusungen durch die Identifizierung und Bereinigung sensibler, in SaaS- und Cloud-Umgebungen gespeicherter Daten verringert wird.

Einheitliche Richtlinienverwaltung

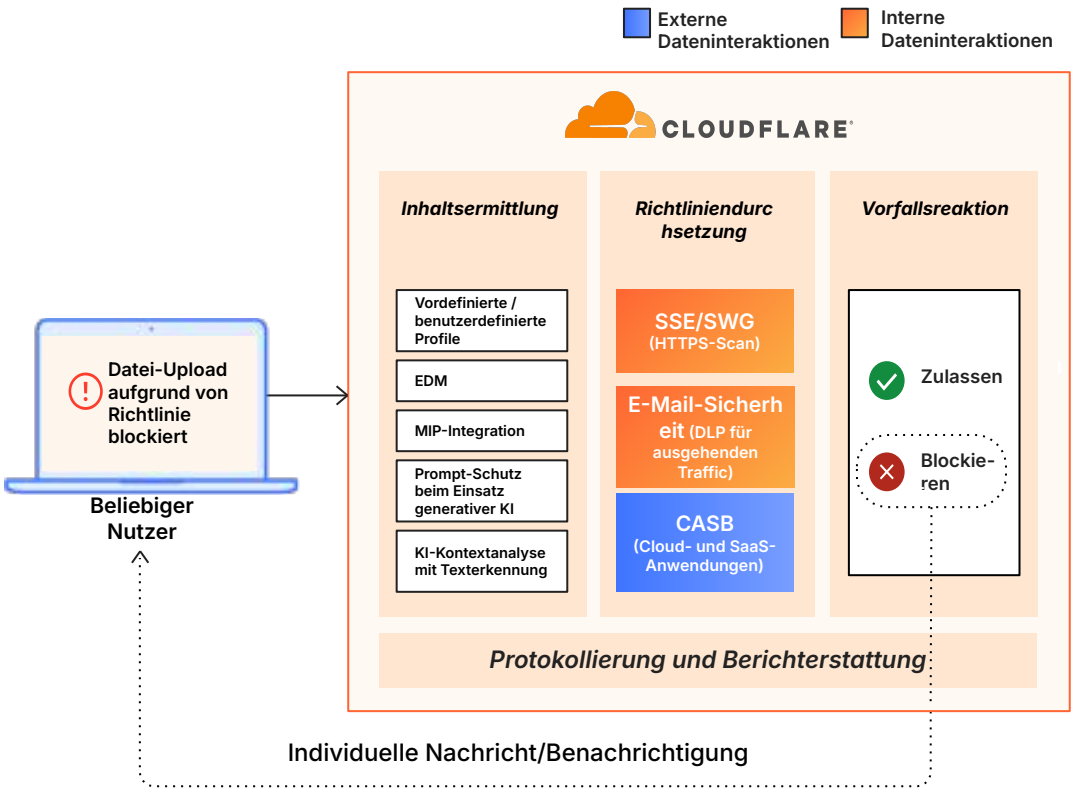
Über die Konfiguration von DLP-Profilen, Erkennungsvorgaben und Microsoft Purview-Vertraulichkeitsbezeichnungen wird der Schutz von ausgehendem Datenverkehr, Dokumenten, PDF und Bildern an einem Ort zusammengeführt.

Anpassungsfähige Datenkontrolle

Durch Feedback zu jeder Erkennung wird die KI-Kontextanalyse verfeinert und die Erkennungsgenauigkeit erhöht. DLP passt sich an Ihre spezifischen Datenmuster und Ihren Traffic an, um die Zahl der Fehlalarme zu verringern.

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

Absicherung von Daten für alle Arbeitskanäle



So funktioniert's

Cloudflare DLP ermöglicht eine automatische, kontextbezogene Überprüfung des HTTPS- und E-Mail-Traffics.

Die Lösung ist nativ in das Zero Trust-Framework von Cloudflare integriert und beseitigt Sicherheitslücken, indem sie die Absicherung von Daten in einer einzigen, übergreifenden Plattform bündelt. So wird nahtlose Übersicht und Kontrolle über sämtliche Kanäle gewährleistet.

Eine Auswahl an DLP-Funktionen

DLP-Profile	Durch die Verwendung vordefinierter Profile für personenbezogene Informationen wie Gesundheit-, Finanz- oder Anmeldedaten oder die Erstellung benutzerdefinierter Profile wird die Sicherheit firmeneigener Assets wie interner Projektnamen oder nicht veröffentlichten urheberrechtlich geschützten Materials gewährleistet.
Microsoft Information Protection (MIP)	Zur automatischen Durchsetzung von Richtlinien ohne Neukennzeichnung von Dateien lassen sich MIP-Vertraulichkeitsbezeichnungen (z. B. „Vertraulich" blockieren) übernehmen.
Exact Data Match (EDM)	Wenn per Hashing verschlüsselte Datensätze (z. B. eine bestimmte Kundendatenbank) hochgeladen werden, lassen sich exakte Werte anstelle von generischen Mustern aufspüren. Bestimmte Einträge können blockiert werden, während man gleichzeitig die Zahl der Fehlalarme reduziert.
Fingerprinting von Dokumenten	Sensible Dokumente werden durch die Erstellung und Speicherung eindeutiger „Fingerabdrücke" (Hashes/Muster) geschützt. Diese können dann mit dem Netzwerk-Traffic abgeglichen werden, um ähnliche Dokumente zu erkennen und ihre Übertragung zu unterbinden.
Prompt-Schutz beim Einsatz generativer KI	HTTPS-Anfragen an Tools wie ChatGPT oder Gemini werden überprüft, damit sensible Daten (Quellcode, personenbezogene Kundendaten) nicht in öffentliche LLM gelangen und für eine sichere KI-Nutzung gesorgt werden kann.
KI-Kontextanalyse und Einstufung der Vertrauenswürdigkeit	Mithilfe von maschinellem Lernen können Kontext und die Nähe zu Keywords analysiert werden. Durch das Festlegen von Schwellenwerten zur Vertrauenswürdigkeit werden Treffer, für die ein hohes Risiko angezeigt wird, automatisch blockiert. Ereignisse mit geringerem Vertrauenswürdigkeitsniveau werden zur späteren Optimierung protokolliert.
Texterkennung	Text aus Bilddateien (PNG, JPG/JPEG) wird automatisch gescannt und extrahiert, damit Sicherheitsmaßnahmen nicht durch Screenshots von sensiblen Dokumenten umgangen werden können.
Anleitung und Aufklärung der Nutzer	Es können anpassbare Echtzeit-Benachrichtigungen angezeigt werden, die Nutzern sofort mitteilen, wenn sie gegen Sicherheitsrichtlinien verstoßen.
Forensik und Protokollierung an einem einzigen Ort	Eine detaillierte Ereignisprotokollierung wird mit einer sicheren Überprüfung der Nutzdaten kombiniert. Bestimmte Datenschnipsel und der Nutzerkontext können analysiert werden, um Vorfälle sofort zu bestätigen und eine Feinjustierung von Richtlinien vorzunehmen.

