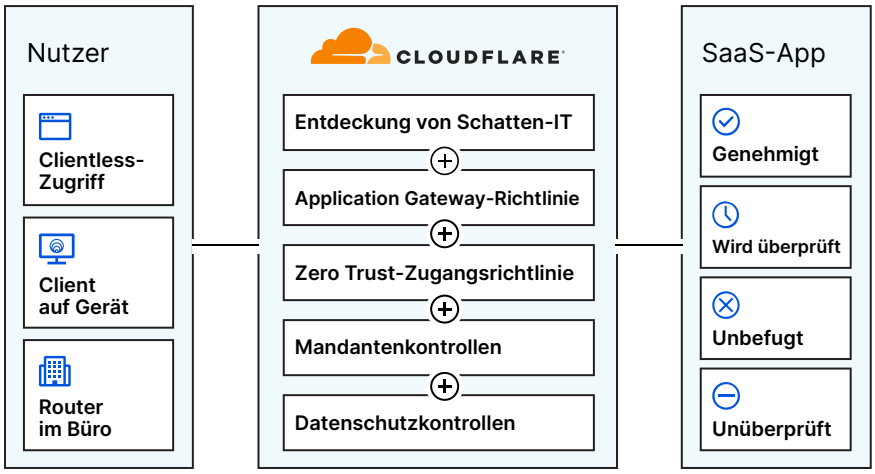
KURZDARSTELLUNG

Sichtbarkeit und Kontrolle jeder SaaS-Anwendung dank Zero Trust

SaaS-Anwendungen bieten Firmen mehr Möglichkeiten als je zuvor. Mit der Flexibilität und Freiheit, die den Beschäftigten damit geboten wird, gehen allerdings auch Sicherheitsrisiken, Unübersichtlichkeit und Probleme bei der Zugriffskontrolle einher.

Cloudflare bietet Unternehmen die nötigen Tools für den Schutz ihrer Daten und Belegschaft, ohne die Mitarbeitenden an der Nutzung hilfreicher Arbeitswerkzeuge zu hindern.



Schatten-IT aufspüren und kontrollieren

Fehlt Unternehmen der Überblick über die von ihren Angestellten verwendeten Anwendungen, haben sie auch keine Kontrolle darüber, wie vertrauliche Daten gespeichert, weitergegeben oder gegenüber Dritten offengelegt werden. Cloudflare hilft Firmen bei der Ermittlung, Kategorisierung und Kontrolle aller intern verwendeten Applikationen, ob genehmigt oder nicht. Dabei wird jede Verbindung und Anfrage zentral erfasst.

Zero Trust-Zugangsrichtlinien anwenden

SaaS-Anwendungen werden außerhalb des Firmennetzwerks gehostet. Deshalb haben Sicherheitsteams nur wenig Spielraum, wenn sie kontrollieren wollen, wie Nutzer darauf zugreifen oder Daten an diese Applikationen übermitteln und von ihnen beziehen. Cloudflare schaltet SaaS-Anwendungen mehrere Zero Trust-Sicherheitsmaßnahmen vor, authentifiziert legitime Nutzer und verhindert den Datei- und Datenzugriff durch Unbefugte oder Geräte, die ein Risiko darstellen.

Mandanten- und Datenschutzkontrollen durchführen

Wenn Mitarbeitende auf die falsche Anwendungsinstanz zugreifen, kann es passieren, dass sie Firmendaten an den falschen Orten abspeichern oder übertragen. Dadurch entsteht ein Einfallstor für Datenlecks und andere Sicherheitsrisiken. Cloudflare unterstützt Unternehmen dabei, die Kontrolle über den Transfer und die Speicherung ihrer Daten zu behalten – sei es bei der Übertragung über unser Netzwerk oder bei der Verwendung in unserem Remote-Browser. Zum Schutz der Daten innerhalb eines beliebigen SaaS-Mandanten können jetzt Zero Trust-Richtlinien für Browser erstellt und angewandt werden. Gleichzeitig wird verhindert, dass Beschäftigte auf die falschen Anwendungen oder die falschen Mandanten genehmigter Applikationen zugreifen.

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

Schatten-IT aufspüren und kontrollieren

Die von Beschäftigten benutzten Anwendungen bewerten

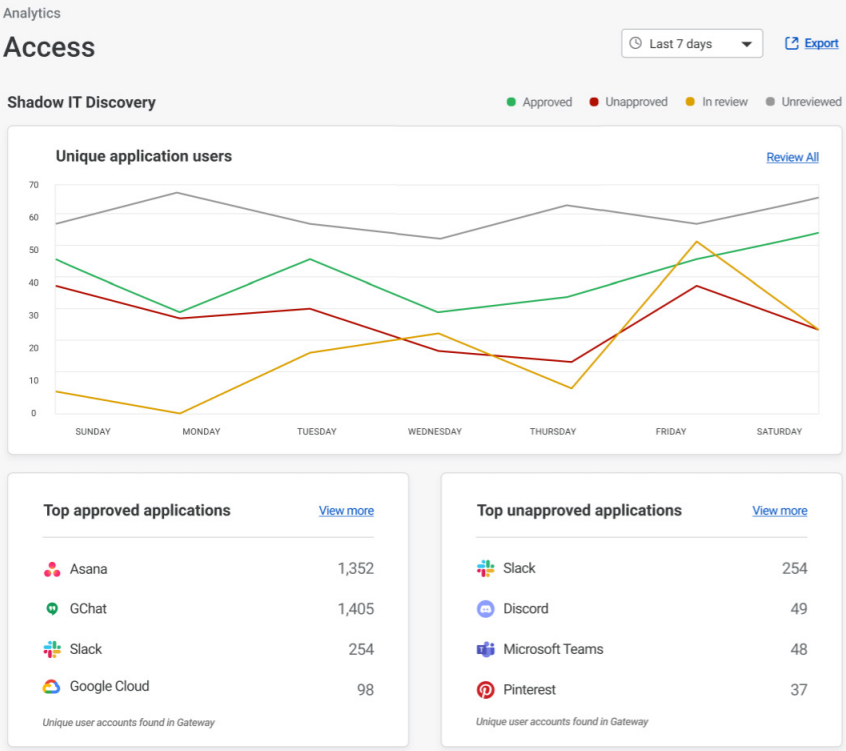
Wenn eine IT-Abteilung nicht sehen kann, welche Anwendungen von Mitarbeitenden benutzt werden, hat sie auch keine Kontrolle darüber, was mit den Daten innerhalb der jeweiligen Applikation passiert. Cloudflare bündelt und kategorisiert automatisch alle HTTP-Anfragen in einem Aktivitätsprotokoll nach Anwendungstyp. Unternehmen können dann den Status festlegen und die Nutzung zugelassener und nicht zugelassener Anwendungen firmenweit verfolgen.

Jede Verbindung und Anfrage protokollieren

Wenn Mitarbeitende auf nicht autorisierte Anwendungen zugreifen oder vertrauliche Informationen mit nicht von der Firma verwalteten Geräten abrufen, birgt dies gewisse Risiken, die Unternehmen mithilfe von Cloudflare abmildern können. Alle Verbindungen und Anfragen werden zentral protokolliert, damit erkennbar ist, welche Anwendungen verwendet werden und was die Nutzer damit tun. Administratoren haben auch die Möglichkeit, Anfragen an SaaS-Anwendungen zu blockieren oder zu genehmigen. Damit werden Nutzer daran gehindert, wichtige Sicherheitskontrollen zu umgehen und sich eigenmächtig Zugang zu Applikationen, Ressourcen und Daten des Unternehmens zu verschaffen.

Wichtigste Funktionen

- Automatischer Überblick über die bereits von Cloudflare geschützten Anwendungen
- Speicherung von Protokollen im Cloudflare-Netzwerk für bis zu sechs Monate
- Ein- oder mehrfacher Export von Protokollen zur Speicherung in der Cloud und bei SIEM-Anbietern



Anwendung von Zero Trust-Zugriffsrichtlinien auf SaaS-Anwendungen

Sicherer SaaS-Zugang über den Cloudflare-Identitätsproxy

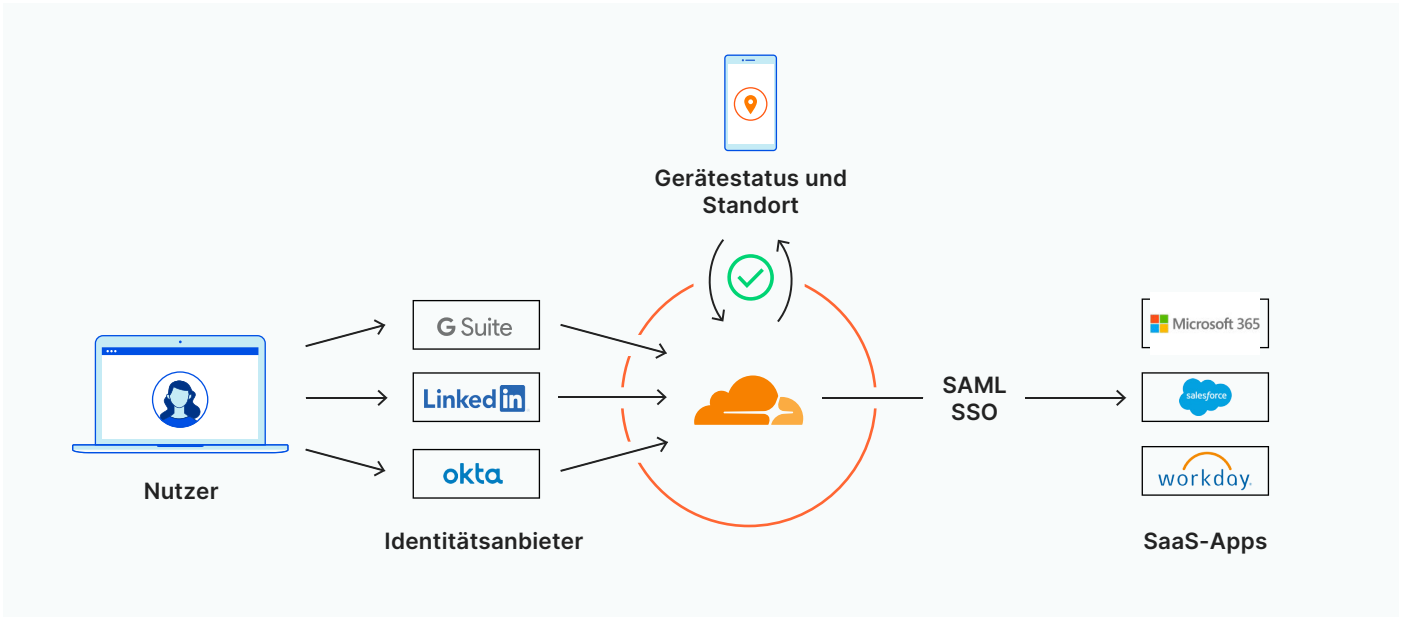
SaaS-Anwendungen werden von externen Anbietern gehostet und oft von einem bestimmten Geschäftsbereich verwaltet. Daher haben IT-Abteilungen oft nur wenig Mitspracherecht, wenn es darum geht, wie sich Nutzer mit diesen Anwendungen verbinden. Cloudflare schaltet sich zwischen den Identitätsanbieter und die SaaS-Applikation, was den Unternehmen die Erstellung und Anwendung identitätsbewusster und kontextorientierter Zero Trust-Regeln für das Login erlaubt, ohne die Endnutzererfahrung zu beeinträchtigen.

Zugriffsrechte von Nutzergeräten für Anwendungen festlegen

IT-Abteilungen müssen präzise festlegen können, auf welche Weise sich Geräte, die von dem Unternehmen verwaltet werden, bei SaaS-Anwendungen anmelden. Cloudflare integriert Zero Trust-Regeln in die Einmalanmeldung für alle Anwendungen, die eine SAML-Authentifizierung unterstützen. Nutzer authentifizieren sich zunächst bei ihrem Identitätsanbieter. Anschließend überprüft Cloudflare die Anfrage anhand des Gerätestatus und Standorts, bevor der Zugang zu einer SaaS-Anwendung mit flexibler Sitzungsverwaltung für eine kontinuierliche Verifizierung genehmigt wird. Sicherheits-Administratoren können auch gerätespezifische Richtlinien erstellen, damit Nutzer nur auf Anwendungen zugreifen können, wenn ihre Geräte zuvor festgelegten Sicherheitsanforderungen gerecht werden (also beispielsweise über mTLS-Zertifikate verfügen).

Wichtigste Funktionen

- Bündelung mehrerer Identitätsanbieter oder Instanzen unter dem Dach eines Providers
- Bestätigung der Nutzeridentität anhand anwendungsspezifischer Regeln (z. B. MFA erfordert Hardware-Token)
- Bestätigung des Gerätestatus anhand anwendungsspezifischer Regeln (z. B. durchgesetzte SWG-Richtlinie, installiertes EPP, mTLS-Zertifikat, aktivierte Festplattenverschlüsselung) und des Standorts
- Mit dem Cloudflare-Portal für Anwendungsstarts können Nutzer sämtliche für sie genehmigten SaaS-Applikationen sehen und darauf zugreifen



Durchführung von Mandanten- und Datenschutzkontrollen bei allen SaaS-Anwendungen

Beschränkung des Zugriffs auf externe Anwendungsinstanzen

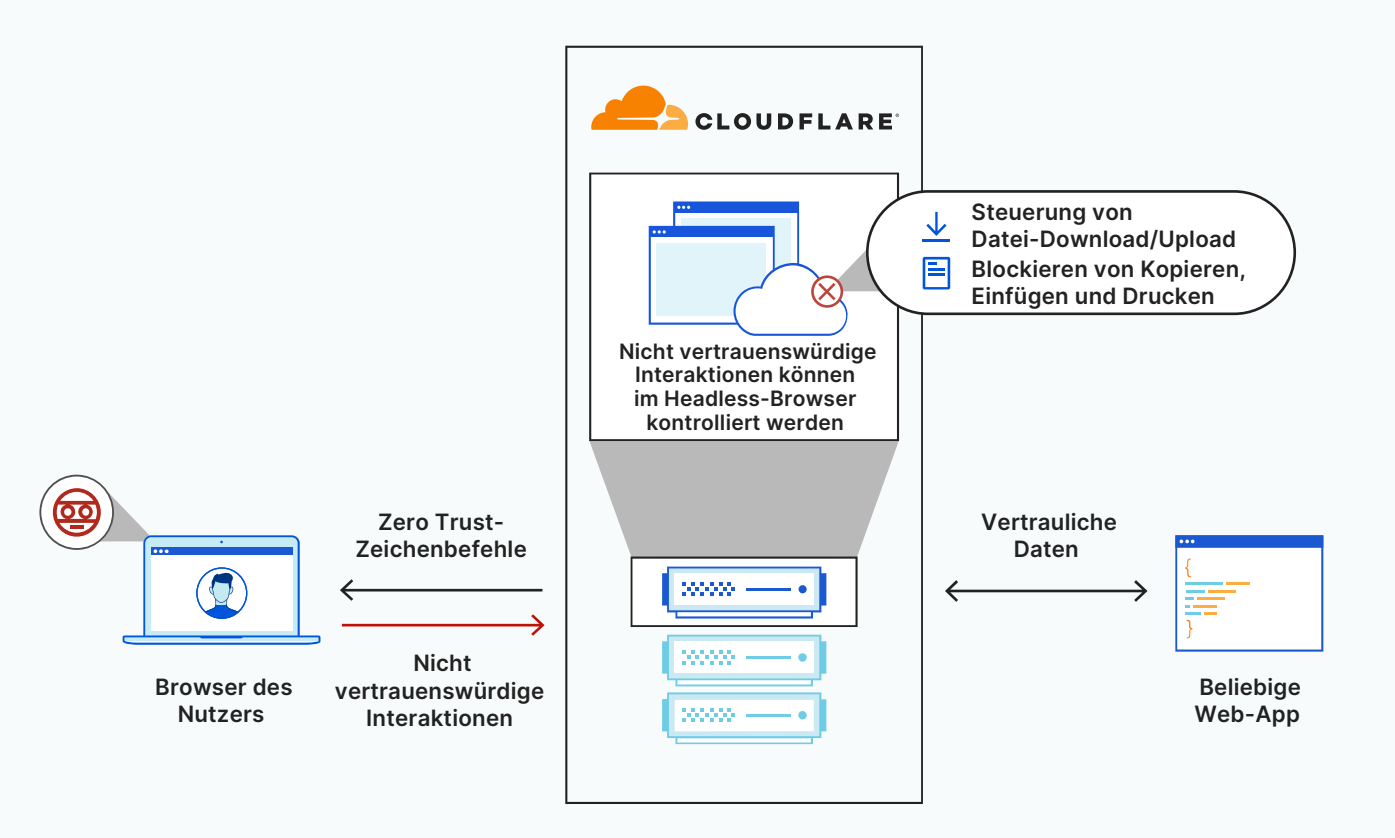
Cloudflare ermöglicht Mandantenkontrolle mittels HTTP Gateway-Richtlinien, die so konfiguriert werden können, dass Nutzer am Zugriff auf die Verbraucherversionen von Anwendungen gehindert werden. Anstatt diese Richtlinien mit lokalen Proxy-Servern über Firmen-VPNs durchzusetzen, filtert und überprüft Cloudflare den gesamten Datenverkehr und alle Anfragen in einem großen globalen Rechenzentrumsnetzwerk. Auf diese Weise wird die Nutzererfahrung nie durch erhöhte Latenz oder Performanceprobleme beeinträchtigt.

Übertragung von Firmendaten aus eigenen Mandanten verhindern

Mit Cloudflare lassen sich Zero Trust-Richtlinien für Browser zur Kontrolle und zum Schutz von Daten in webbasierten Applikationen mühelos erstellen und anwenden. Der gesamte Anwendungscode wird nicht auf Endpunkt-Geräten ausgeführt, sondern in einem sicheren Headless Browser, der extern in unserem weitreichenden globalen Netzwerk betrieben wird. Auf diese Weise werden vertrauliche Daten vor kompromittierten oder nicht vertrauenswürdigen Geräten und Zero Day-Bedrohungen abgeschirmt. Zudem behalten die Administratoren die Kontrolle darüber, wie Nutzer auf diese Daten zugreifen und sie weiterleiten. So sinkt das Risiko eines versehentlichen Datenverlusts oder schwerwiegenderer Datenlecks erheblich.

Wichtigste Funktionen

- Genehmigung oder Blockierung von Browserverhaltensweisen anhand von Kriterien wie Anwendung, Anwendungstyp, Hostname, Nutzeridentität und Sicherheitsrisiko
- Kontrolle der Nutzeraktionen innerhalb des Browsers: Hoch- und Herunterladen, Kopieren und Einfügen, Tastatureingabe und Drucken



Cloudflare macht den Unterschied

Breitgefächertes Angebot

Mit Cloudflare werden Zero Trust-Kontrollen der Zugriffe (ZTNA), Gateways (SWG) und Browser vor SaaS-Anwendungen geschaltet, ohne dass IT-Abteilungen dafür ein spezielles CASB-Produkt konfigurieren und betreiben müssen.

Von Grund auf neu entwickelte Lösungen

Die CASB-Funktionen von Cloudflare ergänzen nahtlos unsere ZTNA-, SWG- und RBI-Services, weil alle diese Lösungen von Grund auf neu entwickelt wurden. Dadurch entfällt beim Schutz von Anwendungen und Teams die Notwendigkeit, diverse Einzellösungen aufeinander abzustimmen.

Zentrale Kontrollebene

Mit Cloudflare können Unternehmen über ein zentrales Dashboard Richtlinien festlegen, den Zugriff auf Anwendungen und ihre Verwendung verwalten. So haben sie auf einen Blick die Übersicht über alle Anfragen und Berechtigungen.

Mit einer nativ integrierten Serie an Zero Trust-Sicherheitslösungen unterstützt Cloudflare Unternehmen bei der Überwachung, dem Schutz und der Kontrolle von SaaS-Anwendungen.

Jetzt mehr erfahren