

Cloudflare Zero Trust

Die schnellste Plattform für Zero Trust-Surfen und Anwendungszugriff

Risiken jenseits des Perimeters

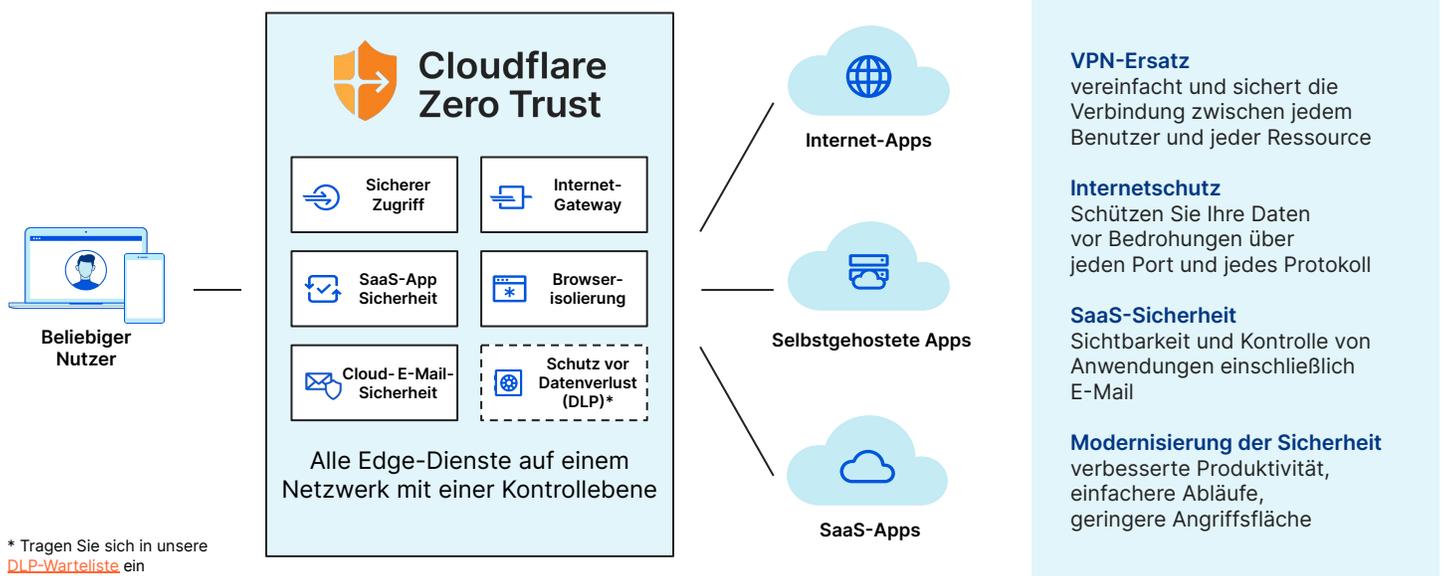
Als Anwendungen und Nutzer den Firmenperimeter verließen, mussten die Sicherheitsteams Kompromisse eingehen, um die Daten zu schützen. Standortbezogene Methoden zur Sicherung des Datenverkehrs (wie VPNs, Firewalls und Web-Proxys) konnten dem Druck nicht standhalten. Unternehmen haben daher nun mit eingeschränkter Sichtbarkeit, widersprüchlichen Konfigurationen und extremen Risiken zu kämpfen.

Angesichts der allgegenwärtigen Risiken wenden sich Unternehmen der Zero-Trust-Lösung in der Cloud zu, um sich anzupassen.

Internet-natives Zero Trust einführen

Cloudflare Zero Trust ist eine Sicherheitsplattform, die für mehr Transparenz sorgt, Komplexität verringert und das Risiko beim Anwendungs- und Internetzugriff durch Beschäftigte senkt, ob von zu Hause oder im Büro. In einer Single-Pass-Architektur wird der Datenverkehr überprüft, gefiltert, inspiziert und von Bedrohungen isoliert.

Sie wird über eines der schnellsten Anycast-Netzwerke der Welt in über 275 Städten in über 100 Ländern betrieben, um schneller und mit besserer Performance als andere Anbieter zu arbeiten.



* Tragen Sie sich in unsere [DLP-Warteliste](#) ein

Vorteile für Unternehmen

Vertrauensvorschuss reduzieren

Schützen Sie Anwendungen mit identitäts- und kontextbasierten Zero Trust-Regeln. Blockieren Sie Ransomware, Phishing und andere Online-Bedrohungen. Isolieren Sie Endgeräte von Risiken, indem Sie nicht vertrauenswürdigen Webcode außerhalb der Geräte ausführen.

Komplexität beseitigen

Verringern Sie die Abhängigkeit von veralteten Einzelprodukten und wenden Sie Standard-Sicherheitskontrollen auf den gesamten Datenverkehr an – unabhängig davon, wie die Verbindung hergestellt wird oder an welcher Stelle im Netzwerk-Stack sie verortet ist.

Überblick zurückgewinnen

Umfangreiche Protokolle für DNS-, HTTP-, SSH-, Netzwerk- und Schatten-IT-Aktivitäten. Überwachen Sie Nutzeraktivitäten über alle Anwendungen hinweg. Senden Sie Protokolle an mehrere Ihrer bevorzugten Cloud-Speicher- und Analysetools.

VPN-Ersatz und -Ergänzung (ZTNA)

Eine schnellere, einfachere und sicherere Methode, um Remote-Nutzer mit Apps zu verbinden

Herausforderung: Langsame, komplexe und riskante VPNs

Herkömmliche VPNs sind zunehmend eine Belastung. Langsame Performance schadet der Produktivität der Nutzer. Administratoren kämpfen mit einer unübersichtlichen Konfiguration. Außerdem machen es VPNs Malware leicht, sich lateral über ein Netzwerk zu verbreiten.

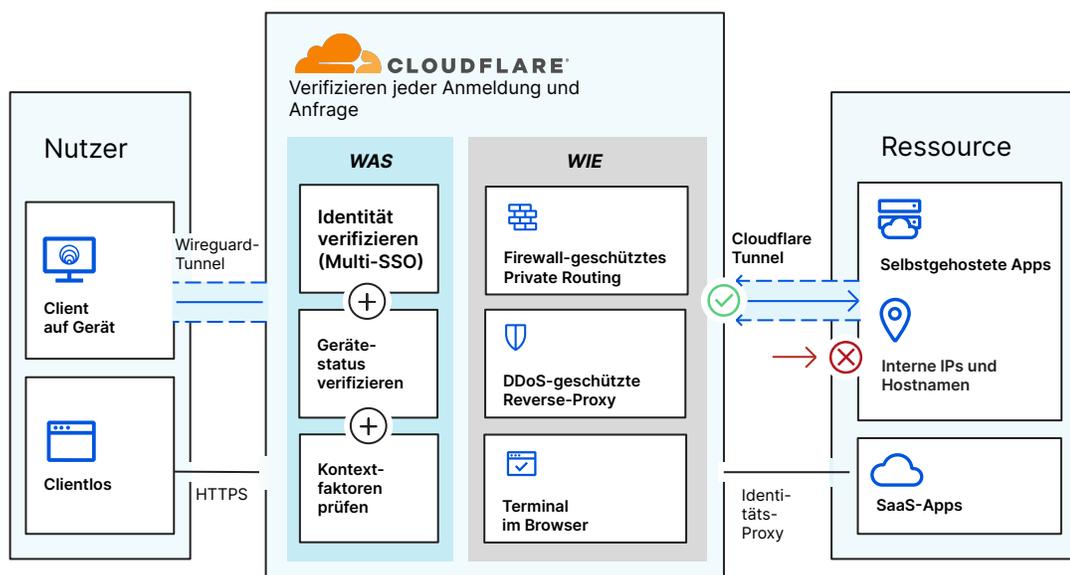
Die beschleunigte Einführung der Cloud und hybrides Arbeiten haben diese Schwachstellen weiter offengelegt und VPNs anfälliger gemacht.

Zero-Trust-Netzwerkzugriff (ZTNA)

Cloudflare Access, unser ZTNA-Service, ergänzt oder ersetzt VPN-Clients, indem er jede Anwendung in jedem On-Premise-Netzwerk, jeder öffentlichen Cloud oder SaaS-Umgebung schützt.

Access ist kompatibel mit Ihren Identitätsanbietern und Plattformen für den Endpunktschutz, um Zero-Trust-Regeln durchzusetzen, die den Zugriff auf Unternehmensanwendungen, private IP-Bereiche und Hostnamen beschränken.

So funktioniert's



Clientlose Bereitstellung für Web-, SSH- oder VNC-basierte, selbst gehostete Anwendungen, die über einen Browser zugänglich sind.

Nutzen Sie den Geräte-Client von Cloudflare, um sich mit internen IPs, Hostnamen und Nicht-Web-Anwendungen zu verbinden.

Wichtige Anwendungsfälle



Remote-Arbeit und BYOD-Initiativen unterstützen

Überprüfen Sie den Zugriff für alle Nutzer, egal wo sie sich befinden, auf der Grundlage von Identität, Gerätestatus, Authentifizierungsmethode und anderen kontextbezogenen Faktoren.

Setzen Sie diese Zero Trust-Richtlinien für Ihre hybride Belegschaft durch. Unterstützen Sie Bring-your-own-device (BYOD)-Initiativen, indem Sie sowohl verwaltete als auch nicht-verwaltete Geräte sichern.



Zugriff von Dritten mit Flexibilität optimieren

Beschleunigen Sie die Einrichtung des Zugangs für Auftragnehmer, Lieferanten, Agenturen, Mitarbeiter usw.

Binden Sie mehrere Identitätsanbieter (IDPs) auf einmal ein. Legen Sie Regeln für die geringsten Privilegien fest, basierend auf den IDPs, die sie bereits verwenden.

Vermeiden Sie die Bereitstellung von SSO-Lizenzen, die Einrichtung von VPNs oder die Erstellung einmaliger Berechtigungen.



Administrative Konfiguration und Support vereinfachen

Fügen Sie in wenigen Minuten neue Nutzer, Identitätsanbieter oder Zero Trust-Regeln hinzu.

Setzen Sie neue Produktivität frei, indem Sie die Onboarding-Zeit für Mitarbeiter reduzieren ([eTeacher Group](#)), und sich von der IP-basierten Zugangskonfiguration lösen ([BlockFi](#)). Keine Notwendigkeit, eigenes Personal für die Verwaltung von VPNs einzustellen ([ezCater](#)).

Schutz von Daten und vor Internetbedrohungen (SWG & RBI)

Filtern, überprüfen und isolieren Sie den für das Internet bestimmten Traffic

Herausforderung: Bedrohungslandschaft im Wandel

Es war noch nie so schwierig, die Sicherheit zu erhöhen und gleichzeitig die Produktivität der Nutzer zu erhalten. Remote-Arbeit bedeutet mehr nicht verwaltete Geräte, die mehr sensible Daten lokal speichern. Mittlerweile haben Ransomware, Phishing, Schatten-IT und andere internetbasierte Bedrohungen an Umfang und Raffinesse stark zugenommen.

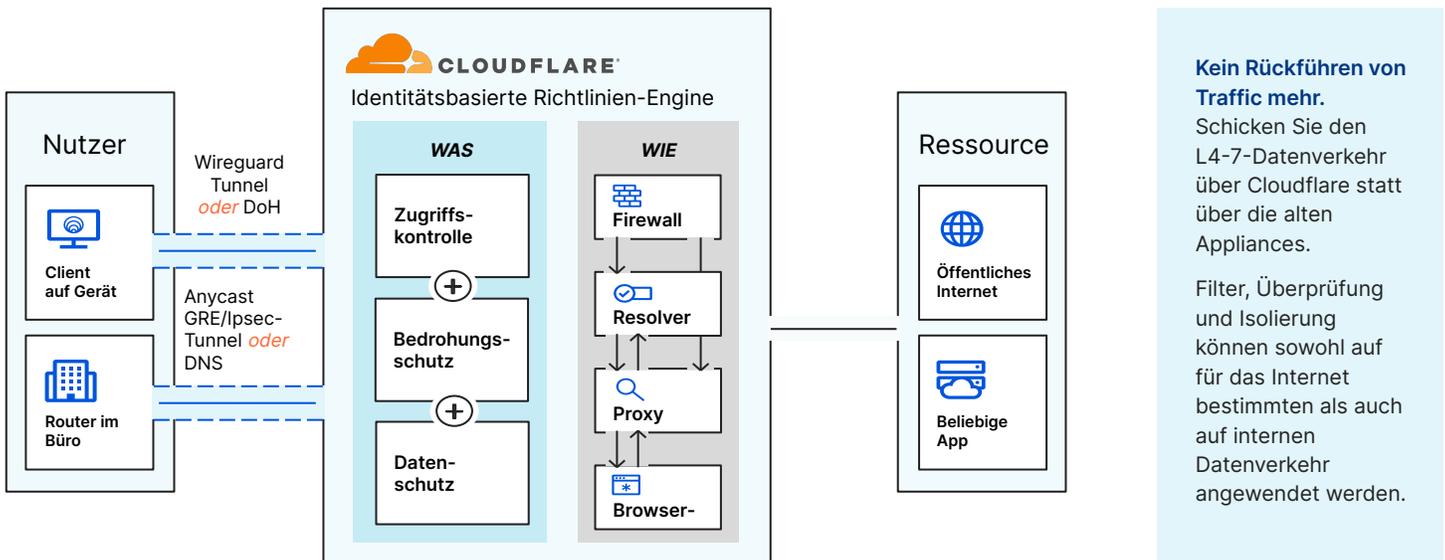
Sich auf veraltete Einzellösungen und Daten-Backups zu verlassen, ist eine riskante Strategie zum Schutz vor der nächsten Ransomware-Bedrohung.

SWG mit Zero Trust-Browsing

Cloudflare Gateway, unser Secure Web Gateway (SWG), schützt Nutzer mit identitätsbasierter Webfilterung und nativ integrierter Remote Browser Isolation (RBI).

Beginnen Sie mit der DNS-Filterung, damit sich für Remote- oder Office-Nutzer erste Vorteile rasch einstellen. Wenden Sie als nächstes eine umfassendere HTTPS-Prüfung an und erweitern Sie schließlich die RBI-Kontrollen, um Zero Trust für alle Internet-Aktivitäten einzuführen.

So funktioniert's



Kein Rückführen von Traffic mehr.

Schicken Sie den L4-7-Datenverkehr über Cloudflare statt über die alten Appliances.

Filter, Überprüfung und Isolierung können sowohl auf für das Internet bestimmten als auch auf internen Datenverkehr angewendet werden.

Wichtige Anwendungsfälle



Stoppen Sie Ransomware

Blockieren Sie Ransomware-Websites und -Domains auf der Grundlage unserer globalen Netzwerkinformationen. Isolieren Sie das Surfen auf riskanten Websites, um den Schutz zu erhöhen.

Kombinieren Sie SWG-Filterung und RBI mit standardmäßiger Verweigerung und ZTNA, um das Risiko einer Ransomware-Infektion zu verringern, die sich lateral ausbreitet und die Privilegien in Ihrem Netzwerk ausweitet.



Blockieren Sie Phishing

Filtern Sie bekannte und „neue“ / „neu entdeckte“ Phishing-Domains. Isolieren Sie das Surfen, um zu verhindern, dass schädliche Payloads lokal ausgeführt werden. Stoppen Sie die Eingabe sensibler Informationen auf verdächtigen Phishing-Seiten über die Tastatureingabekontrolle von RBI.

Plus: In Kürze können Administratoren die E-Mail-Filterung mit einem einzigen Mausklick aktivieren – ermöglicht durch [Area 1](#).



Verhindern Sie Datenlecks

Durch die Implementierung von Lösungen zum Schutz vor Datenverlust (Data Loss Prevention – DLP) mit Dateitypüberprüfung können Nutzer daran gehindert werden, Dateien auf Websites hochzuladen.

Setzen Sie Zero Trust-Browsing ein, um die Daten, die in webbasierten Anwendungen gespeichert sind, zu kontrollieren und zu schützen. Kontrolle der Nutzeraktionen innerhalb des Browsers: Hoch- und Herunterladen, Kopieren und Einfügen, Tastatureingabe und Drucken.

SaaS-Sicherheit (CASB)

Optimieren Sie die SaaS-Sicherheit für mehr Transparenz und Kontrolle mit weniger Aufwand.

Herausforderung: Verbreitung von SaaS-Anwendungen

Moderne Arbeitskräfte verlassen sich heute mehr denn je auf SaaS-Anwendungen. Aber SaaS-Anwendungen sind jeweils anders konfiguriert, erfordern andere Sicherheitsüberlegungen und arbeiten außerhalb des Schutzes des traditionellen Perimeters.

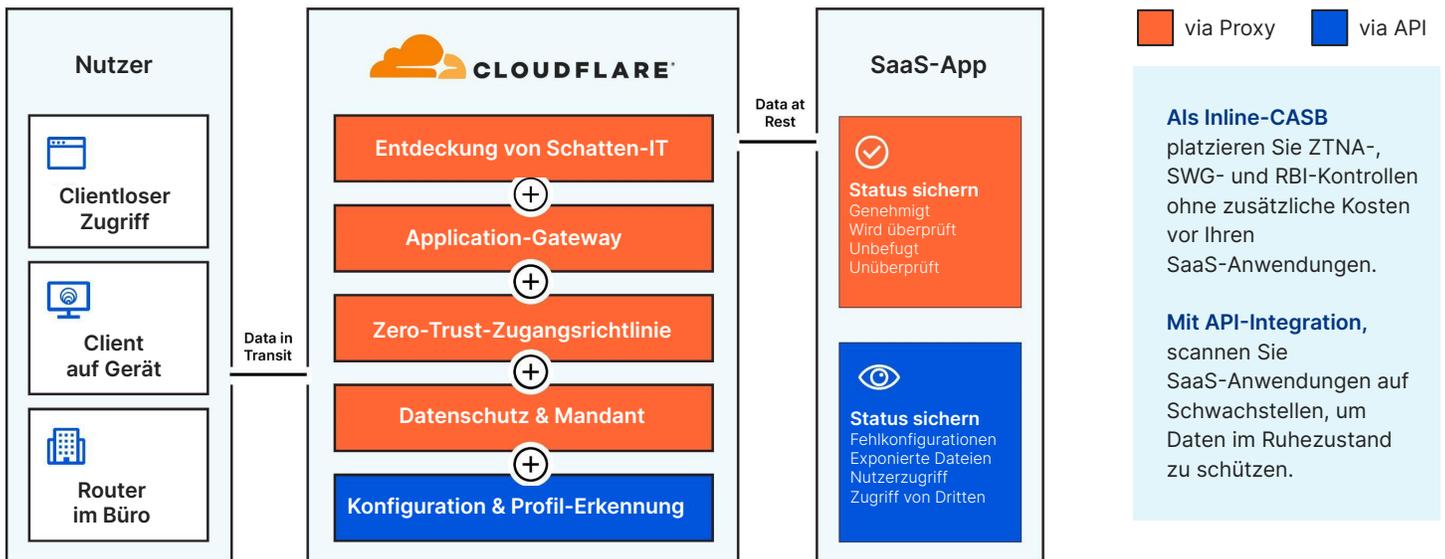
Wenn Unternehmen Dutzende oder gar Hunderte von SaaS-Anwendungen einsetzen, wird es immer schwieriger, eine einheitliche Sicherheit, Transparenz und Performance zu gewährleisten.

Cloud Access Security Broker (CASB)

Der CASB-Service von Cloudflare bietet umfassende Transparenz und Kontrolle über SaaS-Apps, so dass Sie Datenlecks und Compliance-Verstöße leicht verhindern können.

Blockieren Sie Insider-Bedrohungen, riskanten Datenaustausch und böse Akteure. Protokollieren Sie jede HTTP-Anfrage, um nicht zugelassene SaaS-Anwendungen aufzudecken. Scannen Sie SaaS-Anwendungen, um Fehlkonfigurationen und verdächtige Aktivitäten zu erkennen.

So funktioniert's



Wichtige Anwendungsfälle



Mandanten- und Datenschutzkontrollen durchführen

Wenden Sie die Mandantenkontrolle über HTTP-Gateway-Richtlinien an, um zu verhindern, dass Nutzer versehentlich oder böswillig auf die falschen Versionen beliebter SaaS-Anwendungen zugreifen und dort Daten speichern.

Kontrollieren Sie Nutzeraktionen (z.B. Kopieren/Einfügen, Downloads, Drucken usw.) in webbasierten SaaS-Anwendungen, um das Risiko von Datenverlusten zu minimieren.



Schatten-IT eindämmen und kontrollieren

Minimieren Sie die Risiken, die durch nicht zugelassene SaaS-Anwendungen entstehen.

Cloudflare bündelt und kategorisiert automatisch alle HTTP-Anfragen in unserem Aktivitätsprotokoll nach Anwendungstyp. Unternehmen können dann den Status festlegen und die Nutzung zugelassener und nicht zugelassener Anwendungen firmenweit verfolgen.



Identifizieren Sie neue Bedrohungen und Fehlkonfigurationen

Verbinden Sie sich über API mit beliebten SaaS-Anwendungen (Google Workspace, Microsoft 365 usw.) und scannen Sie nach Risiken.

Verschaffen Sie Ihren IT- und Sicherheitsteams Einblick in Berechtigungen, Fehlkonfigurationen, unsachgemäßen Zugriff und Kontrollprobleme, die ihre Daten und Mitarbeiter gefährden könnten.

Demnächst bei Zero Trust: Cloud-E-Mail-Sicherheit (CES)

Ausweitung von Zero Trust auf E-Mails



Am 1. April 2022 schloss Cloudflare die Übernahme von [Area 1 Security](#) ab, einem führenden Cloud-nativen E-Mail-Sicherheitsunternehmen, das Nutzer vor Phishing-Angriffen in E-Mail-, Web- und Netzwerkumgebungen schützt. Lesen Sie die [Pressemitteilung](#).

Herausforderung: E-Mail ist der Bedrohungsvektor Nr. 1

E-Mail ist die wichtigste Kommunikationsform für Teams, aber auch die wichtigste Art und Weise, wie sich Angreifer Zugang verschaffen. Eine aktuelle Studie ergab, dass **91%** aller Cyberangriffe mit einer Phishing-E-Mail beginnen.

E-Mail macht jeden zu einem Insider, auch Personen außerhalb Ihres Unternehmens wie Ihre Lieferanten, Partner und Kunden.

Fazit: Es gibt zu viel implizites Vertrauen in E-Mails, und Angreifer nutzen dies aus, indem sie gängige Geschäftsabläufe fälschen (z.B. Zurücksetzen von Passwörtern, Benachrichtigungen über Dateifreigaben) oder vertrauenswürdige Einrichtungen (z.B. CEO, ein Lieferant/Partner, der Rechnungen verschickt).

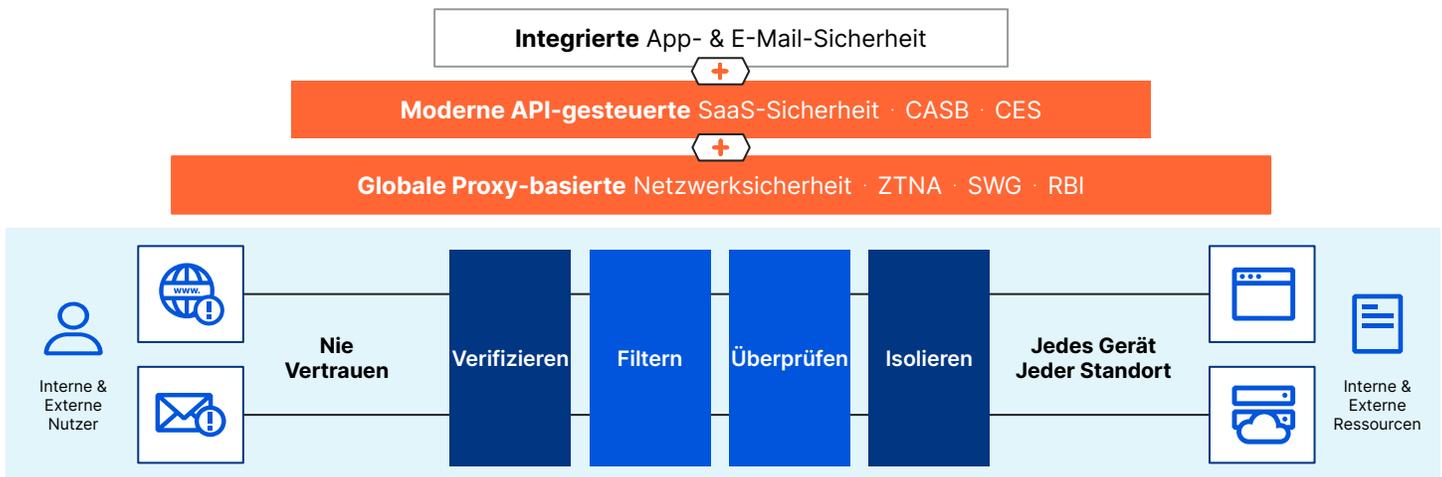
Integration von Cloud-nativer E-Mail-Sicherheit

Die Erweiterung von Cloudflare Zero Trust mit der E-Mail-Sicherheit von Area 1 beseitigt implizites Vertrauen in E-Mails, um Phishing- und BEC-Angriffe (Business Email Compromise) präventiv zu verhindern. Außerdem sparen Sie Zeit bei der Erstellung und Anpassung von Richtlinien für E-Mail-Bedrohungen.

Da wir niemals einem Absender vertrauen, wird der gesamte Datenverkehr des Nutzers, einschließlich E-Mails, überprüft, gefiltert, inspiziert und von Internet-Bedrohungen isoliert. Area 1 hilft seinen Kunden, fortgeschrittene Bedrohungen zu stoppen, eine proaktive Sicherheitshaltung einzunehmen und die Reaktionszeit auf Phishing-Vorfälle um 90% zu reduzieren.

E-Mail-Sicherheit wird in unsere Zero Trust-Dienste integriert, gebündelt mit leistungsstarken Features wie RBI, CASB und mehr. Sind Sie beispielsweise skeptisch gegenüber einem Link in einer E-Mail, möchten ihn aber nicht gleich blockieren? Rendern Sie ihn in einem isolierten Browser und blockieren Sie vorsichtshalber die Texteingabe.

So funktioniert es: Zero Trust für den gesamten internen und externen Netzwerk-, Web- und E-Mail-Traffic



Modernisierung der Sicherheit: Cloudflare macht den Unterschied

Starkes Fundament für die Modernisierung der Sicherheit

Einfache Implementierung

Cloudflare bietet eine einheitliche und modular aufgebaute Plattform für einfache Einrichtung und Betrieb. Durch reine Software-Konnektoren und einmalige Integrationen arbeiten unsere Cloudflare-On-Ramps und Edge-Services alle zusammen.

Dies führt zu einer besseren Erfahrung für Ihre IT-Mitarbeiter und Endbenutzer.

Robustes Netzwerk

Unsere End-to-End-Automatisierung von Traffic gewährleistet zuverlässige und skalierbare Netzwerkkonnektivität mit einheitlichem Schutz von jedem Standort aus.

Bei Cloudflare ist jeder Edge-Service so aufgebaut, dass er an jedem Netzwerkstandort läuft und jedem Kunden zur Verfügung steht – anders als bei anderen Sicherheitsanbietern.

Schnelle Innovation

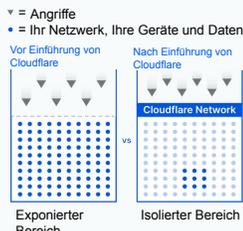
Dank unserer zukunftssicheren Architektur können wir neue Sicherheits- und Netzwerkfunktionen sehr schnell entwickeln und bereitstellen.

Ob es um die rasche Übernahme neuer Internet- und Sicherheitsstandards oder um die Entwicklung kundenorientierter Anwendungsfälle geht, unsere technische Erfahrung spricht für sich selbst, und unser Fundament bietet maximale Flexibilität.

5 Wege, wie Zero Trust Ihrem Unternehmen Zeit und Geld spart

Reduktion d. Angriffsfläche

91 % ↓



Reduktion d. Kosten einer Datenschutzverletzung

35 % ↓



Beschleunigung des Onboardings von Mitarbeitern

60 % ↑



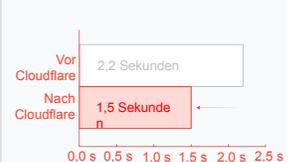
Reduktion von IT-Tickets

80 % ↓



Reduktion von Nutzerlatenz

39 % ↓



Optimiert für Benutzerfreundlichkeit

Eine einzige Verwaltungsschnittstelle

Vereinfachen Sie die Konfiguration mit einem nativen Dashboard für Richtlinien für den Anwendungs- und Internetzugang.

Nutzen Sie ein einziges Dashboard für die Integration mit Identitätsanbietern, Endpunktschutz und Netzwerk-On-Rampen.

Eine einzige zentrale Plattform

Ersetzen Sie einen Flickenteppich aus VPN-Clients, lokalen Firewalls und andere einzelne Sicherheitslösungen durch eine Plattform und eine Steuerungsebene.

Senken Sie Kosten und Komplexität, indem Sie die Sicherheit an die Edge verlagern.

Unübertroffenes Nutzererlebnis

Cloudflare ist näher an Ihren Nutzern und Diensten und leitet Anfragen schneller weiter, indem es ein optimiertes, intelligentes Routing über unser riesiges Anycast-Netzwerk mit mehr als 275 Standorten in mehr als 100 Ländern auf der ganzen Welt nutzt.



Beschleunigen Sie Ihre Umstellung auf Zero Trust

JETZT TESTEN

Kontakt