CLOUDFLARE

KURZDARSTELLUNG DES PRODUKTS

Cloudflare Zero Trust

Die schnellste Plattform für Zero Trust-Surfen und Anwendungszugriff

Risiken jenseits des Perimeters

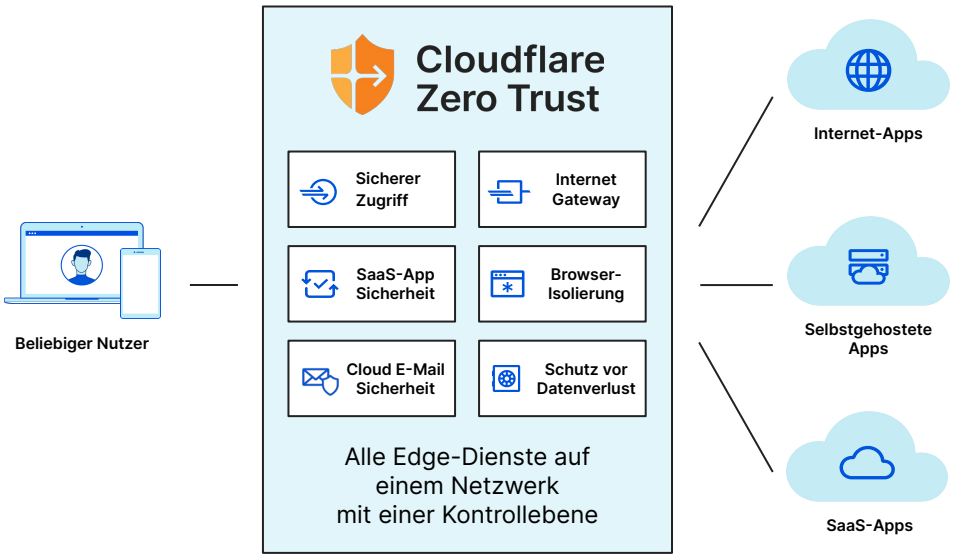
Als Anwendungen und Nutzer den Firmenperimeter verließen, mussten die Sicherheitsteams Kompromisse eingehen, um die Daten zu schützen. Standortbezogene Methoden zur Sicherung des Datenverkehrs (wie VPNs, Firewalls und Web-Proxys) konnten dem Druck nicht standhalten. Unternehmen haben daher nun mit eingeschränkter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



Sicherer Zugriff
vereinfachter und sicherer Zugriff zwischen jedem Nutzer und jeder Anwendung, auf jedem Gerät, an jedem Ort

Bedrohungsabwehr
Schützen Sie Ihre Nutzer und Daten vor Bedrohungen aus dem Internet, per E-Mail und über mehrere Kanäle

Sicher mit Microsoft
Transparenz und Kontrolle aller SaaS-Suites von Microsoft, Google und anderen Anbietern

Sicheres hybrides Arbeiten
Verbesserung der Teamproduktivität, Verringerung von Cyberrisiken und Steigerung der technischen Effizienz

Vorteile für Unternehmen

Vertrauensvorschuss reduzieren

Schützen Sie Anwendungen mit identitäts- und kontextbasierten Zero Trust-Regeln. Blockieren Sie Phishing, Ransomware und andere Online-Bedrohungen. Isolieren Sie Endpunkte von Risiken, indem Sie nicht vertrauenswürdigen Code von den Geräten und nicht vertrauenswürdige Nutzeraktivitäten von den Daten fernhalten.

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.

Sicherer Zugriff (ZTNA)

Eine schnellere, einfachere und sicherere Möglichkeit, jeden Nutzer mit jeder Anwendung zu verbinden

Herausforderung: Langsamer, komplexer und riskanter Zugang

Herkömmliche perimeterbasierte Zugangskontrollen (wie VPNs) sind zunehmend eine Belastung. Langsame Performance beeinträchtigt die Produktivität der Nutzer, Administratoren haben mit unhandlichen Konfigurationen zu kämpfen, und laterale Bewegungen lassen sich nur schwer eindämmen.

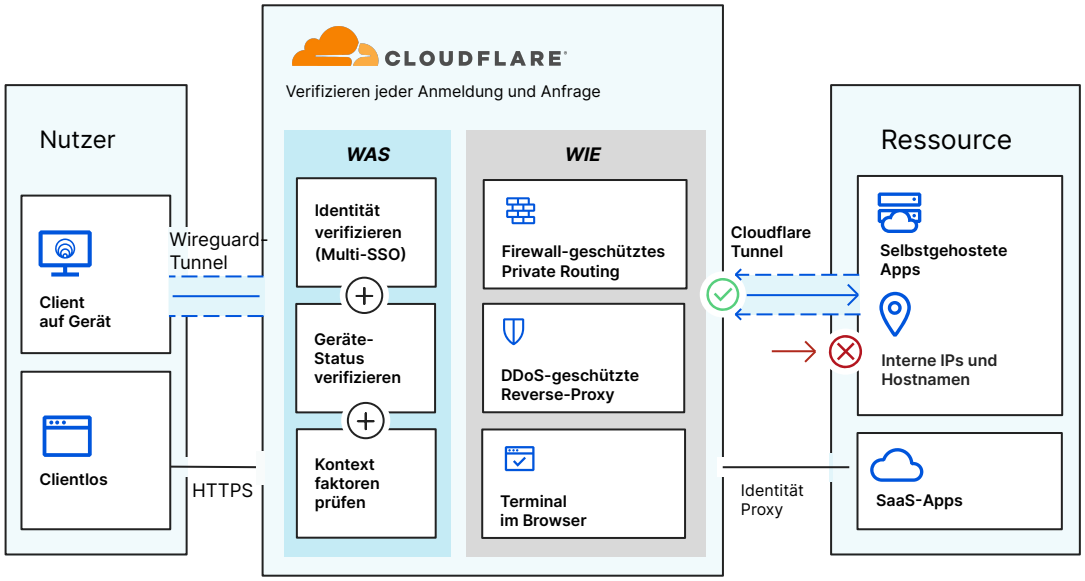
Die beschleunigte Einführung der Cloud und hybrides Arbeiten haben diese Schwachstellen weiter offengelegt und VPNs anfälliger gemacht.

Zero-Trust-Netzwerkzugriff (ZTNA)

Der ZTNA-Service von Cloudflare, Access, ergänzt oder ersetzt VPN-Clients, indem er jede Anwendung in jedem Netzwerk vor Ort, jeder öffentlichen Cloud oder SaaS-Umgebung schützt.

Der ZTNA von Cloudflare 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 ungen 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).

Bedrohungsabwehr (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.

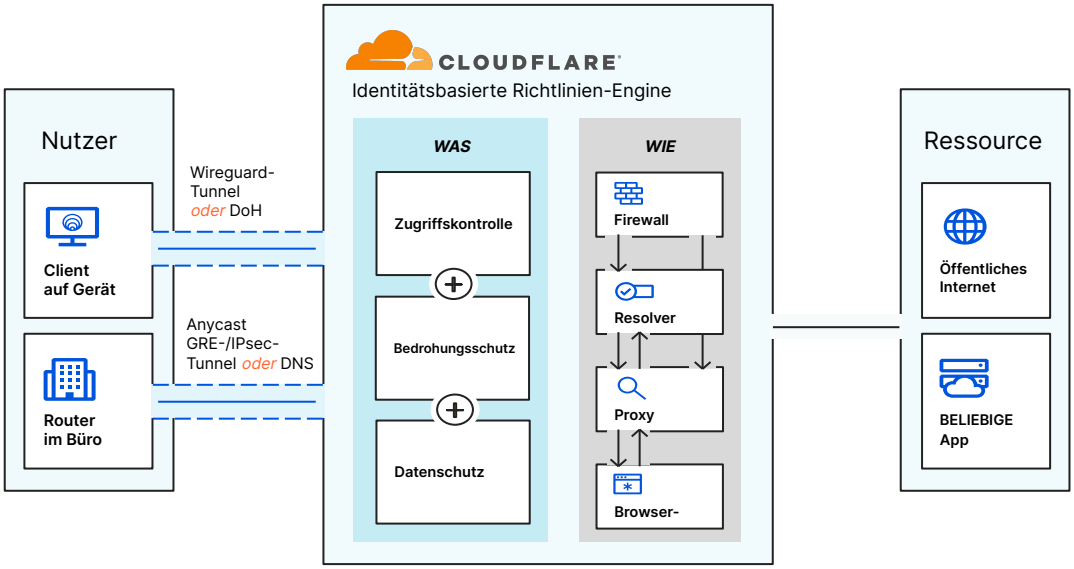
Sich auf veraltete Einzellösungen und Daten-Backups zu verlassen, ist eine riskante Strategie zum Schutz vor Bedrohungen über mehrere Kanäle.

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.

Sicher mit Microsoft (CASB)

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

Herausforderung: Verbreitung von SaaS-Anwendungen

Moderne Belegschaften verlassen sich heute mehr denn je auf SaaS-Anwendungen wie Microsoft 365. Aber jede SaaS-Anwendung erfordert andere Sicherheitsüberlegungen und arbeitet außerhalb der Schutzmaßnahmen des traditionellen Perimeters.

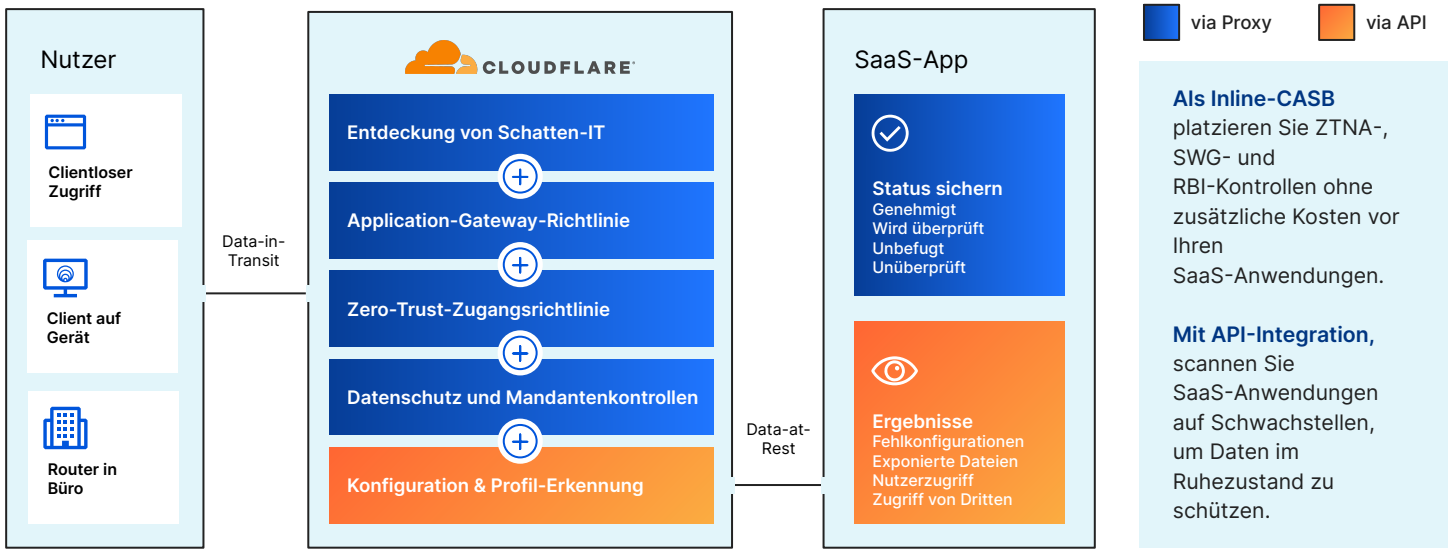
Wenn Unternehmen Dutzende von SaaS-Anwendungen einsetzen, wird es immer schwieriger, eine einheitliche Sicherheit, Transparenz und Performance zu gewährleisten.

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



Als Inline-CASB platzieren Sie ZTNA-, SWG- und RBI-Kontrollen ohne zusätzliche Kosten vor Ihren SaaS-Anwendungen.

Mit API-Integration, scannen Sie SaaS-Anwendungen auf Schwachstellen, um Daten im Ruhezustand zu schützen.

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.

Phishing-Schutz (CES)

Erweitern Sie Zero Trust auf E-Mails für umfassenden Schutz vor Bedrohungen

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.

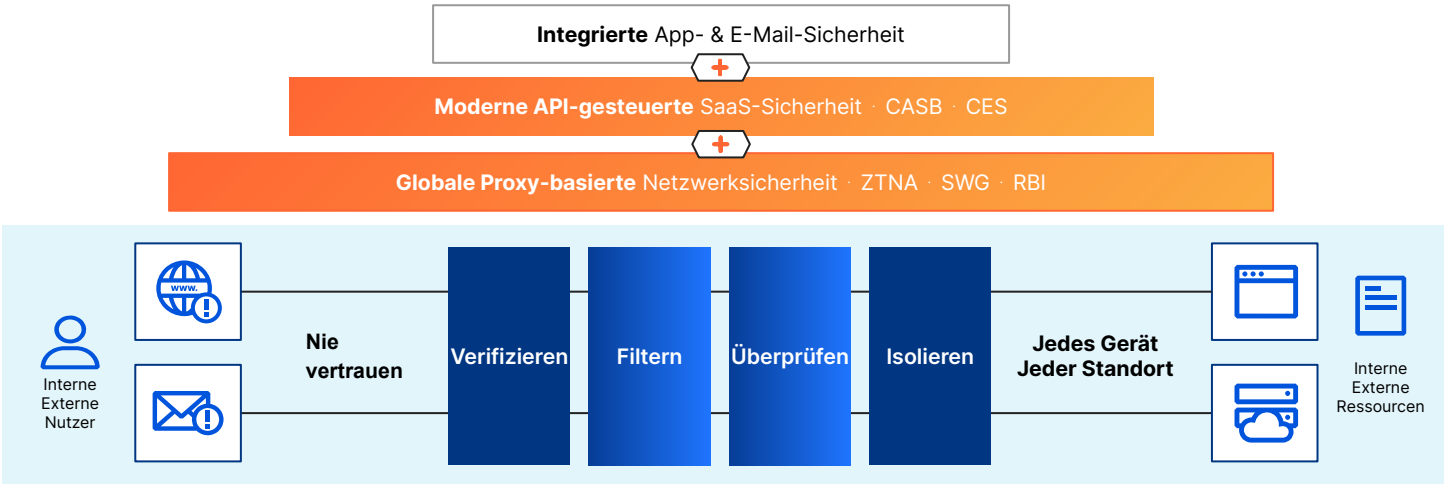
Angreifer haben es häufig auf das hohe Maß an Vertrauen abgesehen, das der E-Mail-Kommunikation oft entgegengebracht wird, und nutzen es erfolgreich aus.

Integration von Cloud-nativer E-Mail-Sicherheit

Durch den Einsatz von Area 1 Cloud-E-Mail-Sicherheit (CES) als Teil einer umfassenden Zero-Trust-Strategie wird das implizite Vertrauen in E-Mails aufgehoben, um Phishing- und BEC-Angriffe (Business Email Compromise) präventiv zu verhindern.

Der gesamte Traffic der Nutzer, einschließlich E-Mails, wird überprüft, gefiltert, inspiziert und von bekannten und unbekannten Bedrohungen isoliert. Area 1 hilft Kunden, E-Mail-Bedrohungen zu blockieren, eine proaktive Sicherheitshaltung einzunehmen und die Reaktionszeit auf Phishing-Vorfälle um 90 % zu reduzieren.

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



Wichtige Anwendungsfälle

Verhinderung von BEC und E-Mail-Betrug

Stoppen Sie ausgeklügelte BEC-Angriffe (Business Email Compromise) und die Übernahme von Konten von Lieferanten durch Sentiment-Analyse, Social Graphing von Partnern, Klassifizierung von Nachrichten und Analyse von Kampagnenquellen.

Automatische Blockierung, Quarantäne und Eskalation von betrügerischer Finanzkommunikation.

Schutz vor Multi-Channel-Angriffen

Blockieren Sie mühelos Angriffskampagnen, die über verschiedene Kommunikationskanäle wie E-Mail und Internet auf Einzelpersonen abzielen, indem Sie es Nutzern ermöglichen, verdächtige oder unbekannte Links sicher in einem entfernten, isolierten Browser zu laden.

Fangen Sie zeitversetzte Phishing-Angriffe ab, die Links nach der Zustellung als Waffe einsetzen, indem Sie nach dem Zeitpunkt des Anklickens des Links klassifizieren.

Beschleunigung der Phishing-Ersteinschätzung und -Reaktion

Setzen Sie Sicherheitsuntersuchungszyklen frei, gewinnen Sie nützliche Einblicke in Ihre E-Mail-Umgebung und verkürzen Sie die Reaktionszeiten mit speziellen Ressourcen, die Ihr bestehendes Team ergänzen, um Phishing-Bedrohungen schnell zu neutralisieren.

Profitieren Sie von zusätzlicher Unterstützung und Sicherheitsexpertise durch verwaltete E-Mail-Sicherheitsdienste.

Sicheres hybrides Arbeiten: Cloudflare macht den Unterschied

Moderne Sicherheit für eine moderne Belegschaft

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-Rampen 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

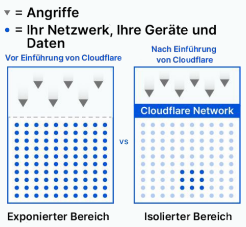
Dank unserer zukunftssicheren Architektur können wir neue Sicherheits- und Netzwerkfunktionen sehr schnell entwickeln und bereitstellen.

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 extreme Flexibilität.

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

Reduktion der Angriffs-oberfläche

91 % ↓



Reduktion der Datenleck kosten

35 % ↓

Beschleunigtes Onboarding von Mitarbeitern

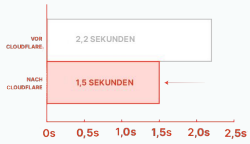
60 % ↑

Reduktion der IT-Ticket Belastung

80 % ↓

Reduktion der Nutzer-latenz

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