CLOUDFLARE

KURZDARSTELLUNG

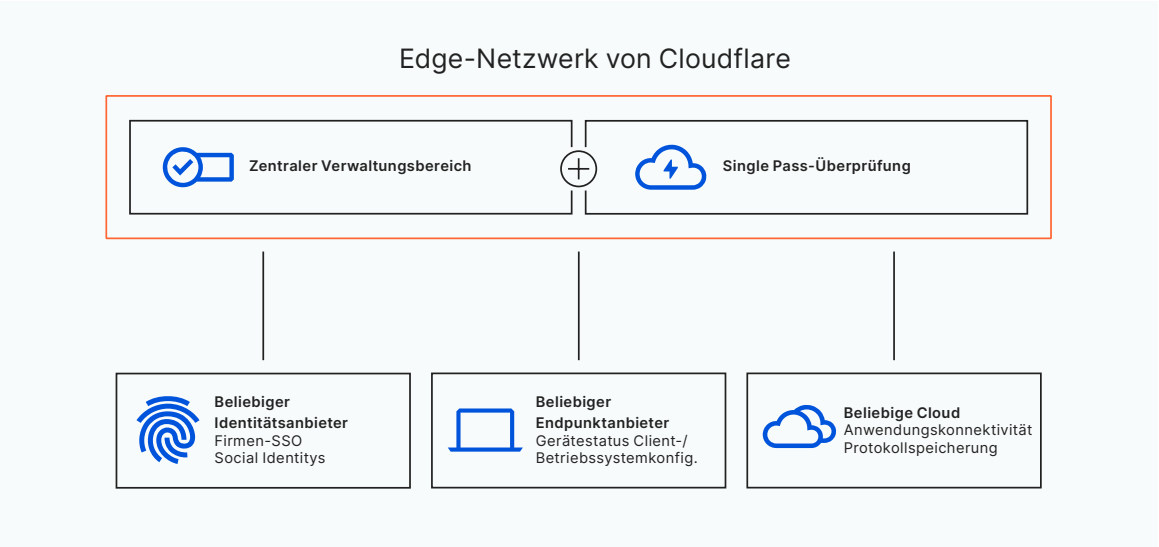
Zero Trust-Integrationen von Cloudflare

Verwendung gewohnter Identitäts-, Endpunktschutz- und Cloud-Provider

Das innerhalb eines Unternehmens mit verschiedenen Identitäts-, Endpunktschutz- und Cloud-Anbietern jongliert werden muss, ist zwar unvermeidlich, muss aber keine Belastung sein. Cloudflare hat das Ziel, Unternehmen die solideste Sicherheit bei größtmöglicher Anwenderfreundlichkeit zu bieten. Im Gegensatz zu anderen Anbietern haben wir kein persönliches Interesse daran, mit welchen konkreten Providern aus diesen Bereichen Sie aktuell oder in Zukunft zusammenarbeiten.

Wir sind anbieterneutral. Deshalb verfolgen wir seit Langem die Strategie, Cloudflare Zero Trust so zu gestalten, dass unser Angebot mit so vielen anderen Lösungen wie möglich kompatibel ist.

Cloudflare führt durch Integrationen die Meldungen der verschiedenen Provider zusammen und fungiert als eine einzige Kontrollebene, mit der detaillierte und durch Kontext angereicherte Richtlinien in unserem gesamten weltweiten Netzwerk durchgesetzt werden können. Für diese Integrationen müssen nicht einmal dicke Handbücher gewälzt werden, denn es existieren vordefinierte Workflows, um eine reibungslosere Verwaltung über eine einzige Schnittstelle zu ermöglichen.



Wir sind in drei Bereichen anbieterneutral, um unsere Kunden genau dort abholen zu können, wo sie gerade stehen:

- **Identität:** Zur Abdeckung sämtlicher Nutzer können für die Authentifizierung unterschiedliche Arten von Identitätsprovidern genutzt werden, ganz ohne Konfigurationsschwierigkeiten.
- **Endpunktschutz:** Überprüfungen des Gerätestatus können detaillierter und flexibler gestaltet werden und sowohl Informationen der bevorzugten Endpunktprovider als auch unseres Gerätеclients einbeziehen.
- **Cloud:** Um eine Langzeitbindung an bestimmte Anbieter zu vermeiden, können Anwendungen in jeder beliebigen Public Cloud oder (lokalen) Private Cloud geschützt werden.

Nutzung verschiedener Identitätsanbieter bei Cloudflare

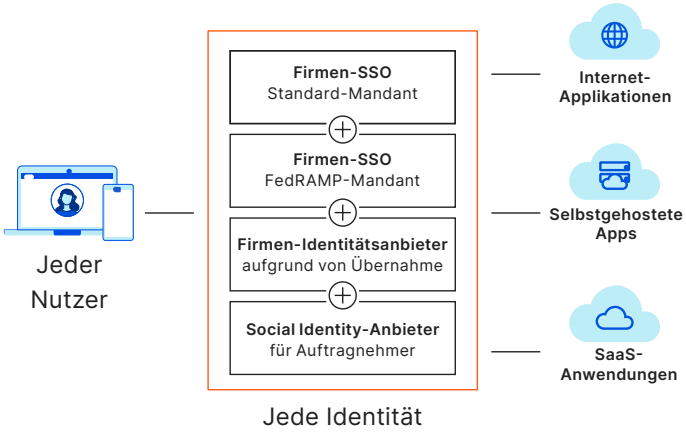
Mehrere SSO-Lösungen

Cloudflare hat eine der ersten Zero Trust-Zugangslösungen entwickelt, die mehrere Identitätsanbieter gleichzeitig unterstützt. Inzwischen bieten wir Integrationen für führende Anbieter von Firmenidentitäten (wie Okta oder Azure AD) sowie für Provider von Social Identitys (wie LinkedIn oder Github) und Open Source-Standards (wie SAML oder OIDC). Außerdem unterstützen wir verschiedene Instanzen des gleichen Identitätsanbieters, zum Beispiel Okta mit und ohne FedRAMP.

Gleichzeitige Einbindung mehrerer Identitätsanbieter

Unsere Fähigkeit, Identitäten über viele Identitätsanbieter hinweg zu bündeln, kann den Prozess der Erstellung identitätsbasierter Richtlinien beschleunigen. Unternehmen müssen keine individuellen Integrationen zwischen ihren Identitätsanbietern mehr erstellen.

Für Unternehmen im Wachstumsstadium mit einer begrenzten Zahl an Mitarbeitenden im Bereich Informationssicherheit, die den Aufwand der Konsolidierung eines einzigen zentralen Verzeichnisses scheuen, ist eine solche Einbindung unter Umständen ein wirkungsvolles Werkzeug zur Skalierung eines Zero Trust-Modells.



Wichtigste Funktionen

- Cloudflare bietet eine parallele Integration mehrerer branchenführender Identitätsanbieter
- Bündelung diverser Provider und Instanzen jedes Anbieters
- Schnelleres Onboarding für Drittnutzer und Partner aus Fusionen und Übernahmen

Anwendungsfall:

Erstklassiges Anwendererlebnis auch für Drittnutzer

Die von Cloudflare im Hinblick auf Identitätsanbieter angebotene Neutralität ist besonders praktisch bei der Zusammenarbeit mit Dritten wie Auftragnehmern, übernommenen Firmen oder Partnern. Zugangsregeln nach dem Prinzip der minimalen Rechtevergabe können in wenigen Minuten auf Grundlage der bereits bestehenden Nutzeridentitäten eingerichtet werden.

Dank dieser unkomplizierten und flexiblen Lösung können die Ineffizienz und Sicherheitsrisiken, die mit der Bereitstellung von SSO-Lizenzen, dem Einsatz von VPNs oder der Erstellung von Einmalberechtigungen verbunden sind, vermieden werden.

Branchenführende Partner im Bereich Endpunktschutz

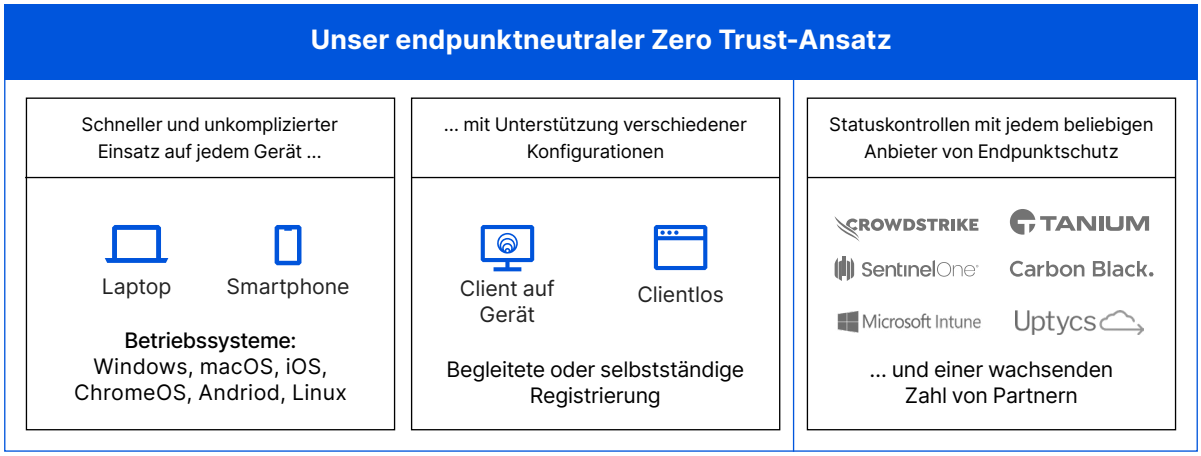
Partnerschaften

Cloudflare arbeitet mit CrowStrike, SentinelOne, VMware Carbon Black, Tanium, Uptycs und Microsoft Intune zusammen.

Kunden können sofort mehrere Anbieter von Endpunktschutz eingliedern und Sicherheitsdaten sowie Risikobewertungsfunktionen dieser Lösungen nutzen.

Konfiguration

Dank vordefinierter Workflows lassen sich diese Provider über das Cloudflare-Dashboard mit wenigen Klicks konfigurieren. Nach der Einrichtung kann Cloudflare kontrollieren, ob auf den Geräten die vom Kunden bevorzugte Endpunktsoftware läuft, um laufend auf Malware und andere Bedrohungen hin zu prüfen, bevor der Zugang zu einer geschützten Anwendung gestattet oder verwehrt wird.



Erweiterte Integration dank unseres Geräteclients (WARP)

Zur Verstärkung der Sicherheit ist oft ein Geräteclient erforderlich, der die Überprüfung des Gerätestatus durch zusätzliche Attribute bereichern kann. Wir haben unseren Client gezielt optimiert, um eine flexible und mühelose Einführung zu ermöglichen.

Kompatibilität mit den meisten Betriebssystemen

- Unser Enterprise-Client – WARP – funktioniert mit einer steigenden Zahl der beliebtesten Betriebssysteme (beispielsweise Windows, macOS, Linux, iOS, ChromeOS und Android).
- Unsere moderne WireGuard-Architektur erfordert höchstens geringfügige betriebssystemspefische Feinabstimmungen.
- Unser Enterprise-Client ist in einer Verbraucherversion verfügbar, die täglich millionenfach verwendet wird. Dank der Erprobung durch eine so große Zahl von Nutzern ist WARP besser für Zero Trust gerüstet als die meisten anderen Clients.

Optionen zur begleiteten oder selbstständigen Registrierung

- Bei verwalteten Geräten dokumentieren wir Implementierungen mit jeder beliebigen skriptbasierten Methode, die von beliebten Softwarelösungen für das Mobilgerätemanagement verwendet wird.
- Die selbstständige Registrierung bei WARP kann für Drittnutzer von Vorteil sein und lässt sich von jedem Desktop oder Smartphone aus innerhalb weniger Minuten abwickeln.

Keine Bindung an einen bestimmten Anbieter

Problem

Einigen monolithischeren Anbietern geht es in erster Linie darum, dass ihre Kunden ihre Clouddienste in möglichst großem Umfang nutzen, insbesondere auf Speicher- und Rechenebene.

Es ist daher nur logisch, dass ihre nachträglich hinzugefügten Sicherheitslösungen keine so reibungslose Integration mit anderen Cloudanbietern erlauben, wie es wünschenwert wäre. Kleinere Unannehmlichkeiten wie eine weniger solide Dokumentation und Bugs summieren sich mit der Zeit. Diese Bindung an einen bestimmten Technologiestapel macht ihrer Abteilung für Informationssicherheit das Leben schwer.

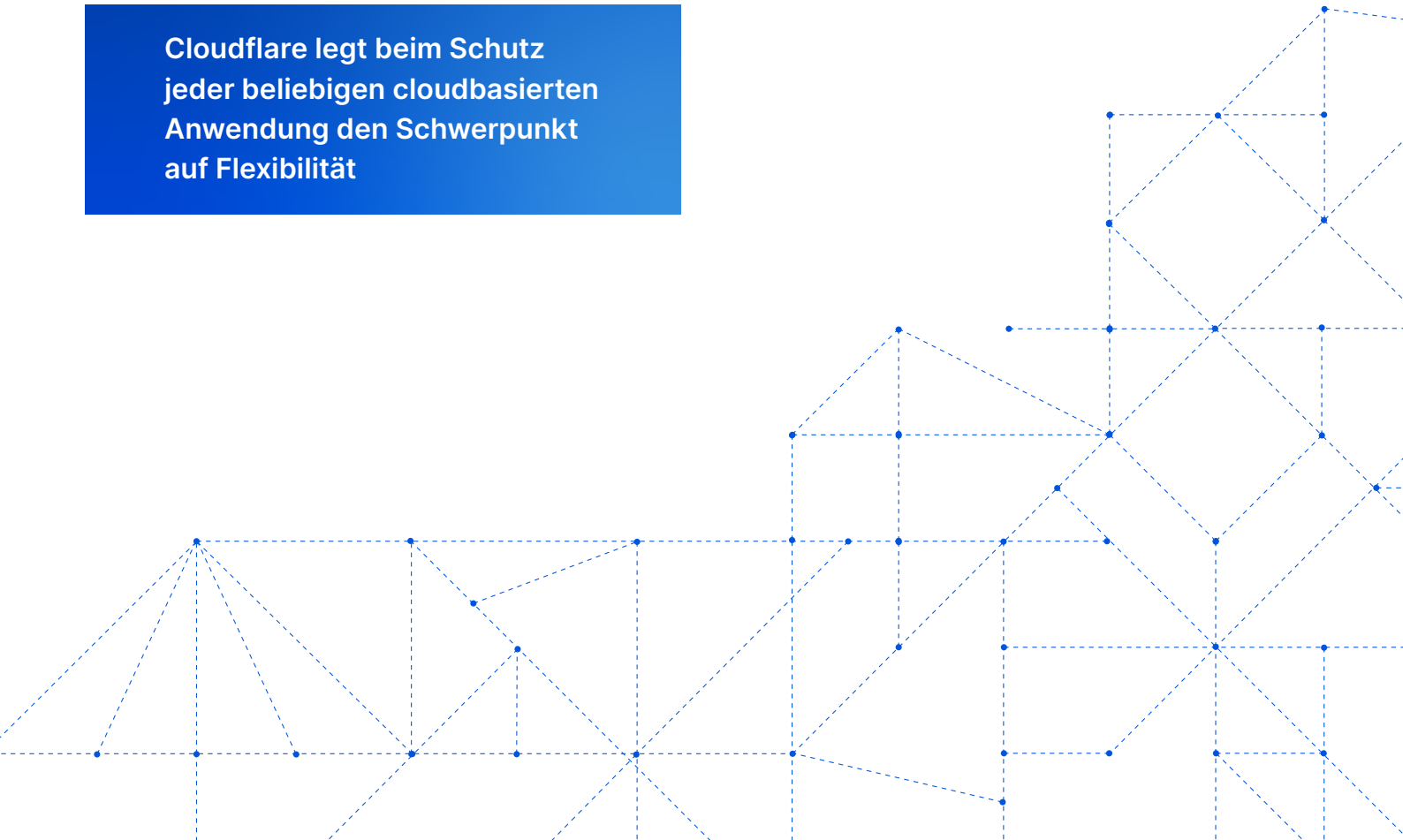
Lösung

Im Gegensatz dazu liegt der Fokus unserer Strategie nicht auf der Intensität bzw. dem Umfang der Cloudnutzung, sondern auf Sicherheit. Cloudflare ist cloudneutral. Wir schützen den Zugriff auf jede Ressource in allen Public-, Private- oder SaaS-Cloudumgebungen.

Cloudflare legt beim Schutz jeder beliebigen cloudbasierten Anwendung den Schwerpunkt auf Flexibilität

Wichtigste Funktionen

- Zero Trust-Zugang für Public-, Private- und SaaS-Cloudumgebungen
- Keine Bindung an bestimmte Anbieter von Cloudrechen- oder -Speicherdiensten
- Anwendungskonnektoren, Partner zur Netzwerkeingliederung und Speicherintegrationen für müheloses Interagieren mit Anwendungen in jeder Cloud



Die Stärken von Cloudflare

Erweiterung von Verbindungen auf Applikationen in jeder Cloud

Unser schlanker Anwendungskonnektor funktioniert in jeder Cloud

- Betrieb eines Kommandozeilen-Tools im „as a Service“-Modell unter Linux und anderen Betriebssystemen
- Aufbereitung als Docker-Container
- Unterstützung von Replikationen für moderne Kubernetes-Umgebungen
- Tunnelkonfiguration und -überwachung über Nutzerschnittstelle

Weitreichende Vernetzung mit Cloud-Providern

- 11.000 Schnittstellen zwischen unserem Netzwerk und anderen Cloudanbietern, von denen es sich in 50 Fällen um private Interconnections mit Microsoft, Amazon und Google-Rechenzentren handelt, bieten Nutzern schnelle Verbindungen

Verschiedene cloudneutrale Partner für die Netzwerkeingliederung

- Jede Public- oder Private-Cloudumgebung kann mit der gewohnten SD-WAN-Routingmethode (z. B. VMware) mühelos mit unserem Netzwerk verbunden werden; alternativ besteht die Möglichkeit einer privaten Interconnection bei einem von mehr als 1.600 Colocation-Standorten (z. B. der Firma Equinix)

Ablage von Protokolldateien in jeder Cloud

Speicherung von Protokolldateien in verschiedenen Clouds oder direkte Übermittlung an Analysedienstleister

- Integrierte parallele Unterstützung eines oder mehrerer Speicherziele wie AWS, Azure, Google Cloud und jede S3-kompatible API (z. B. Digital Ocean Spaces)
- Integrationen mit Analyse- und SIEM-Tools wie Sumo Logic, Splunk und Datadog

Sicherheit für jede Public oder Private Cloud

Große Auswahl an Zero Trust-Integrationspartnern

Im Laufe der Zeit wird Cloudflare die Informationen von einer noch größeren Zahl an den von unseren Kunden bevorzugten Providern bündeln. Dies wird mit Daten von unserer Zero Trust-Plattform und aus unserem globalen Netzwerk unterfüttert.

Identitätsanbieter

Firmen-SSOs

- Centrify
- Citrix ADC
- Google Workspace
- Jumpcloud
- Microsoft Azure Active Directory (AD)
- Okta
- OneLogin
- Ping Identity

Social Identitys

- Facebook
- GitHub
- Google
- LinkedIn
- Yandex

Open Source

- OIDC
- SAML 2.0

Endpunktanbieter

Anbieter von Lösungen für den Endpunktschutz

(für den Gerätesicherheitsstatus)

- Crowdstrike
- Microsoft Endpoint Manager
- SentinelOne
- Tanium
- Uptycs
- VMWare Carbon Black

Anbieter von Lösungen für Endpunktverwaltung

(zur Client-Implementierung)

- Hexnode
- Ivanti
- Jamf
- Jumpcloud
- Kandji
- Microsoft Intune

Partner für Netzwerkeingliederung

Partner für physische Interconnections

- 365 Rechenzentren
- BBIX
- CoreSite
- Cyxtera
- Databank
- Digital Realty
- EdgeConneX
- Equinix
- Netrality Data Centers
- Teraco
- Zayo

Partner für Fabric-Interconnections

- Console Connect / PCCW
- CoreSite
- Epsilon Infiny
- Equinix Fabric
- Megaport
- PacketFabric

SD-WAN

- Aruba (Silverpeak)
- Cisco
- VMWare (Velocloud)

Cloud-Anbieter

Cloud-Speicherziele:

- AWS S3
- Google Cloud Storage
- Microsoft Azure Blob Storage
- Andere Anbieter mit einer S3-kompatiblen API

Cloud Analytics- und SIEM-Partner

- Azure Sentinel
- Data Dog
- Elastic
- Google Cloud
- Graylog
- IBM QRadar
- Looker
- New Relic
- Splunk
- Sumo Logic

Mehr über Cloudflare Zero Trust erfahren und eine Demo oder einen Proof of Concept bei einem unserer Vertriebsmitarbeiter anfordern können Sie unter: https://www.cloudflare.com/de-de/products/zero-trust.

CLOUDFLARE

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

REV:BDES-3795.2022SEP26