

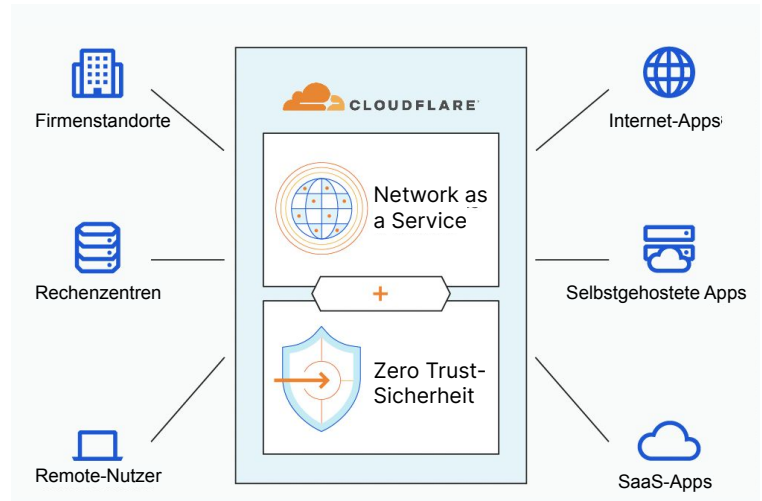
Cloudflare One

Stellen Sie Ihr Firmennetzwerk neu auf und bereiten Sie sich auf die Zukunft vor mit unserer Zero Trust-Network-as-a-Service-Plattform.

Teure Firmenstandleitungen können durch ein einziges globales Netzwerk mit integrierter Zero Trust-Sicherheit, DDoS-Abwehr auf Layer 3-7, einer Netzwerk-Firewall und Traffic-Beschleunigung ersetzt werden.

Nutzer werden auf unkomplizierte und sichere Weise ohne VPN mit Ressourcen verbunden, wodurch sich das Onboarding neuer User für manche Kunden um bis zu 60 % beschleunigt. Lateralen Bewegungen wird ein Riegel vorgeschoben und Ransomware, Malware und Phishing-Versuche werden blockiert.

Unsere **Secure Access Service Edge (SASE)**-Lösung Cloudflare One kombiniert Netzwerkverbindungsdienste und Zero Trust-Services auf einem der schnellsten, eigens dafür entwickelten globalen Netzwerke.

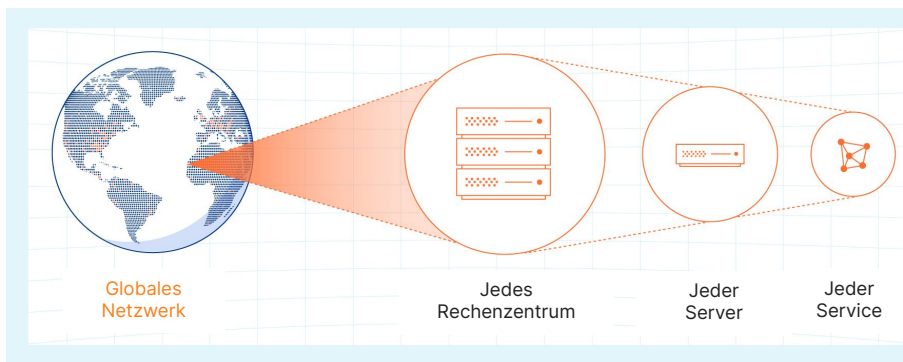


Warum gerade jetzt?

Trends seit Beginn der Pandemie:

- 80 %** Zunahme der Zahl der remote tätigen Wissensarbeitenden
- 23 %** Anstieg der Cloud-Einführungen
- 138 %** Zunahme von Ransom-DDoS- und Ransomware-Angriffen

Das Zero Trust-Modell nutzt eine Proxy-basierte Architektur, die eine Authentifizierung und Autorisierung jeder ein- und ausgehenden Anfrage sowie aller Anfragen zwischen den Instanzen eines Netzwerks verlangt. Den Nutzern wird also kein blindes und uneingeschränktes Vertrauen entgegengebracht, sobald sie Zugang zum Firmennetzwerk erhalten haben. Vielmehr können sie nur auf Anwendungen zugreifen, wenn sie dazu auch explizit berechtigt sind.



Einheitliche Geschwindigkeit und Dimension überall auf der Welt

Alle Funktionen für Sicherheit, Performance und Zuverlässigkeit können auf sämtlichen Servern in jedem Cloudflare-Rechenzentrum unseres Netzwerks eingesetzt werden, das sich aktuell über 275 Städte erstreckt. Da alle Dienste an jedem Standort betrieben werden, kann der Datenverkehr der Kunden jeweils in dem Rechenzentrum geprüft werden, das dem Ursprung des Traffics am nächsten ist.

10 → 1 Verbessern Sie die geschäftliche Flexibilität und sparen Sie Kosten

Zehn Einzelprodukte können durch eine einzige Plattform nach dem Baukastenprinzip ersetzt werden. Cloudflare One kann leichter implementiert werden und wird den Anforderungen besser gerecht als eine Kombination aus Einzellösungen verschiedener Anbieter. Die Verwaltung des WAN und der Netzwerksicherheit über ein einziges Dashboard spart Betriebskosten.

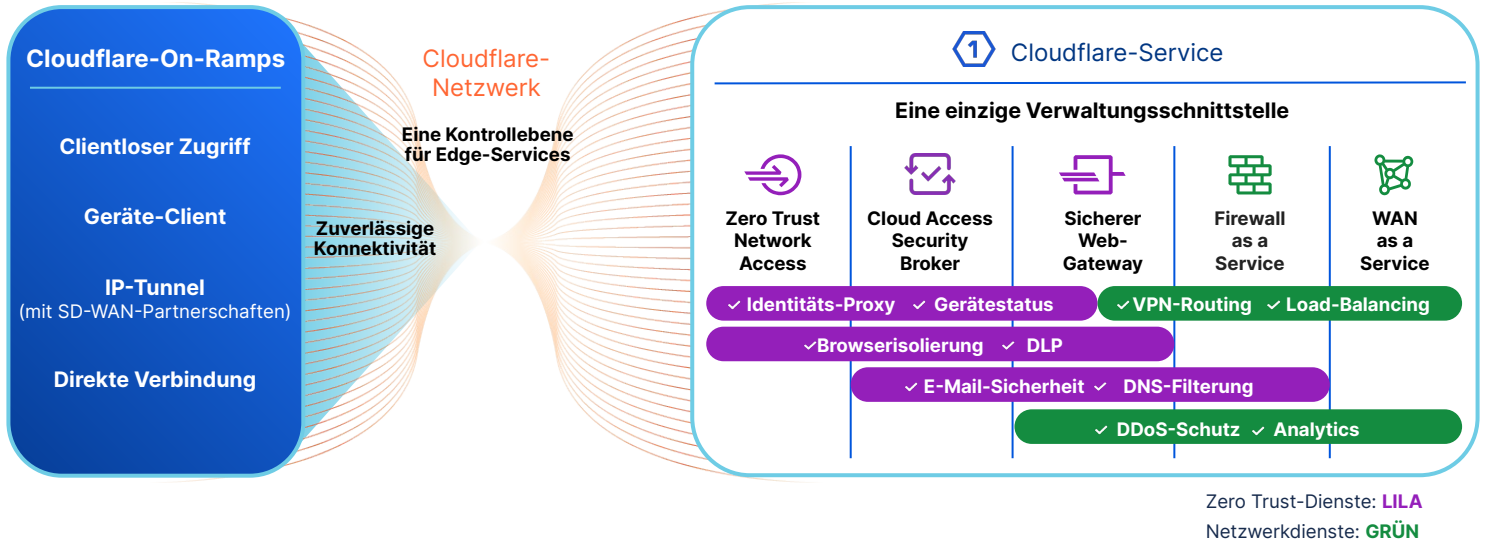
↓ 95 % Verringern Sie Ihre Angriffsfläche

Mithilfe unserer Edge kann Cloudflare One Bedrohungen gleich welchen Umfangs auf Netzwerkebene verzögerungsfrei Einhalt gebieten. Bevor die Nutzer Zugriff auf Anwendungen erhalten oder im Internet surfen können, werden ihre Anfragen in der Edge geprüft. Dadurch verringern sich Angriffsfläche und Abwehrzeiten. (Laut Schätzungen von Gartner sinken diese durch die Einführung von SASE um bis zu 95 %).

Möglichkeit der Verknüpfung mit bereits genutzten Systemen

Cloudflare One ist eine offene Plattform, die das On-Ramping der bereits genutzten Identitäts-, Endpunkt-, Cloud- und Netzwerkdienstleister unterstützt. Sie ist benutzerfreundlich und muss nur ein einziges Mal integriert werden.

So funktioniert Cloudflare One



Zero Trust-Netzwerkzugang

- Durchsetzung von Zero Trust-Regeln, die den Zugang zu selbstgehosteten Applikationen, SaaS-Anwendungen und privaten Netzwerk-IPs oder Hostnamen von Unternehmen beschränken.
- Schnellere und sicherere Verbindung von Nutzern als per VPN, wodurch der Zeitaufwand für einschlägige IT-Tickets um 80 % reduziert wird.
- Kompatibel mit mehreren Identitäts-, Endpunktschutz- und Cloud-Anbietern gleichzeitig für optimale Flexibilität.

Cloud Access Security Broker

- Verhindern Sie Datenlecks durch Transparenz und Kontrolle von SaaS-Anwendungen.
- Entdecken Sie Schatten-IT und legen Sie Richtlinien für das Zulassen/Blockieren von Apps fest.
- Scannen Sie SaaS-Anwendungen über die API-Integration auf Fehlkonfigurationen, unzulässigen Zugriff und andere Risiken, um Daten im Ruhezustand zu schützen.
- Fügen Sie Cloud-E-Mail-Sicherheit (CES) hinzu, um den Schutz für Ihre meistgenutzte und am stärksten beanspruchte SaaS-Anwendung – E-Mail – zu verbessern.

Sicheres Web-Gateway

- Schutz von Daten vor Malware, Ransomware, Phishing, Command & Control, Shadow IT und anderen Gefahren für alle Ports und Protokolle.
- Kontrollieren Sie den Datenfluss durch Durchsetzung von DNS-, HTTP-, Netzwerk- und Browserisolierungsregeln mit unbegrenzter TLS 1.3-Prüfung.
- Setzen Sie die Browserisolierung ein, um die Daten zu schützen, die in webbasierten Anwendungen enthalten sind, und kontrollieren Sie die Aktionen der Nutzer.

Firewall as a Service

- Cloudnative Netzwerk-Firewall für Ihr Unternehmen.
- Einheitliche Richtlinien für Netzwerksicherheit im gesamten WAN, einschließlich Firmenzentrale, Zweigstellen und virtuellen privaten Clouds.
- Weltweite Anwendung detaillierter Filterregeln in weniger als 500 ms – alles über ein gemeinsames Dashboard.

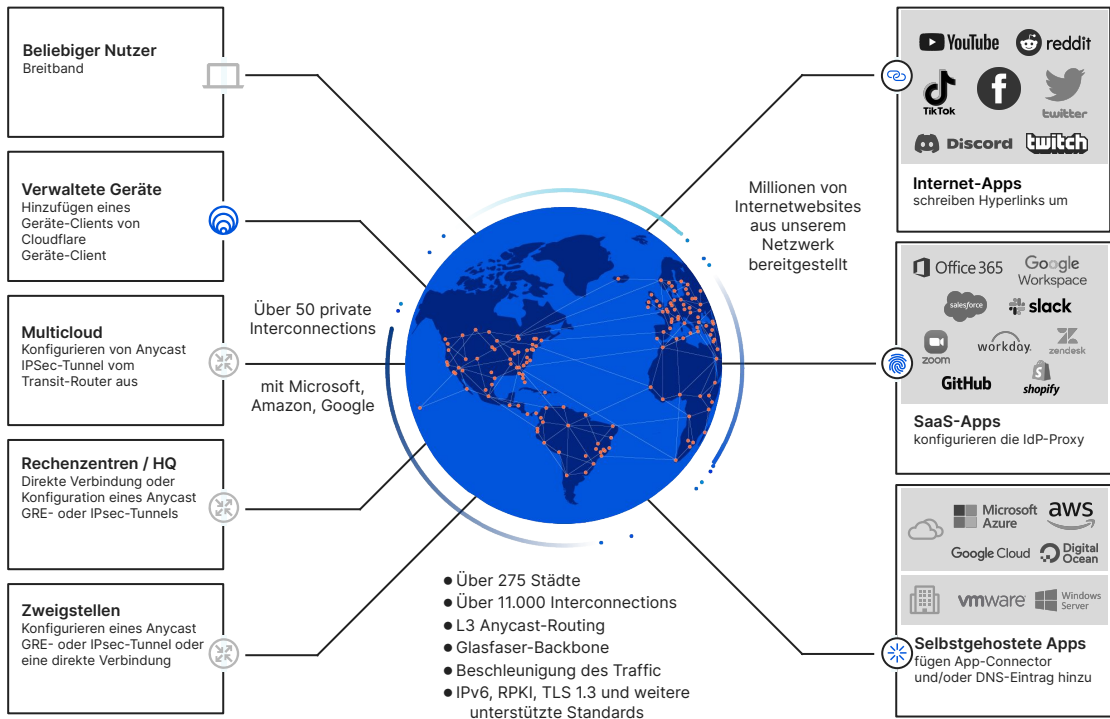
WAN as a Service

- Any-to-Any Full-Mesh-Konnektivität mit nativ integrierter Sicherheit, Performance und Kontrolle über eine einzige Schnittstelle.
- Partnerschaften mit führenden SD-WAN-Anbietern erleichtern die Arbeit mit Ihren bestehenden Investitionen.
- Verbinden Sie Rechenzentren und Zweigstellen direkt mit Cloudflare Network Interconnect (CNI), um die Zuverlässigkeit zu erhöhen und die Performance durch schnellere Bereitstellung zu verbessern.

Cloudflare-Netzwerk

- Single-Pass-Überprüfung für den gesamten Datenverkehr, um einen einheitlichen und schnellen Schutz für alle Nutzer zu gewährleisten.
- 100 %-Verfügbarkeit-SLA für kostenpflichtige Tarife, die nur eine Anycast-Architektur bieten kann.
- Mit einer kompatiblen, entwicklerfreundlichen Cloud-Plattform entwickelt, die es uns ermöglicht, neue Dienste zu entwickeln und bereitzustellen und neue Internet- und Sicherheitslösungen schnell einzuführen.

On-Rampen zu Cloudflare One



Über 10.000
Unternehmen vertrauen auf das Netzwerk von Cloudflare, wenn es darum geht, ihre Mitarbeiter mit internen Ressourcen zu verbinden

Über 5.500
Teams nutzen Cloudflare als sichere Verbindung zum Internet

Hunderttausende
Firmenanwendungen geschützt

Angaben nach Stand vom Dezember 2021

Gartner® Peer Insights™ Berichte



„Der Zero-Trust-Dienst von Cloudflare namens Cloudflare One ist erstklassig und hat unser Netzwerk vor mehreren Angriffen geschützt. Die Zusammenarbeit mit diesem Anbieter war ein absolutes Vergnügen. Das Team war bei jedem Schritt zur Stelle, um unsere Bedürfnisse zu verstehen und gemeinsam mit uns eine globale Lösung zu entwickeln.“

Director, Professional Services

„Wirkt definitiv wie ein Impulsgeber für die Kategorie, wenn nicht sogar wie ihr Erfinder. Die Menge an Innovationen, die seit der ersten Ankündigung im Jahr 2020 hervorgebracht wurde, ist schlichtweg unglaublich.“

Was gefällt Ihnen am besten?: „Die klare Vision, die das Unternehmen hat, wie es die Vorteile seines Edge-Netzwerks nutzen kann...“

Chief Technology Officer, Versicherungsunternehmen

„Wir hatten bereits Zscaler im Einsatz, aber uns wurde Cloudflare One empfohlen. Nach eingehender Prüfung und einem Benchmarking mit unserem derzeitigen Anbieter und anderen Providern haben wir uns für Cloudflare One entschieden und könnten nicht zufriedener sein. Die bisherigen Erfahrungen sind mehr als positiv.“

Projekt-Manager, Transportunternehmen mit 1–3 Mrd. \$ Jahresumsatz

„Wir haben Cloudflare One sehr oft genutzt und es ist ein leistungsstarker All-in-One-Dienst. Das globale Netzwerk von Cloudflare hält unsere Anwendungen stets verfügbar, der Zero Trust-Dienst schützt sie und ist damit eine hervorragende Alternative zu unserem VPN.“

Network Engineer, Finanzunternehmen mit 3–10 Mrd. \$ Jahresumsatz

Wechseln Sie jetzt zu einem schnelleren, zuverlässigeren und sichereren Netzwerk

Beratung anfragen

Noch nicht bereit für Ihre Analyse?
Erfahren Sie noch mehr über [Cloudflare One](#)

Gartner Peer Insights-Inhalte bilden die subjektiven Meinungen einzelner Endnutzer ab, die auf ihren Erfahrungen mit den auf der Plattform aufgeführten Anbietern beruhen. Weder sind sie als Tatsachenbehauptungen auszulegen, noch spiegeln sie die Ansichten von Gartner oder verbundenen Unternehmen wider. Gartner unterstützt keine Anbieter, Produkte und Dienstleistungen, die in diesen Inhalten dargestellt werden, und übernimmt in Bezug auf diese Inhalte, ihre Korrektheit und Vollständigkeit weder ausdrückliche noch stillschweigende Gewähr, wodurch auch die Mängelgewährleistung und die Gewährleistung der Eignung für einen bestimmten Zweck ausgeschlossen sind. GARTNER ist eine eingetragene Handels- und Dienstleistungsmarke und PEER INSIGHTS ist eine Handels- und Dienstleistungsmarke von Gartner, Inc. und/oder den Tochtergesellschaften des Unternehmens in den USA und anderen Ländern, die im Folgenden mit Genehmigung verwendet wird. Alle Rechte vorbehalten.