Absicherung hybrider Arbeit

Reduzieren Sie Risiken und erhöhen Sie die Transparenz für alle Nutzer, sowohl innerhalb als auch außerhalb des Netzwerks.

Verbindungen jedes Nutzers geräte- und ortsunabhängig schützen

Unsere Zukunft des ortsunabhängigen Arbeitens: Nach Jahren der globalen Pandemie und angesichts der bevorstehenden Rezession wird die hybride Arbeitsweise wohl auch in Zukunft beibehalten werden. IT- und Sicherheitsteams müssen durchgängigen Schutz und einheitliche Erfahrungen für alle Nutzer und Geräte bieten, unabhängig davon, ob sie im Büro oder an einem anderen Ort arbeiten. Herkömmliche standortbezogene Tools (wie VPNs und IP-basierte Kontrollen) werden dieser Aufgabe nicht gerecht.

Moderne Sicherheit für eine moderne Belegschaft: Als Reaktion darauf überdenken viele Unternehmen ihre IT- und Sicherheitsarchitektur und setzen auf cloudbasierte Sicherheit, die sich an die Bedürfnisse verteilter Belegschaften anpasst und bewährten Praktiken für Zero Trust folgt.

Cloudflare macht es einfach, jede Verbindung zu sichern, so dass Nutzer auf jedem Gerät oder an jedem Ort sicher und produktiv bleiben, wenn sie auf Anwendungen oder das Internet zugreifen.

Was Gartner® sagt:

> *2026 werden 75 % der Arbeitnehmer ihre Arbeitszeit weiterhin zwischen ihrem Zuhause und dem traditionellen Büro aufteilen, ein leichter Rückgang gegenüber 77 % auf dem Höhepunkt der Pandemie im Jahr 2021.*[1]

> *Konzepte für die Netzwerksicherheit, die auf einer Reihe von Sicherheitsanwendungen am Rande des Netzwerks basieren, sind für die dynamischen, jederzeit und überall verfügbaren Anforderungen eines modernen digitalen Unternehmens und seiner hybriden digitalen Belegschaft nicht geeignet.*[2]

Inhaltsverzeichnis nach Seiten

Möglichkeiten zur Modernisierung der Sicherheit

Sicherer Anwendungszugriff ohne VPN

Da die Nutzer so weit verstreut sind, verlangsamt die Rückführung des Traffics (Backhauling) über lokale Anwendungen wie VPNs die Performance und birgt das Risiko, dass sich Bedrohungen lateral über das Unternehmensnetzwerk ausbreiten.

Gewinnen Sie stattdessen wieder Transparenz über alle Anfragen und setzen Sie identitätsbasierte Kontrollen durch, die näher am Nutzer sind, um die Produktivität zu erhalten. Keine Rückführung von Traffic erforderlich.

Optimieren Sie die SaaS-Sicherheit

Mehr denn je verlassen sich die Mitarbeiter auf SaaS-Anwendungen, die nicht von herkömmlichen Unternehmensnetzwerken kontrolliert werden.

Als Reaktion darauf benötigen Unternehmen eine umfassendere Transparenz und Kontrolle über ihre SaaS-Anwendungen, um Zugriffsrichtlinien festzulegen, Datenschutzkontrollen anzuwenden, die Schatten-IT einzudämmen und Anwendungen auf Fehlkonfigurationen zu überprüfen.

Schützen Sie Nutzer und Daten vor Bedrohungen im Internet

Ransomware, Phishing und andere Internet-Bedrohungen sind allgegenwärtig und werden immer raffinierter.

Durch die Einführung einer cloudbasierten Überprüfung und Isolierung des ausgehenden Traffics sind die Nutzer vor Malware geschützt. Darüber hinaus können Administratoren Kontrollen anwenden, um zu verhindern, dass sensible Daten auf lokale, nicht verwaltete Geräte gelangen.

Hybride Arbeit für reife Unternehmen

Reife Unternehmen können die Sicherheit für hybrides Arbeiten zuverlässig modernisieren

Herausforderung: Komplexe, veraltete Umgebungen

Die Unternehmen experimentieren mit Modellen für die Arbeit im Büro. Allerdings ist es in diesen hybriden Szenarien schwierig, durchgängige Schutzmaßnahmen und Nutzererfahrungen zu gewährleisten.

Diese Unternehmen sind in der Regel etablierter und verfügen über umfangreichere (oft komplexe) On-Premise- und Legacy-Investitionen. Der Start eines neuen Sicherheitsprojekts kann sich angesichts des rezessiven Gegenwinds zu riskant und schwierig anfühlen.

Chance: Einfacher Weg zur Modernisierung

Unternehmen verdienen es, die digitale Transformation in ihrem eigenen Tempo voranzutreiben, ohne ein unbegrenztes Budget, teure „Proofs-of-Concept“, komplexe Implementierungsphasen oder verkettete Services zu benötigen.

Um den Anforderungen dieser reifen Unternehmen im Bereich der hybriden Arbeit gerecht zu werden, ist Cloudflare so konzipiert, dass es einfacher und schneller zu implementieren ist als andere Zero-Trust-Dienstanbieter wie Zscaler.

Beispiele für Anwendungsfälle

Telekommunikation

Situation: Ein über 100 Jahre altes europäisches Telekom-Unternehmen mit über 20 Mrd. USD Jahresumsatz wollte einen einzigen Anbieter für die Bereitstellung von Internetfiltern und die Authentifizierung des Zugriffs auf ältere Anwendungen, die kürzlich in mehrere Cloud-Umgebungen migriert worden waren.

Lösung: Das Unternehmen entschied sich für Cloudflare, um seine Dienste zusammenzuführen und eine einheitliche Plattform zu nutzen, um sowohl die Anwendungen als auch den Internetzugang seiner über 100.000 Mitarbeiter zu sichern.

US-Bundesregierung

Situation: Das U.S. Department of Homeland Security (DHS) ist führend bei Investitionen in den Schutz vor Internet-Bedrohungen in allen Bundesämtern, Standorten und Infrastrukturen.

Lösung: DHS beauftragte Cloudflare und Accenture Federal Services mit der Entwicklung einer gemeinsamen Lösung zur Filterung von DNS-Anfragen an bösartige und riskante Ziele, die in allen Bundesbehörden eingesetzt werden soll.

Medien & Werbung

Situation: Medienkonglomerat (über 10 Mrd. USD Umsatz und mehr als 100.000 MA weltweit) sieht sich Cyberangriffen auf die interne Infrastruktur ausgesetzt, einschließlich einer Lösegeldforderung.

Lösung: Cloudflare sichert Hunderte von Web- und Nicht-Web-Anwendungen mit identitätsbasierten Zero-Trust-Regeln. Das Unternehmen führt den Schutz für 50.000 Mitarbeiter innerhalb von 3 Monaten ein und plant eine Ausweitung auf die gesamte Belegschaft innerhalb von 9 Monaten.

Energieversorgung

Situation: Der Fortune-500-Erdgasversorger suchte nach einem verbesserten Schutz vor den zunehmenden Cyber-Bedrohungen, die auf den Sektor abzielen, sowohl für seine verteilten Rechenzentren als auch für seine über 1.500 Mitarbeiter.

Lösung: Das Unternehmen entschied sich Zscaler durch Cloudflare zu ersetzen. Als Gründe nannte man die bessere Zuverlässigkeit und Einheitlichkeit beim Schutz von Anwendungen und Internetzugang sowie langfristig einen einfacheren Weg, um erweiterte Kontrollen mit Remote-Browserisolierung einzuführen.

ZITATE VON KUNDEN

> *Cloudflare gibt uns starken Rückenwind auf unserem Weg zu Zero Trust.*

John McLeod
CISO, National Oilwell Varco

> *Cloudflare hat es der Ziff Media Group ermöglicht, unsere internen Tools nahtlos und sicher für Mitarbeiter auf der ganzen Welt auf jedem Gerät bereitzustellen, ohne dass komplizierte Netzwerkkonfigurationen erforderlich sind.*

Josh Butts
SVP Product & Technology,
Ziff Media Group

> *„Mit Cloudflare konnten wir unsere Abhängigkeit von VPNs und IP-Positivlisten für Entwicklungsumgebungen reduzieren.*

Alexandre Papadopoulos,
Director of Cyber Security,
INSEAD

Remote-first-Belegschaften für Digital Natives

Für Digital Natives: Agile Sicherheit priorisieren, um Flexibilität bei der Remote-Arbeit zu unterstützen

Herausforderung: Cloud-Sicherheit skalieren und automatisieren

Viele Unternehmen setzen auf Remote-First-Neueinstellungen. Oft handelt es sich dabei um jüngere Unternehmen, die sich schon früh für die Cloud entschieden haben, über eine begrenzte lokale Infrastruktur verfügen und deren Geschäftsmodelle auf sicheren, schnellen und zuverlässigen digitalen Diensten beruhen.

Flexibilität bei der Arbeit von überall aus kann ein wichtiges Unterscheidungsmerkmal sein, erfordert aber auch Sicherheitstools, die ebenso flexibel sind, da die Nutzer sich bewegen und auf persönliche Geräte angewiesen sind.

Die Gelegenheit: Zusammensetzbare, skalierbare Sicherheit

Da weniger IT-Altlasten abgeschafft werden müssen, können diese Digital Natives unsere Internet-native Architektur und Bereitstellungsflexibilität nutzen, um bei der Modernisierung ihrer Sicherheit flexibel zu bleiben.

Unsere zusammensetzbaren Dienste, das API-first-Design und die Verwaltung über eine einzige Schnittstelle erleichtern den Einstieg und die Anpassung der Sicherheit. Die Geschwindigkeit, der Umfang und die Zuverlässigkeit unseres globalen Netzwerks entsprechen den Anforderungen einer reinen Remote-Belegschaft.

Beispiele für Anwendungsfälle

B2B SaaS

Situation: Die australische Grafikdesign-Plattform Canva (2021 mit 40 Mrd. USD bewertet) setzte Cloudflare vor der Pandemie ein, um den Zugang für Nutzer von Drittanbietern zu optimieren und die Schwierigkeiten bei der Implementierung eines VPN zu vermeiden.

Lösung: Im Laufe der Zeit hat Canva Richtlinien für den ZeroTrust-Anwendung-szugriff für die gesamte wachsende Belegschaft eingeführt und die Internet-Filterung und -Überprüfung erweitert.

Fintech & Blockchain

Situation: BlockFi – eine auf Blockchain-Technologie basierende Vermögensverwaltungsplattform – musste angesichts der Cyber-Bedrohungen gegen sein wachsendes verwaltetes Vermögen und seine Remote-First-Belegschaft für mehr Sicherheit sorgen.

Lösung: Mit Cloudflare konnte BlockFi zu einer identitätsbasierten Authentifizierung für den Anwendungszugang übergehen und sich von zeitaufwändigen IP-basierten Kontrollen lösen.

Social Media

Situation: Bei einer globalen Social-Media-Plattform gab es eine vielbeachtete Datenschutzverletzung, bei der der interne Anwendungszugang und VPN-Konfigurationen ausgenutzt wurden.

Lösung: Als Reaktion darauf beschloss das Unternehmen, seinen Ansatz für den Fernzugriff zu überarbeiten, indem es die Zero Trust Network Access (ZTNA)-Lösung von Cloudflare für 13.000 Mitarbeiter und Auftragnehmer einführte und seine VPN-Implementierungen abschaffte.

E-Commerce

Situation: Eine globale E-Commerce-Plattform (über 4 Mrd. USD Umsatz und über 15.000 MA) strebte einen besseren Schutz für Nutzer an, die außerhalb des Netzwerks im Internet surfen und auf sensible SaaS-Anwendungen zugreifen.

Lösung: Das Unternehmen setzt Cloudflare ein, um Funktionen zum Schutz vor Bedrohungen wie DNS-Filterung zu nutzen und gleichzeitig einen besseren Einblick in die Nutzung von SaaS-Anwendungen zu erhalten.

ZITATE VON KUNDEN

> *Hier bei Delivery Hero sind wir immer bestrebt, unseren Kunden ein tolles Erlebnis zu bieten. Cloudflare hilft uns dabei, dasselbe für unsere internen Teams zu erreichen: Die Lösung bietet ihnen weltweit eine sichere Arbeitsumgebung und eine einfache Möglichkeit, schnelle, zuverlässige und datenschutzkonforme Anwendungen zu entwickeln.*

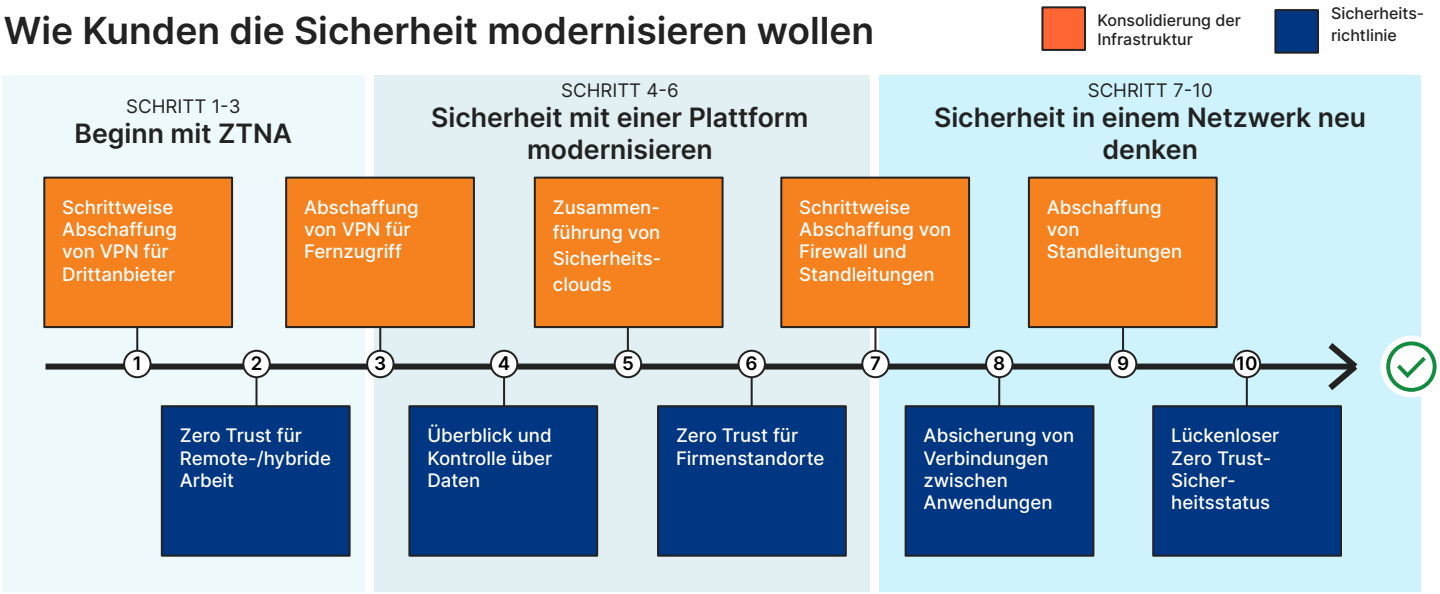
Christina von Hardenberg
CTO, Delivery Hero

> *Cloudflare ist für die Absicherung unserer schnell wachsenden Remote-Belegschaft unerlässlich. Die Einführung von Zero Trust für den Anwendungszugriff verschaffte unseren Administratoren mehr Transparenz und präzisere Kontrollen, die sie mit früheren Tools nicht erreichen konnten.*

Marccio Alcaide
Head, IT Security, Facily

Illustrative Roadmap für hybride Arbeit

Wie Kunden die Sicherheit modernisieren wollen



Roadmap für die Modernisierung der Sicherheit

Die obige Roadmap veranschaulicht den Ansatz, den wir bei Unternehmen sehen, wenn sie ihre Sicherheit modernisieren, um sich für hybride Arbeit zu rüsten. Diese Roadmap verfolgt zwei wesentliche Ziele:

1) **Oberste Reihe (in orange):** Zusammenführung der Konnektivitäts- und Sicherheitsinfrastruktur weg von Einzelprodukten und Hardware hin zu einer Cloud-nativen Plattform.
2) **Untere Reihe (in blau):** Um die Transparenz und die Kontrollen für die Einführung von Zero-Trust-Sicherheit zwischen Nutzern und Ressourcen auf jedem Gerät und an jedem Ort zu erhalten.

Phasen 1 - 5: Sicherung von App und Internetzugang

Für viele bedeutet die Umstellung auf hybride Arbeitsformen, dass sie zunächst die Art und Weise modernisieren müssen, wie die Mitarbeiter die Unternehmensressourcen erreichen.

Phase 1: Oft besteht der erste Schritt darin, den VPN-Datenverkehr auszulagern und für ausgewählte Benutzer – wie Auftragnehmer, Entwickler, Partner oder neu erworbene Teams – auf internetnative Kontrollen umzustellen. Cloudflare macht es besonders einfach, selbst gehostete Apps zu sichern, auf die über einen Browser zugegriffen werden kann, ohne dass Software auf Endpunkten bereitgestellt werden muss.

Phase 2: Dieses moderne Instrumentarium bietet die notwendige Transparenz, um Richtlinien für einzelne Anwendungen auf der Grundlage von Rollen, MFA- und Hard-Key-Anforderungen sowie Identitäts- und Gerätestatus zu erstellen.

Phase 3: Nachdem die Teams Vertrauen in diesen Ansatz aufgebaut haben, schaffen sie ihr VPN vollständig ab und schützen private Netzwerke, die nicht zum Internet gehören, mit Zero Trust.

Phase 4: Dann fokussiert man sich darauf, die Transparenz zu steigern und Kontrollen für SaaS-Apps zu verbessern, sodass man etwa Schatten-IT eindämmen, Mandanten verwalten und Datenexfiltration verhindern kann.

Phase 5: Da interne und SaaS-Anwendungen nun von einer einzigen Plattform aus verwaltet werden, wollen Unternehmen die Kontrollen für den ausgehenden Internetzugang erweitern und Tools zum Schutz vor Bedrohungen wie DNS-Filter und Secure Web Gateways zusammenführen.

Phasen 6-10: Verlagerung der Konnektivität in die Cloud

Die verbleibenden Roadmap-Phasen sind bei den meisten Unternehmen noch in Planung, aber ihr Ziel ist es, die gesamte Netzwerkkonnektivität und -sicherheit auf ein einheitliches Cloud-Netzwerk zu verlagern.

Phase 6: Hier versuchen Unternehmen, einheitliches Zero Trust auf alle Netzwerkstandorte wie Hauptsitz, Zweigstellen, Rechenzentren und Satellitenbüros auszuweiten, um hybrides Arbeiten zu unterstützen.

Phase 7: Da der Traffic in den Büros zunehmend an Cloudflare gesendet wird, können Unternehmen herkömmliche Firewalls und andere private Netzwerkanwendungen abschaffen.

Phase 8: Diese fortschrittlichen Anwendungsfälle konzentrieren sich auf die Sicherung der App-to-App-Konnektivität in hybriden Multi-Cloud-Umgebungen und bereiten das Netzwerkinfrastrukturteam auf die Ablösung von MPLS-Verträgen mit Telekommunikationsunternehmen in **Phase 9** vor.

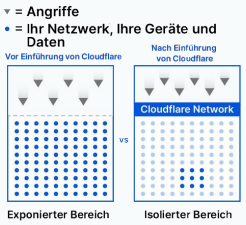
Phase 10: Obwohl die Modernisierung nie wirklich abgeschlossen ist, wird angestrebt, dass sich Zero Trust auf alle Nutzer, Geräte, Daten, Anwendungen und Umgebungen erstreckt.

Ergebnisse für Unternehmen und Sicherheit

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

Reduktion der Angriffsoberfläche

91 %↓



Reduktion der Kosten Einer Datenschutzverletzung

35 %↓

Beschleunigung des Onboardings von Mitarbeitern

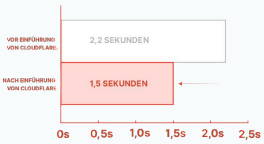
60 %↑

Reduktion der Anzahl an IT-Tickets

80 %↓

Reduktion der Nutzerlatenz

39 %↓



Sonstige Geschäftstreiber

Produktivität der Belegschaft steigern

Für Administratoren

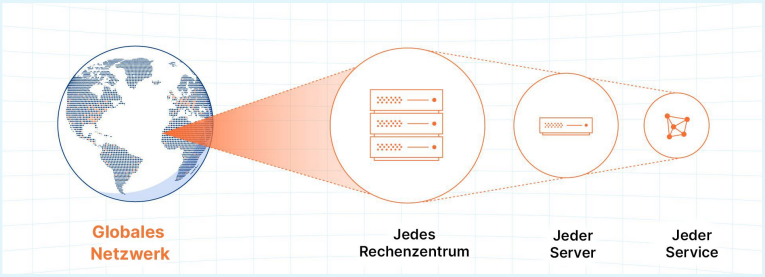
- Vereinfachte Konfiguration mit einer einzigen Verwaltungsschnittstelle zur Festlegung von Richtlinien für Anwendungen und Internetzugang
- Konfigurieren Sie alle Integrationen mit Identitätsanbietern, Endpunktschutz, Cloud-Anbietern und Netzwerkzugängen über dieselbe Verwaltungsoberfläche

Für Endnutzer

- Reibungslose Authentifizierung und native Browsing-Erlebnisse mit Sicherheit, die nicht im Weg ist

Kostenreduzierung bei bestehenden Diensten

- Ersetzen oder erweitern Sie Ihre Virtual Private Network (VPN)-Appliances und verwenden Sie stattdessen Zero Trust Network Access (ZTNA)
- Umstellung von lokalem Web-Proxy oder Firewall auf cloud-native L3-L7-Sicherheitsdienste
- Auslagerung von Anwendungsfällen aus der virtuellen Desktop-Infrastruktur mit Remote Browserisolierung (RBI)
- Tauschen Sie das herkömmliche sichere E-Mail-Gateway gegen moderne Cloud-E-Mail-Sicherheit



Einheitliche Geschwindigkeit und Skalierbarkeit zum Schutz aller Nutzer im Büro oder an anderen Standorten

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.

Beschleunigen Sie Ihre Roadmap zur Zero-Trust-Implementierung

JETZT TESTEN | Kontakt

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

REV: PMM-2022JJUL

[1] *Top Network Practices to Support Hybrid Work*, Gartner, Karen Brown, Andrew Lerner, Mike Toussaint, 04/08/2022
[2] *2022 Strategic Roadmap for SASE Convergence*, Gartner, Neil MacDonald, Andrew Lerner, John Watts 06/24/2022