CLOUDFLARE

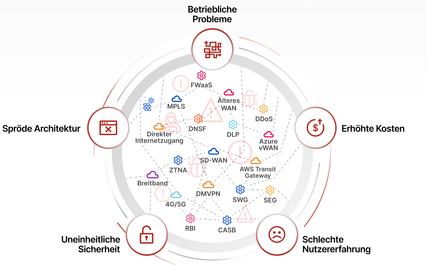
Jeder Pfad ist wichtig

Ist es an der Zeit, den Netzwerkverkehr umzuleiten?

Ältere Unternehmensnetzwerke konzentrierten sich nur auf interne Konnektivität und Sicherheit. Hybrides Arbeiten, cloudbasierte Anwendungen und schnelle Investitionen in die digitale Modernisierung haben jedoch drastisch verändert, wo und wie Netzwerk-Traffic fließt.

Was passiert, wenn die Netzwerkinfrastruktur den heutigen Geschäftsanforderungen nicht gewachsen ist?

Ältere Unternehmensnetzwerke erleben häufig folgende Herausforderungen:



52 % der Führungskräfte sagen, dass **Komplexität die größte Hürde** für den Sicherheitsbetrieb ist[1]

70 % der CEOs weltweit sagen, dass sich der Reifegrad ihres **Netzwerks negativ auf** den Geschäftsbetrieb auswirkt[2]

101 % ist die durchschnittliche Rendite für plattformisierte Organisationen, im Vergleich zu 28 % für jene, die keine Plattformisierung eingeführt haben[1]

In herkömmlichen Architekturen erhöht die **Verwendung von Dutzenden verschiedenen Lösungen zur Abdeckung der vier Netzwerkverkehrsströme** ebenfalls die Komplexität

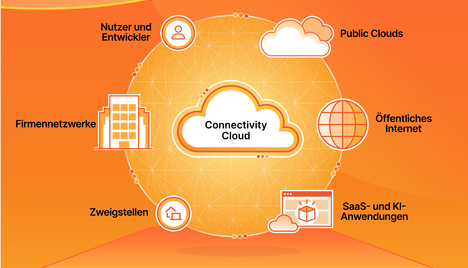
Traffic-Fluss	Erforderliche Produkte	Herausforderungen
Eingehender Traffic aus dem Internet	Traditionell abgedeckt durch Firewalls, VPN, DMZ-Infrastruktur, ISP-Filterung	• DoS- und DDoS-Angriffe • Zero-Day-Schwachstellen • Phishing • Schadsoftware
Ausgehender Traffic zum Internet und zu cloudbasierten Anwendungen	Traditionell durch lokale Firewalls und Proxys geschützt	• Laterale Bewegung • Datenoffenlegung • Verbreitung von Ransomware • Botnetz-Beteiligung
WAN-Vernetzung über Campus- und Zweigstellenstandorte hinweg	Traditionell abgedeckt durch physische/virtualisierte Netzwerke, SD-WAN, private Interconnects, MPLS	• Höhere Investitionsausgaben • Latenz im Netzwerk • Bandbreitenbeschränkungen • Schlechte Nutzererfahrung
Multicloud für Anwendungen in mehreren Clouds	Traditionell von DIY-Produkten abgedeckt.	• Probleme mit Transparenz und Richtliniendurchsetzung • Komplexität der Vorschriften

Was muss sich **ändern?**

Veraltete Netzwerke	vs.	Moderne Netzwerke
• Eingefügte Appliances, um neue Funktionen oder Regionen hinzuzufügen — was Ausfallzeiten und Serviceunterbrechungen erfordert. • Nutzer und Zweigstellen wurden mit den im Rechenzentrum gehosteten Anwendungen verbunden und abgesichert • Implizit „vertrauenswürdiger" Datenverkehr innerhalb des Perimeters • Wurden für die Unterstützung von Mitarbeitenden im Büro optimiert		• Setzen zusammensetzbare Dienste anstelle von Appliances ein, um die Komplexität und Störungen zu reduzieren • Müssen überall Cloud-, SaaS- und Private-Cloud-Anwendungen unterstützen • Müssen davon ausgehen, dass jede Entität, einschließlich verteilter Nutzer, Geräte, Anwendungen und Daten, „nicht vertrauenswürdig" ist. • Können den Standort des Benutzers nicht annehmen, und müssen Benutzer unterstützen, die von überall aus arbeiten

Wie können Sie moderne Anforderungen erfüllen und gleichzeitig alle Traffic-Ströme bewältigen?

Anstatt für jeden Traffic-Pfad separate Lösungen zu verwenden, adressiert eine Connectivity Cloud die Netzwerkmodernisierung ganzheitlich.



Eingehender Traffic

Schützen Sie Netzwerke und Anwendungen vor DDoS und anderen Bedrohungen aus dem Internet

Ausgehender Traffic

Schützen Sie Benutzer und Niederlassungen vor Bedrohungen, setzen Sie einheitliche Richtlinien durch und kontrollieren Sie Daten in Anwendungen

WAN-Netzwerk

Verbinden und sichern Sie Büros, Benutzer, Geräte, Rechenzentren und Infrastruktur

Multicloud-Datenverkehr

Stellen Sie Netzwerkdienste bereit, um Apps in Public Cloud-/Hybrid Cloud-Umgebungen zu verbinden, zu sichern und zu erstellen

Die Connectivity Cloud von Cloudflare verwendet eine zusammensetzbare, programmierbare Architektur, um Ihren Benutzern Netzwerk- und Sicherheitsdienste bereitzustellen, und zwar in Ihrer Cloud-fähigen Geschäftsinfrastruktur und Ihren Anwendungen.

- Keine Notwendigkeit für den Ausbau oder die Erweiterung privater Rechenzentren
- Verwenden Sie cloudbasierte Netzwerk- und Sicherheitsdienste anstelle von Hardware-Appliances.
- Reduzieren Sie mit Zero Trust übermäßiges „Vertrauen" in das Netzwerk

Erfahren Sie mehr darüber, wie Sie mit Cloudflare die Netzwerkmodernisierung vereinfachen und beschleunigen können

Mehr dazu

1. Ali, Mohamad, und Jenkins, BJ., „Capturing the cybersecurity dividend." IBM, https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/unified-cybersecurity-platform. Letzter Zugriff am 26. Juni 2025.

2. „70% Of CEOs Say Their Network Is Slowing Business Growth, New NTT Study Finds." Business Wire, 20. Okt. 2022, https://www.businesswire.com/news/home/20221020005135/en/70-Of-CEOs-Say-Their-Network-Is-Slowing-Business-Growth-New-NTT-Study-Finds. Pressemitteilung.

© 2025 Cloudflare, Inc. Alle Rechte vorbehalten. CLOUDFLARE® und das Cloudflare-Logo sind Marken von Cloudflare. Bei allen weiteren Firmen- und Produktnamen und Logos kann es sich um Marken der jeweiligen Unternehmen handeln, mit denen sie verbunden sind.

+49 89 2555 2276 | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-7841.2025.JUL.31

CLOUDFLARE