

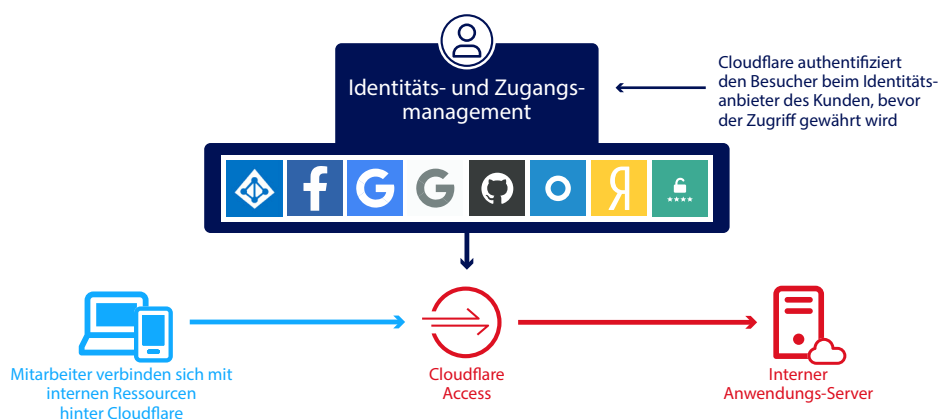


Cloudflare Access

Sicherer Anwendungszugriff ohne VPN

Die Absicherung interner Anwendungen über ein VPN ist teuer, potenziell unsicher und umständlich. Die VPN-basierte Zugriffskontrolle ist nicht granular und erfüllt nicht die Leistungsanforderungen mobiler Benutzer.

Cloudflare Access verbessert die Sicherheit, senkt die Kosten und schützt interne Ressourcen, indem es den Zugriff pro Benutzer und pro Anwendung sichert, authentifiziert und überwacht. Mit Cloudflare Access können nur authentifizierte Benutzer mit den erforderlichen Berechtigungen auf bestimmte Ressourcen zugreifen. Die Unterstützung bestehender Identitätsanbieter wie GSuite und Okta stellt sicher, dass die richtigen Benutzer unabhängig vom physischen Standort einfachen und sofortigen Zugriff haben.



Kontrolle des Benutzerzugriffs auf Anwendungen Durchsetzen des Zugriffs auf bestimmte Anwendungen auf einer Pro-Benutzer-Basis mit einfach zu erstellenden und zu verwaltenden Regeln Hinzufügen und Entfernen des Zugriffs auf Anwendungen ohne Hinzufügen einmaliger Gruppen oder Erstellen zusätzlicher Benutzerkonten. Einfaches Ändern der Zugriffsrichtlinien über das Dashboard oder die API.

Benutzerzugriff und Änderungsprotokolle überwachen Zeigen Sie Echtzeit-Zugriffsprotokolle im Dashboard an, und durchsuchen Sie sie, oder integrieren Sie SIEMGet von einem Drittanbieter. Sie erhalten einen vollständigen Überblick über: aktuelle Anmeldungen, Zugriffsanfragen und Richtlinienänderungen. Suchen Sie direkt im Dashboard nach Protokollen und erweitern Sie diese, um betroffene Benutzer, zugehörige IPs, Domänen, ergriffene Massnahmen und Zeitstempel anzuzeigen.

Zugriff auf die Infrastruktur ohne SSH-Schlüssel Statische SSH-Schlüssel auf lokalen Rechnern überflüssig machen. Zugriff auf bestimmte Rechner prüfen, auf anomales Verhalten überwachen und das Offboarding von Mitarbeitern automatisieren. Ersetzen der SSH-Schlüssel von Entwicklern durch kurzlebige Zertifikate.

Schnelle Anwendungen für Geräte an jedem beliebigen Ort bereitstellen Einfacher, sicherer und schneller Zugriff auf interne Anwendungen, unabhängig von Standort und Gerät des Benutzers. Das globale Netzwerk von Cloudflare beschleunigt Anwendungen und eliminiert gleichzeitig zusätzliche Latenzzeiten und die unnötigen Authentifizierungsschwierigkeiten von VPNs.

Schnelle Bereitstellen & Verwalten der Zugriffssteuerung Nutzung vorhandener Identitätsanbieter und Authentifizierung im globalen Cloudflare-Netzwerk. Die Verwaltung mehrerer oder gemeinsam genutzter Benutzerkonten für interne Ressourcen ist nicht mehr erforderlich. Unterstützte Identitätsanbieter gehören dazu: Google™, G Suite™, Github™, Okta™, Facebook™ und weitere.

Cloudflare Access

VPN vs. Cloudflare-Zugriff – Vergleich von Gesamtbetriebskosten und Leistungsmerkmalen

Wenn Sie Ihr VPN mit Cloudflare Access ersetzen, werden Ihre Support- und Sicherheitsteams vom Troubleshooting von unnötigen VPN-Problemen befreit. Darüber hinaus erhöhen sowohl Ihr Team als auch die Entwickler die Produktivität und Sicherheit beim Schutz und bei der Verbindung zu Anwendungen unabhängig vom Gerät.

Unterhalb finden Sie eine Übersicht über die jährlichen Kosten für den Besitz eines VPN im Vergleich zu Cloudflare Access und einen Funktionsvergleich.

	Einheit	Standard VPN	Cloudflare Access
Jährliche Gesamtbetriebskosten		pro Jahr	pro Jahr
Physische Geräte	2	CHF 10'900.-	CHF 0.-
Nutzungsgebühr	1000	CHF 43'600.-	CHF 50'500.-
Laufende Unterstützung	10 Stunden / Monat	CHF 1'800.-	CHF 0.-
Entwicklerzeit (25 Entwickler)	Minuten x CHF 45,52	CHF 102'400.-	CHF 28'700.-
Hinzufügen neuer Anwendungen	Minuten x CHF 45,52	CHF 24'600.-	CHF 1'100.-
Kosten für interne Kundenbetreuung	Minuten x CHF 45,52	CHF 163'900.-	CHF 32'800.-
Kosten des Teams für innere Sicherheit	Minuten x CHF 45,52	CHF 65'500.-	CHF 32'800.-
Total		CHF 412'700.-	CHF 145'900.-

Feature-Vergleich	Standard VPN	Cloudflare Access
Web & SSH-Unterstützung	✓	✓
Granulare Zugriffskontrolle für Anwendungen	✗	✓
Pfadbasierte Richtlinien	✗	✓
Zugriff auf Wildcard-Apps	✗	✓
Dynamischer Spalttunnelbau	✓	Nicht erforderlich
Zertifikat-Ansteckung	✓	✓
SAML 2.0 SSO	✓	✓
Erweitertes SAML 2.0	✓	✓
IdP-Unterstützung von Drittanbietern (Okta, G-Suite usw.)	✗	✓
Unterstützung mehrerer IdPs	✗	✓