# So ersetzt Cloudflare Access ein VPN

Viele Unternehmen waren auf die wachsende Beliebtheit von Remote-Arbeit nicht vorbereitet. Als sie in VPN-Lizenzen und Anwendungskapazitäten investierten, wollten sie damit oft nur einen Teil ihrer Mitarbeiter versorgen. Nun kommen diese Ressourcen an ihre Grenzen, weil die Menschen deutlich seltener im Büro arbeiten.

Cloudflare Access unterstützt Sie dabei, Ihr VPN durch einen modernen Authentifizierungsansatz für intern verwaltete Anwendungen zu entlasten. Access nutzt das globale Netzwerk von Cloudflare, um Web-Applikationen, SSH-Verbindungen, Remote Desktops und andere Protokolle zu schützen: Bei jeder Anfrage, die an eine Ressource gestellt wird, erfolgt eine Identitätsprüfung. Mit Access geschützte unternehmenseigene Tools erinnern an moderne SaaS-Anwendungen und der Login-Prozess für Mitarbeiter ist unkompliziert und einheitlich gestaltet.

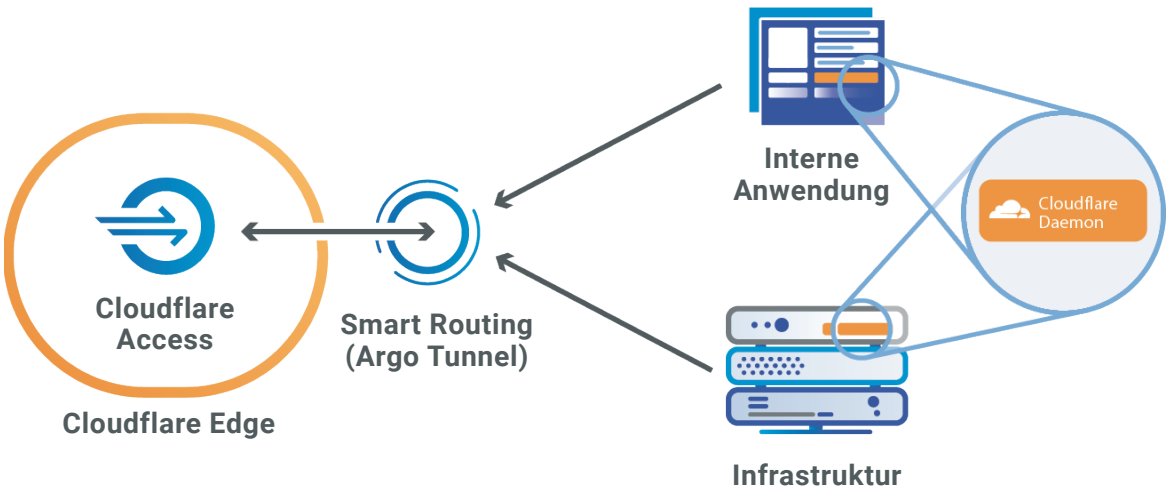
Wir verraten Ihnen, wie Access mithilfe des Netzwerks von Cloudflare ein VPN ersetzt.

## 1. Cloudflare Access verbindet interne Tools sicher mit dem Internet

In Ihrer Infrastruktur wird eine Argo Tunnel genannte sichere ausgehende Verbindung zwischen Teamressourcen und Access aufgebaut, um Anwendungen und Rechner mit Cloudflare zu verbinden. Argo Tunnel stellt Webserver in abgesicherter Form für das Internet bereit, ohne Firewall-Ports zu öffnen und ACLs zu konfigurieren.

Dieser Tunnel führt nur ausgehende Aufrufe des Cloudflare-Netzwerks durch.

Unabhängig davon, ob Anwendungen lokal ausgeführt oder bei einem Cloud-Anbieter gehostet werden, kann Argo Tunnel Ihre Infrastruktur mit Cloudflare verbinden.

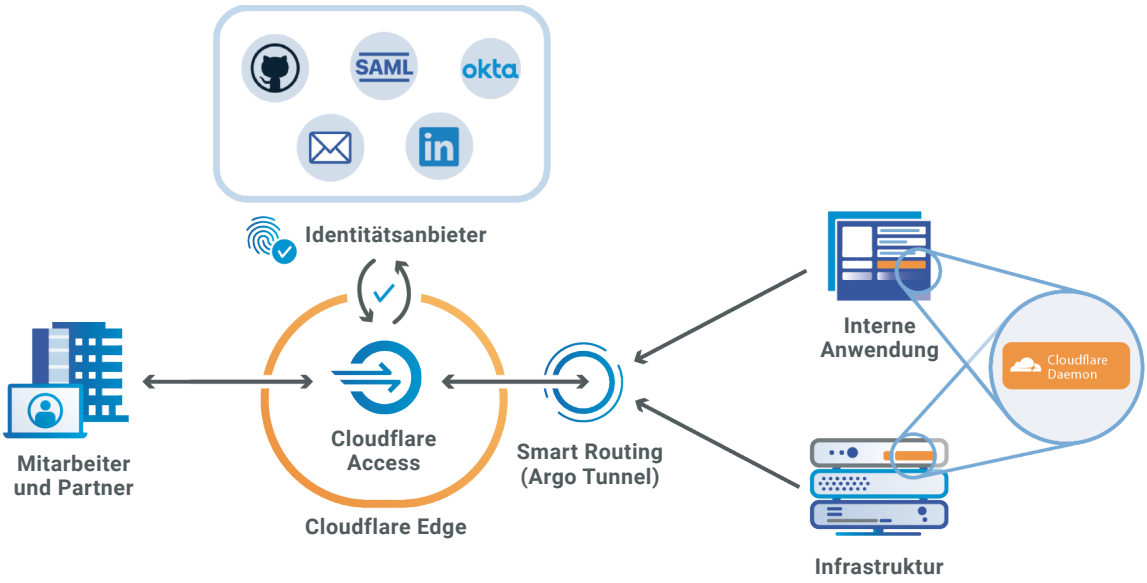


## 2. Anfragen an geschützte Ressourcen werden durch den Cloudflare-Edge geroutet

Argo Tunnel nutzt eine Technologie namens Argo Smart Routing; sie sorgt dafür, dass der Traffic innerhalb des Cloudflare-Netzwerks über den schnellsten Pfad zwischen dem Benutzer und den Rechenzentren, die Ihrem Ursprungsserver am nächsten liegen, geroutet wird.

99 % der Bevölkerung mit Internetanschluss in den Industrieländern sind maximal 100 Millisekunden vom nächsten Cloudflare-Rechenzentrum entfernt.

Wenn eine Anfrage an Ihre Ressource den Netzwerkrand von Cloudflare erreicht, fungiert Access als Hüter der Ressource, der entscheidet, welche Anfragen zugelassen werden.

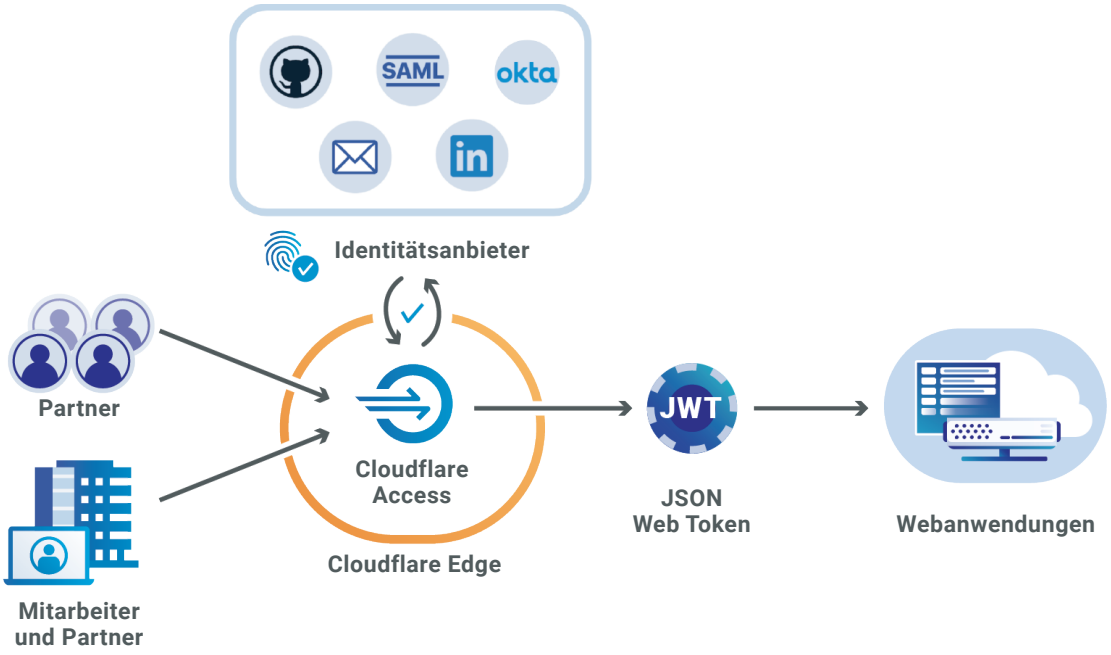


## 3. Am Cloudflare-Edge wendet Access die Richtlinien an, die bei Ihrem Identitätsanbieter (IDP) festgelegt wurden, um Anfragen zuzulassen oder zu blockieren

Dank der Einbindung des Identitätsanbieters Ihres Unternehmens in Cloudflare Access kann die Identität der Benutzer ermittelt werden. Wenn Nutzer eine Verbindung zu einer durch Access geschützten Anwendung herstellen, werden sie aufgefordert, sich über den konfigurierten Identitätsanbieter anzumelden.

Access unterstützt neben öffentlich verfügbaren Anbietern wie LinkedIn© und GitHub© auch Identitätslösungen, die von Ihrem Team verwaltet werden, wie Okta©, G Suite© und AzureAD©.

Mit Access können Sie mehrere Identitätsanbieter gleichzeitig und auch Mandanten gleichen Typs unterstützen.



## Was Access schützen kann

### SSH-Verbindungen

Mit dem SSH-Protokoll (Secure Shell) können Benutzer eine Verbindung zur Infrastruktur herstellen und beispielsweise Befehle über eine Remote-Verbindung ausführen lassen. Cloudflare Access kann Verbindungen über Secure Shell (SSH) absichern. Wenn Benutzer Ressourcen über Befehlszeilen erreichen wollen, öffnet Access ein Browserfenster, in dem sie aufgefordert werden, sich bei ihrem Identitätsanbieter anzumelden.

### Webanwendungen

Mit Access können Sie intern verwaltete Anwendungen wie Jira, WordPress, GitLab und SAP schützen, sodass Benutzer sich ohne VPN aus der Ferne anmelden und diese Ressourcen nutzen können. Cloudflare Access untersucht die Anfragen an Ihre Anwendung und stellt anhand der von Ihnen definierten Richtlinien fest, ob Besucher autorisiert sind.

### Remote Desktops

Mit dem Remote Desktop Protocol (RDP) können Nutzer von einem anderen Computer aus eine Verbindung zu einem Desktop herstellen. Mit Cloudflare Access können sich Endnutzer ohne VPN bei ihrem SSO-Anbieter (Single Sign-On) authentifizieren und über RDP eine Verbindung zu freigegebenen Dateien herstellen.

### Andere Protokolle

Mit Access können Sie auch für SMB-Filesharing (Secure Messaging Block) oder Anwendungen, die beliebiges TCP verwenden, eine Authentifizierung einrichten.

## Unterstützte Identitätsanbieter

Dank der Einbindung des Identitätsanbieters Ihres Unternehmens in Cloudflare Access kann die Identität der Benutzer ermittelt werden. Wenn Nutzer eine Verbindung zu einer durch Access geschützten Anwendung herstellen, werden sie aufgefordert, sich über den konfigurierten Identitätsanbieter anzumelden. Unternehmen können beliebig viele Identitätsanbieter gleichzeitig verwenden.

- GSuite©
- Okta©
- Microsoft Azure AD©
- Centrify©
- Yandex©
- Citrix ADC©
- Facebook©
- Generic OIDC©
- GitHub©
- Google©
- JumpCloud SAML©
- KeyCloak SAML©
- LinkedIn©
- PingIdentity©
- OneLogin (OIDC und SAML)©
- One Time Pin (OTP) Login©
- Atlassian© Jira und Confluence SSO
- Redash©

Registrieren Sie sich noch heute für Access unter teams.cloudflare.com