Cloudflare Zero Trust Network Access with Private Routing

Prevent lateral movement and reduce VPN reliance.

Trusting network-based controls (like VPNs and IP location restriction) for application access can increase your attack surface, limit visibility and frustrate end users. Cloudflare's Zero Trust Network Access works with your identity providers and endpoint protection platforms to enforce default-deny, Zero Trust rules that limit access to corporate applications, internal IP spaces and hostnames. Powered by Cloudflare's vast and performant Anycast network, it makes user connections faster than a VPN.

Cloudflare and Rackspace Technology | Better Together

Rackspace Technology has been helping organizations like yours strengthen security for over 20 years. Our multicloud security experts have deep knowledge and experience in both IT and cloud security. We hold 800+ security-industry certifications, including 150+ technical certifications across leading technologies. Our partnership with Cloudflare helps to drive efficiencies in all processes and automation to Cloudflare-specific technologies, like Zero Trust.

Key Benefits of Cloudflare Zero Trust Network Access

- **Protect any application:** Cloudflare is both identify and application agnostic, allowing you to protect any application, SaaS, cloud or on-premises setup with your preferred identity provider.
- **Connect users flexibly, with or without a client**: Facilitate web app and SSH connections without the need for client software or end use configurations. For non-web applications, RDP connections and privet routing, utilize one comprehensive client across Internet- and application-access use cases.
- **Enable identity federation across multiple identity providers:** Integrate all your corporate identity providers (Okta, Azure AD, and more) for safer migrations, acquisitions and third-party user access. Enable one-time pins for temporary access or incorporate social identity sources like LinkedIn and GitHub.
- **Restrict lateral movement between corporate resources:** Apply strong, consistent authentication methods to legacy applications with IP firewall and Zero Trust rules.
- **Enforce device-aware access:** Before you grant access to a resource, evaluate device posture including presence of Gateway client, serial number and mTLS certificate, ensuring only safe, known devices can connect to your resources. Integrate device posture from Endpoint Protection Platform (EPP) providers.

rackspace technology®

Why Rackspace Technology?

Rackspace Technology is your trusted partner across cloud, applications, security, data and infrastructure.

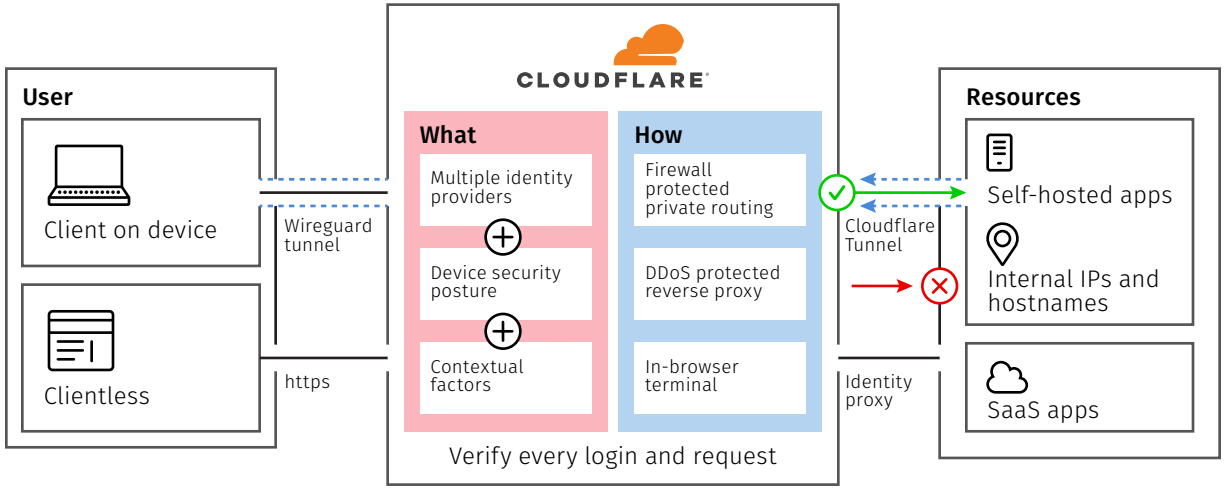
- 2,600+ certified experts
- Hosting provider for more than half of the Fortune 100
- 20+ years of hosting experience
- Customers in 120+ countries
- HITRUST CSF-certified dedicated hosting environment
- Certified Level 1 PCI Service Provider on AWS
- 1,300+ AWS technical certificates worldwide
- AWS Security Hub Partner
- AWS Perimeter Protection MSSP Provider
- Microsoft Azure Gold Competency: Security
- Google Cloud Platform Security Specialization
- IDC- and Forrester-recognized security practices
- 800+ security certifications, including 100+ cloud security certificates from AWS, Microsoft Azure, and Google Cloud Platform

*Initial response is sent via automated alert and SLAs are based on event severity

- **Log user activity across any app:** Log any request made in your protected applications – not just log in and log out. Aggregate activity logs in Cloudflare or export them to your SIEM provider.

Cloudflare integrates with several Identify and access management (IAM) integrations and endpoint protection platform (EPP) integration providers.

How it Works



Instead of a VPN, users connect to corporate resources through a client or a web browser. As requests are routed and accelerated through Cloudflare's edge, they are evaluated against Zero Trust rules incorporating signals from your identity providers, devices and other context. Before, RDP software, SMB file viewers and other thick client programs used to require a VPN for private network connectivity. Now, teams can privately route any TCP or UDP traffic through Cloudflare's network where it's accelerated, verified and filtered in a single pass, facilitating improved performance and security.

Additional Services

The Rackspace Elastic Engineering for Security service provides on-demand access to a pod of security experts to help businesses customize, optimize and manage their comprehensive Cloudflare platform, including leveraging Cloudflare Zero Trust for a modernized SASE architecture that can scale rapidly with your strategic cloud initiatives.

Take the next step

Learn more: www.rackspace.com/lp/cloudflare-zero-trust-ebook
Call: 1-800-961-2888

rackspace technology.

The Cloudflare Difference

Unbeatable performance

Routes requests faster with optimized, intelligence-driven routing across Cloudflare's Anycast network. On average, web apps are accessed 30% faster and TCP connections see a 17% decrease in round-trip time. Our intelligence is based on analyzing network data from 25M HTTP requests/second and 39K new TCP connections/second.

Simpler management

Combines Zero Trust Network Access, Secure Web Gateway, Remote Browser Isolation and more into a single control plane with an admin experience built from the ground up, not acquired and stitched together from multiple vendors.

Single-pass inspection

Verifies, filters, isolates and inspects traffic speedily and consistently across the globe, because every Cloudflare service is deployed on every data center in our 250+ locations worldwide.