

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, private IP spaces and hostnames. Powered by Cloudflare's vast and performant Anycast network, it makes user connections faster than a VPN.

Since deploying Zero Trust Network Access internally, Cloudflare has seen the following benefits:

- 91% reduction in attack surface¹
- 2x cost savings from reduced IT efforts
- 80% reduced time spent servicing VPN related tickets
- 70% reduction in ticket volume
- 300+ annual hours of unlocked productivity during new employee onboarding

What you can do with Access

Protect any application

Cloudflare is both identity and application agnostic, allowing you to protect any application, SaaS, cloud, or on-premises with your preferred identity provider.

Connect users flexibly, with or without a client

Facilitate web app and SSH connections with no client software or end user configuration required. For non-web applications, RDP connections, and private routing, utilize one comprehensive client across Internet and application access use cases.

Enable identity federation across multiple identity providers

Integrate all of 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 even 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 including CrowdStrike, Carbon Black, Sentinel One, and Tanium.

Log user activity across any app

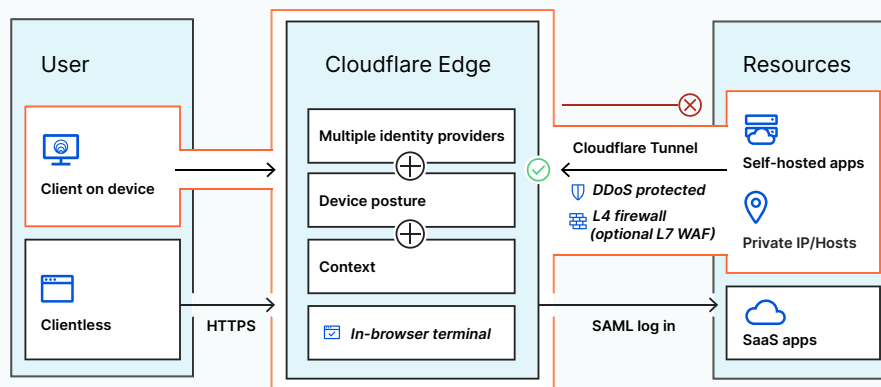
Log any request made in your protected applications - not just login and log out. Aggregate activity logs in Cloudflare, or export them to your SIEM provider.

¹When Zero Trust Network Access is combined with Internet Browsing

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 one 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 200+ locations worldwide.

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. Where RDP software, SMB file viewers, and other thick client programs used to require a VPN for private network connectivity, teams can now privately route any TCP traffic through Cloudflare’s network where it’s accelerated, verified, and filtered in a single pass, facilitating improved performance and security.

“Cloudflare Access saved us from having to develop our own Identity and Access Management (IAM) system. We don’t have to build user permission functions into the apps that Access protects. We went all in; everyone in the company has a seat.”

Jim Tyrell
Head of Infrastructure, Canva



“At delivery Hero, we always strive to deliver an amazing experience to our customers. Cloudflare Access helps us do the same for our internal teams: offering them a secure working environment, and removing the need for a VPN to access all of our applications across the globe.”

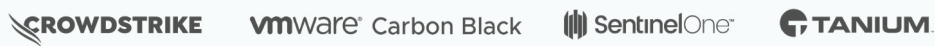
William Carminato
Senior Director, Engineering, Delivery Hero

Delivery Hero


Identity and access management (IAM) integrations





Endpoint protection platform (EPP) integrations





Key Features

|  Consistent policy | |
|--|------------------|
| Custom application, private network, and Internet access policies | Unlimited |
| Authentication via enterprise and social IdPs | ✓ |
| Device posture using third-party integrations and Cloudflare | ✓ |
| CSV-based bulk import for corporate device serial number lists | ✓ |

|  Increase visibility | |
|--|-----------------|
| Activity log retention | 6 months |
| Identity-based country, state, and device detail views | ✓ |
| Push logs to cloud storage or SIEMs | ✓ |

|  Secure connectivity | |
|--|-------------------------------|
| Client-based encrypted connections to the Internet (WARP client) | Win, Mac, iOS, Android |
| Clientless secure access to self-hosted and SaaS applications | ✓ |
| Private connections for self-hosted applications, IPs, and hostnames (Cloudflare Tunnel) | ✓ |

|  Simple interoperability | |
|--|---|
| Endpoint and mobility management integrations | ✓ |
| Split-tunneling for local or VPN connectivity | ✓ |
| Client self-enrollment for unmanaged devices | ✓ |
| Customizable app launcher | ✓ |
| Authentication supports multiple identity providers concurrently | ✓ |
| Generic and custom connectors to support SAML and OIDC | ✓ |
| Token-based authentication for automated services | ✓ |
| Certificate-based auth for IoT and other mTLS use cases | ✓ |

|  No performance sacrifices | |
|--|---------------|
| Uptime SLA | 100% |
| Fastest, global edge network (200+ PoPs) | ✓ |
| Fastest, global policy updates (<500ms) | ✓ |
| Fastest, intelligent IP routing (<100ms) | ✓ |
| Fastest, secure remote browser (2x speed of others) | Add on |

Interested in learning more? Visit cloudflare.com/teams/access to start an account, free for up to 50 users.