The Zero Trust guide to developer access

Unburden technical teams with safer, faster access to critical tools and infrastructure

Engineers need privileged access to infrastructure to keep your business moving, and they don't like to be slowed down. ZTNAs allow privileged technical users to access your critical infrastructure from anywhere, without the performance tradeoffs of corporate VPNs. Learn how Zero Trust security can empower your technical teams to work faster, while strengthening the security of your build environment.

In a recent Forrester study commissioned by Cloudflare, 83% of security decision makers plan to focus on enabling faster and safer developer access this year.[1]

3 ways to accelerate technical teams with Zero Trust access

Protect build environments

Connect developers to applications without exposing them to the public Internet. Utilize secure tunnelling software to create a private tunnel to Cloudflare's network, and use our policy engine to enforce multifactor authentication policies.

Reduce VPN reliance

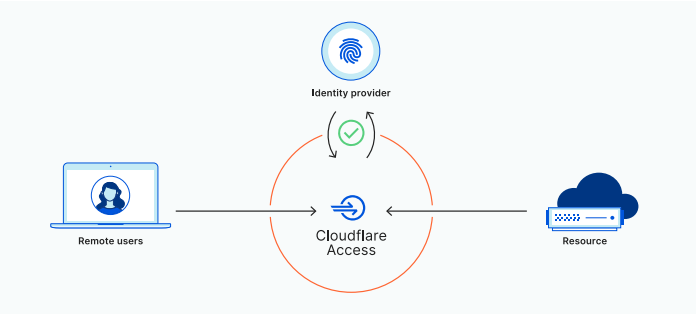
Connecting to infrastructure over a VPN tunnel can add latency, especially for globally distributed teams. Users experience lightning fast performance when they connect to your tools through one of Cloudflare's data centers in 250+ locations around the world.

Log everything

Log any request made in your protected applications — not just entrances and exits. Aggregate activity logs in Cloudflare, or export them to your SIEM provider for analysis.

How it works

Cloudflare's global edge network is in 250+ locations around the world; always close to your users and to the applications they need. With Cloudflare Access in front of your infrastructure, VPN tunnels and backhauling are no longer needed. Developers get fast, reliable performance, wherever they are.



What you can protect with Cloudflare Access

SSH Connections

Secure Shell (SSH) protocol allows users to connect to infrastructure to perform activities like remote command execution. Cloudflare Access can secure connections over Secure Shell (SSH). When users attempt to reach resources from command lines, Access launches a browser window prompting them to login with their identity provider.

Web and SaaS Applications

Use Cloudflare Access to protect internally-managed applications like Jira, WordPress, GitLab, so users can login to access them without a VPN. Cloudflare Access evaluates requests to your application and determines whether visitors are authorized based on policies you define.

Remote Desktops

The Remote Desktop Protocol (RDP) allows users to connect to a desktop from a different machine. Cloudflare Access lets end users authenticate with their single sign-on (SSO) provider and connect to shared files over RDP without being on a VPN.

Other Protocols

You can use Cloudflare Access to add authentication to Server Message Block (SMB) file shares or applications that use arbitrary TCP or UDP.

Interested in learning more?
Visit cloudflare.com/products/zero-trust/access

1. Forrester Opportunity Snapshot: Zero Trust, October 2020

"Discord is where the world builds relationships. Cloudflare helps us deliver on that mission, connecting our internal engineering team to the tools they need. With Cloudflare, we can rest easy knowing every request to our critical apps is evaluated for identity and context — a true Zero Trust approach"

Mark Smith
Director of Infrastructure at Discord

DISCORD

"OneTrust relies on Cloudflare to maintain our network perimeter, so we can focus on delivering technology that helps our customers be more trusted. With Cloudflare, we can easily build context-aware Zero Trust policies for secure access to our developer tools. Employees can connect to the tools they need so simply teams don't even know Cloudflare is powering the backend. It just works."

Blake Brannon
CTO of OneTrust

OneTrust