

# Cloudflare Access

Zero Trust Network Access (ZTNA) verifies context like identity and device posture to secure access across your entire environment — no VPN required.

## Modernize remote access

### Fast, reliable Zero Trust Network Access

Distributed work environments call for a distributed approach to security. The “perimeter” no longer exists, and traditional remote access solutions like VPNs cannot meet modern security or performance expectations.

Cloudflare’s [ZTNA](#) service provides simple, secure access between any user and resource, on any device, in any location by continually checking granular context, such as identity and device posture for each request. With a cloud-native approach, there is no longer a “balancing act” between security and user experience. ZTNA enables your business with seamless access to apps and infrastructure, while protecting data.

It also helps organizations stay agile and navigate change more easily, whether it be onboarding new contractors or unmanaged devices or navigating access throughout a cloud migration or merger and acquisition (M&A) activity. Cloudflare can become the heart of an organization’s Zero Trust or security modernization strategy, delivering ZTNA on our global, programmable [connectivity cloud](#).



“Cloudflare simplifies how we deliver Zero Trust across our organization — that helps us mitigate risk more effectively with less effort.”

**Anthony Moisant**  
SVP, CIO & CISO



## Empower your business with modernized access



### Strengthen user experience

Improve team productivity with modernized security that makes on-prem apps feel just like SaaS apps. No more slow, clunky VPNs or employee complaints.



### Eliminate lateral movement

Reduce cyber risk and shrink your attack surface by granting context-based, least privilege access per resource — rather than network-level access.



### Scale Zero Trust effortlessly

Improve tech efficiency by protecting high-risk apps or user groups, then expanding Internet-native ZTNA to protect your entire organization.

## Top use cases for Access

### Adopt Zero Trust and secure hybrid work

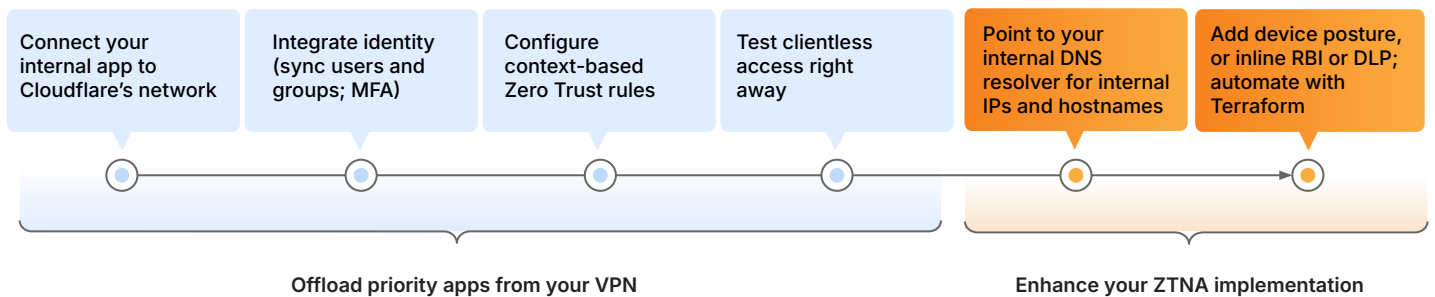
- ★ **VPN augmentation and replacement** — Access is faster and safer than traditional VPNs. Start [offloading](#) critical users and apps for better security and end user experience.
- ★ **Contractor/BYOD access** — Authorize [third-party users](#) or employees on personal machines with browser-based access options.
- **Infrastructure access** — Provide [privileged access](#) to sensitive infrastructure, without disrupting developer workflows.

### Enable digital modernization

- **Accelerate M&A** — Avoid a traditional network merge entirely. Integrate with multiple identity providers and provide per-app internal access during M&A.
- **Support cloud migrations** — Provide access continuity during app modernization projects by using ZTNA on both sides of a migration.
- **Secure DevOps workflows** — Protect service-to-service workflows with mesh/P2P connectivity, supporting bidirectional traffic.

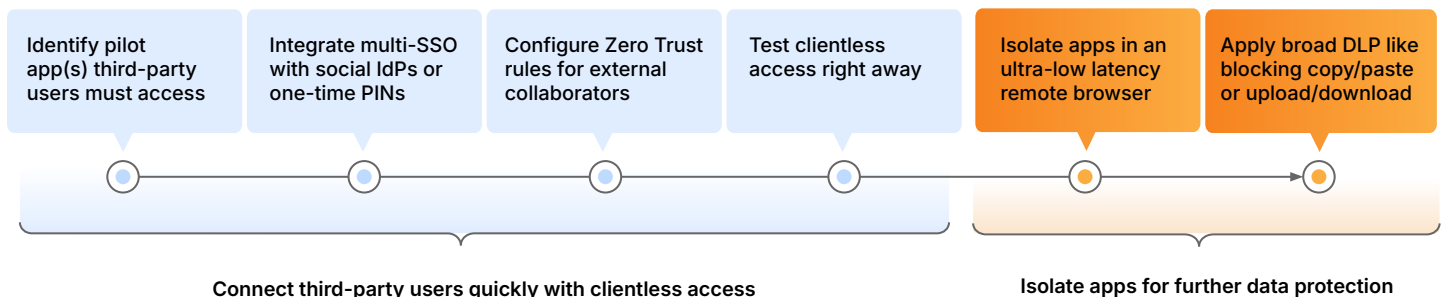
### Getting started with VPN augmentation and replacement

Prioritize critical apps or risky users for a ZTNA pilot to augment your VPN. Use clientless access to web apps to help expedite testing. Gradually move toward full VPN replacement over time, and adopt additional inline services to enhance your [SSE](#) or [SASE](#) deployment with more contextual signals or data controls.



### Getting started with contractor/BYOD access

Provide least privilege access to third-party users or unmanaged devices, while mitigating risks of lateral movement or data exfiltration. Configure simple authentication options for contractors — no end user software required. Apply data controls within an isolated browser to enhance your implementation.



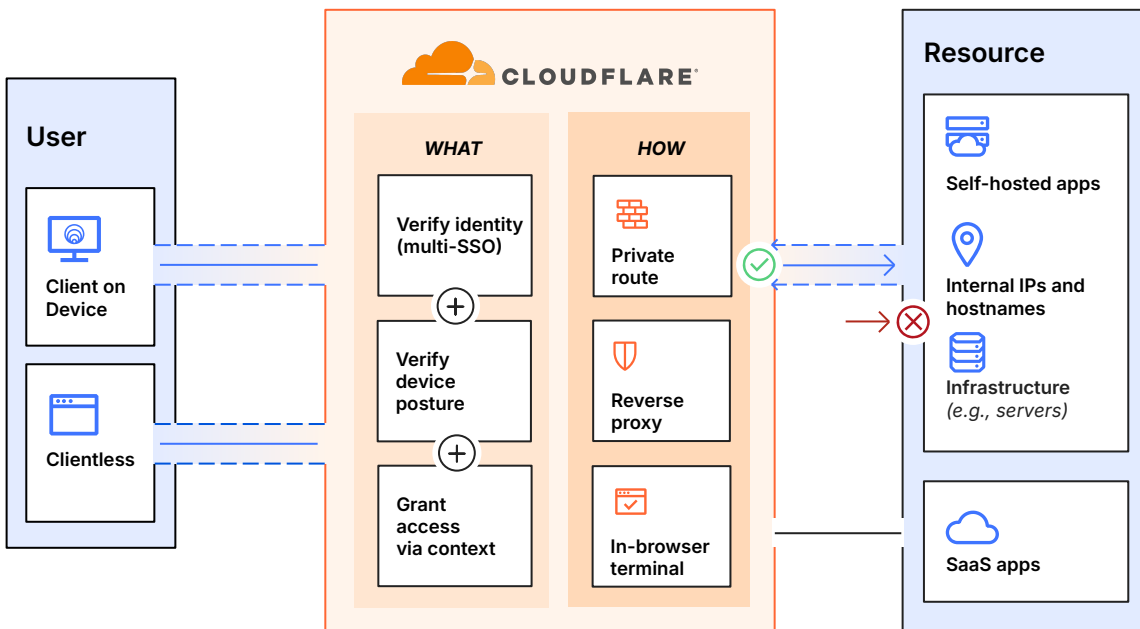
## How Access works

Simplify and secure access to all of your organization's resources individually, creating a software-defined perimeter using [Cloudflare Access](#). Our ZTNA service is a flexible aggregation layer that continuously verifies granular context, such as identity and device posture. When a user authenticates and meets all access policy criteria, Access issues a signed JSON Web Token (JWT) valid for a specified session duration. We perform single-pass inspection on all user requests through our composable [SASE platform](#), and our centralized policy administration experience applies policy changes globally in seconds.

Unified clientless and client-based operation handles all device types. We use one device client across our platform that encrypts traffic to our network to maintain the privacy of our customers' data. We also provide simple, secure access to devices outside the enterprise through our clientless setup. Our ZTNA, [DNS](#), and leading [WAF](#) and [DDoS](#) protection services work together to create and secure public hostnames accessible to third-party users and a hybrid workforce on any device. Our userless authentication options (tokens or mTLS certificates) also address automated service and IoT device use cases.

For Zero Trust controls, resources use public hostnames for reverse proxy to self-hosted apps (cloud/on-prem) or browser-based [SSH/RDP](#), identity proxy to SaaS apps, or client/tunnel-based private routing via L4-7 forward proxy to any web or non-web (e.g., [infrastructure target](#) or arbitrary TCP/UDP) resource within a private subnet. Our global network and app connector software combined support any compute environment—public cloud, including Kubernetes and containers or legacy on-prem network resources—without requiring virtual machine infrastructure and without throughput limitations.

Stay agile and build alongside the tools admins already use. Third-party identity, endpoint, network on-ramp, logging/analytics, and SIEM tools are integrated onto Cloudflare's unified dashboard, with native options also provided for our device client and analytics.



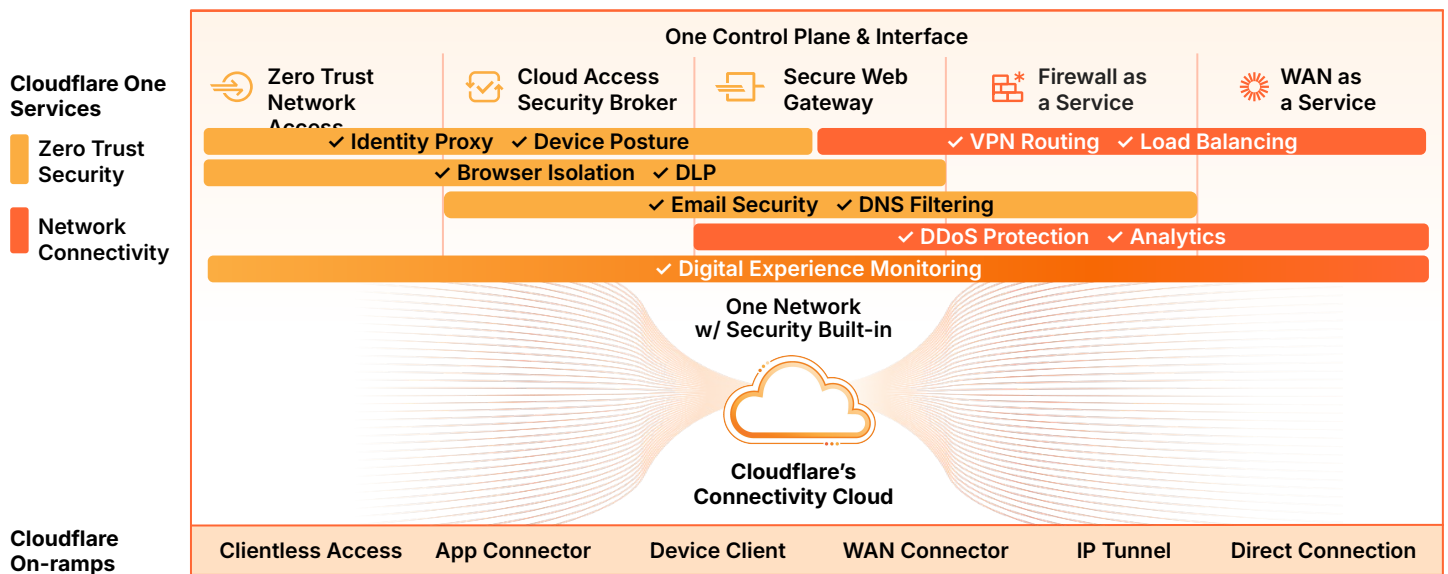
## Access as part of Cloudflare's SSE and SASE platform

SSE and SASE is often a multi-year strategic journey; however, organizations frequently start with ZTNA to quickly demonstrate cross-functional business value. Organizations seeking to secure hybrid work, defend against threats, and protect their data on their path to consolidation, increasingly choose Cloudflare as their trusted partner — whether they are just getting started with modernizing remote access, or getting a stalled Zero Trust project back on track.

Cloudflare's deployment flexibility and composable architecture enable any organization to protect and accelerate the performance of devices, apps, and entire networks to keep hybrid work secure and productive. For this, we support clientless onboarding for end users, clientless web isolation to contain suspicious traffic, and a unified management dashboard that provides visibility into all security and network services, regardless of where admins or users are connecting from. The breadth of Cloudflare's global network enables security to be enforced closer to end users, minimizing latency and providing a better employee experience. Our resilient Anycast architecture helps route around Internet disruptions, keeping teams online and helping ensure service continuity.

Bolster your security posture with simplified implementation and policy maintenance. Shared context between our ZTNA, CASB, DLP, and SWG policies provides consistent admin workflows; the same identity and device posture attributes can inform policy decisions across all services.

ZTNA, RBI, and email security can also be used together to provide conditional access to resources while insulating users from malicious content (links, attachments) across email and collaboration tools. Third-party contractors or employees on personal devices can be provided least privilege access to isolated corporate resources with browser-based data controls (e.g., DLP policies or broad controls like disable upload/download, copy/paste, keyboard input).



## You're in good company



Cloudflare is named a Customers' Choice in the 2024 [Gartner® Peer Insights™](#) Voice of the Customer: Zero Trust Network Access<sup>1</sup>




**100K+**  
hybrid workers'  
Internet and application  
access secured.

Fortune 500  
[Read case study](#)



**44K**  
global workers protected  
and replaced VPN for hybrid  
workforce with Zero Trust.

E-commerce  
[Read case study](#)



**3 months**  
to replace VPN  
for 13,000 employees and  
2,000 contractors.

#1 job website  
[Read case study](#)

**THG 1 week**  
to migrate policies  
and replace Zscaler for 7K+  
workers to simplify  
operations.

E-commerce  
[Read case study](#)

"Cloudflare Access became available just in time to prevent us from having to go through the hassle of deploying a VPN. It was an easy choice for us, and it was shockingly simple to deploy."

Conor Sherman  
Head of Security



"Before we implemented Cloudflare, preparing an application for safe deployment was a two-to four-week project. With Cloudflare Zero Trust, we save almost 90% of that time."

Ricardo Girardelli  
Network Engineering Team Lead



## Access capabilities

Creating/editing Zero Trust policies for secure access	
<b>Granular, custom access policies</b>	Unified app definition enables consistent <a href="#">policy administration</a> experience. Web apps are secured at a <a href="#">subdomain and path level</a> with <a href="#">wildcard</a> and multi-hostname support, and support <a href="#">CORS requests</a> . Policy changes apply globally in seconds. Includes <a href="#">policy tester</a> .
<b>Breadth of resources:</b> What we can protect and how	Resources use public hostnames for reverse proxy to <a href="#">self-hosted apps</a> (cloud/on-prem) or browser-based SSH/RDP, identity proxy to <a href="#">SaaS apps</a> , or client/tunnel-based private routing via L4-7 forward proxy to any web / non-web (e.g., <a href="#">infrastructure target</a> or arbitrary <a href="#">TCP/UDP</a> ) resource within a <a href="#">private subnet</a> . Also supports resources/workflows with <a href="#">bidirectional traffic</a> (e.g., VoIP/SIP or CI/CD pipeline).
<b>Identity</b>	Authenticate via all major enterprise and social <a href="#">identity providers</a> (IdPs), including multiple IdPs concurrently. Can also use generic <a href="#">SAML</a> and <a href="#">OIDC</a> connectors. Supports (and can <a href="#">enforce</a> ) any IdP-provided AuthN method, <a href="#">temporary AuthN</a> , <a href="#">purpose justification</a> , re-AuthN intervals on global or per-app/policy <a href="#">session</a> basis, and immediate session <a href="#">revoke</a> option per-app or per-user. Can use <a href="#">device client (WARP) as AuthN method</a> (cached identity per WARP session).
<b>Device posture</b>	Verify <a href="#">device posture</a> using device client and third-party endpoint protection provider (EPP) integrations. Use service-to-service <a href="#">integrations</a> (or <a href="#">custom</a> integration to any API) to pull EPP risk scores into Zero Trust policies.
<b>Contextual signals for policies</b>	Configure <a href="#">signals</a> like email group, IP ranges, geolocation, login method (e.g., MFA type, IdP type), valid mTLS or SSH certificate, service token, serial # list, device posture attributes, device client installed, session duration, SWG rule enforcement, or signals from <a href="#">external API calls</a> . Can also reference <a href="#">Microsoft Entra ID conditional access</a> authentication contexts directly.
<b>Other related support</b>	<ul style="list-style-type: none"> <li>• <b>SCIM:</b> Automatically provision/deprovision users to sync changes across all IdPs</li> <li>• <b>Internal DNS:</b> Configure <a href="#">local domain fallback</a> and resolve private network requests</li> <li>• <b>Split tunnels:</b> <a href="#">include/exclude IPs</a> for private networking or running alongside a VPN</li> <li>• <b>mTLS authentication:</b> <a href="#">Certificate-based</a> authentication for IoT and other mTLS use cases</li> <li>• <b>App isolation:</b> With a single checkbox, <a href="#">isolate apps</a> in a lightning-fast remote browser*</li> </ul>
On- and off-ramps	
<b>App connector</b>	<a href="#">Simple orchestration</a> of lightweight app connector ( <a href="#">Cloudflare Tunnel</a> ) expedites connecting resources to Cloudflare, without requiring VM infrastructure and without throughput limitations. Includes <a href="#">monitoring</a> , <a href="#">virtual networks</a> (for IP overlaps), and <a href="#">redundancy and failover</a> capabilities.
<b>Device client:</b> When to use	<ul style="list-style-type: none"> <li>• <b>Clientless:</b> Extend Zero Trust policies to third-party users on <a href="#">unmanaged devices</a>; also pairs with <a href="#">clientless RBI</a> to enforce data controls (eg. block up/download, copy/paste) and L7 <a href="#">DLP policies</a>* through the browser. Supports web apps and browser-based SSH, RDP, and VNC.</li> <li>• <b>Client-based:</b> Our device client (<a href="#">WARP</a>) extends secure access to private networks, enables service-to-service device posture integrations, and is <a href="#">location-aware</a> to apply tailored policies for office users. Supports <a href="#">multi-user</a> mode on Windows devices, and uses <a href="#">MASQUE protocol</a> for better captive portal handling. Can connect any two or more devices running WARP to <a href="#">create private networks</a>. Users can <a href="#">self-enroll</a> or can deploy via <a href="#">MDM</a>.</li> </ul>
Extensibility and visibility	
<b>Page customization</b>	Upload custom HTML for block and app launcher screens to fit your branding or convey specific access instructions to streamline the end user experience.
<b>Logging</b>	<a href="#">Comprehensive logging</a> across authN events and requests to protected URI paths / infrastructure targets. Includes <a href="#">SSH</a> logs. Can use <a href="#">logpush</a> or API to integrate with existing SIEM, orchestration, and analysis tools. <a href="#">Shadow IT</a> discovery provides visibility across both sanctioned and unsanctioned SaaS apps and private network origins.
<b>Automation</b>	<a href="#">Intuitive APIs</a> and <a href="#">Terraform provider</a> available to programmatically manage all aspects of a Zero Trust implementation. Can use <a href="#">service tokens</a> for userless, automated systems.

\*using capabilities across other parts of the SSE / SASE platform

## Why Cloudflare?



### Faster and simpler to deploy

Get started with ZTNA quickly, simplify day-to-day management, and scale easily across locations with flexible on-ramps and a unified dashboard and API.



### Better global end-user experience

Ensure fast and consistent policy enforcement close to end users due to Cloudflare's massive scale and Anycast network architecture with built-in resilience.



### Agile architecture for the future

Simplify your long-term modernization plan with one unified network and control plane of composable, cloud-native services designed to work together.

Let's discuss simple, secure access for your organization

Request a workshop



Not quite ready for a live conversation?

Keep learning more in our [SASE reference architecture](#), or see how it works in an [interactive tour of our Zero Trust platform](#).



1. Gartner, Voice of the Customer for Zero Trust Network Access, 30 January 2024, Peer Contributors. GARTNER, PEER INSIGHTS and The Gartner Peer Insights Customers' Choice badge are trademarks of Gartner, Inc., and/or its affiliates, and are used herein with permission. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.