Zero Trust Network Access

Cloudflare Zero Trust, specifically Access, improves team productivity and reduces risk as all users access your self-hosted, SaaS, or non-web apps—without a VPN.

Simple, secure access for hybrid work

Internet-native Zero Trust Network Access (ZTNA)

Today's distributed work environment calls for a distributed approach to security. The "perimeter" no longer exists, and traditional remote access solutions like VPNs can't meet modern security or performance expectations.

ZTNA provides simple, secure access between any user and app, on any device, in any location by continually checking granular context like identity and device posture on a resource by resource basis. With an entirely new approach, there is no longer a "balancing act" between security and user experience. ZTNA enables your business by improving both.

It also makes organizations more agile and better able to navigate change, whether it be cloud migration, M&A activity, or innovating and scaling quickly. Cloudflare is the heart of a Zero Trust or security modernization strategy, delivering ZTNA on our programmable, global network.

80% Average time reduced spent resolving remote access support tickets related to using a VPN[1]

72% Saved ongoing time for monthly policy configuration compared to their prior vendor[1]

68% Saw significant impact for streamlining authentication experiences for employees and contractors[1]

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 critical apps or highest risk user groups, then expanding Internet-native ZTNA to protect your entire business.

Top use cases for Access

Secure hybrid work

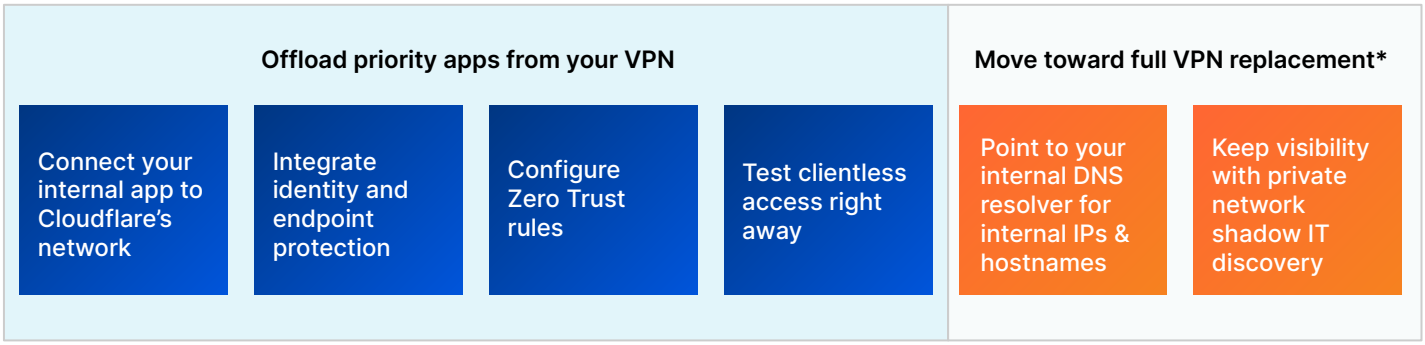
- ★ **VPN augmentation & replacement** — Access is faster and safer than traditional VPNs. Start offloading critical apps for better security and end user experience.
- ★ **Contractor access** — Authenticate third-party users like contractors with clientless options, social IdPs, and more.
- **Developer access** — Provide privileged technical users secure access to critical infrastructure without performance tradeoffs.

Empower business transformation

- **Accelerate mergers & acquisitions** — Avoid a traditional network merge entirely. Integrate with multiple IdPs and provide per-app internal access during M&A.
- **Cloud migration** — Maintain business continuity during times of transformation, like migrating apps or identity directories to the cloud.
- **Phishing-resistant MFA** — Roll out strong authentication, like FIDO2-compliant security keys, everywhere.

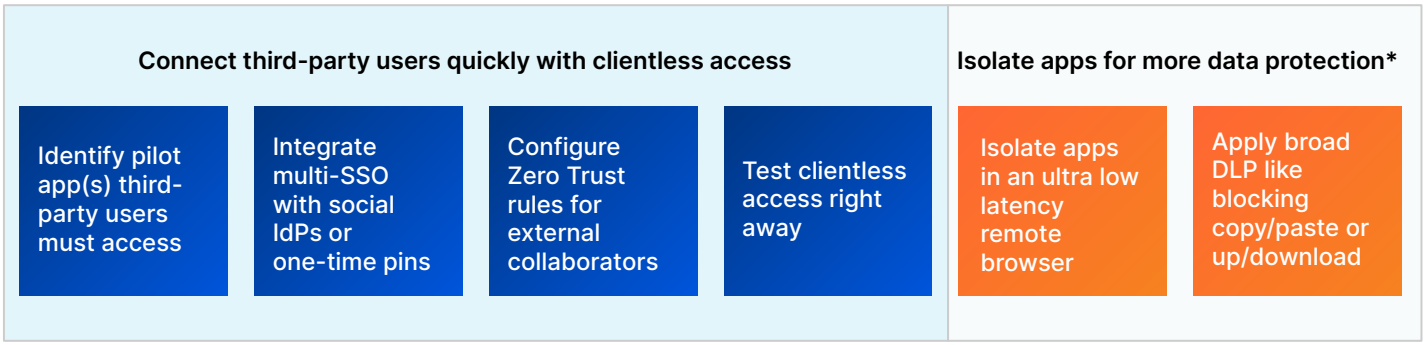
Getting started with VPN augmentation & replacement

Prioritize critical apps or risky users for a ZTNA pilot to augment your VPN. Use clientless access for web apps or in-browser SSH to expedite testing. Adopt advanced capabilities over time to move toward full VPN replacement and maintain dynamic visibility as your network shifts.



Getting started with contractor (third-party) access

Provide smooth user experiences while mitigating risk from unmanaged devices. Configure simple authentication options for contractors — no end user software required. Adopt advanced capabilities over time to apply further data protection.



**using capabilities across other parts of the Zero Trust platform*

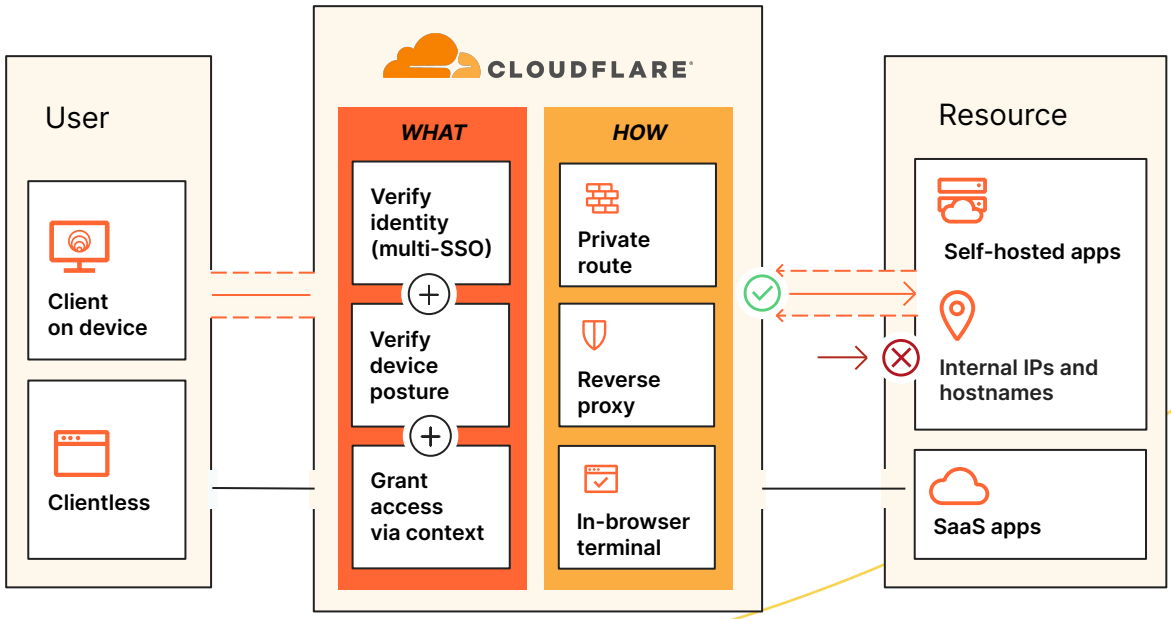
How Access works

Cloudflare Access is a flexible aggregation layer that continuously verifies granular context like identity and device posture to provide simple, secure access to all of an organization's resources individually, creating a software-defined perimeter. When a user authenticates and meets all access policy criteria, Access issues a signed JSON Web Token valid for a specified session duration. We perform single-pass inspection on all user requests through our composable platform, and our centralized policy administration experience profilerates policy changes globally in seconds due to our unique Anycast network architecture.

Unified clientless and client-based operation handles all device types. We use one device client for all Zero Trust services 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, & market-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 in-browser SSH/VNC, identity proxy to SaaS apps, or client/tunnel-based private routing via L4-7 forward proxy to any web or non-web (e.g., 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 VM infrastructure and without throughput limitations unlike other Zero Trust vendors.

Third-party identity, endpoint, network on-ramp, logging/analytics, and SIEM tools are integrated into our dashboard alongside native options for our device client and analytics, enabling admins to stay agile and build alongside the tools they already use.



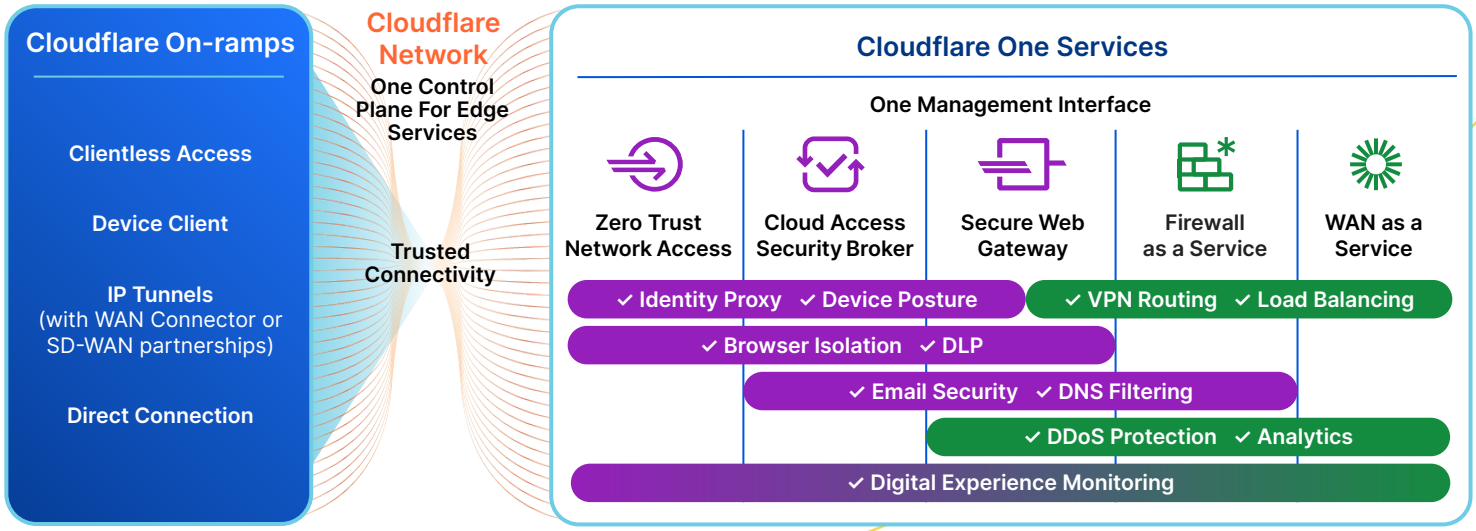
Access as part of Cloudflare's SSE and SASE platform

While SSE and SASE often involve a multi-year strategic journey, Cloudflare frequently sees organizations starting with ZTNA because it involves actionable and approachable steps for IT teams while demonstrating significant short-term business value. IT leaders seek to secure hybrid work, defend against threats, and protect their data on their path to consolidation, and they're increasingly choosing Cloudflare as their trusted partner.

Cloudflare's deployment flexibility and composable architecture enables 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 agentless onboarding for end users, clientless web isolation to contain unsecure traffic, and a unified management dashboard that allows 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 slick employee experience. Our Anycast architecture helps route around Internet disruptions, keeping teams online and helping ensure business continuity.

With our unified SSE and SASE platform, shared context between our ZTNA, CASB, DLP, and SWG policies helps bolster security posture while simplifying implementation through a consistent admin workflow. The same identity and device posture attributes can inform both access policies for ZTNA and CASB as well as SWG policies, simplifying policy management across organizations.

ZTNA, RBI, and email security can also be used together to provide conditional access to resources while insulating users from malicious content (links, attachments) that they're exposed to across email and collaboration tools. Contractors and users on unmanaged devices can be provided limited access to corporate resources with user interactions (e.g. upload/download, copy/paste, keyboard input) disabled to prevent data compromise, and other L7 DLP policies can be applied to detect sensitive data.



Zero Trust services: **PURPLE**
Network services: **GREEN**

What customers are saying

"Cloudflare Access is an amazing alternative to traditional VPNs. Users just open their browsers and log in, without having to download and configure additional software."

— **Platzi**, Head of Cloud Engineering

"Access is much simpler and more secure than a VPN for limiting access to internal assets. We just activate it and add users. It just works!"

— **Bitpanda**, CTO and Co-Founder

"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."

— **ezCater**, 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"

— **Creditas**, Network Engineering Team Lead

What analysts are saying

IDC

Cloudflare named a Leader in 2023 IDC MarketScape for Zero Trust Network Access (ZTNA)

IDC cites Cloudflare's "aggressive product strategy to support enterprise security needs." We believe our recognition validates our approach to help businesses of any size get started with Zero Trust and secure access for any user to any resource, without VPNs.

kuppingercole ANALYSTS

Cloudflare named a Leader in 2022 KuppingerCole Leadership Compass for ZTNA

Through its 2022 ZTNA market analysis, KuppingerCole Analysts AG cited several Cloudflare strengths such as our fully integrated organically developed security platform, large global cloud infrastructure, and massive market presence.

Access capabilities

Creating/editing Zero Trust policies for secure access	
Granular, custom access policies	Centralized policy administration experience. L7 apps are secured at a subdomain and path level with wildcard and multi-hostname support, and support CORS requests. Policy changes proliferate globally in seconds. Includes policy tester.
Breadth of resources: What we can protect and how	Resources use public hostnames for reverse proxy to self-hosted apps (cloud/on-prem) or in-browser SSH/VNC, identity proxy to SaaS apps, or client/tunnel-based private routing via L4-7 forward proxy* to any web / non-web (arbitrary TCP/UDP) resource within a private subnet.
Identity	Authenticate via all major enterprise and social identity providers (IdPs), including multiple IdPs concurrently. Can also use generic SAML and OIDC connectors. Supports (and can enforce) any IdP-provided AuthN method, temporary AuthN, purpose justification, re-AuthN intervals on global or per-app session basis, and immediate session revoke option per-app or per-user.
Device posture	Verify device posture using device client and third-party endpoint protection provider (EPP) integrations. Use service-to-service integrations to pull EPP risk scores into Zero Trust policies.
Contextual signals for policies	Configure signals 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 external API calls. Can also reference Microsoft Entra ID (Azure AD) conditional access policies directly.
Other related support	• **SCIM:** Automatically provision/deprovision users for self-hosted and SaaS apps (examples for Okta and Azure AD) • **Internal DNS:** Configure local domain fallback and resolve private network requests • **Split tunnels:** Include/exclude IPs for private networking or running alongside a VPN • **mTLS authentication:** Certificate-based authentication for IoT and other mTLS use cases • **App isolation:** With a single checkbox, isolate apps in our lightning-fast remote browser*
On- and off-ramps	
App connector	Simple orchestration of our lightweight app connector (Cloudflare Tunnel) expedites connecting resources to Cloudflare, without requiring VM infrastructure and without throughput limitations. Includes monitoring, virtual networks (for IP overlaps), and redundancy and failover capabilities.
Device client: When to use	• **Clientless:** Extend Zero Trust policies to third-party users on unmanaged devices; also pairs well with clientless RBI and L7 DLP policies*. Clientless access supports web apps and in-browser SSH/VNC. • **Client-based:** Our device client (Cloudflare WARP) extends secure access to private networks, enables service-to-service device posture integrations, and is location-aware to apply tailored policies for on-prem users. Can also connect any two or more devices running WARP to create private networks. Users can self-enroll or can deploy via MDM.
Extensibility and visibility	
Page customization	Upload custom HTML for block and app launcher screens to fit your branding or convey specific access instructions to streamline the end user experience.
Logging	Comprehensive logging for all requests, users, and devices. Can use logpush or API to integrate with existing SIEM, orchestration, and analysis tools. For unknown assets, our shadow IT for internal infrastructure passively catalogs unique traffic surfacing all origins.
Automation	Intuitive APIs and Terraform provider available to programmatically manage all aspects of a Zero Trust implementation. Also offer userless service token support for automated services.

**using capabilities across other parts of the Zero Trust platform*

Why Cloudflare?

Easy setup and management

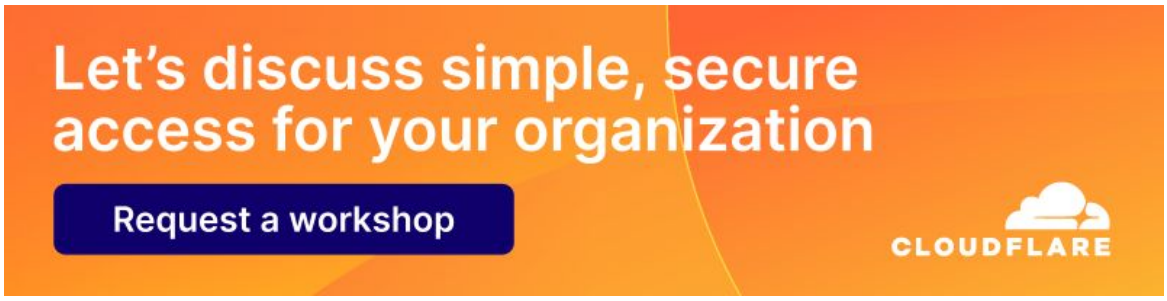
Radically simplify the setup and operation of on-ramping traffic to private resources with app connector software and tunnel orchestration.

Seamless, always-on experience

Achieve peak end user performance and resilience to network outages with Cloudflare's global Anycast technology, ensuring reliability.

Rapid, early-adopter innovation

Keep up with the evolution of the Internet itself with a provider that constantly out-innovates its peers to make app access faster and more secure.



Not quite ready for a live conversation?

Keep learning more about **Cloudflare's SSE & SASE platform**

1. 2023 survey: techvalidate.com/product-research/cloudflare/charts