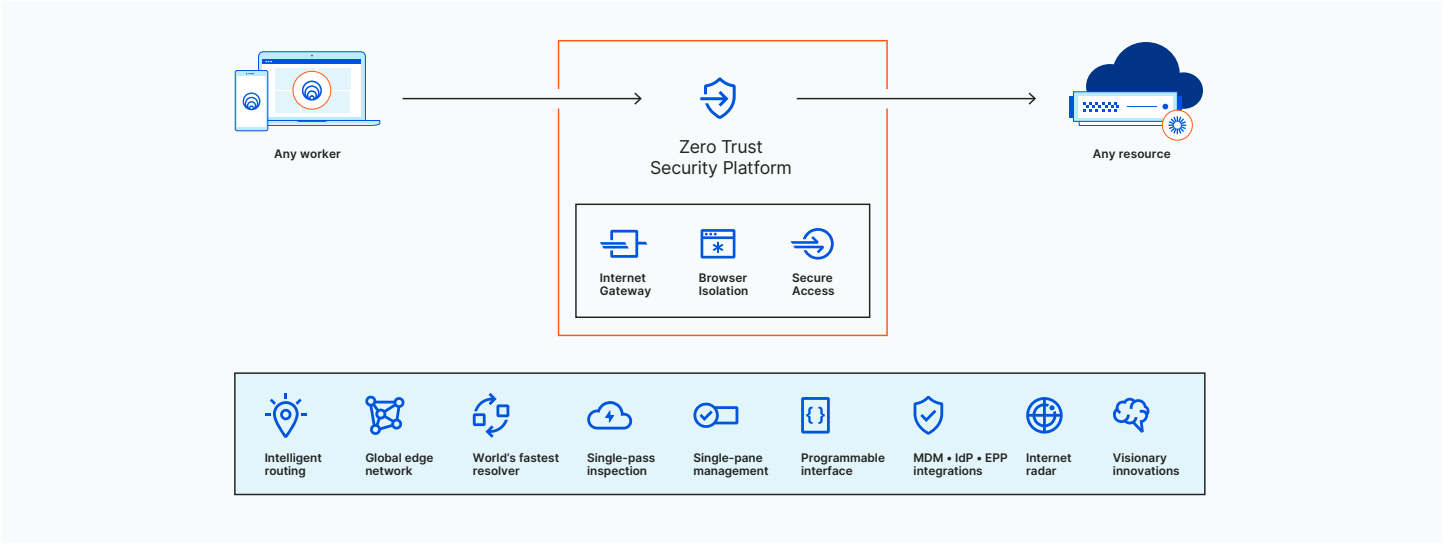
Cloudflare for Teams

The fastest Zero Trust browsing and application access platform

When applications and users left the walls of the enterprise network, security teams had to compromise on how to keep data safe. The location-centric methods they deployed to secure employee traffic - like VPNs, access control lists, and IP allow-listing - have now broken down under pressure, leaving companies with limited visibility, conflicting configurations, and excessive risk.

Cloudflare's Zero Trust security platform increases visibility, eliminates complexity, and reduces risks as employees connect to applications and the Internet. It runs on the world's fastest edge network to deploy faster and perform better than other providers.

Verify, filter, inspect and isolate workforce traffic, in one lightning-fast, single-pass inspection



Benefits

Reduce excessive trust

Protect corporate applications with identity and context-based Zero Trust rules, and isolate endpoints from risks by executing untrusted web code away from devices.

Eliminate complexity

With reduced reliance on legacy VPNs and point security products, administrators can apply standard security controls to all traffic - regardless of how that connection starts or where in the network stack it lives.

Restore visibility

Increase visibility with detailed logs for DNS, HTTP, login, and in-application activity. Administrators can monitor user activity in self-hosted and SaaS apps, with an audit trail to investigate incidents.

Deployment Outcomes

80%↓

less time spent resolving IT tickets and security posture for employees.

91%↓

reduction in attack surface by placing Cloudflare in front of application access and internet browsing.

30 min

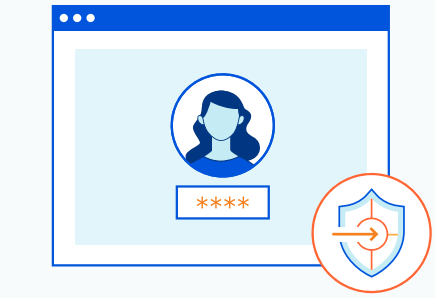
of setup time to unlock faster and safer application and Internet access.

Zero Trust Network Access with Private Routing

- Protect applications with identity, posture, and context-driven rules
- Enforce consistent access controls and visibility across cloud, on-premise, and SaaS applications
- Apply strong authentication methods to even legacy applications with network firewall and Zero Trust rules

Secure Web Gateway with Zero Trust Browsing

- Block phishing and malware with intelligence from our network firewall and Zero Trust rules
- Isolate browsing activity from corporate endpoints, mitigating the impact of breaches
- Stop data from leaving corporate apps and gain Shadow IT visibility



The Cloudflare Difference

One management interface

Provide better ease of use for administrators with a natively built dashboard for application and Internet access including integrations with identity providers, endpoint protections, and network onramps.

One consolidated platform

Reduce complexity with one easy-to-manage platform that consolidates Secure Web Gateway, Zero Trust Network Access, DNS Filtering, Cloud Access Security Broker (CASB) and Data Loss Prevention into one streamlined control plane. Replace VPN clients, on-premise firewalls, and other legacy security solutions as you move security and connectivity to the edge.

Unrivaled end-user experience

Cloudflare routes requests faster utilizing optimized, intelligence-driven routing across our vast Anycast network, with 200+ locations in more than 100 countries around the world.

On average, web apps are accessed 30% faster and TCP connections see a 17% decrease in round trip time.

CLOUDFLARE

Cloudflare for Teams features

Support	
Communication channels	**24×7×365 Phone 24×7×365 Chat Email**
Median email response time	**Less than 1 hour**

Reduce risk	
Zero Trust Network Access	✓
Secure Web Gateway	✓
→ *Recursive DNS Filters*	✓
→ *Layer 4 Firewall Filters*	✓
→ *Layer 7 Proxy Filters*	✓
→ *Antivirus Inspection*	✓
→ *CASB*	✓
→ *Remote Browser Isolation*	**Add on (natively-integrated)**

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

Consistent policy	
Custom application, private network, and Internet access policies	**Unlimited**
Authentication via enterprise and social IdPs	✓
Security categories (13) via machine learning and intelligence feeds	✓
Content categories (100+) for acceptable use	✓
Custom block, allow, or decryption bypass lists	✓
Granular HTTP and URL rules	✓
File type controls	✓
Device posture using third-party integrations and Cloudflare	✓
CSV-based bulk import for lists	✓

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)	✓
Network-level security for physical locations	**50**
Editable IP network locations	✓

Simple interoperability	
Endpoint and mobility management integrations	✓
Split-tunneling for local or VPN connectivity	✓
Client self-enrollment for unmanaged devices	✓
Authentication supports multiple identity providers concurrently	✓
Customizable app launcher	✓
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 seconds)	✓
Fastest, intelligent IP routing (<100ms)	✓
Fastest, private DNS resolver (7-31ms)	✓
Fastest, secure remote browser (2x speed of others)	**Add on**

Ready to try Cloudflare for Teams? Visit www.cloudflare.com/teams/ today