Cloudflare Zero Trust

Secure any user accessing any application, on any device, in any location

Plan overview	Free	Pay as you go	Contract
Pricing[1]	$0 forever	$7/user/month	annual custom price per user
Best for teams...	with <=50 users, or running proof-of-concept tests	that do not require max support and security controls	that want max support and security controls
Usage and uptime	up to 50 users	no user limit with 100% uptime SLA	no user limit with 100% uptime SLA
Support channels and response time	community forums available for tips and troubleshooting	email and chat with 4 hour median initial response for urgent issues	priority phone, email, and chat with 1 hour median initial response for urgent issues
Dashboard activity logging	up to 24 hours	up to 30 days	up to 6 months
Application connector software	✓	✓	✓
Device client (agent) software	✓	✓	✓
Zero Trust Network Access (ZTNA)	✓	✓	✓
Secure Web Gateway (SWG)	✓	✓	✓
Cloud Access Security Broker (CASB)	in-line only	in-line only	✓ multi-mode
Remote Browser Isolation (RBI)		add-on	✓
mTLS authentication			✓
Logpush to SIEM/cloud storage			✓
Cloud Email Security (CES, Area 1)			✓
Data Loss Prevention (DLP)			✓

[1] Cloudflare Zero Trust pricing is based on number of users. Unlike some of our peers, Cloudflare does not charge for increased bandwidth, number of app connectors, or volume of threats mitigated.

Access controls

Cloudflare Access enforces Zero Trust rules for users accessing any application in any on-premise private network, public cloud, or SaaS environment. Start with clientless methods to protect high-risk apps or third-party users like contractors, then layer in identity and endpoint protection and offload additional apps from your legacy VPN(s). Faster and safer than VPNs, ZTNA is a meaningful starting point for organizations' Zero Trust journeys.

Capability	Free	Pay as you go	Contract	Details
Customizable access policies	✓	✓	✓	Custom application and private network policies, plus policy tester. Supports temporary authentication, purpose justification, and any IdP-provided auth method.
Protect access to all your apps and private networks	✓	✓	✓	Protect self-hosted, SaaS, and non-web (SSH, VNC, RDP) apps, internal IPs and hostnames, or any arbitrary L4-7 TCP or UDP traffic.
Authentication via Identity Providers (IdPs)	✓	✓	✓	Authenticate via enterprise and social IdPs, including multiple IdPs concurrently. Can also use generic SAML and OIDC connectors.
Identity-based context	✓	✓	✓	Configure contextual access based on IdP groups, geolocation, device posture, session duration, external APIs, etc.
Device posture integration	✓	✓	✓	Verify device posture using third-party endpoint protection provider integrations.
Clientless access option	✓	✓	✓	Clientless access for web apps and browser-based SSH or VNC
Browser-based SSH and VNC	✓	✓	✓	Privileged SSH and VNC access through in-browser terminal
Split tunneling	✓	✓	✓	Split tunneling for local or VPN connectivity
Application launcher	✓	✓	✓	Customizable app launcher for all apps, including bookmarks to apps outside of Access
Token authentication	✓	✓	✓	Service token support for automated services
Internal DNS support	✓	✓	✓	Configure local domain fallback. Define an internal DNS resolver to resolve private network requests.
Infrastructure-as-code automation (via Terraform)	✓	✓	✓	Automate deployment of Cloudflare resources and connections.
mTLS authentication			✓	Certificate-based auth for IoT and other mTLS use cases

Threat protection

Cloudflare Gateway, our Secure Web Gateway (SWG), protects remote or office users with identity-based web filtering. Start with DNS filtering to achieve quick time-to-value before layering on more comprehensive protections like HTTPS inspection and our natively-integrated remote browser isolation (RBI).

Capability	Free	Pay as you go	Contract	Details
Comprehensive security categories	✓	✓	✓	Block by ransomware, phishing, DGA domains, DNS tunneling, C2 & botnet, and more.
Recursive DNS filtering	✓	✓	✓	Filter by security or content category. Deploy via our device client or via routers for locations.
HTTP(S) filtering	✓	✓	✓	Control traffic based on source, destination country, domains, hosts, HTTP methods, URLs, and more. Unlimited TLS 1.3 inspection.
L4 firewall filtering	✓	✓	✓	Allow or block traffic based on ports, IPs, and TCP/UDP protocols.
Antivirus inspection	✓	✓	✓	Scan uploaded / downloaded files across types (PDFs, ZIP, RAR, etc.)
Integrated threat intelligence	✓	✓	✓	Detection via our own ML algorithms and third party threat feeds.
IPv6-only & dual stack support	✓	✓	✓	All functionality available for IPv4 and IPv6 connectivity.
SSH proxying and command logging	✓	✓	✓	Create network policies to manage and monitor SSH access to your applications
Network-level policies for physical locations	Up to 3 locations	Up to 20 locations	Up to 250 locations	Secure connectivity for DNS filtering directly from offices.
Remote Browser Isolation (natively-integrated)		Add-on	✓	Render all browser code at the edge, instead of locally, to mitigate threats. Deploy with or without a device client. Selectively control what and when to isolate activity.
Cloud email security			✓	Stop phishing and business email compromise with Cloudflare Area 1 email security
Proxy endpoints for PAC file support			✓	Apply HTTP policies at the browser level by configuring a PAC file. Apply filters without deploying client software on user devices.
Dedicated egress IPs			Add-on	Dedicated range of IPs (IPv4 or IPv6) geolocated to one or more Cloudflare network locations.

Data protection

Cloudflare Zero Trust offers holistic protection and controls across data in transit, in use, and increasingly at rest. Within any subscription, leverage ZTNA and SWG services to guard against inadvertent or malicious data leakage. Add RBI, CASB, and DLP to apply more granular controls, inspections, and detections for data risks.

Capability	Free	Pay as you go	Contract	Details
Zero Trust access to mitigate data leakage (via ZTNA)	✓	✓	✓	Set least-privilege policies per application to ensure users only access data they need.
File upload / download controls based on Mime type (via SWG)	✓	✓	✓	Allow or block uploads / downloads of files based on Mime type.
Application and application type controls (via SWG)	✓	✓	✓	Allow or block traffic to specific apps or app types.
Controls over data interactions within a browser (via RBI)		Add-on	✓	Restrict download, upload, copy/paste, keyboard input, and printing actions within isolated web pages and applications. Prevent data leakage onto local devices, and control user inputs on suspicious websites. Deploy with or without a device client.
API-driven CASB to detect risk of data leakage from SaaS apps			✓	Add Cloudflare CASB to detect if misconfigurations in SaaS applications leak sensitive data.
Data Loss Prevention (DLP)			✓	Inspect HTTP(S) traffic and files for the presence of sensitive data, and configure allow or block policies for the data patterns, such as Credit Card Numbers and U.S. Social Security Numbers.

SaaS app protection

Cloudflare delivers inline and API-based Cloud Access Security Broker (CASB) capabilities for comprehensive visibility and protections over SaaS applications. Inline CASB, ZTNA, SWG, and RBI controls come with any plan. With contract plans, enable API-based controls to scan SaaS apps for vulnerabilities to protect data at rest.

Capability	Free	Pay as you go	Contract	Details
Inline access and traffic controls for every SaaS app	✓	✓	✓	All access controls, data controls, and threat protection capabilities (as outlined in prior sections) apply consistently across SaaS apps.
SaaS app tenant controls	✓	✓	✓	Allow traffic only to corporate tenants of SaaS apps. Prevent leakage of sensitive data to personal or consumer tenants.
Shadow IT discovery	✓	✓	✓	Review apps your end users visit. Set approval status for those apps.
In-depth SaaS app integrations			✓	Via API, integrate with your most used SaaS apps (e.g. Google Workspace, Microsoft 365) to scan, detect, and monitor for security issues.
Continuous monitoring of data security risks and user activities			✓	API integrations continuously monitor SaaS apps for suspicious activities, data exfiltration, unauthorized access, and more.
File sharing detection			✓	Identify inappropriate file sharing behaviors within your most used SaaS apps.
SaaS app posture management and remediation			✓	Discover misconfigurations and incorrect user permissions within SaaS apps. Immediately action surfaced security findings with step-by-step remediation guides.
Data Loss Prevention (DLP)			✓	Inspect inline traffic from SaaS apps for sensitive data (e.g. Credit Card Numbers and SSNs) and configure allow or block policies.
Phishing detection for cloud-based email apps			✓	Stop phishing and business email compromise with Cloudflare Area 1 email security.[2]

[2] Cloudflare Area 1 provides comprehensive cloud email security which includes business email compromise and fraud prevention, advanced threat protections, email hygiene maintenance, and more.

Visibility

Increase visibility by intercepting and logging requests from managed and unmanaged devices. Comprehensive logs for DNS, HTTP, SSH, network, and Shadow IT activity. Monitor user activity across all apps. Send logs to multiple of your preferred cloud storage and analytics tools.

Capability	Free	Pay as you go	Contract	Details
Activity log retention	24 hours	30 days	6 months	On contract plans, DNS logs are stored 6 months, and HTTP and network logs for 30 days.
Access and authentication logs	✓	✓	✓	Comprehensive details for all requests, users, and devices, including block reasons. Block policy decisions are stored for a week, and authentication logs for 6 months.
App connector (tunnel) logs	✓	✓	✓	Audit logs for the connection status of tunnels and for when a new DNS record is registered for an app.
Shadow IT visibility with categorized application groups	✓	✓	✓	Track usage and review approval status across applications end users visit.
SSH command logging	✓	✓	✓	Full replay of all commands run during an SSH session. Provides SSH visibility at a network layer.
Private network discovery	✓	✓	✓	Passively monitor private network traffic to catalog discovered apps and users who access them.
Exclude personally identifiable information (PII)	✓	✓	✓	By default, logs will not store any employee PII (source IP, user email, user ID, etc.) and be unavailable to all roles in your organization.
Redact PII			✓	PII can be redacted from logs for all permission roles except for those specially designated.
Logpush to SIEM			✓	Integrations with analytics and SIEM tools like Sumo Logic, Splunk, and Datadog.
Logpush to cloud storage			✓	Built-in support for one or more storage destinations concurrently including AWS, Azure, Google Cloud, and any S3-compatible API.

Network performance and connectivity on-ramps

Capability	Free	Pay as you go	Contract	Details
Lightning-fast network speed	✓	✓	✓	~50ms away from 95% (or ~20ms away from 80%) of the Internet-connected population globally
Global Anycast network	✓	✓	✓	Anycast network spanning 275+ cities in 100+ countries with 155 Tbps of network edge capacity
Global interconnects	✓	✓	✓	11K interconnects, including major ISPs, cloud services, & enterprises
One control plane for all edge services	✓	✓	✓	Network architected so that every service operating at the edge is built to run in every data center and available to every customer.
Single-pass inspection for L3 - L7 traffic	✓	✓	✓	All traffic is processed in a single pass at the data center closest to its source. No backhauling.
Smart routing over virtual backbone	✓	✓	✓	Optimized routes to avoid congestion issues.
Device client (agent) software	✓	✓	✓	Available across all major OSes (Win, Mac, iOS, Android, Linux, ChromeOS).
Multiple modes for device client (agent)	✓	✓	✓	Default mode sends traffic through WireGuard tunnels to enable the full range of security functionality. Use DoH mode to only enforce DNS filtering policies, or use proxy mode to filter traffic only to specific apps.
Managed deployment and self-enrollment options	✓	✓	✓	Deploy to your entire device fleet via MDM tools. Or, users can download the device client themselves to self-enroll.
App connector (tunnels)	✓	✓	✓	Connect resources to Cloudflare without a publicly routable IP address. Deploy via UI, API, or CLI.

Note: Cloudflare One includes more on-ramps for physical location connectivity and services to transport East-West traffic. Use Cloudflare Anycast IP tunnels over GRE or IPSec, which are made easier with SD-WAN partnerships that leverage your existing investments. Or use direct connections physically at Cloudflare colos, virtually at 1600+ exchange partner colos, or via the wiring closets of select multi-tenant offices worldwide.