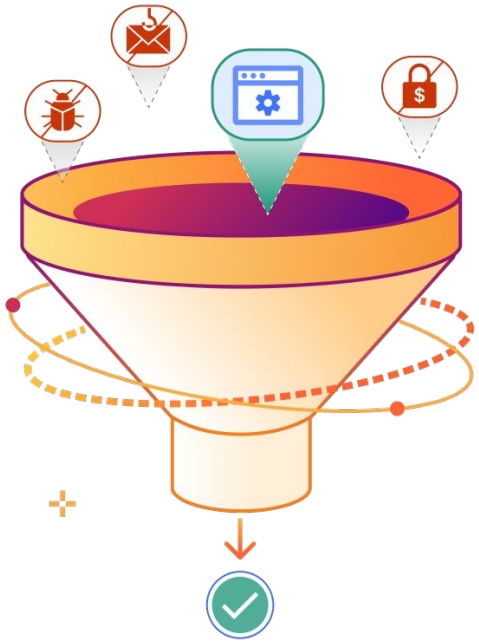
Secure Web Gateway (SWG)

Cloudflare Gateway, a composable service within Cloudflare One, protects users and data from cyber threats with identity-aware Internet filtering.



Simple, modern threat defense

Replace complex legacy web security

Cyber threats are everywhere and continue to exploit gaps in your organization's growing attack surface. Juggling multiple point solutions (like DNS resolvers, web gateways, and network firewalls) only increases cost, complexity, and risk.

Cloudflare Gateway simplifies security with consistent protections and visibility for access to the Internet and internal resources. Reduce cyber risk with identity-aware policies that help your organization:

- **Stop Internet threats** like ransomware, phishing, command & control, and more
- **Control and monitor L4-L7 traffic** with DNS, HTTP, network, and browser isolation rules
- **Enforce acceptable use policies** across remote and office workers

In a single-pass architecture, all traffic is verified, filtered, inspected, and isolated from threats.

SWG today, Security Services Edge (SSE) tomorrow

Moderning SWG controls is a common step towards consolidating security with an SSE architecture and embracing Zero Trust best practices.

Explore what that journey can look like with Cloudflare.

Why Cloudflare?

Unified security

1 network

and control plane for all services across Security Services Edge (SSE), web application and API protection (WAAP), email security, and other domains.

Mass scale threat intelligence

2 Trillion

DNS queries served per day. This real-time visibility across new, newly seen, and risky domains powers AI/ML-backed threat hunting models.

Built for scale

310+

network locations in 120+ countries. Every SWG and Zero Trust / SSE function is available for customers to run in every location, such that enforcement is always fast and consistent.

Use case: Threat defense for remote workers and office locations

Problem

Hybrid work has expanded your attack surface, and the security gaps from managing disparate tools makes it easier for ransomware, phishing, and other cyber threats to hurt your wallet and brand reputation.

Solution

Cloudflare's SWG offers consistent web security across remote and office workers. Most organizations start with DNS filtering to achieve quick time-to-value, before layering on more comprehensive inspections and controls across all Internet activity.

Getting started

Send traffic to Cloudflare's network first for DNS resolution (and later for full HTTP inspection)

Enforce DNS filtering by identity / device for remote workers or by location for offices

Layer more granular controls including HTTP, network, and browser isolation rules.

Deploy cloud email security inline as MX, via API, or both (multi-mode)

First, secure web browsing for users on-and off- network

Next, layer email security

Reduce risk, while improving team productivity

Simple, flexible deployments

Use network routers for DNS resolution. Send L3 traffic via GRE/IPsec tunnels, WAN connector or existing SD-WAN.

Or deploy our device client to forward proxy traffic.

Fast, consistent protection

Single-pass inspection across our network for fast, consistent policy enforcement everywhere.

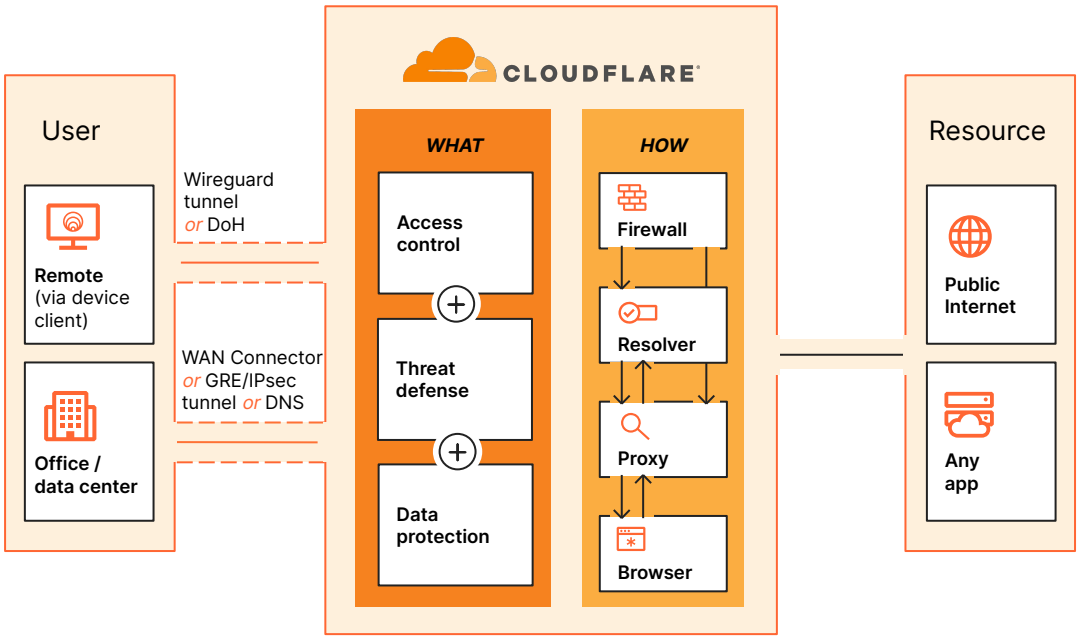
Proven faster than vendors like Zscaler, Netskope, and Palo Alto Networks.

Accelerate Zero Trust adoption

One unified control plane with one policy manager across composable SSE/SASE services.

Start with web and email security and layer other Zero Trust controls your own pace.

How the SWG works



Simplify security.

Apply firewall, resolver, proxy, and browser controls to both Internet-bound and internal resource traffic.

Build policies from one policy manager.

Layer SSE controls on your SWG foundation

By forward proxying traffic through Cloudflare's SWG, your organization can extend security controls and visibility further by leveraging capabilities across our natively-integrated and composable SSE services.

Protect web and app activity with RBI

- Insulate local devices from malware by running all browser code on Cloudflare's global network with low latency
- Isolate apps to protect data with DLP scans and browser controls (e.g. block copy-paste, restrict up/download, printing) — with or without a device client

Protect data with multi-mode DLP and CASB

- Prevent data leaks by detecting and blocking sensitive data in HTTP(S) traffic and files with predefined (e.g. financial / health data) or custom profiles (e.g. exact data match)
- Scan SaaS suites for misconfigurations with integrated DLP detections for sensitive data and take prescriptive steps to remediate.

Extend identity-aware access policies with ZTNA

- Enforce Zero trust rules that limit access to self-hosted corporate apps, SaaS apps, and private network IPs or hostnames.
- Integrate identity and endpoint protection providers once and apply posture checks across Internet and app access rules using the same rule builder

Increase visibility

- Maintain detailed audit logs across managed and unmanaged devices (on contract plans DNS logs are stored for 6 months and HTTP and network logs for 30 days)
- Logpush to your preferred SIEM for correlation and further analysis

Gateway capabilities

Threat defense and secure access	
Security & application categories	Comprehensive coverage of ransomware, phishing, DGA domains, DNS tunneling, new and newly seen domains, C2 & botnet, and other security risks. Inline CASB coverage of 25 app categories, including AI.
Recursive DNS filtering	Allow / block / override domains and IP addresses by security or content categories. DNS filters can be managed via our Tenant API for parent-child configurability.
HTTP(S) filtering and inspection	Control traffic based on source, destination, domains, HTTP methods, URLs, and more. HTTP1/2/3 inspection enables AV & DLP scans, file controls, device posture, tenants, RBI and more.
Unlimited TLS 1.3 inspection	Unlimited TLS 1.3 inspection by default. All HTTPS traffic is decrypted, policies apply & requests are re-encrypted with our cert or your custom cert — all with market-leading low latency. DNS over TLS (DoT) & DNS over HTTP (DoH) standards supported. Enable only FIPS 140-2 compliant cipher suites.
L4 FWaaS	L4 network policies apply to all public/private TCP/UDP packets, controlling access to non-HTTP resources by detected protocol, geolocation, SNI domain & more. Audit SSH traffic over port 22. (L3 FWaaS capabilities built into WAN networking services.)
Antivirus inspection	Scan uploaded / downloaded files across types (PDFs, ZIP, RAR, etc.) for viruses.
Identity and device posture checks	Set policies based on all major enterprise identity providers, social identities, or SAML and OIDC standards. Verify device posture via the device client or your third-party endpoint protection provider.
Integrated threat intelligence	Threat intel is based on our own AI/ML models and 3rd party feeds. 1st party intel is derived from global telemetry as one of the largest authoritative and recursive DNS resolvers (2T+ queries/day). Our web crawler also indexes the entire web (8B+ pages) every few weeks to uncover emergent campaign infrastructure. Custom threat feeds and signatures (IPs, URLs, and domains, etc.) are also supported.
On- and off- ramps	
With device client	Forward proxy traffic via our device client (WARP) through full WireGuard tunnels or over DoH. Self-enroll or deploy via MDM. Enables device posture checks. Detects if device is on-network.
Clientless options	Options include: network-routed DNS queries from customer locations; Anycast GRE/IPsec tunnels; WAN connector, proxy endpoints via PAC files; and clientless web isolation via a rewritten URL.
IPv4 & IPv6 support	All functionality available for IPv4 and IPv6 connectivity (whether IP6-only or dual stack).
Traffic routing	
Dedicated egress IPs and egress policies	Dedicated range of static IPs (IPv4 or IPv6) that can be used to allowlist traffic based on source IP. Use egress policies to select which egress IP is used, based on attributes like identity, geolocation, or device posture. Each egress IP is unique to an individual account and not used by other customers.
Resolver policies	Route DNS requests to custom DNS resolvers to reach non-publicly routable domains, such as private network services and internal applications. (By default, DNS requests use Cloudflare's own public DNS resolver, 1.1.1.1, one of the fastest and most reliable in the world.)
Split tunnelling	Exclude / include IP addresses or domains for private networking or running alongside a VPN.
Visibility and extensibility	
Logging	Comprehensive logging for all DNS queries, L4 network packets, and HTTP requests inspected over any port. Use logpush or API to integrate with existing SIEM, orchestration, and analysis tools. Admins can choose to exclude and/or redact collection of personally identifiable information (PII) across users.
Shadow IT discovery	Track, review, and approve SaaS and private network origins that your end users visit via inline CASB.
Page customization	Upload custom HTTP block pages to fit your branding or convey instruction for a better user experience.
Automation	Intuitive APIs and Terraform provider available to programmatically manage all aspects of an SSE / Zero Trust implementation. Also offer userless service token support for automated services.

How customers use our SWG

Cloudflare & Accenture secure Internet access for the U.S. Cybersecurity & Infrastructure Security Agency (CISA)

100+ **U.S. civilian agencies** with office locations secured with Cloudflare's DNS filtering

Learn more

bouvet

Scandinavian IT and digital communications consultancy

"We depend on Cloudflare to reduce our attack surface by securing our ports, filtering threats, and cleaning up our traffic."

— Victor Persson, Security Operations Lead

Read the case study

classmethod

Japanese cloud integrator and consultancy

4K **requests blocked per week** to harmful and unwanted Internet content across hundreds of employees

Read the case study

Sample competitive comparison vs. Zscaler

Criteria	Cloudflare Gateway	Zscaler Internet Access
Architecture	✓ One cloud platform, One control plane	✗ Many fragmented clouds, Many control planes
Management interface	✓ One interface for all SSE	✗ Separate for SWG and ZTNA
Single pass inspection	✓ YES for all SSE services	✗ NO
IPv6-only support	✓ YES	✗ NO
Uptime SLA	✓ 100% for all services	✗ 99.999% for most services 99.9% for DNS resolver

Continue comparing Cloudflare vs. Zscaler

Faster protection

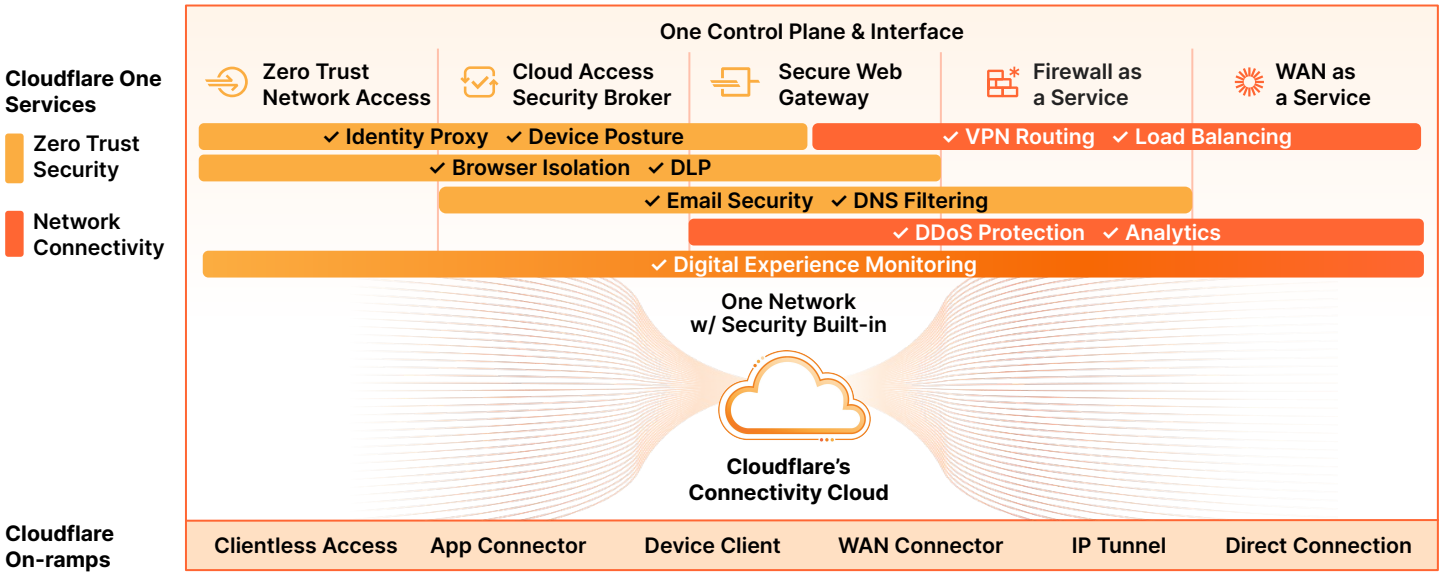
13-58% **faster for Secure Web Gateway (SWG)**

45-64% **faster for Remote Browser Isolation (RBI)**

Based on first-party testing and third-party testing

Modernize security with Cloudflare's SSE platform

Cloudflare Gateway is a composable service within Cloudflare One, our SSE platform. Build from your SWG foundation and extend visibility and controls with Cloudflare One's interoperable security capabilities across web, SaaS, and private app environments.



One unified platform

- **Secure access** by verifying and segmenting any user to any resource
- **Threat defense** by covering all channels with network-powered AI/ML & threat intel
- **Data protection** by increasing visibility and control of data in transit, at rest and in use

One programmable network

- **More effective** by simplifying connectivity and policy management
- **More productive** by ensuring fast, reliable, and consistent UX everywhere
- **More agile** by innovating rapidly to meet your evolving security requirements

Not quite ready for a live conversation?

Keep learning more about Cloudflare's SSE & SASE platform