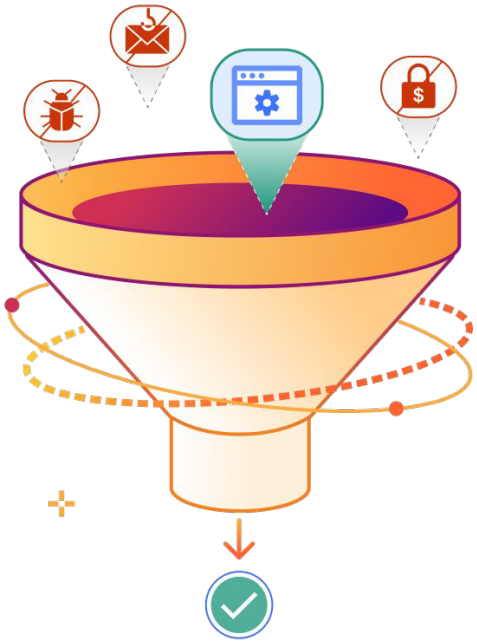
Secure Web Gateway (SWG)

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.