

Cisco Umbrella vs. Cloudflare One

Choose Cloudflare for your best-of-breed DNS filtering and for your unified Zero Trust SSE platform.

Simplify web security and beyond

Whether you use Umbrella as a point solution for DNS filtering or alongside other Cisco services, Cloudflare can streamline your security approach.

First: Migrate DNS filtering to Cloudflare

Cloudflare offers rigorous, high speed, and reliable DNS filtering (aka. protective DNS) backed by a larger, more distributed global network than Cisco Umbrella.

Flexible deployments and intuitive policy management help you start realizing value quickly, whether you prefer a 'set & forget' or a more custom approach.

For Umbrella users, Cloudflare will feel familiar, including similarly comprehensive coverage of security and content categories and threat intel as a large-scale recursive DNS resolver.



VS



Later: Zero Trust SSE modernization

With Cisco, expanding from DNS filtering to broader Zero Trust uses cases, requires upgrading from Umbrella to Cisco Secure Access, a separate security service edge (SSE) platform running on a separate architecture.

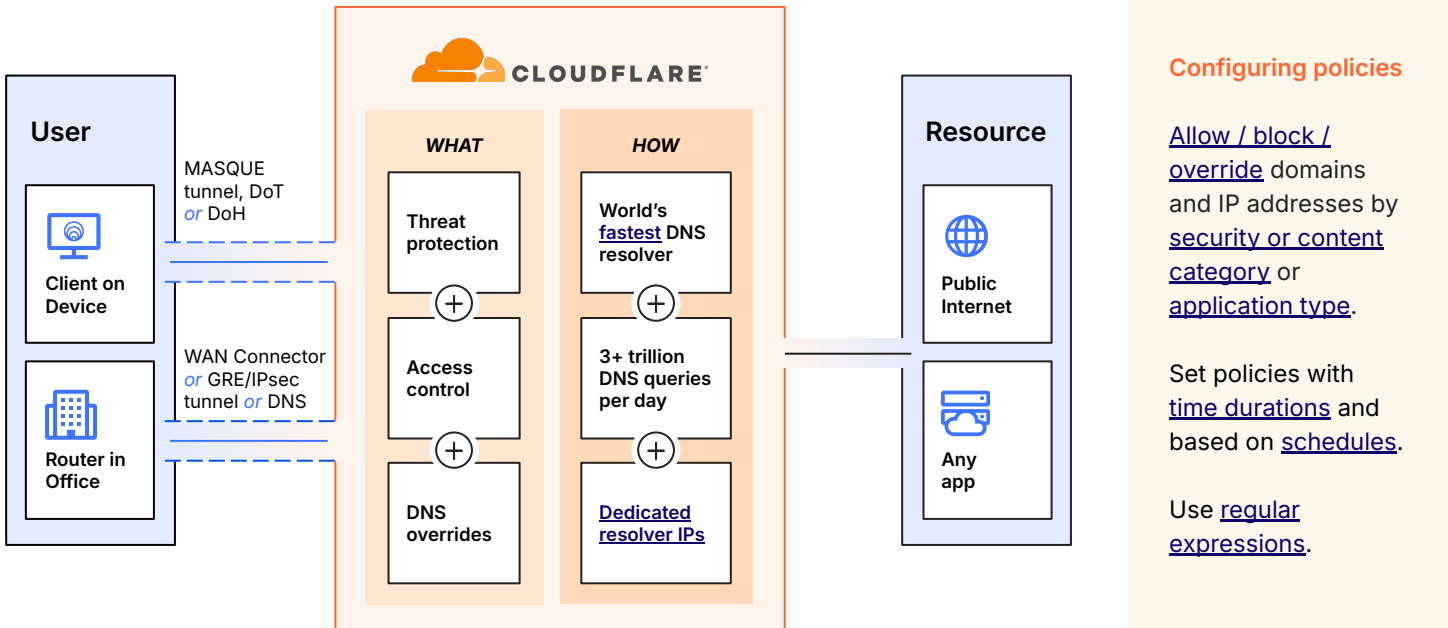
With Cloudflare, that expansion takes place on one platform and control plane with one management interface. This unified architecture supports agility and consistency as you modernize security.

Why Cloudflare?		
	For best-of-breed DNS filtering	For Zero Trust SSE modernization
Simple management & architecture	Multiple deployment modes with and without a device client across office and remote users, so you can get started quickly. Automate policy setup and onboarding via APIs, including with our Terraform provider.	One platform, one control plane, and one policy manager for all SSE services. All services are 100% cloud-native and built from the ground up on our network — not 'acquired and stitched' together.
Global speed, consistency, & reliability	Cloudflare's DNS filtering is built on one of the world's fastest and most reliable DNS resolvers (1.1.1.1.) for a seamless user experience.	Unlike with Cisco Umbrella, all services are available across all of Cloudflare's network, which today spans 330+ cities in 120+ countries.
AI-backed threat intelligence	Visibility across 3+ trillion authoritative and recursive DNS queries resolved per day powers our own AI/ML-backed threat hunting models.	Cloudflare is also used as a reverse proxy by ~20% of all websites. Powered by this visibility, protections against vulnerability exploits, DDoS, and bots are built in for any internal app protected by Cloudflare.

See comparison table on the last page

How it works: Best-of-breed DNS filtering

Available as standalone service and packaged as 'Cloudflare Gateway'



User attribution for DNS filtering: All corporate SSOs, social identities, and open-source identity methods are supported across all Cloudflare plans. By contract, Cisco Umbrella's DNS security plans only support a subset of identity providers.

Threat intelligence

- [AI/ML threat hunting models](#) based on 3.6T+ authoritative & recursive DNS queries per day detect algorithmically-generated domains, DNS tunneling techniques, and more
- 3rd-party intel sourced from best-in-class OSINT and premium feeds

Customizability

- [Route DNS requests](#) to custom DNS resolvers to reach non-publicly routable domains (e.g. private network services and internal apps)
- [Custom](#) threat feeds and signatures (IPs, URLs, and domains, etc.) are supported

Global scalability & resilience

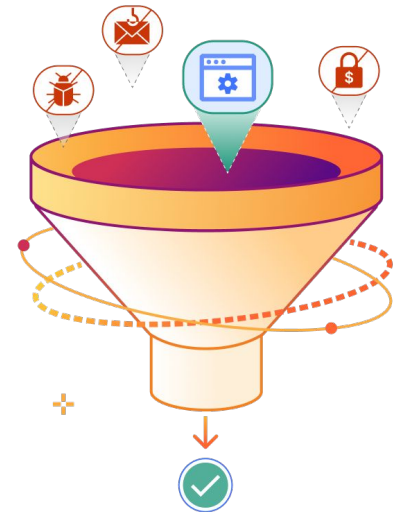
- Built of on one of the world's fastest and most reliable DNS resolvers ([1.1.1.1](#))
- 330+ network locations in 120+ countries and ~13,000 interconnects
- 321 Tbps of network capacity and 100% uptime SLA for all services

Agile configuration with APIs

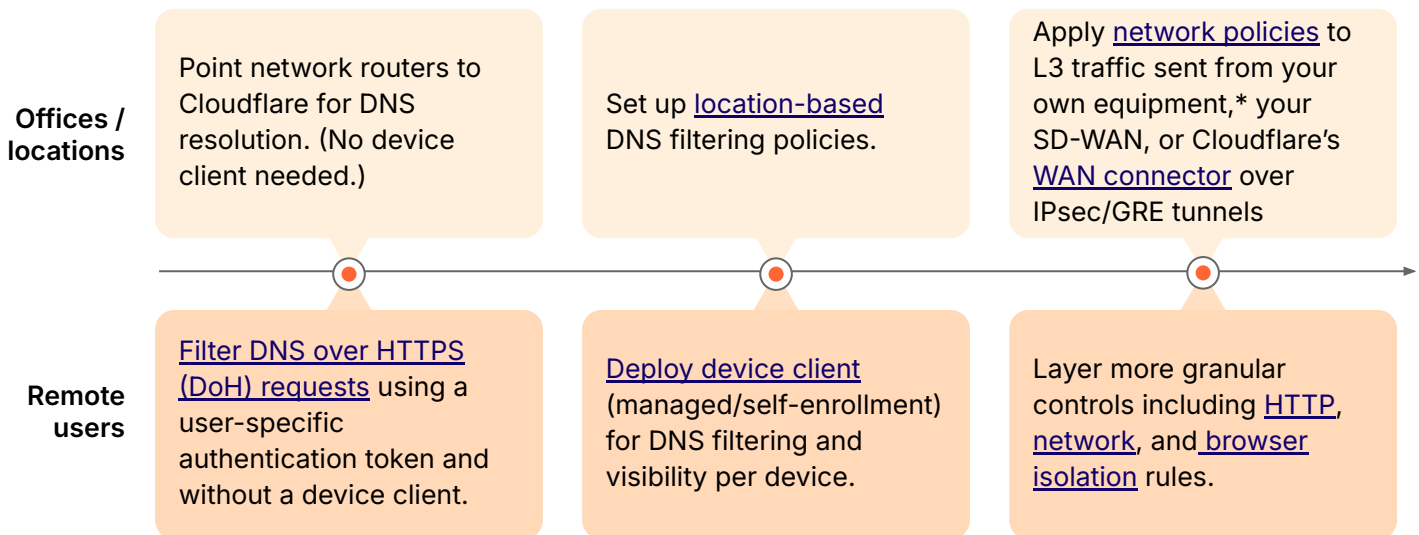
- Automation support via [Terraform](#) — unlike Cisco Umbrella
- [One API](#) across all Cloudflare services — unlike Cisco Umbrella
- Manage via our [Tenant API](#) for parent-child tiering of accounts and policies

DNS filtering use cases


- **Block Internet threats** like malware, ransomware, phishing, DNS tunnelling, C2 & botnet, and other risky domains and IPs
- **Support compliance** with regulations, government directives, and standards (like, [NIST SP 800-42](#) in the US and [NIS2](#) in the EU)
- **Encrypt all DNS requests** over HTTPS (DoH) or over TLS (DoT) for security & privacy
- **Enforce acceptable use policies** and filter content on guest WiFi across retail, hospitality, public spaces, and other locations
- **Replace legacy appliances** and avoid inefficiencies of backhauling Internet-bound traffic through on-prem security
- **Block access to unauthorized SaaS and cloud apps** to mitigate the risks of shadow IT



Steps to get started



Customers



100K+
hybrid workers protected.

Fortune 500 telecom unifies web and application access with Cloudflare, replacing traditional VPNs and Cisco Umbrella.

[Learn more](#)

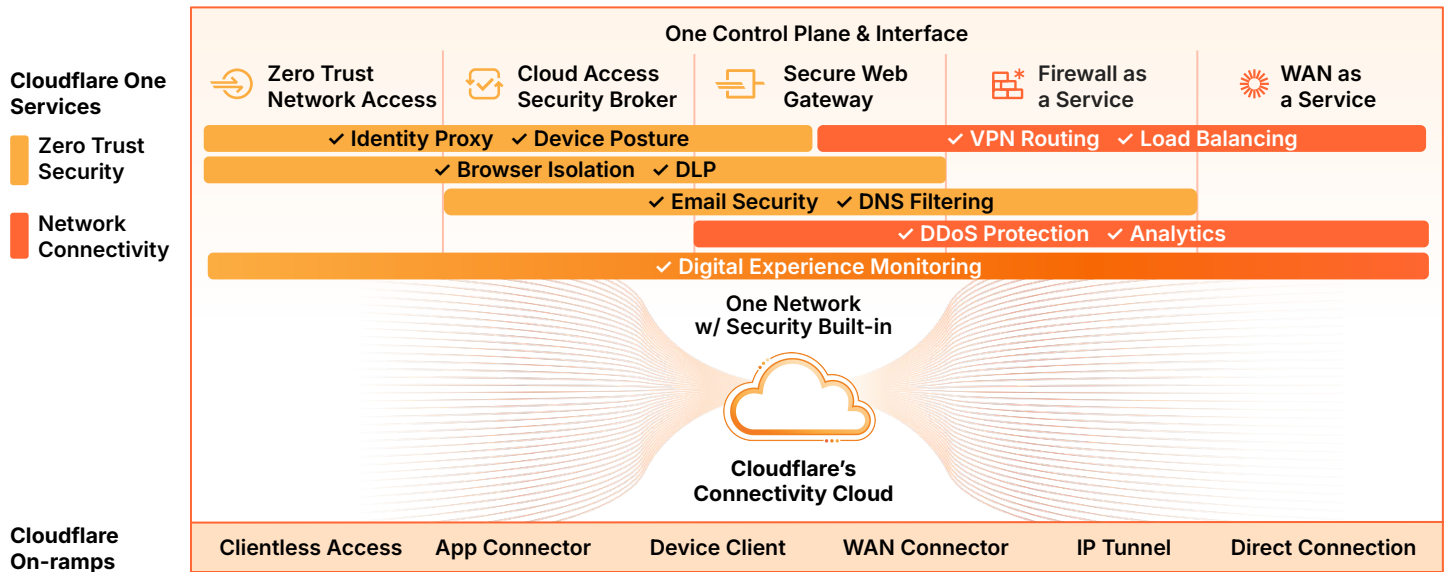


100+
U.S. civilian agencies with office locations secured with Cloudflare's DNS filtering

[Learn more](#)

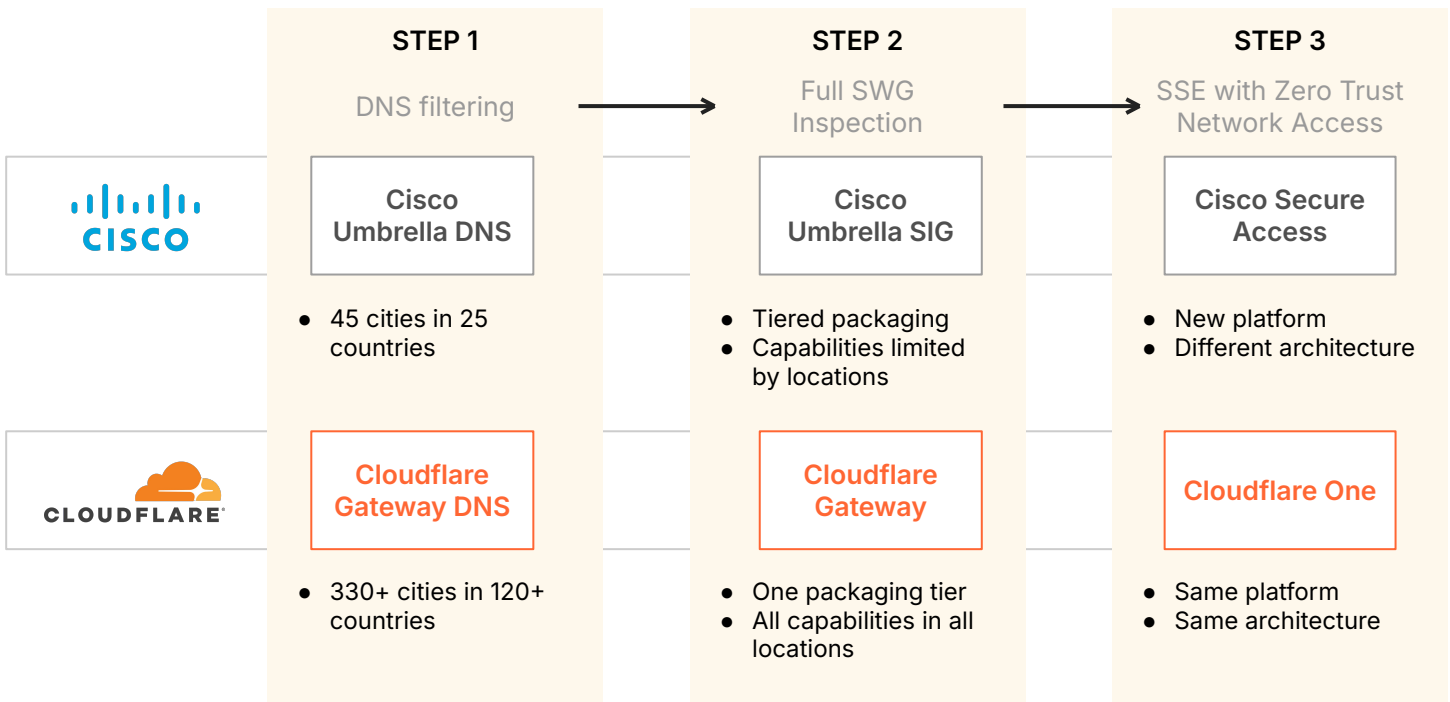
Accelerate your Zero Trust SSE transformation

After starting with DNS filtering, many organizations extend visibility and controls across web, SaaS, and private app environments with [Cloudflare One](#), our SSE/SASE platform. All Cloudflare One services are composable, natively-integrated, and built from the ground up on our network, so you can advance your Zero Trust security and network modernization projects with agility.



Adoption roadmap

Cloudflare's unified platform provides a strong foundation as you layer new capabilities.



Comparison table

Based on data as of December 2024	Cloudflare One	Cisco Umbrella
DNS filtering: Threat protection		
Billions of recursive DNS queries per day to inform threat intelligence	✓	✓
Block domain requests and IP responses by security risks and content categories	✓	✓
Enable SafeSearch	✓	✓
Custom threat indicator feeds	✓	✓
File inspection	All the time in all plans	Depends on plan
DNS filtering: Policy management		
Custom block pages and bypass options	✓	✓
Parent-child configuration	✓	✓
DNS override	✓	✗
Automation via Terraform	✓	✗
Virtual appliance (for local on-prem DNS servers)	✗	✓
User attribution and policy creation by identity provider (IdP) for DNS filtering only	<p><i>All of the below supported across all plans:</i></p> <ul style="list-style-type: none"> • Corporate SSOs (Microsoft Entra, Google Workspace, Okta, PingIdentity, and more); • Social IdPs (Github, LinkedIn, and more); • Open Source (OIDC, SAML 2.0) 	<p>Microsoft Entra, Okta, or manual import with Cisco Umbrella DNS plans.</p> <p>Additional IdPs supported with Cisco Umbrella SIG plans.</p>
Dedicated / reserved IPs	Available as add-on	Available as add-on
Network scale		
Anycast network footprint	330+ cities in 120+ countries	45 cities in 25 countries
All services running in all network locations	✓	✗
Traffic acceleration via a private backbone	✓	✗
SSE / SASE platform		
SWG with integrated CASB, DLP, & RBI	✓	✓
Full suite of SSE services (including ZTNA)	✓	Available with Cisco Secure Access
Unified management interface and platform for DNS filtering and SSE	✓	✗
One API for all services	✓	✗