CLOUDFLARE®

Approachable and affordable DNS security

Replace Cisco Umbrella's DNS security services with Cloudflare's global network — built for performance — and pay nothing until your contract expires.*

Challenge with Cisco Umbrella

With Umbrella, your organization is probably paying for capabilities that you don't really need. Even if you prefer 'set-and-forget' DNS policymaking, your admins will need to adapt their approach over time to accommodate new users, devices, and threats.

Cloudflare for DNS security

Cloudflare Gateway delivers the same rigorous security, high speed, and simple management that you expect from cloud-native DNS security solutions like Cisco Umbrella.

Cloudflare capabilities

Block harmful destinations with ransomware, phishing, and more

Both Gateway and Umbrella ingest best-in-class lists of risky domains and generate proprietary threat intelligence on over 600B recursive DNS queries per day.

With this visibility, Cloudflare particularly excels at identifying suspicious 'new' and 'newly seen' domains with our own machine learning models.

Speed and reliability around the globe with 100% uptime

Neither Gateway nor Umbrella have ever experienced outages in their DNS security services.

But only Cloudflare Gateway is built off of the world's fastest public DNS resolver (1.1.1.1).

Plus, Cloudflare stands behind a 100% uptime SLA across our 250+ cities in 100+ countries.

One policy manager, one device client, one unified experience

In Gateway, admins can set DNS security policies with a few clicks from a single dashboard. Our single device client can be flexibly deployed across different operating systems.

Unlike with Cisco's multi-product portfolio, you continue using Cloudflare's single dashboard and single client across new services and Zero Trust use cases.

Limited-time offer

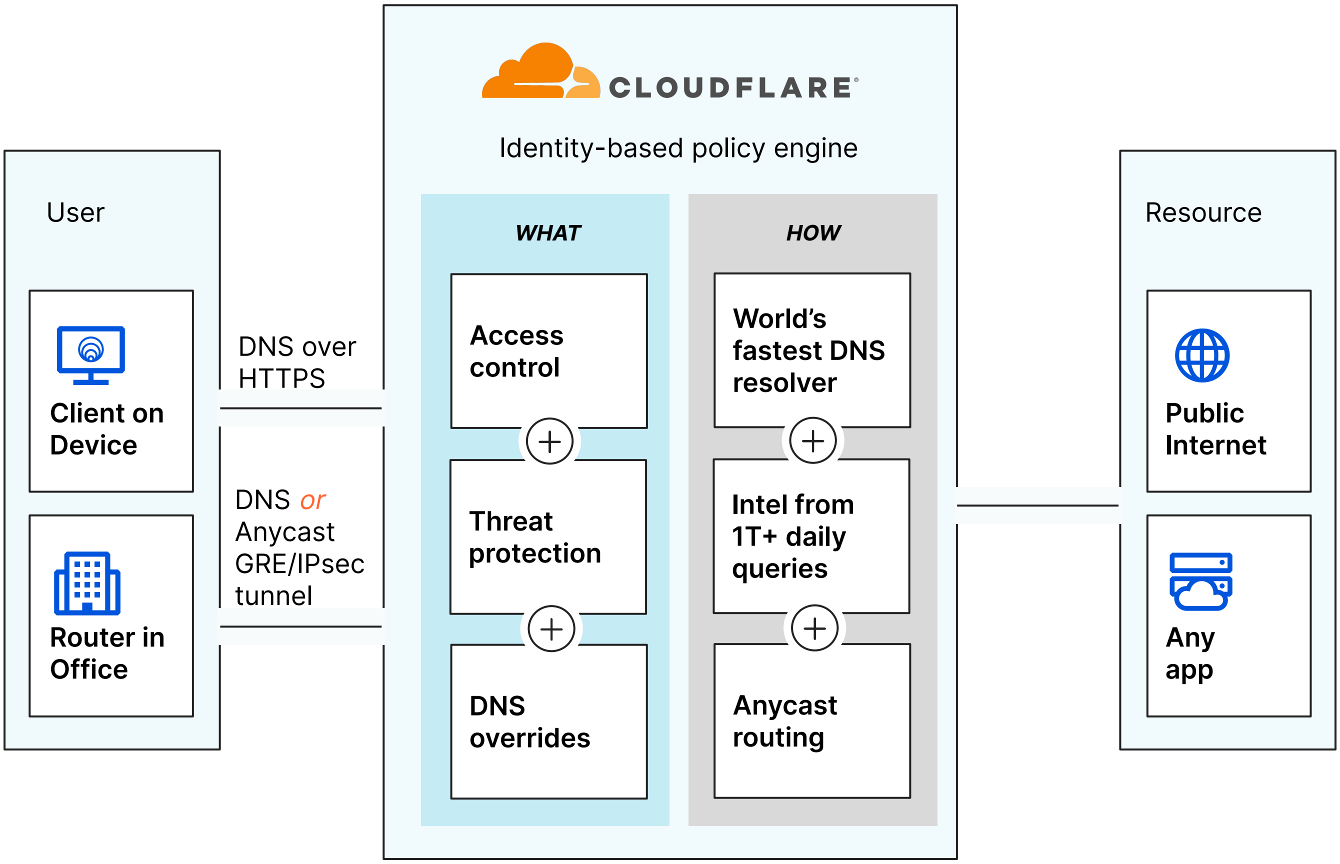
If you currently use Cisco Umbrella's DNS security services,* swap in Cloudflare Gateway today.

For a limited time...start a Gateway subscription at no charge until the expiration of your current Umbrella contract for up to 12 months. After this 'promotional period,' we will aim to beat the price you are paying Cisco for the paid period of the subscription. Additional terms and conditions apply.*

How it works

Today, Cloudflare Gateway is commonly used to protect remote workers and office locations with encrypted DNS security.

Users send an encrypted query to Cloudflare. We decrypt and check the query against policies to block, allow, or override it before resolving the domain.



*Terms and conditions of the current promotion

To take advantage of this promotion, you must purchase Cloudflare Gateway from Cloudflare by 31 March 2022. You must agree to Cloudflare's standard Enterprise Subscription Agreement and to a 12-month minimum term following the expiration of your current contract. Expiration of your current contract is the earliest date at which you can terminate your contract with a minimal or no fee. The price beat does not apply to any introductory or promotional price of competitors'. The no charge period cannot exceed 12 months. Other usage limits may apply.

You are only eligible for this promotion if your existing contract is with Cisco for DNS Security Essentials, DNS Security Advantage, or their equivalent legacy Umbrella packages - Professional and Insights. Your participation in this promotion is at Cloudflare's sole discretion. Cloudflare reserves the right to discontinue this promotion at any time.

Feature comparison

(as of 01 February 2022)

	Cisco Umbrella DNS	Cloudflare Gateway
Threat protection		
600B+ recursive DNS queries per day to inform threat intelligence	✓	✓
Block domain requests and IP responses per 13 security risks	✓	✓
Block direct-to-IP traffic for C2 callbacks that bypass DNS	Depends on plan	✓
Antivirus scanning	Selectively applied, depending on plan	✓ All the time in all plans
Network scale		
Anycast network footprint	37 locations in 23 countries Anycast IPsec does not apply to all locations.	250+ locations in 100+ countries Anycast IPsec in all locations
Public DNS resolver	✓ 208.67.222.222	✓ 1.1.1.1 Ranked the fastest consistently by third parties
Uptime SLA	99.999%	100%
All services running in all data centers	✗	✓
Consistent policy creation		
Category-based filtering	✓	✓
Custom block pages and bypass options	✓	✓
Allow list-only	✓	✓
User attribution and policy creation by identity provider	✓ Integrations with: • Microsoft Active Directory included in DNS-forwarding packages • Other identity providers available in higher-tier packages, but not available to DNS forwarding services only	✓ Integrations with: • Corporate SSOs (Microsoft Active Directory, Okta, OneLogin, Ping Identity, and more) • Social identities (GitHub, LinkedIn) • Open Source (OIDC, SAML 2.0)
Overrides (respond to all DNS queries for a given domain to another destination)	✗	✓
Policies based on regular expressions	✗	✓
Administration and management		
Automation support with Terraform	✗	✓
Mobile device client	Apple or Android (Managed enrollment only)	Apple or Android (Managed and self-enrollment)
Desktop (roaming) device client	Mac, Windows, Chrome OS	Mac, Windows, Chrome OS, Linux
On-prem DNS forwarder virtual appliance	✓	✗
DNS log retention	30 days	6 months
Log export to cloud storage	AWS S3 or Cisco-managed S3 bucket	AWS S3, Google Cloud Storage, Microsoft Azure Blob Storage, and more
Multi-org console add-on	✓	✗

Simplify your Zero Trust journey with Cloudflare

Switching to Cloudflare Gateway today for DNS security can streamline your longer term Zero Trust adoption.

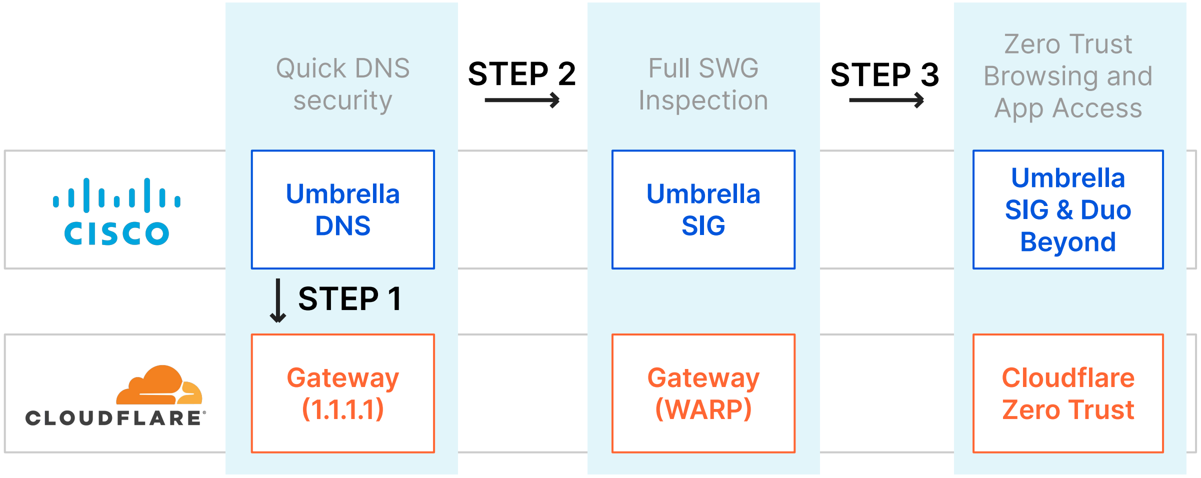
Cloudflare brings together many once-distinct security services into a unified platform, called Cloudflare Zero Trust.

With Cloudflare, leveling up security with equivalent solutions should be easier and more cost-efficient than with Cisco.

Key comparison

- Our Secure Web Gateway, Zero Trust Network Access, and Browser Isolation solutions are natively integrated and built on the same developer platform run on Cloudflare's network.
- By contrast, Cisco's "acquire-and-stitch" approach will have your admins switching between multiple interfaces across their standalone SWG and ZTNA solutions and weaving an overly complex web of inconsistent policies over time.

Implementation Roadmap



	Quick DNS security	Full SWG Inspection	Zero Trust Browsing and App Access
CISCO	Umbrella DNS	Umbrella SIG	Umbrella SIG & Duo Beyond
CLOUDFLARE	Gateway (1.1.1.1)	Gateway (WARP)	Cloudflare Zero Trust

Step 1

Security, performance, and ease of use with Cloudflare:

- The world's fastest, privacy-first DNS resolver (1.1.1.1)
- Reliable Anycast network across 250+ cities
- 600B+ recursive daily DNS queries feeding threat intel

Step 2

Cisco
- Slower migration
- Expensive upgrade
- Runs in limited locations

vs. Cloudflare
- No migration, activate in minutes
- No additional cost
- Runs in all locations

Step 3

Cisco
- Different UI / API
- Different device client
- Mostly on-prem

vs. Cloudflare
- Same UI / API
- Same device client
- Cloud-delivered

Contact us today to request your one-on-one engagement with a Cloudflare solution specialist.