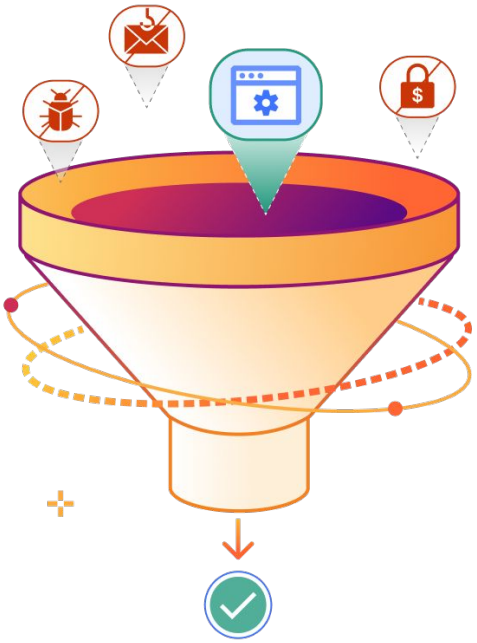
DNS Filtering

Cloudflare Gateway filters web activity across your office and remote users to mitigate risks and safeguard your organization reputation.



Cloud-native DNS filtering

With Cloudflare Gateway's DNS filtering, restrict access to dangerous or inappropriate web content.

Scale consistent, cloud-native protections and visibility across your workforce and simplify how you:

- **Block Internet risks** like malware infections, ransomware, phishing, and more
- **Enforce acceptable use policies** and secure guest WiFi
- **Enable productivity** with simple, 'set & forget' policies and high-speed enforcement

Replace legacy tools, modernize your threat defense

Stop backhauling Internet-bound traffic through slow, inefficient appliances. Instead, switch to Cloudflare for DNS filtering for quick time-to-value, and over time, layer more granular inspections and controls to reduce risks across web and cloud environments.

DNS filtering today, Zero Trust and SSE tomorrow

Modernizing DNS filtering is a common early step towards Zero Trust adoption and consolidation with a security service edge (SSE) architecture.

Why Cloudflare?

Simple & flexible deployments

Multiple

deployment modes for office and remote users both with and without a device client, so you can get started faster with less operational overhead.

Fast & consistent enforcement

330+

network locations in 120+ countries. DNS filtering runs with high-speed, single-pass inspection close to users, wherever they are.

Mass scale threat intelligence

3+ Trillion

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

Use case: DNS filtering for threat protection

Mitigate web & cloud risks

Block domains with comprehensive coverage of ransomware, phishing, DGA domains, DNS tunneling, new & newly seen domains, C2 & botnet, and other online risks.

Even block access to unauthorized SaaS and cloud destinations to mitigate the risks of shadow IT.

Simplify security operations

Decrease manual effort with built-in threat intelligence that automatically blocks new risks and helps reduce mean times to detect (MTTD) and respond (MTTR).

Automate workflows like policy setup and onboarding to embrace a 'set and forget' approach to configuration.

Getting started

Offices / locations	Point network routers to Cloudflare for DNS resolution. (No device client needed.)	Set up location-based DNS filtering policies.	Apply network policies to L3 traffic sent via GRE/IPsec tunnels, your SD-WAN, or Cloudflare's WAN connector.
Remote users	Filter DNS over HTTPS (DoH) requests using a user-specific authentication token and without a device client.	Deploy device client (managed/self-enrollment) for DNS filtering and visibility per device.	Layer more granular controls including HTTP, network, and browser isolation rules.

As you progress, learn about full secure web gateway (SWG) functionality.

Related use case: Enforce acceptable use policy (AUP)

Comply with AUP and secure guest WiFi

Block harmful and unwanted content (e.g. adult, gambling) to support compliance with your AUP.

Also filter to mitigate risks on guest WiFi networks across retail, hospitality, education, public spaces, and other locations with visitors.

Get started with location-based DNS filtering without deploying any software to endpoints.

Customer impacts

Enterprise

FORTUNE 500

Learn more

100K+

hybrid workers protected.

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

Cloudflare's own deployment

CLOUDFLARE Learn more

Phased rollout

1. Set up office location filtering within days
2. Remote user filtering within a year
3. Granular HTTP(S) inspection
4. Selective isolation of Internet browsing
5. Geography-based logging

Digital natives

bouvet

Scandinavian IT 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

Learn more

korzinka

Uzbekistan retail supermarkets

"Cloudflare's web and email security helps us stop phishing across multiple channels and mitigates many of our top security concerns around financial and data theft"

— Alexandr Zorin, CISO

Learn more

Public sector & education

Department of Homeland Security — 20 Years

100+

Learn more

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

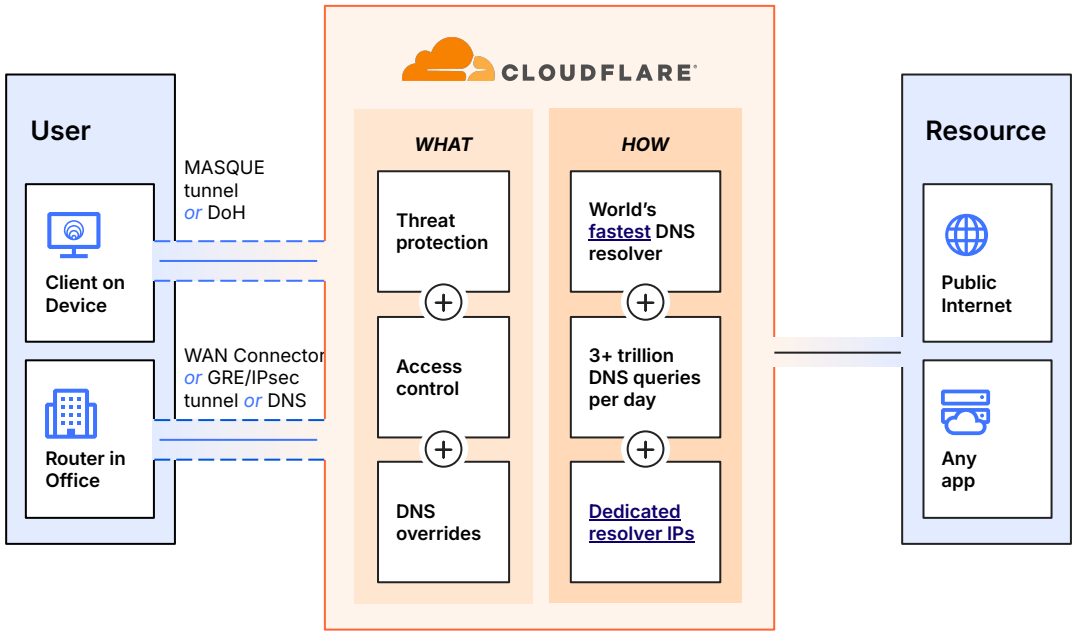
seine 77 &marne LE DÉPARTEMENT

129

Learn more

state-run schools
with guest WiFi protected with Cloudflare's DNS filtering

How it works: DNS filtering within Cloudflare's Secure Web Gateway (SWG)



Configuring policies

Allow / block / override domains and IP addresses by security or content category or application type.

Set policies with time durations and based on schedules.

Manage via our Tenant API for parent-child configurability.

Threat intelligence

- Proprietary AI/ML threat hunting models based on 3T+ DNS queries per day detect algorithmically-generated domains and DNS tunneling techniques.
- 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, such as private network services and internal applications.
- Custom threat feeds and signatures (IPs, URLs, and domains, etc.) are supported

Simplify and accelerate your security projects

After starting with DNS filtering, many organizations extend Cloudflare's visibility and controls across additional web, SaaS, and private app environments. Cloudflare's Zero Trust / SSE services are natively-integrated and composable, so you progress with agility on projects such as:

Securing web & cloud access

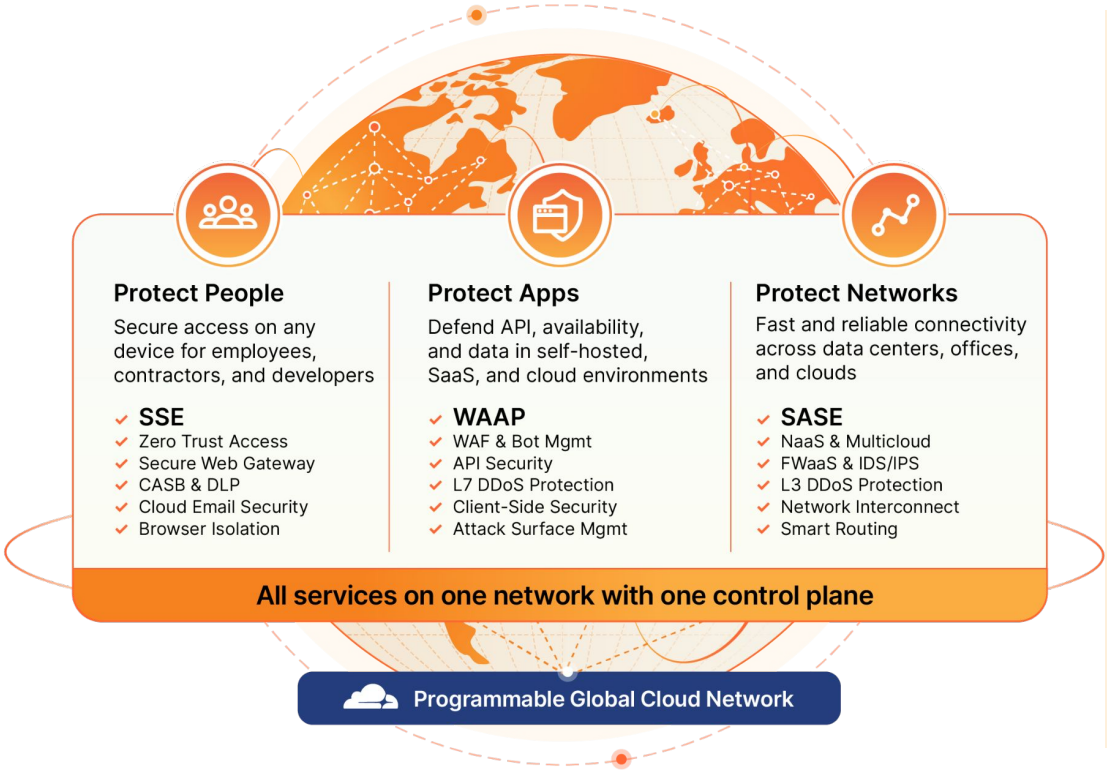
- Insulate local devices from malware with RBI
- Prevent data leaks with DLP detections
- Isolate apps to control data movement within
- Manage shadow IT, including genAI apps

Adopting Zero Trust for apps / VPN replacement

- Streamline contractor / 3rd party access
- Secure developer / privileged access
- Enforce phishing-resistant MFA
- Simplify ITOps for joiners / leavers

The Cloudflare cybersecurity portfolio

Unify your security approach with security services edge (SSE) including email security, web app and API protection (WAAP), and many more domains. Adopt new capabilities at your own pace.



Simplify security
Consolidate vendors to reduce complexity and enterprise risk.

See more, protect more
Leverage real-time threat intelligence and risk posture from a massive global network to protect more enterprise data.

Scale everywhere
Resilient protections across any location around the world.

Modernize your cybersecurity approach

Request a workshop

CLOUDFLARE