CLOUDFLARE

SOLUTION BRIEF

Protective DNS: Threat defense for the public sector

Filter web content across locations and remote users to stop threats and enforce compliance.

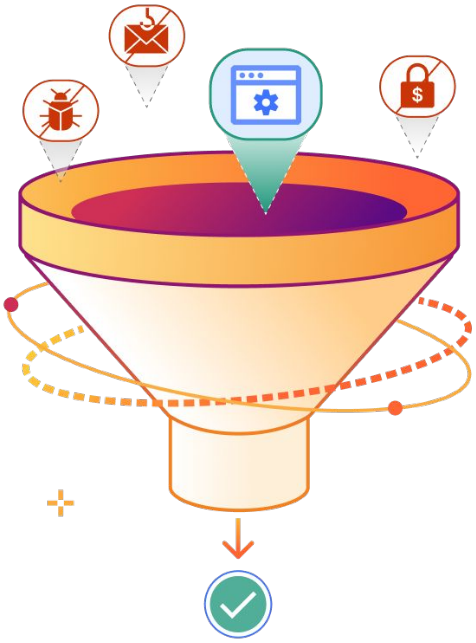
Simple & effective web security

With Cloudflare's protective DNS (PDNS), prevent users from ever reaching known malicious or inappropriate domains and/or IP addresses.

Benefits:

- **Block Internet threats** like malware infections, ransomware, phishing, and more
- **Support compliance** with regulations, government directives, and standards
- **Enforce acceptable use policies** and filter content on guest WiFi
- **Encrypt all DNS requests** over HTTPS (DoH) or over TLS (DoT) for security & privacy
- **Replace legacy appliances** to lower costs and avoid inefficiencies of backhauling traffic

Scale PDNS across your organization for consistent protection and visibility with quick time-to-value.



High speed resolution — everywhere

Cloudflare's PDNS is built on one of the world's fastest and most reliable DNS resolvers (1.1.1.1.) to deliver seamless experiences for end users.

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.

Unmatched global scale

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 and IPs 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).

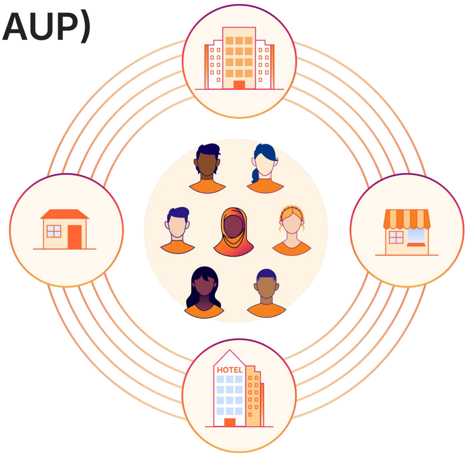
Automate workflows like policy setup and onboarding to embrace a ‘set and forget’ approach to configuration.

Getting started

Offices / locations	Point network routers to Cloudflare for DNS resolution. (No device client needed.)	Set up location-based protective DNS / filtering policies.	Apply network policies to L3 traffic sent from your own equipment,* your SD-WAN, or Cloudflare’s WAN connector over IPsec/GRE tunnels
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 filtering controls 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.

Filter web browsing to mitigate risks on guest WiFi networks across education, government agencies, and other civic locations with visitors.

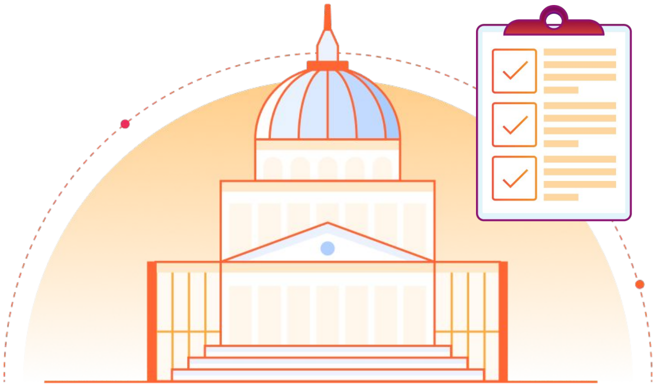
Protect offices and other locations without deploying any software to endpoints.

*With Cloudflare Network Interconnect, customers can connect their network infrastructure directly with Cloudflare rather than via the public Internet.

Use case: Enforce compliance with regulations & standards

Protective DNS helps public sector organizations meet legal requirements, government directives, and standards by:

- **Stopping threats** like malware, ransomware, phishing, command & control, and more
- **Protecting data** by mitigating risk of data breaches and preventing unauthorized access
- **Enabling Zero Trust best practices** by verifying traffic before reaching its destination
- **Supporting reporting & audit** with detailed logs



United States examples:

- NIST SP 800-53
- FISMA
- CISA directives
- Executive Order 14028 (2021)

Europe examples:

- Security measures to support GDPR
- NIS2 Directive
- EU Cybersecurity Act

International standards:

- ISO/IEC 27001 and 27035 for threat prevention & incident response
- SOC 2

Certifications & commitments

FedRAMP

Cloudflare achieved a **FedRAMP Moderate Authorized ATO** in 2022 for all services.

Learn more or View marketplace listing

Cloudflare signed CISA’s pledge as part of our commitment to industry-leading solutions that are secure by design and by default. Learn more

Customer impacts

Government

USA

100+

Learn more

Homeland Security

U.S. civilian agencies
with office locations secured with Cloudflare's protective DNS in partnership with Accenture.

"This [Cloudflare's DNS resolver] is a very reliable, very distributed, high availability service that also is capable of scaling and supporting a very large number of organizations with a very large number of users."

— Branko Bokan, lead architect, protective DNS at CISA (source)

United Kingdom

Partnership with

National Cyber Security Centre

Protective DNS to protect central and local government authorities, healthcare, emergency services, and more in England and the UK. 'PDNS for Schools' extends protections to schools.

Delivered in partnership with Accenture.

100+

UK organizations protected

£59M

Average annual losses prevented

Education

France

129

Learn more

seine & marne LE DÉPARTEMENT

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

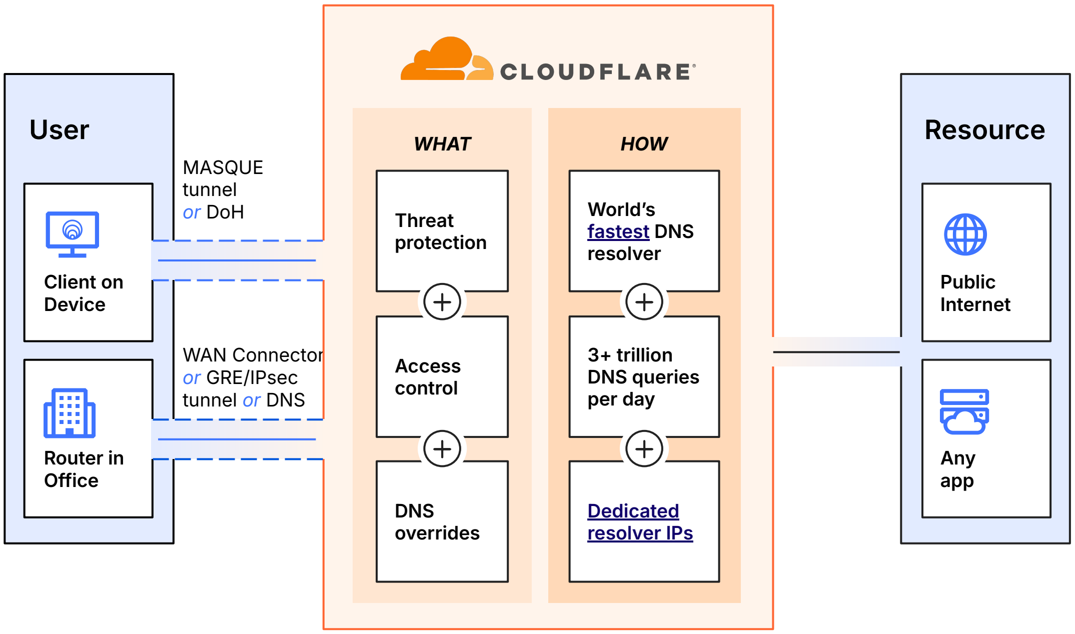
USA

THE WHITE HOUSE
WASHINGTON

120+

school districts in nearly 30 states with free access to Cloudflare's PNS via 'Project Cybersafe Schools', announced as part of White House initiative

How it works: PDNS 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.

Threat intelligence

- Proprietary AI/ML threat hunting models based on 3.6T+ 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

Global scalability & resilience

- 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

- Manage via our Tenant API for parent-child tiering of accounts and policies
- Automation support via Terraform
- One API across all Cloudflare services

Deploy with partners

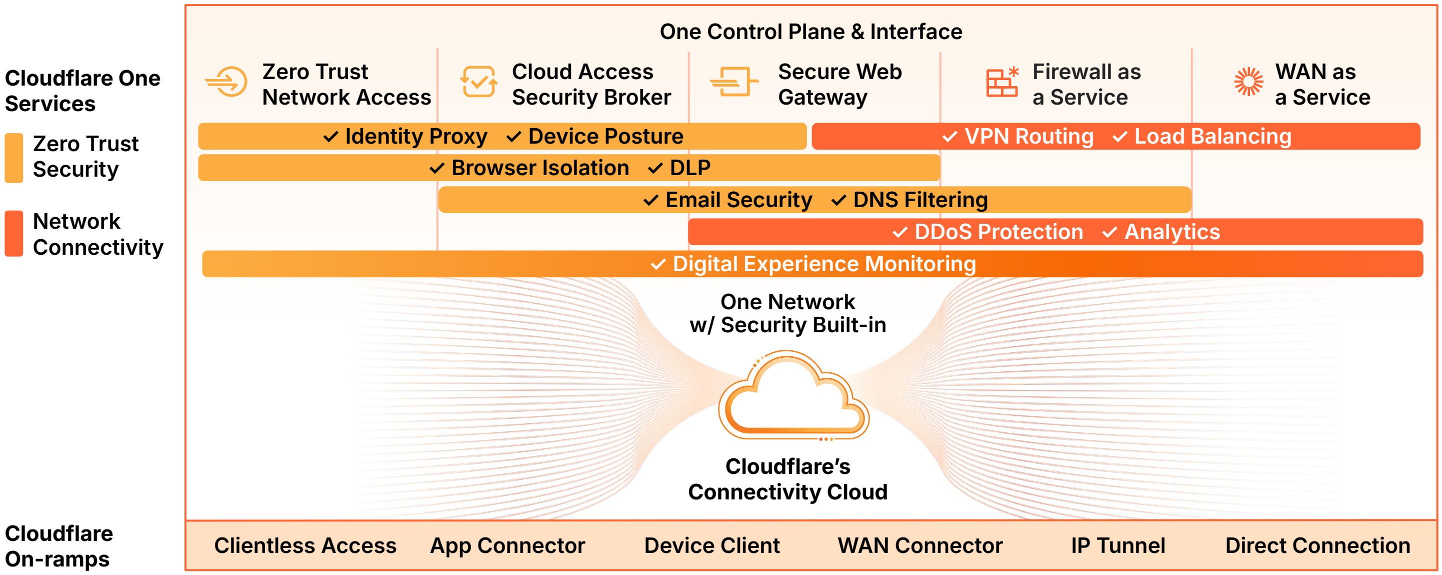
accenture kyndryl NTT

Work with our global ecosystem of

- Managed service providers
- Authorized delivery partners
- Global system integrators

PDNS today, Zero Trust & SASE tomorrow

After starting with Protective DNS, many organizations extend visibility and controls across web, SaaS, and private app environments with Cloudflare One, **our SASE platform**. All Cloudflare One services are natively-integrated and composable, so you can progress with agility on your Zero Trust security and network modernization projects.


One Control Plane & Interface
Cloudflare One Services
🟨 Zero Trust Security
🟥 Network Connectivity
Zero Trust Network Access
Cloud Access Security Broker
Secure Web Gateway
Firewall as a Service
WAN as a Service
✓ Identity Proxy ✓ Device Posture
✓ VPN Routing ✓ Load Balancing
✓ Browser Isolation ✓ DLP
✓ Email Security ✓ DNS Filtering
✓ DDoS Protection ✓ Analytics
✓ Digital Experience Monitoring
One Network w/ Security Built-in
Cloudflare's Connectivity Cloud
Cloudflare On-ramps
Clientless Access
App Connector
Device Client
WAN Connector
IP Tunnel
Direct Connection

Extend security on one unified platform & network control plane

Secure 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

Adopt Zero Trust for apps / VPN replacement

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

Request a consultation to get started