CLOUDFLARE

Cloudflare for Government

Comprehensive TIC 3.0 security capabilities, accelerated by Cloudflare's global backbone

Cloudflare is your trusted mission partner for TIC 3.0 and beyond. Our FedRAMP authorized connectivity cloud helps you meet TIC 3.0 objectives, advance your Zero Trust Architecture, and deliver better experiences for your workforce and the public.

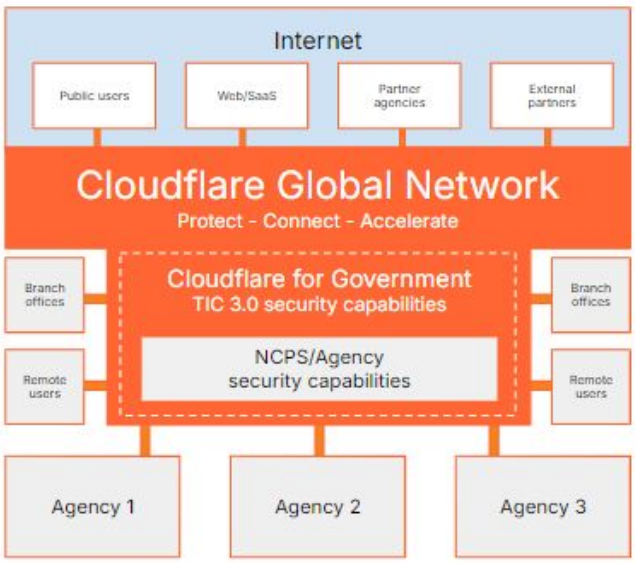
Before TIC, each agency managed its own internet connections and security stacks using a traditional network perimeter. This approach was insecure, inefficient, and adversely affected workforce productivity and digital service performance.

TIC 3.0 addresses these challenges, while enabling agencies to enhance security with modern Zero Trust architectures, benefit from cloud services, empower remote workforces, improve scalability and increase digital service resilience.

Cloudflare for Government delivers the modern, comprehensive security capabilities for every TIC 3.0 use case, accelerated by the power of the our global network. You'll be able to:

- **Protect** mission assets and data with modern TIC security capabilities in the cloud
- **Connect** everything and everyone with our high-performance, global backbone
- **Accelerate** TIC objectives while maturing your Zero Trust architecture

Cloudflare's modern TIC 3.0 architecture



How much time and effort does your agency exhaust on meeting TIC requirements?

With Cloudflare, you can:

- Access 32 TIC locations across 11 metro areas
- Turn day-to-day operations over to Cloudflare
- Have it all today

"The TIC initiative has evolved from simply reducing external network connections to protecting agency enterprise perimeters, mobile, and cloud connections with a focus on increasing the use of boundary protection capabilities to protect agency assets from an evolving threat landscape."

– TIC 3.0 Core Guidance Volume 1: Program Guidebook

Cloudflare is your mission partner for every TIC security objective

Manage Traffic

Cloudflare Application Services include WAF with API protection, rate limiting, smart routing and load balancing to help you observe, validate, filter, and control data connections

Protect Traffic Confidentiality

Cloudflare Zero Trust Services include Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG) and Data Loss Prevention (DLP) to limit help maintain the confidentiality of sensitive information.

Protect Traffic Integrity

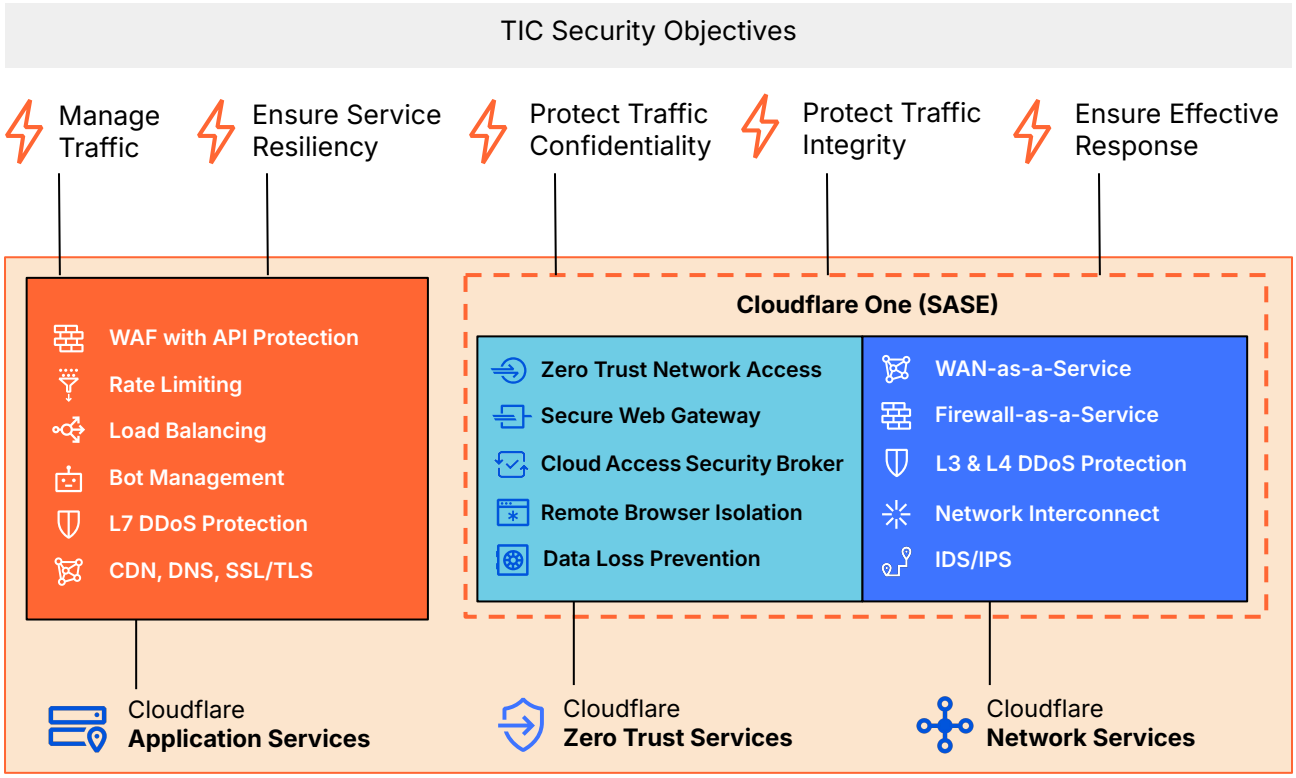
Cloudflare Network Services encrypt data in transit, and we're deploying post-quantum cryptography across our network today. Our Application Services offer SSL/TLS services to ensure integrity of web traffic.

Ensure Service Resiliency

Cloudflare Application Services promote resilience with application-layer DDoS protection and bot management capabilities to help ensure continuous availability despite growing attack sophistication.

Ensure Effective Response

Cloudflare's global threat intelligence helps identify and stop threats, and our Cloudflare anycast network defends against DDoS everywhere we provide services.

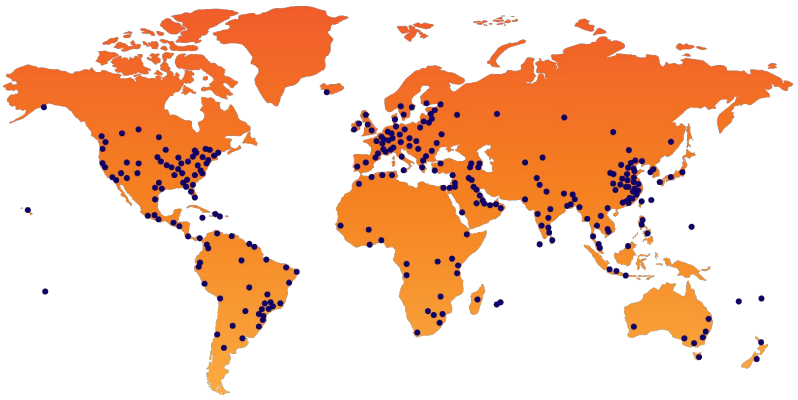


Cloudflare or Government's comprehensive application, Zero Trust, and Network services align with TIC Security Objectives.

The Cloudflare advantage over any other approach

Cloudflare Global Network

As one of the most interconnected networks, Cloudflare delivers local capabilities with global scale



32
FedRAMP data centers across 11 metro areas

330
cities in 120+ countries

12,500+
networks directly connect to Cloudflare, including every major ISP, cloud provider, and enterprise

296 Tbps
global network edge capacity, consisting of transit connections, peering and private network interconnects

~50 ms
from 95% of the world's Internet-connected population

150+
AI inference locations powered by GPUs

Cloudflare for Government

Our unique approach to FedRAMP authorized capabilities gives you maximum capability– everywhere

FedRAMP™

Every service at every location

No special FedRAMP enclaves that limits or delays the innovative capabilities you need

Single platform capabilities

Application and network services delivered consistently from our unified platform

Direct network connections

Connect your data centers directly to the Cloudflare's network for maximum performance and security

Cloudflare Universal Advantages

As the world's first connectivity cloud, Cloudflare delivers differentiated capabilities that millions of customers depend on

Significant Cost Savings

Vendor consolidation
CapEx offload
Administration

Threat Intelligence

Extensive visibility
Threat models
Intercepted attacks

Data Localization

Data restriction
Regulatory compliance
End user privacy

Simplicity and Ease of Use

Dashboard
Integrations
Automation

Cloudflare for Government TIC Security Capabilities

Cloudflare for Government covers a wide range of TIC security capabilities across all use cases. The tables below offer a high-level view some of our service mappings, but please see our detailed whitepaper for the comprehensive mapping that follows the TIC 3.0 Overlays Handbook standards.

Universal Security Capabilities

Enterprise-level security capabilities that outline guiding principles for TIC use cases.

Security Capability	Cloudflare Services
Resilience (3.UNI.RESIL)	All Cloudflare for Government services
Enterprise Threat Intelligence (3.UNI.ETINT)	All Cloudflare for Government services
Situational Awareness (3.UNI.SAWAR)	API Gateway, Bot Mgmt, DDoS, WAF
Dynamic Threat Discovery (3.UNI.DTDIS)	API Gateway, Bot Mgmt, DDoS, WAF
Con Mon Reporting (3.UNL.CMREP)	All Cloudflare for Government services
Governance & Policy Auditing (3.UNL.GPAUD)	All Cloudflare for Government services

Policy Enforcement Point (PEP) Security Capabilities

Network-level security capabilities that inform technical implementation for relevant use cases.

Security Capability	Cloudflare Services
Anti-malware (3.PEP.FI.AMALW)	Gateway, Uploaded Content Scanning, Security Center
Data Loss Prevention (3.PEP.FI.DLPRE)	Gateway, CASB, API gateway, WAF, Sens. Data Detection
Break and Inspect (3.PEP.WE.BINSP)	Gateway, Spectrum, SSL/TLS, WAF
Domain Resolution Filtering (3.PEP.WE.DRESF)	Gateway
Network Segmentation (3.PEP.NE.NSEGM)	Tunnel, WARP Connector, Gateway, Magic Firewall
DDoS Protections (3.PEP.RE.DDSPR)	Advanced DDoS, Magic Transit, Rate Limiting, Spectrum, WAF

Please see the Cloudflare Overlay Guidance white paper for a comprehensive mapping

Cloudflare for Government helps you secure federal data, networks, and boundaries while providing visibility into agency traffic, including cloud communications – the fundamental goals of the TIC 3.0 program.

Are you ready to protect, connect, and accelerate your TIC 3.0 architecture?

Learn more about Cloudflare for Public Sector, or contact us today.

1 888 99 FLARE | cloudflare.com/public-sector