CLOUDFLARE

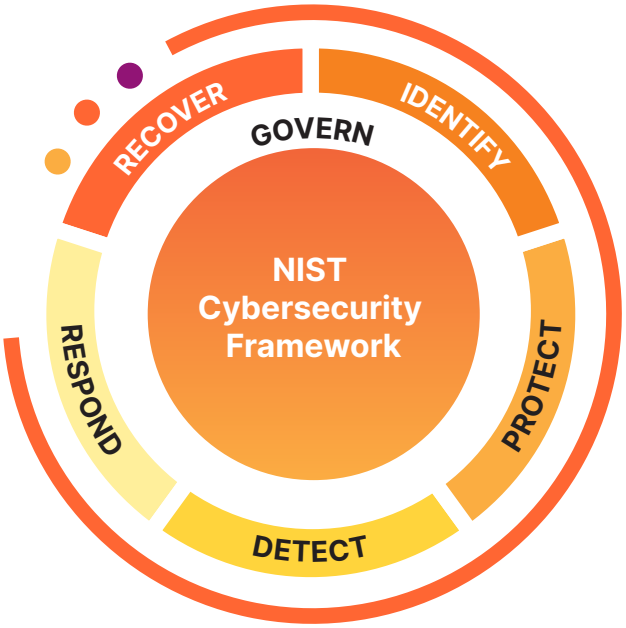
SOLUTION BRIEF

Cloudflare and NIST Cybersecurity Framework help you accomplish your public-sector cyber priorities

The NIST CSF helps you understand and improve cyber risk management

Every public sector organization is focused on its mission, and every mission depends on strong cybersecurity. The key is effectively and efficiently managing cyber risk, a major challenge that involves policy, people, process, and technology continually across the entire enterprise. Often, the first hurdle is deciding on a standard framework to guide the program, but many existing cyber risk management frameworks are complicated and cumbersome to adopt.

The National Institute of Standards and Technology (NIST) recognized that challenge and developed the Cybersecurity Framework (CSF). Rooted in cyber best practices, yet simple and easy to follow, the NIST CSF has a proven record of helping organizations of all sizes measure, organize, and communicate cyber risk strategies. Organizations that adopt the NIST CSF make better, risk-informed investment decisions that strengthen their cyber postures with clear security outcomes.



Cloudflare helps you accomplish your NIST CSF goals

While much of the NIST CSF covers policy, people, and process, there's no escaping the need for modern security technology. Therefore, public sector organizations need technology partners to help them accomplish their goals. However, it's often difficult for them to understand vendor offerings in the context of the NIST CSF without additional help.

At Cloudflare, we understand the power of the NIST CSF, and we're your trusted partner to help achieve the CSF's outcomes efficiently and effectively. With clear capability alignments to the CSF, we make it easy to understand how we protect and accelerate public sector missions while improving resilience and responsiveness for your workforce, mission partners, and the people you serve. Additionally, because no vendor covers everything, Cloudflare is designed to integrate with what you already have — like identity providers or endpoint detection and response solutions — without the need for rip-and-replace.

Partner with Cloudflare to boost your cyber resilience

Here's how Cloudflare aligns with the NIST CSF's core functions:

Govern through effective strategy and oversight:

- Cloudflare helps achieve risk strategy expectations (CSF GV.OC) by improving availability, integrity, and confidentiality.
- Cloudflare helps with policy enforcement and compliance reporting (GV.PO), including data localization support to fulfill mandates related to regional data use and protection.

- Supply Chain risks (GV.SC) are addressed through Cloudflare support for vendor consolidation/ optimization. Today's security architectures are complex, so Cloudflare solutions provide extensive security capabilities to work with the solutions you already have — or are consolidating with.

Identify what matters:

- Manage knowledge about agency assets (ID.AM) through Cloudflare Security Center, tracking known systems and services while alerting about possible rogue devices.
- Assess and treat risk (ID.RA) by managing threats against public-facing applications and vulnerabilities with Cloudflare application services, including Coudflare Web Application Firewall (WAF) and distributed denial-of-service (DDoS) protection.
- Cloudforce One's embedded team of world-class threat researchers analyze intelligence pulled from Cloudflare's global network — one of the largest and most interconnected networks in the world.

Protect against and Detect vulnerabilities and threats, now and in the future:

- Improve human factors by increasing awareness (PR.AT) of known attack patterns. Cloudflare provides security architects and analysts with clear documentation, educational videos, and webinars to maximize the benefits of Cloudflare services.
- Authentication and authorization (PR.AA) are key elements of the CSF, and Cloudflare's integration with enterprise identity management solutions ensures use of strong authentication. Security Service Edge (SSE) and Secure Access Service Edge (SASE) help organizations fulfill outcomes related to access permissions, entitlements, and authorizations. In fact, Cloudflare was named an industry leader in the 2024 Gartner® Magic Quadrant™ for SSE.
- Cloudflare Network Services encrypts data to protect it in transit across our global backbone network, ensuring data security (PR.DS) is managed consistent with the organization's risk strategy. Be ready for tomorrow's challenges with NIST-compliant post-quantum cryptography for the quantum computing world of the future.
- Cloudflare's SOC-as-a-Service monitors (DE.CM) for security threats and potential operational disruptions, performs deep analysis to identify attack vectors, and helps deploy countermeasures. Cloudflare's emergency hotline is there to help you respond to DDoS, ransomware, identity or access, network, web, and application attacks. Key products include the Cloudflare WAF, sensitive data detection, and API Gateway alerts on web applications or API responses containing sensitive data.

Respond (RS) with effective actions regarding a detected cybersecurity incident, including actions to Recover (RC) important assets and operations affected:

- Logs of all network data (e.g., through Magic Firewall, WAF, and Security Analytics) that occur across the connectivity cloud edge assist in the remediation of malicious activity and rapid, effective recovery. Research has shown as much as a 75% improvement in response.

Are you ready to effectively manage risk with the NIST Cybersecurity Framework?

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

1. See https://blog.cloudflare.com/cloudflare-sse-gartner-magic-quadrant-2024/

REV:BDES-7063.2025FEB04