INFOGRAPHIC

Is your government agency's network safe from DDoS attacks?

A distributed denial of service (DDoS) attack can cause significant disruption to the network, applications or services your government agency relies on. This can adversely affect your operational capabilities, in addition to being potentially costly and impacting the public trust. Yet, many government leaders are unprepared to address cybersecurity threats.

Government is a popular hacker target

2,286

The number of weekly cyberattacks experienced by the average government entity in 2024.[1]

43%

The increase in the number of weekly cyberattacks experienced by the average government organization from 2023 to 2024.[2]

DDoS threats are expanding

Today's large-scale DDoS attacks are designed to flood and overwhelm your internet connectivity, preventing access to online resources for staff and citizens. Cybercriminals exploit agencies with limited cybersecurity budgets, a shortage of dedicated cybersecurity staff and outdated security technologies.

203%

The increase in network-layer DDoS attack volume experienced by governments from 2023 to 2024.[3]

>20%

The percentage of hacktivist DDoS attacks targeting government in 2024, the most of any industry.[4]

Goals of attacks on government agency networks

- Extort agencies for a ransom to stop the attack.
- Interrupt time-sensitive data collection and distribution.
- Disrupt scheduled activities or cause chaos.
- Overload a network and prevent access to government resources.
- Hinder online collaboration among government staff.
- Prove it can be done, which is easy when an agency's network lacks protection.

$6,130 Average cost of an application-layer DDoS attack per minute.[5]

Reasons DDoS attacks are on the rise in government

More unsecured connected devices makes it easy to launch attacks.

Disruptions in critical government services gain widespread news coverage and provide desired notoriety for attackers.

The proliferation of Internet of Things (IoT) devices has expanded governments' attack surface.

Inadequate resources complicate an agency's ability to fend off attacks.

Easy access to affordable DDoS tools and instructions online simplifies attacks.

$30 a month

The cost of a subscription for DDoS attack-for-hire tools on the dark web.[6]

174%

The increase, noted by one platform in a single month in 2024, in the use of botnets, a key component of many DDoS attacks.[7]

Implement a security strategy that includes DDoS protection

To prevent disruptions to your network and safeguard your agency, DDoS mitigation measures need to thwart attackers and prevent downtime. An ideal solution will:

Monitor and evaluate
Offer intelligent monitoring and comprehensive traffic evaluation that uses advanced analytics to identify anomalies.

Provide fast resolution
Quickly and proactively detect, redirect and mitigate malicious traffic, minimizing the impact of attacks.

Scale with needs
Easily and seamlessly expand the solution as the demands of your agency change.

Offer continuous support
Provide always-available network and security expertise for swift issue resolution.

80% The percentage of state and local government organizations — including some that have over 10,000 total staff — that have fewer than five dedicated cybersecurity employees.[8]

Be prepared and don't go it alone. A network service provider is uniquely positioned to provide the DDoS protection you need.

Discover how DDoS Protection from Spectrum Business® can help protect your network.

Learn more

1. "The State of Cyber Security 2025," Check Point Research, 2025.
2. Ibid.
3. "2025 Global Threat Analysis Report," Radware, 2025.
4. Ibid.
5. "Application Security in a Multi-Cloud World 2023," Radware, November 8, 2023.
6. Michael Hill, "DDoS Attack-for-Hire Services Thriving on Dark Web and Cyber Criminal Forums," Cyber Security Hub, December 4, 2023.
7. "Cyber Threat Trends Report: From Trojan Takeovers to Ransomware Roulette," Cisco, June 2024.
8. "Nationwide Cybersecurity Review: 2023 Summary Report," Center for Internet Security, September 27, 2024.

SE-MSGV-IG004

Spectrum BUSINESS®