INFOGRAPHIC

How to protect your government network from cyber threats

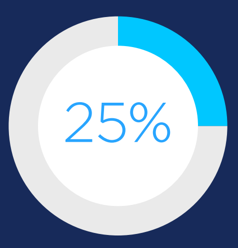
State and local governments are under pressure to provide easy and convenient digital data access to citizens. However, as exposure increases and threats evolve, governments are increasingly challenged to safeguard their sensitive information.

Understand why government networks are at risk

Data housed on government networks is a favorite target of cybercriminals. Challenges for IT leaders include:[1]

- Unsecure legacy systems.
- Lack of resources.
- Lack of cybersecurity expertise.

Attacks can have devastating results and require immediate action



of attacks on government agencies attempt to access potentially sensitive data.[2]

79%

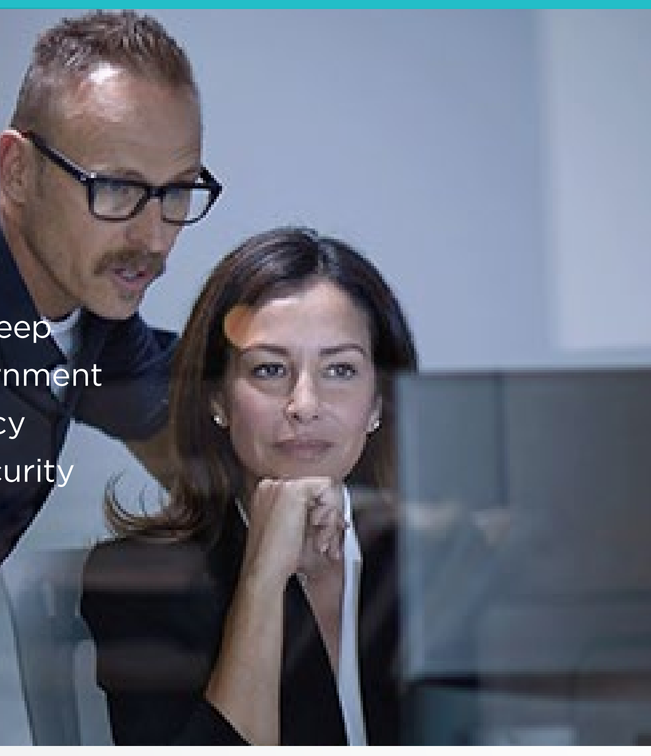
increase in the cost of public-sector data breaches in 2021.[3]

Track the evolving threat profile

To protect your organization, it pays to understand the most prevalent types of cyberattacks threatening state and local governments.

- **Malware:** The FBI reports that cybercriminals are gaining access to government networks with increasingly sophisticated email scams to insert malware.[4]
- **Email spoofing:** Masquerading as software as a service (SaaS) companies, cybercriminals use email spoofing to steal credentials and gain access to sensitive information.
- **Advanced persistent threats (APTs):** APTs attack a network and mine data over time without an organization even knowing what's happening, sometimes taking over an entire network in a few hours.
- **Distributed denial of service (DDoS) attacks:** DDoS attacks can flood a network to bring it down and can also happen in small bursts of malicious content through seemingly innocent activities like group chats.

Find comprehensive coverage and support



Widespread, coordinated network protection can keep you one step ahead of evolving and growing government network threats. Learn how to protect your agency and citizens and what to look for in a network security provider in our government cybersecurity guide.

Get the guide

Sources

1. "The Future State CIO: How the Role Will Drive Innovation," NASCIO, 2020.
2. Limor Kessem, "Threat Actors' Most Targeted Industries in 2020: Finance, Manufacturing and Energy," Security Intelligence, March 31, 2021.
3. "Cost of a Data Breach Report 2021," IBM Security, 2021.
4. "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure and Private Sector Organizations," Cybersecurity & Infrastructure Security Agency, April 15, 2021.

Spectrum ENTERPRISE