INFOGRAPHIC

Protect your government network from cyberthreats

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 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:

Evolving threats
with **82%** of government decision-makers concerned about cyberattacks becoming more sophisticated due to AI.[1]

Sensitive data
with **68%** of state governments identifying improving data security and privacy measures as a key priority driving updates to the constituent experience.[2]

Limited resources
with **over half** of government agencies citing reducing costs as a top priority through 2030.[3]

Attacks are becoming more frequent and more damaging

44 U.S. states experienced major cyberattacks on state and local government agencies from January through October 2025.[4]

1.5M Number of records affected by ransomware attacks on government agencies in 2024.[5]

Track the evolving threat profile

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

- ☑ **Social engineering**
  Phishing attacks have become widespread, with attackers often impersonating legitimate entities to steal data or plant malware through malicious files or downloads.
- ☑ **AI-powered cyberthreats**
  AI is being used to create automated attacks that are difficult to detect and thwart. Nearly 80% of IT decision-makers in state and local governments are concerned about AI cybersecurity threats evolving faster than their agency can keep up with.[6]
- ☑ **Ransomware and other malware**
  The average ransom demanded from government agencies during ransomware attacks in 2024 was $2.3 million, with payments to attackers averaging $923,000.[7]
- ☑ **Distributed denial of service (DDoS) attacks**
  Efforts to overwhelm networks continue to grow in size and sophistication. Government agencies saw a 203% increase in network-layer DDoS attack volume from 2023 to 2024.[8]
- ☑ **Data breaches**
  Unauthorized access or use of confidential data remains a risk for government. The average cost of a data breach in the public sector was $2.86 million as of 2025.[9]

Know where you're vulnerable

Cyberattacks on state and local governments frequently target:

Sensitive records
Data breaches often expose personal information like Social Security numbers, driver's license data and tax information that can be sold on the dark web to facilitate identity theft.

Critical infrastructure
Ransomware can disable systems required for essential public services, including public safety, to extort state and local governments.

Payment systems
Criminals use social engineering and compromised credentials to facilitate fraudulent payments.

Find comprehensive coverage and support

Widespread, coordinated network protection can keep you one step ahead of evolving government network threats. Spectrum Business®, a Charter Communications brand, offers a complete set of managed services that can help protect your agency and the public while simplifying cybersecurity.

Learn more

---

1. Suzanne Vitale, "EY Government State and Local 2025 Survey Findings," EY, June 18, 2025.
2. "Constituent Experience: State Government IT Strategies," National Association of State Technology Directors, 2025.
3. "EY GPS 2025 Federal Trends Report," EY, 2025.
4. "Threat Snapshot: Cyber Threats Remain Heightened Amid Lapse in Information Sharing Authorities, Government Shutdown," House Committee on Homeland Security, October 31, 2025.
5. Rebecca Moody, "Ransomware Roundup: 2024 End-of-Year Report," Comparitech, January 9, 2025.
6. Vitale, "EY Government State and Local 2025 Survey Findings."
7. Moody, "Ransomware Roundup."
8. "2025 Global Threat Analysis Report," Radware, 2025.
9. "Cost of a Data Breach Report 2025: The AI Oversight Gap," Ponemon Institute and IBM Security, July 2025.

Spectrum BUSINESS®