A CENTER FOR DIGITAL GOVERNMENT ISSUE BRIEF | AT&T

The Business Case for Modernizing Network Security Infrastructure

How state and local governments can embrace stronger, more resilient technologies

In today's complex threat environment, it's not a question of whether your organization will be hit by a cyberattack, but when. For state and local governments, the best way to prepare is to modernize network infrastructure with new policies and technologies that tighten security and thwart cybercriminals.

Confronting Network Security Issues

Agencies often have years' worth of accumulated network infrastructure in need of modernization. Legacy firewalls, intrusion-detection systems, anti-virus software, network access controllers, virtual private networks (VPNs) and other infrastructure assets can't keep pace with the evolution of cyber threats.

The rise of hybrid cloud infrastructure also requires new thinking about network security. "The minute we started moving to cloud and multiple clouds, the game changed," says Deborah Snyder, a senior fellow with the Center for Digital Government (CDG) and former chief information security officer for New York state.

Too many state and local government networks have outdated, inflexible and insecure infrastructure, Snyder says. Agencies also grapple with:

- **Knowledge gaps.** Leaders have a hard time staying up to date on the technical knowledge and threat awareness they need.
- **Unique local factors.** Every jurisdiction is different, making all-in-one solutions impractical.
- **Inconsistency**. Local agencies' technologies may not mesh well with those of state or federal agencies.
- **Isolation.** Data, application and operational silos prevent collaboration within agencies and across departmental lines.

These issues hamstring agency leaders' ability to assess the likelihood of attack and the limitations of security policies and technologies.

The rise of cloud technology changed the game in network security.

Understanding Network Modernization

Network modernization means embracing cloud technologies and virtualized network equipment to improve scale and flexibility.

A modern network security strategy includes:

Zero-Trust Network Access (ZTNA). Zero Trust might seem like a buzzword, but it represents a fundamental shift in network security philosophy. ZTNA ensures every device, user and workload are consistently verified, and that users access only the applications, data and network areas they need to do their work.

Defense in depth. Multiple layers of defense go far beyond firewalls and VPNs to protect users, applications, devices and data. A defense-in-depth strategy adds protections behind the network security perimeter, and it lets agencies adopt a more proactive security approach.

Learning automation. Advanced artificial intelligence and machine learning (AI/ML) help discern the difference between proper and improper network behavior. If a member of your staff suddenly appears to be logging in from a foreign country, AI/ML controls automate the process of flagging a possible breach and setting the proper response in motion.

Business continuity. Modern redundancy and recovery technologies reduce the cost and impact of cyberattacks. "Modern network tools tend to be more resilient from a system standpoint," Snyder says. "They help you recover better from disruptions and minimize downtime."

Third-party expertise. Few government agencies have the resources to manage network security completely in house. Partner with network vendors that have extensive global experience managing cyber threats.

Network Modernization Best Practices

Fundamentals to embrace

- **Planning.** Assess your current network and define security objectives. Find a solution that aligns with your needs and develop a phased implementation strategy.
- **Change management.** Collaborate with key stakeholders to ensure training, monitoring and support.
- **User experience.** Strike a balance between ease of use and comprehensive protection.
- **Research.** Conduct due diligence on network security design, policy, processes and procedures.

Plan for compliance requirements from the start. "If you start by designing with compliance in mind, you're more likely to be compliant in the end," Snyder says.

Pitfalls to avoid

- Oversimplifying threat management.
- Taking the cheapest or easiest route.
- Second-guessing your plan along the way.

Also, understand the limits of AI/ML for threat detection. "It's pretty easy for a threat actor to manipulate AI training data," says Alex Souza, lead product marketing manager with AT&T Cybersecurity. Before training AI/ML models to detect normal and abnormal network behavior, make sure you have no undetected intruders in your network.

Ultimately, network security modernization protects critical data, safeguards essential government services and ensures data privacy. It can help streamline processes, improve regulatory compliance and enhance public trust in government.

But it really comes down to gaining visibility into your network and the potential threats to it, Souza says. "If you don't have insight into what's going on inside your network, it's hard to defend it."

Technology features to look for in a modern network:

- Redundancy to prevent domino effects from single points of failure.
- Up-to-date encryption standards and methodologies such as containerization, decryption and inspection of traffic.
- Access limitations that control for specific tasks, roles, data, applications and devices.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from AT&T.

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.
www.centerdigitalgov.com.

Sponsored by: AT&T

We simplify securing valuable business assets by providing broad cybersecurity experience and award-winning services for network security, extended detection and response, and endpoints. From traditional computing to edge computing, we're focused on business innovation. We help make complexity easy to understand and navigate.

By providing affordable, strategic services, our clients rely on us as trusted advisors. Our cybersecurity consulting is product neutral, so you get unbiased answers for your business. Our managed security services, threat awareness, and ground-breaking research are dedicated to help keep you protected today and prepared for tomorrow.

AT&T Cybersecurity manages the risk. You reap the reward.
www.att.com/publicsector

SHUTTERSTOCK.COM