

Modernize Government Security and Networking to Improve the Citizen Experience

How to modernize state and local government services to increase efficiency while protecting people and data



Overview

Use Cases

Why AT&T

Building the Government of the Future

Initiatives Driving Modernization

Top Challenges for CIOs

Performance and Security to Digitize Services

Modernize Government Services

Employ Advanced Threat Protection

Secure Remote Sites

Connect Smart Devices

Converged Cybersecurity and Networking



Building the Government of the Future

State and local governments are in a unique position when it comes to technology. Some agencies maintain legacy systems that are older than many of their employees, while others look to build the smart cities of the future powered by artificial intelligence (AI) and the internet of things (IoT). They must continually deliver crucial services to citizens while attempting to modernize and build a robust digital infrastructure.

No matter where you are in the modernization journey, you need fast and reliable connectivity between government services and citizens; between distributed offices and branches. Those connections must also be secure to protect the availability of services and critical infrastructure. Sensitive data that is a popular target of cyber criminals requires protection to maintain privacy and comply with regulations.

Modernization can be a tremendous challenge for governments with limited IT and cybersecurity expertise. However, the right solutions can speed transformation. In this eBook, we'll examine the initiatives driving technology modernization in state and local government, the challenges CIOs and CISOs face, and how reducing complexity through convergence of cybersecurity and networking will accelerate outcomes that improve citizen experiences and protect critical infrastructure. Through a series of use cases, you can explore multiple ways to bring people, data, and technology together.

Overview			Use Cases				Why AT&T	
Building the Government of the Future	Initiatives Driving Modernization	Top Challenges for CIOs	Performance and Security to Digitize Services	Modernize Government Services	Employ Advanced Threat Protection	Secure Remote Sites	Connect Smart Devices	Converged Cybersecurity and Networking

Initiatives Driving Technology Modernization

State and local governments are responsible for a variety of services that impact the everyday lives of every resident, which means keeping those services secure and available is critical. Therefore, it's not surprising that the number one priority for state CIOs in 2023 is cybersecurity and risk management.¹ They are also still focused on priorities that came to the forefront during COVID-19, including:

- 1. Increased attention on digital government services and citizen experience**
- 2. Increased investment in legacy modernization**
- 3. Investments in broadband expansion and adoption²**

1. ["State CIO Top Ten Policy and Technology Priorities for 2023,"](#) National Association of State Chief Information Officers, December 2022.
 2. ["The People Imperative: The 2022 State CIO Survey,"](#) National Association of State Chief Information Officers, October 2022.
 3. Lindsay McKenzie, ["Mayors urged to pounce on federal broadband grants,"](#) StateScoop, January 2023.



Integrated security

CIOs and CISOs are looking to improve governance, security frameworks, data protection, and training. Many agencies use siloed point products in their security strategy today that hamper visibility and response. A converged integrated platform approach will be more effective, but many government groups require assistance to make the transition successfully.



Digital transformation

Whether updating legacy systems that can include aging mainframes or improving the citizen experience through modern applications, government is moving slowly but surely to the cloud and solutions as a service. Many are also looking to adopt IoT devices to monitor infrastructure and increase operational efficiency. With the increasing digitization, government entities must prioritize cybersecurity and data privacy measures.



Broadband expansion

The Federal Internet for All program has provided grants to state governments to expand broadband coverage for citizens. Local government now needs to develop their grant applications to share in the funding.³ This will allow local government to pursue digital equity for their communities by assisting lower income residents access to high-speed internet.



Compliance reporting

Regulations around data privacy, data protection, and environmental standards are changing rapidly. California, Colorado, Connecticut, Utah, and Virginia have new state data privacy laws that take effect in 2023 that require not just compliance, but demonstration of that compliance. Unified reporting from converged cybersecurity and networking tools can reduce compliance efforts and create agility to comply with new privacy laws.

Overview

Use Cases

Why AT&T

Building the Government of the Future	Initiatives Driving Modernization	Top Challenges for CIOs	Performance and Security to Digitize Services	Modernize Government Services	Employ Advanced Threat Protection	Secure Remote Sites	Connect Smart Devices	Converged Cybersecurity and Networking
---------------------------------------	-----------------------------------	-------------------------	---	-------------------------------	-----------------------------------	---------------------	-----------------------	--

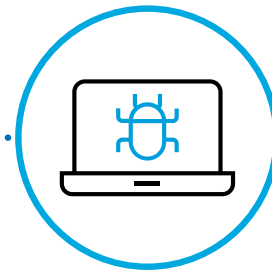
Top Challenges for State and Local Government CIOs

Government IT faces a mix of challenges, ranging from budgets that restrict both security resources and infrastructure modernization to being a frequent target of attackers. Here are some of the top challenges cited by government CIOs and CISOs:



Limited budgets

Sixty-three percent of local government IT leaders say their security budgets are insufficient to support their information security initiatives, and 61% of elected leaders are only “somewhat” engaged on cybersecurity issues. Only 39% of surveyed cities and counties have a CISO role to manage cybersecurity.¹ These limitations mean IT leaders must make careful decisions to maximize their budgets.



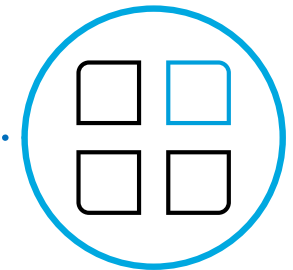
Increasing attacks

There were 353 reported ransomware attacks on state and local governments in the past five years, with likely many more unreported.² Recent targets for cyberattacks have included water treatment plants, hospitals, police departments, and other infrastructure. As the IT and OT environments become more complex and attacks become more sophisticated, resource-limited teams struggle to keep up.



Cybersecurity skills gap

This challenge is two-fold: both a lack of skilled cybersecurity personnel to protect infrastructure and limited cybersecurity awareness among the workforce, increasing risk. This is a challenge shared across industries, but budget restrictions make it even more difficult to attract and retain security talent in government.



Legacy infrastructure

Modern security tools weren’t built for legacy systems like mainframes, leaving those systems vulnerable to emerging threats. Legacy infrastructure is the number one barrier cited by state CISOs in 2022.³

1. Benjamin Freed, “[Local IT leaders still struggle to hold elected officials’ attention on cyber](#),” StateScoop, December 2022.

2. “[Ransomware Attacks Map](#),” StateScoop, accessed January 2023.

3. Srin Subramanian and Meredith Ward, “[2022 Deloitte-NASCIO Cybersecurity Study](#),” National Association of State Chief Information Officers, October 2022.

Overview				Use Cases				Why AT&T
Building the Government of the Future	Initiatives Driving Modernization	Top Challenges for CIOs	Performance and Security to Digitize Services	Modernize Government Services	Employ Advanced Threat Protection	Secure Remote Sites	Connect Smart Devices	Converged Cybersecurity and Networking

Combine Performance and Security to Digitize Government Services

To be better equipped to provide digital services for citizens and protect critical infrastructure, state and local governments need fast and secure connectivity and reliable digital infrastructure. Whether you choose to adopt technologies such as SD-WAN, fiber, or 5G, connections must protect personal and confidential data, be easy to manage, and be affordable to maximize taxpayer dollars.

State and local governments also need robust security solutions to stand up to sophisticated attacks, as the data and infrastructure they control is especially attractive to cyber criminals. Yet these solutions must also

work with limited IT budgets and personnel skillset. Experienced Managed Security Service Providers (MSSPs) can help identify, implement, and even manage the right mix of security products to effectively defend against ransomware and other attacks.

Let's uncover how converged cybersecurity and networking solutions can help you reduce complexity to protect sensitive data while improving the citizen experience and public engagement. The following four use cases demonstrate possible applications.



Modernize Government Services



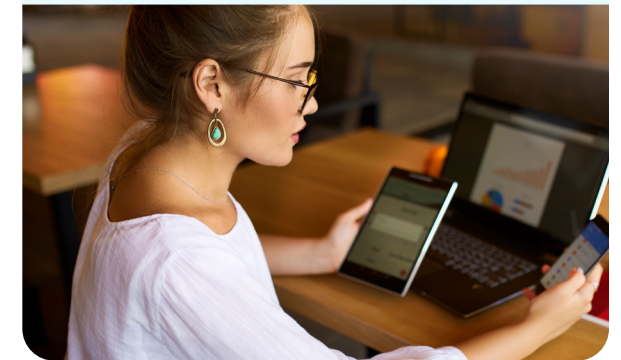
Employ Advanced Threat Detection



Secure Remote Sites



Connect Smart Devices



Overview

Use Cases

Why AT&T

Building the Government of the Future

Initiatives Driving Modernization

Top Challenges for CIOs

Performance and Security to Digitize Services

Modernize Government Services

Employ Advanced Threat Protection

Secure Remote Sites

Connect Smart Devices

Converged Cybersecurity and Networking



Use Case: Modernize Government Services

State and local governments want to improve the citizen experience with easier ways to access government services. Whether via web portals or mobile applications, access can be improved and simplified to increase engagement. In addition, many local governments want to improve broadband access for residents to help close the digital divide.

However, complexity is slowing down these digital initiatives. Applications are distributed in the cloud, in the data center, and as a service. Users are in constant movement between home, office, and travel. More devices than ever are accessing applications. In response, most organizations add new networking or security point solutions, leading to too many IT and security stacks, too many vendors, and too many products that operate in a silo with their own policies and their own management consoles. This operational complexity is the #1 challenge teams can start solving right now with the engagement of an MSSP.

Modernization starts with a best-in-class network that can be deployed easily with fast speeds and high performance. An MSSP can assist with selecting and deploying the right type of networking to meet your needs. The network must also be secured to protect its availability and to ensure data isn't compromised.

Look for solutions that include network access control to detect and monitor devices on the network for malicious activity. Identity and access management can prevent intruders from accessing the network with stolen credentials. For modern applications, you also need to be able to protect increasingly complex cloud and hybrid infrastructure. Fast networking combined with secure, reliable infrastructure and knowledgeable consultants will help you move from legacy systems with confidence.



Benefits:



More efficient engagement with citizens



Secure digital access and connectivity



Simplified security management and automation

Overview

Use Cases

Why AT&T

Building the Government of the Future	Initiatives Driving Modernization	Top Challenges for CIOs	Performance and Security to Digitize Services	Modernize Government Services	Employ Advanced Threat Protection	Secure Remote Sites	Connect Smart Devices	Converged Cybersecurity and Networking
---------------------------------------	-----------------------------------	-------------------------	---	-------------------------------	-----------------------------------	---------------------	-----------------------	--

Use Case: **Employ Advanced Threat Protection**

With the rise in sophisticated cyberattacks and challenges in hiring skilled security personnel, state and local governments are looking to advanced threat protection tools and services to fill the void. These options offer automated threat blocking to provide 24/7 protection and can help address cybersecurity skill gaps by leveraging MSSP expertise and resources.

Today's siloed security tools can also make effective threat protection difficult. They require greater time for management and manual correlation of data to detect issues. Consolidating security in a single platform offers shared intelligence and insights in addition to easier management. An MSSP can further improve your security posture with around-the-clock monitoring and advanced detection and response tools.

For an effective defense against sophisticated threats, consider a service that offers:

- Real-time threat intelligence backed by machine learning to provide accurate identification of threats quickly
- Accelerate threat detection with intrusion detection systems
- Malware protection and endpoint detection and response (EDR) to block threats

The right solution can protect critical infrastructure with advanced protection without burdening your limited IT and security resources.



Benefits:



Lower risk of a costly breach



Faster response to multiple types of threats



Complete, around-the-clock coverage

Overview

Use Cases

Why AT&T

Building the Government of the Future

Initiatives Driving Modernization

Top Challenges for CIOs

Performance and Security to Digitize Services

Modernize Government Services

Employ Advanced Threat Protection

Secure Remote Sites

Connect Smart Devices

Converged Cybersecurity and Networking



Use Case: Secure Remote Sites




Government services are often spread across dozens, hundreds, or even thousands of assorted facilities. Providing connections between these branches and the main IT infrastructure has historically required expensive multiprotocol label switching (MPLS) infrastructure that is expensive and complicated to deploy, making it difficult for budget-constrained municipalities to expand network coverage.

In addition, vast open networks are vulnerable to cyberattacks due to a large number of devices that are often unsecured. Using SD-WAN to allow traffic to travel between offices and other branch locations via the public internet or a virtual network vastly reduces the need for MPLS. Secure access service edge (SASE) combines SD-WAN with additional security features for high-speed networking that protects sensitive data. It can be deployed more quickly and at lower costs than traditional networks and can reliably connect multiple locations.

Because SASE combines networking and security, network management can be performed from a single console, and secure web gateways and firewalls, and provide additional security to protect against malicious traffic or data loss. Deploying SASE as a service further reduces the burden on under-resourced IT teams, as the service provider handles the security and network service deployment, monitoring, and management,



Benefits:

-  High-performance networking across locations
-  Fewer disruptions to critical services
-  Reduced risk of a cyberattack or outage

Overview

Use Cases

Why AT&T

Building the Government of the Future

Initiatives Driving Modernization

Top Challenges for CIOs

Performance and Security to Digitize Services

Modernize Government Services

Employ Advanced Threat Protection

Secure Remote Sites

Connect Smart Devices

Converged Cybersecurity and Networking

Use Case: **Connect Smart Devices**

Governments want to take advantage of IoT and operational technology (OT) for more efficient operations, such as modernizing traffic management, collecting real-time data from smart water meters, or monitoring critical infrastructure. However, these devices expand the attack surface and can create silos in the security architecture, creating more work for understaffed security teams.

However, a managed solution designed to connect and secure IoT and OT could help you take a big technological leap forward to improve digital services and increase operational efficiency. Look for a service provider that can:

- Monitor critical infrastructure in real-time to reduce or eliminate outages
- Simplify physical security management by integrating voice, video, and surveillance systems with cybersecurity architecture
- Connect, verify, and monitor all devices connected to the network to prevent access by malicious or compromised devices
- Detect threats based on real-time information and threat intelligence
- Integrate security across multi-cloud and edge deployments

With improved security integration and automated threat detection managed by security experts, you can scale protection to accommodate the increased demand IoT and OT bring. In turn, state and local governments can begin to implement new technologies to improve efficiency, safety, and sustainability.



Benefits:



Detect infrastructure issues faster



Harden the IoT and OT attack surface to reduce risk



Build sustainable smart cities

Overview

Use Cases

Why AT&T

Building the Government of the Future

Initiatives Driving Modernization

Top Challenges for CIOs

Performance and Security to Digitize Services

Modernize Government Services

Employ Advanced Threat Protection

Secure Remote Sites

Connect Smart Devices

Converged Cybersecurity and Networking



Converged Cybersecurity and Networking Solutions from AT&T Business with Fortinet

AT&T Business with Fortinet provides secure connectivity that allows state and local governments to deliver better citizen experiences. Bring people, data, and technology together with flexible managed services backed by an industry-leading security platform for reliable and safe communication and modern digital infrastructure.

AT&T Business is the number one managed SD-WAN provider with a wide breadth of network integration solutions. Fortinet brings a broad portfolio of security and networking products and single pane-of-glass management across the Fortinet Platform Solution to simplify operations and reduce network security complexities. AT&T's managed services backed by Fortinet technology provide high-performance networking and security at scale to modernize government services and ensure the physical and digital safety of networks, infrastructure, and citizens.

business.att.com • fortinet.com



Overview

Use Cases

Why AT&T

Building the Government of the Future

Initiatives Driving Modernization

Top Challenges for CIOs

Performance and Security to Digitize Services

Modernize Government Services

Employ Advanced Threat Protection

Secure Remote Sites

Connect Smart Devices

Converged Cybersecurity and Networking