White paper

Power your missions with the right technology

Learn how managed network services can help you modernize infrastructure, strengthen security and keep your agency ready for what's next.

verizon

Emerging technologies, evolving threats and new ways of working are reshaping how agencies approach modernization. As artificial intelligence (AI) becomes part of daily operations, there's a growing need for network infrastructure that's capable of handling advanced data workloads. At the same time, cyberthreats continue to grow in sophistication, targeting the networks, systems and data that agencies rely on to meet their objectives.

For federal agencies, modernization carries a deeper strategic importance. Network upgrades mean more than faster speeds or larger capacity; their ability to help strengthen mission delivery, enhance security and ensure that services remain available is what defines their value.

When technology decisions are tied directly to mission priorities, agencies can create systems that sustain readiness now and into the future.

Understanding the challenges your agency is facing

Missions today operate in a more complex technology environment than they did just a few years ago. Infrastructure that once met operational needs is now expected to support AI initiatives, defend against increasingly sophisticated cyberthreats and enable secure access for teams working across multiple locations. Federal agencies are tasked with balancing these priorities against limited resources, tight budgets and legacy systems that weren't designed for modern demands.

These pressures overlap and amplify each other to create operational strain.

Understanding how these challenges stack up is the first step toward building an infrastructure that can help improve mission outcomes.

How these challenges stack up

Legacy IT and technical debt

Many systems in operation today are several technology cycles old, making integration with modern platforms slow or difficult. Manual processes for updates and maintenance increase the time required to adapt. Plus, hardware limitations can prevent adoption of tools such as cloud services, Internet of Things (IoT) integration and software-defined wide area network (SD WAN). As infrastructure ages, costs often rise while performance declines.

Resource scarcity

Agencies are managing increasingly complex technology environments at the same time that specialized IT and cybersecurity talent is harder to find. Staffing changes add pressure, leaving teams to balance day-to-day operations with strategic projects. Without additional support, modernization efforts can lose momentum.

A primary objective driving organizational investments is to reduce IT workload (42%).[1]

Budget constraints

Capital investments for large-scale upgrades can take significant time to approve. Leaders are seeking approaches that stretch existing budgets, avoid major one-time expenditures and allow for growth that can adapt to changing demands.

Accelerated AI adoption

AI offers agencies opportunities to improve efficiency and extend capabilities – but these benefits depend on having infrastructure that can support intensive workloads securely and efficiently.

93%

of organizations report employees using generative AI (genAI) tools.[2]

64%

view data compromise from employees entering sensitive information into genAI as their top mobile risk.[3]

Rising security threats

Broader connectivity, more remote endpoints and growing volumes of sensitive data have expanded the attack surface. Threat actors are adapting quickly, making it essential that defenses are not only robust but also able to evolve alongside the threat landscape.

63%

of organizations that suffered downtime from a mobile-related security incident reported major repercussions.[4]

78%

of Public Sector breaches identified in the Verizon 2025 Data Breach Investigations Report (DBIR) were from system intrusion, miscellaneous errors and web application attacks.[5]

60%

of all confirmed data breaches identified in the DBIR involved a human element.[6]

Top drivers for increased security spending:[7]

More users (43%)
More devices (41%)
Remote/hybrid workforce (39%)

Taking a managed approach to mission success

When you're trying to balance day-to-day operations with long-term modernization, an integrated solution such as managed network services can make a real difference. By bringing network management, security operations and scalability planning together, you can stay focused on the mission ahead.

Think of managed network services as a force multiplier for your agency. Managed network services don't just keep things running; they expand your capacity, strengthen your security posture and accelerate the changes you've been wanting to make. And because managed network services are built with flexibility in mind, they can help future-proof your mission, so your infrastructure is ready for whatever tomorrow brings.

Modern, software-defined and cloud-ready platforms can help reduce the time and complexity of integrating new capabilities, offering a flexible foundation for emerging technologies without disruptive overhauls.

Managed network services can ease the burden on internal teams by handling monitoring, updates and optimization, freeing staff to focus on mission priorities. Consumption-based models such as network as a service can replace large capital expenditures with predictable operational costs, allowing resources to scale as needed. AI-ready platforms can enable secure, efficient deployment of new tools alongside existing systems. And layered security frameworks, proactive threat intelligence and adaptive policies – such as zero trust – can help strengthen resilience and keep defenses ready for evolving risks.

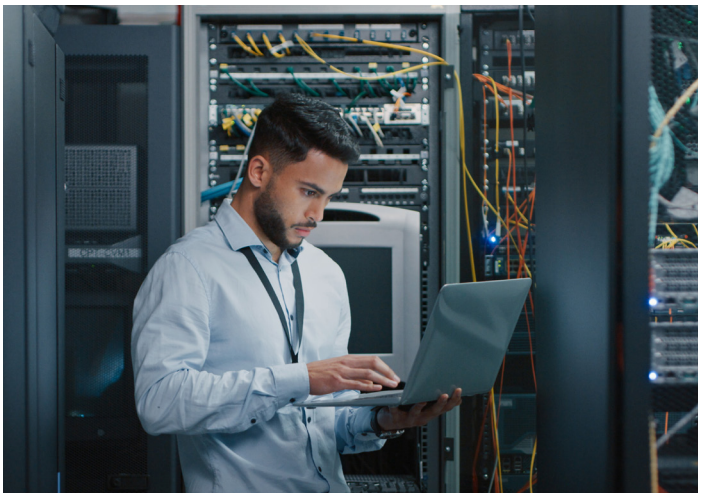
The cost of falling behind

When resource, infrastructure and security challenges converge, they often slow modernization to a reactive pace. IT teams focus on immediate problems, such as network outages, urgent security patches and hardware failures – instead of long-term improvements.

This can result in delayed adoption of new capabilities, ranging from AI-powered tools to advanced connectivity. It can also escalate operational risks, increasing vulnerability during emergencies. If your technology can't keep up, your agency may struggle to deliver consistent, secure services when they are needed most.

Driving results with managed network services

A modernization strategy becomes most effective when it links directly to your agency's real-world challenges. Managed network services can help address these needs through solutions designed to be practical today and adaptable tomorrow.



Use case: Transforming legacy systems into future-ready platforms

Challenge

Legacy networks slow modernization efforts, create bottlenecks, and make integration with modern tools complicated and time-consuming. They often depend on manual maintenance, which increases the chance of human error and limits agility. Over time, these systems require more resources to maintain while delivering less value, and their incompatibility with emerging technologies can delay the innovations your mission depends on.

Solution

Shift to SD WAN and cloud-centric architectures supported by managed maintenance and updates. With these foundations, your agency can integrate modern services without lengthy downtime or complex retrofits, and updates can happen effortlessly as part of ongoing management.

Benefits

You can achieve faster integration of technologies such as IoT, AI and advanced cloud services; reduce operational downtime that helps keep critical functions running; and improve scalability to handle new priorities and larger workloads as mission requirements change.

Use case: Harnessing automation to amplify your capabilities

Challenge

Limited skilled staff must manage increasingly complex networks, systems and security environments. This overload can result in slower issue resolution, reduce focus on innovation and increase burnout among high-value team members. Without support, modernization initiatives compete with the demands of day-to-day management.

Solution

Introduce advanced platforms and automation tools to handle network monitoring, patch management, performance optimization and threat detection. Managed network services provide specialized skills to manage these tools, freeing agency teams from routine upkeep.

Benefits

Your in-house teams can take advantage of reduced workloads to focus on mission-critical objectives; continual oversight that helps ensure systems remain optimized; and faster detection and resolution of performance or security issues that helps improve operational efficiency.

Use case: Scaling your network to match your operations

Challenge

Traditional capital expenditure models demand significant up-front investments that can be difficult to approve and adapt, often locking agencies into capacities that may not fit future demand and delaying the rollout of new capabilities or sites.

Solution

Adopt a network as a service approach, leveraging shared enterprise security, resource optimization and consumption-based billing. Capacity can be increased or decreased as needed without major approvals for capital budgets.

Benefits

You gain predictable monthly or quarterly expenses that can improve budget planning; reduce financial risk by scaling services in line with real demand; and improve return on investment by tying spending directly to operational performance.

Use case: Modernizing infrastructure to keep pace with AI

Challenge

AI applications require high-performance, secure and adaptive infrastructure. Without it, AI deployments are slower and less effective – sometimes forcing agencies to shelve projects until major upgrades can be funded and implemented.

Solution

Create an AI-ready network foundation with secure integration points for data flows and processing designed to scale with new AI workloads over time. Managed network services help ensure that as AI tools evolve, the network evolves alongside them without costly reinventions.

Benefits

You can have smooth, secure AI deployments without heavy resource strain; faster adoption curves that enable your agency to capitalize on AI capabilities sooner; and operational efficiencies driven by automation and insight from AI tools that are fully supported by the network.

Use case: Strengthening defenses against evolving threats

Challenge

Agencies face increasingly sophisticated cyberattacks targeting broader and more complex attack surfaces. These threats can affect mission continuity, cause compliance failures or expose sensitive data. Without proactive defenses, response times increase and risks multiply.

Solution

Deploy layered protection measures including near-real-time threat intelligence, zero-trust architecture and automated security operations capable of adapting to new vulnerabilities as they appear. Managed security helps ensure constant monitoring, quick mitigation and ongoing updates to defense models.

Benefits

You get continuous coverage that can lead to fast incident response and limited operational impact; strong compliance adherence through proactive security posture management; and a reduced likelihood of undetected breaches.

Modernization that works for your mission

When agencies choose a managed approach, modernization becomes a strategic advantage rather than a disruption. Services scale as priorities shift, security measures stay ahead of new threats, and networks remain agile enough to handle planned initiatives and urgent demands. With flexible consumption models directing budgets where they matter most, agencies can modernize confidently—protecting critical operations today while staying ready for tomorrow.

Why partner with Verizon

Agencies like yours need a partner that can not only deliver technology expertise but also work alongside your teams to build a plan that can keep up with your operational demands.

Verizon brings decades of experience supporting federal networks, along with dedicated support teams that understand compliance, security and mission priorities. Our national infrastructure footprint is built with mission-critical redundancy, and our leadership in technologies such as SD WAN, 5G, zero trust and AI-ready architectures means that we can help your agency select and implement solutions with confidence.

To learn more about Verizon managed network services, visit verizon.com/publicsectorservices.

1. "2025 Mobile Security Index," Verizon. Oct 16, 2025. https://www.verizon.com/business/resources/reports/2025-mobile-security-index.pdf
2. Ibid.
3. Ibid.
4. Ibid.
5. "2025 Data Breach Investigations Report," Verizon, Apr 21, 2025. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf
6. Ibid.
7. "2025 Mobile Security Index," Verizon. Oct 16, 2025. https://www.verizon.com/business/resources/reports/2025-mobile-security-index.pdf