Five ways network transformation advances your mission

Your network is a critical asset that can enhance mission success across government operations. By improving areas like operational efficiency, secure digital services and citizen engagement, we help agencies achieve their mission objectives, drive innovation and reduce risks.

Contents

The network: a key to agency success

Without a robust network, mission success is unattainable. More than 9 in 10 organizations recognize that their networks directly impact their most pressing operational and digital transformation challenges, according to NTT DATA's 2022–23 Global Network Report.

Global Network Report 2022-23

The report highlights that many top-performing organizations – defined by their ability to meet objectives efficiently — are investing more in their networks. This investment drives operational excellence, enabling digital transformation while enabling secure and efficient service delivery to stakeholders.

Gone are the days when networks simply provided access to the internet and email. Today, public sector networks are designed and managed to align with mission-critical objectives. A network is defined by the value it creates for agencies, citizens and public safety.

Leveraging the network as a driver of mission outcomes

Traditional networks were often built with a focus on technical capabilities. However, mission-driven network management prioritizes outcomes such as securing critical infrastructure or supporting public safety through integrated technologies like 5G and IoT.

Public sector networks must be scalable, allowing agencies to adapt to policy changes, security mandates or increased demand for public services. An adaptable network infrastructure opens the door to innovation and enhanced citizen services.

For hybrid working environments, mission-driven networks enable high-performance access to communication and collaboration systems, improving government workforce productivity and operational efficiency. Networks that support smart resource management, such as environmental monitoring systems, also help agencies reduce costs and increase sustainability.

The network is critical for AI systems, providing the infrastructure needed to integrate innovative technologies and transfer large data volumes securely. This is essential for real-time data processing in public safety, healthcare and other critical sectors. Advanced security protocols embedded within the network protect sensitive public data and enhance system resilience.

Rapid advances in AI, including generative AI, provide public sector organizations with tools to make their networks more efficient and secure. AI-driven algorithms can analyze network data to predict outages, detect inefficiencies, enhance security and keep critical infrastructure online and available.

Turning your network refresh into a strategic win

Legacy infrastructure can hinder mission success if not aligned with modern digital strategies. However, few organizations can simply replace their networks overnight.

A successful network refresh requires managing legacy systems while integrating modern technologies. This involves strategies for integrating or replacing older systems without disrupting essential services.

The first step is to assess and catalog legacy infrastructure, understanding which systems are critical and which can be phased out. This helps ensure that decisions about upgrades or replacements are aligned with agency objectives and security requirements.

Prioritizing upgrades that directly affect key services allows for an incremental approach to integrating recent technologies, managing the lifecycle of current hardware and software while extending the network's overall lifespan. Additionally, transforming workforce skills and enabling access to expert resources are vital for a smooth transition.

Once new systems are in place, regular reviews and updates will help ensure that the network continues to meet the agency's and citizen's needs, keeping operations efficient and secure.

Five ways network transformation advances your mission

1. Advancing digital transformation to enhance public services

Digital transformation — the integration of digital technology across public sector operations – fundamentally changes how agencies deliver services to citizens. Mission-driven networks provide the infrastructure necessary to streamline processes, use resources efficiently, minimize human error and leverage data to improve service delivery.

These networks also support automation technologies that enhance productivity, enable consistent results and reduce risk by automating repetitive tasks.

Automation within the network can help manage traffic, monitor system performance and respond swiftly to security alerts, all of which are crucial in maintaining secure and efficient operations.

As digital transformation often leads to increased data volumes and the integration of innovative technologies, mission-driven networks need to be flexible, allowing for capacity and functionality adjustments as needed.

Ensuring seamless connectivity across departments and regions

As you adopt more digital tools, seamless connectivity becomes essential. The network must connect all parts of the organization to enable better collaboration and communication across departments and geographic locations, especially in the era of hybrid and remote work.

Fast, reliable and secure connectivity also enables effective data management and analytics by enabling data to flow smoothly and securely across the organization, empowering decision-making and service delivery.

Facilitating cloud adoption for operational efficiency

Cloud technologies are integral to digital transformation. Moving resources to the cloud enhances accessibility and optimizes operational costs. Mission-driven networks must be adaptable for secure and efficient cloud integration, enabling connections between government services and public/private cloud providers to be reliable.

Strengthening security as the digital footprint grows

As digital transformation expands an organization's digital footprint, the risk of cyberthreats increases, making robust network security measures essential. Networks must enable the protection of sensitive citizen data and help maintain compliance with government regulations.

Aligning network strategy with agency goals

Working with a managed service provider can help align your organization's network strategy with its mission. According to our network report, nearly 8 in 10 top-performing organizations have successfully aligned their network and operational strategies, compared with only about 40% of underperformers.

2. Connecting hybrid cloud environments

Hybrid cloud environments, which blend on-premises infrastructure with private- and public-cloud services, offer a powerful combination of speed, flexibility and security for public sector organizations. These environments allow for more efficient data processing and analytics, particularly for mission-critical edge computing applications. The hybrid model also enables greater scalability, while maintaining the strong security and compliance needed for managing diverse types of workloads across various locations.

Networks play a pivotal role in connecting these hybrid environments, helping organizations harness the best of both worlds: the control and security of on-premises infrastructure, alongside the scalability and efficiency offered by the cloud.

According to our network report, 94% of organizations agree that cloud-based workloads require greater availability, scale and performance from the network. Aligning network and cloud strategies is essential to supporting the dynamic needs of public sector operations.

Ensuring seamless connectivity and security

Seamless connectivity between on-premises data centers and cloud services is a fundamental requirement. It allows data and applications to move between environments without sacrificing performance or security. Optimizing traffic flow through solutions like software-defined wide-area networks (SD-WAN) enables the intelligent routing of data between cloud and on-premises infrastructure based on real-time conditions.

This optimization is key to managing the dynamic workloads of hybrid cloud environments, enabling the network to scale resources up or down without disrupting operations. A flexible network infrastructure that adjusts automatically enables consistent performance, even as demand changes.

Centralized management for cost efficiency

Centralized network management tools provide visibility and control over both on-premises and cloud resources. By leveraging these tools, public sector organizations can optimize their use of cloud resources and manage network traffic dynamically. For example, adjusting traffic based on time of day or network congestion helps contain IT costs without compromising performance.

Addressing complex security challenges

While hybrid cloud environments offer tremendous flexibility, they also introduce new security challenges, particularly in data privacy and regulatory compliance. Mission-driven networks use advanced security features such as end-to-end encryption, intrusion detection and identity management to enhance data security as it moves between environments. This level of security is critical for protecting sensitive public sector data and maintaining compliance with government regulations.

3. Reducing the risk of a security breach

According to our network report, more than 90% of organizations agree (42% strongly) that ever-increasing security and compliance risks pose significant challenges to IT and network operations. Many organizations are also concerned about a lack of in-house expertise in these areas, prompting them to increasingly partner with managed service providers to address these concerns.

Mission-driven networks, with advanced embedded and layered security controls — including technologies like zero trust network access, advanced threat protection and Secure Access Service Edge (SASE) – are designed to match an organization's specific risk profile and compliance requirements. This targeted approach protects against cyberthreats more effectively than generic, one-size-fits-all solutions.

Since security is prioritized as a fundamental component of the network architecture, public sector organizations can adopt a proactive security posture. This enables them to anticipate and mitigate potential threats before they escalate into critical issues. Comprehensive visibility across the network is crucial for real-time monitoring, analytics and rapid threat detection and response.

Segmentation for enhanced security control

A key feature of secure-by-design networks is the ability to segment the network into zones, allowing for more granular control over data and resource access. This segmentation limits the potential impact of a security breach by containing it within a specific segment, reducing the overall risk to the organization's operations.

AI-driven threat detection and automation

AI-driven security systems can detect anomalies that may indicate cybersecurity threats, such as unusual access patterns or large data transfers. These systems continuously learn from network activity, becoming more accurate over time and allowing for more effective threat detection and response.

Mission-driven networks also use identity-based access controls, which enforce security policies based on user identity and context. This helps ensure that users have the appropriate level of access to network resources depending on their role, location and other contextual factors.

In cases where a threat is detected, these networks often incorporate AI-led automation to respond dynamically. This may include adjusting access controls, rerouting traffic or isolating affected network segments, all of which help contain the threat while easing the burden on cybersecurity teams.

Enabling regulatory compliance

Public sector organizations can meet stringent regulatory requirements for data protection and privacy through controlled data flows, secure data storage and transmission mechanisms. Comprehensive reporting tools also provide transparency and enhance compliance with government regulations regarding cybersecurity.

> **AI-driven security systems can detect anomalies that may indicate a cybersecurity threat, such as unusual access patterns or large data transfers.**

4. Optimizing resource usage for greater efficiency and sustainability

Mission-driven networks enable optimized operations, including designs that prioritize energy efficiency. Public sector organizations are increasingly looking to reduce their environmental impact, and modern networks support these sustainability goals.

Today's network devices are built with energy efficiency in mind, using less embodied carbon, efficient power supplies and responsibly sourced materials. These devices are also shipped with 100% recyclable packaging. Additionally, technologies like software-defined networking (SDN) and virtualization allow for better resource management by reducing the need for physical hardware, thereby lowering energy consumption. Efficient routing and switching protocols help ensure that data travels through the network using the least energy possible.

AI-enhanced efficiency

AI systems integrated into networks can optimize cooling systems and power usage, significantly reducing the carbon footprint of network operations. These networks also integrate seamlessly with cloud services, which are generally more energy-efficient than traditional on-premises data centers.

A lifecycle approach to sustainability

Networks facilitate better asset lifecycle management by providing valuable data on usage patterns, maintenance needs and opportunities for end-of-life recycling. This lifecycle approach allows public sector organizations to extend the lifespan of their network products and implement circularity programs for responsible disposal and recycling.

Supporting remote work and reducing carbon footprint

Network reliability is essential for supporting remote and hybrid work models, which help reduce the carbon footprint associated with commuting. By enabling more employees to work remotely, public sector organizations can reduce their physical office space, lowering heating, cooling and lighting demands.

5. Boosting employee collaboration, productivity, and output

According to NTT DATA's 2023 Global Employee Experience Trends Report, nearly 6 in 10 employees globally are now working in hybrid or fully remote models. For public sector organizations, mission-driven networks must support this evolving workplace by providing a secure and reliable technological foundation for collaboration across dispersed work environments.

At the heart of the hybrid workplace is the need for seamless connectivity, regardless of where employees are working. The network must enable secure, efficient access to government resources, whether employees are in the office or working remotely. This includes access to cloud services and software-as-a-service (SaaS) applications that are essential for day-to-day operations

> **The network must allow employees to access corporate resources securely and efficiently, whether they are working in the office or another location.**

Collaboration in a distributed workforce

Collaboration tools such as videoconferencing, real-time messaging and shared digital workspaces are crucial for maintaining productivity in hybrid work environments. These tools depend on a robust network infrastructure to function effectively. Mission-driven networks can prioritize traffic to enable critical applications like videoconferencing to have the necessary bandwidth, allowing employees to communicate and collaborate smoothly, regardless of location.

Such networks also enhance the employee experience by enabling features like occupancy and space tracking, asset management and indoor wayfinding in physical workspaces. When integrated with collaboration systems, these capabilities create a workplace that attracts employees, fostering engagement and productivity.

Securing the hybrid workplace

With the distributed nature of hybrid work, security is a top priority. Networks must incorporate advanced security features such as virtual private networks (VPNs), end-to-end encryption and zero trust principles. These measures help enable secure access to sensitive data while allowing employees to use personal devices for work without compromising security. In doing so, public sector organizations can meet regulatory compliance standards while safeguarding their networks.

Optimizing the network for hybrid work

Insights gained from advanced network analytics allow public sector organizations to optimize their networks to better support hybrid work patterns. By analyzing data on network usage and employee behavior, agencies can make more informed decisions about resource allocation and help ensure that their networks continue to support productivity and collaboration.

Take the next step

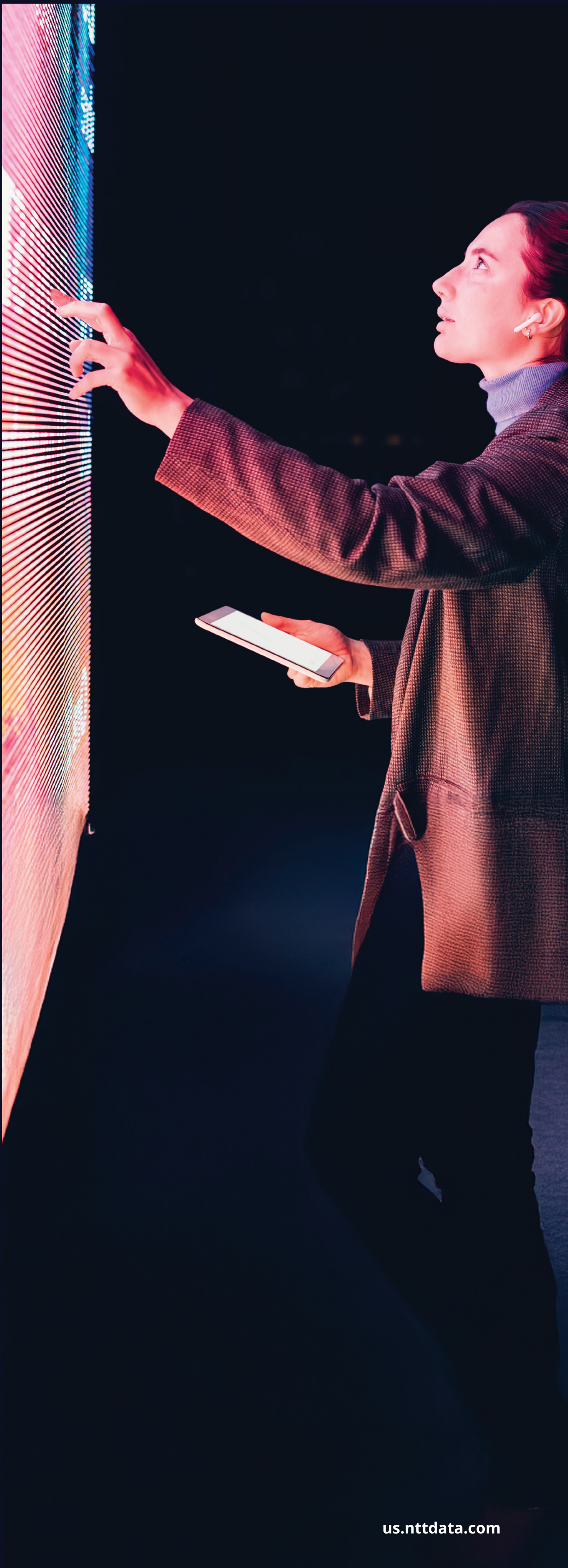
Reduce risk and manage costs in your network

As your public sector organization navigates today's challenges and prepares for tomorrow's opportunities, selecting the right partner is essential for delivering the network needed to support your mission.

An experienced systems integrator and managed service provider can assess your network requirements and design a customized solution that aligns with your digital transformation, cloud adoption, security, sustainability and hybrid workplace needs.

Whether you choose to manage your network in-house or partner with a managed service provider, NTT DATA can help. With access to the latest technologies and industry best practices, we have the expertise to deliver a more efficient and cost-effective network, creating value across your organization.

Learn more about how NTT DATA's mission-driven network solutions can future-proof your network.



Visit us.nttdata.com to learn more.

NTT DATA is a trusted global innovator of business and technology services, helping clients innovate, optimize and transform for success.
As a Global Top Employer, we have diverse experts in more than 50 countries and a robust partner ecosystem. NTT DATA is part of NTT Group.

© 2024 NTT DATA, Inc. All rights reserved. | 1631448