A New Network Approach for Lasting Digital Transformation

State and local governments face unprecedented disruption as they rally to deliver new digital services, reallocate technology resources, accommodate flexible approaches to work, and adjust to budget-related changes. In an informal Center for Digital Government (CDG) survey, 63 percent of respondents said their organization is reaffirming its digital transformation strategies given recent events.[1] While digital transformation has been on the shortlist of IT priorities for several years, there is now increased urgency. The need for a new network approach — one that accelerates digital transformation and ensures it is sustainable regardless of possible future disruptions — is more critical than ever.

A NEW NETWORK APPROACH

To navigate disruption while staying on course with long-term digital transformation plans, organizations need a new network approach that relies on three key strategies to optimize the bandwidth, performance, and security capabilities of their existing network investments.

Strategy #1: Move to a network that can adapt

A network that can adapt to change enables organizations to optimize their existing infrastructure while incorporating new technologies and new ways of working. It includes the following components:

Programmable infrastructure: Orchestrate the deployment and management of devices and infrastructure via a single pane of glass, allowing IT staff to easily adjust bandwidth, routing, and other resources to meet the demands of applications and services running on top of the infrastructure. As a result, they can deploy new applications and services to citizens as quickly and reliably as possible.

Analytics and intelligence: Gain actionable, data-driven insights from network telemetry and accurately predict future impacts on performance based upon traffic patterns. For example, analytics and intelligence of network traffic patterns by agency and location can identify areas of potential

URGENT DEMANDS, DISAPPEARING BUDGETS

Heightened need for digital services. Citizens and businesses expect digital services so they can carry on with their daily lives — from registering vehicles and receiving social services to obtaining marriage licenses and applying for building permits. Organizations also need digital services to help address backlogs and staffing and other resource shortages.

Uncertain budgets. Reduced sales tax revenue and delayed individual income tax revenue are forcing states and municipalities to freeze or reallocate budgets. The Center on Budget and Policy Priorities estimates states will see budget shortfalls of about 15 percent this year and more than 25 percent in 2021.[2]

Hybrid work models. As state and local agencies reopen, they will need to adapt technology and workflow processes to support employees who continue to work from home, as well as those who provide in-person essential services in the field or office.

Increased bandwidth, performance, and security demands at all endpoints. Organizations need to rapidly allocate bandwidth, as well as flexibly implement new security controls as they increase their use of videoconferencing, add VPNs to enable remote work, extend workflow processes across the enterprise, and rely on online applications to serve record numbers of people seeking services.

congestion or outage and alert staff or an automation platform to take proactive resolution steps.

Software-based control and automation: Automate network actions based on telemetry and analytics, with intent-based, software-enabled management of performance, resiliency, security, costs, and other factors. When used for service assurance, for example, intelligent automation can reduce the time to resolve issues and, in many cases, decrease the volume of problems by predicting and averting issues before they occur.

Strategy #2: Ensure security is built in

Built-in network security is an important differentiator when it comes to protecting data and infrastructure. State and local governments must understand, identify, and protect against threats at all edges of the network — including mobile devices, cloud environments, IoT sensors, and other endpoints. By building encryption, firewall, and other security technologies into the network, organizations can ensure data is protected as it moves between agency locations and data centers.

The advantages of built-in network security can be amplified when accompanied by a well-established network provider that has multiple global points of presence, intelligent automated monitoring and analysis, advanced threat intelligence teams, and extensive mitigation capabilities. While many organizations are tempted to rely solely on machine-readable intelligence from subscription-based services, human experts bring invaluable experience and context so organizations can better prioritize threats.

Strategy #3: Engage a trusted partner

A trusted network partner helps navigate and simplify network modernization by providing proven processes, a broad array of state-of-the-art technology solutions, and expertise that is difficult to maintain in-house. Their solutions should be flexible and reconfigurable as needed to meet evolving demands without requiring protracted, labor-intensive physical installations.

Depending on their business requirements, organizations can work with a partner to build out their own in-house solution or have the partner handle some or all network security via a

CREATING CONNECTED HEALTH CLINICS

A local government needs to set up network connectivity at multiple locations that would serve as temporary health clinics to test and treat overflow patients during an emergency. Each site would need network connectivity to access medical images, electronic health records, and other digital applications located in multiple offsite clouds and data centers. The cost of deploying and managing network devices for each location is significant. Their network partner can offer a better option: With Network Functions Virtualization (NFV), the local government could put multiple functions like router, firewall, and accelerator into software, which can be centrally managed, updated, and troubleshot from a single location. This would allow the local government to get the services it needs at each location, at a lower cost than deploying individual network technologies. And the central control enables more time and resources to be allocated to serving patients.

managed services model. In such a model, organizations do not own the network infrastructure, so they do not have to worry about technology management, maintenance, or upgrades. Managed services also help fill skills gaps and allow IT teams to focus on more strategic tasks.

A MORE RESILIENT FUTURE

Doing more with less, especially in unpredictable times, requires a new approach to networking. A network that is adaptable with built-in security, and engagement with a trusted partner, are core to this approach. These strategies will help state and local governments navigate the current environment while ensuring they are prepared and resilient for whatever comes next.

Endnotes:

1. CDG Webinar. Network Demand Is Higher Than Ever: Learn How Intelligent Automation Can Help Now and in the Future. June 2, 20202

2. Center on Budget and Policy Priorities. States Grappling with Hit to Tax Collections. June 2020. https://www.cbpp.org/research/state-budget-and-tax/states-grappling-with-hit-to-tax-collections

THE ADVANTAGES OF A NEW NETWORK APPROACH

A new network approach enables state and local governments to:

• Maximize the capabilities of their current network
• Deploy network services that rapidly enhance agility
• Free up staff for higher-value projects
• Enhance security and data protection

• Go at their own pace and budget
• Build a foundation for future innovation
• Reduce operational expense