Navigating Next-Generation Networks

Simply refreshing network technology is no longer sufficient. Agencies need to be thinking about network transformation and innovation.

The network is the lifeblood of federal agencies' many missions today. The readiness of people and organizations to do the work required by the mission depends more and more on leveraging a reliable, resilient and secure network to access and share information.

However, much of today's network architecture was developed more than a decade ago when applications and data storage were primarily on-site. Today, data is stored in multiple, often off-site locations and mission applications are often cloud based to enable greater collaboration and consistency. Additionally, government users today are mobile, and consequently must have and expect anytime, anywhere access to data.

In many cases, existing agency network architectures have created complex legacy ecosystems not optimized for today's network utilization. This results in service delivery, provisioning, troubleshooting and repair challenges, not to mention a complex cyber-resiliency challenge.

Maintaining these legacy networks is costing federal agencies a small fortune. Agencies report that they spend 80 percent of their IT budgets just on maintaining legacy IT systems. That doesn't leave much funding left for innovation and transformation.

shutterstock.com

Just as missions have transformed, the approach to network architecture must transform. We are on the precipice of a network evolution that requires thinking differently about network architecture, one in which we give up the belief that the network is rigid, inflexible, static and often considered "in the way" of innovation and service delivery.

THE PATH TO CONTINUED INNOVATION

If an agency's network isn't as efficient as it could be, and isn't sufficiently elastic to support dynamic bandwidth requirements, then what's the solution? A simple answer would be to upgrade the network, but that is likely to be an imperfect fix. The better solution requires changing people's mindsets from network patches to network transformation, which allows continuous innovation to achieve needed efficiency and security while future-proofing the network.

"As newer cybersecurity solutions are introduced and continually evolve, the agencies' underlying networks need to be able to take advantage of the capabilities they afford," said Tim Meehan, Senior Vice President and General Manager of CenturyLink Government.

Adopting a network transformation mindset means combining best-of-breed technology

and managed services, and then wrapping those around an agency's current application and mission requirements. With this mindset, agencies can continue to adopt the right technologies to handle changing requirements without major network overhauls. Effective network transformation not only improves cybersecurity, service delivery times and overall mission response, but it also simplifies and reduces the cost of the agency's network operations.

Federal executives agree. In a recent keynote address, Federal CIO Tony Scott said the modernization of the federal government's IT environment is a high priority. "We're going to have to replace large parts of what we have because [existing network architecture] just was never designed for the mission and for the challenges that we face today."

ACHIEVE NETWORK TRANSFORMATION

The modern network requires several key capabilities in order to provide to the agency the flexibility necessary to quickly deliver solutions that meet rapidly changing mission demands in a secure manner. These key capabilities include on-demand network scalability, endpoint virtualization, and multilayer security.

On-demand network scalability: This is the ability of a network to scale up and down as needed to meet capacity and performance requirements. The best way to accomplish this is by incorporating software-defined networking (SDN), where a fully programmable and centrally managed network infrastructure can create a virtualized pool of network resources that users can access on demand.

"SDN lets users get services that used to take 30 days or more to order and now can be installed in minutes," said Rob McLaughlin, Director of the Department of Defense Division of Ciena Government Solutions. "The idea is to be able to take advantage of smarter, more intelligent platforms and next-generation capabilities as they become available, and SDN provides a path that achieves that goal."

Endpoint appliance virtualization: This is also called network functions virtualization (NFV). It's an effective way to improve both cost-efficiency and service delivery speed. It does both of these goals by moving network functions like routing, switching, firewalls, network accelerators and intrusion detection systems from hardware appliances to software that runs on off-the-shelf servers, network and storage platforms.

With this software-based approach, it's easier to request and manage services, such as firewalls, routers, DPI and so on. Network managers can quickly and easily deliver services, and decommission them when appropriate. Contrast that to a typical request for a network accelerator from a large federal agency, which can take months because it involves physically provisioning the network.

This concept can be extended beyond administrative services to field readiness. Warfighters, for example, could benefit by having their own commoditized x86 servers along with the controlling authority for specific missions. The system could push out profiles for those specific missions to authorized personnel, who would be able to use the resources and then tear them down once the mission is complete. When an unexpected need arises, it would be a simple, rapid process to provision a circuit between two points.

MULTILAYER SECURITY

Multilayer security is another benefit of a transformed network. And this depth of security has two primary aspects:

Protect the Data: Modern networks secure both at-rest and in-flight data. To ensure that all data, regardless of protocol, is protected, employ encryption at Layer 1. Wire-speed encryption at the transport layer ensures that traffic will be encrypted from end to end, and latency will no longer be a concern.

Protect the network: Protecting the network is also important to ensure both resiliency and data security. Driven by intelligent software, modern networks also improve situational awareness

Network Demands by the Numbers*

23: Percentage of federal respondents who rate their agencies as fully cyber-secure

25: Percentage of federal agencies that believe data on their network is fully protected

48: Percentage of federal respondents who say their current networks are too complex

56: Percentage of federal respondents who say lack of internal resources to implement and maintain networks are top challenges agencies face in improving their networks

75: Percentage of all Web application attacks targeted at U.S. sites

180: Percentage by which DDoS attacks have increased compared to the same time last year

1121: Percentage by which information security incidents affecting systems supporting the federal government have grown since 2006

* Survey results from the 2015 Federal Network Security Report by Market Connections and 2015 State of the Internet Security Report.

across the entire network infrastructure, and apply monitoring and detection and automated response to suspicious activity.

"Agencies need to be able to detect anomalies and potential breaches before they become issues and then react to them very quickly before they cause real impact," said McLaughlin. Many agency legacy networks simply don't have the capacity, bandwidth or agility to handle the volume and variety of cyberthreats that many agencies are currently experiencing.

Evolving the network doesn't require a complete network overhaul or a disruptive shift in network design. It does require reconsidering traditional views on network architecture and that new thinking evolves in order to start down the path of transformation.

WORK TOGETHER

Combining their expertise and technology, network specialist Ciena and communications and hybrid IT leader CenturyLink can help federal agencies create and manage a network transformation plan for configuration management, change management, and technology refreshes and insertions. That's everything an agency needs to ensure that its network is never out of sync with its mission. Using the cost-effective "as-a-service" model, CenturyLink can provide the expertise and Ciena can provide the networking equipment.

Together, CenturyLink and Ciena continue to push the envelope, both in terms of customer service and technology. For example, CenturyLink recently completed a 1 Terabit trial on part of its fiber network in central Florida using Ciena's 6500 packet-optical platform. This Terabit superchannel more than doubled the network's traffic carrying capacity during the trial. CenturyLink has also developed a Programmable Services Backbone using Ciena's BluePlanet SDN controller for orchestration.

TAKE THE FIRST STEP

Regardless of the route an agency chooses to pursue network transformation, taking that step is the only way to prepare for the future. Simply put, many federal agency networks aren't prepared for the security, bandwidth, capacity and scalability demands that today's agency missions require.

"One size doesn't fit all. Not every network needs to be reworked from scratch, but they all need to transform," said CenturyLink's Meehan. "The discipline to commit to a process of continuous evolution is the key. By inserting innovation into networking planning, an agency's IT infrastructure will be in a state of perpetual transformation—which is more effective than doing a network refresh once every 10 years."

For more information, please visit www.TransformingNetworks.com

ciena

CenturyLink® Government

The Business Case for Networking as a Service

Whether it was with software, platforms, infrastructure, disaster recovery or security, most federal agencies have at least dipped a toe into the "as-a-service" concept. By moving previously agency-maintained processes to a third-party service provider, agencies can effectively outsource day-to-day troubleshooting and IT management. And as a result, they can focus on their core missions while reducing the amount of time onsite IT specialists spend running software or hardware.

Agencies also reap cost benefits from this strategy. Instead of making large capital outlays for application licenses, hardware and IT staff, employees can simply access the services they need when they need them—and agencies only pay for the time the services are in use. This helps shift expenditures from capital expenses to operational expenses (CapEx to OpEx). OpEx costs are more predictable, and federal financial executives generally believe that operational expenses are easier to justify and provide more control over capacity.

Another area where agencies can take advantage of managed services is networking. Networking as a Service (NaaS) means IT managers have just one link through which they can provision, access and manage services. For example, if an agency runs a critical application that thousands of employees across the globe actively use, it no longer needs to own and manage the entire infrastructure. Instead, managers can focus on making sure employees can access applications and data quickly whenever and wherever needed.

It also means that agencies no longer have to worry about changing bandwidth usage. According to a survey commissioned by Ciena, the top challenge affecting network connectivity planning and requirements for all industries was bandwidth. With the NaaS model, if bandwidth requirements suddenly increase or decrease, it's not an issue. Agencies can simply spin up and reduce network capacity as needed, while only paying for what they use.