Network Modernization - The Promise of the Adaptive Network

RESEARCH BRIEF

ciena govloop

Introduction

During the past several years, many government organizations have started reevaluating their existing networks. Some built decades ago are aging better than others, because of a combination of factors that include changing public demands, new regulations and evolving mission requirements.

These legacy networks often are managed and maintained using older, largely manual methods such as off-line planning tools, spreadsheets, custom code and software that are reaching or have reached their end of life. As a result, agencies are experiencing more network outages. According to a recent GovLoop survey of nearly 100 federal, state and local government employees, more than half of agencies endure outages at least once in a while, with a healthy percentage experiencing them a few times each month (See Figure 1).

Agencies must be able to rely on their networks for performance and security. In fact, 73% of survey respondents named security as their top priority for network modernization. They also need to be able to use the valuable information their network produces to increase efficiencies and save money, but that's often not possible with existing network technology. Luckily, 77% of respondents said that agency leaders considered modernization a top priority or somewhat a priority.

To learn more about the status of network modernization in government, GovLoop partnered with Ciena to survey the landscape. The results provide a lot of food for thought, not only about what agencies want in a modern network, but what they value most. In this report, you'll hear from a Ciena expert about what agencies can do to improve their networks to make them more adaptive, responsive and secure.

I work for...

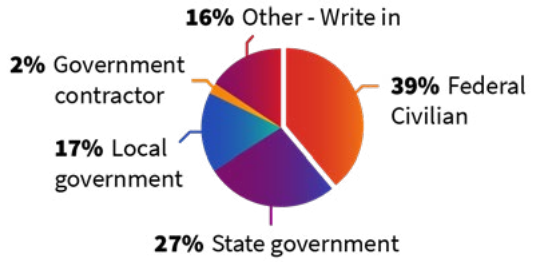


Figure 1

How often does your network experience an outage?

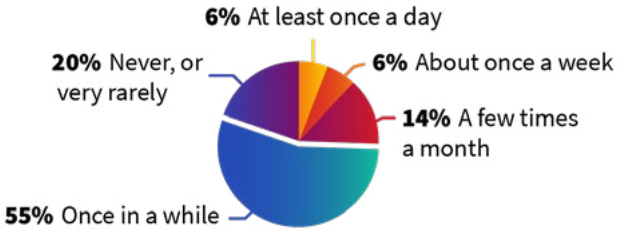


*Chart percentages may not add up to 100 due to rounding.

What Agencies Want in a Next-Generation Network

Agencies across the board want to be able to take advantage of next-generation technologies and capabilities to improve the responsiveness, efficiency and effectiveness of government. They want to be able to use analytics to predict problems and anticipate trends, increase the use of virtualization, expand the use of modern technologies such as the Internet of Things, and move toward a "citizen first" model. Most significantly, our survey found that 58% believe a modern network would help improve agency cybersecurity (See Figure 2).

In many cases, however, existing networks hold agencies back. According to our survey, the biggest issue affecting agencies' ability to modernize their networks is budget (42%), followed by too many other IT priorities (28%); the limitations of legacy systems, models and protocols (27%); and multiple manual processes (18%) (See Figure 3).

Many legacy networks lack the capacity or speed to handle advanced processing and modern capabilities, often because they still run older protocols. Even if they have moved to Ethernet or Time-Division Multiplexing (TDM), they may still be using slower, less powerful services (See Figure 4).

For many agencies, the first step in enabling these next-generation capabilities is transitioning to the cloud. Although the move often makes sense, it also can highlight some of the weaknesses of older networks. Getting good performance to and from the cloud requires high performance, and older network infrastructure often doesn't allow for that.

Older networks also still use many manual processes. Though fine for smaller, relatively static networks, manual processes can become a big problem as networks scale.

"When you start getting into the cloud and adding more modern applications, your bandwidth demands increase and the variety and locations of the traffic go up," explained Jim Westdorp, Chief Technologist at Ciena Government Solutions. "The only solution is automation."

Figure 2

What are the top mission goals that a modern network would help you achieve? Up to 3 choices were allowed.

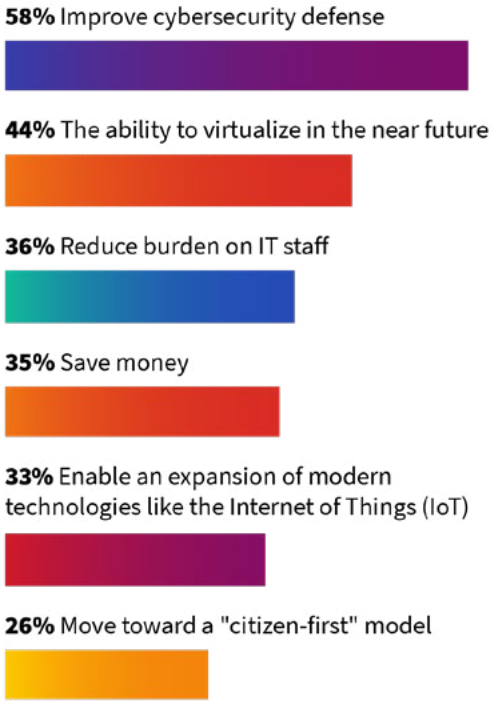


Figure 3

What are the biggest issues affecting your agency's ability to modernize your Layer 0-3 network? Up to 2 choices were allowed.

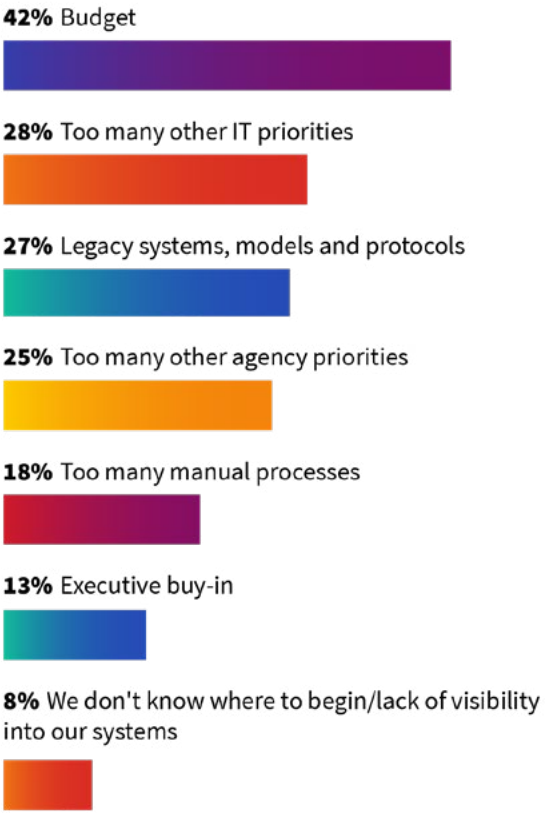
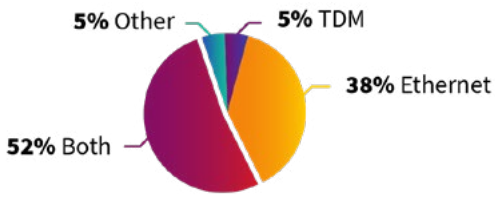


Figure 4

Does your agency's network use Time-Division Multiplexing (TDM) or Ethernet to handle your traffic flows?



*Data does not include respondents who said they did not know.

"You have to choose where you spend your money, and it makes sense to spend it modernizing the parts of the network that give you the most value: capacity, process and automation."

- Jim Westdorp, Chief Technologist at Ciena Government Solutions

Automating networks improves performance and efficiency and can reduce costs. Although it costs money up front to address process issues and add automation, the result is a network with drastically reduced operational expenditures.

Pick and choose

Many agencies know that they must modernize their networks, but they struggle to decide where to start. It's not necessary to replace the entire network all at once, which is too expensive and impractical anyway. Instead, pick and choose what to upgrade and in what order.

Before diving in, have an honest discussion with all stakeholders about what types of applications will run, what bandwidth different locations need, and what type of reliability and performance users and applications require. The results of those discussions will make clear what parts of the network to upgrade first. If your IT department has enough knowledge and expertise, it can perform this analysis itself. Some external providers can also perform a thorough network assessment and make informed recommendations.

"You have to choose where you spend your money, and it makes sense to spend it modernizing the parts of the

network that give you the most value: capacity, process and automation," Westdorp said. "It's about finding a way to live with existing legacy systems while growing with some of the new protocols."

It's important to choose an architecture and set of equipment with backward-compatibility with your legacy systems. There are two basic ways to approach this: You can either wrap your legacy analog protocols into a more modern TDM protocol such as OTN or convert it to Ethernet. The key is creating an adaptation layer at the edge of the network that lets you carry legacy protocols over to a new network while allowing for growth on newer protocols.

In many cases, agencies start by upgrading elements toward the edge of the network first and then upgrading the core. "That makes a lot of sense, because much of the intelligence and capabilities that provide dynamic services are provided by edge equipment," Westdorp added.

And don't underestimate the importance of network edge devices. As new applications develop and user needs change, it will become even more important to have flexible, programmable edge devices that can adapt to changing requirements.

Network Security: Always Top of Mind

Federal and regional leaders are all too aware of challenges around network security. At the federal level, the Office of Management and Budget (OMB) documented the problem in a 2018 report, pointing out that "agencies lack visibility into what is occurring on their networks, and especially lack the ability to detect data exfiltration."

The report notes that at the time, 73% of federal agencies were unable to determine when large amounts of data are removed from their networks. Today, the Cybersecurity and Infrastructure Security Agency (CISA) works with all federal departments and agencies on matters related to cybersecurity. One of CISA's main missions is to improve federal network security.

The problem is no less significant at the state and local levels. Cybersecurity is the top priority for state chief information officers (CIOs) in 2020, and state and local governments, recognizing the issues, have banded with CISA and the National Association of State CIOs to improve network security.

Despite these efforts, agencies at all levels of government are still very concerned about network security — 54% of respondents at the federal level cited it as a top concern with existing networks and it was a top priority for network modernization across all levels (See Figure 5). The majority also cited cybersecurity as a top mission goal that a modernized network would provide (See Figure 2).

As cybersecurity threats continue to change, networks must change with them.

"Older networks just weren't designed for the kind of aggressive cyber environment we find ourselves in today," said Westdorp. "They were designed to transport bits, but they aren't really security-aware."

Over time, agencies have added security tools such as

firewalls and deep packet inspection to their networks to improve cybersecurity. Those efforts are a good stop-gap measure, but a much more effective way to manage security as networks and threats evolve is to adopt a modern, modular network with automation and security built in. For example, a modern network should be able to analyze data flow to and from a network to identify patterns. This type of intelligence also allows IT staff to analyze configuration and provisioning, which can be part of the cybersecurity equation.

"A lot of times a network can be insecure because something was mis-provisioned, or somebody made a change in the network without really understanding what the second- and third-order effects of those changes would be," Westdorp explained.

Automation goes hand in hand with intelligence in securing networks. It enables networks to handle provisioning tasks instead of delegating those tasks to humans, who can make errors.

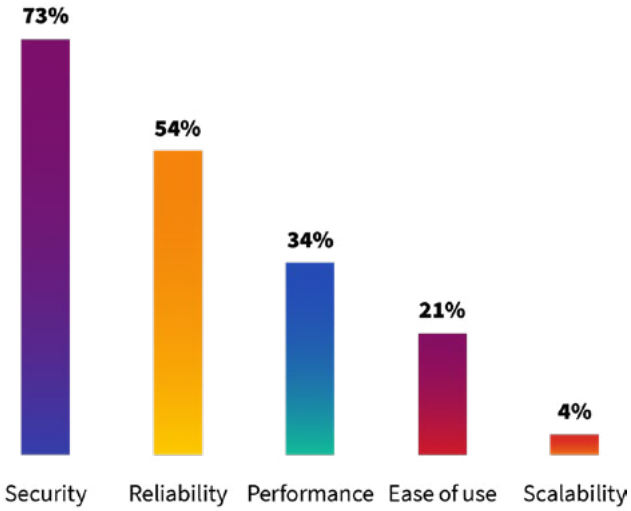
The combination of automation, intelligence and modularity can significantly increase visibility — something OMB considers a major drawback of current networks. Using these capabilities to monitor and analyze networks not only helps ensure peak efficiency and service continuity, but can help solve difficult problems that threaten network security.

"As an industry, we're still figuring some things out, but there are a few things we know for sure: Intelligence, visibility, automation and modularity are critical."

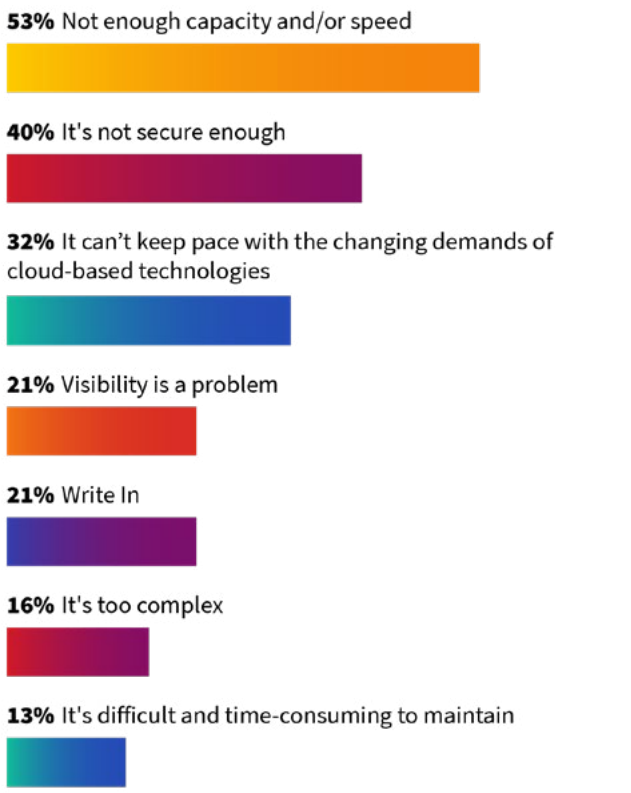
- Jim Westdorp, Chief Technologist at Ciena Government Solutions

Figure 5

What are your top priorities for network modernization? Up to 2 choices were allowed.



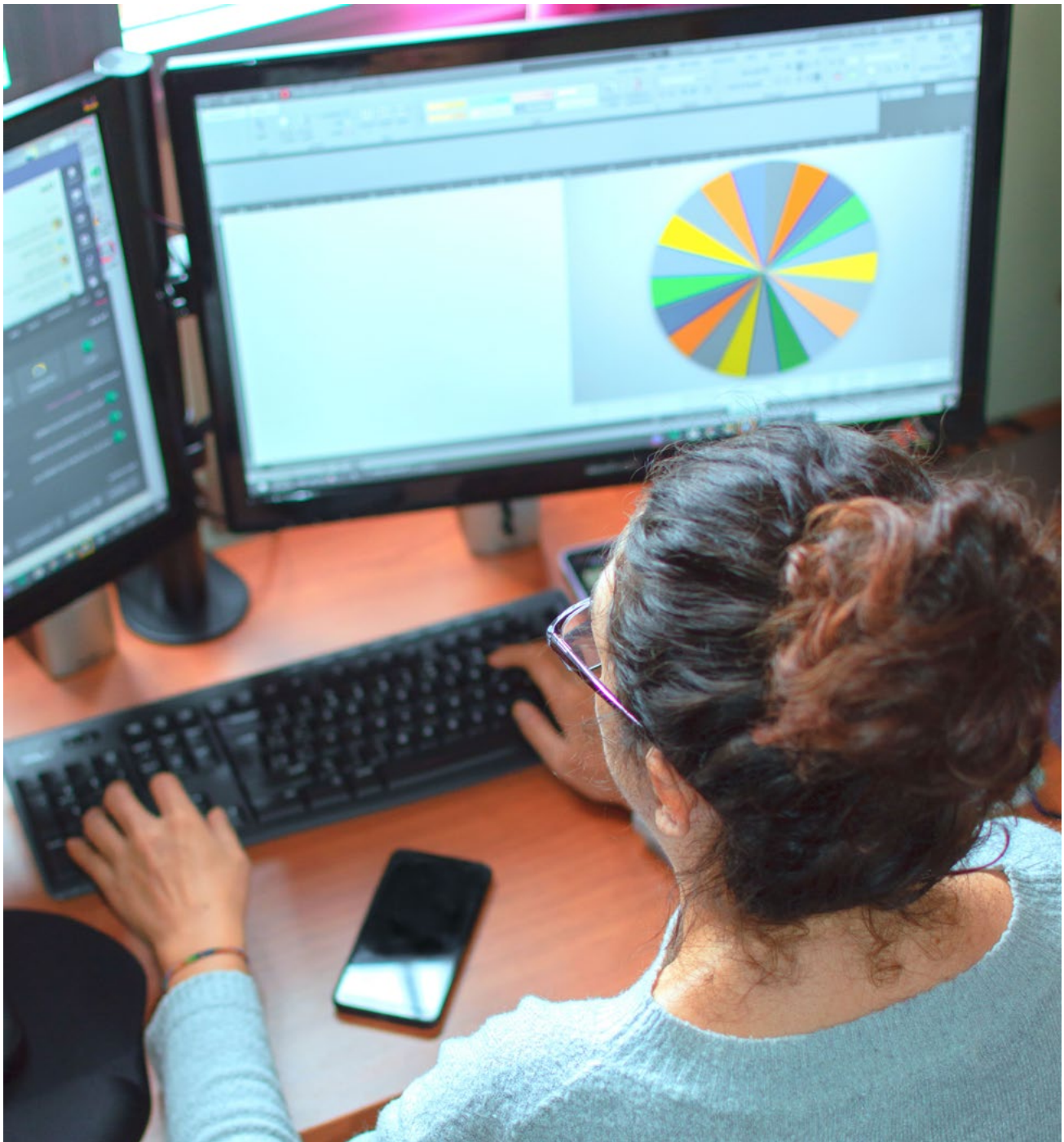
If you answered "somewhat" or "no," what are your biggest concerns?



In one case, a government agency was experiencing so much latency that it could not replicate highly sensitive data to a central repository. Despite attempts to uncover the problem, the agency was able to solve it only after deploying intelligent route technology that had full visibility into the transport network's core. With this technology, the agency was finally able to isolate the root cause and show not only that the network was at fault, but exactly how it was failing. Once the agency knew the cause, it was relatively simple to fix the problem.

Keeping networks secure is an ongoing challenge for agencies and vendors.

"As an industry, we're still figuring some things out, but there are a few things we know for sure: Intelligence, visibility, automation and modularity are critical," Westdorp said. "Without these, you can't confidently control how data is flowing or analyze the information coming from the network, and those are the keys to effective overall cyber protection."



The Adaptive Network

When it comes to networks, agencies know what they want: better reliability and security, ease of use, reasonable costs, and reduced complexity. They want their networks to be more intelligent, capable of automating time-consuming tasks, and according to our survey, 47% of respondents want to be able to use analytics to predict problems and anticipate trends (See Figure 6).

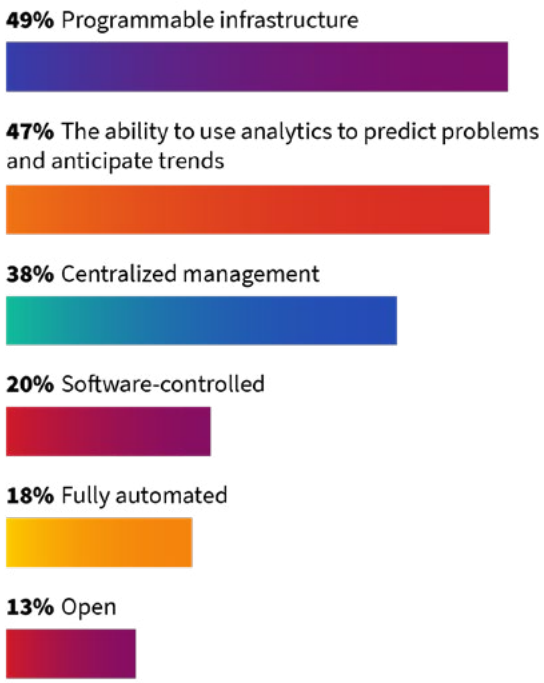
These features are critical to helping agencies accomplish what they want, and to remain secure and fully functional going forward.

A ***programmable infrastructure*** allows network professionals to monitor the network's physical and virtual elements and extract information about network health, how it is operating, and what type of load it is experiencing. An effective programmable infrastructure will be very intelligent, capable of interpreting data so the network can make decisions about traffic routing and other issues. In most cases, programmable devices that can transport information provide programmable infrastructure.

Analytics and ***intelligence*** is another component of the Adaptive Network. Working in tandem with the programmable infrastructure, real-time predictive and prescriptive analytics can help network operators make critical decisions. It can also help the network learn information about traffic patterns and vulnerabilities and adjust as needed.

Figure 6

What are the most important attributes of a modern network? Up to 2 choices were allowed.



The third part of the Adaptive Network is ***software control*** and ***automation***, typically software that implements the identified changes. Centralized software-defined orchestration is critical to simplifying end-to-end management, security, efficiency and reliability.

In a nutshell, the Adaptive Network is an automated, modular, comprehensive approach to optimizing network flows in a closed-loop process that ties everything together.

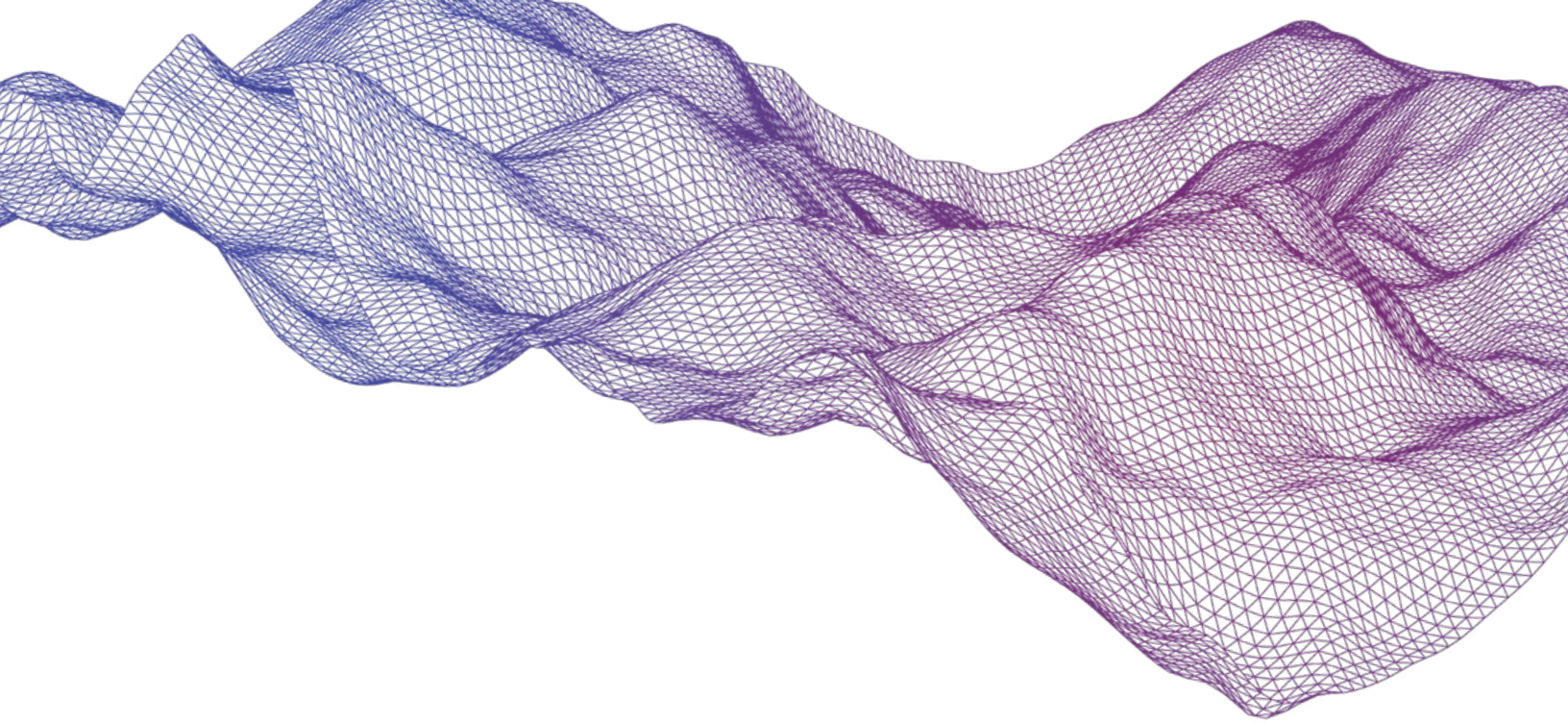
In a nutshell, the Adaptive Network is an automated, modular, comprehensive approach to optimizing network flows in a closed-loop process that ties everything together.

“Think of it as a loop that starts with an intelligent, programmable packet and optical infrastructure that streams information to the analytics function. The analytics function uses machine learning and artificial intelligence to determine the state of the network, predict potential network problems and anticipate trends,” Westdorp explained. For example, it may require moving some flows around or changing capacity in certain areas.

The next stop on the loop is orchestration software, which determines how to implement the changes that the analytics function recommends. In Ciena’s case, this consists of Multi-Domain Service Orchestration, federated inventory, and centralized, software-defined control of individual network domains. And off to the side, but still a key enabler, are supporting services that can increase optimization and insights.

This type of next-generation approach to networking has many benefits. It helps resolve network problems before they become unwieldy, allows organizations to use unused network margin to improve scalability and reduces time to resolution for trouble tickets.

The automation and intelligence of the Adaptive Network also can help agencies meet the requirements of fast-growing networks. Instead of having to hire more employees to run the network – an expensive and difficult undertaking – a more modern network can meet all requirements without additional human resources.



How Ciena Helps

Ciena provides government agencies with a range of network services, including network infrastructure modernization and software-driven network virtualization. Its Adaptive Network helps agencies optimize existing networks while incorporating new technologies and ways of working. By combining the best of existing networks with automated, intelligent, modern technologies, agencies can economize while creating a future-proofed infrastructure that still supports legacy systems and applications.

Ciena continues to innovate, most recently, by converging packet and optical layers into a single device. This ensures the programmability of the network infrastructure layer to enable real-time response to changing mission needs. Its Blue Planet® software is at the forefront of developing and implementing software-defined networking and network functions virtualization solutions that enable an innovative approach to creating virtualized networks, without requiring organizations to dismantle their existing networks.

Conclusion

Agencies today must find ways to keep networks and data safe while fostering next-generation capabilities that require performance and agility. In most cases, this requires modernizing existing networks.

Instead of the “rip and replace” mentality that has typically accompanied this type of modernization, newer technologies, combined with automation, intelligence and modularity, allow agencies to mix legacy elements with modern capabilities. With the right guidance, technologies and tools, agencies can transform their aging networks into a dynamic, intelligent, mission-centric and secure strategic tool that enables new services, improves cyber resiliency and speeds mission response.

About Ciena Government Solutions

Ciena (NYSE:CIEN) is a networking systems, services, and software company. We provide solutions that help our customers create the Adaptive Network™ in response to the constantly changing demands of their users.

By delivering best-in-class networking technology through high-touch consultative relationships, we build the world's most agile networks with automation, openness, and scale.

To learn more visit ciena.com.

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

www.govloop.com | @GovLoop

1152 15th St. NW Suite 800
Washington, DC 20005

P (202) 407-7421 | F (202) 407-7501
www.govloop.com
@GovLoop