As Cybersecurity Threats Evolve, Government Networks Must Change with Them

ciena

Government IT leaders know that with innovation often comes risk. As agencies look to modernize their infrastructure, they must also take proactive measures to ensure their network is secure—especially as more workers transition to telework and cyberattacks become even more advanced.

In fact, according to a survey from Science Applications International Corporation, 82 percent of federal employees expect remote work to continue into the future. Moreover, 41 percent of respondents expect to work remotely four or five days a week—more than twice the average number prior to the pandemic.

Part of the challenge of remote work is that it widens the attack surface. "You move from defending one primary office to defending potentially hundreds or thousands, with endpoints now living in each employee's home instead of a central office building," says Jim Carnes, Chief Security Architect at Ciena Government Solutions, Inc. "As you move everybody out to the edge, you now have to protect end points that are sitting at each employee's home."

Another cybersecurity risk of remote work is the increased reliance on public networks. Unfortunately, without proper encryption, data traveling across a public network runs the risk of being intercepted by bad actors, which could lead to dire consequences. Carnes warns, "If a global infrastructure dependent upon public networks suffers a disruptive attack on its confidentiality or integrity, it may not only disrupt communications, but could affect the life of a U.S. soldier."

The power of the Adaptive Network™

No wonder government agencies are increasingly looking for ways to upgrade their current networks to ease these concerns and mitigate cybersecurity threats as they evolve. According to a recent Ciena and GovLoop survey of 80 federal, state and local government employees, nearly 62

"As you move everybody out to the edge, you now have to protect end points that are sitting at each employee's home."

Jim Carnes
Chief Security Architect
Ciena Government Solutions

percent of respondents believe that a modern network would help improve their cybersecurity defense. The majority of respondents (75 percent) rank security highest among the top priorities for network modernization, followed by reliability (56 percent), performance (31 percent), and ease of use (21 percent).

A network's adaptability relies on its ability to self-configure and optimize based on constantly changing demands and emerging security threats. For example, by proactively providing updates based on occurrences, such as a potential security threat, Ciena's Adaptive Network can dynamically alter the route of traffic. This translates into a network system that reconfigures automatically, updating traffic flows in real time to meet security considerations.

"The ability to have a network that can quickly reconstitute itself, bring up new defenses, and mitigate attacks much faster is incredibly important," says Carnes. "Recognizing what's going on in a network and having the ability to respond is really what's at the core of the Adaptive Network."

Programmable hardware and innovative encryption techniques are also key advantages of Ciena's Adaptive Network when it comes to meeting the most stringent security requirements. "Legacy hardware that requires agencies to physically send someone out to a site to make changes just doesn't work in today's environment," says Carnes.

Fortunately, programmable infrastructure can ensure continuous protection of not only data at rest—including data residing in databases, files, and storage systems—but also data in flight. This is critical, as Carnes explains, "The minute you start transmitting data from any two locations, there are risks to confidentiality, integrity, and availability."

Ciena's Adaptive Network vision Learn More

SURVEY RESULTS

80 federal, state and local government employees were asked to rank their top priorities for network modernization. These are the percentages of participants who agreed on the ranking.

75%
RANK
SECURITY
#1

56%
RANK
RELIABILITY
#2

31%
RANK
PERFORMANCE
#3

21%
RANK
EASE OF USE
#4

Securing certainty

At the same time, in-flight encryption techniques can camouflage traffic, preventing intruders from reading or manipulating data as it traverses the network, even disguising the fact that there is traffic flowing at all.

From there, government IT leaders can layer on enhanced analytics-driven intelligence with Artificial Intelligence (AI) and machine learning (ML). An integrated network analytics and machine learning framework, such as Blue Planet® Unified Assurance and Analytics (UAA), provides agencies with actionable insights from network performance data by using AI and ML to interpret, recommend, and act based on real-time data within predefined policies.

But even actionable insights can prove counterproductive if they're riddled with inaccuracies, burdening government IT teams with false alerts of potential security vulnerabilities.

"An overly instrumented network without a lot of tuning is actually worse because you're training staff to ignore security alerts," says Carnes. Instead, he recommends tightening the telemetry and the measurements on particular network segments so that detecting an anomaly comes with a high degree of certainty, thereby eliminating false positives.

Even more certain is that Ciena's Adaptive Network offers the perfect combination of security capabilities—from always-on, high-capacity, wire-speed optical encryption to user authentication and intrusion-detection forensics. "It will become more and more central to agencies' ability to perform their mission and provide critical services," says Carnes. "Because if the network isn't secure, the mission can't be."

Gain more mission-critical insights Learn More

Was this content useful?

Yes No

* As a supplier of equipment and services to government agencies Ciena takes a comprehensive approach toward maintaining the security and continuity of its supply chain