Visibility and the quest for **zero trust**

Telework is here to stay; agencies must adapt with pervasive network visibility and analytics

Dennis Reilly
Vice President of Public Sector, Gigamon

THE RAPID MOVE TO TELEWORK during the COVID-19 pandemic was initially a continuity-of-operations issue. But now we are seeing some interesting reports that federal workers are as productive when they work from home as they are in the office — maybe even more productive. As a result, many people may continue working from home even after the pandemic recedes.

Adapting a security model to that new normal will be crucial. Visibility into network traffic will remain essential and become particularly challenging with the increased use of personal devices that are not managed by the enterprise.

Those challenges extend beyond federal agencies and affect the broader public sector because state and local governments and educational institutions face similar issues in providing citizen services and distance learning.

Using visibility to enhance existing tools

For the foreseeable future, agencies will use a blend of on-premises data centers, virtual environments, and public and private clouds. To better manage and protect those resources, agencies must have maximum visibility into all their data, including data in transit and encrypted data.

A unified solution that provides pervasive visibility and manages information from a single pane of glass is increasingly important. That visibility enhances the security tools agencies are already using to defend their networks and improves the way they detect, investigate and respond to cybersecurity threats.

In addition, zero trust architecture has gained a lot of momentum in the federal government. However, although agencies report that 80% or more of their network traffic is encrypted, we have seen that only about 30% is actually inspected. It's a significant blind spot that must be addressed. Without pervasive visibility into data in motion — whether it's in a physical or cloud-based environment — agencies can't implement a zero trust architecture.

Gaining better insight into network traffic

One of the best ways to address that blind spot is by deploying a next-generation network packet broker, which can decrypt traffic and then allow the agency's suite of cybersecurity tools to inspect it. That approach removes the decryption responsibility from the cybersecurity tools and allows them to operate at maximum efficiency.

Agencies still face challenges in fully staffing their security operations centers, which continue to be plagued by excessive false positives. A strong network detection and response capability alleviates that burden and allows security teams to triage and address the highest-risk threats first.

To achieve a robust security posture, agencies must have pervasive visibility into their entire IT infrastructure and all the data that traverses it. ■

Dennis Reilly is vice president of public sector at Gigamon.