Cybersecurity starts **with visibility**

A pervasive view into far-flung networks is essential, and next-generation packet brokers can help

Dennis Reilly
Vice President of Federal, Gigamon

IN TODAY'S RAPIDLY evolving threat landscape, agencies can't protect what they can't see. They need a clear view of all the traffic on their physical and virtual networks, and as more agencies shift workflows to the cloud, they must extend their visibility into that area as well. Even in cloud environments, agencies remain responsible for the security of their data and applications.

Pervasive visibility is necessary to quickly identify breaches and the lateral movement that could signal that an adversary is conducting command and control or setting the stage for data exfiltration.

Further, agencies must have a view into the estimated 78 percent of traffic that's encrypted. Adversaries can go largely undetected in encrypted channels, which means that what used to be a secure channel is now a threat vector. It's one of the reasons why it took so long to discover the Office of Personnel Management breach in 2014.

Agencies can see into encrypted traffic through a technique called "break and inspect," which involves "breaking the traffic," decrypting it, inspecting it, re-encrypting it and sending it down the network line.

Maximizing the return on investment

A next-generation network packet broker (NGNPB) can play a key role in all those areas. It's a force-multiplying technology that helps the government achieve the greatest financial return for every cybersecurity dollar it invests while also ensuring that agencies receive the maximum return in terms of readiness and a stronger cybersecurity posture.

With an NGNPB, agencies can have their cybersecurity, network and application tools performing at peak capacity. Given the fact that agencies typically use dozens of tools to see, secure and manage the data going across their networks, an improvement in efficiency of just 20 percent would be a tremendous return on investment.

In some cases, NGNPBs can achieve a fivefold productivity improvement. In a recent study, Forrester Research discovered that the technology can reduce cybersecurity costs by 50 percent and pay for itself in just seven months.

Staying ahead of adversaries

The government has recognized the value of such force-multiplying technologies by making them available through the Department of Homeland Security's Continuous Diagnostics and Mitigation program. As agencies continue their digital

davooda/Shutterstock/FCW Staff

> A secure, well-performing network results in satisfied internal and external customers. And **it's essential for reaping the benefits** of machine learning and automation.

transformation and seek to modernize their infrastructure on a limited budget, a program like CDM becomes even more critical as a way to give a booster shot to cybersecurity efforts.

However, because it can be challenging for the government to keep up with adversaries who are investing in machine learning and round-the-clock operations, agencies must continue exploring new ways to recruit and retain talented cybersecurity professionals even as they automate routine tasks and reserve the higher-order activities for our scarce human resources. In addition, the government needs to adopt force-multiplying technologies like NGNPBs to catch up, get ahead and then stay ahead of adversaries.

It all comes back to knowing who's on the network, what's happening on the network and how the data is traversing the network. Agencies must have that pervasive visibility so that they can manage and defend their IT infrastructure. A secure, well-performing network results in satisfied internal and external customers. And it's essential for reaping the benefits of machine learning and automation. ■

Dennis Reilly is vice president of federal at Gigamon.