FCW | Workshop

Article Source: FCW Zero Trust Workshop | May 4, 2022

The Network Still Matters

Network visibility is a cybersecurity necessity and foundational to a zero trust architecture

AGENCIES LOOKING TO ACCELERATE their move to a zero trust architecture should improve network visibility to better manage and protect their data and bolster their overall cybersecurity posture.

Organizations need actionable intelligence about what is happening on their network, especially as the volume of network traffic they manage on a daily basis continues to grow. The traditional approach of installing more cybersecurity instrumentation is inefficient, costly, and prone to human errors.

Pervasive visibility into network data-in-motion—whether it is on-premises, virtual or in the cloud—will help agencies secure their enterprise and bolster their efforts to achieve zero trust.

> “We look at the network as the single best version of the truth. If something happens on the network, there is going to be a record of that.”
>
> DENNIS REILLY
> Vice President, Public Sector,
> Gigamon

“The network still matters,” said Dennis Reilly, vice president of Public Sector at Gigamon. “We look at the network as the single best version of the truth. If something happens on the network, there is going to be a record of that.”

Organizations need data about network traffic, assets and infrastructure to make informed decisions about access, he said.

For instance, if an adversary penetrates the enterprise and starts to move laterally or stages data in preparation to steal it, network visibility will help agencies interrupt that attack quickly.

Visibility also enables network segmentation and micro segmentation and ensures networks are monitored within and between segments.

“You don’t want to disrupt network activities, or break the network when you are moving toward that segmented construct,” Reilly said. “Having visibility into traffic-in-motion is essential for that.”

Segmentation increases the need for organizations to decrypt and inspect network traffic, but maintaining visibility into the network will help agencies detect anomalies that cannot or should not be decrypted.

SPONSORED BY: Gigamon®

A GOVFORWARD™ Event

"Visibility into what is going on into the network through a visibility fabric powered by a next generation packet broker will be critical," he said. "Ultimately, what you want to have is no blind spots. You can't defend what you can't see."

Agencies should analyze network traffic data to mitigate risk from incomplete end point coverage, and to detect lateral movement of threats. Endpoint detection and response systems "can't monitor all end points," he said.

In the Colonial Pipeline attack, for example, the hackers tuned down the logging on the end point detection and response system, making it difficult for them to be detected.

"You can't trust any one component or any one technology," Reilly said. "You need to have defense-in-depth, and you need to be able to validate against various records you have in your system."

> "Visibility into what is going on into the network through a visibility fabric powered by a next generation packet broker will be critical... Ultimately, what you want to have is no blind spots. You can't defend what you can't see."
>
> **DENNIS REILLY**
> Vice President, Public Sector,
> Gigamon

In a recent zero trust pilot program, Gigamon showed the Defense Department's DreamPort cyber innovation facility the benefits of network visibility into its physical, virtual and cloud environments.

The pilot showed that their network was vulnerable to lateral movement, and that the agency lacked a global picture of what was going on. The SPAN ports being used to pull traffic from the router switch architecture to the cybersecurity tools weren't providing the right kind of fidelity, and tests into unauthorized access that should have tripped alarms, didn't.

The Gigamon packet broker provided complete visibility into key traffic paths in all network environments, was able to optimize and scale tools over time, and helped control costs by reducing redundant packets, Reilly said. The next phase of the pilot will add cloud visibility and inline TLS decryption to the visibility fabric.

Focusing on the network pillar of zero trust architecture helps agencies gain pervasive visibility and secure their IT and operational technology systems, Reilly said. "A next generation network packet broker can be a force multiplier because it helps an agency get so much more out of the instrumentation it has already invested in." ■

The Network Pillar: Leveraging Network Traffic Visibility to Accelerate Zero Trust

MF3d / iStock