Gigamon Adds Crucial Network Visibility to Zero Trust at the Department of Defense

> The Gigamon platform enables us to feed all the different tool sets we have acquired and offers us X-ray capability, not only in the physical world but also in the virtual world."
>
> DAVID JONES
> Department of Defense

CHALLENGES

+ Zero Trust initiative lacked visibility across the entire network
+ Vulnerable to lateral movement
+ Privilege escalation from adversaries

SOLUTION

+ Gigamon Deep Observability Pipeline
+ GigaVUE-FM (fabric manager)
+ GigaVUE V-Series virtual nodes
+ GigaVUE-HC3 nodes
+ GigaVUE TA10 traffic aggregators
+ GigaVUE OS
+ GigaSMART® Application Intelligence
+ Flow Mapping®
+ GigaSMART Packet De-Duplication

CUSTOMER BENEFITS

+ Brought full visibility across on-premises, virtual, and cloud networks
+ Reduced noise to allow for deeper analysis
+ Enabled intricate packet inspection to get to the root of issues
+ Integrated tasks to boost overall efficiency

ADDRESSING NETWORK VULNERABILITIES AT THE DEPARTMENT OF DEFENSE

The problem all started in late 2018, when the Department of Defense (DoD) conducted an assessment on certain classified networks. They discovered alarming shortcomings in both network visibility and security.

"We'd known for years that the perimeter defense was a bit aged," says David Jones, Chief Architect for Zero Trust Cloud, at the DoD. Security was based on when the internet first started, and being able to defend it was getting harder."

Of the shortcomings, three stood out:

+ First, the network was vulnerable to lateral movement. The agency needed to limit East-West traffic once someone had gotten beyond the perimeter.
+ Second was privilege escalation: People who didn't have privileges — including adversaries — were garnering credentials and gaining access where they shouldn't.
+ Third and most notable was the lack of visibility across the physical, virtual, and cloud network. "We didn't have a global picture of what was going on. During the assessment, we conducted tests that should have — but didn't — trip any alarms because the visibility wasn't there to sound the alarm," David adds.

A PUSH TOWARD A ZERO TRUST ARCHITECTURE

In response to the discovery, the Defense Information Systems Agency (DISA), United States Cyber Command (USCYBERCOM) and National Security Agency (NSA) joined forces to evaluate the potential of moving toward a Zero Trust Architecture to shore up network security.

PROTECTING THE CROWN JEWELS: DATA

David says that Zero Trust enables protection of an organization's crown jewels: the data. It lets you switch from focusing on protecting network flows, where you might trust things that shouldn't be trusted. Instead, "With Zero Trust, we protect the data and work outward from there to applications, servers and networks."

Starting in January 2019 and over several months, the team worked on a prototype to demonstrate that a Zero Trust Architecture could solve many of the DoD's network security challenges. "We wanted to create a rudimentary Zero Trust environment that enabled us to see what was going on in the network and respond in real time versus just depending on logs," he says.

A cybersecurity architecture based on Zero Trust principles moves away from implied trust based on network location and perimeter-based security alone and instead continuously evaluates trust on a per-transaction basis to ensure data is protected. This makes Zero Trust particularly well-suited for defense and intelligence applications as users become more geographically distributed and as public cloud usage grows.

EARLY DECISION NOT TO INCLUDE VISIBILITY THREATENED THE PROJECT

At first the implementation did not include Gigamon visibility solutions, but midway through the team determined that the Gigamon Deep Observability Pipeline was critical to tie everything together and provide crucial visibility into the physical, virtualized, and cloud environments.

"We ran a test and realized we couldn't see certain events because we're weren't inspecting the packets going across the wire. At that point, phone calls were made, and we brought Gigamon on," he says.

PHASE 1: THE VISIBILITY IMPLEMENTATION

The team and Gigamon started with the physical network, and as the project moved along, implemented the virtual Software-Defined Networking (SDN) environment, where they were able to leverage GigaVUE-HC3 appliance to gain pervasive visibility into both physical and virtual traffic. Gigamon controls and decouples packet collection, aggregation, and delivery of data to tools. This provides each tool or sensor with the exact data needed, dramatically reducing tool load and enhancing tool efficiency and scalability.

The Gigamon Deep Observability Pipeline gives agencies adopting Zero Trust a single pane of glass to collect, process and forward data to the policy engine supporting their implementation, as depicted in Figure 1.

ADDED BENEFIT: EFFICIENT TOOLS

By reducing irrelevant and duplicate packets, Gigamon also brought new efficiency to the team's network and security monitoring tools. Greater efficiency is accomplished by using GigaSMART® traffic intelligence capabilities, such as De-duplication, SSL/TLS Decryption, Packet Slicing, Application Metadata Intelligence, and Application Filtering Intelligence, to generate efficient custom data sets for tools and sensors.

"Being able to shrink the packets and metadata lets us monitor more data because we're giving tools exactly what they need instead of the whole universe," he says.

David further states that the tools not only perform better because they're no longer overstressed, but they also produce better data. "It's almost like an efficiency drill by getting rid of a lot of the waste," he says. For tool costs that are based upon consumption of data, this can produce significant cost savings and control for operational budgets.

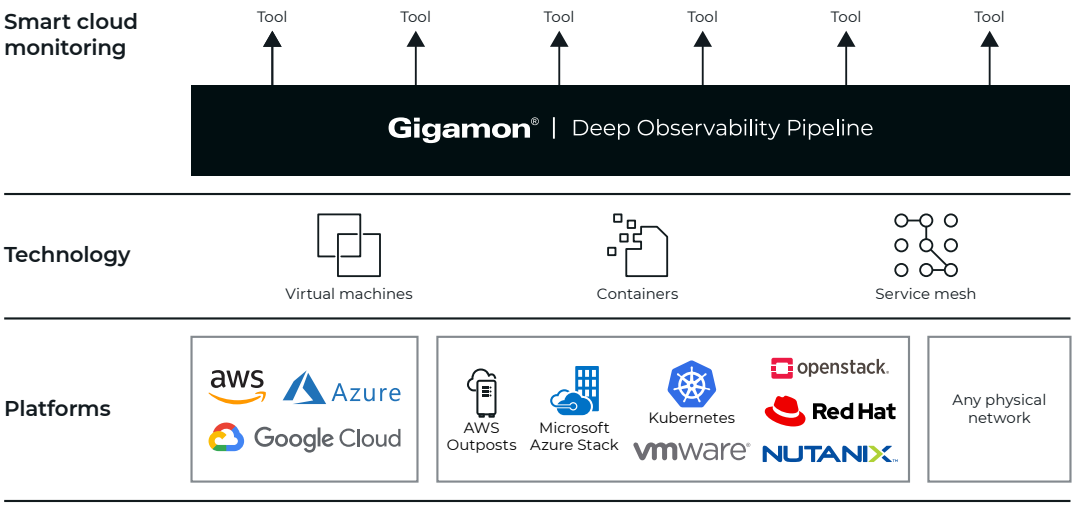

Figure 1: Gigamon technology and platform coverage

PHASE 2: CLOUD VISIBILITY

Following the success of the DoD physical deployment, a second project phase has extended the reference architecture to cloud platforms to support the next generation of DoD IT initiatives.

Gigamon is playing a central role in this phase through its ability to provide a unified view of activity across traditional data centers, private cloud environments and multi-provider public cloud deployments, as shown in Figure 1. This approach aligns well with broader DoD and IC security requirements, including those outlined in the "DoD Cloud Computing Security Requirements Guide."

ABOUT GIGAMON

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

DAVID'S ADVICE FOR A SUCCESSFUL ZERO TRUST ROLLOUT

#1 Use universal visibility to truly know your network

The biggest key to Zero Trust is understanding what data you want to protect, where it's located and what data gets into your visibility layer. And only full visibility will tell you if you're successful at protecting access to your data.

In contrast, if you cannot see what's going on, you'll be blindly applying security rules and won't know if they're effective. Furthermore, you don't want service tickets to act as your leading indicator of a problem. Instead, you need to see problems before they arise to the level of a user problem.

#2. Work hard to change the culture

Equally important, you've got to work continuously to your organization's culture to embrace Zero Trust — including from the CTO's office. Zero Trust will bring difficult growing pains, but if you get enough people onboard at the beginning, it's much easier.

"The new expectation is that everyone does NOT need access to everything — even if you are the CTO," David says. "In the end, however, these rules benefit everyone."

© 2020–2023 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com