Case Study

Gigamon Enhances Mobile Identify’s Security to Strengthen Attack Preventions

> I’m impressed with the Gigamon Deep Observability Pipeline. It’s easy to consume and self-explanatory. The documentation is also very good. It’s easy to understand for those that didn’t install it. The fact that it’s taking something fairly complicated and simplifying it is pretty impressive.

DANIEL DUDKIN
Network Architect, Mobile Identify by Bastion

Challenges

- Tapping into VMware NSX-T traffic flows
- Maintaining compliance with ISO 27001 Information Security Certification
- Simplifying a complex architecture for greater ease of use
- Feeding NSX-T traffic into Vectra AI detection software

Customer Benefits

- Production of evidence to maintain ISO Certification
- Significantly less CPU consumption than a homegrown solution
- Ability to do load balancing and filtering
- Full visibility of the environment for improved threat detection

Solution

- Gigamon Deep Observability Pipeline
- GigaVUE Cloud Suite™ for VMware

About Customer

Mobile Identify by Bastion is a SaaS company based in Dublin, Ireland, that provides fraud prevention and mobile identity authentication to all of Ireland's largest banks and the majority of its credit unions. The company's technology processes over 200 million transactions per year for 100 financial institutions.

"As more people are banking through their phone, it has become critical for banks to clearly identify if the person who has the bank account is the same person using the app on their phone," explained David Morrisey, one of the inventors of the technology.

A common type of fraud in financial services is SIM swapping, where the fraudster convinces a telecommunications operator to swap an actual customer's phone number onto a replacement phone and SIM card. Once the fraudulent SIM card is enabled, the real customer's phone stops working, and the fraudster is able to intercept text messages, install apps, and try to access the customer's banking. Mobile Identify intercepts this type of fraud across Ireland.

Business Challenge

The company recently expanded to two high-availability physical data centers at different locations, with a private circuit running between them. Each location hosts its own VMware kit. The company is contractually obligated to run its own kits and has no cloud presence.

Mobile Identify moved into its new dual data center architecture with VMware NSX-T virtualization and security technology that allowed them to create virtual networks from their physical networks. Once the upgrade was complete, the team realized that the company needed to phase out its legacy solution and deploy a new generation network detection and response (NDR) or extended detection and response (XDR) solution to gain visibility into this traffic. Previously, the company operated a single data center and relied on an older generation XDR solution that functioned like a moat around its perimeter-based network. With this solution, the security team did not have the high degree of visibility they needed to protect against the types of threats they expect to see in the future, attack vectors, and data exfiltration attempts.

Daniel Dudkin, the network architect for Mobile Identify, developed a homegrown solution to get the traffic flow from the VMware environments, but it cost an "incredible" amount of CPU resources. He was concerned about having to eventually acquire more hardware to solve constraint problems that would be caused by this heavy burden on CPU resources.

Another key challenge was compliance. Although the company does not deal directly with banking customers — it does not hold personal information or banking data — it does deal with data from the mobile networks, which is considered personally identifiable information (PII) data. For this reason, the company is ISO 27001 Information Security Certified, and its new visibility solution would have to help check that box.

Resolution

Mobile Identify worked with UK-based Vizst Technology, named Gigamon 2023 Cloud Partner of the Year, to deploy GigaVUE Cloud Suite for VMware at each of Mobile Identify's data center locations. The deployment started with a proof of concept (POC) to demonstrate how GigaVUE® could get greater visibility into traffic flows from the NSX-T environment.

Daniel was pleased with the smooth onboarding process and excellent support he received from the Vizst Technology team. "It was click, click, click, deploy. The GigaVUE Cloud Suite was really easy to bring up, and we had it running in a matter of days," he shared. Once the GigaVUE Cloud Suite was up and running, it was an easy decision to fully deploy the solution.

The ease of deployment came as a huge relief to Daniel. He had recently attempted installing a different solution to replace his homegrown one, but the solution consumed costly CPU resources and even caused an outage. "It was a terrible experience, and I was very afraid to try it again. But with Gigamon, it just worked and didn't cause me a problem," he confirmed.

Benefit

Ankit Dhyani, who oversees risk and compliance for Mobile Identify, was impressed by how quickly and efficiently the Vizst Technology team solved his requirements with the GigaVUE Cloud Suite. “I’ve talked to many people over the months when searching for a solution, but what stood out to me was Gigamon and the Vizst Technology team’s focus on removing the pain points from our journey in a very short amount of time,” he said. With the GigaVUE Cloud Suite, he now has easy access to the logs he needs to maintain the company’s ISO certification.

From Daniel’s perspective, the benefits of leveraging Vizst’s expertise with Gigamon became apparent quickly. “The onboarding and the support from Vizst Technology was built into the cost, and it was worth every penny,” he remarked.

Mobile Identify is now tapping 100 percent of the environment and consuming significantly less CPU power. Daniel set up load balancing between two generic routing encapsulation tunneling (GRETAP) interfaces and put filtering in place as well so he could eliminate the noise and optimize his feeds for improved threat detection.

About Vizst Technology

Vizst Technology is a privately owned, UK-based technology partner, supporting SME, enterprises and public sector organisations with technologies and strategies to enable and improve business performance.

From networking and cyber security to visual solutions and meeting rooms, Vizst provide full-service, innovative IT strategies and solutions that simplify complexities and reduce stress for our customers.

As one of only two platinum Gigamon partners in the UK, Gigamon Cloud Partner of the Year 2023 and Gigamon Marketing Partner of the Year 2023, Vizst are best placed to support customers in their cyber security and networking strategies. To learn more, please visit vizst.com.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived intelligence to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit gigamon.com.

Gigamon®

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