Case Study

Corpay Safeguards Its Large Multi-Cloud Environment with Gigamon

Cloud visibility is extremely important to us, and Gigamon allows us to understand our traffic and potential threats and gives us the ability to be proactive with any threat intelligence we get.

WADDAAH KEIRBECK
Global Chief Technology Officer

Challenges

- Insufficient East-West visibility in a large, segmented multi-cloud environment
- Needing to accelerate Mean Time to Resolution (MTTR)
- Struggling with limited and outdated technologies
- Maintaining a high level of security while migrating workflows to the cloud

Customer Benefits

- Achieved advanced cloud visibility into East-West traffic
- Fully integrated, with the ability to forward traffic to other monitoring, management, and security tools
- Improved understanding of traffic and potential threats
- Proactive use of threat intelligence that comes in

Solution

- GigaVUE® HC Series
- GigaVUE-FM
- GigaVUE TA Series
- Application Metadata Intelligence (AMI)

About Customer

Headquartered in Atlanta, Georgia and founded in 2000, Corpay (formerly FLEETCOR Technologies) is a global financial technology (fintech) company with 10,500 employees. Its corporate spend management platform helps organizations manage and control business expenses, employee spending, and accounts payable processes with simplified and automated digital solutions. Corpay integrates with common accounting systems to streamline bookkeeping, increase employee efficiency, and provide real-time reporting and analytics.

Waddaah Keirbeck, Corpay Global Chief Technology Officer, explained that the company employs a multi-cloud strategy with private clouds in VMware and Nutanix, as well as public clouds in Amazon Web Services (AWS) and Microsoft Azure. The rationale for this hybrid multi-cloud approach is cost and compliance regulations. As a financial sector company, Corpay is required to adhere to PCI-DSS 4.0 global standards as well as the Sarbanes-Oxley Act (SOX). For now, its core business applications will continue to be in private clouds, while its back office is moving to Azure.

Business Challenge

The key challenge Keirbeck was looking to solve for Corpay was advanced visibility. He needed the ability to monitor East-West traffic, which was his greatest security concern with moving workloads to the cloud. In addition to improving cloud visibility, Corpay needed a solution to accelerate Mean Time to Resolution (MTTR) and mitigate performance bottlenecks and latency in its network.

Prior to Gigamon, the company was using another vendor's solution for network visibility and performance monitoring but was not happy with the results. Although the legacy solution had a deduplication capability, overall, Keirbeck described the technology as "limited and outdated."

Corpay's application performance tools were also unable to provide the needed visibility into East-West traffic that is important to Keirbeck for security. The team also struggled to make use of an existing network detection and response (NDR) tool, but they found that it too was insufficient to meet their needs, as it was "flooded with irrelevant NetFlow traffic data," as Keirbeck explained.

Resolution

After researching the options and performing tests on multiple solutions, Keirbeck determined that Gigamon was the best choice for Corpay to achieve deep observability into its hybrid multi-cloud network.

"What keeps us up at night is what we do not know—potential threats we haven't seen before or potential challenges that might come to us from different threat actors," remarked Keirbeck. Because the company has a large segmented network, deep observability from Gigamon would allow his team to monitor not just inbound and outbound traffic, but also East-West traffic.

The team deployed the GigaVUE HC Series and GigaVUE TA Series traffic visibility appliances in combination with the GigaVUE-FM. The Gigamon appliances and single-pane-of-glass dashboard make it easy to set up flow mapping and to see at a glance which network ports are delivering which packets to individual tool ports. In addition to delivering specific traffic to specific tools at the right time, Application Metadata Intelligence is generating telemetry from this traffic to for network-level application identification, performance telemetry and indicators of undetected protocol issues. The Gigamon Deep Observability Pipeline replicates, filters, and selectively forwards network traffic to Corpay's monitoring, management, and security tools while creating network telemetry for operational and security dashboards for additional visibility. Corpay uses Splunk and Dynatrace for application visibility and performance monitoring, Cisco Stealthwatch for threat detection and security analytics, and SolarWinds for additional network management.

"Gigamon is the leader in virtual visibility, with features we could leverage, such as Gigamon Application Metadata Intelligence (AMI) and Gigamon Precryption technology," Keirbeck asserted. AMI provides close to 6,000 metadata elements through deep packet

inspection, which helps Corpay quickly zero in on performance bottlenecks, quality issues, and potential network security risks. Precryption eliminates blind spots in lateral threat activity by providing the Corpay's security stack with plaintext visibility; no decryption is required. Both tools enable Corpay to monitor threat activity across its entire multi-cloud environment.

Benefit

Gigamon provides advanced East-West visibility that helps Keirbeck sleep at night. "Cloud visibility is extremely important to us, and Gigamon allows us to understand our traffic and our potential threats and gives us the ability to be proactive with any threat intelligence we get," he said.

As the company re-architects its workloads and moves some to the cloud, maintaining application dependencies and security is extremely important. Gigamon helps protect Corpay's environment throughout this complex process. Overall, Gigamon has enabled Corpay to optimize, simplify, and secure the management of its hybrid cloud network.

"Gigamon has helped us in a number of areas: advanced visibility, performance capability, and intelligent and advanced threat management," asserted Keirbeck. "Today we are leveraging AMI telemetry to help us troubleshoot performance issues and safeguard our PCI environment as we move to PCI-DSS 4.0."

Keirbeck looks forward to deepening his partnership with Gigamon in the near term and over the long term. "I believe that companies can get further by working together than by working independently. I'm excited about the opportunity to collaborate with Gigamon," he said.

About Gigamon

Gigamon offers a deep observability pipeline that efficiently delivers network-derived telemetry to your cloud, security, and observability tools, helping organizations eliminate security blind spots, reduce tool costs, and better secure and manage your hybrid cloud infrastructure. Gigamon goes beyond security and observability log-based approaches by extracting real-time network intelligence derived from packets, flows, and application metadata to deliver defense-in-depth and complete performance management. 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 worldwide. To learn more, please visit gigamon.com.

Gigamon®

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

07.25_02