Case Study

Gigamon Helps Hospital Sírio-Libanês Enhance Visibility, Security, and Compliance

When we look for deep observability, Gigamon shows us everything we have in all layers of our infrastructure, including the cloud. We see the access network traffic, the packet, the flow, and so on—all the information that comes from our application metadata.

LEANDRO RIBEIRO
Chief Information Security Officer,
Hospital Sírio-Libanês

Challenges

- Comprehensive visibility into network threats
- Cloud security for applications and infrastructure
- Internet-of-things (IoT) security for devices
- Compliance with regional regulations on personal and health data protection

Customer Benefits

- Deeper understanding of network traffic
- Enhanced ability to identify insider threats
- Reduced the need for additional tools
- Strengthened protection of sensitive patient data

Solution

- GigaVUE Cloud Suite™
- GigaVUE® HC Series
- GigaVUE TA Series
- GigaVUE-FM fabric manager
- GigaSMART®

About Customer

Hospital Sírio-Libanês is a large Brazilian healthcare provider with 103 years of experience leading to today's state-of-the-art medical facility with specialized teams, investments in teaching and research, and pioneering initiatives. The institution, which boasts one of the largest medical image diagnostic centers in Brazil, ranks among the top 100 hospitals in the world and operates in 9 locations in São Paulo and Brasília, where it employs a staff of 14,000.

The hospital has a hybrid IT cloud environment, with 70 percent to 80 percent of its applications and infrastructure hosted in the cloud, primarily on Amazon AWS. Chief Information Security Officer Leandro Ribeiro, a seasoned professional with over 15 years of experience in cybersecurity and 20 years in healthcare, joined Hospital Sírio-Libanês to up level its cybersecurity program. Prior to joining the hospital, Leandro worked for major healthcare companies, including UnitedHealth Group. His expertise in healthcare cybersecurity makes him a valuable asset to the organization.

Business Challenge

When Ribeiro joined Hospital Sírio-Libanês, he found that the legacy security stack lacked the visibility and capabilities needed by the security team to effectively detect and respond to cyberthreats—especially in the cloud.

As a result, Ribeiro and his team of 22 network and cybersecurity professionals had three primary concerns. First, cybersecurity staff had difficulty monitoring network traffic from all directions, particularly east-west traffic within the data center. This limited visibility made it challenging to identify and address shadow IT and potential insider security threats that may originate from within the network. Second, the growing number of IoT devices, such as medical equipment and wearable devices, exposed new vulnerabilities, expanded the attack surface, and put patient health and personal data at risk. These devices, often with limited security controls, could be exploited by attackers to gain unauthorized access to the hospital's network. Finally, the hospital needed to comply with the Brazilian General Personal Data Protection Act (LGPD), which requires strong cybersecurity measures for patient data protection and privacy. Noncompliance with these regulations could result in significant fines and reputational damage.

In his previous roles at other healthcare institutions, Ribeiro had a positive experience with the Deep Observability Pipeline and the team that supported him. "I had worked closely with the Gigamon team in Brazil, who was proactive about solving visibility issues specific to our environment. My teams were not always conversant with the tools, so the support we received from Gigamon was invaluable to get everyone up to speed so quickly," he said. "I knew immediately that Gigamon was the best solution for Hospital Sírio-Libanês."

Resolution

The business challenges at Hospital Sírio-Libanês were resolved by gaining a deeper understanding of network activity to identify and address potential security risks more effectively.

The hospital implemented a comprehensive cybersecurity solution with Gigamon, ExtraHop, and Claroty Medigate, two Gigamon cybersecurity partners. Gigamon provides a unified view of data in motion across the entire network, enabling the hospital to monitor traffic from all directions (North-South and lateral East-West). ExtraHop, a network detection and response (NDR) solution, complements Gigamon by offering advanced threat detection and analysis capabilities. "The integrated solution makes it easier for us to uncover insider threats and anomalous behavior from endpoints and servers," noted Ribeiro.

Specifically, the Deep Observability Pipeline provides an entire security and performance tool stack that removes blind spots with complete visibility across the infrastructure. ExtraHop receives raw packets provided by Gigamon from across the infrastructure, extracts metadata from the packet using machine learning, and analyzes the intelligence using over 1 million different predictive models to gain a thorough understanding of the hospital's network activity. ExtraHop's machine learning algorithms analyze network traffic to identify suspicious activity and lateral movement techniques that expose the presence of threats at the early stages, such as malware, ransomware, and insider threats to help mitigate risks and prevent security breaches.

The solution also enables the hospital to effectively discover, monitor, and manage IoT devices, identifying vulnerabilities and preventing unauthorized access to these critical assets—without the need to invest in expensive, high-maintenance hardware. "This is where Gigamon was able to help us save money. We never really knew how many devices we had in our network. Now that we have full visibility to all our devices, we are able to implement network segmentation to better protect them," said Ribeiro.

By using the combination of Gigamon and ExtraHop, the hospital can demonstrate regulatory compliance by providing evidence of strong cybersecurity measures, ultimately enhancing patient safety and data security.

Benefit

The Gigamon implementation yields many significant advantages for Hospital Sírio-Libanês. By gaining a comprehensive understanding of network traffic, Ribeiro can identify and address potential security risks more rapidly and effectively—on premises and in AWS.

"When we look for deep observability, Gigamon shows us everything we have in all layers of our infrastructure. We see the access network traffic, the packet, the flow, and so on—all the information that comes from our application metadata," attested Ribeiro.

The combined solution allows the hospital to detect and respond to threats more quickly, reducing the frequency and impact of security incidents. Additionally, the hospital can secure its IoT devices, preventing unauthorized access and mitigating the risk of data breaches. By consolidating multiple security tools into a single platform, the hospital also realizes significant cost savings. For example, Gigamon augments the threat detection efficacy of Claroty Medigate, a SaaS healthcare platform that secures connected healthcare technology and devices, from IV pumps to ultrasounds.

The Gigamon and Claroty integration expands visibility into network traffic traversing XIoT/OT medical devices at the hospital, enabling faster and more accurate threat detection and response.

Finally, the solution helps to meet compliance requirements by providing a strong cybersecurity posture. By strengthening cybersecurity, the hospital is able to protect sensitive patient data and ensure the continuity of critical services, improving patient safety and overall operational efficiency.

"In the healthcare environment, delivering the best possible care to our patients is mission-critical, so everything we do is time-sensitive. Thanks to the expanded and deep visibility afforded by Gigamon, we are now several steps ahead of the game when an incident does occur. As soon as we identify a threat, we can stop it in its tracks and ensure that it does not impact hospital operations and the health and safety of our patients," pointed out Ribeiro.

In the near future, he and his team plan to further explore other Gigamon capabilities, including integration with SIEM, TLS/SSL Decryption for all traffic, and Gigamon Precryption™ technology to eliminate blind spots in East-West cloud traffic.

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

11.24_01