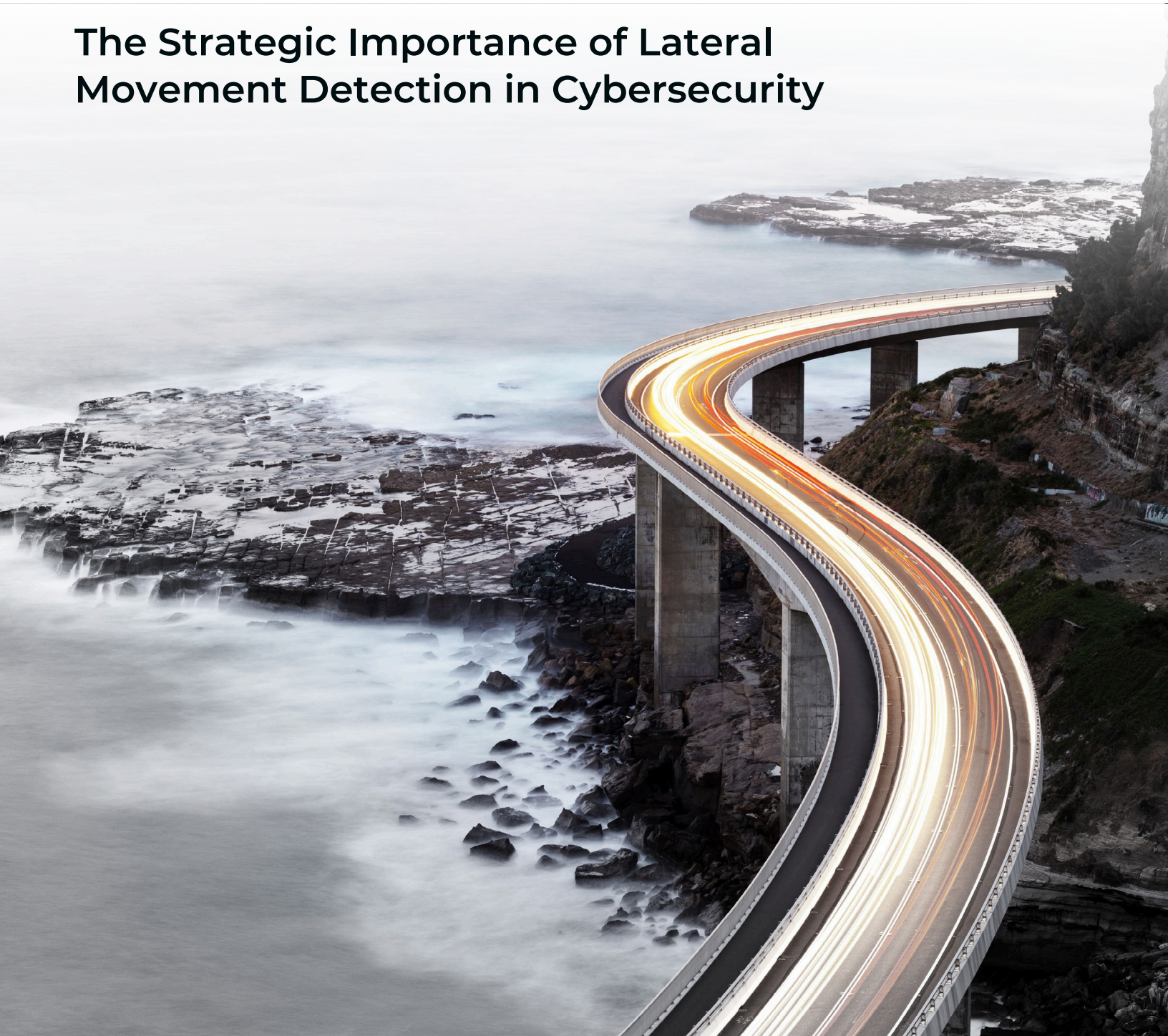
Unmasking the Hidden Threats in Network Traffic

The Strategic Importance of Lateral Movement Detection in Cybersecurity



Introduction

Lateral (or East-West) network communication has grown in importance in recent years, especially because the lack of lateral visibility exposes organizations to undetected blind spots, leaving them vulnerable to malware and ransomware attacks. The average cost of an insider breach in 2023 was reported to be $16.2M, with 90 percent of organizations feeling exposed to insider threats. Disconcertingly, 96 percent of lateral movement behavior does not trigger a corresponding alert in tools like a SIEM solution, creating unknown visibility gaps in the network1.

Gigamon provides deep observability into hybrid and multi-cloud network infrastructure, including providing visibility into East-West, North-South, container, and encrypted traffic, eliminating network blind spots while improving overall security posture.

The challenges of securing hybrid cloud environments continue to evolve as threat actors develop new tactics to exploit vulnerabilities created at the intersection of an expanding digital economy, an increasingly mobile workforce, and network complexity. It is no longer sufficient to rely solely on exterior protection, organizations must operate under the assumption that their network has been breached with undetected threat actors lurking within their network. Gigamon has established themselves as a market leader in the high growth deep observability market with solutions that harness actionable network-level intelligence to eliminate these security blind spots.

ALAN WECKLE
Founder and Technology analyst of 650 Group

What Is Lateral Visibility and Why Is It Important?

Lateral network traffic originates from one internal network segment and is destined for another internal network segment. This encompasses communication across hybrid cloud environment between devices, servers, virtual machines, or cloud and containerized services.

North-South traffic, on the other hand, is data flow between an internal network and an external network like the internet. It enters or exits the network perimeter and crosses into a different network.

East-West network communication has become increasingly consequential in recent years because of digital transformation, virtualization, cloud computing, microservices architectures including containerization, and the Internet of Things (IoT). As these technologies become more common, East-West traffic accounts for the majority of data center traffic.

Lack of East-West network traffic visibility can lead to significant cybersecurity risks for organizations; attackers (internal and external) can easily move laterally and spread malware, exfiltrate data, compromise assets and services, exploit zero-day vulnerabilities, and wreak other damage.

In 2023, MGM Resorts fell victim to a ransomware attack by the BlackCat (ALPHV) group, incurring over $110 million in damages. This cybercriminal organization, known for leveraging readily available tools like Mimikatz, Cobalt Strike, and Rsync for lateral movement within networks, exploited a critical industry vulnerability: limited visibility into east-west traffic.

Experts estimate 70-80 percent of successful cyberattacks exploit this blind spot2. Unmonitored east-west traffic allows free movement for ransomware, insider threats, and lateral activity aimed at exfiltrating sensitive data. Despite record cybersecurity spending exceeding $188 billion in 20233, the number and scale of cyberattacks continue to increase, with ransoms exceeding $1 billion in the same year4. As cybercriminals develop more sophisticated tactics, traditional security tools struggle to keep pace. A staggering 96% of lateral movement goes undetected by SIEM solutions, which adds to the challenge5.

Visibility into East-West traffic is critical to malware and ransomware defenses, allowing organizations to detect and mitigate lateral malware movement within the network. This observability is more critical than ever as malware and ransomware attacks—and resulting successful breaches—are seeing a significant increase. The 2023 Cybersecurity Ventures report projected a 15 percent rise in ransomware attacks in 2023, with a total cost of $265 billion to businesses and individuals worldwide. According to the Ponemon Institute1, almost 25 percent of all breaches in 2023 involved ransomware; the average recovery time was 21.1 days, with an estimated cost of $4.45 million, an increase of 15 percent over 3 years.

The complexity of hybrid multi-cloud networks brings forth blind spots, increase in cost, network inflexibility, regulatory challenges, and application and infrastructure issues.

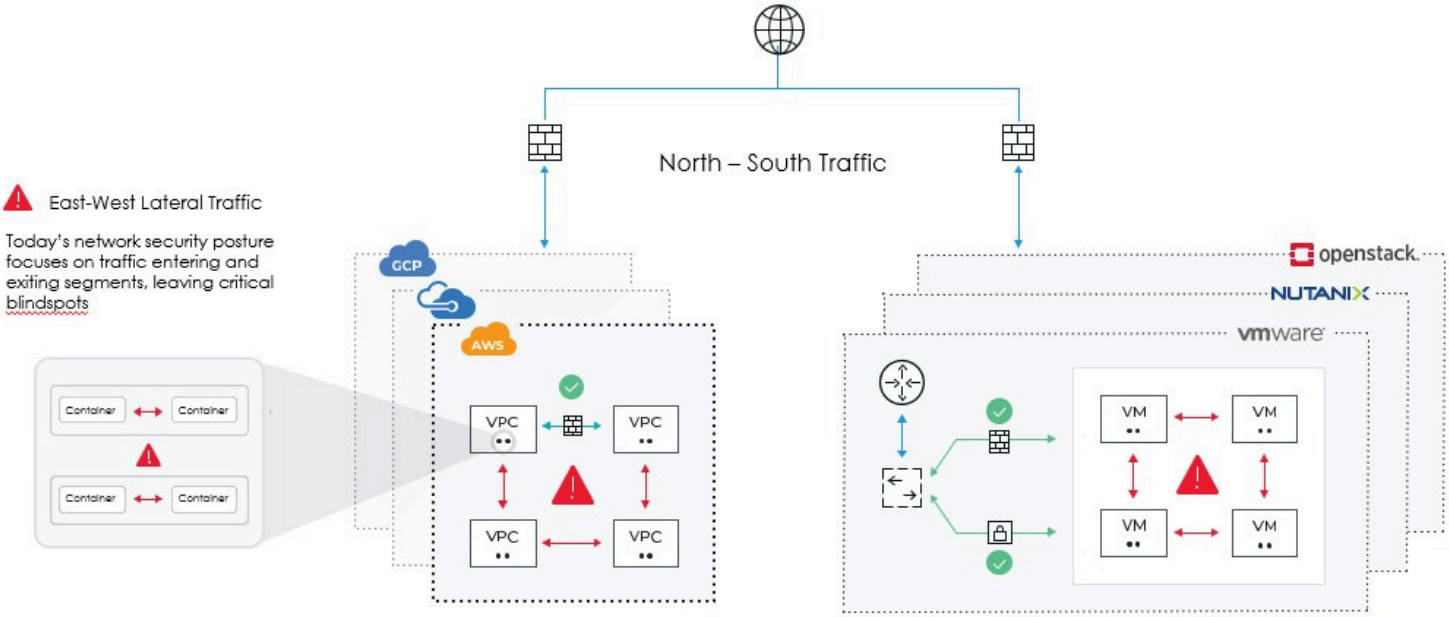


Figure 1. Eas-West traffic often goes unmonitored in cloud workloads..

East-West visibility needs redefining. The original concept of East-West traffic versus data that flows from north-south references a perimeter-focused, on-premises network, which simply doesn't exist anymore in the hybrid cloud world. Today's modern infrastructure means that deep observability across laterally moving data is just as important as visibility into traffic coming from external sources.

IAN FARQUHAR
Security CTO, Gigamon

7 Reasons Organizations Need East-West Network Traffic Visibility

Effective management, security, and optimization of East-West traffic are vital for maintaining the performance and security of modern IT environments. Traditional network security models primarily focused on securing the perimeter. However, with the increased prominence of lateral traffic, newer security approaches have emerged to safeguard internal communications within the network.

Deep observability into East-West network traffic offers many benefits that help organizations counter today's cyber threats and strengthen their security posture, including:

1. **Detecting lateral movement.** Once adversaries are inside the network, they often seek to move horizontally to escalate privileges and access valuable assets. East-West network observability empowers security teams to monitor and identify this lateral movement, recognizing unauthorized access attempts or abnormal behavior within internal resources. By promptly detecting and

responding to lateral movement, organizations can contain the attack and minimize potential consequences.

2. **Detecting malware and ransomware attacks.** East-West visibility plays a crucial role in effectively detecting, containing, and responding to malware and ransomware threats. By enabling visibility into internal network, cloud, virtual and container environments, security teams are capable of early detection and threat hunting, proactive containment and defense, and investigation and mitigation of malware attacks.

3. **Identifying insider risks.** Insider threats, whether malicious or unintentional, present a significant hazard to organizations. East-West network observability allows monitoring of internal communications and interactions, enabling security teams to identify any suspicious activities or behavioral anomalies exhibited by insiders. Organizations want to be able to effectively detect insider risks, such as data exfiltration, unauthorized access, or attempts to exploit pri v ile ge s .

4. **Detecting advanced persistent threats (APTs).** Advanced persistent threats are sophisticated, covert attacks that often reside within a network for an extended duration, aiming to remain undetected. East-West network observability is crucial for identifying indicators of compromise (IOCs) associated with APTs, such as command-and-control communications or patterns of lateral movement. By analyzing East-WestEast- West traffic, security teams can proactively detect and respond to APTs, thus minimizing potential harm.

5. **Strengthening forensics and incident response capabilities.** By monitoring internal network communications, organizations can swiftly detect and investigate security incidents. With clear visibility into East-West traffic, security teams can determine the extent and impact of an incident, isolate affected systems or resources, and initiate an appropriate response to contain the threat. This observability helps reduce the time required to identify and address security incidents.

6. **Identifying unauthorized or suspicious activities.** East-West network observability enables organizations to pinpoint unauthorized or suspicious activities within the internal network. By analyzing communication patterns between resources, security teams can detect activities such as data exfiltration, attempts at lateral movement, or unauthorized access to critical systems.

7. **Compliance monitoring and policy enforcement.** By analyzing network traffic, organizations can effectively enforce security policies, such as access controls and segmentation rules, within their internal network. This enables them to detect deviations from established policies, assess compliance with regulatory requirements, and promptly address any violations or non-compliance issues.

Lateral network visibility is vital for cybersecurity, so that organizations can protect their assets, detect and respond to threats, and maintain a strong security posture.

How Can Organizations Secure East-West Traffic with Gigamon?

The Gigamon Deep Observability Pipeline brings the depth of network-derived intelligence to observability and security tools for hybrid cloud workloads. It goes beyond current observability approaches that rely exclusively on analysis of metrics, events, logs, and traces (MELT).

The Deep Observability Pipeline uses advanced technologies to collect, process, and analyze data from various sources within the organization's infrastructure, enabling real-time monitoring, threat detection, and optimization across public cloud, private cloud, on-premises, or hybrid environments for physical, virtualized, or containerized workloads. Unlike MELT telemetry, which can be altered or disabled, Gigamon provides an immutable source of truth that increases the effectiveness of security posture and practices, eliminates blind spots, improves tools efficiency, and reduces cost.

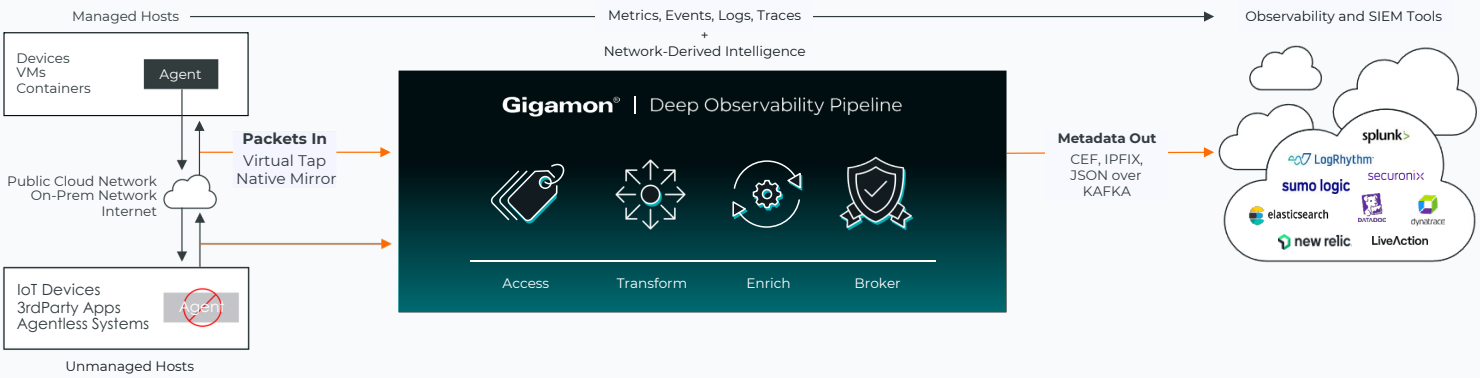


Figure 2. The Gigamon Deep Observability Pipeline.

Using the Gigamon Deep Observability Pipeline, organizations can eliminate blind spots in East-West network traffic, ensuring effective threat detection and response. This solution addresses potential blind spots, enhances overall cybersecurity posture, and reduces the risk of undetected malicious activity by providing:

Traffic capture and aggregation. The Gigamon Deep Observability Pipeline captures, consolidates, optimizes, and enriches network traffic within, between, and across hybrid cloud environments, including East-West traffic. It collects data from workloads such as virtual machines, containers, and cloud instances, eliminating blind spots and ensuring comprehensive coverage of network communication within the hybrid cloud infrastructure.

Visibility into encrypted traffic. Most cyber threats (91 percent) are using encrypted channels to avoid detection. The Gigamon Deep Observability Pipeline with licensed GigaSMART® decryption enables operations teams to have full visibility into encrypted traffic, including TLS 1.3, on any TCP port or application, allowing security teams to inspect the contents of encrypted East-West traffic. By decrypting TLS/SSL traffic, organizations can analyze the payloads, identify potential threats, and apply security controls to protect against malicious activities hidden within encrypted communications. More details can be found on the TLS/SSL decryption webpage.

Plaintext visibility into East-West encrypted cloud traffic. Gigamon Precryption™ technology is a breakthrough approach to eliminating the biggest blind spot in modern hybrid cloud infrastructure: lateral activity by threat actors concealed within encrypted communications. Organizations can maintain security compliance with a common solution for all forms of TLS without key management and build a solid foundation for Zero Trust architecture. More information can be found on the Gigamon Precryption webpage.

Threat detection and response. The enhanced East-West network visibility provided by the Gigamon Deep Observability Pipeline enables security and incident response teams to detect and respond to threats in real time. By analyzing the lateral traffic captured and aggregated by Gigamon, security tools can identify otherwise invisible suspicious activities, detect indicators of compromise, and trigger alerts for swift incident response. This capability helps organizations mitigate risks and minimize the impact of potential security incidents within their hybrid cloud environments, thus improving the overall security posture.

Cloud-native integration. The Gigamon Deep Observability Pipeline is designed specifically for cloud environments, providing native integration with leading cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). This integration enables seamless deployment and visibility into lateral movements between workloads in the cloud environments, ensuring compatibility, optimal performance, and blind spot elimination.

Traffic reduction and security tools optimization. Gigamon utilizes a number of traffic reduction and optimization technologies to process and eliminate the noise of network and application traffic and improve the efficiency of security, monitoring, and analytics tools. These capabilities include removing duplicated packets, metadata generation, traffic load balancing, application filtering and forwarding, packet slicing — to name a few. This can significantly reduce the volume of traffic that needs to be inspected, ensuring that security tools can focus on analyzing high-value network traffic, enhancing their efficiency and effectiveness. The Gigamon online traffic reduction calculator can be found here.

End-to-end granular application visibility. Application Filtering Intelligence (AFI) brings granular application awareness to on-prem and cloud-based network and security operations centers by letting you automatically identify, select, and deliver only the application data that are most important to security tools. This ensures that relevant traffic is directed to the appropriate security solutions, improving the efficiency and effectiveness of security monitoring and threat detection within the cloud environment.

App-related metadata extraction for deep packet inspection. Application Metadata Intelligence (AMI) expands upon application layer visibility derived from Gigamon Application Visualization and Filtering and supports a comprehensive approach to obtaining application behavior. It provides valuable information about East-West traffic without capturing the entire packet. Metadata extraction helps reduce the volume of data being processed, making it more manageable for analysis. It includes attributes such as source and destination IP addresses, ports, protocols, timestamps, and other relevant contextual information used in threat detection and investigation. Gigamon AMI supports nearly 7,000 protocols, applications, user behaviors, and L4–L7 attributes spanning over 4,000 standard and custom applications.

Integration with security tools and platforms: The Gigamon Deep Observability Pipeline integrates seamlessly with a wide range of security tools and platforms, including security information and event management (SIEM) systems, intrusion detection and prevention systems (IDS/IPS), network traffic analyzers, and threat intelligence and observability platforms. This integration enables security teams to leverage these tools effectively for complete network visibility, threat detection, and incident response. Gigamon extends the value of cloud, security, and observability tools with real-time network visibility and intelligence, delivering in depth defence and complete performance management across organizations' hybrid and multi-cloud IT infrastructure.

Security teams face an ever-evolving and rapidly changing threat landscape being driven by increasingly sophisticated threat actors. That's why complete visibility into workloads across hybrid cloud environments is essential to ensure organizations are equipped to detect and defend themselves against modern cyber threats and manage the related risks.

The Gigamon Deep Observability Pipeline plays an essential role in cybersecurity and threat detection by eliminating blind spots and providing packet-level visibility, scalability, and performance while integrating seamlessly with leading cloud platforms, security, and observability tools.

A couple of incidents that we had within the last six months we were able to catch quite quickly — within about an hour or so of the time the attacker took ownership of a server. We were able to catch them just in time before any real damage was done. And the reason is we have security tools in place, and Gigamon is feeding all the data into those security tools.

KAJEEVAM RAJANAYAGAM
Director of Cybersecurity, University Health Network

Conclusion

Complete visibility into the network is essential for overall security posture. But visibility must be coupled with a high-quality data feed to provide the deep insights needed to make quick, smart decisions. Gigamon provides this detailed visibility into East- West traffic across on-prem, virtual, OT/ICS, and cloud environments, ensuring no data is missed and enabling the security tools to detect lateral movements and internal threats that could otherwise go unnoticed.

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.

1. https://www.picussecurity.com/resource/blog/why-do-organizations-need-to-simulate-lateral-movement-attacks#:~:text=Moreover%2C%20the%20same%20report%20reveals%20that%2096%25%20of%20lateral%20movement,the%20attack%20even%20more%20difficult.
2. https://blog.ariacybersecurity.com/blog/just-what-is-a-ransomware-attack-and-can-you-prevent-one
3. https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024
4. https://www.chainalysis.com/blog/ransomware-2024/
5. https://www.mandiant.com/resources/security-effectiveness-2020-deep-dive-into-cyber-security-reality

Gigamon®

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

04 . 24 _01