Enhancing NDR Effectiveness

with the Gigamon Deep Observability Pipeline

> People want to spend 99 percent of their budget on NDR and 1 percent on getting good quality data, when in fact that slider needs to move quite a bit further over the other side. Because if you're getting too many unnecessary and unwanted packets into your tools, it doesn't matter what you put on the NDR side. It's garbage in, garbage out.
>
> **SAM AINSCOW,** CISO, Barrett Steel

Organizations are increasingly adopting hybrid cloud infrastructure to advance digital transformation and enhance their operational efficiency and scalability. However, with this shift to the cloud comes a pressing need for robust security monitoring solutions that help them to effectively monitor, secure, and manage on-premises, virtual, container, and private and public cloud workloads.

A common way to strengthen security is to deploy a Network Detection and Response (NDR) solution, which for many organizations has become an indispensable tool for securing their infrastructure against increasingly complex and frequent threats like ransomware, zero-day exploits, and malware. In addition, the rapid proliferation of AI-powered threats often use novel evasion techniques designed to bypass traditional security controls. All these threats pose significant risks to organizations of all sizes, making a robust NDR solution critical to their success.

Current Business and Technical Challenges of Deploying NDR

The effectiveness of NDR solutions relies significantly on the depth and quality of network visibility and telemetry collect to monitor and analyze network traffic. While distinct, both components are critical to strengthening overall network security.

Network telemetry involves gathering intelligence from network traffic from various points on the network, including traffic patterns, performance metrics, and security events. This real-time data is essential for NDR tools, providing insights into network behavior and helping to detect potential security threats and anomalies.

Network visibility, on the other hand, refers to the ability to monitor and analyze all network traffic and activities. It provides a comprehensive view of the entire hybrid cloud network, enabling NDR tools to fully understand the network environment and respond to security incidents more swiftly and effectively.

A key challenge for NDR tools is identifying threats concealed in network blind spots. These blind spots often result from IoT/OT devices that do not support security agents, as well as the increased use of network segmentation, subnets, and VLANs in operational environments. Attackers can exploit these areas to conceal malicious activities, leading to undetected threats and an increased risk of breaches. Therefore, achieving visibility into these blind spots is crucial to enhancing NDR's threat detection capabilities and ensuring comprehensive protection across the entire network infrastructure.

NDR solutions face another significant challenge: limited visibility into lateral traffic and encrypted communications. This limitation hampers their ability to effectively monitor and detect suspicious activities within the network, especially those hidden within encrypted traffic. AI-driven threats, such as AI-powered malware, often use encrypted channels to evade detection. As encryption becomes more prevalent in securing communications, ThreatLabz research shows that the effectiveness of NDR and other security tools can improve fivefold when encrypted traffic is decrypted prior to analysis.

The increasing adoption of hybrid and multi-cloud infrastructure has also introduced complexities in maintaining visibility and security. NDR tools struggle to adapt to these dynamic environments, where virtual workloads and containers are rapidly expanding, making it difficult to detect and respond to threats across various cloud platforms. To overcome this, NDR solutions must offer seamless integration and visibility across hybrid and multi-cloud infrastructure, enabling organizations to maintain a strong security posture while benefiting from the flexibility and scalability of the cloud.

Key Gigamon Features that Maximize NDR Benefits

Gigamon Deep Observability Pipeline Overview

Gigamon helps organizations eliminate blind spots by providing comprehensive visibility into all network traffic—Egress-Ingress, North-South, lateral (East-West), and both encrypted and unencrypted communications. Additionally, Gigamon provides visibility over AI-generated traffic to enable NDR solutions to accurately distinguish legitimate AI operations from potential threats like data exfiltration, unexpected data transfers, or unusual communication patterns.

No matter the size or complexity of a hybrid cloud infrastructure, Gigamon efficiently delivers network-derived intelligence to NDR and other security tools. This deep observability approach integrates traditional log-based tools with packet-level network insights, enabling security teams to proactively detect and respond to threats. As a result, organizations can maximize the efficiency and effectiveness of their existing NDR investments.

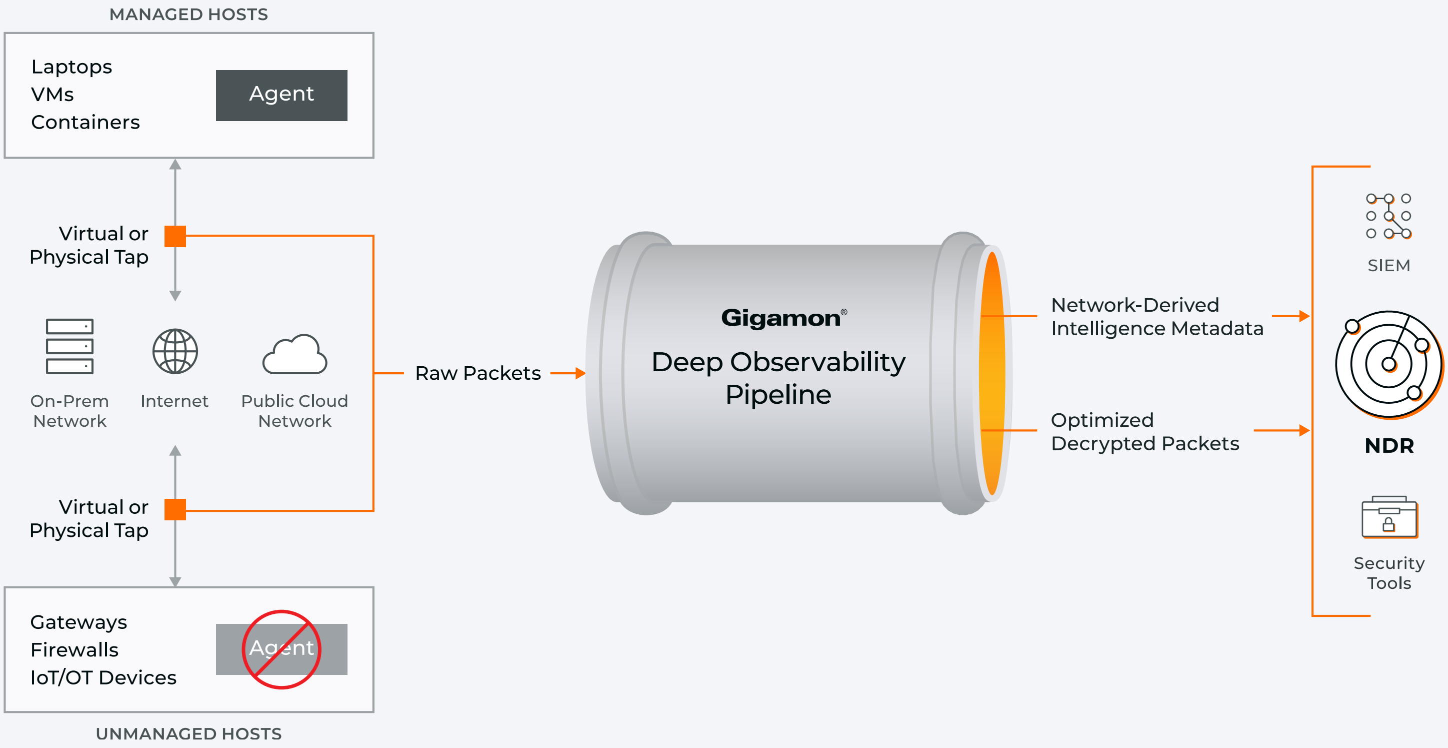


Figure 1. Eliminate blind spots, optimize and automate traffic management.

Key Features

The Gigamon Deep Observability Pipeline enables:

- **Effective network security monitoring** by combining proven analysis strategies with efficient access to network-derived intelligence
- **Instant identification** of applications and AI-generated traffic communicating across hybrid cloud infrastructure
- **Simplified access to traffic** that is difficult to analyze, including encrypted, AI-generated, container-to-container, and VM-to-VM traffic
- **Deep observability** into all lateral traffic across hybrid cloud infrastructure, spanning virtual, physical, public cloud, with container workloads and AI-generated traffic

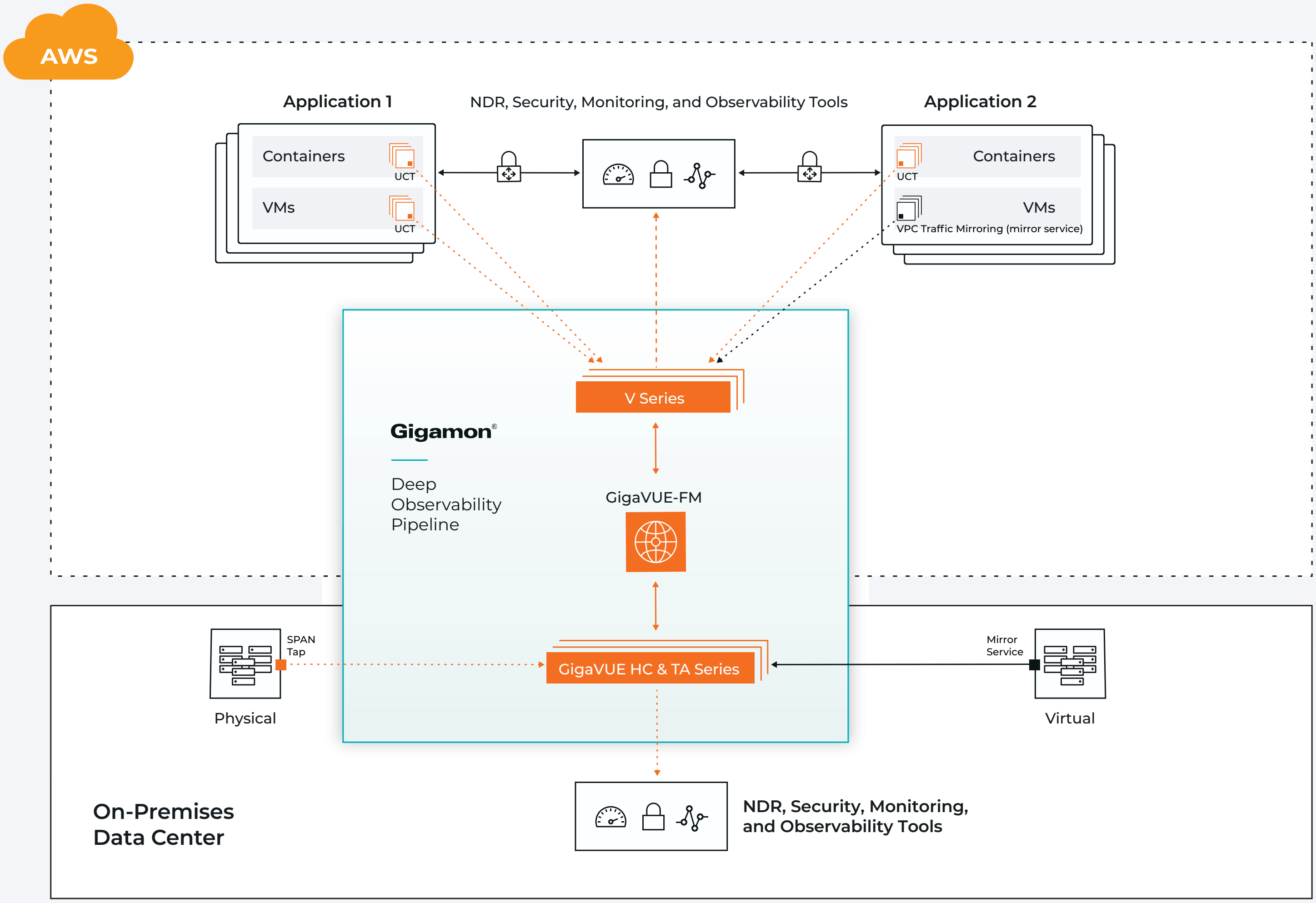


Figure 2. Gigamon Deep Observability Pipeline acquires, processes and forwards traffic to NDR tools in hybrid cloud networks to remove security blind spots.

Key Benefits

- Improved threat detection and response capabilities
- Enhanced visibility into network activities for proactive security measures. With detailed insights into AI-traffic, security teams are enabled to proactively hunt threats that exploit AI systems or leverage them as attack vectors
- Compliance with regulatory requirements for encrypted traffic inspection
- Reduction of cloud NDR operational costs

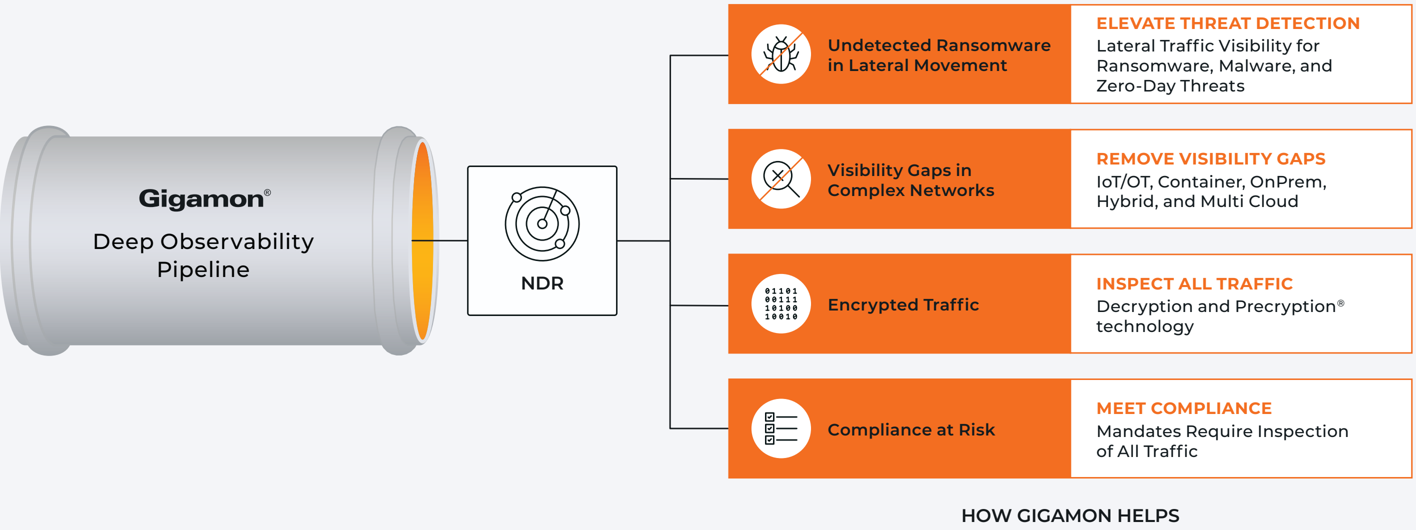

Gigamon®
Deep Observability Pipeline
NDR
Undetected Ransomware in Lateral Movement
ELEVATE THREAT DETECTION
Lateral Traffic Visibility for Ransomware, Malware, and Zero-Day Threats
Visibility Gaps in Complex Networks
REMOVE VISIBILITY GAPS
IoT/OT, Container, OnPrem, Hybrid, and Multi Cloud
01101 00111 10100 10010
Encrypted Traffic
INSPECT ALL TRAFFIC
Decryption and Precryption® technology
Compliance at Risk
MEET COMPLIANCE
Mandates Require Inspection of All Traffic
HOW GIGAMON HELPS

Figure 3. No more missed threat detections.

Use Cases and Business Scenarios:

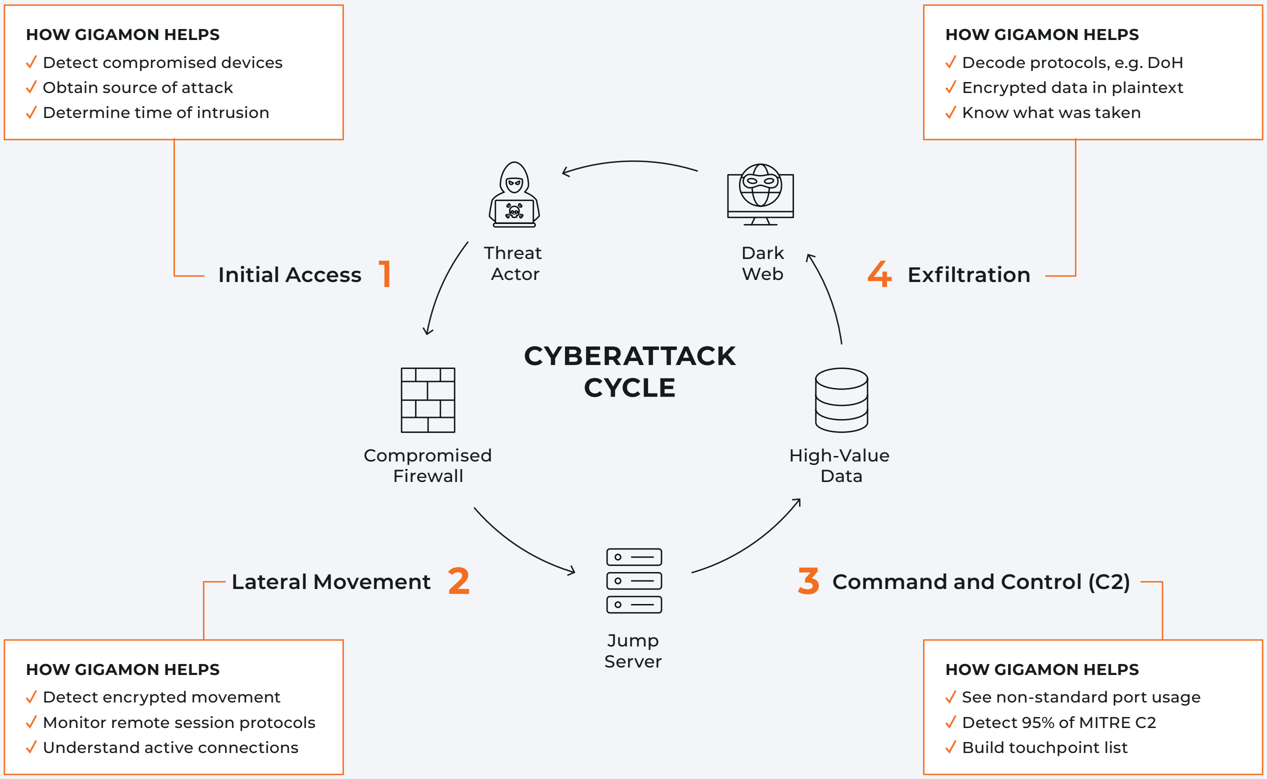
One key advantage Gigamon provides to NDR tools is full visibility into all types of network traffic—North-South, lateral (East-West), Encrypted-Decrypted, Ingress-Egress, and AI-generated. This allows NDR solutions to detect unusual patterns and anomalies in real time, identifying potential security incidents early. This proactive approach enables timely action to mitigate threats, even those designed to evade endpoint and perimeter security tools, and minimize their impact on the organization.

Capabilities	NDR	NDR + Gigamon
On-Prem, containerized, virtual, hybrid, and multi-cloud network traffic visibility	Limited	Yes
Complex networks: subnets, VLANs, segmented	Limited	Yes
Plaintext visibility on encrypted traffic for effective threat discovery and analysis	No	Yes
Visibility across network traffic in all directions including AI-generated (N-S, Lateral E-W, Ingress-Egress)	Limited	Yes
IoT/OT and legacy devices monitoring	Limited	Yes
Cloud NDR costs control	Limited	Yes

Below are two use cases where Gigamon enhances and adds significant value to NDR solutions:

Use Case 1: Elevating NDR Threat Detection

Let's explore, in Figure 4, the attack progression of a data exfiltration scenario and how Gigamon network traffic visibility exposes the presence of threats faster at multiple stages:



HOW GIGAMON HELPS
- ✓ Detect compromised devices
- ✓ Obtain source of attack
- ✓ Determine time of intrusion

HOW GIGAMON HELPS
- ✓ Detect encrypted movement
- ✓ Monitor remote session protocols
- ✓ Understand active connections

HOW GIGAMON HELPS
- ✓ See non-standard port usage
- ✓ Detect 95% of MITRE C2
- ✓ Build touchpoint list

HOW GIGAMON HELPS
- ✓ Decode protocols, e.g. DoH
- ✓ Encrypted data in plaintext
- ✓ Know what was taken

Figure 4. Attack progression of a data exfiltration scenario—How Gigamon helps understanding scope, origin and impact.

1

Once a threat actor gains **initial access**—often through methods like a phishing campaign—it becomes a race against time for the security team to detect their presence and minimize the impact. Quickly identifying key artifacts, such as the compromised device, the source of the attack, and the time of intrusion, is crucial for effective threat containment.

+

Gigamon enhances NDR tools by offering deep observability into all network traffic and application-level data, enabling faster detection of abnormal patterns. With detailed metadata, including protocols, ports, traffic source and destination, and timestamps, NDRs can quickly identify suspicious activity and the applications behind it. With detailed insights into AI-traffic, security teams are enabled to proactively hunt threats that exploit AI systems or leverage them as attack vectors.

2

Once the perpetrator establishes initial access, further reconnaissance typically begins, followed by **lateral movement** techniques such as session hijacking, exploiting remote services, and propagating offensive tools to expand their foothold. Advanced attackers often disguise these lateral movements within network traffic, frequently using encrypted traffic to evade detection.

After infiltration, attackers manipulate logs to conceal their activity and maintain their presence going undetected. According to Mandiant's 2024 Report, the average dwell time for attackers in 2024 is 10 days.

+

Gigamon reduces detection time by providing visibility into all network traffic—both encrypted and unencrypted—across Ingress-Egress, North-South, and East-West directions. By handling decryption, Gigamon allows NDR tools to more effectively analyze active connections, exposing techniques like RDP misuse, exposing intruders, even within encrypted traffic.

Gigamon also provides visibility over AI-generated traffic to enable NDR solutions to accurately distinguish legitimate AI operations and potential threats like data exfiltration, unexpected data transfers, or unusual communication patterns leveraged by command and control techniques. Additionally, Gigamon addresses a key challenge: relying solely on logs for security, which can be spoofed. NDR detections based on network data offer an independent source of truth, ensuring threat actors can't evade or disable security controls unnoticed.

3

Command and Control: At this stage, the attacker is nearing their goal of data exfiltration. Their primary focus is to establish covert communication channels and remain undetected for as long as possible.

+

Gigamon enhances the detection of Command and Control channels by providing deep observability into all network traffic. This allows NDR tools to quickly expose advanced evasion techniques, such as traffic over non-standard ports, protocol tunneling using SMB or DNS, or suspicious patterns from offensive remote access tools.

4

The final stage of the attack is often the most damaging for any organization, as this is when data **exfiltration** begins, often to locations like the Dark Web. Some attacks are so carefully orchestrated that it can take months for security teams to detect the root cause of the data breach.

+

Gigamon enhances NDR tools' effectiveness in uncovering these threats by providing network visibility into outbound and lateral traffic, protocols, ports, and applications. This helps expose advanced exfiltration techniques, such as scheduled transfers, alternate protocols, or even data exfiltration through cloud storage resources.

Use Case 2: Control NDR Cloud Costs

The shift toward hybrid and multi-cloud infrastructure can quickly increase complexity and costs for organizations. To mitigate the cybersecurity risks associated with this complexity, security teams depend on NDR tools that offer consistent threat detection and response by providing comprehensive visibility into all data-in-motion across their hybrid or multi-cloud networks.

The Gigamon Deep Observability Pipeline enables organizations to access, broker, transform, and enrich packet-level traffic across both on-premises and cloud environments. The GigaVUE Cloud Suite™ optimizes traffic acquisition through the GigaVUE Universal Cloud Tap, traffic mirroring, or tunneling allowing the capture, filter, and distribution of cloud traffic to NDR tools. This can lower cloud data visibility costs by up to 80 percent by:

- Standardizing cloud-native traffic acquisition, often eliminating the need for load balancing and gateway services.
- Eliminating the need for NDR and other security tools to run independent agents, minimizing compute cycles, and bandwidth usage. This reduces the amount of traffic sent to NDR tools while preserving accuracy through techniques such as Application Filtering Intelligence and Application Metadata Intelligence.
- Reducing backhaul costs by transmitting only relevant network traffic to NDRs. If the NDR solution cannot process metadata, Gigamon ensures compatibility by sending raw data instead.

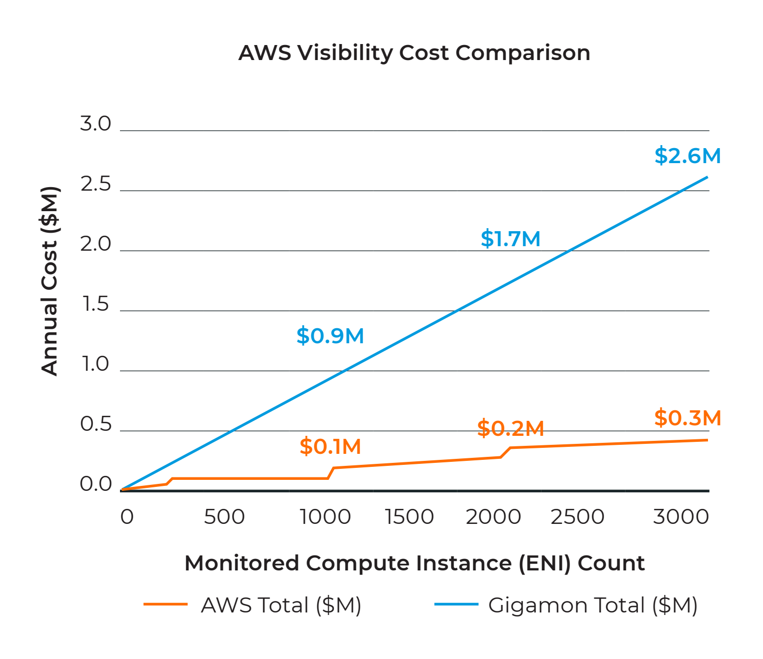


Figure 5. Example chart shows total infrastructure cost for each scenario, including tapping cost, transport cost, compute cost to run tool sensors and GigaVUE V Series, and CoreVUE Cloud Suite license, for the AWS US West region.

Depicted scenario assumes avg of 0.025 Gbps per monitored ENI, with V Series Node processing 25 TBpd, and 20 instances of GWLB with 400 GWLB Endpoints. Assumes sensors are deployed in same availability zone as monitored instances.

Conclusion

Adopting NDR solutions powered by comprehensive, high-fidelity network-derived intelligence and insights not only prevents missed detections but also strengthens defenses against emerging threats in an increasingly cloud-centric world.

Gigamon helps organizations to eliminate security blind spots by delivering deep observability into all traffic across all directions—Egress-Ingress, North-South, and East-West—boosting the effectiveness of NDR tools. With visibility spanning on-premises, virtual, IoT/OT, containerized, and hybrid cloud environments, Gigamon enables NDR tools to more efficiently and effectively enable security teams to detect and respond to threats, strengthening the security posture for their organizations.

Additionally, Gigamon optimizes traffic management by sending only relevant data to cloud-based NDR solutions, reducing cloud costs while enhancing threat detection and response across hybrid environments. The Gigamon Deep Observability Pipeline provides the critical visibility needed for NDR tools to proactively defend against advanced threats to protect your organization's digital assets.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived telemetry 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