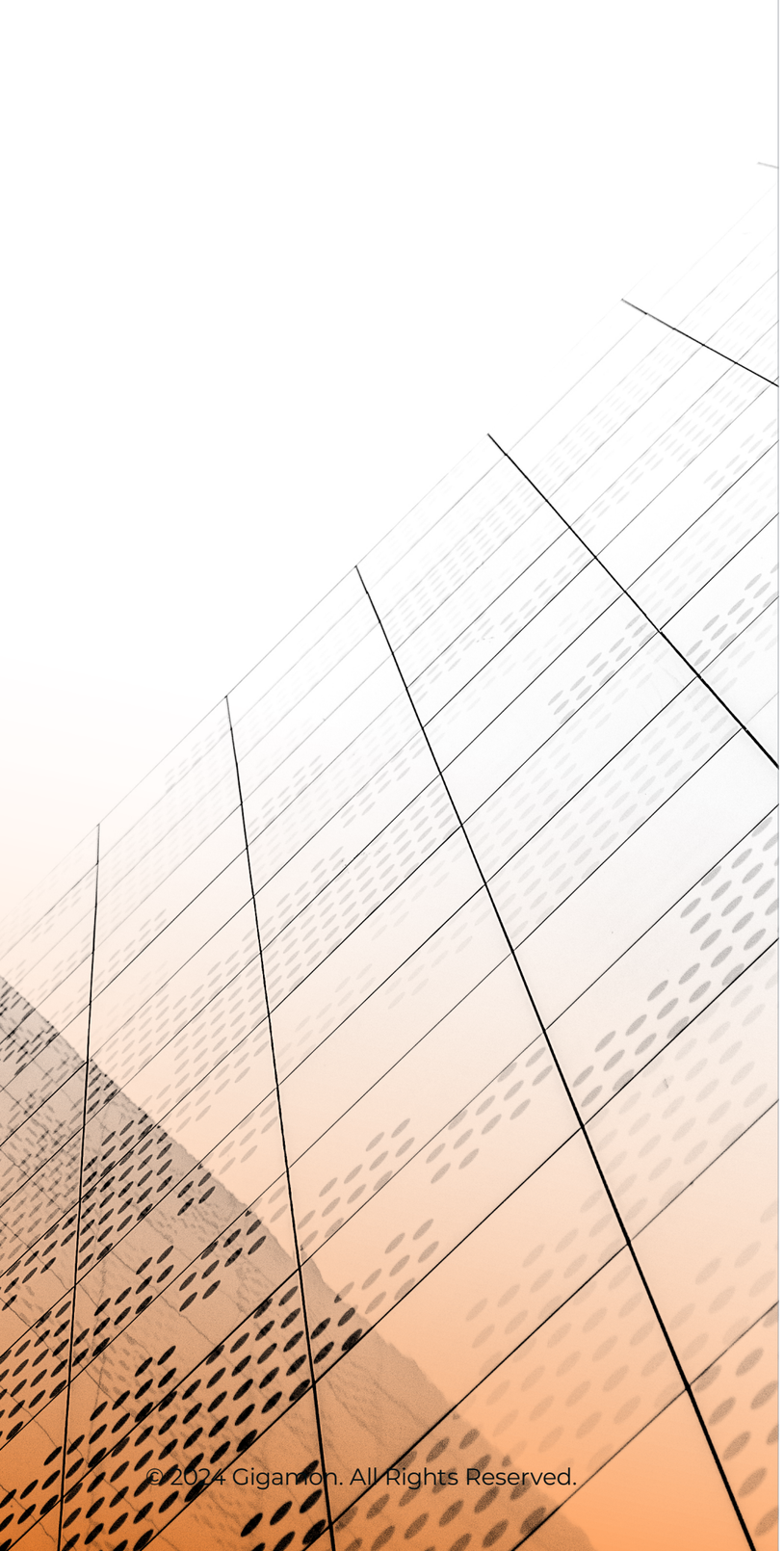
THREE WAYS TO BOOST YOUR NDR USAGE

Gigamon®



Three Ways to Boost Your NDR Usage

How do you maximize the efficiency and effectiveness of NDR tools?
It starts with gaining deep observability into network traffic so you can:

1. Eliminate security blind spots
2. Gain visibility into encrypted traffic
3. Access IoT/OT traffic

60%

of organizations lack visibility into lateral, East-West traffic.[1]

Eliminate Blind Spots

Even the most robust security tools can't protect you if you can't see the network traffic running across your hybrid cloud infrastructure. To give tools the best chance at detecting threats and identifying and eliminating blind spots, you need to gain deep observability into all network traffic.

Deep Observability Is the Foundation for NDR Excellence

Efficiently delivering network-derived intelligence and insights to your NDR tools significantly enhances your ability to detect and respond to threats. NDR tools can only respond to threats that they can see. Your tools must have North-South and lateral East-West visibility across all environments and sources, including on-premises, virtual, hybrid or multi-cloud, encrypted, and container traffic to ensure that your security posture is providing the maximum level of protection.

Eliminating Blind Spots

Gain User and Application Behavioral Insights

Gaining deep observability across your hybrid cloud infrastructure empowers you to not only see more but understand more. Gigamon offers prebuilt integrations with leading security and performance tools, including NDRs, to deliver deep observability into complex application behavior. This network-derived intelligence provides the context you need to pinpoint potential threats and resolve issues faster.

53%

Over half (53 percent) of security and IT leaders state they haven't tackled decryption as they believe it is time-consuming and/or expensive.[1]

Decrypting Traffic

Extend Your Security Posture to Public Cloud

Architected for today's hybrid and multi-cloud infrastructure, the Gigamon Deep Observability Pipeline spans your physical, virtual, and cloud environments. It enables you to acquire, optimize, and share selected traffic across your security and monitoring tools, extending your decryption capabilities and security posture to the public cloud without compromise.

Traditional techniques for defending network perimeters no longer apply as hybrid and multi-cloud infrastructure becomes more and more complex. This complexity includes encrypted traffic. How can you see and secure critical traffic when it's encrypted? The answer starts with decrypting and gaining visibility to eliminate security blind spots.

Deep Observability Into Encrypted Traffic

Encryption is essential for safeguarding sensitive data and communications, but it's also quickly becoming part of modern malware's attack techniques — particularly command-and-control communications. Gigamon provides centralized decryption, including TLS 1.3, eliminating the need for each security tool to perform its own decryption that consumes valuable resources. Organizations benefit from deep visibility into all network traffic to eliminate blind spots, expose malware hidden in encrypted traffic, and maximize monitoring efficiency.

65%

of Security and IT leaders believe existing security tools are not as effective as they could be when it comes to detecting breaches.[1]

Accessing IoT/OT Traffic

As your organization becomes increasingly connected, even a short service interruption or minor breach can impact customer experience, slow productivity, and jeopardize your business. Shortening your threat response time is more critical than ever in today's complex hybrid and multi-cloud world. IoT, OT, and other devices on the network negatively affect both threat detection and response due to the sheer complexity of gaining visibility into each of these devices. Devices are continuously added, removed, and moved across networks, creating a significant visibility challenge for all organizations.

Clear IoT/OT Device Visibility, Faster Detection and Response

Investigate suspicious behavior, proactively hunt for potential risks, and direct fast and effective response to active threats from a visibility landscape that includes IoT/OT devices. Gigamon provides your NDRs deep observability into every single device within an infrastructure, fortifying the effectiveness of your security posture.

Gigamon Deep Observability Pipeline

With increasing cloud adoption also comes increasing cost and complexity in securing and managing your hybrid cloud infrastructure. Most security tools inspect north-south traffic but often neglect lateral movement — which can put your organization at risk.

The Gigamon Deep Observability Pipeline provides your NDR tools with the deep observability needed to cut through complexity and understand what's really happening in your infrastructure. Our deep observability pipeline helps customers to achieve a 75 percent increase in network visibility and a 50 percent reduction in network downtime.

It's time to supercharge your NDR tools with the network-derived intelligence and insights they need so you can effectively detect and respond to threats.

Why Gigamon

Traditional security tools that gain visibility exclusively through metric, event, log, and trace (MELT) data are limited in what they can identify and how deeply or broadly they can monitor today's complex infrastructure.

The Gigamon Deep Observability Pipeline goes beyond traditional approaches by extracting intelligence directly from network traffic and efficiently delivering it to your NDR tools in real time. With this network-derived intelligence, your NDR tools can detect previously hidden threats and help mitigate the cost and severity of an attack, empowering you to better secure and manage your hybrid cloud infrastructure.

For more information, visit gigamon.com/observability-demo.

A market leader in deep observability, with a 61 percent market share in 2024.[2]

4,000+
CUSTOMERS WORLDWIDE

10/10
TOP U.S. FEDERAL AGENCIES

83/100
FORTUNE 100 COMPANIES

8/10
TOP HEALTHCARE PROVIDERS

9/10
TOP MOBILE NETWORK OPERATORS

7/10
TOP GLOBAL BANKS

[1] Hybrid Cloud Security: Closing the Cybersecurity Preparedness Gap, Gigamon, 2024.

[2] Defining the TAM for the Deep Observability Product Line Along with Competitor Analysis, Frost & Sullivan, June 2024.

Gigamon®

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

07.24_03