FROST & SULLIVAN

TRANSFORMATIONAL GROWTH LEADERSHIP

Transforming Cybersecurity Visibility: How Gigamon is Enabling Deep Observability in the AI Era

Gareth Maclachlan
Chief Operating Officer, Gigamon
in conversation with
Jarad Carleton
Global Research Director, Cybersecurity, Frost & Sullivan

The rapid expansion of hybrid cloud environments, artificial intelligence workloads, and distributed infrastructure is reshaping the cybersecurity landscape. As organizations adopt new technologies at speed, their attack surfaces continue to expand, while traditional approaches to visibility struggle to keep pace.

In this Transformational Growth Leadership discussion, Gareth Maclachlan shares how deep observability and network-derived telemetry are helping organizations gain comprehensive visibility across increasingly complex environments. He explains how enterprises can reduce blind spots, improve detection, and build a stronger foundation for AI-driven security operations.

> “Without visibility across every part of your infrastructure, you lose the ability to understand and secure what’s happening.”
>
> — Gareth Maclachlan, Chief Operating Officer, Gigamon

Defining the Visibility Challenge in an AI-driven Landscape

Jarad Carleton: *From what you are seeing, where are organizations struggling most when it comes to visibility today?*

Gareth Maclachlan: The biggest shift we are seeing is driven by the economics of AI. Organizations are investing heavily to move faster and scale capabilities, but at the same time, attackers can now exploit these systems with unprecedented speed.

There was a recent example where an AI-driven attack was able to identify exposed endpoints, gain access, and prepare data exfiltration in just a couple of hours. That highlights how quickly the landscape is changing.

At the same time, most organizations are still experimenting with AI. Architectures are evolving rapidly, and no one really knows what the final state will look like. That uncertainty makes it critical to focus on what can be controlled today.

The foundation comes down to three elements: visibility across all traffic flows, identity awareness, and endpoint instrumentation. If organizations establish that foundation now, it is far easier and more cost-effective than trying to retrofit it later.

Frost & Sullivan's **Transformational Growth Leadership Program** aims to honor visionary business leaders who possess the foresight and leadership acumen to drive positive change within their organizations. The leaders we celebrate hail from diverse sectors and company sizes, yet they all share an unwavering commitment to innovation and excellence.

Accelerating Threat Dynamics in the Age of AI

Jarad Carleton: *How is AI changing the speed and nature of cyberattacks?*

Gareth Maclachlan: We're seeing how AI is being used to find novel zero-days and develop new malware and code attacker tool chains. Much of security still works on matching against things that have been seen before, but the economics have now shifted – new, single use attacks are cheap. That highlights how quickly the landscape is changing.

As organizations invest in AI to accelerate innovation, attackers are also leveraging the same technologies to scale their capabilities. This creates an environment where both innovation and risk are moving at unprecedented speed, making it critical for organizations to strengthen their visibility and detection capabilities.

Navigating Visibility Across Hybrid and Multi-cloud Environments

Jarad Carleton: *How has the move to hybrid and multi-cloud environments changed the visibility challenge for organizations?*

Gareth Maclachlan: One of the biggest misconceptions has been the reliance on cloud logs. Many assumed that logs would provide everything needed for visibility, but in reality, they are delayed, incomplete, and do not capture all traffic flows.

Organizations miss traffic between clouds, direct connections from data centers, and other critical interactions. As enterprises move toward sovereign cloud strategies and alternative providers, this challenge becomes even more complex.

To address this, organizations need visibility that spans across all environments: on-premise, public cloud, and hybrid architectures, without gaps.

Rethinking Visibility in an Encrypted and AI-driven Environment

Jarad Carleton: *As more traffic becomes encrypted, how does that change the way organizations approach visibility?*

Gareth Maclachlan: Encryption does limit what can be directly inspected, but that does not mean visibility is lost. Gigamon enables customers to selectively decrypt suspicious traffic for example; but in addition organizations can use techniques such as fingerprinting and protocol analysis to identify suspicious behavior. By combining network telemetry with identity, it becomes possible to focus inspection efforts only where it matters.

A growing concern is internal AI usage. While organizations may control external tools, they often lack visibility into internal experimentation. If someone deploys an open-source model inside the network, it can unintentionally create new attack surfaces.

That is where network-level visibility becomes critical. It allows organizations to detect and understand activity that would otherwise remain hidden.

Addressing Hidden Risks from Internal AI Adoption

Jarad Carleton: *Are organizations fully aware of the risks from internal AI usage?*

Gareth Maclachlan: A growing concern is internal shadow AI usage. While organizations may have controls in place for external tools, they often lack visibility into internal experimentation.

If someone deploys an open-source model inside the network, it can unintentionally create new attack surfaces. These activities can occur outside traditional monitoring frameworks, making them difficult to detect using conventional tools.

That is where network-level visibility becomes critical. It allows organizations to detect and understand activity that would otherwise remain hidden, helping them maintain control in increasingly dynamic environments.

From Tool Sprawl to Data-centric Security Architectures

Jarad Carleton: *Are you seeing organizations move toward consolidating tools, or is the focus shifting elsewhere?*

Gareth Maclachlan: We are seeing a shift from vertically integrated tools to horizontally layered architectures.

Historically, each function, including security, performance, operations, used its own tools, each collecting and processing data independently. Now, organizations are moving toward centralized data strategies where telemetry is collected once and used across multiple use cases.

The key is ensuring that data is clean, consistent, and accessible. When that happens, AI can extract value from it much more effectively.

This shift also challenges traditional software models. Instead of relying on fixed dashboards and workflows, organizations are increasingly using AI-driven queries and dynamic interfaces to interact with data.

Advancing Deep Observability as a Strategic Capability

Jarad Carleton: *How would you explain deep observability, and how is it different from traditional approaches like logs and metrics?*

Gareth Maclachlan: Traditional observability relies heavily on metrics, events, logs, and traces (MELT), which provide only partial visibility. It is like having cameras at two points on a road. You know something passed by, but not what happened in between.

Deep observability provides a continuous, end-to-end view of network activity. It allows organizations to see how data flows across systems, rather than relying on fragmented snapshots.

This is particularly important during incident response. Instead of piecing together information from multiple sources, teams can quickly identify affected systems, understand attack patterns, and take action.

Leveraging Network Telemetry to Enhance Security Outcomes

Jarad Carleton: *Can you share how better telemetry actually improves detection and response in real-world scenarios?*

Gareth Maclachlan: Network telemetry enables both efficiency and effectiveness.

For example, by filtering and optimizing traffic, organizations can significantly reduce the cost of deploying security tools. In many cases, traffic volumes can be reduced dramatically while still preserving the most relevant data.

More importantly, telemetry can be integrated with platforms such as SIEM (Security Information and Event Management) and endpoint security tools. This allows security teams to correlate events across different layers and gain a more complete understanding of incidents.

As AI-driven security operations evolve, telemetry becomes even more valuable. It provides the signals that autonomous systems can use to detect threats and initiate responses.

Translating Visibility into Measurable Business Outcomes

Jarad Carleton: *How does better visibility translate into real outcomes for security teams and the business?*

Gareth Maclachlan: Network telemetry helps to uncover threats that would otherwise go undetected, bringing the full picture into view.

At the same time, integrating telemetry with platforms such as SIEM and endpoint tools allows teams to correlate events more effectively, improving detection and accelerating response.

AI, Automation, and the Future of Security Operations

Jarad Carleton: *What role is AI starting to play in observability and security operations today?*

Gareth Maclachlan: One of the biggest challenges in cybersecurity has always been the volume of data. AI has the potential to process that data at scale, identify patterns, and surface insights that would be difficult for humans to detect.

However, AI is only as effective as the data it receives. If visibility is incomplete or fragmented, the outputs will be limited, making it difficult for organizations to rely on AI-driven insights with confidence.

This is why establishing strong telemetry and visibility foundations is critical. Once that foundation is in place, AI can significantly enhance detection, automate response, and improve overall security outcomes.

Building the Foundation for Scalable and Secure AI Adoption

Jarad Carleton: ***Given how quickly AI and architectures are evolving, where should organizations focus first to stay ahead?***

Gareth Maclachlan: Most organizations are still experimenting with AI, and architectures are evolving rapidly. The reality is that no one fully knows what the end state will look like, which makes it difficult to design perfect systems from the start.

Because of that uncertainty, the focus needs to be on establishing strong fundamentals that will remain relevant regardless of how architectures evolve. The foundation comes down to three core elements: visibility across all traffic flows, identity awareness, and endpoint instrumentation.

If organizations can establish that foundation early, they are in a much stronger position to adapt as new technologies and use cases emerge. Trying to retrofit these capabilities later becomes significantly more complex and costly.

This is particularly important in the context of AI, where both innovation and risk are accelerating at the same time. Having a strong visibility and telemetry foundation ensures that organizations can scale securely while maintaining control over increasingly dynamic environments.

Closing Reflection: Visibility as the Foundation of Cyber Resilience

As organizations continue to adopt AI, hybrid cloud, and distributed architectures, the need for comprehensive visibility is becoming more critical than ever. Traditional approaches based on logs and fragmented monitoring are no longer sufficient to address the complexity of modern environments.

Our focus on deep observability and network-derived telemetry reflects a broader shift toward data-centric security architectures. By enabling continuous visibility across all environments, organizations can reduce blind spots, improve detection, and build more resilient security operations.

In an increasingly dynamic threat landscape, visibility is no longer just a technical requirement; it is the foundation for effective cybersecurity and operational confidence.

Gareth Maclachlan | Chief Operating Officer, Gigamon

Gareth Maclachlan is **Chief Operating Officer**, responsible for leading the global product organization and partnering across the leadership team to sharpen company strategy, accelerate innovation, and deliver transformative outcomes for customers as part of the company's AI-powered deep observability vision. He brings more than 25 years of cybersecurity and enterprise technology experience, most recently serving as Chief Product and Technology Officer at Trellix, where he led more than 1,500 people across engineering, security research, and product management. Gareth previously held senior leadership roles at FireEye, AdaptiveMobile, and PwC Consulting. He holds an MBA from London Business School and a BSc in Architecture from University College London.

Jarad Carleton | Global Research Director, Cybersecurity, Frost & Sullivan

Carleton brings 25+ years of experience in the USA and Europe to his role. He works with organizations in Israel, North America, Europe, and Asia, focusing on various security domains such as Active Directory, zero-trust enterprise browsers, managed security services, digital risk protection, digital trust, IoT security and privacy, encrypted voice and text messaging, automated security validation, vulnerability management, IT/OT security convergence, fraud detection and prevention, and CSP security services. His quantitative research on security trends, maturity, services, and products informs legislators, regulatory bodies, and CXOs, helping them make data-driven decisions that enhance growth.

Ready to Lead the Transformation?

- **Book a Growth Strategy Session:** Align your growth roadmap with Frost & Sullivan's Visionary Growth Pipeline™ Dialog.
- **Engage with Growth Experts:** Co-design AI-enabled, data-driven operating models that scale industry-specific and commercial impact.
- **Share Your Transformation Story:** Position your organization as a transformation leader through Frost & Sullivan's Transformational Growth Leadership platform.
- **Join the Growth Council:** Collaborate with industry leaders shaping the future of your ecosystem.
- **Nominate for Best Practices Recognition:** Be recognized for excellence in growth strategy, execution, and customer impact.
- **Demonstrate Industry Positioning on the Frost Radar™:** Benchmark your growth performance and innovation strength against industry competitors.
- **Activate Brand & Demand Growth:** Accelerate awareness, engagement, and revenue growth through integrated brand and demand generation strategies.

Annexure: Advancing Deep Observability and AI-driven Cybersecurity

As enterprise environments grow more complex, organizations are increasingly adopting data-centric security strategies built on deep observability, network telemetry, and AI-driven analytics. These capabilities enable continuous visibility across hybrid and multi-cloud environments while improving threat detection, response, and operational efficiency.

To support organizations navigating this transformation, Frost & Sullivan provides forward-looking intelligence across cybersecurity innovation, observability platforms, and AI-enabled security operations, including:

- Insights for CISOs: The Strategic Imperative for Deep Observability
- Frost Radar™: Network Detection and Response, 2025
- Network Detection and Response (NDR) Sector, Global, 2024–2029
- Zero Trust Architecture: Next-generation Cybersecurity Framework for Digital Enterprises

Together, these analyses reinforce the central themes of this Transformational Growth Leadership discussion: deep observability, unified telemetry, and AI-driven security operations as the foundation for modern cyber resilience.

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. →

FROST & SULLIVAN