Gigamon®

2025 COMPANY OF THE YEAR

Driving impact across the customer value chain

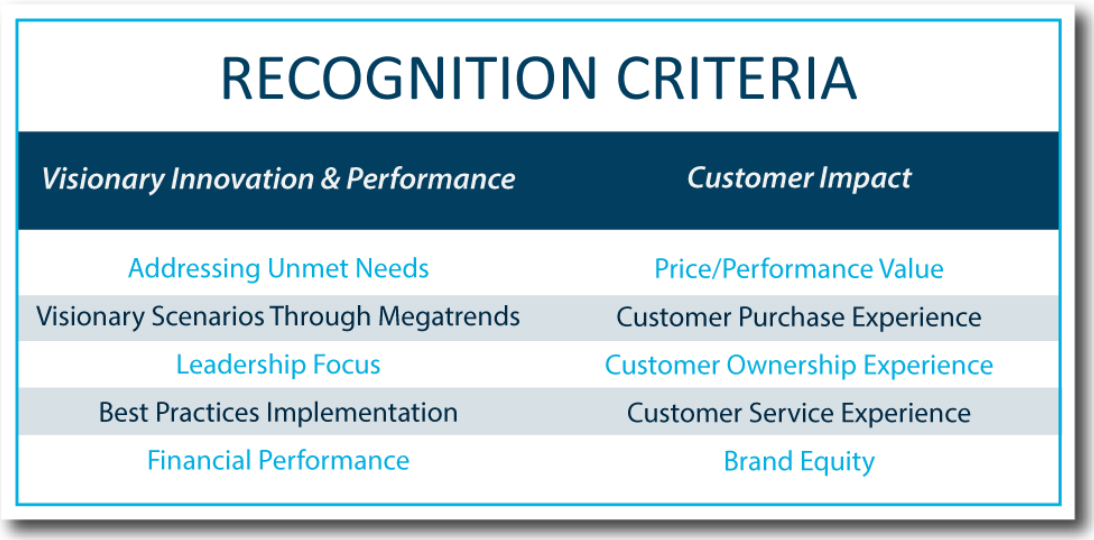
RECOGNIZED FOR BEST PRACTICES IN THE GLOBAL NETWORK OBSERVABILITY FOR CYBER SECURITY INDUSTRY

FROST & SULLIVAN

Table of Contents

Best Practices Criteria for World-class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each recognition category before determining the final recognition recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. Gigamon excels in many of the criteria in the network observability for cyber security space.



The Transformation of the Network Observability for Cyber Security Industry

The network observability market has evolved rapidly to address visibility gaps across today's complex hybrid and multi-cloud infrastructures. Conventional observability models based on metric, event, log, and trace (MELT) data can fail to identify threats in east-west and encrypted traffic that can spread throughout an organization to locate and exfiltrate high-value data. By fusing network-derived telemetry in the form of packets, flows, and metadata with MELT data, organizations gain deep observability into all data-in-motion to identify threats in encrypted and lateral traffic that security and observability tools might otherwise miss.

As a result, deep observability has become a strategic priority as organizations implement zero-trust architectures to assure compliance with regulations such as the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and the European Union (EU)'s Digital Operational Resilience Act (DORA). By delivering clean, structured, and actionable network-derived telemetry to downstream platforms—such as security information and event management (SIEM) systems, threat detection tools, and analytics engines—without centralizing raw traffic, a deep observability solution can dramatically reduce operational overhead and enhance security posture.

Adoption is accelerating as enterprises shift to cloud-native and distributed environments, with over half of global applications already migrated and more expected by 2025, driving demand for consistent, high-fidelity visibility.[1] Organizations require insight across hybrid infrastructures, encrypted communications,

[1] Insights for CISOs: The Strategic Imperative for Deep Observability (Frost & Sullivan, January 2025)

and unmanaged assets—capabilities a deep observability pipeline can provide. While many observability vendors focus on application performance or infrastructure metrics, deep observability leaders complement this by delivering enriched, network-derived telemetry and intelligence. As companies seek scalable, interoperable, and cost-efficient solutions, deep observability is becoming essential for advancing cybersecurity maturity and achieving operational resilience.

Providing Deep Observability That Strengthens Security, Simplifies Operations, and Optimizes Costs

> *"The Gigamon Deep Observability Pipeline delivers flexible packet processing, Precryption™-based visibility into encrypted traffic, and deep traffic inspection. These capabilities complement MELT-based tools by enriching them with network-derived telemetry that improves their effectiveness."*
>
> ***- Georgia Edell***
> ***Senior Consultant***

Gigamon leads the global network observability sector by providing real-time, actionable visibility into data-in-motion, helping security teams respond to evolving threat vectors, hybrid cloud complexity, and escalating regulatory pressures. At the core of its strategy lies the Gigamon Deep Observability Pipeline, an integrated architecture that extracts telemetry from data-in-motion and transforms it into actionable security insights across on-premises, private and public cloud, virtualized and containerized environments.

Gigamon closes visibility gaps, particularly in encrypted and east-west traffic across hybrid and multi-cloud environments. While north-south inspection has become standard in cybersecurity architecture, lateral observability between virtual machines, containers, and on-premises assets remains insufficient. Gigamon provides deep observability across these environments, allowing customers to monitor unmanaged devices, IoT endpoints, and inter-container traffic without deploying agents. As containerization, microservices, and zero-trust architecture deployments accelerate, the company's solution aligns with these megatrends by extending security policies across ephemeral workloads.

The Gigamon GigaVUE® Universal Cloud Tap (UCT) simplifies cloud complexity and reduces operational costs through a cloud-agnostic approach that overcomes the limitations of native cloud tools. UCT leverages Gigamon Precryption™ Technology to gain plaintext visibility into encrypted traffic without full decryption, utilizing eBPF for efficient, agentless tapping into Linux environments. This eliminates blind spots while safeguarding data privacy and application integrity.

As generative AI (Gen AI) adoption accelerates, Gigamon enables network-level identification and classification of Gen AI traffic. Using Gigamon Application Metadata Intelligence (AMI) and traffic pattern recognition, AMI identifies interactions with AI models, including those via third-party applications. This supports policy enforcement and AI usage monitoring without relying solely on endpoint tools, offering visibility into Gen AI data flows, internal model interactions, and hidden risks from conventional monitoring tools.

These innovations deliver measurable value across complex enterprise environments. For example, a US-based global payments company deferred investing in a standalone network detection and response (NDR) solution after utilizing Gigamon AMI to deliver network-derived telemetry to Splunk, addressing the organization's visibility requirements. Operating under PCI DSS standards, the customer leveraged

Gigamon to support compliance, simplify audits, and mitigate latency-related revenue risks. In another case, Gigamon saved public cloud costs by 85% by removing the need for cloud provider's load balancers.[2]

Across deployments, organizations typically reduce tool spend by 50% to 60% by utilizing Gigamon packet deduplication, load balancing, and traffic optimization.[3] In cloud environments, Gigamon lowers traffic acquisition costs from $0.75 to $0.04 per gigabyte by eliminating intermediary services.[4] These cost efficiencies and architectural simplifications position the company as a strategic differentiator in environments where security, scalability, and budget alignment are critical.

The Gigamon Deep Observability Pipeline delivers flexible packet processing, Precryption™-based visibility into encrypted traffic, and deep traffic inspection. These capabilities complement MELT-based tools by enriching them with network-derived telemetry that improves their effectiveness. This approach enables consistent security across cloud, on-premises, and hybrid environments, including unmanaged assets and transient workloads. GigaSMART® applications such as SSL/TLS decryption, advanced flow slicing, and AMI enhance SIEM with enriched telemetry and improve NDR performance by delivering high-fidelity data and reduced ingestion volume. Integrated automation and orchestration capabilities further streamline operations, offering control rarely found in bundled or siloed solutions.

Frost & Sullivan finds that Gigamon resolves critical visibility challenges that competitors have yet to address. While many vendors bundle observability into broader enterprise agreements or rely heavily on native cloud tools, they often lack essential capabilities such as inline decryption, metadata generation, and scalable traffic optimization. The Gigamon Deep Observability Pipeline enables secure inspection of encrypted traffic and optimizes data flows, ensuring complete, scalable, and actionable visibility across all environments.

With its clear focus on innovation, customer impact, and alignment with enterprise priorities, Gigamon distinguishes itself as a front-runner in operationalizing cybersecurity observability. Its ability to detect complex, encrypted, and emerging traffic types reinforces its relevance in a rapidly evolving threat sector. Frost & Sullivan recognizes the company for consistently helping organizations strengthen security, reduce complexity, and maximize value.

Aligning Observability with Evolving Compliance and Risk Management Demands

Security leaders in highly regulated industries like financial services and healthcare increasingly turn to Gigamon to maintain digital resilience, audit readiness, and threat detection efficacy. By integrating observability into compliance operations, Gigamon enables organizations to validate that they are meeting evolving compliance mandates such as PCI DSS 4.0, HIPAA, and the EU's DORA. Its solution captures real-time traffic and metadata across information technology (IT), operational technology (OT), and IoT networks, allowing customers to identify risks, enforce policies, and accelerate investigations with minimal disruption. Unlike standalone tools that rely on endpoint agents or offer siloed views, Gigamon provides a unified observability layer across hybrid environments.

[2] Gigamon, "Gigamon Saves Cloud Ops Costs", June 2025
[3] Gigamon, "Deep Observability Pipeline", June 2025, https://www.gigamon.com/content/dam/resource-library/english/solution-brief/sb-deep-observability-pipeline.pdf
[4] Ibid

For example, a US-based payment processor implemented Gigamon to troubleshoot latency issues and reduce regulatory exposure. The company faced daily fines for unresolved PCI DSS violations, and its endpoint detection and response (EDR) and logging tools lacked visibility into unmanaged and agentless devices. Gigamon helped the customer to tackle these challenges by delivering enriched metadata to the client's SIEM and co-developing a PCI-focused dashboard, later adopted as a standard product feature. This solution reduced tool sprawl, improved threat detection, and enhanced compliance.

> *"Large enterprises choose Gigamon for its scalable metadata generation, seamless integration with SIEM and observability platforms, and high-performance telemetry across complex environments. This telemetry-first architecture continues to earn trust among IT security leaders focused on operational resilience without added complexity."*
>
> ***- Ain Sarah Aishah***
> ***Best Practices Research Analyst***

Gigamon also aligns strongly with the EU's DORA framework, mapping its capabilities to the regulation's 5 core pillars: risk management, incident reporting, resilience testing, third-party oversight, and information sharing. Its deep observability pipeline spans hybrid environments and supports real-time traffic analysis, enabling customers to meet stringent information and communications technology (ICT) resilience standards. As a result, organizations can detect incidents earlier, shorten remediation timelines, and maintain operational continuity amid emerging threats.

Gigamon delivers deep observability across cloud, on-premises, and hybrid infrastructures by providing enriched network-derived telemetry that complements security tools such as SIEM and NDR, enhancing security operations with broad and consistent traffic insights. While many vendors treat compliance as an add-on or rely on limited native cloud integrations, Gigamon embeds compliance readiness into its observability approach. Frost & Sullivan recognizes the company for enabling organizations to meet evolving regulatory standards with confidence and resilience.

Delivering Scalable Threat Visibility and Operational Efficiency Through Ecosystem-driven Innovation

The company's focus on network telemetry and deep observability aligns closely with customer and partner needs, eliminates channel conflict, and broadens integration with leading ecosystem players. This strategy has driven growth in NDR-related revenue in 2024, supported by stronger go-to-market (GTM) alignment with partners.

In 2024, Gigamon launched the Power of 3 initiative—a strategic model that enhances hybrid cloud security through 3-way partnerships. These collaborations integrate the Gigamon Deep Observability Pipeline with ecosystem partners to enhance traffic visibility and threat detection. For example, a collaboration with ExtraHop and WWT combines the company's deep observability with ExtraHop RevealX to help joint customers eliminate blind spots across cloud, edge, and data center environments, addressing modern cybersecurity needs with precision and scale.

These partnerships underscore the role Gigamon plays in powering the cybersecurity ecosystem with high-fidelity packets and enriched metadata. By enhancing partner solution performance and reducing operational overhead, Gigamon enables NDR vendors to cut cloud inspection costs by up to 90% through

the integration of its UCT.[5] This strategy improves product performance, minimizes alert fatigue, and supports scalable cybersecurity operations.

The company's strategy consistently proves its value in high-stakes customer deployments. Large enterprises choose Gigamon for its scalable metadata generation, seamless integration with SIEM and observability platforms, and high-performance telemetry across complex environments. This telemetry-first architecture continues to earn trust among IT security leaders focused on operational resilience without added complexity.

Gigamon also delivers measurable cost savings through data reduction and tool optimization. By filtering irrelevant traffic, eliminating redundancy, and enriching data at the source, customers reduce tool overload and avoid unnecessary license expansions. The modular deployment and universal license model provide architectural flexibility and scalability without licensing complexity or hidden fees.

This operational efficiency extends across various deployments:

- A major Latin American bank adopted Gigamon as a scalable complement to full-scale NDR implementation, using it to provide broad visibility while focusing NDR tools only in critical environments. By integrating Gigamon AMI with Google SecOps and Elastic, the bank improved data ingestion, observability, and threat response. The deployment also enabled TCP-based performance monitoring and helped future-proof infrastructure for evolving compliance needs.
- One of Brazil's busiest ports improved east-west lateral visibility using Gigamon and selectively routed traffic into FortiNDR Cloud for critical environments, reducing unnecessary security infrastructure investments. Gigamon AMI supports protocol-level monitoring, improving threat detection, performance troubleshooting, and mean time to resolution.

These examples demonstrate how Gigamon maximizes the value of existing cybersecurity and performance monitoring tools. The company consistently outperforms competitors in public cloud packet brokering, encrypted traffic inspection, and advanced filtering. While rival vendors offer bundled features, they often lack metadata fidelity, cloud-native efficiency, and performance scalability. As procurement shifts toward outcome-based performance and architectural alignment, Gigamon delivers a demonstrably stronger return on investment.

Gigamon improves observability efficiency across cloud, on-premises, and hybrid infrastructures by eliminating intermediary services, enriching telemetry at the source, and reducing downstream compute loads. This aligns with the growing enterprise trend to decouple telemetry from tools and centralized data in scalable analytics environments. The company's continued investment in high-performance, cloud-agnostic packet processing cements its leadership in a market increasingly driven by precision, speed, and architectural agility.

[5] Bassam Khan (Vice President of Product and Technical Marketing Engineering, Gigamon), discussion with authors, June 2025

Conclusion

Gigamon drives the evolution of network observability to meet modern cybersecurity demands. Its telemetry-first architecture, agentless deep observability, and real-time traffic intelligence enable organizations to strengthen security, simplify compliance, and optimize operational efficiency across hybrid, multi-cloud, and on-premises environments. By delivering high-fidelity metadata and scalable packet processing, Gigamon reduces tool sprawl, eliminates blind spots, and extends coverage to unmanaged and ephemeral assets. Through strategic partnerships, a cloud-agnostic platform, and measurable customer impact, Gigamon positions itself as more than a visibility provider. It supports security operations that prioritize resilience, cost-efficiency, and long-term agility. Gigamon demonstrates clear innovation leadership, a consistent focus on outcome-driven deployments, and a strong ability to address the evolving needs of the global cybersecurity ecosystem.

With its strong overall performance, Gigamon earns Frost & Sullivan's 2025 Global Company of the Year Recognition in the network observability for cyber security industry.

What You Need to Know about the Company of the Year Recognition

Frost & Sullivan's Company of the Year Recognition is its top honor and recognizes the market participant that exemplifies visionary innovation, market-leading performance, and unmatched customer care.

Best Practices Recognition Analysis

For the Company of the Year Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Visionary Innovation & Performance

Addressing Unmet Needs: Customers' unmet or under-served needs are unearthed and addressed to create growth opportunities across the entire value chain

Visionary Scenarios Through Megatrends: Long-range scenarios are incorporated into the innovation strategy by leveraging mega trends and cutting-edge technologies, thereby accelerating the transformational growth journey

Leadership Focus: The company focuses on building a leadership position in core markets to create stiff barriers to entry for new competitors and enhance its future growth potential

Best Practices Implementation: Best-in-class implementation is characterized by processes, tools, or activities that generate consistent, repeatable, and scalable success

Financial Performance: Strong overall business performance is achieved by striking the optimal balance between investing in revenue growth and maximizing operating margin

Customer Impact

Price/Performance Value: Products or services offer the best ROI and superior value compared to similar market offerings

Customer Purchase Experience: Purchase experience with minimal friction and high transparency assures customers that they are buying the optimal solution to address both their needs and constraints

Customer Ownership Excellence: Products and solutions evolve continuously in sync with the customers' own growth journeys, engendering pride of ownership and enhanced customer experience

Customer Service Experience: Customer service is readily accessible and stress-free, and delivered with high quality, high availability, and fast response time

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty, which is regularly measured and confirmed through a high Net Promoter Score®

Best Practices Recognition Analytics Methodology

Inspire the World to Support True Leaders

This long-term process spans 12 months, beginning with the prioritization of the sector. It involves a rigorous approach that includes comprehensive scanning and analytics to identify key best practice trends. A dedicated team of analysts, advisors, coaches, and experts collaborates closely, ensuring thorough review and input. The goal is to maximize the company's long-term value by leveraging unique perspectives to support each Best Practice Recognition and identify meaningful transformation and impact.

		VALUE IMPACT	
STEP		WHAT	WHY
1	**Opportunity Universe**	Identify Sectors with the Greatest Impact on the Global Economy	Value to Economic Development
2	**Transformational Model**	Analyze Strategic Imperatives That Drive Transformation	Understand and Create a Winning Strategy
3	**Ecosystem**	Map Critical Value Chains	Comprehensive Community that Shapes the Sector
4	**Growth Generator**	Data Foundation That Provides Decision Support System	Spark Opportunities and Accelerate Decision-making
5	**Growth Opportunities**	Identify Opportunities Generated by Companies	Drive the Transformation of the Industry
6	**Frost Radar**	Benchmark Companies on Future Growth Potential	Identify Most Powerful Companies to Action
7	**Best Practices**	Identify Companies Achieving Best Practices in All Critical Perspectives	Inspire the World
8	**Companies to Action**	Tell Your Story to the World (BICEP*)	Ecosystem Community Supporting Future Success

*Board of Directors, Investors, Customers, Employees, Partners

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Generator™

Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.

Learn more.

Key Impacts:

- **Growth Pipeline:** *Continuous Flow of Growth Opportunities*
- **Growth Strategies:** *Proven Best Practices*
- **Innovation Culture:** *Optimized Customer Experience*
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** *Industry Leadership*

The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.

Analytical Perspectives:

- Megatrend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)