Horizons

S&P Global
Energy

451 Research Market
Insight Report Reprint

Gigamon fuses network telemetry with agentic AI to accelerate threat detection

April 13, 2026

by Mike Fratto

The company has introduced Gigamon Insights, an application that fuses trusted network data from the Gigamon Deep Observability Pipeline with agentic AI to accelerate threat detection and troubleshooting across hybrid cloud infrastructure.

Introduction

Gigamon introduced Gigamon Insights, an agentic AI application for network-derived telemetry that delivers guidance for security and IT operations teams, in 2025. Launching with integrations into security information and event management and observability platforms from Elastic NV and Splunk and cloud services from Amazon Web Services and Google, the application helps analysts ask questions, query trusted metadata and receive context-rich insight within existing workflows. This follows the company's earlier AI initiatives, including AI Traffic Intelligence and GigaVUE-FM Copilot. At the core of Gigamon Insights is Application Metadata Intelligence, which enriches network-derived telemetry with application-level context to ensure insights generated are both trusted and actionable.

THE TAKE

Gigamon Insights represents an evolution of the company's deep observability pipeline, positioning network-derived telemetry as a foundational data layer for AI-driven security and IT operations. The solution addresses a blind spot that log-centric security information and event management tools struggle to close: visibility into encrypted East-West traffic, application-layer metadata, and network behavior that reveals lateral movement and command-and-control activity. Gigamon attempts to reduce adoption friction of network AI analytics while expanding the addressable use cases for its Application Metadata Intelligence beyond traditional packet analysis. The company's flexible large language model architecture demonstrates awareness of data sovereignty concerns that could otherwise impede enterprise AI adoption in security contexts.

Context

Gigamon is a deep observability vendor that transforms, enriches and optimizes network-derived telemetry before delivering it to cloud, security and observability tools. The company serves over 4,000 customers worldwide, including more than 80% of Fortune 100 enterprises and nine of the 10 largest mobile network providers. The Gigamon Deep Observability Pipeline acquires traffic from physical, virtual, cloud and container environments, then transforms and enriches it before forwarding to security and observability tools.

The company has been building AI capabilities throughout 2025, starting with AI Traffic Intelligence, which identifies and classifies traffic from more than 40 generative AI and LLM engines without deploying agents. This was followed by GigaVUE-FM Copilot, an embedded assistant in Fabric Manager that delivers AI-powered guidance to simplify configuration and operations. Gigamon Insights represents the third pillar of the company's AI strategy, applying agentic AI directly to the network telemetry that flows through its pipeline.

The timing reflects market urgency around AI-driven threats. Traditional log-based security information and event management (SIEM) tools struggle to detect lateral movement and encrypted threats that operate below the application layer, creating a visibility gap that network telemetry can address.

Technology and products

Gigamon Insights is an agentic AI application that integrates with leading SIEM, observability and cloud platforms including Elastic Security, Splunk and AWS services. Security and IT analysts can ask natural language questions, run pre-defined prompts or craft free-form queries to analyze network-derived telemetry and receive context-rich answers directly within existing workflows. The technology will support both private hosted models in the future and bring-your-own enterprise LLMs, maintaining full data privacy and control.

The foundation of Gigamon Insights is Application Metadata Intelligence (AMI), which the company claims extracts close to 6,000 traffic-protocol and application-related metadata attributes from network traffic, enabling more precise detection of threats, performance anomalies and anomalous behavior patterns. AMI provides deep packet-level performance analysis including TCP performance metrics such as round-trip times, retransmission bytes, packet loss indicators and microsecond-precision timing. The technology offers application-layer deep inspection including file transfer forensics with actual filenames accessed, user identity at protocol level, email metadata and database activity monitoring.

AI Traffic Intelligence, another component of Gigamon's AI strategy, identifies and classifies traffic from more than 40 GenAI and LLM engines without deploying agents. This capability provides visibility into sanctioned and unsanctioned AI usage across public, private, virtual and container environments, supporting governance policies and spending optimization.

GigaVUE-FM Copilot delivers AI-powered configuration assistance, automated setup with human-in-the-loop verification and a conversational assistant that accelerates onboarding and troubleshooting.

Strategy

Gigamon AI strategy centers on embedding AI-driven intelligence across three core areas of the deep observability pipeline: traffic identification, operational automation and analytical acceleration. The company is targeting security operations centers and IT teams struggling with alert fatigue, skills gaps and blind spots in encrypted traffic. By integrating with established SIEM and observability platforms rather than competing directly, Gigamon positions itself as an enabler that enhances existing tool investments.

The partner-first approach allows customers to adopt Gigamon Insights by leveraging existing data stores, enterprise LLMs and operational workflows. This distribution strategy reduces time-to-value and lowers adoption risk compared with stand-alone AI security products that require infrastructure replacement. The flexible LLM architecture supporting both private hosted models in the future and customer-owned AI systems addresses data residency and sovereignty requirements that are critical for regulated industries including financial services and healthcare.

Competition

In the network performance monitoring segment, Gigamon encounters competition from Kentik, LogicMonitor and SolarWinds. Kentik provides a network observability platform with AI-powered insights for multicloud and hybrid environments, competing on network analytics and performance monitoring use cases. The company's big-data architecture enables analysis of massive flow datasets across complex distributed environments. LogicMonitor and SolarWinds deliver infrastructure-monitoring platforms serving managed service providers and enterprises with established IT service management integrations, although both typically rely on flow data, SNMP metrics and agent-based collection rather than comprehensive packet inspection.

Gigamon Insights adds some competitive pressure in security analytics. In network detection and response (NDR), Insights can be used to delay the acquisition NDR or replace the need for NDR with customers that do not need a full recording product set. In that sense, the company competes with Cisco Systems Inc.'s Encrypted Traffic Analytics within Secure Network Analytics, Darktrace's network AI platform, and ExtraHop's Reveal(x), all of which analyze network traffic for threat detection. Darktrace positions its platform around autonomous AI that learns network behavior patterns and detects anomalies without requiring predefined rules, competing directly with the Gigamon AI-driven approach. ExtraHop's Reveal(x) platform provides real-time wire data analysis with machine learning for threat detection and investigation, offering similar capabilities in network visibility and encrypted traffic analysis. Cisco emphasizes integration with its broader security portfolio and leveraging its installed base advantage in enterprise networking infrastructure.

The company also faces indirect competition from observability platform vendors including Elastic, Datadog Inc. and Splunk, which are Gigamon Insights integration partners. These platforms ingest multiple telemetry types including logs, metrics and traces but traditionally lack native network context capabilities that provide visibility into East-West and encrypted traffic flows. By positioning as an enabler rather than replacement, Gigamon differentiates itself from vendors requiring tool replacement while expanding use cases for its deep observability pipeline beyond traditional packet brokers including APCON, Keysight Technologies Inc. and NetScout Systems Inc. The agentic AI layer represents a strategic evolution that positions network-derived telemetry as a foundational data source for security and IT operations, addressing blind spots that log-centric platforms cannot close.

SWOT Analysis

STRENGTHS

Gigamon maintains a strong foundation in network visibility, providing an established pipeline for deploying AI-enhanced capabilities. Its partner-first strategy leverages existing customer tool investment rather than requiring replacement, reducing adoption friction while expanding addressable use cases. The flexible LLM architecture supporting both private hosted in the future and bring-your-own models addresses data sovereignty concerns critical in regulated industries.

WEAKNESSES

Its positioning as an infrastructure layer rather than an end-user tool means that the company relies on partner platform adoption and integration quality for market success. The network-centric approach requires customers to deploy and maintain the Gigamon Deep Observability Pipeline, adding operational complexity compared with agent-based or cloud-native alternatives. The Deep Observability Pipeline can simplify the distribution and management of network data to multiple tools but customers need to have enough complexity to gain significant benefit.

OPPORTUNITIES

The surge in AI-driven threats creates urgent demand for network-level visibility that traditional log-based tools cannot provide. The expansion of GenAI workloads drives new use cases for AI governance and performance monitoring that Gigamon AI Traffic Intelligence can address. Growing adoption of zero-trust architectures and microsegmentation policies requires continuous validation of East-West and encrypted traffic flows, an area where network-derived telemetry provides advantages over endpoint-centric approaches.

THREATS

Integration partners could develop native network telemetry capabilities that reduce dependency on third-party pipeline infrastructure. The convergence of security and observability markets brings well-funded platforms that could acquire network visibility capabilities through M&A activity. Economic pressure on enterprise IT budgets may limit willingness to invest in specialized network infrastructure when organizations already deploy multiple observability tools with overlapping capabilities.

CONTACTS

Americas: +1 800 597 1344
Asia-Pacific: +60 4 296 1125
Europe, Middle East, Africa: +44 (0) 203 367 0681

www.spglobal.com/energy
www.spglobal.com/en/enterprise/about/contact-us.html