SOLUTION BRIEF

Gigamon Insight Solution

Insight | Detect | Investigate

Key Benefits

- Dramatically increases the effectiveness and efficiency of SOC teams
- Simplified view of the threat environment with severity and confidence indicators
- Quickly detect and remediate incidents
- Improved organizational risk profile
- Predictable costs

Move from Managing Tools to Securing Your Organization

Cybersecurity professionals have come to terms with the inevitability of breaches but still remain working in a reactionary state of mind due to limited visibility, fractured tool sets, alert fatigue, and manual processes.

Complete network visibility in combination with accessibility to historical event data can automate and accelerate the identification and mitigation of threats and moves the advantage from the attacker back to the defender.

Network Threat Analytics at Scale

Leveraging network data as the single source of truth, Gigamon Insight sensors deployed in cloud, physical or virtual infrastructures receive metadata and feed it to the Gigamon Insight. Combine Gigamon Insight with GigaSECURE® Security Delivery Platform and you can ensure optimized data acquisition and increase your efficiency and ROI immediately.

Using a rich set of APIs, the web interface or a Gigamon application, as shown in Figure 1, SOC teams can quickly identify and act with confidence on threats of the highest severity. Offered as a SaaS solution, Insight is packaged with Gigamon Detect and Gigamon Investigate so your SOC teams work with easy-to-use applications that consolidate fundamental security capabilities in a single dashboard, making them easily accessible to the SOC analyst.

Gigamon Detect

Gigamon Detect is an Insight application that SOC teams use to quickly identify and act with confidence on threats of the highest severity. It features an entity-driven architecture with cross-lookup capabilities to provide analysts with the critical information they need to act including quick identification of malicious activities, whether an entity has previously generated an alert, context into traffic type and recommendations on next steps.

Gigamon Investigate

Gigamon Investigate is an Insight application the SOC teams use to investigate security incidents in their environment. It features data correlation and enrichment, and real-time search response times to help quickly understand the chain of events leading to an incident. Investigate dramatically increases the efficiency of the SOC, and significantly narrows the window between identifying and remediating an event.

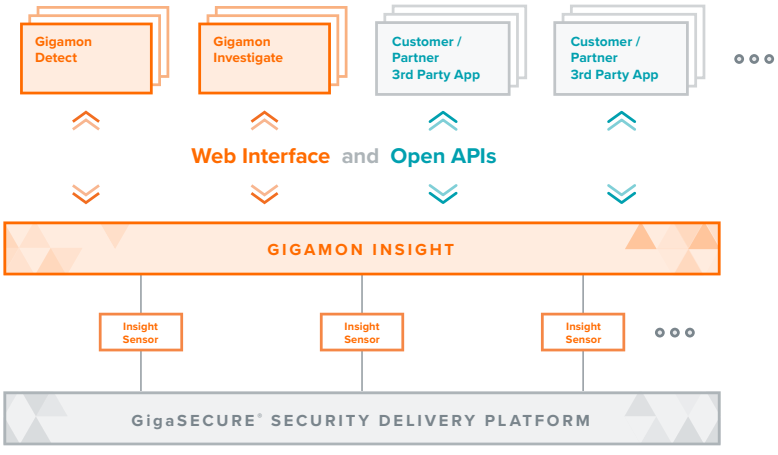

Figure 1 - Gigamon Insight, Gigamon Detect, and Gigamon Investigate

Additional Features

Organizations can supplement Gigamon Insight applications with their own queries and custom applications built on the Insight Query language (IQL). SOC teams can move from managing multiple security tools and manual correlation of alert and event data to a simple and efficient SaaS-based network threat analytics solution. Gigamon Insight empowers SOC teams with a core set of security functionality and the ability to rapidly deploy new security applications to improve their organization risk profile, with predictable costs.

Customers also receive the added benefit of having an assigned Technical Account Manager (TAM) on their account. Each TAM is a seasoned incident response practitioner and Gigamon Insight expert in detecting and investigating threats in a variety of network environments. This expert team helps use case expansion with real-world experience, alignment to industry best practice and user-relevant content creation.

Applied Threat Research Team

Gigamon Insight is supported by a world-class Applied Threat Research (ATR) team whose mission is to research, detect, and dismantle an adversaries' ability to impact customers by prototyping leading-edge detection, investigation, and response capabilities.

ATR experts leverage the Insight solution in addition to other data sources to research threats and deliver detection capabilities. As part of these efforts, ATR develops and maintains curated signatures enabling our customers to identify known threat indicators as well as generic suspicious activity. These signatures come complete with threat descriptions, assessed confidence and severity and actionable next steps.

The ATR team also builds analytic capabilities to deliver a deeper contextual understanding of the events and entities involved in network activity as well as enabling behavior-based threat detection. The intelligence provided by ATR expertise guides innovation and prototypes future capabilities

Feature/Application	Benefit
Rapid solution deployment across physical, virtual, private and public cloud environments	Gigamon Insight sensors can be deployed in minutes to the cloud, and in virtual and physical infrastructures. Using Gigamon Insight, you can start threat hunting and building reports quickly.
Powerful network security monitoring capabilities at scale	Gigamon Insight sensors can process over 100Gbps of sustained network throughput, providing visibility to traditional, "Bring you own device" (BYOD), cloud, mobile and Internet of Things (IoT) endpoints. This network traffic is processed and stored as metadata in the data platform, along with any selective on-demand packet captures (PCAP) required for threat hunting.
Rich query language for threat hunting	Gigamon Insight offers a rich, structured intelligent query language. SOC teams use it to hunt for threat indicators or to query the data set to rapidly understand the chain of events leading to an incident. With it, they can easily pivot from hunting to investigation and quickly build additional queries.
Real-time curated detections	The Gigamon Applied Threat Research team curates threat intelligence and signatures across a broad data set to provide targeted insights across customer tenants. This shared intel means your analysts spend less time with low quality detections and more time investigating real threats.
Threat intelligence data feeds	Gigamon Insight includes over 100 threat intelligence data feeds from a wide variety of sources, including commercially purchased feeds; open source threat intelligence data; vertical, industry and government information sharing organizations; as well as closed, trust-based communities. This threat intelligence data, which is reviewed and curated by the Gigamon Applied Threat Research team, allows for real-time matching of network data against known indicators.
Retroactive detection capabilities	The robust data set built over time gives SOC teams the ability to look back in time and understand the past impact of newly authored queries.
Sub-second searches	Reduce the mean time to remediation and answer critical investigative questions with sub-second real-time forensics to quickly scope incidents. Answer questions such as how a security event started, how many systems were impacted, and which data was accessed.

Deep file and artifact extraction	Extract file artifacts from network streams and perform static analysis to identify malicious files in transit.
Full packet capture capabilities	Sensors can be tasked to start selective full packet capture triggered on events. This enables SOC teams to dig deeper into key indicators of compromise to provide broad context into all network activity.
Fully managed from deployment to ongoing support	Network security specialists support you at every stage. Sensor configuration and maintenance is handled entirely by Gigamon.
Robust integrations	Pre-configured integrations for Splunk, IBM QRadar, ThreatStream/Anomali and DomainTools.
Application Programmer Interfaces (APIs)	Fully documented APIs allow workflow integration to optimize visibility withouwwt increasing workload while easily connecting to existing security tools.

Supported Protocols

Metadata and event types are collected from network traffic and sent to the Gigamon Insight data lake for different network protocols, including:

- IP flows
- DNS
- HTTP connections
- SMTP
- SSL/TLS sessions
- X509 certificates
- Kerberos network authentication protocol
- Portable Executable (PE) file transfer
- Remote Desktop Protocol (RDP)
- SSH session
- DHCP

Ordering Information

Gigamon Insight and Gigamon Detect are offered on a subscription basis.
Contact your sales representative for a specific pricing model or SKU information.

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