Effective Detection and Response Requires Fast Access to Information

Information security and incident response teams struggle because they cannot see what is happening on the network, cannot detect threats with confidence, and cannot respond to attacks quickly and effectively due to a lack of visibility.

Limited situational awareness and fractured toolsets force a dependence on heavily manual processes to fill information gaps in detection, investigation, and response activities. Frequent maintenance interrupts operations and place an additional burden on limited resources. The resulting alert fatigue, slow response times, and increased risk of a breach are unsustainable realities in a world where network complexity continues to grow.

Gain a Defenders Advantage with Fast Network Detection and Response

Gigamon Detect and Gigamon Investigate, included with Insight, consolidate fundamental network detection and response capabilities using enriched metadata collected from sensors deployed in physical, virtual, or cloud infrastructures. Customers minimize mean-time-to-detection and response by cutting through the noise with high confidence threat detection and real-time access to data for threat investigation searches.

Designed by responders, for responders, Insight is a unique cloud-based Network Detection and Response solution. Broad situational awareness in combination with real-time access to historical metadata accelerate threat detection and response, shifting the balance of power from attackers to defenders.
**Gigamon Detect**
Reduce mean-time-to-detection for the most advanced threats that operate subtly to evade independent gateway and endpoint defenses but cannot avoid revealing malicious network activity. Insight delivers high-confidence detections that give responders real-time access to associated context, drill-down details, and ‘next step’ recommendations developed by the Gigamon Applied Threat Research (ATR) team composed of experienced responders.

**Gigamon Investigate**
Reduce mean-time-to-response with unique investigation, threat hunting, and overall incident response capabilities. Eliminate large search delays and the manual overhead of correlating data from disparate systems. Gigamon Insight is a single tool for quickly understanding the chain of events and performing efficient threat hunting. Make responders more effective while reducing risk, cost and alert fatigue.

**Fast Deployment, Fast Value**
Plug-n-play deployment can produce results in a few hours, while the zero-maintenance advantage of a SaaS solution allows analysts to spend more time fighting threats, and less time fighting tools. Gigamon maintains Gigamon Detect, Gigamon Investigate and network sensors to provide customers immediate access to new capabilities with no downtime. Even the web interface design focuses on the analyst function to help new users or less experienced analysts to become productive quickly.

**Additional Features**
Gigamon Insight is also a platform, built from the ground up for easy integrations into existing products and workflows. Fully documented APIs provide analysts the ability to integrate Insight functionality into existing workflows and security products.

Insight supports the ability to operationalize third party threat intelligence feeds, matching threat indicators in-line to the data, and enabling you to both search for, and alert on, those matches. Included as part of your subscription, Gigamon ATR collects and analyzes over 100 threat intelligence feeds, in addition to Gigamon proprietary threat intelligence, for use by all of our customers.

The Gigamon Insight subscription includes a designated Technical Account Manager (TAM), who is a seasoned incident response practitioner and Gigamon Insight expert in detecting and investigating threats in a variety of network environments. This expert helps with use case expansion with real-world experience, alignment to industry best practice and user-relevant protection coverage.

**Gigamon Security Delivery Platform to Further Enhance Performance**
Combine Gigamon Insight with the Gigamon Security Delivery Platform to help ensure optimized data acquisition and increase efficiency and ROI immediately.

The Gigamon Security Delivery Platform is a next-generation network packet broker focused on threat prevention, detection, and response. It helps ensure optimal data acquisition across physical, virtual and cloud networks, with the performance that is vital to the effectiveness of all your security solutions that depend on the right tools receiving the right traffic at the right time, every time. The platform can also off-load SSL decryption, traffic filtering, de-duplication, and other functions to extend the value of your security investments by letting security solutions focus on their core functions while eliminating non-essential and performance draining operations.

**Applied Threat Research Team**
Gigamon Insight is supported by a world-class Applied Threat Research team whose mission is to research, detect, and dismantle an adversaries’ ability to impact customers by producing leading-edge detection, investigation, and response capabilities.

ATR analysts leverage the Insight solution, in addition to other data sources, to research threats and deliver detection capabilities. As part of these efforts, the team develops and maintains curated signatures enabling our customers to identify known threats as well as generic suspicious activity. These signatures come complete with threat descriptions, assessed confidence and severity ratings 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 with the goal of making today’s users more equipped to detect tomorrow’s threats.
<table>
<thead>
<tr>
<th>Feature/Application</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid deployment across physical, virtual, private and public cloud</td>
<td>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 detecting malicious activity quickly.</td>
</tr>
<tr>
<td>Powerful network security monitoring capabilities at scale</td>
<td>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 in-depth analysis.</td>
</tr>
<tr>
<td>Rich query language for threat hunting</td>
<td>Gigamon Insight offers a rich, structured Insight 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.</td>
</tr>
<tr>
<td>Real-time curated detections</td>
<td>The Gigamon Applied Threat Research team curates threat intelligence across a broad data set to provide understanding at a global scale. This shared intel means your analysts spend less time with low quality detections and more time investigating real threats.</td>
</tr>
<tr>
<td>Threat intelligence data feeds</td>
<td>Gigamon Insight metadata 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; as well as closed, trust-based communities. This threat intelligence, which is reviewed and curated by the Gigamon Applied Threat Research team, allows for real-time matching of network data against known indicators.</td>
</tr>
<tr>
<td>Retroactive detection capabilities</td>
<td>The robust data set built over time gives SOC teams the ability to look back in time and apply newly authored queries for improved understanding.</td>
</tr>
<tr>
<td>Real-time search results</td>
<td>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.</td>
</tr>
<tr>
<td>Deep file and artifact extraction</td>
<td>Extract file artifacts from network streams and perform static analysis to identify malicious files.</td>
</tr>
<tr>
<td>Targeted packet capture capabilities</td>
<td>Sensors can be tasked to start selective full packet capture for traffic of interest. This enables SOC teams to dig deeper into key indicators of compromise to provide broad context into all network activity.</td>
</tr>
<tr>
<td>Fully managed from deployment to ongoing support</td>
<td>Network security specialists support you at every stage. Sensor configuration and maintenance is handled entirely by Gigamon.</td>
</tr>
<tr>
<td>Robust integrations</td>
<td>Pre-configured integrations for Splunk, IBM QRadar, ThreatStream/Anomali and VirusTotal.</td>
</tr>
<tr>
<td>Application Programmer Interfaces (APIs)</td>
<td>Fully documented APIs allow workflow integration to optimize visibility without increasing workload while easily connecting to existing security tools.</td>
</tr>
</tbody>
</table>
Supported Protocols

Metadata and event types are collected from network traffic and sent to the cloud-based Gigamon Insight metadata repository for different network protocols, including:

- FLOW
- DNS
- HTTP
- SMTP
- SSL
- X509
- KERBEROS
- PE
- RDP
- SSH
- SOFTWARE
- DHCP
- SURICATA
- SMB_FILE
- SMB_MAPPING
- NTLM
- TUNNEL
- FTP
- DCE-RPC

Ordering Information

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