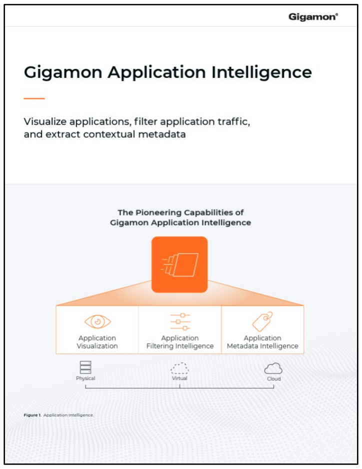
Gigamon®

carahsoft.



Gigamon®

Gigamon Application Intelligence

Visualize applications, filter application traffic, and extract contextual metadata

The Pioneering Capabilities of Gigamon Application Intelligence

Application Visualization
Application Filtering Intelligence
Application Metadata Intelligence
Physical
Virtual
Cloud

Figure 1. Application Intelligence.

Gigamon Application Intelligence

Visualyze applications, filter application traffic, and extract contextual metadata

Thank you for downloading this Gigamon Solution Brief. Carahsoft is the distributor for Gigamon Cybersecurity solutions available via NASPO ValuePoint, NJSBA, The Quilt and other contract vehicles.

To learn how to take the next step toward acquiring Gigamon's solutions, please check out the following resources and information:

For additional resources:
carah.io/GigamonResources

For upcoming events:
carah.io/GigamonEvents

For additional Gigamon solutions:
carah.io/GigamonSolutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Gigamon@carahsoft.com
703-673-3515

To purchase, check out the contract vehicles available for procurement:
carah.io/GigamonContracts

For more information, contact Carahsoft or our reseller partners:
Gigamon@carahsoft.com | 703-673-3515

Gigamon Application Intelligence

Visualize applications, filter application traffic, and extract contextual metadata

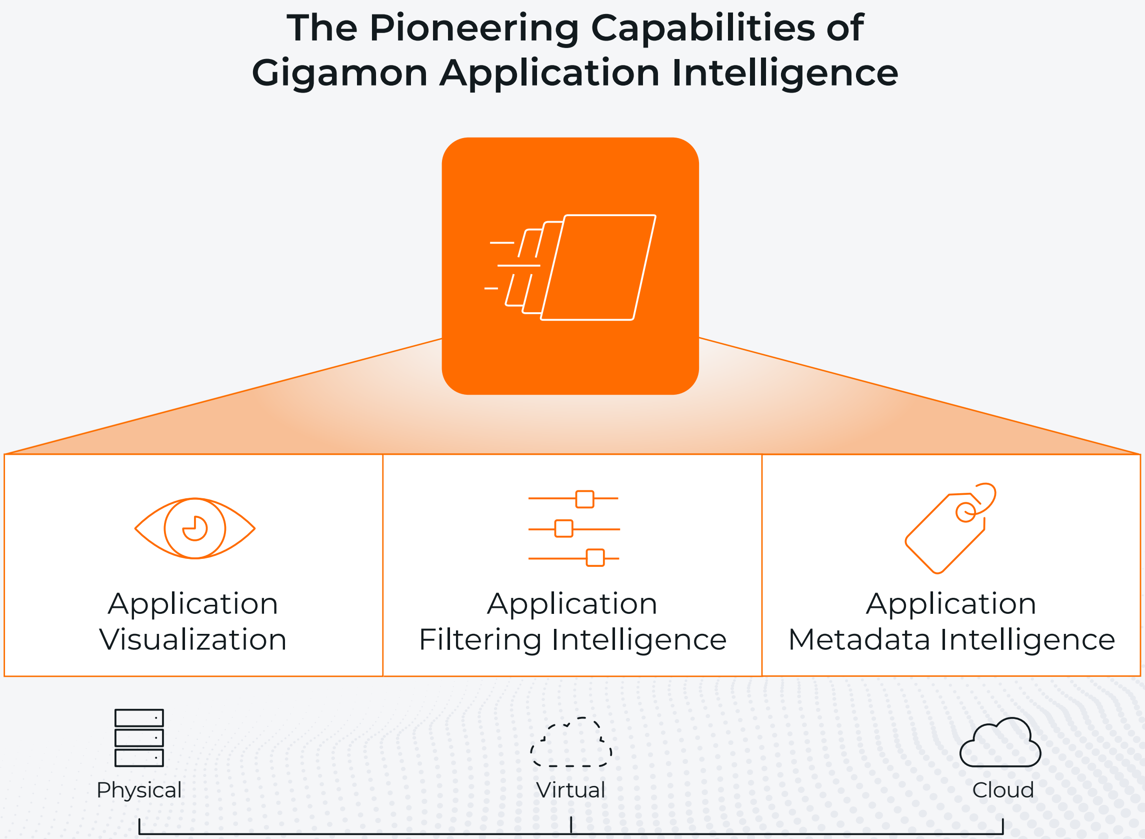

The Pioneering Capabilities of
Gigamon Application Intelligence
Application Visualization
Application Filtering Intelligence
Application Metadata Intelligence
Physical
Virtual
Cloud

Figure 1. Application Intelligence.

Gigamon Application Intelligence is a pioneering set of capabilities for getting the visibility and context across the Gigamon Deep Observability Pipeline needed to discover, manage, and secure even complex, multi-tier applications regardless of location: on-premises or in multi-cloud deployments.

Gigamon Application Intelligence automatically identifies more than 4,000 applications and up to 6,000 application metadata elements.

It enables IT teams to visualize each application and its elements, extract that data for delivery to the right tools, and use application metadata to ensure strong security and great customer experiences.

In the AI era, visibility is no longer enough. What's required is deep observability infused with AI — delivering the ability to extract, analyze, and act on the most relevant network-derived telemetry and insights, along with AI traffic visibility and control.

Key Features

- Deep packet inspection identifies more than 4,000 apps and classifies them based on pre-defined application families and tags
- Selectively filters traffic based on standard and custom apps, and application families and tags
- Generates up to 6,000 advanced L4– L7 attributes
- Pre-built connectors for popular SIEMs and out-of-box integration with third-party tools
- Available for GigaVUE® HC Series and GigaVUE Cloud Suite™
- Identify applications independent of the ports on which they are configured to run
- Identify GenAI apps for enhanced security with AI traffic visibility and control

Key Benefits

- Isolate, extract, and send only app-specific traffic to the proper monitoring and security tools
- Detect, manage, and isolate shadow IT and rogue applications and block as appropriate
- Identify users and applications using excessive bandwidth and throttle their use
- Application Metadata Intelligence provides contextual insights to further improve security and aids troubleshooting without having to turn on additional logs and traces
- Offload metadata generation from endpoints and tools and normalize data from diverse traffic sources for tool optimization
- Generate metadata for managed, unmanaged, and remote endpoints
- Combine with other Gigamon products for additional traffic optimization
- Add deeper context to events and logs with application metadata that is tough to disable or modify and is hard to spoof
- Customize or add new use cases for monitoring metadata on the fly
- Identify the prevalence of GenAI apps and audit their usage for fine tuning security controls

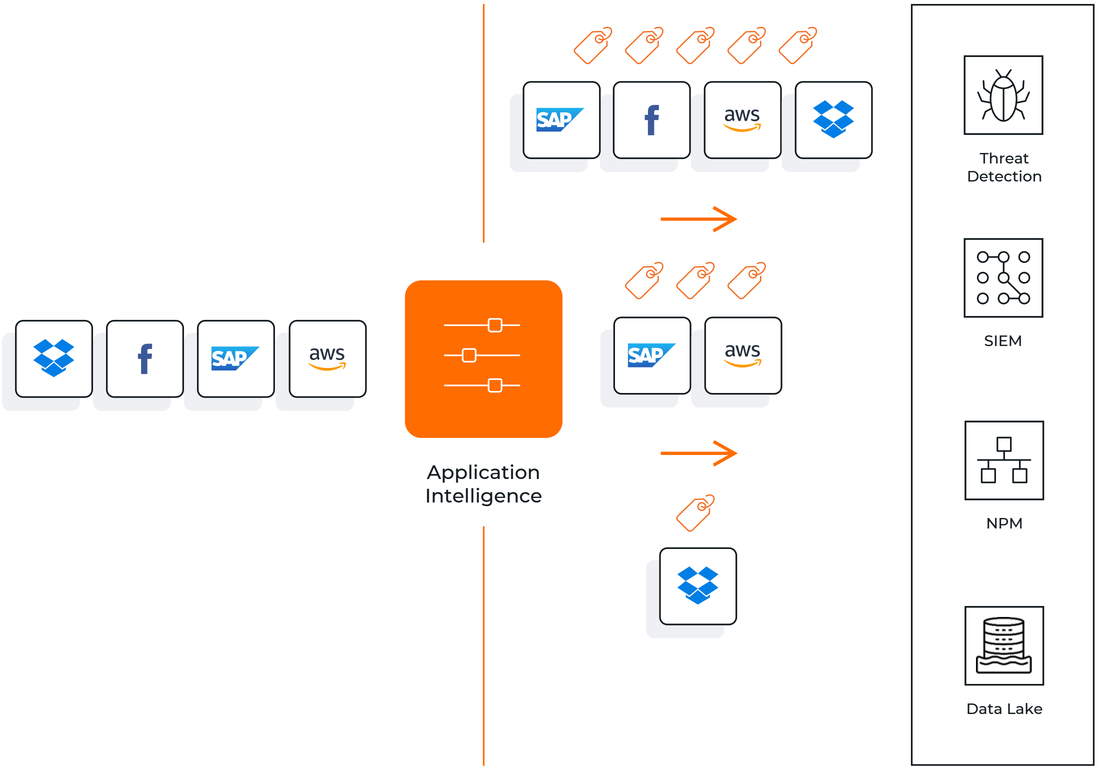


Figure 2. Gigamon Application Intelligence employs flow pattern matching, bi-directional flow correlation, heuristics, and statistical analysis to accurately identify thousands of standard and custom applications, and directs that information, along with Application Metadata Intelligence, to selected tools to improve their effectiveness.

Overcome Networking and Application Visibility Challenges

In an ideal world, managing and securing your network would be smooth and efficient. Your on-premises and cloud-based tools would have full network and application visibility, without any blind spots. Tools could obtain not only basic NetFlow metadata but also application-aware attributes to make your SIEMs and other security appliances more powerful. They would also have the option to select only relevant application traffic to maximize utilization. And all of this would be achieved without taking days or weeks of IT time. It's a world worth striving for, but today's reality is much different:

- Visibility into network and application data is limited
- Tools are bombarded with irrelevant traffic without application context for proper security and customer experience analysis
- It's difficult for NetOps teams to deliver the right application traffic to the right analytics tools
- Application owners cannot identify bottlenecks in distributed applications
- Security teams find it difficult to meet security and compliance requirements
- Generating basic NetFlow or L4–L7 advanced metadata attributes in the cloud is virtually impossible
- Emergence of AI-driven challenges, including traffic surges, AI-powered adversaries, and increased complexity

To address these problems, IT teams must take manual steps to identify applications based on network traffic, by either hardwiring ports to specific applications or by writing regular expressions to inspect traffic patterns and identify apps. Manual workarounds, however, bring their own challenges. Among them: Whenever change occurs, such as growth in an application's usage or the introduction of new applications, NetOps teams must update the physical network segmentation. While regular expressions-based application identification can work, an application's traffic pattern and behavior can change over time as it gets updated. This means IT must constantly test and update their homegrown regex signatures each time.

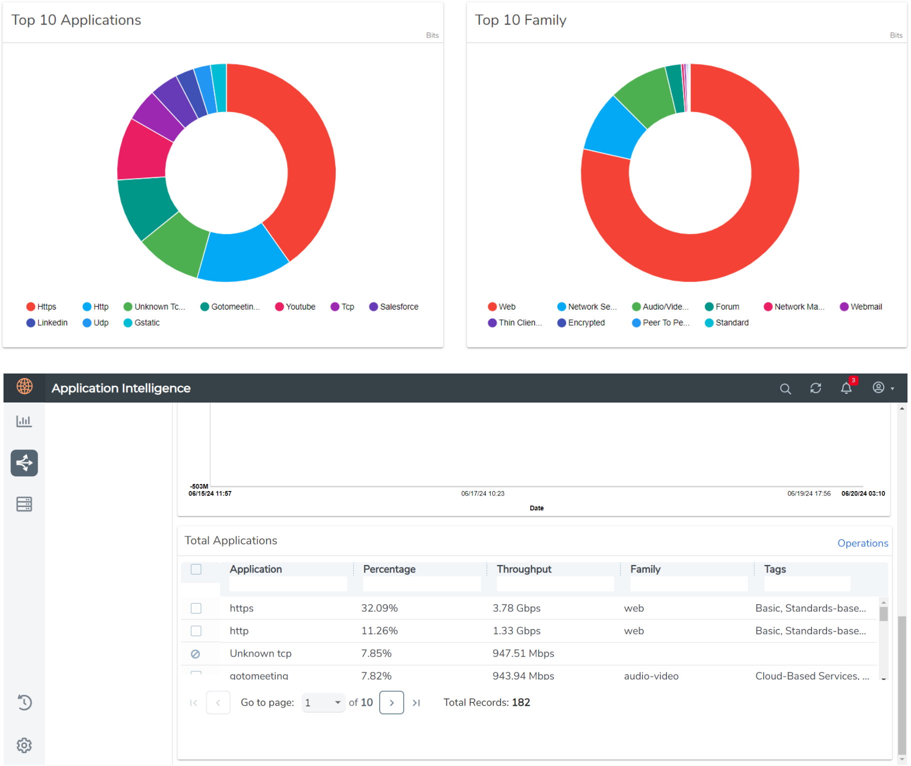
Fortunately, a solution to these problems is at hand. It's called Gigamon Application Intelligence, and it's a pioneering set of capabilities for getting the visibility and context needed to discover, manage, and secure even complex, multi-tier applications.

The Solution

Gigamon Application Intelligence is composed of three components:

- Application Visualization
- Application Filtering Intelligence
- Application Metadata Intelligence
- Application Metadata Exporter

This license is available for all GigaVUE HC Series physical appliances and GigaVUE Cloud Suite with GigaVUE V Series.



Total Applications

Operations

□	Application	Percentage	Throughput	Family	Tags
□	https	32.09%	3.78 Gbps	web	Basic, Standards-base...
□	http	11.26%	1.33 Gbps	web	Basic, Standards-base...
⊘	Unknown tcp	7.85%	947.51 Mbps		
□	gotomeeting	7.82%	943.94 Mbps	audio-video	Cloud-Based Services, ...

Go to page: 1 of 10 Total Records: 182

Figure 3. GigaVUE-FM fabric manager provides a dashboard to highlight the applications present on the network and their bandwidth utilization.

Application Visualization

Most traffic volume comes from a few top applications. Yet these may not include your most mission-critical applications or be the main sources of security or noncompliance concerns. The inability to identify these critical apps can mean that your organization's most important activities stay dark.

Gigamon Application Intelligence identifies more than 4,000 applications, including GenAI. To facilitate management and policy enforcement, Gigamon automatically classifies these applications into specific categories, including GenAI, social media, streaming media, shadow IT apps, VoIP services, messaging, and P2P applications.

Furthermore, internally developed applications also need monitoring. Gigamon Application Intelligence identifies custom or proprietary applications, so they're identified and managed like any other application.

Application Filtering Intelligence

Historically, all applications were treated equally as data from every application was sent to every tool. However, each application is unique in its importance to such tools. For example, high volume low risk traffic need not be forwarded to the tools, only unknown applications could be forwarded to a packet capturing tool for further analysis, only internal applications could be forwarded to APMs.

With Application Filtering Intelligence, you can extract and precisely match an application's traffic with the right tool. The solution provides the ability to isolate the application, and its components and protocols, and direct that traffic using the GigaVUE-FM fabric manager.

To further facilitate apps-to-tool matching, you can easily enforce policies on categories of applications. For example, administrators can define a set of tools that analyze all corporate traffic, another for all database traffic, and a third set for shadow IT and P2P traffic.

Application Metadata Intelligence

Gigamon Application Metadata Intelligence derives app behavior and details pertaining to flows, reduces false positives, helps in identifying nefarious data extraction, and accelerates threat detection through proactive, real-time monitoring versus reactive forensics.

Application Metadata Intelligence provides summarized and context-aware L2-L7 information about network packets. It can export up to 6000 attributes that can help organizations in network, applications and security monitoring. These include:

- Identification: Social media user, file and video names, SQL requests
- HTTP: URL identification, commands response codes levels
- DNS parameters: Request, response, queries, and device ID
- IMAP and SMTP email-based communications with addresses
- Service identification: Audio, video, chat, and transfers for VoIP and messaging

Application Metadata Exporter

Customers consolidating their network and security tools stack in the cloud can use Application Metadata Exporter (AMX) to aggregate, enrich, normalize, and reliably and securely export or stream network telemetry from hybrid cloud environments.

AMX application supports the following data sources and exports the data to the tools in JSON or OCSF format. It supports out-of-the-box integrations with Splunk Cloud, Elastic, Dynatrace, MS Sentinel, New Relic, and other eco-system partner tool vendors.

- NetFlow/IPFIX ingestion and export, including from Gigamon AMI application and third-party devices such as switches, routers, firewalls, etc
- Network application metadata ingestion from Gigamon AMI application and export to the tools.

- For the Mobile Service Provider Network, Control plane ingestion from the Gigamon mobility application and export to the tools.

For mobile networks, it can enrich user-plane data from the AMI application with control-plane metadata from the Mobility application for monitoring, troubleshooting, and analytics.

It can provide deeper situational awareness for private and public cloud environments by enriching the AMI application metadata with external AWS, Azure, and VMWare data. This helps to improve troubleshooting performance and latency issues, capacity utilization, threat detection, and incident response.

Gigamon Application Intelligence Use Cases

Shining a Light on Shadow IT

Gigamon Application Intelligence automatically identifies a wide range of applications and their underlying components. Security tools can now flag shadow IT activities and rogue apps that should be blocked or closely tracked.

SecOps teams can also identify and proactively address risky application configurations within each tier or service. Once a vulnerability is identified, either internally or through third-party feeds, SecOps teams can automatically take remedial actions.

Optimizing Network and Security Tools

Gigamon Application Intelligence enables IT to select traffic by application or family of applications and send it to the appropriate tools. This ultra-granular control lessens the burden on tools and allows them to focus on mission-critical applications.

For example, you can filter out trusted traffic, such as Microsoft Windows updates or streaming media from Netflix or Apple, allowing your tools to detect suspicious activities more quickly and operate much more efficiently. Through a simple drag-and-drop process via GigaVUE-FM, traffic flow definitions can be implemented in minutes.

Managing and Monitoring DX Applications

The success of any digital transformation initiative depends on the underlying applications performing optimally. Application Metadata Intelligence, in conjunction with your analytics tools, can help pinpoint poor user experiences. For example, it can extract key metadata attributes in a video embedded in a customer-facing application, such as:

- Starting frames per second rate and how it changes over time
- Bitrate changes over time
- Drop from HD to standard video quality
- Length of video
- When the user stopped the video

Application and network performance monitoring tools can use this information to determine the user's true video viewing experience and potential causes of service degradation.

Faster Threat Detection and Remediation

Perhaps the biggest beneficiaries of Gigamon Application Intelligence are security analytics tools. Application Visualization and Application Filtering capabilities direct specific applications to the right tools to improve tool efficiency, while application metadata provides the context to improve tool accuracy and accelerate corrective action.

As an example, export and monitor any malicious HTTP URLs in SIEMs. This allows to correlate those malicious URLs with inline security controls such as firewalls and proxies to bridge any gaps. It helps the tool to take corrective action proactively and improve overall efficiency.

Regulate GenAI usage

Usage of GenAI has made organizations more susceptible to data breaches, governance risks and supply chain attacks. While a blanket ban on using the GenAI apps is impractical, organizations are required to better regulate it for driving innovation and productivity. Using Gigamon Application Intelligence, organizations can identify the prevalence of GenAI productivity apps in their hybrid cloud environment and audit their usage for fine tuning the security controls.

For more insights into the dozens of Application Intelligence use cases, download the following technical briefs:

- Optimize Your Network Across Layers with Gigamon Application Filtering Intelligence
- Keep Networks Responsive and Secure with Gigamon Application Metadata Intelligence
- In These Transformative Times, Take These Practical Steps to Ease the Network Burden

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived telemetry to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit gigamon.com.

For more information about Gigamon or to contact a local representative, please visit: gigamon.com.

Gigamon®

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