SOLUTION BRIEF

Gigamon Application Intelligence

The Need for True Application Visibility

Key Capabilities

Application Visualization

- Automatically identifies applications through deep packet inspection
- Covers over 3,000 applications with auto-classification of apps into families
- Detects proprietary applications, including components within custom applications

Application Filtering

- Isolates and extracts application-specific traffic for delivery to the appropriate tools via simple traffic flow control
- Enables traffic flow control over common and custom apps, families of apps and application components
- Lets you select certain applications for additional scrutiny and deprioritize others to ease the burden on tools

Application Metadata

- Automatically generates application metadata
- Provides over 5,000 metadata elements related to various types of analysis, such as security, user experience and performance metrics
- Offers pre-built connectors to popular SIEMs and out-of-the-box integration with third-party tools

In an ideal world, managing and securing your network would be smooth and efficient. Your tools would have full network and application visibility, without any blind spots. They would also have the option to select only relevant network 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

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 are:

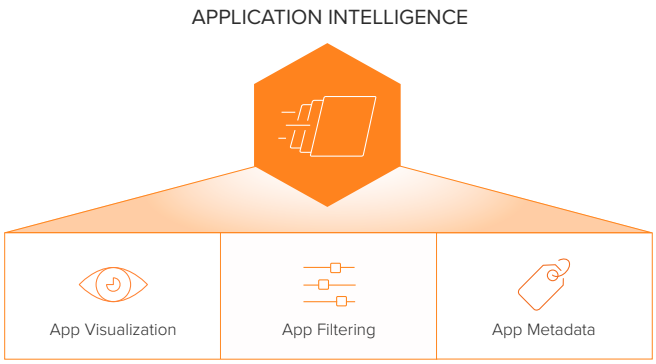
- Whenever change occurs, such as growth in an application's usage or the introduction of new applications, NetOps teams must update the physical network segmentation
- While regular expressions-based application identification can work, an application's traffic pattern and behavior can change over time as it gets updated. This means IT must constantly test and update their homegrown regex signatures each time.

Gigamon Application Intelligence: True Application Visibility

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 the context needed to discover, manage and secure even complex, multi-tier applications.

Gigamon Application Intelligence automatically identifies more than 3,000 applications and more than 5,000 application metadata elements. It enables IT teams to visualize each application and its components, extract that data for delivery to the right tools and use the application metadata to ensure strong security and great customer experiences.

Gigamon Application Intelligence comprises three main capabilities:



Application Visualization
To be effective, an application intelligence solution needs to identify applications from network packets. It needs to inspect OSI Layer Layer 2–3-based packets and extract Layer 4–7-based information.

The Workaround that Didn't Work Well
In the past, the workaround was to classify applications based on TCP ports being used. For example, you would classify:

- Port 22 for SSH
- Port 80 for HTTP
- Port 443 for SSL

Unfortunately, this approach proves ineffective because application developers often choose non-standard ports. There's also the problem of port spoofing, in which an attacker attempts to bypass perimeter safeguards by directing network traffic with malicious intent using non-standard (read: unexpected) ports.

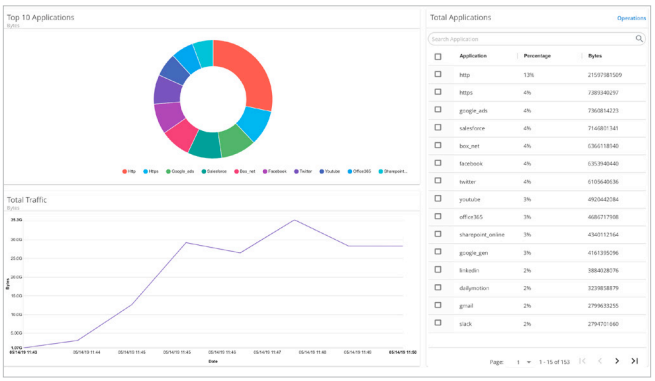
Precise Identification Using Deep Packet Inspection
Unlike such port-based application identification, Gigamon Application Intelligence is powered by deep packet inspection. Applications are classified based on several immutable attributes around traffic behavior and involve flow-based matching, bi-directional flow correlation, heuristics and statistical analysis. Packet data is matched against analysis from Gigamon researchers and maintained for accuracy.

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

That's why Gigamon Application Intelligence can identify more than 3,000 unique applications. To facilitate management and policy enforcement, Gigamon automatically classifies these applications into specific categories, including:

- Social media
- Streaming media
- Shadow IT apps
- VoIP services
- Messaging
- 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 app.



Application data is graphically presented through the GigaVUE® Fabric Manager.

Isolation of Application Components for Analysis
Modern apps commonly have multiple tiers of code, including app, web and database tiers, along with search capabilities. This complexity is exacerbated when the app is containerized with micro-service designs. Such apps developed by DevOps teams allow rapid code revision and updates and faster rollout and time-to-revenue.

The downside? These containerized apps comprise dozens and potentially hundreds of services. And each service may run in different containers, in different networks and may involve multi-cloud environments. It is impossible to run agent software from application performance monitoring and security tools next to each application component and thus they are too complex to monitor and secure with traditional tools. Any app identity solution needs to account for and offer granular insight into each of these services.

Gigamon Application Intelligence provides a single platform to monitor multi-tiered digital applications. It drills down, collects and centralizes traffic data from the various tiers and services, and then identifies application components, such as Oracle query, Elastic Search action and even industrial control system calls.

Application Filtering
Historically, all applications were treated equally in the sense that the data from every application was sent to every tool. However, each application is unique in its importance to such tools. For example, forensic solutions need to see all traffic. Web Application Firewalls need to only see web traffic. Intrusion Detection System appliances can ignore Spotify. Secure Email Gateways primarily care about email, attachments and embedded URL links. Security Information and Event Management (SIEM) solutions don't need to store streaming video.

Once applications are identified and categorized, the next step is to send focused traffic to tools by controlling the traffic flow. Without advanced application-aware solutions, such as with Gigamon Application Intelligence, administrators are forced to direct traffic to various tools based only on protocol information. For example, send:

- HTTP traffic to Advanced Threat Protection (ATP) and Intrusion Prevention Systems (IPS)
- POP3/IMAP traffic to secure email gateways
- DNS traffic to a DNS application firewall

Matching the Right Data with the Right Tools
In contrast, with Gigamon Application Intelligence it's now possible to extract and precisely match an application's traffic with the right network data analysis or security tool. The solution provides the ability to isolate the application, its components and protocols, and to direct that traffic through the GigaVUE Fabric Manager.

For instance, within the HTTP protocol, one set of tools can process Salesforce.com and Workday.com traffic, while another set of tools can analyze Dropbox and Slack. This laser-like precision removes the noise and brings clarity to each tool, which dramatically increases the tool's effectiveness and efficiency and decreases security vulnerabilities.

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
Application metadata is the simplest and most comprehensive way to obtain application behavior. You can learn critical details pertaining to flows, reduce false positives by separating signals from noise, identify nefarious data extraction and accelerate threat detection through proactive, real-time traffic monitoring versus reactive forensics.

SIEM solutions, for example, use this information to correlate and analyze log data from servers and security appliances, such as IPS, anti-malware and firewalls.

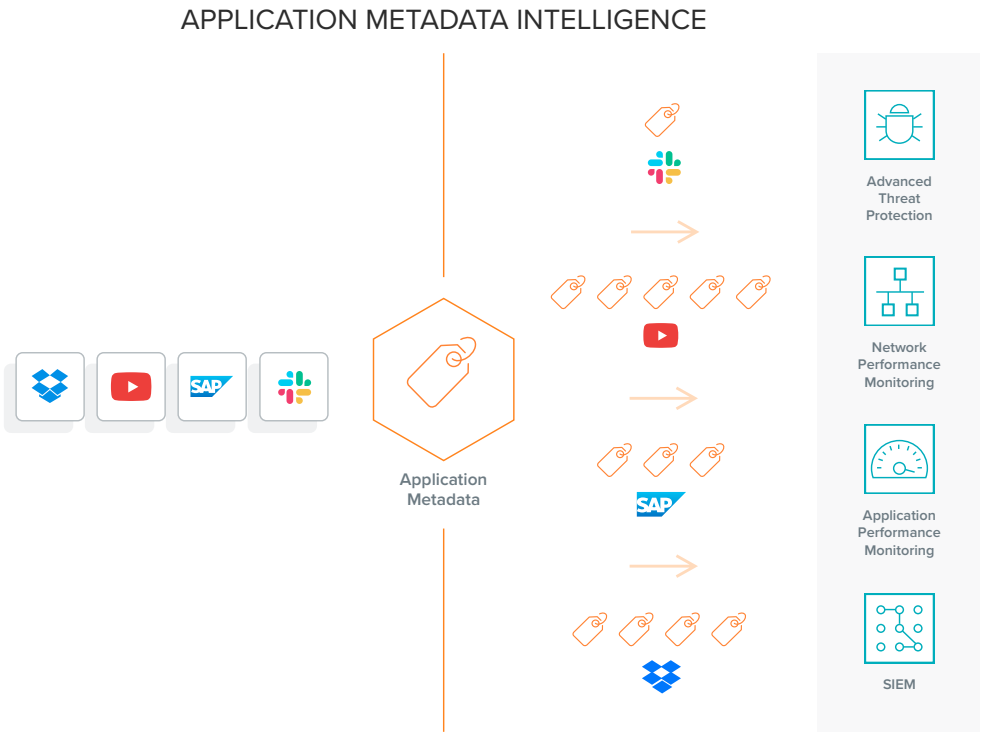
Gigamon Application Metadata, powered by deep packet inspection, provides summarized and context-aware information about raw network packets based on Layers 4–7. It supplies network and security tools more than 5,000 L4–L7 metadata attributes that shed light on the application's performance, customer experience and security.

Gigamon extracts and appends these elements to NetFlow and IPFIX records, including:

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

Easily Incorporate Metadata Elements Into Your Current Monitoring and Security Tools

Gigamon Metadata Intelligence comes with pre-built connectors for Splunk and IBM QRadar. You'll also benefit from a growing ecosystem of third-party vendors who are integrating Gigamon Application Metadata into their tools for more powerful advanced threat protection and data loss prevention out of the box.



Gigamon Application Intelligence extracts metadata elements for use by ecosystem tools.

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, by filtering out trusted traffic, such as streaming media from Netflix or Apple and Microsoft Windows updates, the tools can detect suspicious activities more quickly and operate much more efficiently. Through a simple drag-and-drop process via the GigaVUE Fabric Manager, traffic flow definitions can be implemented in minutes.

Managing and Monitoring DX Applications
The success of any digital transformation initiative depends on the underlying application performing optimally. Application Metadata, 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, social media usage, such as Facebook, should be directed to ATP solutions. If, on top of understanding the application involved, the tool knows a Messenger chat window was opened and the user subsequently received an executable file during the exchange, the tool can use sandboxing to quarantine the file until is it analyzed. The ATP tool is more effective, log data is more comprehensive and alerts are generated faster.

Learn More

To learn how Gigamon Application Intelligence can help your business, visit www.gigamon.com/app-intel.

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