Gigamon Application Intelligence

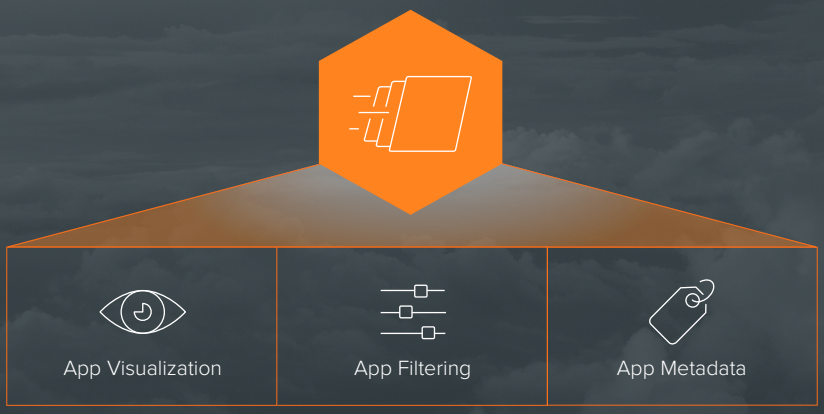
Visualize, extract and share application traffic and metadata

Gigamon Application Intelligence is 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 7,000 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 application metadata to ensure strong security and great customer experiences.

THE PIONEERING CAPABILITIES OF GIGAMON APPLICATION INTELLIGENCE

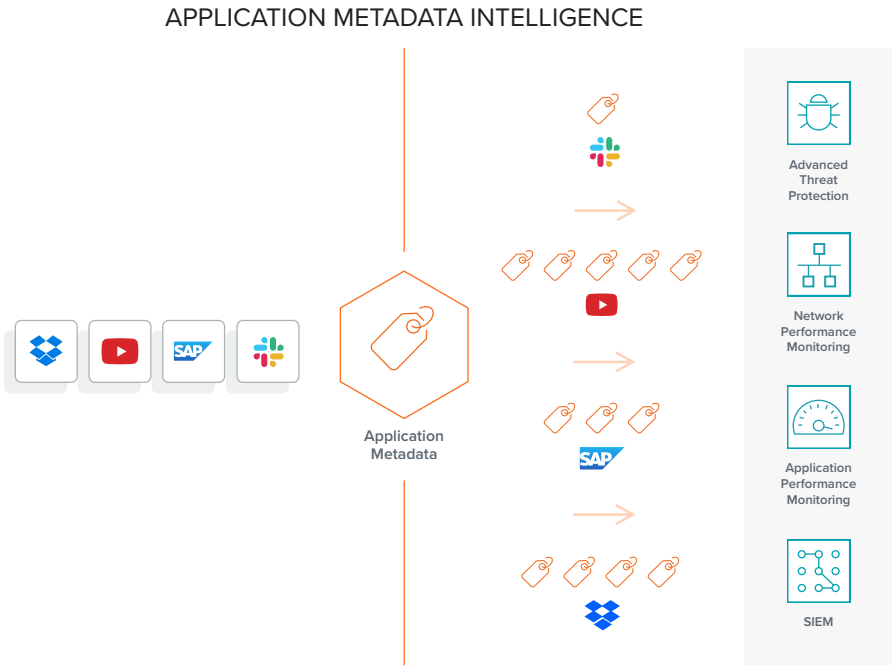


KEY FEATURES

- Deep packet inspection identifies more than 3,000 apps and auto-classify into families
- Selectively filter traffic based on standard and custom apps
- Automatically generates more than 7,000 advanced L4–7
- Pre-built connectors for popular SIEMs and out-of-box integration with third-party tools

KEY BENEFITS

- Isolate, extra and send only app-specific traffic to 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-aware metadata provides contextual insights to further improve security



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 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 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

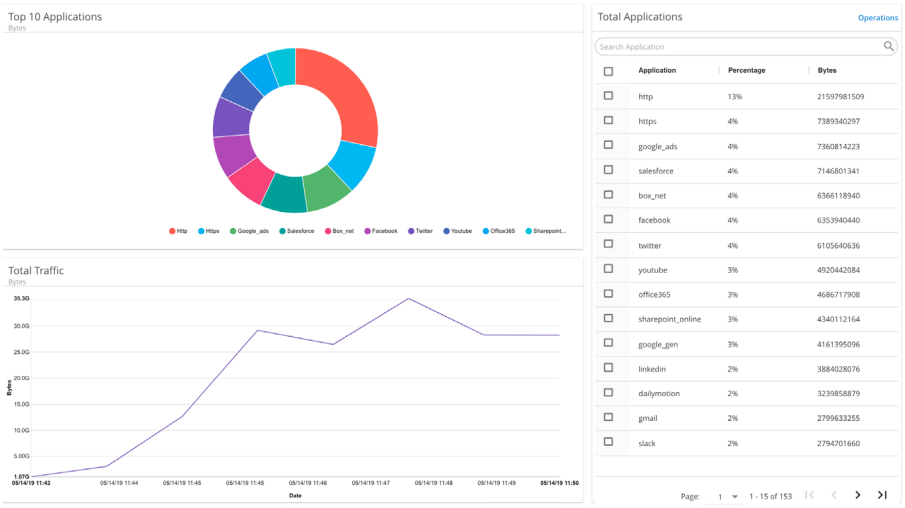
To address these problems, IT teams must take manual steps to identify applications based on network traffic, by either hardwiring ports to specific applications or by writing regular expressions to inspect traffic patterns and identify apps. Manual workarounds, however, bring their own challenges. Among 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.

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.

THE SOLUTION

Gigamon Application Intelligence is composed of three components:

- Application Visualization
- Application Filtering
- Application Metadata



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

Application Visualization

Most of 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 non-compliance 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 3,000 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 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

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, forensic solutions need to see all traffic. Web application firewalls need to see only web traffic. Secure email gateways care about email, attachments and embedded URLs.

With Application Filtering you can extract and precisely match an application's traffic with the right tool. The solution provides the ability to isolate the application, its components and protocols, and to direct that traffic through 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

Derives app behavior and details pertaining to flows, reduces false positives, identifies nefarious data extraction and accelerates threat detection through proactive, real-time monitoring versus reactive forensics.

Application Metadata provides summarized and context-aware L4–7 information about network packets. It supplies tools more than 7,000 attributes that highlight performance, customer experience and security, and appends to NetFlow and IPFIX records. These include:

- 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 ID
- IMAP and SMTP email-based communications with addresses
- Service identification: audio, video, chat and transfers for VoIP and messaging

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 Microsoft Windows updates or streaming media from Netflix or Apple, your tools can detect suspicious activities more quickly and operate much more efficiently. Through a simple drag-and-drop process via the 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, 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 Advanced threat protection (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.

For more information on GigaVUE Application Intelligence, please read the Application Filtering Product Brief and Application Metadata Intelligence data sheet. Learn more at www.gigamon.com/app-intel.

Gigamon®

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

11.19_02