Gigamon Visibility and Analytics Fabric

Test Drive Guide
Thank you for registering to test drive the Gigamon Visibility and Analytics Fabric™.

You will have access to our demo environment and be able to test drive two of our most popular GigaSMART® applications:

+ SSL/TLS Decryption
+ Application Intelligence

During the session you will see firsthand how you can automatically visualize applications running on your network, turn on decryption and send specific traffic flows to your monitoring tools.
Gigamon in Your Network

The Gigamon Visibility and Analytics Fabric serves as the visibility layer between your network infrastructure and your network monitoring and security tools. Gigamon helps ensure each tool receives all relevant traffic it was designed for, and nothing more.

BEFORE GIGAMON

Figure 1. Tools plugged directly into the network. Each tool receives raw packets and misses dropped packets from SPAN ports. Common functions, like de-duplication and decryption, are performed repeatedly by each tool.

AFTER GIGAMON

Figure 2. Simplified architecture. Tools are now plugged into Gigamon, which centrally processes traffic (decrypt, identify, optimize) and sends only relevant traffic to each tool.
**Demo Topology**

The topology for this demo consists of:

+ A single link that’s tapped between the edge firewall and the switch
+ Several inline tools: Web application firewall (WAF), intrusion prevention system (IPS), firewall and DDOS attack tool, each connected individually or in a group with load-sharing configuration
+ Two out-of-band tools, an intrusion detection system (IDS) and Splunk, connected to collect out-of-band traffic from Gigamon Application Intelligence

**Login**

Let’s start by logging into the GigaVUE-FM demo environment. Note that while you can go through the configuration workflows, you cannot apply the changes as this is a read-only demo.

+ Go to [https://demo.gigamon.com](https://demo.gigamon.com)
+ Using the credentials provided in the email you received, type in the username and password and then click **Log In**
Overview of GigaVUE-FM

The GigaVUE-FM fabric manager provides single-pane-of-glass visibility and control across your physical, virtual and cloud environments. You can view, manage and send specific traffic flows to both inline and out-of-band tools. GigaVUE-FM offers intent-based orchestration that also speeds up deployment of your network tools by enabling you to easily map traffic flows to tools using a simple guided process.

While this demo guide focuses on two capabilities — SSL/TLS Decryption and Application Intelligence — feel free to navigate around the GigaVUE-FM user interface and explore other features.
Gigamon SSL/TLS Decryption in Action

Before we walk through how Gigamon SSL/TLS Decryption works, let’s address why decryption is needed. SSL/TLS encryption protects data, but it is also a blind spot for network security and application monitoring tools. It is critically important that security tools can inspect encrypted traffic flows. More than 50 percent of new malware campaigns use various forms of encryption and obfuscation to conceal delivery and ongoing communication, including command-and-control and data infiltration.

You can choose to have each tool do the decryption, but this task is computationally intensive and can introduce network latency. And out-of-band application monitoring and security tools are unable to decrypt perfect forward secrecy (PFS) encryption, which makes up most of the encrypted network traffic today.

Gigamon offers a centralized approach to decrypting SSL/TLS — all the way up to TLS 1.3. With Gigamon, you can decrypt once and distribute to multiple tools, and still provide controls for privacy and compliance.

1. After logging in, select Traffic from the top navigation and then Inline Flows on the left-hand menu. Click on the host ID to see Inline Network.

2. Under Inline Network, click default_inline_net_1_3_4 to see how the inline traffic flows are set up for the demo network.
3. The following is a brief explanation of the upper two demo flow maps in the screenshot above. Note that any tool that appears next to or that you place next to the GS ssl-decrypt box will see decrypted traffic.

+ **Web-Traffic Map:** This flow map defines the rule to filter out all web port 80 and SSL port 443 traffic.
  - **GS ssl-decrypt app:** This is the GigaSMART SSL/TLS decryption application.
  - **OOB Copy from GS ssl-app:** This is an out-of-band tool connected to the port. It receives a copy of the decrypted traffic since it is next to the GS ssl-decrypt app.
  - **WAF-Group:** This is a tool group of two inline tools with load balancing.
  - **IPS Tool:** This is an individual tool that sees all web port 80/443 traffic. This tool will also see decrypted traffic.

+ **Collector Map:** This flow map defines how all remaining traffic will be forwarded to the tools.
  - **Firewall Group:** This is a tool group of two tools set up in a load-balancing configuration.
  - **DDOS Tool:** This is an individual tool set up to receive all traffic (except web traffic).

**Note:** Flow map changes cannot be made on this read-only demo. In a live implementation of GigaVUE-FM, setting up or changing flow maps is a simple drag-and-drop process using the Configuration Canvas.

4. You can click on each component to view more detail. Click on the **GS ssl-decrypt** box to see the SSL/TLS decryption options.
5. Close the pop-up. To see SSL statistics, click on the **Statistics** tab.

6. Click **More ...** at the bottom to see more detailed statistics. This will open a pop-up that shows session, monitor and certificate statistics.
Application Intelligence in Action

Now let's walk through how you can apply Gigamon Application Intelligence to your network. Application Intelligence consists of Application Filtering Intelligence (AFI), which provides application-level visibility along with control over network flows, and Application Metadata Intelligence, which delivers rich, contextual metadata to your monitoring tools.

Application Filtering Intelligence enables you to automatically identify over 3,000 common and proprietary applications. A primary use case for AFI is to visualize applications of interest together with the bandwidth they consume so you can direct specific application flows to the appropriate security and monitoring tools. With a granular app-aware view and flow control, you can offload irrelevant traffic, thereby significantly reducing scaling needs and improving tool effectiveness.

1. Select App Intelligence on the left-hand menu.

2. Click the ID number under Cluster ID.
3. On the Application Intelligence panel, you'll see a pie chart showing the top ten applications running on the network, total traffic by date/time and all the applications on your network with corresponding percentages of total traffic and volume.

4. You can search for a specific application by entering the name of the app (in this case, BitTorrent) in the search bar. Click the gear icon to view Bytes, Packets or Flows for that application.
5. Let’s start to filter out application traffic that you don’t need to send to certain tools for processing. To filter out applications, click **App-Intel** on the left-hand menu and select **Edit**.

The pop-up shows the settings for Application Intelligence.
6. Scroll down the pop-up panel until you see **Application Filtering**. You will see a list of tools and **App Editor** buttons that will allow you to select applications to be passed to each tool or dropped. Click **App Editor** next to **Pass Applications**.

7. View the apps that are passed to your tool (in this case, Splunk).
8. In the **Application Editor** next to Drop Applications, you can drop an individual app or a whole family of apps so this application traffic will not be sent to the tool.

![Application Editor](image)

**NOTE:** Because this demo is read-only, you will not be able to save your changes.

9. Application Intelligence also allows you to send application metadata rather than full packets to your tools, such as your SIEM. To see how this works, select **Application Metadata** and click **App Editor** next to **Application List**.

![Application Metadata](image)
10. Add a family or families of applications (in this case, audio-video and antivirus).

11. To see which application metadata attributes are available, select an application and click the expand arrow next to the application name (in this case, Facetime). Check **Select All** to export all attributes or select specific attributes to export by checking their box.
Next Step: Try Gigamon in Your Own Environment

This demonstration shows just a fraction of the ways you can use Gigamon solutions to your advantage. We’d be happy to show you more with a no-obligation proof of concept (PoC) at your location. To get started, go to gigamon.com/live-demo.