Optimize Your Network Across Layers With Gigamon Application Filtering Intelligence

KEY BENEFITS

- Filters lower-priority applications so NetOps, CloudOps, and SecOps teams can focus on critical applications
- Ensures high-volumes of North-South and East-West traffic don't overwhelm performance monitoring and security tools
- Improves network security by freeing up tool resources to protect a larger attack surface, including East-West traffic

Introduction

Much of the world now uses a hybrid working model, and that has transformed how you and your team support employees. You need to maintain network availability, performance, and great user experiences as network traffic has shifted from on-premises to hybrid cloud at a scale beyond what was planned. You also need to secure the increased attack surface and vulnerabilities this shift has created, all while doing more with less as revenues drop and IT budgets are reduced or frozen.

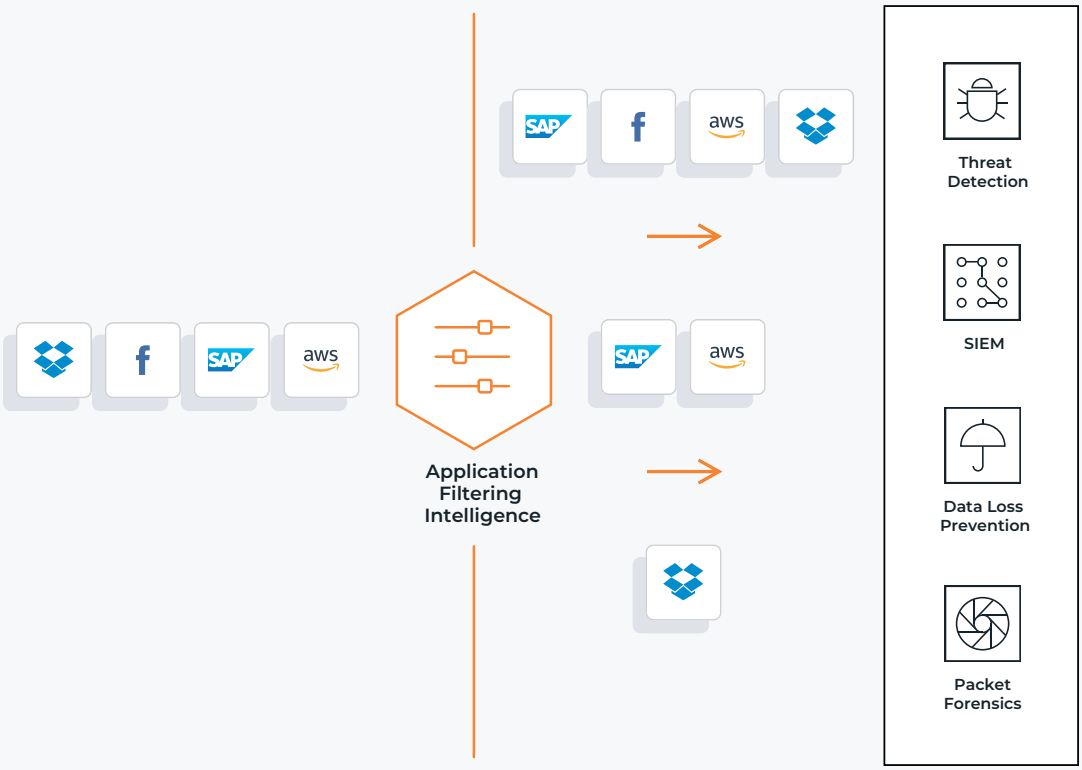

Figure 1. Application Filtering Intelligence helps you filter applications and send data to the right tools.

Security and analytics tools are a particular pain point: They are being overwhelmed, for example, by elevated flows of network traffic as packets boomerang through VPN connections. That can overwhelm available resources, which reduces performance and increases overall risk. But Gigamon Application Filtering Intelligence (AFI), a key component of Gigamon Application Intelligence, gives network operations (NetOps), cloud operations (CloudOps) and security operations (SecOps) teams Layer 7 visibility and control over applications, ensuring tools see only the packets or applications they need to inspect, helping you make the best use of your existing infrastructure.

AFI uses deep packet inspection (DPI) to identify applications and protocols from network packets and filter them as appropriate. Typical network traffic includes high-volume/low-risk traffic, such as video and social media streams or custom applications, that network and security tools don't need to process.

AFI classifies applications based on various attributes around traffic behavior and involves flow-based matching, bi-directional flow correlation, heuristics, and statistical analysis. This lets you accurately identify and filter traffic from over 4,000 off-the-shelf software applications as well as custom applications.

AFI provides this discovery process independent of encapsulation, port number, or encryption, so you can target the traffic you feed to your tools. With AFI, you can focus on high-risk, application-specific traffic, sending those packets to the right security tools for the best security posture. Once the applications generating network traffic are identified, Gigamon Flow Mapping® directs that traffic under the auspices of the GigaVUE-FM fabric manager. For more details, read the Application Filtering Intelligence data sheet.

By inspecting targeted network protocols and specific applications of interest and sending appropriate traffic to the right tools, you can achieve better ROIs by improving the performance-and-detection efficacy of your existing tools. You can maintain existing network availability, performance, and security in the face of increased traffic, without spending more on infrastructure or monitoring tools.

Use Cases

AFI allows you to create different sessions to monitor different sites. You can then select the applications to be filtered for monitoring at each site. Application Visualization provides distinct dashboards for each site. You can either use the same tools stack for monitoring all the traffic or use different tools to monitor different sites.

AFI also natively supports packet slicing. For instance, you could send all traffic to a network detection and response (NDR) tool but slice all SSL traffic.

Additionally, you can conserve storage, especially when required to store packets for network forensics. You can choose to retain only packet headers and discard payloads.

Focus on Relevant Flows to Optimize Security Tools

Some network tools focus exclusively on certain applications and protocols, so feeding them anything outside of a narrow protocol suite such as HTTP, email is unnecessary. If these tools spend processing power inspecting all network traffic, then most of the tools' resources are expended without yielding any additional threat detection. To optimize tool performance, therefore, it's best to refine traffic with a laser focus on specific applications or protocols and offload irrelevant traffic from expensive resources. For example, forwarding only OT/IoT/IoMT traffic to network/application monitoring tools.

Filter High-Volume and Low-Risk Traffic

Threat detection tools are primarily interested in suspicious traffic. To optimize tool performance and prevent traffic from exhausting limited tool capacity, it's best to not feed them high-volume/low-risk traffic. Some content can be deemed safe by design, such as high-bandwidth Netflix or Hulu streaming media and Windows updates. This content does not have, for instance, hidden command/control code, and it's from a known, secure source. IT needs to distinguish this from other content that is not safe, such as certain YouTube channels where the content could contain hidden malware. For example, do not send Netflix traffic to IDS.

Find and Stop Rogue Applications

As AFI identifies thousands of applications, discover known and unknown applications, including shadow IT applications running on the network. In the age of bring your own device (BYOD) and cloud-based SaaS services, such usage is common. While the primary focus is to filter this traffic and rely on security tools for protection, you can also use AFI to proactively find and eliminate unsanctioned applications, particularly those with known vulnerabilities. For example, detect known and unknown applications.

Identify Encrypted Applications Running on Nonstandard Ports

Applications normally are assigned to specific ports, and IT can to some degree identify and filter based on port. However, for many applications, this is not the case, especially when TLS/SSL is encrypted, running on nonstandard ports, and IT desires to filter out ports such as 443. AFI provides this ability.

Throttle Bandwidth by Application

Application Visualization provides not only the identification of numerous applications but also the amount of capacity they are drawing. The main dashboard shows the top ten applications by usage, as well as details on all other applications and traffic levels. IT can leverage this data to enforce bandwidth limits by application via rate-limiting or other methods. With users utilizing corporate resources for Facebook, Instagram, or other social networking sites or streaming media, these non-critical, personal-use-only applications can cause higher-priority traffic to suffer performance loss — particularly as a hybrid workforce has shifted network traffic from LANs to WANs. For example, rate-limit BitTorrent.

Prioritize and Forward Specific Traffic to Tools

Modern networks typically incorporate quality of service (QoS) methods to give priority to select traffic, but this is based on L2–L4. With AFI, you can forward specific applications to tools for monitoring.

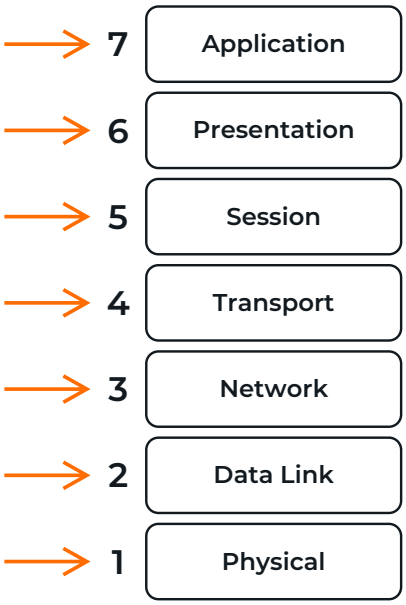

Figure 2. AFI helps you expand your QoS optimization to Layer 7 of the OSI model.

Identify and Filter Custom Applications

Large organizations typically run hundreds of custom applications that are often developed in-house for specific functions. With growing network traffic, these applications tend to outgrow the available hardware resources needed to support this expansion. To prevent future network disruptions, it's crucial to identify the exact resources these applications need.

Fulfill Most Stringent Compliance Requirements

Compliance makes monitoring custom applications essential since they could also be vulnerable to attacks. As these applications are not as dynamic as standard applications and their structure is well known, some IT departments use IP address ranges or port numbers to help identify them. That isn't ideal, though, because these in-house applications may use the same port; a better approach is to leverage AFI's DPI capabilities by defining signatures and searching for these regex patterns in the header or payload. Once found, they can be filtered out as needed. For example, identify in-house applications.

Identify Connections Using Nonstandard Ports

For communication protocols such as SSH, DNS, Telnet, and RDP, the ports are well known and normally used. If these connections are using different ports, this could indicate compromise or misconfiguration since it only occurs during manual intervention.

Protect Against Port Spoofing

With traditional client-server traffic, hackers can use port spoofing techniques where they send SSH traffic over port 443, which is used for SSL. If you cannot identify applications, this technique works, and traffic is improperly shown as SSL. AFI, in contrast, can see through this misdirection and properly list this traffic as SSH. For example, Remote Desktop on any port other than 3389.

Conclusion

Unlock the potential to uncover concealed threats within both incoming and outgoing encrypted traffic using the dynamic combination of the Gigamon Deep Observability Pipeline and GigaSMART. Through a single decryption process, empower seamless information sharing across all tools, effectively scaling and enhancing the efficiency of each one by eliminating the processor burden. The outcome is a suite of tools operating at the pinnacle of their performance, fully equipped to excel in their specialized role — the mitigation of malware.

Support and Services

Gigamon offers a range of support and maintenance services. For details regarding the Gigamon Limited Warranty and its Product Support and Software Maintenance Programs, visit gigamon.com/support-and-services/overview-and-benefits.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves 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 worldwide. To learn more, please visit gigamon.com.

Gigamon®

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

01.24_03