Optimize Your Network Across Layers With Gigamon Application Filtering Intelligence

Gigamon Application Filtering Intelligence at a Glance

Benefits

- Filters lower priority applications so NetOps and SecOps tools can focus on applications that matter most
- Ensures that the new wave of North-South traffic doesn't overwhelm performance monitoring and security tools
- Improves visibility into the increased attack surface that arises from the shift from LAN to WAN

Related Gigamon Products

- GigaSMART® applications
- GigaVUE-FM fabric manager

Much of the world is now using a hybrid working model, and that's transforming how you and your team support employees. You need to maintain network availability, performance and great user experiences as network traffic shifts from LANs to WANs on a scale you never planned for. 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 frozen.

Security and analytics tools are a particular pain point: They're being overwhelmed, for example, by a suddenly spiking flow 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) gives network and security operations (SecOps) teams visibility and control over applications, ensuring that tools see only the packets they need to inspect, helping you make best use of your existing infrastructure.

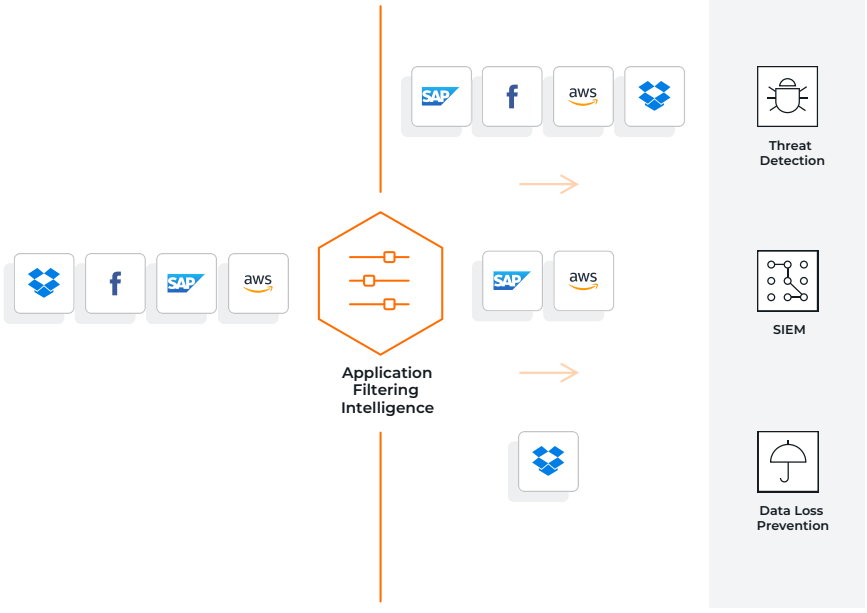

Figure 1. Application Filtering Intelligence helps you optimize your tool stack.

Deep Packet Inspection Is Key

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 3,500 off-the-shelf software applications, as well as from custom apps.

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 apps 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, you 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 tooling.

Use Cases: Targeted Solutions for Getting the Most from Your Network

To help you be more efficient and get the most out of this investment, Gigamon provides a set of validated designs that focus on common use cases across multiple industries. Gigamon Validated Designs (GVDs) are lab-tested solutions that cater to your network and security architects and administrators who want to gain more insights and learn how to deploy these solutions in your environments. The following use cases have been assessed and help you get the most out of AFI.

Focus on relevant flows to optimize security tools.

Some network tools focus exclusively on certain applications and protocols, and therefore feeding them anything outside of a narrow protocol suite (HTTP or email, for example) 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 upon specific applications or protocols and offload irrelevant traffic from expensive resources.

Filter high-volume and low-risk traffic.

Threat detection tools are primarily interested in suspicious traffic. To optimize tool performance and to prevent traffic from hogging 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.

Throttle bandwidth by app.

AFI provides not only the identification of numerous apps, but also the amount of capacity they are drawing. The main dashboard shows the top ten apps by usage,

as well as details on all other apps and traffic levels. IT can leverage this data to enforce bandwidth limits by application via rate-limiting or other methods. With users nefariously using corporate resources for Facebook, Instagram or other social networking sites or streaming media, these non-critical, personal-use-only apps can cause higher priority traffic to suffer performance loss— particularly as a home-based workforce shifts network traffic from LANs to WANs.

Find and stop rogue apps.

As AFI identifies thousands of applications, discover those shadow IT apps running on the network. In the age of bring your own device (BYOD) and cloud-based SaaS services, such usage is commonplace. 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 apps, particularly those with known vulnerabilities.

Prioritize the most critical traffic based on apps.

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 give traffic from specific apps precedence. Typically, these apps would involve things like e-commerce, outbound web-based servers or VoIP and would be elevated over things like CRM, email and internal streaming media use.

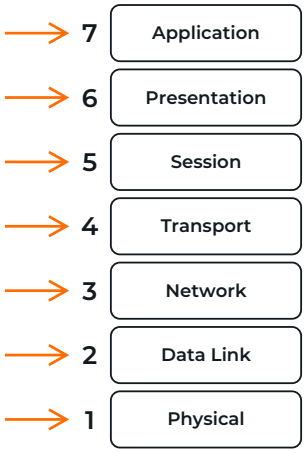

Figure 2. AFI helps you expand your QoS optimization to Layer 7 of the OSI model.

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.

Moreover, compliance makes monitoring custom applications essential since they could also be vulnerable to attacks. As these apps are not as dynamic as standard apps 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 apps 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.

Identify missing or misclassified traffic and direct it to proper tools.

This is a corollary to finding relevant flows. Network operations teams use various methods to properly route traffic. This AFI technique can identify improperly classified traffic or traffic not being directed to the right tools. AFI can also validate legacy routing methods to ensure accuracy, completeness and full visibility.

Identify encrypted apps running on nonstandard ports.

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

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, then this could indicate hackers are using are using them to bypass IT security controls.

Overcome 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.

We're Here to Help Navigate What's Next for Your Organization

Taken together, Gigamon Application Filtering Intelligence lets you better manage, monitor, and secure your infrastructure by leveraging Layer 7 visibility. And to better understand how to solve these ever-evolving use cases, please request a demo and view our on-demand webinar for more insights.

And in a larger sense as we manage through this time of unprecedented change, Gigamon can help your organization run fast and stay secure while optimizing costs. With a unified deep observability pipeline on all information-in-motion across your hybrid infrastructure, your organization can save time, save money and stay prepared for the new tomorrow, whatever it may bring.

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-andservices/overview-and-benefits.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables 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, nine 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

04.23_2