Application Filtering Intelligence

Application awareness to understand, manage, and secure your data in motion

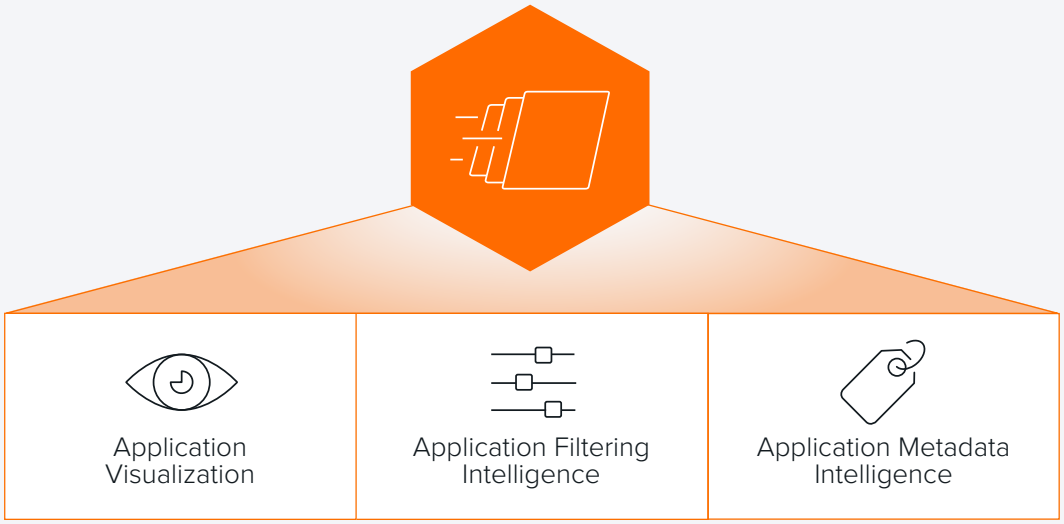

Figure 1. Application Filtering Intelligence is a key component of Application Intelligence.

Overview

Application Filtering Intelligence brings granular application awareness to your on-prem and cloud-based network and security operations centers by letting you automatically identify, select, and deliver only the application data that's most important to you and your tools.

Key Benefits

- **Focus on mission-critical business applications —** See which applications are running on your network and zero in on high-value, high-risk assets
- **Reduce manual work —** Accelerate investigation of business-critical risks with easier data isolation
- **Improve tool efficiency —** Lower processing and storage requirements by filtering irrelevant traffic
- **User-defined signatures —** Create signatures to identify and filter unknown applications on your network
- **Improve security —** Secure more of your network including encrypted and decrypted traffic (ICAP, etc.) and applications
- **Be ready for future needs —** Decrease the time and effort to capture the right application traffic for network, security, compliance, IT audit, and application teams
- **Strengthen compliance —** Filter out sensitive information from monitoring and recording systems

With the ever-increasing volume of network data, it's hard for IT teams and tools to focus on the most actionable activity and avoid wasting resources processing irrelevant traffic. We often inundate security, management, compliance, and monitoring tools with low-risk, low-value traffic, making them less effective and more difficult to scale. Additionally, false positives and alerts can overwhelm network operations (NetOps), cloud operations (CloudOps), and security operations (SecOps) teams, obscuring the root causes of network and application performance issues and the real threats buried in volumes of undifferentiated traffic.

Until now, it's been hard to isolate traffic by application type and specify whether it does or doesn't get inspected by tools. Visibility is siloed and filtering options often only go up to Layer 4 elements, forcing organizations to either pass all traffic through their tools or risk missing potential threats and issues.

However, having each tool (intrusion detection system (IDS), network performance management (NPM), network detection and response (NDR), network forensics, and so on) inspect packets to filter irrelevant traffic is inefficient and unnecessarily costly, as most tool pricing is based on traffic volume and processing load. While packet brokering can be used to reduce traffic, it requires programming knowledge to maintain complex rules and filters.

Although some systems provide a level of application identification, they are hard to use and only identify a limited number of applications. Furthermore, ongoing maintenance of rules and filters is needed since application behavior and identification change over time.

Gigamon Application Filtering Intelligence

Gigamon Application Filtering Intelligence brings application awareness to your on-prem, AWS, Azure, Google Cloud Platform, VMware, and Nutanix environments. It automatically extends Layer 7 visibility to identify more than 4,000 common business and network applications traversing the network and lets you select and deliver only high-value and high-risk data by applications, locations, and activity. Gigamon classifies applications into categories that are automatically updated as the landscape evolves. This allows your team to take actions on a "family" of applications versus setting policies on each individual application. Examples of application families include antivirus, audio/video, database, ERP, gaming, messenger, peer-to-peer, telephony, and webmail. With this approach, each tool is more efficient since it no longer needs to store and process large volumes of irrelevant traffic. NetOps can apply their existing tools across a larger area by prioritizing only core business applications and accelerate their investigation of network and application performance issues with easier data isolation.

SecOps teams can extend their current tools to a larger attack surface, securing more of their network and preventing sensitive information, such as personally identifiable information (PII), from being routed to monitoring and recording tools.

Application Filtering Intelligence improves an organization's security posture by:

- Decreasing alerts and false positives
- Ensuring compliance standards for sensitive data are met
- Identifying instances of shadow IT from users

With Application Filtering Intelligence, IT teams can focus on the data that matters most for their role and make better strategic decisions about network and application security, performance, and investment.

Often there are various unidentified or unknown applications across your network. User-defined application signatures allow you to define these unknown or unidentified applications through the GigaVUE-FM fabric manager UI or CLI. These applications are displayed using Application Visualization, and you can drop or pass packets based on user-defined application signatures.

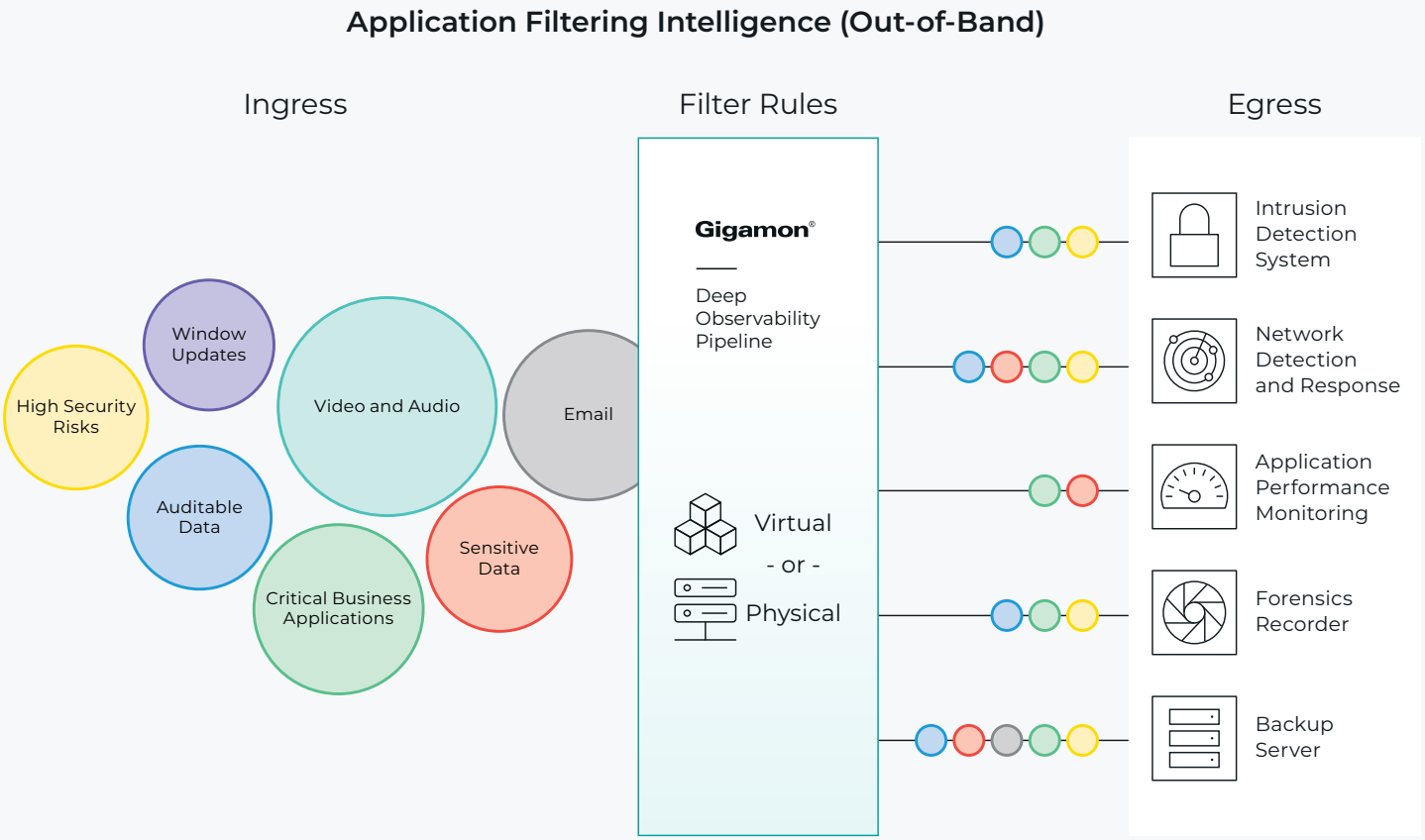

Figure 2. Application Filtering Intelligence (Out-of-Band).

Key Use Cases

Network traffic volumes in hybrid-cloud scenarios are increasing faster than tools and staff can keep up. Tools struggle to cope with the enormous throughput, and IT teams must be more selective in what they choose to analyze. Application Filtering Intelligence offers the flexibility to handle many use cases that require focused analysis of specific business applications and protocols:

- Filter in applications that may be used as attack vectors. For example, forward CRM, ERP, Microsoft Office, and BitTorrent search engine traffic to intrusion detection system (IDS), network performance management (NPM), network detection and response (NDR), and network forensics tools.
- Filter out high-volume, low-risk traffic such as YouTube and FaceTime to prevent tools, staff, and storage devices from being overwhelmed by excessive amounts of irrelevant data.
- Prevent Windows Update traffic from being forwarded to monitoring and security appliances. For example, Microsoft can overwhelm security and performance management systems with “Patch Tuesday” updates that are automatically distributed to Windows OS worldwide. Avoid redundant scanning, such as backup processes that contain known good data.
- Slice and forward encrypted traffic to Network Detection and Response or Network Forensics to monitor only the relevant packets or conserve the available storage space, respectively.

All the above filtering options can be performed on a specific application or a “family” of applications, such as ERP, streaming video, and P2P.

Ordering Information

Requirement	Description
GigaVUE-FM Fabric Manager	Single-pane-of-glass management and monitoring of all the physical and virtual nodes across your on-premises, virtual and public cloud deployments, with simplified workflows for traffic policy configuration, end-to-end topology visualization, hierarchical grouping based on location and customizable dashboards. Available as a hardware or a (software-only) virtual appliance, each GigaVUE-FM instance can manage hundreds of visibility nodes across multiple locations.
GigaVUE Intelligent Appliances: GigaVUE-HCT, GigaVUE-HC1, GigaVUE-HC1-Plus, or GigaVUE-HC3	GigaVUE Intelligent Appliances deliver consistent insight into data that travels across your network, including data centers and remote sites. With the Gigamon solution, you will have the coverage and control you need to safeguard critical network and business assets.
GigaVUE Cloud Suite for Public Cloud	This suite supports the Application Filtering Intelligence license to enable application visualization and filtering in AWS, Azure, and Google Cloud Platform public clouds. The second-generation V Series provides the processing engine to identify and selectively filter applications prior to distributing to the proper tools.
GigaVUE Cloud Suite for Private Cloud	This suite supports the Application Filtering Intelligence license to enable application visualization and filtering in Nutanix and VMware private clouds. The second-generation V Series, configured either as a local traffic acquisition VM or as a second phase aggregation and processing visibility node provides the processing engine to identify and selectively filter applications prior to distributing to the proper tools.

Support and Services

Gigamon offers a range of support and maintenance services. For details regarding 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, nine of the ten 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