Active Visibility for Multi-Tiered Security

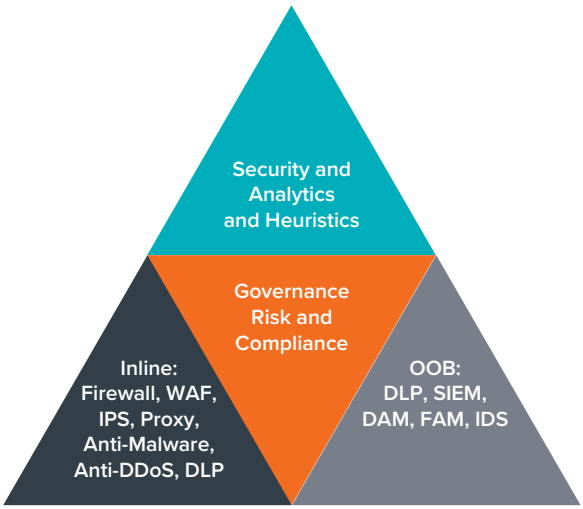
Introduction

Cyber threats are becoming ever more sophisticated and prevalent. Traditional edge and endpoint security approaches such as firewalls and anti-virus protection are not equipped to mitigate and manage modern security threats and risks on their own. Fortunately, security tools are also becoming more sophisticated. The latest generation firewalls, intrusion prevention and detection systems, malware protection appliances, data loss prevention devices, and other security tools have risen to tackle advanced, complex threats. The struggle information security officers often face is not which tools to deploy, but how to deploy them.

Overview of Multi-tiered Security

Multi-tiered security is about not relying on silver bullets and point solutions. It assumes that intruders will get in, malware will move vertically and horizontally through the network, and acknowledges that guarding the gate is not enough. It means taking a zero-trust stance and applying security monitoring and best practices throughout the network and for all traffic. Broadly speaking, the tiers are:

- Out-of-band Tools—These tools receive packets from SPAN and TAP ports and analyze the sessions and payloads for threats. The tools can look at traffic in great detail but only have a partial view of the traffic depending on where and how they are deployed. Examples include intrusion detection, data loss prevention, and malware detection systems.
- Inline Tools—Integrated into the production network, inline tools analyze packets as they pass through. These tools can immediately block suspicious traffic as it comes in rather than waiting for administrative action. Many such tools can operate either out-of-band or inline. Examples include intrusion protection systems, web application firewalls, and tools designed to defend against malware or denial of service attacks.
- Flow-based Analytics—Security analytics and heuristics use NetFlow and related technologies to go beyond signature identification to discover new threats and catch suspicious behaviors that may be invisible at the packet level.
- Regulatory Compliance—Rigorous regulatory standards imposed by PCI-DSS and other government mandates such as HIPAA, SOX, and the GLB Act make maintaining user privacy and compliance a challenge. It is not enough to be compliant—you must also be able to prove your compliance during an audit.



Gigamon provides an architecture that not only gives security tools the visibility they need, but also improves their performance and resiliency while helping to reduce troubleshooting times and accelerating the return on investment (ROI).

Security Challenges

Deploying a multi-tiered security platform can include the following challenges:

- SPAN port contention and bandwidth thresholds limit visibility
- Encrypted and cloud traffic cannot be monitored
- Inline security tools introduce points-of-failure for the network
- Security monitoring may not keep up with growing network speeds and the number of users and applications
- NetFlow generation may not be enabled or even available on the production switches and routers
- Network security and application performance can often conflict
- Budget constraints prevent the deployment of best-of-breed solutions

Steps to Active Visibility for Multi-tiered Security

Multi-tiered, zero-trust security requires a platform with the flexibility and scalability to adapt as IT infrastructure and threats evolve. The following steps identify the key elements to building end-to-end visibility that can help maximize the effectiveness of a multi-tiered security approach and illustrate how you can achieve this by leveraging the Gigamon Visibility and Analytics Fabric architecture.

1. **TAP all critical links**
2. **Connect links to the Gigamon Visibility and Analytics Fabric**
3. **Connect inline security tools**
4. **Connect out-of-band security tools**
5. **Leverage GigaSMART® Traffic and Application Intelligence**
6. **Add non-security tools to maximize ROI**

Step 1 – TAP All Critical Links

Security begins with visibility and visibility begins by tapping the network. By tapping multiple points in the network and supplementing with SPAN ports, you can gain visibility to one-hundred percent of the traffic. TAPs can be deployed at dozens or hundreds of points in the network with zero impact on network or application performance. Optical TAPs are completely passive, require no power, and do not require management. Even high-speed networks with 40Gb bidirectional links can be tapped and monitored; 1Gb and 10Gb copper connections can also be tapped with active, managed devices.

SPAN ports should be used only when necessary. SPAN ports are the lowest priority for production elements and traffic can be throttled down to a fraction of its full rate. This results in an inaccurate view to what is happening on the network and opens up the potential for threats to go unnoticed.

Security tools are often completely blind to threats within the virtual world. Tapping traffic flowing to, from, or between virtual machines is critical to ensuring security for the private or public cloud. Especially for inter-VM traffic, tapping only at the physical layer does not provide full coverage. GigaVUE-VM ties into the hypervisor and virtual switch to not only tap virtual traffic, but also select which traffic is forwarded to the Gigamon Visibility and Analytics Fabric.

Step 2 – Connect Links to the Gigamon Visibility and Analytics Fabric

Sitting between the IT infrastructure and the security and monitoring tools that need the access to data, the Gigamon Visibility and Analytics Fabric provides an extensible and elastic platform for technological and network evolution. The Visibility and Analyics Fabric consists of one or more visibility nodes that receive traffic from network TAPs and SPANs. Once within the fabric, the traffic can be forwarded to any out-of-band tools regardless of where they are physically connected. This provides a flexible platform upon which to build multi-tiered security. Even as network speeds accelerate, new tools can be added and existing tools can be upgraded seamlessly without network disruption. With the Gigamon Visibility and Analytics Fabric, you can aggregate, filter, replicate, and intelligently modify traffic to your security tools.

Gigamon uses its patented Flow Mapping® technology to selectively forward traffic to specific tools without dropping traffic that other tools need to analyze. After all the tool-specific traffic has been forwarded, a collector map will forward all the remaining traffic to a generic monitoring system or storage device, eliminating security blind spots.

Flow Mapping also works for inline tools, defining different traffic profiles for different tools such that each only has to process packets of the type of traffic they want. Traffic that is known to be secure can bypass the inline tools entirely and/or be sent in parallel to out-of-band tools such as an IDS. This application awareness not only improves efficiency, but also improves application performance for traffic that does not need inspection.

Advantages of the Visibility and Analytics Fabric include:

- Instant and pervasive visibility across the network, including physical to virtual environments
- Reduce expenses by simplifying operations and centralizing monitoring
- Eliminate contention among tools and IT departments for access to data
- Optimize security tool performance for greater ROI

Step 3 – Connect Inline Security Tools

Inline tools from simple firewalls to advanced Intrusion Prevention Systems (IPS) are vital to any multi-tiered security solution. Naturally, any inline deployment represents a potential point of failure, but these risks can be mitigated through bypass technology. Physical bypass protection refers to the ability to fail to wire, allowing network traffic to flow in the event of a power failure. Logical bypass protection is the ability to detect the failure of an inline tool and bypass the tool (uninspected) or bring down the network link to allow failover to a redundant path. Bidirectional heartbeat packets are inserted into the traffic stream to verify continued tool health. The bypass action is taken if the heartbeat is blocked or delayed or if the link is lost to the inline tool.

When monitoring networks with redundant paths, inline tools can be shared between the paths or deployed independently. Network link state propagation ensures that downstream or upstream link state can be translated across the inline bypass and network failover can occur.

Inline tools also represent a potential network bottleneck. Scaling inline inspection requires distributing traffic across multiple inline tools so that they share the load and can handle higher network speeds. When a tool goes down, the traffic can be redistributed to the remaining tools providing continued traffic inspection. Alternatively, a standby tool can be used for N+1 redundancy.

Different inline tools can be sent different types of traffic, allowing tools to be optimized for specific applications. Trusted traffic can bypass the inline tool entirely, minimizing latency and improving performance. Inline tools that need to inspect the same traffic can be configured in a serial fashion. In the event that one tool goes down, traffic can be bypassed to the next tool in series. Thus, multiple points of failure are consolidated and protected, making the network more secure and more robust.

Multiple network links, whether part of a link aggregated group or independent segments, can be aggregated and protected by the same tools while maintaining data path integrity and without any cross-traffic. This optimizes usage of inline tool investment and maximizes security for lower-speed links.

In order to be more responsive to detected threats, many out-of-band security tools which used to passively monitor traffic are moving to inline deployments. It is often useful to first install, configure, and optimize a tool out-of-band before bringing it inline. This can be done simply with a software setting rather than having to rewire and reconfigure.

Because the inline tools are not connected directly to the production network, tools can be added, upgraded, or removed with little to no disruption of production traffic. Alerts sent from the Gigamon Visibility and Analytics Fabric when a bypass action is taken allows for timely and orderly maintenance rather than triggering an emergency escalation.

Step 4 – Connect Out-of-Band Security Tools

The majority of security tools operate out-of-band, passively monitoring the network for threats and sending alerts when action is required. Multi-tiered security requires that security tools have access to all the traffic though the Visibility and Analytics Fabric. Malicious payloads that get past sentries at the perimeter can be detected in the core or when they move to different hosts in an effort to conceal their location.

Tools can selectively choose which traffic to monitor and ignore the rest, but simply making that choice uses up CPU cycles. A security tool that specializes in monitoring emails for threats, for example, does not need to see any non-email traffic. At the same time, tools geared towards web applications or database monitoring will want to see that traffic but not emails.

Flow Mapping forwards specific traffic to one or more tools based on user-defined map rules. Out-of-band tools can also supplement inline tools by inspecting a copy of the traffic sent to, or received from, the inline tools. Intrusion detection can take place in parallel with intrusion prevention. In addition, out-of-band traffic can be distributed across multiple out-of-band tools to share the load and achieve full security visibility

Step 5 – Leverage GigaSMART® Traffic and Application Intelligence

GigaSMART technology extends the intelligence and value of the Gigamon Visibility and Analytics Fabric architecture by expanding visibility, generating NetFlow data, improving tool performance, and protecting privacy while easing regulatory compliance. Any traffic bound for out-of-band monitoring tools can benefit from GigaSMART intelligence regardless of where it entered the Visibility and Analytics Fabric.

- TLS/SSL Decryption—Encrypted traffic can be a sizable portion of the traffic on the network, yet most tools are either unable to decrypt and monitor encrypted traffic or take a severe throughput penalty in doing so. Furthermore, malware can hide its activities within encrypted sessions. GigaSMART has the power to decrypt packets and send clear traffic to out-of-band monitoring tools.
- Header Stripping—Traffic encapsulated in protocols such as VXLAN or Cisco FabricPath can vex monitoring tools or use precious processing resources. GigaSMART can strip off those headers before sending the packets to the tools.
- Tunneling—Security tools are often too costly to deploy at remote sites, leaving them vulnerable to attacks or data loss. GigaSMART can tunnel traffic from remote sites back to the tools in the main data center where it can be inspected.
- NetFlow Generation—GigaSMART can offload NetFlow generation from the production network and send the data to multiple collectors. It does this without traffic sampling so flow-based security tools get the most complete and clear picture possible.
- De-duplication—Duplicate packets waste resources and processing power. By removing duplicates from the traffic stream before sending them to the tools, GigaSMART improves the performance and scalability of security monitoring.

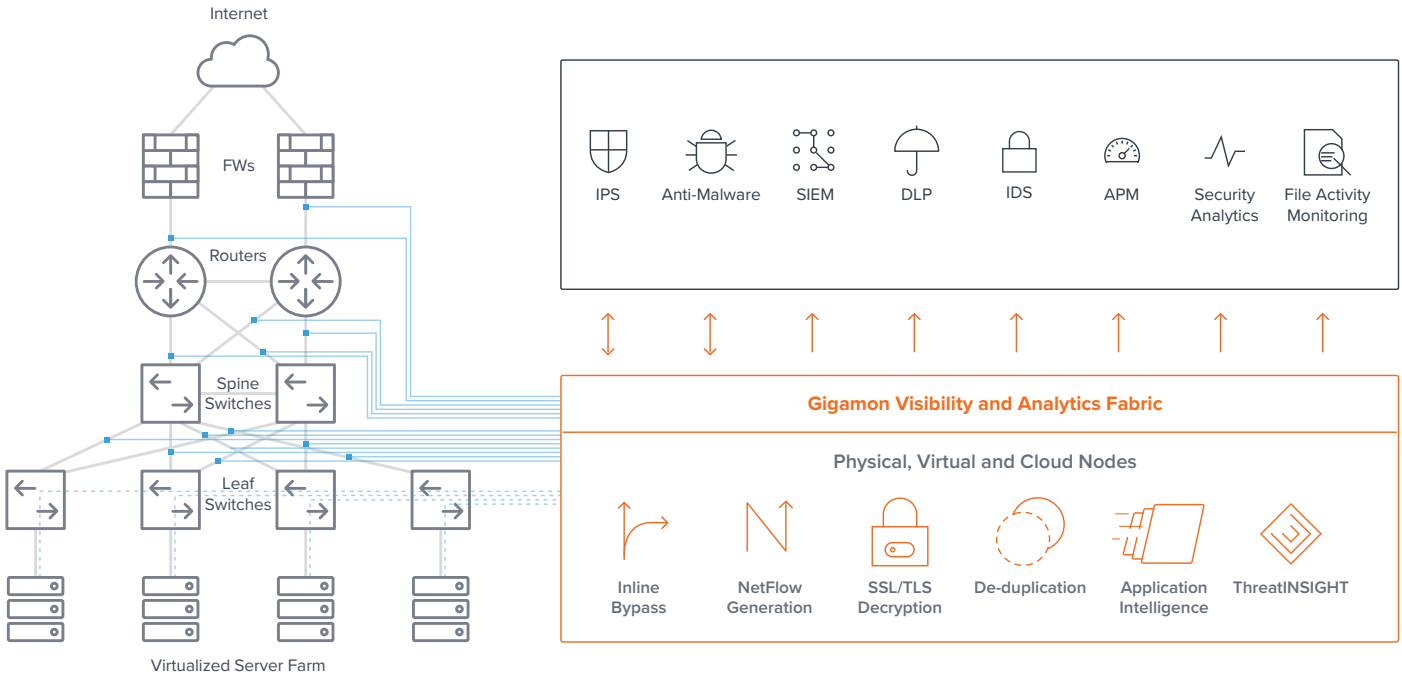


Figure 1: Multi-tiered security supported by he Gigamon Visibility and Analytics Fabric

- Load Balancing—Distributing traffic to multiple tools without GigaSMART maintains sessions, but does not always result in an even balance of traffic across tools. GigaSMART load balancing can take bandwidth, connections, and weighting into account.
- Application Intelligence—GigaSMART provides traffic forwarding decisions based on inner and outer packet headers as well as Layer 7 and payload data. This allows security tools to focus on specific applications even if they are using the same IP addresses and TCP ports.
- Advanced Packet Slicing and Masking—Private and sensitive information contained within packets can be a regulatory headache. By removing that data before sending packets to the tools, GigaSMART removes worries over data storage and compliance audits.

These applications can be combined and/or applied to different traffic profiles to maximize security coverage. For example, TLS traffic can be decrypted and then masked to keep private data secure, or NetFlow can be generated from traffic before or after encapsulation headers have been removed.

Step 6 – Add Non-Security Tools to Maximize ROI

Once in place, the Visibility and Analytics Fabric can also provide traffic to non-security tools, including application and network performance, user experience, and business services monitoring. Because traffic can be replicated to multiple tools, security, and non-security monitoring can inspect the same packets without having to contend for the same SPAN ports. Non-security tools can be added, removed, and upgraded without impacting security monitoring or leaving the network vulnerable. These tools also benefit from expanded visibility across the network, into the cloud, and within encrypted sessions and encapsulated packets. Providing visibility to multiple business units and improving tool performance while detecting and mitigating more threats can provide an immediate return on investment.

Summary

The changing threat landscape and evolving network infrastructure are forcing organizations to fundamentally rethink their approach to security in order to keep advanced threats at bay. Security teams are turning to multi-tiered deployments, leveraging the latest threat intelligence tools to protect their network. However, these tools are only as effective as the information they see. The ability to scrutinize through the deluge of Big Data from across the network in real time is vital to identifying and mitigating today's and tomorrow's threats.

Gigamon's Visibility and Analytics Fabric offers a comprehensive and sophisticated security services delivery platform. It provides scalability while improving resiliency, simplifying management, and enabling the deployment of best-of-breed solutions. Gigamon works with security tools to increase their field of vision, improve their performance, support resiliency, reduce troubleshooting times, and accelerate return on investment. The Gigamon Visibility and Analytics Fabric provides the platform for end-to-end visibility coupled with traffic intelligence that is needed to efficiently manage risks and address threats in this ever-evolving threat and network environment.

About Gigamon

Gigamon is the first company to deliver unified network visibility and analytics on all data-in-transit, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation. In short, we enable you to run fast, stay secure and innovate. Gigamon has been awarded over 75 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations, including 80 percent of the Fortune 100. Headquartered in Silicon Valley, Gigamon operates globally. For the full story on how Gigamon can help you, please visit www.gigamon.com.