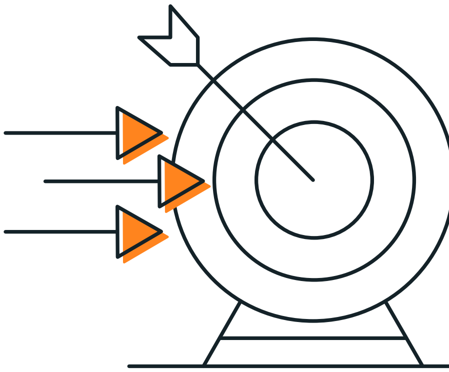
Stop Threats with Speed, Efficacy and Accuracy with Gigamon and ThreatWarrior



THE CHALLENGE

Organizations must have visibility and insights across on-premises, cloud, and hybrid environments to effectively secure their increasingly complex networks. Security teams are responsible for protecting everything from traditional devices to unmanaged entities, industrial control systems and more. Additionally, false positives and high signal-to-noise ratios eat up security teams' time and resources and delay threat detection.

THE SOLUTION

The Gigamon Visibility and Analytics Fabric™ (VAF) and ThreatWarrior™ work together to deliver visibility and insights into your entire IT environment to quickly and efficiently stop threats.

JOINT SOLUTION BENEFITS

- Analyze network traffic in real time and stop active threats across on-premises, cloud, and hybrid environments
- Gain visibility into all network activity through continuous deep packet inspection
- Learn the behavior of everything connected to the network and gain contextual insight
- Identify behavior between entities such as compute instances and Kubernetes clusters
- Save your security team time and resources

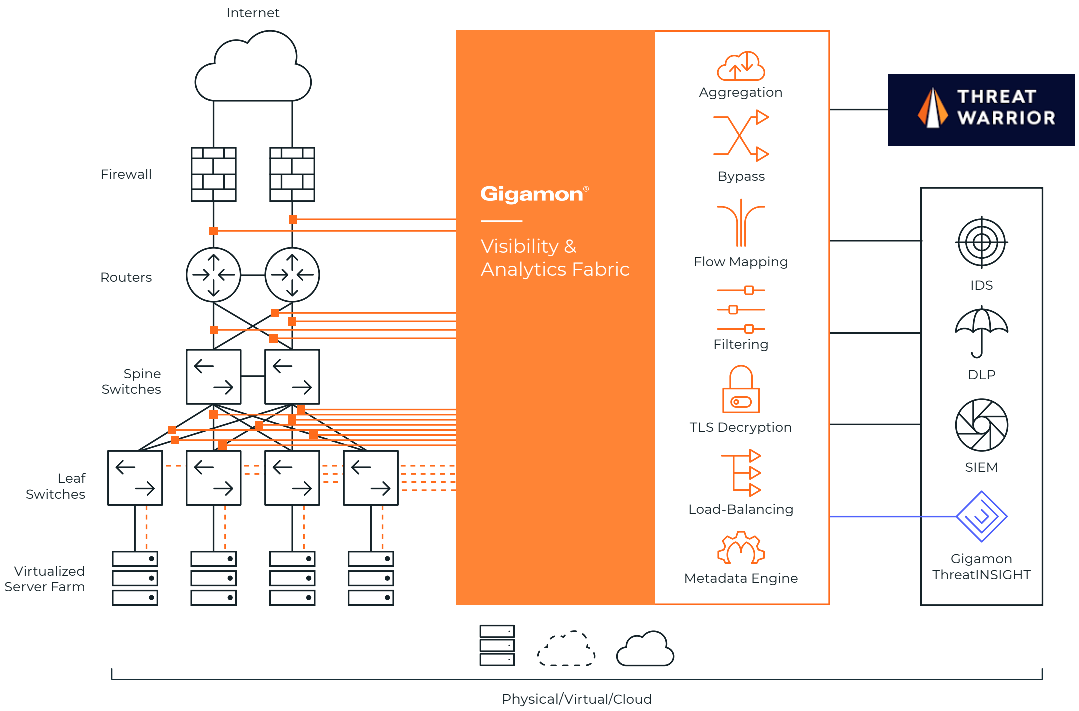
Introduction

ThreatWarrior, the first SaaS-based network threat intelligence platform that combines unsupervised neural networks, deep packet inspection, behavior monitoring, analytics and automated response in a single solution, helps you see and understand the threat environment. The platform utilizes multiple engines that analyze and correlate relevant information to deliver contextual intelligence that helps reduce false positives and improve the signal-to-noise ratio. The VAF simplifies the acquisition and aggregation, filtering and deduplication, and decryption of network packets before forwarding to ThreatWarrior for threat inspection.

The Gigamon + ThreatWarrior Joint Solution

Key VAF features that enhance ThreatWarrior include:

- **Easy access to traffic from physical, virtual and cloud networks:** The VAF enables traffic from across the network to be managed and delivered to ThreatWarrior and other tools efficiently and in the format they need.
- **Aggregation:** The Gigamon VAF selectively aggregates all traffic to be monitored and analyzed together, reducing blind spots and increasing the likelihood of spotting suspicious behavior and covering the issue of asymmetric routing and link aggregation groups. By tagging the traffic, the VAF ensures the source of traffic can be identified.
- **Traffic filtering:** The VAF can be configured to only send relevant traffic — or relevant sessions — to ThreatWarrior, optimizing the delivery of critical information.



+ **Load balancing to spread traffic across multiple devices:** When traffic flows are too large for a single ThreatWarrior sensor, the VAF can split the flow across multiple ThreatWarrior sensors, while ensuring sessions are kept together. Additionally, ThreatWarrior numbers can be incrementally grown by adding new instances.

+ **SSL decryption:** The VAF decrypts SSL/TLS encrypted traffic (including TLS 1.3) for inspection by the ThreatWarrior platform and any other.

+ **Deduplication:** Pervasive visibility requires tapping or mirroring traffic from multiple points in the network, which in turn, means tools may see the same packet more than once. To avoid the unnecessary packet-processing overhead on the ThreatWarrior platform, the VAF removes duplicates before they consume resources.

For more information on Gigamon and ThreatWarrior, visit: www.gigamon.com and threatwarrior.com.

Gigamon®

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