Joint Solution Brief

Gigamon and Interset Use Behavioral Analytics, Machine Learning, and Big Data to Pinpoint Real Threats in Real Time

The Challenge

One of the greatest challenges security analysts face is finding a security platform that's fast, data-hungry, fine-tuned, and capable of providing the actionable intelligence required to surface and remediate insider or cyber-borne threats.

Integrated Solution

Integrated with the Gigamon® GigaSECURE® Security Delivery Platform, the Interset Security Analytics Platform brings machine learning to threat detection, combining unsampled metadata with user, device, and file information to uncover cyber threats.

Joint Solution Benefits

- Interset leverages the GigaSECURE platform's automatic traffic load balancing and aggregation functionality to reduce bottlenecking and port oversubscription
- The GigaSECURE Security Delivery Platform accelerates processing throughput by effectively filtering and distributing relevant traffic from across the network to the Interset Security Analytics Platform
- The GigaSECURE platform generates and sends high-fidelity metadata to the Interset solution, which then applies machine learning capabilities to expose trends that pose potential hazards

Introduction

Threat detection is only half the problem. An unresolved threat without mitigation remains a menace.

Together with the Gigamon GigaSECURE Security Delivery Platform, the Interset Security Analytics Platform addresses the discovery/resolution issue by offering security analysts a new and different way to unearth and remediate security threats across the network.

By connecting the best of open-source, big-data technology with a highly-extensible, machine-learning analytics engine, the highly-scalable Interset platform can ingest massive amounts of data and correlate events with network activity to reveal the who, what, where, and when behind sophisticated breaches.

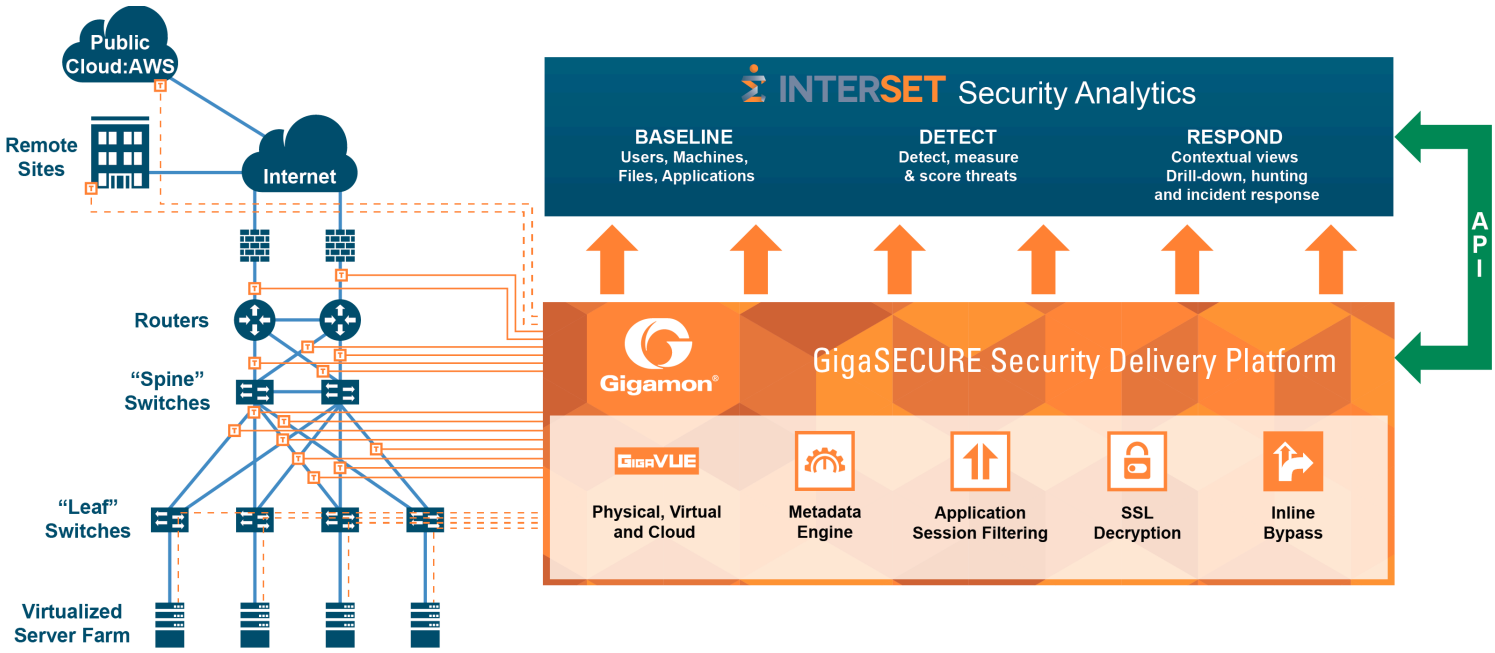
The Gigamon and Interset Joint Solution

With threat detection, context is key—especially in more sophisticated attacks. With proactive threat-hunting, analysts need to be able to query across specific data sources and link security events in the context of users, machines, applications, and files. Using the joint Gigamon and Interset solution, they can do this and more.

By unlocking the power of metadata, user and entity behavioral analytics, machine learning, and Big Data, the Interset Security Analytics Platform examines normally unrelated pieces of data to identify suspected malware and expose potentially hazardous trends. Interset offers highly intelligent, accurate, and early insider threat detection. And with far fewer false positives and much less noise, it helps security analysts validate incidents and create a prioritized list of what needs to be investigated first and why.

Key GigaSECURE Security Delivery Platform features that augment the value of Interset technology deployments include:

Easy access to traffic from physical, virtual and cloud networks: The GigaSECURE platform manages and delivers all network traffic—in the format required—to the Interset platform. To monitor East-West data center traffic and public cloud workloads, Gigamon taps virtual traffic and accesses and incorporates it into the GigaSECURE platform for delivery to Interset, helping to ensure that all traffic can be monitored and analyzed together, avoiding blind spots, and increasing the likelihood of spotting suspicious behavior.



Load balancing to spread traffic across multiple devices: When traffic flows are larger than a single tool can handle, the GigaSECURE platform can be used to split the flow across multiple tools, while sessions are kept together and tool numbers can be incrementally grown by adding new devices to those already connected.

De-duplication: Pervasive visibility requires tapping or copying traffic from multiple points in the network, which, in turn, means tools may see the same packet more than once. To avoid unnecessary packet processing overhead on the Interset platform, the GigaSECURE Security Delivery Platform has a highly effective de-duplication engine that removes duplicates before they consume resources and helps balance monitoring coverage.

Filtering traffic to only send relevant traffic: The GigaSECURE platform can be configured to send only relevant traffic or sessions to the Interset solution to help ensure that it only analyzes traffic that provides security value.

Metadata generation: The Interset Security Analytics Platform is able to surface threats such as lateral movement (East-West) and host infections (North-South) by applying machine learning to the unsampled, enhanced metadata (e.g., DNS queries, HTTP response codes) that is generated by the GigaSECURE Metadata Engine in NetFlow or IPFIX format from any selected traffic stream.

Learn More

For more information on Interset and Gigamon solutions, contact:

INTERSET
www.interset.com

Gigamon®
www.gigamon.com

3219-01 04/17

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