Joint Solution Brief

Dive Deeper into Advanced Threats with Cyphort and Gigamon GigaSECURE Security Delivery Platform

The Challenge

As organizations start to deploy advanced threat detection and mitigation solutions to address the ever-changing threat landscape, scalability and robustness of deployment becomes paramount. Advanced threat detection tools depend on continuously monitoring network activity and requires port mirroring technologies to reliably copy traffic for analysis. This can put a strain on an organization's already limited SPAN/TAP ports and limits their visibility and scalability. Additionally, the aggregation of relevant traffic can become critical for the correlation and detection of threats and their lateral spread.

Integrated Solution

Gigamon's GigaSECURE® Security Delivery Platform and Cyphort's Adaptive Detection Fabric provide an intelligent software security layer that discovers, analyzes, and contains advanced threats targeting your network across web and email. Cyphort's SmartCore engine is a multi-stage analysis process that applies advanced machine learning and behavioral analysis to find previously unknown threats.

Joint Solution Benefits

- Uses broad and deep visibility across physical, virtual, and cloud network traffic flows to augment Cyphort's Adaptive Detection Fabric's ability to detect and respond to advanced threats
- The GigaSECURE platform de-duplicates and filters traffic gathered from multiple collection points and distributes traffic to Cyphort
- The GigaSECURE platform's automatic traffic load distribution and aggregation functionality optimizes traffic for Cyphort
- The GigaSECURE platform decrypts SSL traffic for increased visibility

Introduction

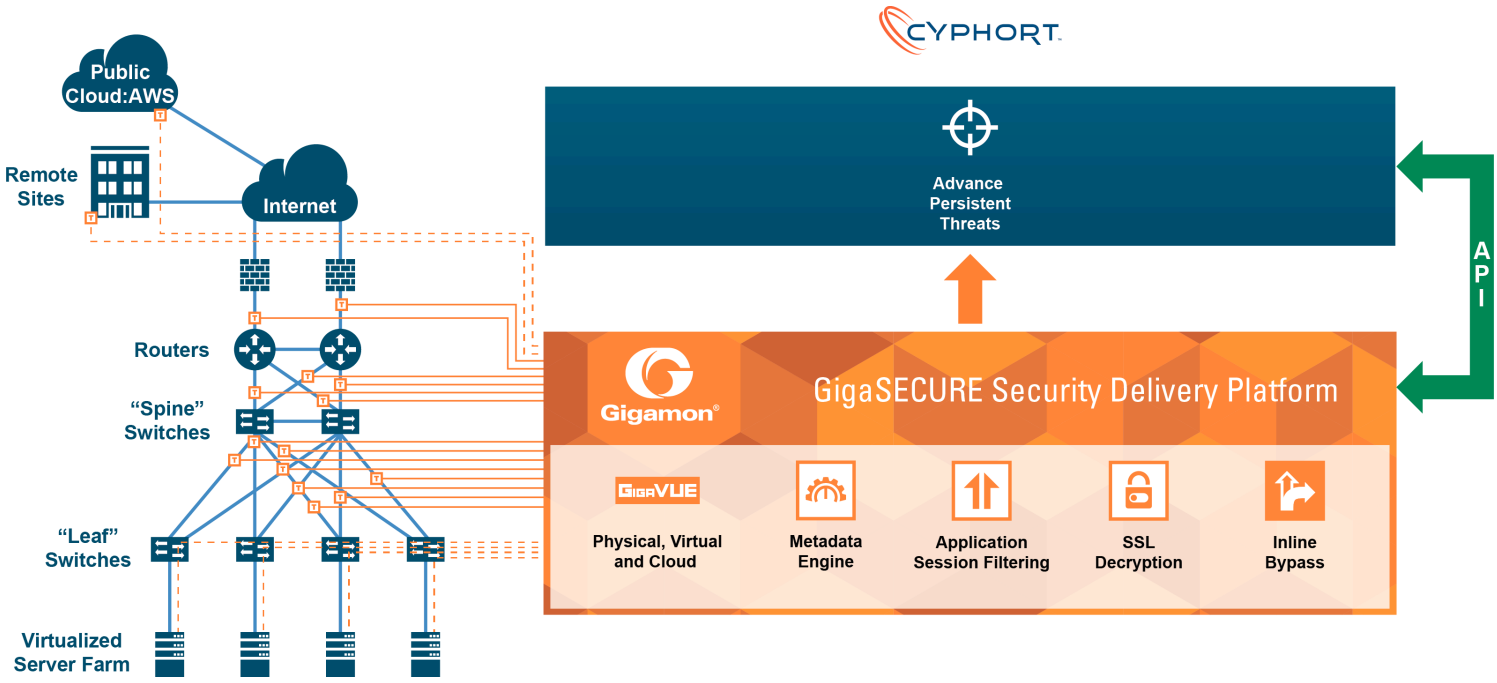
Visibility and detection are critical requirements for every organization's cyber security. Both of these capabilities are delivered through the strategic partnership between Cyphort and Gigamon. The companies have collaborated to create a solution that provides correlated visibility and threat detection for advanced attacks that bypass the first line of security defense (e.g., in-line devices such as firewalls, secure web gateways, etc.). Offering one of the most flexible deployment options coupled with robust performance, the combination of the Cyphort Adaptive Detection Fabric and the Gigamon GigaSECURE Security Delivery Platform helps ensure traffic is analyzed and threats are detected, even when spread across different network locations or public clouds. This helps enable security administrators to quickly detect and prioritize remediation before data is stolen or malware spreads inside the network.

The GigaSECURE platform delivers pervasive and dynamic traffic visibility from across the physical and virtual network environments to centralized tools that manage, analyze, and secure the network. This approach can extend the network reach of the tools to significantly improve return on investment, allow organizations to more efficiently manage and secure their network, and quickly evolve and scale as network needs change.

The Gigamon and Cyphort Joint Solution

Gigamon's GigaSECURE Security Delivery Platfom and Cyphort Adaptive Detection Fabric provide insight into the network for Cyphort to process comprehensive analysis and protection. Deployed out-of-band, the visibility node aggregates and forwards a copy only of the relevant production traffic, based on Gigamon's user-defined Flow Mapping® rules, to Cyphort. Gigamon's GigaSMART® processing engine can also provide deeper traffic intelligence, providing Layer 2-Layer 7 filtering and removal of duplicates, allowing Cyphort's SmartCore to inspect exactly the right traffic and perform at optimum efficiency.

Using Gigamon's GigaStream™ technology, incoming traffic flows are distributed across multiple Cyphort collectors. This parallel processing allows traffic analysis to scale and grow with network speeds and traffic loads. It also provides for optimal device performance and longevity.



Key GigaSECURE Security Delivery Platform features that augment the value of Cyphort include:

Easy access to traffic from physical, virtual and cloud networks: The GigaSECURE Security Delivery Platform manages and delivers network traffic—in the format required—to Cyphort Adaptive Detection Fabric. To monitor east-west data center traffic, and public cloud workloads, Gigamon taps virtual traffic and access and incorporates it into the GigaSECURE platform for delivery to Cyphort Adaptive Detection Fabric, so that traffic is analyzed and threats are detected quickly.

Filtering traffic to only send relevant traffic: The GigaSECURE platform can be configured to send only relevant traffic or sessions to Cyphort Adaptive Detection Fabric so it only analyzes traffic that provides security value.

Aggregation to minimize tool port use: Where links have low traffic volumes, the GigaSECURE Security Delivery Platform can aggregate these together before sending them to Cyphort Adaptive Detection Fabric to minimize the number of ports needed. By tagging the traffic, the GigaSECURE platform provides the identification of the traffic source.

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 Cyphort Adaptive Detection Fabric, the GigaSECURE platform has a highly effective de-duplication engine that removes duplicates before they consume resources and helps balance monitoring coverage.

SSL decryption: Real-time SSL decryption integration increases traffic visibility for Cyphort, broadening its scope for analysis and inspection of malicious activity.

Learn More

For more information on the Cyphort and Gigamon solution, contact:

CYPHORT
www.cyphort.com

Gigamon®
www.gigamon.com

3141-02 02/17

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