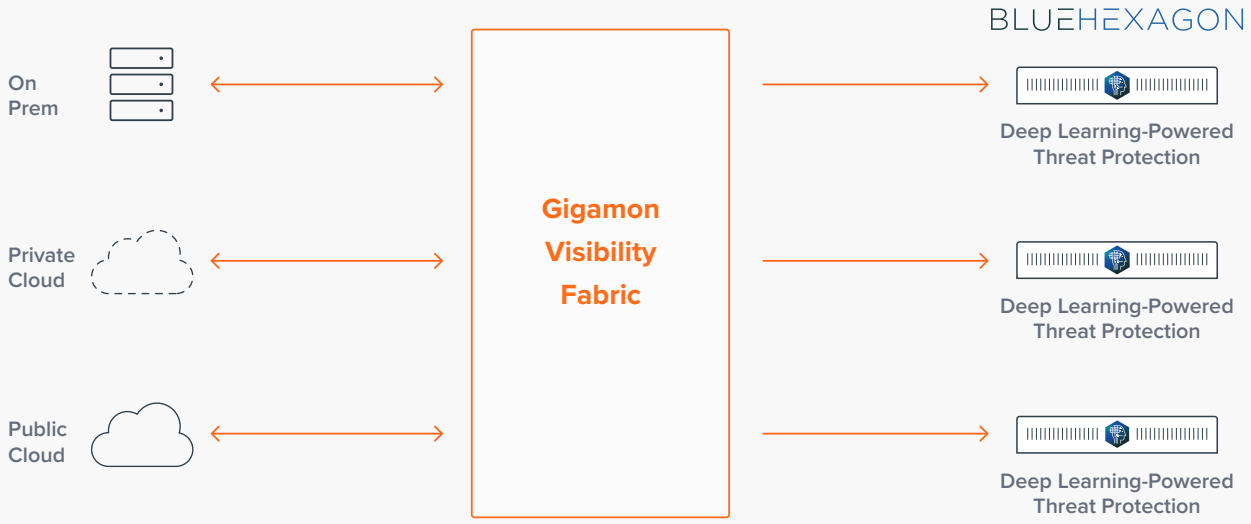
Gigamon and Blue Hexagon

Inspect Encrypted Traffic and Prevent Attacks With Blue Hexagon Deep Learning-Powered Threat Protection



Gigamon Visibility Fabric™, combined with GigaSMART® modules, selectively decrypts specific traffic and sends it to Blue Hexagon for inspection.

CHALLENGE

Hackers are increasingly using encryption to obfuscate malicious content and bypass security controls. More and more internet and email traffic is now encrypted. Most firewall and threat protection solutions, however, are not designed to handle decryption, nor can they scale for multi-gigabit networks.

SOLUTION

Blue Hexagon, the deep learning-based network threat protection platform, uses a proprietary neural network architecture to inspect the complete network traffic flow — including payloads, headers, C2 and URLs — to deliver a threat verdict in less than a second.

Together, the Blue Hexagon deep learning-based network threat protection integrates with the Gigamon Visibility Fabric to inspect encrypted traffic for known and unknown threats at multi-gigabit speeds.

THE GIGAMON AND BLUE HEXAGON JOINT SOLUTION

Traffic filtering: The Visibility Fabric can be configured to send only relevant traffic — or relevant sessions — to Blue Hexagon.

Aggregation to minimize port tool use: Where links have low traffic volumes, the Visibility Fabric can aggregate these together to minimize the number of ports.

SSL decryption: The Visibility Fabric decrypts SSL encrypted traffic and sends it to Blue Hexagon for deep inspection and deep learning analysis.

Easier control of asymmetric routing to help ensure session information is kept together: The Visibility Fabric provides an intelligent and efficient way to help ensure that Blue Hexagon inspection is supported in these architectures.

De-duplication: To avoid the unnecessary packet-processing overhead, the Visibility Fabric removes duplicates before forwarding to Blue Hexagon.

PRIMARY GIGAMON AND BLUE HEXAGON FEATURES

Neural Net Designed for Efficacy:

- The HexNet™ architecture has been designed to detect threats in less than a second.

Real-time Deep Learning Inspection for Payload and Headers:

- Inspection of the complete network flows delivers higher efficacy and perspective on mal-intent.

Real-time Classification:

- Every threat detected is automatically classified, and threat family information and indicators of compromise are provided for deeper analysis.

Dashboard and Kill Chain Visualizer:

- Visibility into infected hosts including communication between hosts, and external communications to malicious domains.

About Gigamon

Gigamon® is the company leading the convergence of network and security operations to help organizations reduce complexity and increase efficiency of their security stack. The Company's Visibility Platform is a next generation network packet broker that helps customers make threats more visible cloud, hybrid and on-prem environments, deploy resources faster and maximize the performance of their security tools.

Learn more at: www.gigamon.com

About Blue Hexagon

Blue Hexagon is a deep learning innovator focused on protecting organizations from cyberthreats. The company's real-time, deep learning platform is proven to detect known and unknown threats with speed, efficacy, and coverage that set a new standard for cyber defense.

Find out more at: bluehexagon.ai/

Gigamon®

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

08.19_01