BLUEHEXAGON

Gigamon®

Blue Hexagon and Gigamon
Partner Solutions Brief

Highlights

Only Blue Hexagon's deep learning-based approach to malware protection can prevent attacks from getting through--in less than a second. When combined with Gigamon, the appropriate network traffic including encrypted traffic, can be directed to Blue Hexagon for optimal, seamless inspection.

For channel partners, this integration provides opportunities to cross-sell the joint solution and position new use cases such as cloud security.

Note that Blue Hexagon replaces signature and sandbox-based detection. The platform addresses perimeter malware and threat defense by inspecting both payloads and headers. This complements Gigamon ThreatINSIGHTS network detection and response that arms security analysts, incident responders and forensics teams with network insights deeper in the kill chain.

Overview

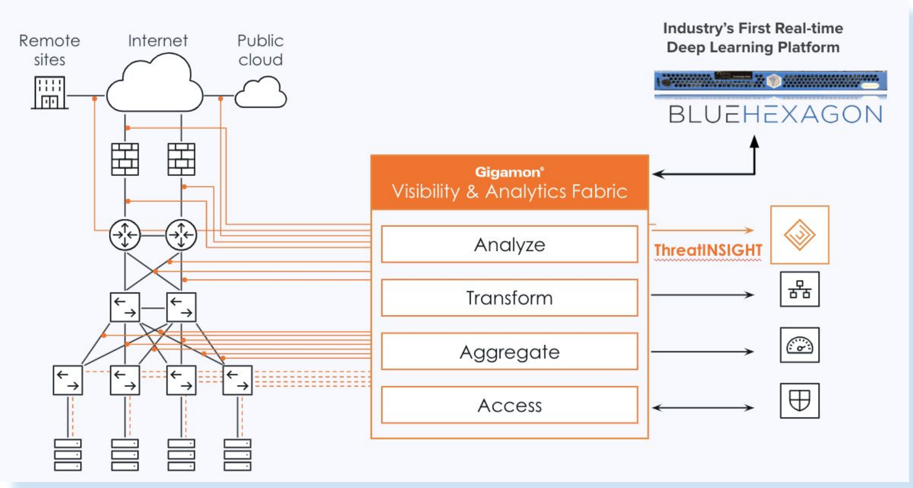
More than 350,000 malware variants are produced each day. That's 231 new malware per minute, 4 every single second[1]. Signature-based defenses cannot keep up with the speed and variants of new malware, while sandboxes have limitations with speed of analysis and file sizes, and are subject to evasion tactics.

Blue Hexagon harnesses deep learning to deliver malware protection at a speed and efficacy that can keep pace with attackers. The Blue Hexagon platform incorporates a proprietary neural network architecture pre-trained with the massive threat data that exists today. The platform can detect malware and malicious command and control (C2) by inspecting network traffic--including payloads and headers--in **less than a second** at **greater than 99.5% efficacy.**

Blue Hexagon requires access to high-fidelity network traffic for malware inspection. This is the benefit of the Blue Hexagon and Gigamon integration. Gigamon provides a security delivery architecture that not only gives Blue Hexagon the visibility to appropriate network traffic for inspection, including into encrypted traffic, but also improves performance and resiliency. Together, Blue Hexagon and Gigamon can be deployed to address critical cybersecurity challenges.

The following are the key integration use cases:

- **Visibility across physical, virtual and cloud with application intelligence:** Blue Hexagon inspects a copy of the traffic at the ingress of the network. The Gigamon Visibility and Analytics Fabric (VAF) consists of one or more visibility nodes that receive traffic from any number of network TAPs and SPAN ports for various network link speeds. Visibility across physical, virtual and cloud is supported. The VAF can be configured to send only relevant traffic — or relevant sessions — to Blue Hexagon.



Blue Hexagon and Gigamon Integration

[1] AV-Test GmbH - "How AI can help stop cyberattacks", Wall Street Journal

- **Traffic Intelligence:** GigaSMART® Traffic Intelligence enables traffic intended for Blue Hexagon malware inspection to be optimized for delivery.
    - 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.
    - Easier control of asymmetric routing: The Visibility Fabric provides an intelligent and efficient way to help ensure that Blue Hexagon inspection is supported and session information is kept together.
    - De-duplication: To avoid the unnecessary packet-processing overhead, the Visibility Fabric removes duplicates before forwarding to Blue Hexagon.

- **SSL Decryption:** Though reports vary, between 35 and 50 percent of traffic is now encrypted, and that number continues to rise.[2] While encryption addresses privacy and legal requirements, security teams now face a challenge where they are blind to a large influx of traffic. The VAF decrypts SSL encrypted traffic and sends it to Blue Hexagon for malware inspection. (Note that Blue Hexagon also inspects encrypted headers for malicious communications)

- **Load Balancing Beyond 10G:** Blue Hexagon malware protection platform is available as hardware and virtual appliances, up to 10G network performance. Gigamon load balancing capabilities enable Blue Hexagon to scale from 10G to 25G, 40G, 100G and beyond.

Deployments

Blue Hexagon and Gigamon can be jointly deployed to inspect network traffic on premises, in private data centers and in public cloud environments:

- **On-premises networks and private data centers:** At the network perimeter, Gigamon can direct the appropriate network traffic to Blue Hexagon for inspection. When malware is detected in less than a second by Blue Hexagon, prevention is orchestrated across security products that are already deployed such as endpoint security and firewalls, to stop malware from executing on the endpoint and blocking C2 communications.
- **Public cloud network:** Tapping traffic flowing to, from, or between virtual machines is critical to ensuring security for the private or public cloud. Gigamon ties into the hypervisor and virtual switch to not only tap virtual traffic, but also select which traffic is forwarded to the VAF and Blue Hexagon. When malware is detected by Blue Hexagon, integration with cloud services API ensures infected virtual machines are immediately isolated and shut down.

Summary

Blue Hexagon's deep learning-based network threat protection is industry's fastest and most accurate malware protection platform. The platform can detect malware in less than a second, at greater than 99.5% efficacy. The ability to do this relies on the fidelity of network traffic, which is why Blue Hexagon and Gigamon integration delivers better together benefits. The Gigamon integration directs appropriate traffic to Blue Hexagon for optimal, seamless inspection. In addition, Gigamon functionality such as traffic intelligence and load balancing enables scalability and performance for the joint solution.

About Gigamon
Gigamon is the first company to deliver unified network visibility and analytics on all information-in-motion 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. Gigamon has been awarded over 75 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations, including over 80 percent of the Fortune 100. Headquartered in Silicon Valley, Gigamon operates globally. For the full story on how Gigamon can help you to run fast, stay secure and innovate, please visit 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 network threats with speed, efficacy, and coverage that set a new standard for cyber defense. Blue Hexagon is headquartered in Sunnyvale, CA, and backed by Benchmark and Altimeter Capital. For more information, visit www.bluehexagon.ai or follow @bluehexagonai.

Blue Hexagon, Inc.
298 S. Sunnyvale Avenue, #205
Sunnyvale, CA 94086 USA
bluehexagon.ai
inquiries@bluehexagon.ai

[2] *J. Michael Butler, "SANS Institute InfoSec Reading Room: Finding Hidden Threats by Decrypting SSL," November 2013; Johnnie Konstantas, "SSL Encryption: Keep Your Head in the Game," Security Week, March 15, 2016.*