Gigamon

BLUVECTOR™

Joint Solution Brief

Real-time, Network-based APT Detection, Logging and Investigation That Won't Impact Network Performance

The Challenge

Traditional security solutions are ineffective at detecting advanced persistent threats (APT) – reports show that most compromises are detected by third parties in an average of 205 days after the intial compromise.[1]

Integrated Solution

Together BluVector and Gigamon enable customers with high-capacity networks to accurately and in real time detect, log and investigate advanced cyber threats—including ones that evade traditional network security defenses. The GigaSECURE platform delivers high-fidelity data streams in a manner that makes most efficient use of BluVector. BluVector then uses proprietary, award-winning machine learning to analyze file types in real-time to detect malicious threats. Security analysts can now effectively hunt, continuously monitoring network traffic to detect, log, and investigate APT-related incidents in minutes.

Key Benefits

- **Scalable threat protection:** Can distribute de-duplicated, high-fidelity network traffic from multiple network links across multiple BluVector instances
- **Pervasive visibility:** Traffic from public cloud, virtual and physical infrastructure can all be analyzed by BluVector
- **Data fidelity and consistency**: Provides broad and consistent analysis of supported file types for APT detection and logging
- **Inspect encrypted traffic:** Decrypts SSL traffic for out-of-band inspection and analysis
- **Near real-time:** Prevents many latencies that could add to incident remediation times

Introduction

Sophisticated and persistent hackers today have found ways past traditional security solutions. Last year, according to M-Trends reports[1], it took an average of 205 days for a company to detect a breach, with 69% learning they were breached from a third party and only 31% discovering it themselves. Clearly, companies need to get better at detecting and investigating malicious activity. A single breach can cause serious damage, including an average financial loss of $3.79 million[1], as well as a hit to brand and reputation.

With only 22% of malware-based advanced threats investigated each week, what is needed is the ability to scan high-capacity network traffic in real time to accurately detect, log, and efficiently investigate advanced persistent cyber threats (APT) in minutes, not months.

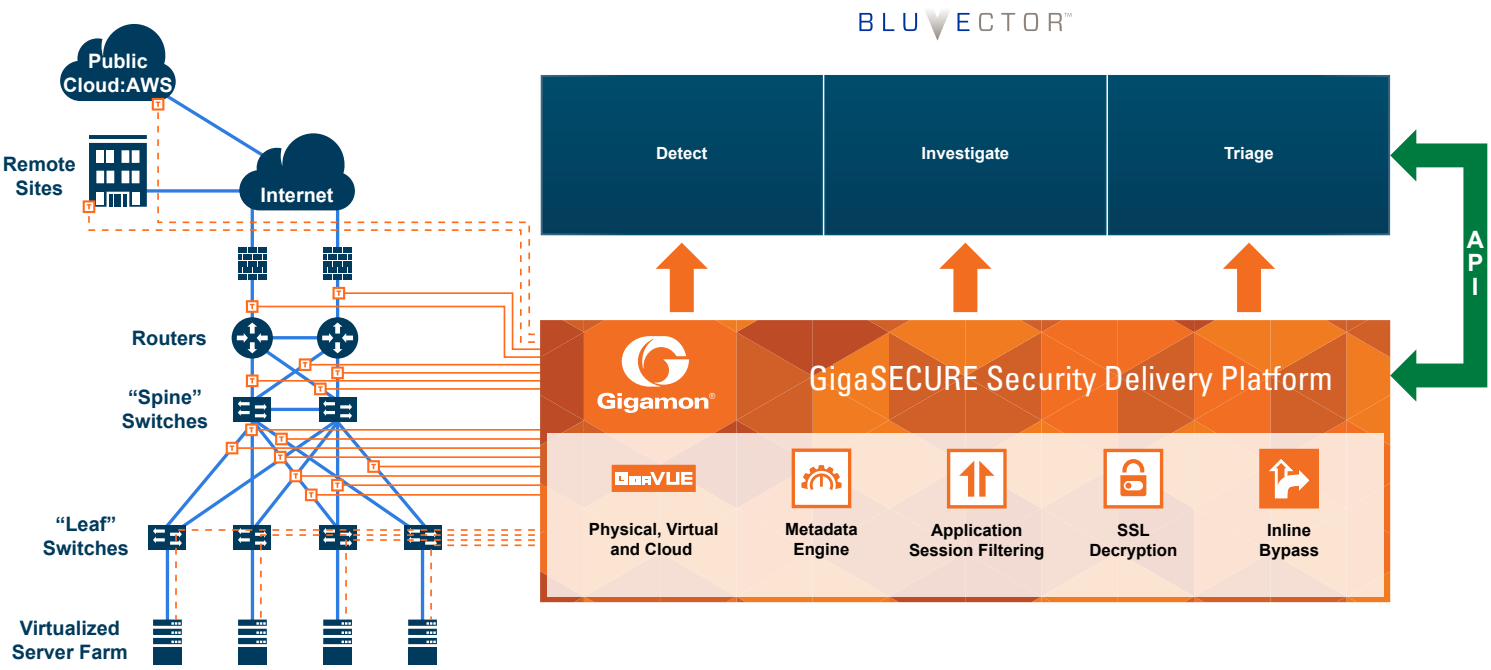
The Gigamon and BluVector Joint Solution

BluVector's high-performance network security appliance combined with Gigamon's GigaSECURE Security Delivery Platform allows customers with high-capacity networks to accurately and efficiently detect, log, and investigate APTs – including ones that evade traditional network security defenses—such as zero-day exploits and polymorphic malware.

The GigaSECURE platform is used to feed traffic from across the network to BluVector from any physical and virtual links. The traffic can be de-duplicated, aggregated, decrypted, and/or load balanced as necessary for maximum efficacy of the deployed BluVector instances. For example, multiple sub-10Gb feeds can be aggregated into a single port on the BluVector instance, or flows larger than 10Gb can be load balanced across multiple BluVector instances to handle large-scale deployments. SSL/TLS encrypted traffic can be decrypted and sent to BluVector for analysis.

BluVector's patented machine learning is able to perform in-memory processing of network sessions to analyze files in milliseconds. Ground-breaking new artificial intelligence adapts BluVector machine-learning classifiers on the appliance, creating a unique detection engine, making it more difficult for adversaries to replicate and evade.

[1] 2015 M-Trends Report



Just like the GigaSECURE Security Delivery Platform, BluVector integrates with existing or custom security solutions, including many major sandboxes, SIEM tools, and threat intelligence feeds. While the GigaSECURE platform allows efficient and straight forward deployment for a suite of security tools, BluVector lets users automate key processes such as forwarding to a sandbox for dynamic malware analysis. Users can also leverage results of detection engines, related logs and third-party intelligence, prepared in an intelligence package for security investigators, to use as context to review and triage threats in minutes.

Learn More

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

BLUVECTOR™
https://www.bluvector.io/

Gigamon®
www.gigamon.com

3207-03 06/17

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