



Joint Solution Brief

Vectra Automated Threat Management with the Gigamon Security Delivery Platform

The Challenge

Despite a strong perimeter defense with next-generation firewalls, IDS and malware sandboxes, cyber attackers will still get into your network. And without visibility into what's happening inside the network, it's impossible to detect and mitigate these attacks.

Integrated Solution

With the GigaSECURE® Security Delivery Platform from Gigamon, the Vectra Networks automated threat management solution provides continuous monitoring of internal network traffic to pinpoint in-progress cyber attacks that evade perimeter defenses.

Vectra automatically detects cyber threats hidden in approved applications and encrypted traffic, correlates those threats to the hosts that are under attack, and delivers unique context about what attackers are doing, enabling security teams to quickly address and mitigate loss.

Joint Solution Benefits

- Vectra detects in-progress cyber attacks that evade prevention security defenses and spread inside networks—automatically and in real time
- Offering visibility into physical and virtual traffic across the network, Vectra combines data science, machine learning and behavioral analysis to detect the typical phases of a cyber attack
- Gigamon enables the relevant traffic and sessions to be sent to the Vectra automated threat management solution, thereby improving efficacy
- Gigamon taps virtual traffic and delivers it to Vectra on the physical network—causing traffic to be monitored and analyzed together and avoiding blind spots

Introduction

Despite strong perimeter defenses using next-generation firewalls, IDS/IPS and malware sandboxes, cyber attackers continue to slip past the signatures and reputation lists used by these prevention systems and spread inside networks. Further, mobile device users can bypass these controls altogether, literally carrying hidden threats from public Wi-Fi hotspots into the network.

The problem is that signatures and reputation lists only detect *known* threats and must be continually updated. It's easy for attackers to mount an assault using different IP addresses or by adding a few bits to a malware file so it can slip by, unknown and undetected.

Security analysts today are also overwhelmed by a never-ending succession of alerts and logs about potential network cyber attacks. It's not humanly possible to sift through and interpret that much data, identify the most serious threats, and then mitigate attacks before they spread.

In addition, security teams often don't know what to look for or where. Many organizations use log managers and SIEMs that rely on feeds from security systems that fail to detect threats in the first place. And they are often required to painstakingly reconstruct each cyber breach in order to understand the extent of damage.

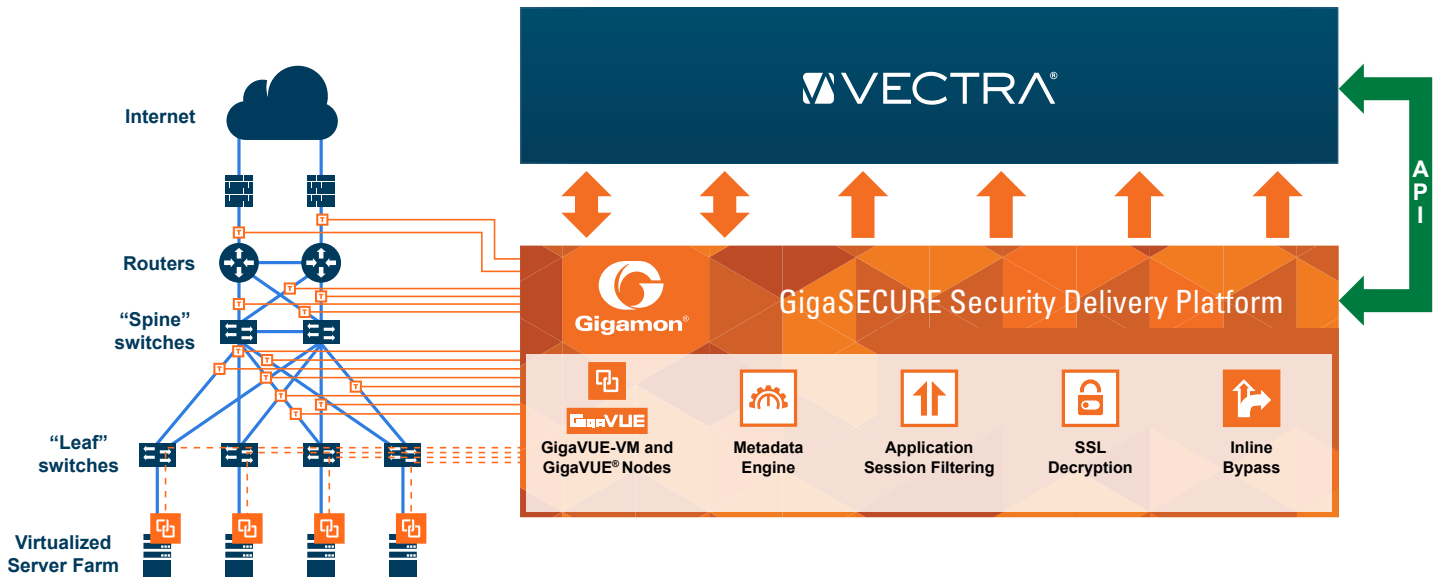
Despite all the prevention security tools at your disposal, there remains a dangerous security gap between the time attackers infiltrate and spread inside a network and the moment organizations discover they've become victims of a data breach.

The Vectra and Gigamon Joint Solution

The Vectra Networks automated threat management solution, augmented with the GigaSECURE Security Delivery Platform from Gigamon, continuously monitors internal network traffic to detect in-progress cyber attacks in real time.

Gigamon provides intelligent filtering on physical and virtual networks and passes that traffic to Vectra for real-time threat analysis. Multiple Gigamon tap points deployed at the edge and core provide Vectra with intelligent traffic filtering at all key points in network.

In addition to automatically correlating detected threats against hosts that are under attack, Vectra provides unique context about what attackers are doing so organizations can quickly address and mitigate loss. Attacks that pose the highest risk are prioritized so IT security teams can focus their attention on the detections that matter most.



Vectra leverages a unique combination of data science, machine learning and behavioral analysis to detect the typical phases of an attack—command and control, botnet monetization, internal reconnaissance, lateral movement and data exfiltration.

Over time, Vectra understands the naturally occurring communities in the network and continuously listens, thinks and learns to adapt to the ever-changing threat landscape. Vectra gives IT security teams the speed and agility to help stop threats that present the biggest danger.

Vectra and the GigaSECURE Platform

The GigaSECURE Security Delivery Platform delivers a wide range of critical features to Vectra automated threat management deployments, including:

- **Easy access to traffic from physical and virtual networks:** The GigaSECURE platform manages and delivers network traffic to Vectra efficiently and in the correct format. To monitor east-west data center traffic, Gigamon taps virtual traffic and incorporates it into the GigaSECURE platform for delivery to Vectra on the physical network. This ensures that traffic is monitored and analyzed together and eliminates blind spots.
- **Filtering traffic to only send relevant traffic:** The GigaSECURE platform can be configured to send only relevant traffic or sessions to the Vectra solution. This ensures that Vectra only analyzes traffic that provides security value.

- **Aggregation minimizes tool ports:** The GigaSECURE platform aggregates links with low traffic volumes before sending them to Vectra, reducing the number of ports that are used. Traffic tagging ensures that the traffic source is always identified.

Together, Vectra and Gigamon close the dangerous cybersecurity gap between perimeter defenses and post-breach analysis by providing network visibility and real-time detection of the fundamental actions and behaviors that attackers perform when they spy, spread and steal inside networks.

Learn More

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

