Vectra and Gigamon Provide Rapid Detection of Supply Chain Attacks

Overview

Supply chain attacks pose a great risk against federal networks. Unprotected federal departments and branches have suffered a severe breach from trusted applications being weaponized against them in various types of supply chain attacks. What other trusted application are vulnerable?

Vectra provides rapid detection and response by examining behavior on the network to detect changes in application communications, while Gigamon provides Vectra with complete visibility into data-in-motion across all IT operations, including cloud and virtualized infrastructure, to eliminate monitoring blind spots.

Vectra Threat Detection and Response Platform

The Vectra Threat Detection and Response Platform automatically detects cyberthreats hidden in approved applications and encrypted traffic in hybrid, on-premises and cloud deployments with learning behavioral models that understand both hosts and identities — tracking and stopping attackers earlier in the kill chain.

By leveraging a unique combination of data science, machine learning and behavioral analysis, it offers real-time early warning and continuous visibility across the attack progression from on-premises to cloud — without dependency on indicators of compromise (IoCs), signatures or other model updates. All of this works to identify and stop attacks like SolarWinds before damage is done.

The Vectra Platform correlates threats to the hosts and accounts under attack, and it delivers unique context about what attackers are doing, enabling security teams to quickly address and mitigate loss.

Gigamon Provides Vectra with Complete Infrastructure Visibility

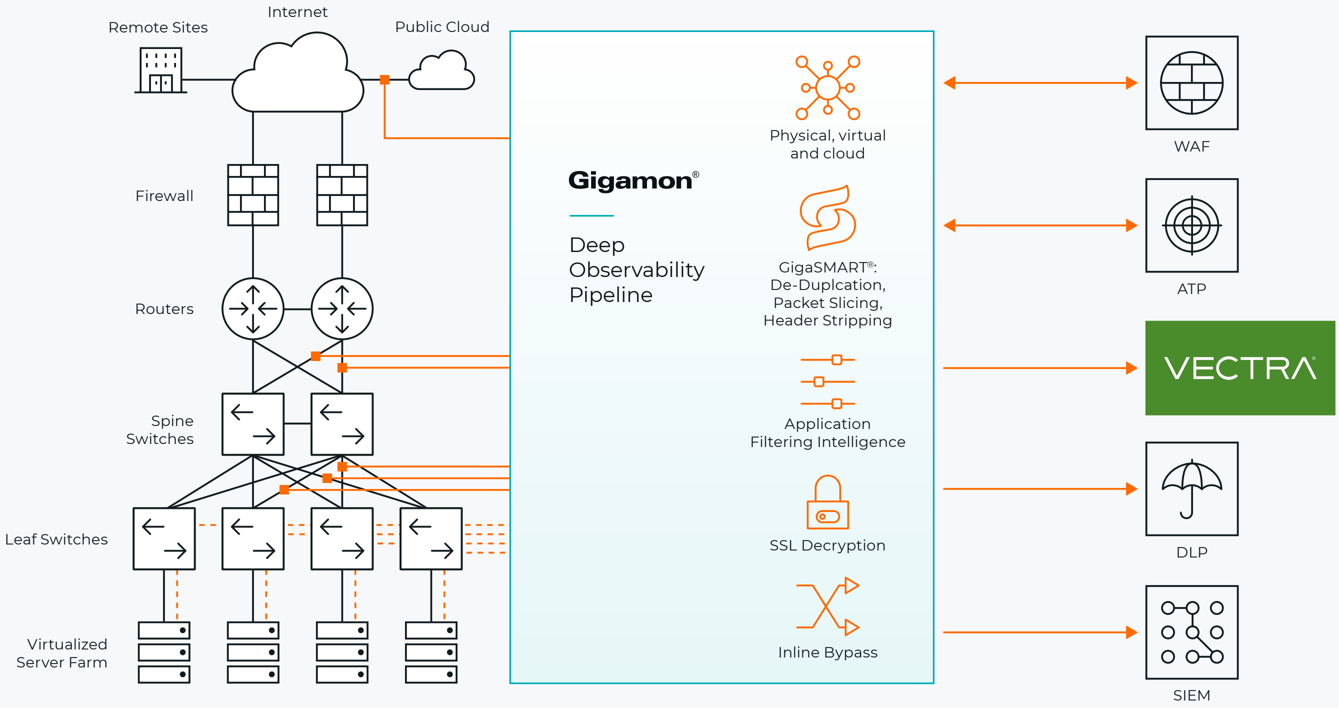
The Gigamon Deep Observability Pipeline provides complete visibility into the data-in-motion across all IT operations — physical networks, virtual networks, private and public clouds — eliminating cybersecurity monitoring blind spots. Gigamon collects and aggregates the network-level traffic and transforms the packets in real-time, including packet de-duplication, header stripping and application traffic identification and filtering. Gigamon then forwards custom sets of monitoring data to Vectra to optimize Vectra coverage and effectiveness.

The Gigamon Deep Observability Pipeline can be deployed using physical chassis/taps or as a 100 percent virtual solution in AWS, Microsoft Azure, Google or OpenStack-based clouds, or within a micro-segmented environment on the network, such as VMware, Nutanix, Kubernetes, IBM/RedHat or Cisco ACI. The instantiation of visibility, data aggregation, processing and forwarding is controlled from the GigaVUE-FM fabric manager interface.

Countering Security Threats with Vectra and Gigamon

Well-documented attacks demonstrate the utility — and necessity — of network monitoring when taking steps to detect breaches that have bypassed preventative security and to protect data. Network-based technologies are critical when countering the increasing sophistication of threats. Preventative security and endpoint controls, while raising the bar, are insufficient, and legacy, signature-based systems have again been proven ineffective when detecting new attacks where IoCs do not yet exist. Leveraging network detection and response — where the network is defined broadly as everything outside of the endpoint — is a more effective approach for defending against this class of attack.

Together, Vectra and Gigamon close the visibility gap between perimeter defenses and postbreach analysis by providing network visibility and real-time detection of the fundamental actions and behaviors that attackers use to take advantage of supply chain trust. This gives IT security teams the speed and agility needed to stop well-funded and deeply motivated threat actors before they cause harm.



The Challenge

- Complete infrastructure visibility
- Disparate streams of intelligence to manage
- Rapid attack detection on trusted supply chain software

The Solution

- Gigamon Deep Observability Pipeline
- GigaSMART applications
- Vectra Threat Detection and Response Platform

Joint Solution Benefits

- Eliminate cybersecurity monitoring blind spots
- Automated detection of cyberthreats hidden in approved applications
- A more effective approach to defend against security attacks

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the ten largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

For more information on Gigamon and Vectra please visit gigamon.com | vectra.ai

Gigamon®

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