Joint Solution Brief

Full Visibility Into Breach Forensics

The Challenge

While the goal of all security teams is to stop breaches before they occur, we're reminded every day that this isn't always possible. Breaches happen, and they can go undetected for hours, days, or even months. When analysts find a breach, they need to figure out quickly how the breach occurred, whether it spread, and what impact it had. To do that, they need access to accurate historical data, including what happened minutes before the breach occurred.

Integrated Solution

Savvius Vigil, with Gigamon's GigaSECURE® Security Delivery Platform, provides security analysts with the full visibility and scalability you need to effectively do your job. The joint solution offers a flexible and efficient platform for collecting, storing, and retrieving the network-level data required to investigate security breaches even if they took place months ago.

Joint Solution Benefits

- Enables network forensics in breach investigations
- Stores months of relevant data
- Integrates with all major security detection systems
- Provides packet intelligence into past incidents
- De-duplicates and filters traffic to ensure only relevant data is stored
- Ensures full traffic visibility by real-time SSL decryption

Introduction

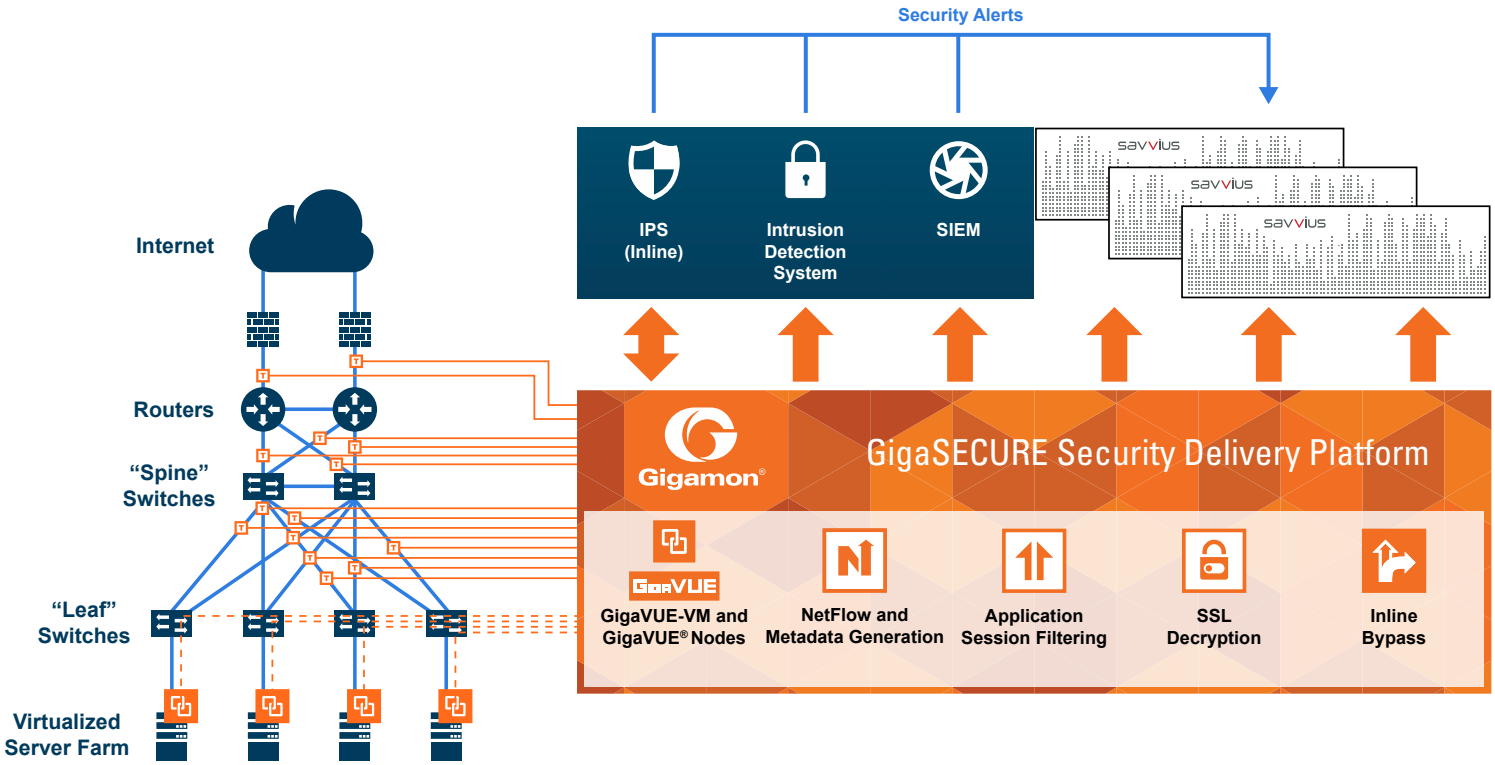
Network breaches are becoming increasingly common. The economic and political advantages that attackers can gain lead to both a higher frequency and greater sophistication of attacks. Breach prevention and detection are critical for reducing the chance of being breached, but breach investigation and quick incident response are also essential as we can't always rely on keeping all the bad guys out. It can sometimes take days, weeks, or months to even realize there has been a breach. We need to ensure our customers have the data they need to investigate the cause, extent and remediation of a breach when they do find it.

The Gigamon and Savvius Joint Solution

Savvius Vigil is the security industry's first network forensics appliance to intelligently store months of packet-level information that can enhance security investigations. Breaches often are discovered weeks or months after the incident occurs. Savvius Vigil lets your organization conduct powerful forensic investigations by extending breach visibility and integrating with key security systems. You can intelligently capture critical packet data before and after an attack occurs allowing your organization to gain a clear and accurate picture of the damage, and react quickly.

Integrated with the organization's existing SIEM/IDS/IPS capabilities, Savvius Vigil will intelligently determine what network traffic is relevant for breach investigations. It continuously collects all network packets and only stores traffic associated with security alerts, discarding unassociated packets. The device also supports feeds from multiple sources simultaneously.

Availability and accessibility of network traffic can be a challenge, especially for high-speed networks. Savvius Vigil requires access to network traffic continuously in order to capture and store the relevant packet data for near-term and delayed-discovery security investigation. For this reason, the Gigamon GigeSECURE Security Delivery Platform is the perfect complement to Savvius Vigil. The Gigamon platform allows traffic to be tapped from any part of the network of interest, through either a virtual or physical connection. The traffic can be de-duplicated to ensure that each packet is only stored once, and packets that are not of interest can be filtered out. For example, an organization may want to store credit card server traffic but not backup server traffic, or store the initial session information for videos flowing over the network for identification sake, rather than storing the whole video which would be a waste of storage resources. Once irrelevant traffic has been removed, the GigaSECURE platform can deliver the remaining traffic to Savvius Vigil. If the traffic stream for storage and processing is larger than a single Vigil device can handle, the GigaSECURE Security Delivery Platform can load-balance the traffic flow across multiple devices, retaining session information for correct analysis later.



When the operator has access to the correct private keys, the GigaSECURE platform can also decrypt traffic streams before delivering them to Savvius Vigil. If the keys are not available, Gigamon and Savvius can provide alternative solutions.

Learn More

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

savvius
www.savvius.com

Gigamon®
www.gigamon.com

3190-01 04/16