Joint Solution Brief

Detect Modern Intrusions with Fidelis Cybersecurity and Gigamon

The Challenge

Attackers are sophisticated and savvy, and traditional prevention and detection solutions organizations have invested in don't dig as deep as attackers hide—leaving them vulnerable to compromise and inevitable data theft.

Integrated Solution

Fidelis Network combined with Gigamon GigaSECURE® Security Delivery Platform and Visiblity Platform for AWS, harnesses the power of complete network visibility to detect attacks and prevent data theft at every stage of the attack lifecycle.

Joint Solution Benefits

- Enhanced visibility and easy access to traffic for on premise physical and virtual networks via the GigaSECURE platform and in the AWS cloud via the Visibility Platform for AWS enables Fidelis Network to accelerate detection and investigation cycles
- Inspect and analyze SSL encrypted traffic out-of-band to uncover previously hidden malicious activity
- With the GigaSECURE platform's dynamic load balancing, Fidelis Network can easily scale to monitor up to 100Gb of traffic
- Aggregate traffic from under-utilized links to enable the most efficient use of Fidelis sensors, maximizing ROI for the Fidelis Network investment
- The GigaSECURE platform's transparent handling of traffic means that Fidelis Network's inline and out-of-band prevention capabilities work at any scale
- In the event of a network outage, GigaSECURE inline bypass functionality supports failover protection and maintains high availability for Fidelis Network and the network it protects

Introduction

Organizations have invested millions to build secure networks and keep would-be attackers out of their enterprises. Despite these investments, determined attackers continue to routinely compromise organizations, remain undetected, and steal intellectual property and financial assets. Security analysts, overwhelmed by alerts and tasked with reviewing and triaging suspected incidents, can't quickly detect threats as they are happening in real time and receive little context on the potential impact—making it extremely difficult to adequately respond to an event.

The net result is analysts often miss the most critical attacks or detect them long after vital data has been stolen. Why? Signs of an initial attack can be stealthy and are difficult to differentiate from noise of the day-to-day deluge of alerts. The sheer number of genuinely important alerts makes it near impossible to respond to all of them. Manual processes slow teams down. Delayed response times due to inaccurately prioritized alerts further compound the issue and create gaps that attackers use to gain a foothold and roam freely across a network.

The Gigamon and Fidelis Cybersecurity Joint Solution

The combination of Fidelis Network™ and Gigamon GigaSECURE Security Delivery Platform and Visibility Platform for Amazon Web Services (AWS) equips organizations to detect, investigate, and stop advanced attackers at every stage of the attack lifecycle—including when attackers move laterally, establish command and control footholds and prepare to steal data. By receiving the right data at the right time from the Gigamon platforms, you get the visibility, context and speed required to identify and prevent modern intrusions. Wherever your data (encrypted or not) is traversing the internet - on premise, or in the AWS cloud - Fidelis and Gigamon have you covered.

- **Detect Attacks Other Solutions Miss:** Modern attacks are no longer confined to advanced malware, exploits, and command and control activity. They now hide deep within content and are obfuscated on your endpoints in ways that other traditional network security tools miss. Fidelis combines the best of all technologies – Sandbox, Deep Packet Inspection (DPI), Deep Session Inspection (DSI), Endpoint, and historical metadata – with Threat Research Teams (TRT) advanced cyberthreat intelligence to uncover new breeds of malicious activity and stop it in its tracks.
- **Identify and Stop Targeted Attacks Just as They Are Beginning:** Quickly identify malicious behavior—including command and control activity and lateral movement—and halt data theft before it begins.

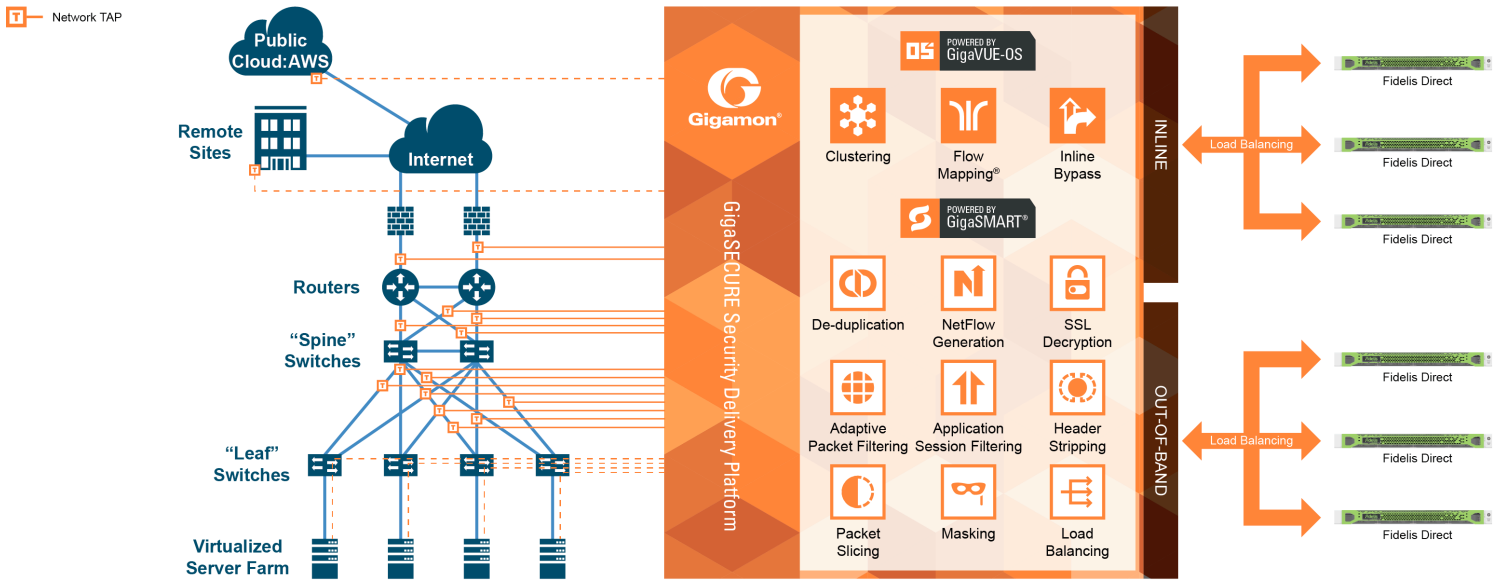

Figure 1: Hybrid Deployment Model

- **Correlate Seemingly Unrelated Network Activity and Behavior:** Find occurrences of past threat activity using Fidelis' rich historical metadata. Correlate and validate alerts from seemingly unrelated network behavior by applying automated hunting and security analytics to retrospective metadata gathered on every network session. Conduct analyses of reconstructed TCP sessions from every port and every protocol and dig deeper by decoding multiple layers of files and objects.
- **Reduce Time to Detect and Resolve Incidents:** Quickly identify and validate the most relevant alerts and apply cyberthreat intelligence to network data. Fidelis provides the context needed to enable security analysts to move, within moments, from alert to investigation to remediation using a single intuitive interface.

Recognize the power of visibility—to accelerate the discovery of suspicious activity and advanced targeted attacks—with Fidelis Network and the GigaSECURE Security Delivery Platform and GigaVUE V Visibility Platform for AWS. Improve your organization's security posture by enabling security analysts to focus on the most relevant information so they can move, within moments, from alert to investigation to threat resolution.

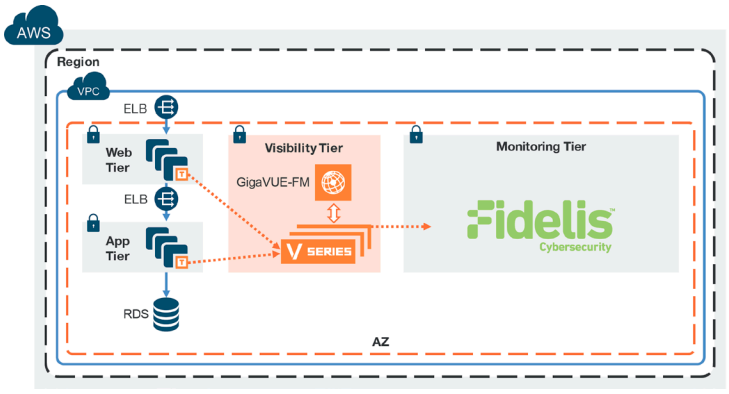

Figure 2: Public Cloud Deployment Model

Learn More

For more information on the Fidelis Cybersecurity and Gigamon solutions, contact:

Fidelis Cybersecurity
www.fidelissecurity.com

Gigamon®
www.gigamon.com

3201-02 05/17