Gigamon® | Fidelis Cybersecurity

# Securing and Protecting Applications and Data Everywhere with Fidelis Cybersecurity and Gigamon

### THE CHALLENGE

Attacks leveraging phishing, social engineering, and drive-bys are increasingly using file-less methods of scripts, macros, and PowerShell to evade prevention-based defenses. Once attackers establish footholds, early reconnaissance enables lateral movement within as little as a few hours. Early detection, investigation, and response are required to reduce dwell time and potential data theft.

### THE SOLUTION

Fidelis Network®, combined with Gigamon GigaSECURE®, harnesses the power of complete network visibility, including cloud-based applications and data to prevent, detect, investigate, and respond with optimized visibility of metadata and automation at every stage of the attack lifecycle.

### JOINT SOLUTION BENEFITS

+ Enhance visibility and gain easy access to traffic for on-premises physical and virtual networks and the cloud via Gigamon, which enables Fidelis Network sensors to accelerate detection, investigation, and response cycles
+ Inspect and analyze SSL/TLS encrypted traffic out-of-band to uncover previously hidden malicious activity
+ GigaSECURE's dynamic load balancing enables Fidelis Network sensors to scale

## Introduction

Cloud adoption of applications and data is well underway, mainly into VMs using infrastructure-as-a-service (IaaS.) What remains are legacy applications and supporting office and campus networks for workplace collaboration and reduced or closed datacenters. Gaining visibility into VM-based cloud applications and data to detect threats and data loss/theft has been challenging with cloud providers. Organizations face a multi-cloud hybrid environment where security controls require new approaches.

## The Gigamon + Fidelis Joint Solution

The combination of Fidelis Network and Gigamon GigaSECURE delivers XDR for on-premise, virtual, hybrid, and cloud-driven organizations, with enhanced capabilities 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. Gigamon delivers vital network communication flows for North-South (direct) and East-West (internal) traffic to Fidelis Network sensors on-premise or in the cloud. Together Fidelis and Gigamon provide deeper detection and triage for SOC and threat hunting teams.

Fidelis Network provides analysis of packet traffic using Deep Session Inspection® (DSI) and includes hundreds of metadata attributes and custom tags for real-time and retrospective analysis for threat detection, threat hunting, and data loss/theft detection. Fidelis Network includes direct, internal, cloud, email, and web sensors for unmatched visibility for hybrid multi-cloud networks.

+ **Deep Session Inspection (DSI):** Network-based IPS, Deep Session Inspection across all ports and protocols, enhanced email and web detections, plus TLS decryption for cloud and on-premise.
+ **Enhanced data loss prevention (DLP):** Enhanced rule set and

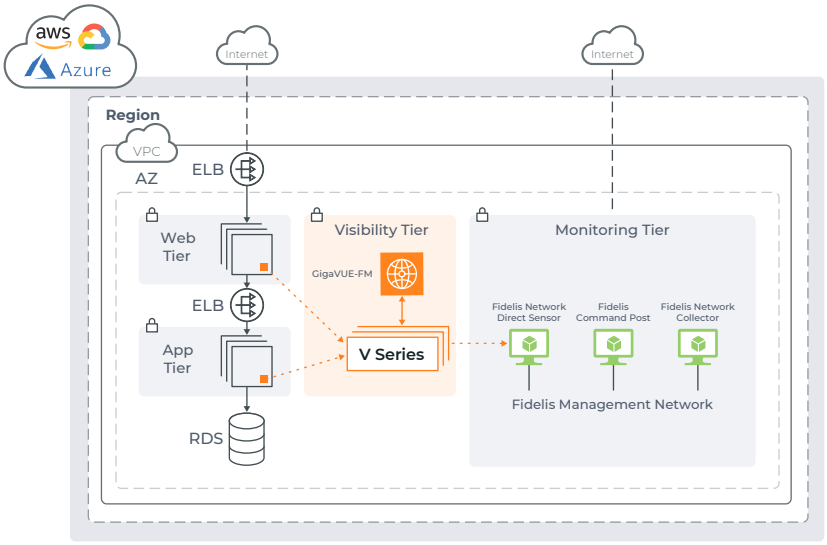


Figure 1: Public cloud deployment model.

search algorithms offer greater insight and visibility for improved data protection and the data loss prevention practices.

+ **Cross-session and multi-faceted analysis, plus machine-learning anomaly detection** enable real-time and retrospective analysis for threat detection, threat hunting, and data loss/theft detection. Security analysts can query, pivot, and hunt on content and context.
+ **Metadata for hundreds of attributes** and custom tags, with the ability to store up to 360 days in the cloud or on-premises, providing content and context not seen in firewall logs or SIEM dashboards.
+ **High-performance network sensor capabilities** with no data sampling or packet drops, plus multi-sensor configurations that scale with network performance requirements.
+ **Fidelis Insight provides threat intelligence** based on threat research team (TRT) research and analysis. Multiple threat intelligence feeds enable security analysts to detect, investigate, and track anomalous activity.
+ **Expand to Fidelis Elevate** with Dynamic Deception, which allows for a continuously changing attack surface to increase adversary cost, complexity, and risk. Adding deception creates a complete threat detection, threat hunting, and data loss and theft detection solution.
+ **Reduce time to detect and resolve incidents:** Quickly identify and validate the most relevant alerts and apply multiple defenses and sources of threat intelligence to network data. Fidelis provides the content and context needed to enable security analysts to move, within moments, from alert to investigation to remediation using a single intuitive interface and automation within workflow phases.
+ **Real-time and retrospective threat detection:** Correlate and validate alerts from seemingly unrelated network behavior by applying automated threat detection and security analytics in real-time and retrospectively to 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 to analyze content and context.

Recognize the power of visibility — to accelerate the discovery of suspicious activity and advanced targeted attacks — with Fidelis Network and GigaSECURE.

**For more information on Gigamon and Fidelis, visit gigamon.com and fidelissecurity.com.**



Gigamon®

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