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 footholds are established, early reconnaissance enables lateral movement within as little as a few hours in most cases. Early detection, investigation and response are required to reduce dwell time and potential data theft.

Integrated Solution
Fidelis Network® combined with Gigamon GigaSECURE® Security Delivery Platform and Visibility Platform for AWS, harnesses the power of complete network visibility including AWS VM-based applications and data to prevent, detect, investigate and respond with unmatched 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 in the AWS 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 platform’s dynamic load balancing enables Fidelis Network sensors to scale to multi-gigabit network performance on-premises and within cloud environments
• 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
Cloud adoption of applications and data, mainly into VMs using infrastructure-as-a-service (IaaS), is well underway with organizations expected to reach 60-80% adoption of their portfolios by 2021. What remains behind are legacy applications and supporting office and campus networks for workplace collaboration and reduced or closed data centers. Gaining visibility of 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 including AWS.

The Fidelis Cybersecurity and Gigamon Joint Solution
The combination of Fidelis Network® and Gigamon GigaSECURE Security Delivery Platform and Visibility Platform for Amazon Web Services (AWS) equips organizations with the visibility 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 communications for north-south and east-west traffic to Fidelis Network sensors on-premise, or in the AWS cloud. Together Fidelis and Gigamon have you covered.

Fidelis Network
• Provides analysis of 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 also provides a Managed Detection and Response (MDR) service for 24/7 cloud monitoring of AWS VMs with proactive incident response (IR) services.
  • Fidelis Network includes direct, internal, cloud, email and web sensors for unmatched visibility for hybrid multi-cloud networks.
  • Deep Session Inspection (DSI) of AWS cloud VM-based communications for all ports and protocols to analyze sessions, content, and obfuscated files and archives.
  • 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.
Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.

Contact Us Today to Learn More
Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.