

# Fidelis Scout 2

## Incident Response & Assessment Platform

### Speed & Agility Matter

Organizations face many challenges where speed and agility are required for incident response and assessment. Whether faced with the challenge of constrained resources and expertise or simply needing rapid network health checks and assurance; a simple, fast and thorough cyber security response and assessment solution is the ideal fit.

Fidelis Scout 2 is a portable and flexible platform optimized for rapid and temporary deployment to help organizations:

- Assess security posture and protect sensitive data from loss
- Detect threats and identify intrusions
- Investigate and respond to incidents

By delivering immediate and deep visibility into network traffic, Fidelis Scout 2 enables faster remediation and delivers actionable reporting for diagnosis and post-incident processes.

### Audit & Assessment Acceleration

Fidelis Scout 2 is an all-in-one platform designed to provide the tools necessary to gain broad network and endpoint visibility for audit, assessment, and incident response teams. With pre-built and customizable detection policies and other included detection mechanisms, Fidelis Scout 2 delivers fast visibility into a network allowing for overall risk assessment within hours of arriving at the audit or investigation site.

### Incident Response, Investigation & Data Protection

Fidelis Scout 2 is purpose-built for threat detection, investigation and incident response. One-click investigation delivers complete and actionable context to the incident responder, investigator or threat hunter. Fidelis is populated with more than enough computing resources to allow for the installation of other useful IR tools.

### Scout 2 Benefits

- **Next-Generation Platform:** Reassemble, decode, and analyze network sessions in memory, in real time. Analyze all types of content no matter how encapsulated, encoded, embedded, compressed, or obfuscated.
- **Fast Deployment:** Available as VM or transportable hardware platform equipped with virtual bundle software. All-in-one form-factor with pre-built and customizable detection policies and other included mechanisms that enable response and assessment to begin within hours of arrival.
- **Intelligent Network Forensics:** Automatically record network sessions of interest in real time.
- **Enterprise Scalability:** Full session analysis of all network traffic, protocols, and applications. Supports gigabit-speed networks.
- **Endpoint Detection and Response:** Advanced EDR capabilities for fast incident response and forensic data collection.

Ideal Fit Scout Scenarios	Description
Threat Hunting	Plug in and start hunting as soon as you arrive on site. Includes reporting & analytics.
Data Leakage Assessment	Focused DLP and suspicious / malicious behavior assessment & reporting.
Network-Endpoint Visibility	Integrated network & endpoint detection, validation & response in a box.
Incident & Breach Response	Fast and integrated detection, remediation, sanitize & reporting platform.
Proactive Assessments	On-the-fly health and security assessment with reports that support recommendations.
M&A Assessments	Check the health and security of networks queued for M&A integration.

## Fidelis Scout 2: Rapid Response & Assessment Platform

Virtual Scout System	vCPU <sup>1</sup>	Memory <sup>2</sup>	Hard Disk <sup>3</sup>
<b>Fidelis Scout 2 VM Bundle including:</b>	<b>30</b>	<b>80 GB</b>	<b>350 GB</b>
CommandPost VM Appliance	8	24 GB	100 GB
Direct 1000 VM Appliance	14	24 GB <sup>4</sup>	50 GB
Collector SA VM Appliance	8	32 GB	200 GB <sup>5</sup>
Fidelis Endpoint	500 user license, customer installed with customer provided Windows License		

<sup>1</sup> Typically two vCPU per physical core CPU with hyperthreading enabled. Tests performed with CPU clock @ 2.8 Ghz. Results may vary with VM host resources.

<sup>2,3</sup> Minimum required

<sup>4</sup> Represents minimum RAM necessary to support Fidelis Insight Policies. Allocate more memory to support custom configurations.

<sup>5</sup> Fidelis Scout 2 Bundle supports a license up to 1TB of Collector Storage. Storage capacity in days varies per environment.

	Fidelis Portable Appliances	
	Scout 2 Elevate (FNA-SCOUT2-ELEVATE)	Scout 2 Elevate with Case (FNA-SCOUT2-ELEVATE-CASE-PERIP)
<b>Form Factor</b>	Ruggedized 1U Server	Ruggedized 1U Server Within Rugged Utility Case
<b>Peripherals Included</b>	No	KVM Adapter, Ethernet Switch, 2 6ft Ethernet Cables
<b>Fidelis Endpoint Included</b>	500 user licenses, field installed*	500 user licenses, field installed*
<b>Memory</b>	512 GB	512 GB
<b>Storage Capacity</b>	9.6 TB SSD storage	9.6 TB SSD storage
<b>Network Adapters</b>	4 x 1GbE	4 x 1GbE
<b>Out of Band Management</b>	iDRAC9 Enterprise	iDRAC9 Enterprise
<b>Dimensions</b>	19" (W) x 21.3" (L) x 1.68" (H)	23.52"(W) x 26.21" (L) x 8.65" (H)
<b>Weight (approx.)</b>	~12.7 kg (28 lb)	~14.1 kg (30 lb)
<b>Power Supply</b>	Dual, Hot Plug, Redundant Power Supply (1+1), 550W	Dual, Hot Plug, Redundant Power Supply (1+1), 550W
<b>Operating Temperature</b>	5°C to 45°C (41°F to 104°F)	5°C to 45°C (41°F to 104°F)
<b>AC Input Requirements</b>	115 ~ 230 V AC, auto ranging	115 ~ 230 V AC, auto ranging

This product includes a transportable hardware platform equipped as outlined above, and an option hard shell utility case. Software includes a VMware vSphere virtualization environment license and the Scout VM bundle software licenses as described above. The Fidelis Scout2 products are optimized and licensed for use in short-term assessments and investigations (not for long-term deployment on production networks).

### Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | [info@fidelissecurity.com](mailto: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](http://www.fidelissecurity.com).