DATASHEET

# Fidelis Elevate™

Platform That Empowers Security Teams to Detect, Hunt and Respond to Advanced Threats

## The Challenge

Increasingly advanced attacks evade preventive defenses making threat detection, hunting, and response critical as your last line of defense. Attacks make lateral movements within hours of initial compromise and learn new environments to quickly embed themselves deep within organizations' environments. Logs and events are not detecting these advanced threats, nor are existing platforms providing high-speed, interactive and iterative detection and investigation capabilities. Additionally, centralized alert monitoring infrastructure designed to address compliance issues is ill-prepared for today's detection, investigation, response, and hunting requirements.

What's missing is rich metadata with the content and context to drive threat detection and hunting from multiple sensors and endpoints in real-time and retrospectively, driven by multiple threat intelligence feeds. Metadata is also the foundation for machine-learning models and applying data science to security use cases.

## Fidelis Elevate Allows You to Engage the Attacker Prior to Impact

Fidelis Elevate™ empowers security analysts to know their environment better than attackers and to engage attackers prior to the point of impact. Regain the advantage with a streamlined security stack that maps your cyber terrain, including all managed and unmanaged assets, and aligns attacker TTPs to MITRE ATT&CK™ so you know their next move and what action to take.

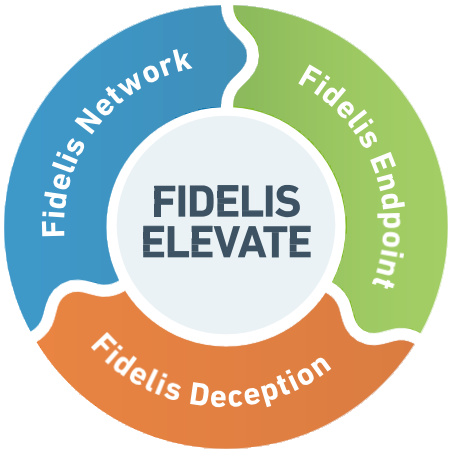
The Fidelis Elevate platform integrates network traffic analysis with endpoint detection and response and deception defenses, automates and orchestrates workflows, correlates rich metadata across these security layers, and leverages machine-learning to gain strong indicators of APTs and potential zero-days attacks. Now you can benefit from higher confidence detections and faster response.

Fidelis Elevate defenses focus on detection, forensics and response including:

- Real-time, customizable prevention and detection from multiple indicator sources, including endpoint behavior, network behavior, and sandboxing analysis
- Real-time, detailed response capabilities with optional automation
- Retrospective analysis that enables hunting via indicators, signatures, and machine-learning anomalies applied to rich metadata from sensors and endpoint metadata
- Deep Session Inspection® provides full session reassembly, protocol decoding, and full content analysis
- Deception layers for real OS VM decoys, IT asset and service decoys, enterprise IoT, and cloud VMs
- Integrated MITRE ATT&CK™ tags to identify techniques associated with recorded behaviors
- Threat intelligence from Fidelis Insight, plus OpenIOC, YARA, Suricata rules, and 3rd party feeds
- Managed Detection Response (MDR) services for 24/7 coverage leveraging Elevate
- Incident Response (IR) retainers and IR services for commercial and federal customer

## Fidelis Elevate Benefits

- Map your cyber terrain of assets and services, plus software inventory and known vulnerabilities
- Improve detection and response by adding rich metadata to your security infrastructure
- Enable machine-learning based defenses across multiple sensors, endpoints and deception layers
- Automate core security analyst tasks for detection, investigation and response to increase efficiency
- Validate alerts from sensors to endpoints and collect forensic evidence, including full disk images
- Empower threat hunting across sensor metadata and endpoint files, processes and event data
- Augment security operations with MDR and IR services



## Top Differentiators

### Fidelis Network®

- **Deep Session Inspection®:** provides full session reassembly, protocol and application decoding, recursive deep content decoding, and full content analysis to detect threats and data exfiltration.
- **Multiple Sensors:** for gateways, internal networks, cloud VMs, email, and web gateways providing full data visibility and collecting metadata of 300 plus attributes and custom tags for real-time and retrospective analysis.
- **Asset Profiling & Classification:** network sensors map cyber terrain including enterprise IoT, shadow IT, and legacy systems, plus importing external sources including Fidelis Endpoint.
- **Prevention and Detection:** using static, dynamic and retrospective defenses including machine learning anomalies, behavior analysis, sandboxing, multi-dimensional rules, emulation and heuristics, signatures, and threat intelligence feeds (Fidelis Insight, third party, shared, internal).
- **Data Theft and Loss:** using pre-defined policies, data profiling, metadata attributes and custom tags for DLP on network, web and email sensors including OCR image to text analysis.
- **Automation:** of prevention, detection, investigation and response for tier-1 security analyst tasks in a single UI of seamless workflows for network, endpoint, and deception defenses.

### Fidelis Endpoint®

- **Detection and Response:** robust EDR for Windows, macOS and Linux systems including behavior monitoring and detection by indicators (IOCs, YARA rules), on/off grid protection, system isolation, and proven forensic integrity with full disk imaging, files and folders, and memory capture.
- **Executable/Script Collection and Metadata:** for endpoint process and event data for 30, 60, or 90 days enabling automated and manual threat detection, hunting, and custom searches, plus first time seen executable files and scripts for analysis.
- **Installed Software and Known Vulnerabilities:** provides endpoint security hygiene for installed software with links to MITRE CVE and Microsoft KB vulnerability reports, plus OS state and applying patches, report and change FW and AV state, and alerts on USB insertion.
- **Live Console:** provides incident responders with direct, remote access into an endpoint's disk, files and processes, to more quickly mitigate threats found on an asset.
- **Script Library:** with hundreds of ready to use scripts for automated gathering of artifacts, response, or restoring endpoints, plus customization for ad hoc or unique customer requirements.
- **Threat Intelligence:** includes Fidelis Insight cloud-hosted sandboxing, machine learning analysis, behavioral indicator rules, and threat research. Also, custom behavior rules, open feeds for IOCs, YARA rules, and third-party TI feeds.
- **Prevention:** provides anti-malware for Windows powered by BitDefender or AV of customer choice. Process behavior blocking and process blocking by IOC or YARA rules run independently of AV engines.

### Fidelis Deception®

- **High Fidelity Alerts:** for cyber security research to learn TTPs and analyze files with real OS decoys, or as a smart alarm system using emulation decoys for no risk, plus supporting enterprise IoT and non-standard devices as decoys.
- **Automation and Scale:** provides discovery of environments to auto-generate decoys, distribute, test access and advertise decoys, plus auto-generate breadcrumbs for distribution to real systems to lure attacks.
- **Wide Choice of Decoys:** Real OS VM decoys, golden image OS decoys, emulated IT assets and services decoys, cloud VM decoys, enterprise IoT decoys, plus loading web pages to HTTP decoys and supporting file uploads into cloud-based sandbox analysis.
- **Traffic Analysis:** scales to enterprise performance levels to determine human traffic from automated malware traffic, detect anomalies and C2, plus provide profiling and classification of assets and services to continuously map environments for changes.
- **Adaptation and Freshness:** deception layers automatically adapt to environment changes, plus provide frequent logins to decoys, publish existence in ARP tables, query DNS servers, and fake accounts with frequent activity in Active Directory.

### On-Premises

- You maintain and manage all appliances, endpoints, and management software
- Fidelis professional services assists with deployment and training
- Available sensors: Direct, Mail, Internal, Cloud VM, and Web
- Maintenance includes intel updates from Fidelis Threat Research Team
- License additional appliances/sensors as your needs grow

### Cloud

- Infrastructure maintained by Fidelis including metadata, so you can focus on security
- Rapid deployment and immediate implementation of sensors, deception layers and endpoints
- Scale up as you grow with as many software sensors and endpoints as you need
- Uninterrupted service as you transition from a trial to production
- Simplified subscription based on bandwidth and storage needs

## Contact Us Today to Learn More

**Three Wire Cybersecurity | 703.776.9731 | info@threewiresys.com**