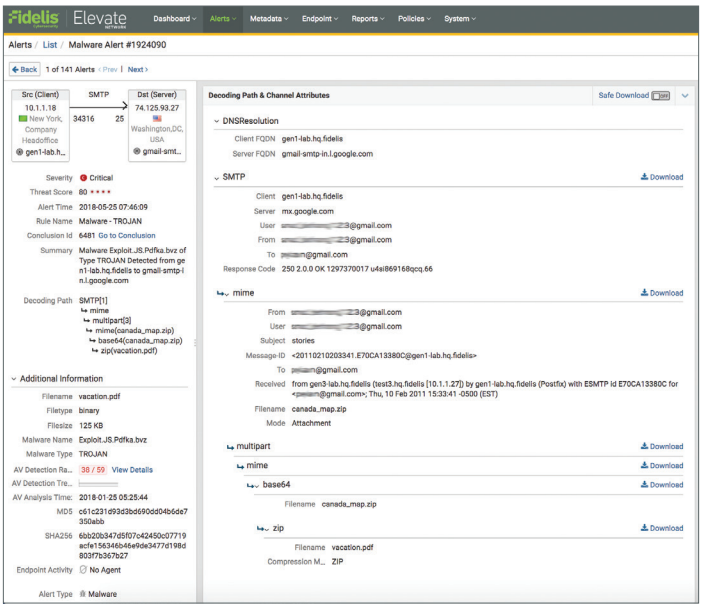
DATASHEET

Fidelis Network®

Ensure Best-of-Breed Breach Detection and Data Loss Prevention

Never Miss a Critical Attack

Enterprise security operations are complex, with siloed visibility across networks, endpoints, and cloud environments, combined with too many tools for understaffed and overwhelmed teams to manage. Security teams need bi-directional visibility into network traffic across all ports and protocols and need valuable metadata to analyze threats and data leakage. This comprehensive visibility combined with contextual threat intelligence leads to detections across the entire threat life cycle. This also allows organizations to respond quickly and effectively to malicious activity at every stage of the kill chain and mitigate data leakage and exfiltration.



Deep Session Inspection® extracts and decodes all data to give you full visibility of content and context. Shown here is the detection of an exploit buried deep within a pdf in a zip file.

Product Overview

Fidelis Network is a critical part of the Fidelis Elevate™ platform which automates threat detection and response while also mitigating data leakage. By integrating network visibility, data loss prevention, endpoint detection and response, and deception, Fidelis Elevate enables understaffed and overwhelmed security teams to focus on the most urgent threats and prevent data loss across the most complex networks.

Fidelis Network bi-directionally scans all network traffic regardless of port or protocol to reveal the network and application protocols, files, and content. Fidelis Network captures the complete content of any violating network communication for further investigation as well as capturing and storing metadata of all traffic for retrospective analysis.

Automated detection is achieved through real-time network analysis that reveals compromises at all stages of the attack lifecycle. Fidelis Network can also apply newly received threat intelligence to the stored metadata and detect attacks and data theft attempts that have happened in the past. This provides a unique perspective into the past and provides valuable insights to prevent such attacks in the future. By leveraging machine learning classifiers, auto generated domain names and frequent/rare values of any network attribute can be highlighted and exposed.

- **See More, Inspect More:** Fidelis Network scans all network traffic bi-directionally, regardless of port or protocol, to reveal the network and application protocols, files, and content.
- **Detect Threats and Data Theft in Progress:** By conducting real-time network analysis and identifying behaviors that indicate compromises, Fidelis Network provides automated detection for the proactive discovery of attackers, suspicious hosts, and malware.
- **Eliminate Alert Fatigue:** Fidelis Network automatically validates, correlates, and consolidates network alerts against every endpoint in your network. Minimize false positives and shift from clues to conclusions so you can quickly address the alerts that matter most.
- **Respond Faster to Breaches:** With added context around an investigation through real-time and retrospective analysis across the kill chain, Fidelis Network enables a faster, more effective response.

Gain full network visibility across all ports and protocols, detect threats, and prevent data loss.

Fidelis Network Capabilities

See What Others Miss

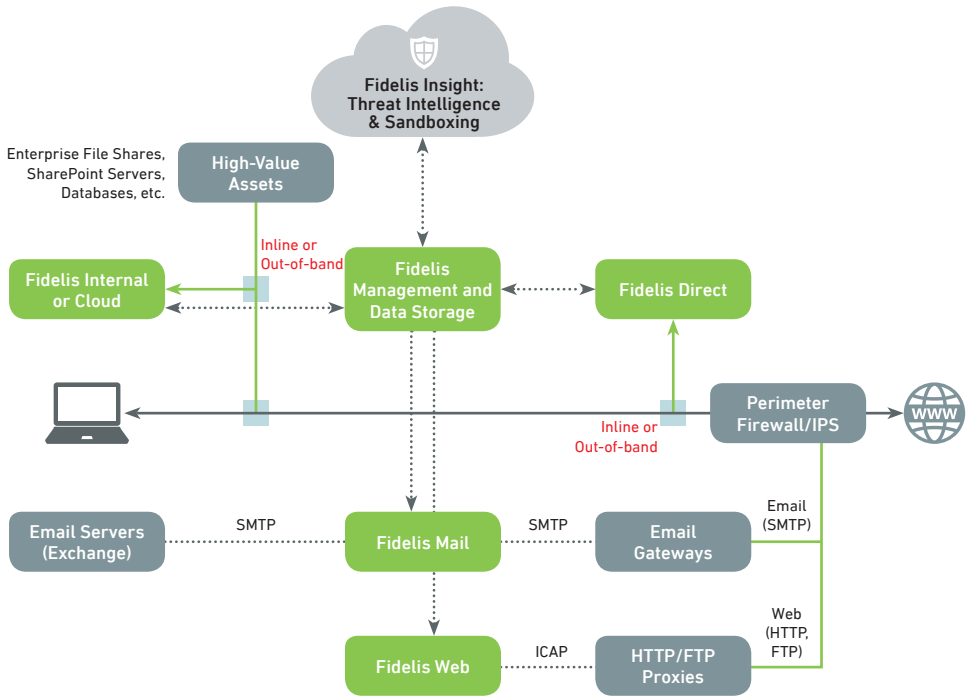
- Patented Deep Session Inspection® as well as Deep Packet Inspection gives you unique visibility across all ports and protocols
- By capturing and storing metadata from every network session, Fidelis Network provides rich information for automated and manual threat hunting
- Automatically decode and analyze traffic to detect and prevent threats and unauthorized data transfers

Automate Threat Detection and Prevention Across the Kill Chain

- Real-time network analysis enables you to uncover and block the initial compromise, suspicious hosts, malware, and compromised hosts
- Retroactively analyze stored metadata based on indicators derived from threat intelligence, machine learning, sandbox results, and Fidelis research
- Confirm and stop data theft by inspecting the content of all outgoing network activity

Quickly Reach Conclusions With Accuracy

- Reduce alert fatigue by automatically consolidating similar alerts and when combined with Fidelis Endpoint, network alerts are automatically validated and correlated against every endpoint



Fidelis Network Architecture

- Leverage multiple defense techniques to analyze suspicious network data, rich content, and files with pre-staged evidence displayed in one view for faster conclusions

Respond Faster to Breaches

- Gain more context around an investigation with real-time and retrospective analysis across the kill chain to ensure a faster, more effective response

Prevent Threats and Data Leakage Across the Network, Cloud, Email, and Web

- Fidelis Direct, Cloud and Internal sensors allow for the dropping of sessions
- The mail sensor enables the ability to quarantine, drop, re-route, and remove email attachments
- Through the web sensor, web pages can be redirected and/or sessions can be dropped

Benefits

- Reduce Theft of Assets & IP
- Reduce Overall Cost of Response
- Lower Disruption to Business
- Mitigate Risk to Reputation/Integrity
- Improve SOC Efficiency

Contact Us Today to Learn More About Fidelis

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis is the leader in automated detection and response. The Fidelis Elevate platform dramatically improves the effectiveness and efficiency of security operations by delivering comprehensive visibility, intelligent deception, alert validation, and automated response across network and endpoints. Fidelis is trusted by the most important brands in the world. See what you've been missing. For more information go to www.fidelissecurity.com.

