

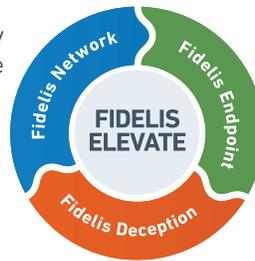
# Executive Summary

## Our Mission

Fidelis combats the full spectrum of cyber-crime and digital espionage by providing critical visibility across complex environments, automating inbound/insider threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy.

## Our Solution

**Fidelis Elevate™** is a unified platform built to arm security teams with the ability to quickly detect, hunt and respond to inbound and insider threats as well as data theft. The Elevate platform provides deep visibility while monitoring all traffic on all ports and all protocols across the entire infrastructure of corporate networks, clouds, endpoints and enterprise IoT environments. Fidelis provides analysts with conclusive evidence by automating the playbooks and tasks of an incident responder, while combining full visibility into content, metadata and sessions with extensive threat intelligence to automate detection and response. Specifically:



**Fidelis Network®** provides Network Traffic Analysis and Data Loss Prevention (DLP) capabilities that decode and analyze all network traffic using our patented Deep Session Inspection® technology. Fidelis Network sensors protect all ports and protocols in a single box with sensors that specialize in prevention of data loss via email and web traffic. Evidence of all network traffic is stored as rich metadata for use by automated analytics and human threat hunting. The metadata captured and stored by Fidelis Network goes well beyond Netflow because it includes details of every network transaction down to the names, hashes and properties of every file transferred – including those deeply embedded and obfuscated in archive and document formats. Fidelis Network was named as a Visionary by Gartner in their most recent Data Loss Prevention (DLP) Magic Quadrant. The same technology used to detect data theft is also used to detect and decode obfuscated malware hidden in plain sight.

**Fidelis Endpoint®** analyzes and records all endpoint events using a single agent that combines Endpoint Detection & Response (EDR) and Endpoint Protection Platform (EPP) technology into a highly effective threat hunting solution. Fidelis Endpoint delivers forensic and response capabilities that include investigation, prevention, visibility into all activity and systems management that are richer and more thorough than any other EDR product on the market. Our EPP technology is an effective first line of defense that can detect and prevent malicious and unwanted programs from executing.

**Fidelis Deception™** significantly reduces dwell time by providing a low-risk, low-friction internal alarm system to detect post-breach attacks and malicious insiders. Fidelis Deception automatically discovers and classifies all attached network assets, including enterprise IoT devices, while displaying all services and connectivity of each asset. With this information, Fidelis Deception creates fake assets (decoys) and uses breadcrumbs as lures on real systems to detect attackers' actions and lateral movements. High-fidelity alerts come from decoys, breadcrumbs, AD credentials, MITM, and poisoned data with network traffic analysis and telemetry data for investigations. Lastly, Fidelis Deception automatically adapts the deception environment to network changes as they occur to remain synchronized for assets, resources, and services.

Relied on by:

**40+** US government agencies and departments

Commercial business across the globe, including:

**12** of the Fortune 50

**24** of the Fortune 100

### Solution Areas include:

- Network Threat Detection & Response
- Network Data Loss Prevention
- Endpoint Detection & Response
- Endpoint Protection
- Deception
- Threat Hunting
- Managed Detection & Response
- Incident Response Services
- Cybersecurity Assessments

**Fidelis Insight** includes curated threat intelligence from leading 3rd parties as well as customer-defined intel, integrated sandboxing, and machine-learning algorithms to extract Indicators of Compromise (IoCs) and deploy highly accurate detection rules across all Fidelis-secured networks, clouds and endpoints.

## Your Force Multiplier

Fidelis Elevate integrates Network, Endpoint, and Deception technologies to answer the question, "What would an experienced threat analyst do in response to an alert?". Fidelis leverages the experience of our Threat Research team, Incident Responders, and Professional Services Teams, to:

- Automate alert triage and validation by analyzing endpoint activity before and after evidence of network malware or DLP
- Provide an execution report from our sandbox based on any malicious activity
- Visually represent activity that shows kill chains, insider threats, decoy interactions, and the context and story behind every alert

Fidelis Elevate also delivers "Conclusions", which provide a unique way to display related activities over time. Rather than having to constantly review individual alerts, Conclusions provide the ability to cluster alerts together as evidence of real threats. Conclusions expose all of the needles in a haystack doing the same or similar things, thus allowing security teams to focus on threat remediation based on validated, high-fidelity detections rather than triaging thousands of alerts and log files every day.

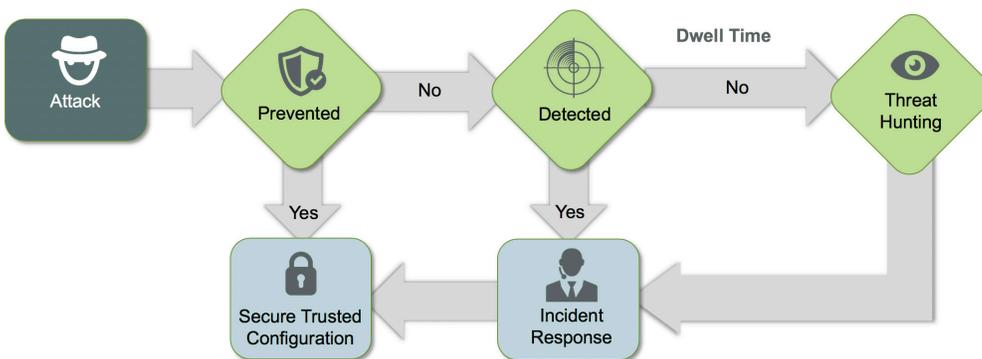
## Fidelis MDR

With the Fidelis Managed Detection and Response (MDR) service, organizations now have a reliable security partner that can hunt your environment for threats and data loss or can augment your existing SOC for threat hunting. Our experienced incident responders and threat hunters are former US Government Intelligence Community analysts and DoD Cyber Warriors. They will manage the Fidelis Elevate platform on your behalf and drive the Fidelis solution to its fullest potential.

## FIDELIS — YOUR LAST LINE OF DEFENSE

When advanced threats bypass your preventive defenses, Fidelis is there to help you detect, hunt for and respond – with speed, accuracy and certainty.

### Reduce the Dwell Time of an Attack



### DEEP VISIBILITY

- See across all traffic, all ports, all protocols, lateral movement and all endpoint activity
- Discover and classify all network assets, including enterprise IoT
- Decode and analyze embedded sessions with patented Deep Session Inspection®
- Inspect all content flowing over the network – from both threat and data loss perspective



### ACCURATE DETECTION

- Capture and store all metadata for real-time and retrospective analysis
- Detect advanced threats quickly and with high accuracy via curated threat intelligence, integrated sandboxing, machine learning algorithms to extract IoCs, and AV
- Automatically validate, consolidate, and correlate network alerts against every endpoint



### FASTER RESPONSE

- Automate response - isolate the endpoint, rollback to previous snapshot, CVE scanning, jumpstart playbooks, and more
- Confirm and stop data theft by content inspection of all outgoing network activity

## 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).