SOLUTION BRIEF

# Fidelis Elevate®

## An Active XDR Platform

Security is as dynamic as the modern computing infrastructures it protects. As fast as environments change, the threat landscape changes even faster, with more sophisticated adversaries, new attack tactics, and continually emerging vulnerabilities.

Fidelis Elevate® is an industry-first Active XDR (eXtended Detection and Response) platform purpose-built for proactive cyber defense so security teams can detect and neutralize adversaries faster. It unifies deception technologies with detection and response on endpoint (EDR), network (NDR), and cloud, making it easier for SOC analysts to quickly find and stop advanced cyber threats and reduce the dwell times that can lead to more significant damage.

Fidelis Elevate provides rich contextual insights and visibility across the entire IT environment. Deception technologies enable users to reshape the cyber terrain to engage with and defeat adversaries earlier in the attack lifecycle. Threat intelligence and insights help users get ahead of adversaries and prevent future attacks.

Fidelis Elevate stores metadata, allowing for a simple query to search through the past to determine if systems were successfully exploited through newly identified attack campaigns. Historical metadata enables the security team to track the attacker's movements, determine what other systems were compromised, eject the attacker, and restore business operations.

### Fidelis Endpoint

Safeguard devices on and off network with unmatched investigations, forensics and response

### Fidelis Network

Detect and respond faster to threats anywhere on the network including email

### Fidelis Deception

Reshape the attack surface and lure, detect, and defend earlier in the attack lifecycle

### Get Ahead of Adversaries with Full Situational Awareness

Cyber terrain knowledge helps defenders better protect their environment. Fidelis Elevate unifies advanced technologies to provide contextual visibility and dynamic cyber terrain mapping across managed and unmanaged endpoints, network traffic, and cloud assets and services. This helps security analysts quickly detect and block attacks, perform Deep Session Inspection®/ analysis of the environment to assess whether any systems have been compromised, and quickly return impacted systems to normal business operations. Fidelis Elevate provides:

- Complete terrain mapping and risk analysis that eliminates blind spots and closes security gaps.
- 360-degree insights collected from all data sources.
- Comprehensive, contextual visibility across the entire IT environment.
- Deep network visibility into embedded content, including encrypted traffic, inbound and outbound, across all ports and protocols.
- Visibility into user and computer behaviors over every process with forensic ability over system memory and file systems.
- Vulnerability and real time monitoring of managed and unmanaged devices on your networks.
- North-south traffic detection, lateral movement and data exfiltration.

### Accelerate the Decision and Response Cycle

Fidelis Elevate improves the accuracy and actionability of alerts and allows SOC teams to operate inside the adversary's OODA (observe, orient, decide, act) loop to detect and respond to advanced threats at line speed. With Fidelis Elevate, users can:

- Actively detect and validate malware enterprise-wide.
- Make faster, more informed decisions with contextualized data.
- Better triage issues with endpoint data integrated with network feeds.
- Automate playbooks with streamlined analysis.
- Implement response actions with accurate and correct data that fuel better decisions.

- Drastically reduce attacker dwell-time and damage with real-time and retrospective analyses using stored metadata.

### Engage Adversaries Before They Stop Business

Deception technologies in Fidelis Elevate enable security teams to reshape the cyber terrain, trap adversaries, and more quickly find, neutralize, and defeat advanced cyber threats. Users can:

- Proactively fortify defenses, including Risk Simulation from red and blue perspectives that provide insight into security weak spots.
- Detect attacks earlier with greater confidence and fewer false positives using threat and behavior-based analytics.
- Fuel faster detection and response with robust threat intelligence.
- Better understand potential avenues of attack through Attack Path Risk Simulation.
- Dynamically control and manage the entire attack surface with industry-leading Deception technology.

### Respond with Automated Actions

Adversaries can infiltrate a network and establish a foothold within minutes. Automated response to detections gives defenders tools to work within the same time frame. Response can be on the network, via packet drops and email quarantine, but must also include reaction at the compromised host. Sometimes, immediate analyst response is required when an automated playbook is either insufficient or unavailable. Fidelis Elevate provides:

- Automated playbooks that react to detections with scripts for investigative, disruptive, and remediation actions.
- Playbook reactions based on detections that come from NDR, EDR, Deception, and email platform capabilities.
- More than 100 scripts with support for Windows, Linux, and Mac systems.
- Custom scripts to increase reactions, created by analysts on site or by copying from our Fidelis Hero user sharing site.
- A console interface to all managed hosts, with a process viewer and a file interface so analysts can perform any required action and script those actions making them repeatable over other hosts.

### Gain an Advantage with Platform Intelligence that Learns and Grows

With Fidelis Elevate, security teams can counter current threats and better prepare for future attacks. A continuous process of investigation and discovery provides insights needed to tune defenses and neutralize threats before they do business damage. Fidelis Elevate makes it easy for user to:

- Automatically deploy threat intelligence.
- Lure and distract adversaries with decoys, breadcrumbs and traps.
- Actively analyze decoy activity and understand activity origin and tactics, techniques, and procedures (TTPs).
- Turn detections into IOCs.
- Easily identify and respond to resurfaced attacks.
- Automate responses to prevent an attack from resurfacing.

### Leverage Existing Security Investments

Fidelis Elevate was designed to be sold as an integrated proactive cyber defense platform. For those who wish to leverage existing investments, Fidelis Elevate also integrates with many third-party solutions to provide an interface into security solutions and workflows that may already be part of a security stack.

## Put Fidelis Elevate to Work Today

Learn how to better protect your organization across endpoints, network to cloud with Fidelis Elevate. Please visit FidelisSecurity.com for details and a no-cost demonstration.

### Think Like A CISO

A CISO's job often involves constantly monitoring improvements over time and looking for a positive trend, such as improving security, speeding mean-time-to-detection or -response, and decreasing risk over time. To create a security posture that bolsters an enterprise against adversaries, a CISO weighs three questions every day:

**Am I more secure today than I was yesterday?**

The Fidelis Elevate platform provides continual threat assessments and risk evaluations. Constant evaluation helps identify weaknesses, fortify enterprise security, demonstrate improvements to security over time, and help quantify the ROI associated with specific security initiatives.

**Am I currently under attack? If so, what is the impact?**

Active with Fidelis Elevate reduces alert fatigue and false alarms by enabling alerts to be consolidated, correlated, and prioritized across the IT environment. The result is high-confidence, actionable alerts that point to threats most likely to impact the enterprise. Get the context and investigative tools to quickly validate alerts, contain and mitigate the threat, and minimize impact to business operations.

**Was I exposed to the most recent threat? If so, what is the impact?**

Each new threat — supply chain compromises, ransomware attacks, and more — exposes new indicators of compromise (IOCs) and launches a scramble to determine if an enterprise was compromised. Easily determine whether you were exposed, and answer critical Who, What, Where, When, and How questions.

## Contact Us Today to Learn More

**Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com**

Fidelis Cybersecurity

Fidelis Cybersecurity, the industry innovator in proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via rich, dynamic cyber terrain mapping and multi-faceted context and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. With Fidelis, organizations emerge stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit www.fidelissecurity.com