

SOLUTION BRIEF

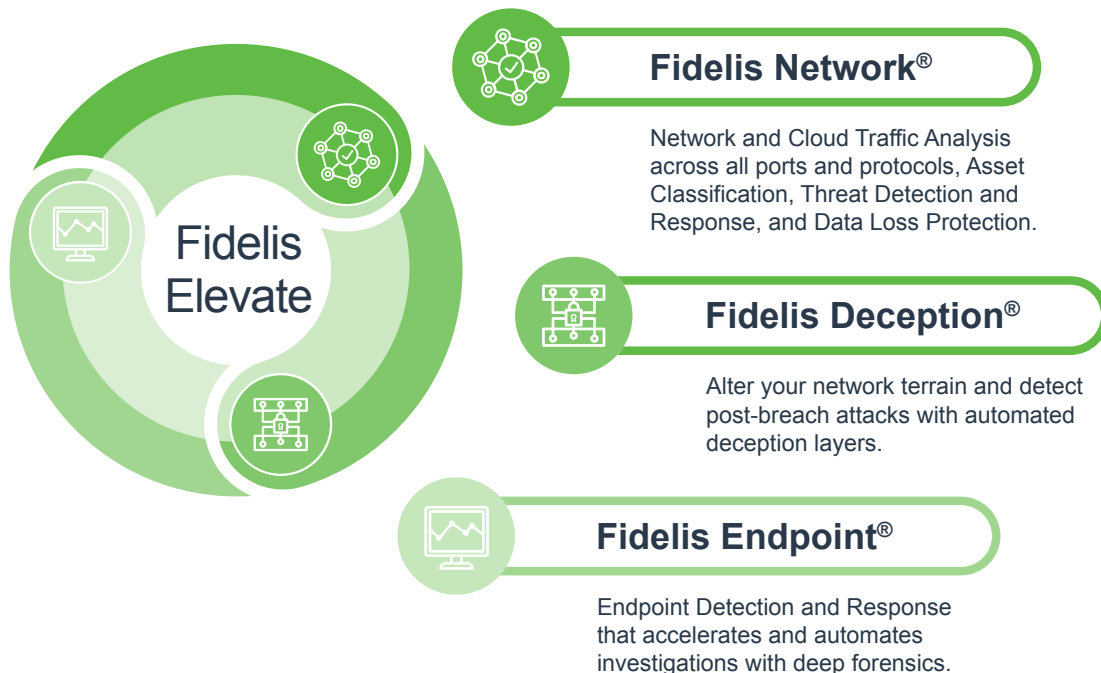
Fidelis Elevate®

Stop Cyber Adversaries Before They Stop Business Operations

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 attacks, new tactics, and continually emerging vulnerabilities and exploits.

Fidelis Elevate® is an industry-first open and extensible Active XDR (eXtended Detection and Response) platform purpose-built for proactive cyber defense. With Fidelis Elevate, security teams can detect and neutralize adversaries faster. It uniquely 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 significant business damage.

With Fidelis Elevate, security teams gain access to rich, contextual metadata, allowing for powerful real-time and retrospective analysis. Integrated deception technologies enable users to reshape the cyber terrain to engage with and defeat adversaries earlier in the attack lifecycle. And high-fidelity alerts, coupled with context and content, provide the means to track attackers' movements faster, hunt for threats better, and eradicate adversaries from endpoints, networks, and cloud. This allows cyber defenders to rapidly restore business operations and prevent future attacks, all from the single Fidelis Elevate CommandPost.



Neutralize Threats Faster

The more defenders know their cyber terrain, the better they can protect their environment. However, with distributed networks, data sprawl, and the proliferation of remote workforces, it can feel impossible to keep up with the changing cyber terrain and shifting attack vectors. 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. With Fidelis Elevate, users can:

- Gain holistic visibility with context across the entire IT landscape with complete terrain mapping and risk analysis
- Monitor data in real-time, continuously, including north-south traffic, lateral movement, and data exfiltration attempts.
- Automate retrospective analysis against current threats.
- Detect and hunt for threats across network, endpoints, and cloud with a single platform.
- Stop attacks at the point of entry, including on- and off-network devices, email, web gateways, and more.
- Automate responses and custom playbooks to shrink the time between detection and response.

Limit Your Exposure

The goal is to stop adversaries before they breach your systems—but that is not always realistic. Fidelis Elevate limits exposure in post-breach incidents by accelerating detection and response, luring and trapping adversaries within convincing deception layers, and providing powerful threat hunting, incident response, and forensic analysis capabilities so SOC teams can eradicate attackers and continually improve defenses. With Fidelis Elevate, users can:

- Hunt for threats, conduct deep forensics, gain actionable insights, and respond to incidents with a single platform.
- Rely on rich, indexable metadata, at both the content and context levels, for more granular threat profiling, classification, and hunting.
- Prevent new attacks from being successful with custom scripts and playbooks based on previous incidents
- Detect threats at any point along the kill chain
- Improve security team efficiency and effectiveness by enabling users to quickly and easily take advantage of provided visibility and workflows.

Think Like A CISO

A CISO's job often involves constantly monitoring improvements and decreasing risk over time. This means looking for a positive trend, such as reducing breaches or speeding mean-time-to-detection or -response. 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, and demonstrate improvements to security over time. It also helps quantify the ROI associated with specific security initiatives.

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

Fidelis Elevate provides high-confidence, actionable alerts that point to threats most likely to impact the enterprise. With rich context and investigative tools, and correlated data from network, endpoint, and deception, SOC teams can quickly validate alerts, identify and mitigate active threats, 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. The Fidelis Elevate platform demonstrates whether you were exposed, and answers critical Who, What, Where, When, and How questions.

Discover Hidden Threats

With the overwhelming complexity of modern networks, adversaries dwell undetected for days, weeks, and even months. They learn systems, explore user privileges, and find lucrative data before springing their trap. Fidelis Elevate helps defenders discover adversaries faster, shrinking the time between detection and response from weeks and months to hours and minutes. With Fidelis Elevate, users can:

- Create realistic deception layers based on real assets that lure and trap adversaries, while providing actionable alerts to SOC teams that pinpoint the attacker's location.
- Visualize cyber terrain and understand risk with real-time, bi-directional traffic monitoring across all ports and protocols.
- Find embedded threats deep within files with patented Deep Session Inspection®.

Stop Data Loss

In today's data-driven environments, robust data protection is imperative. Fidelis Elevate protects data where it resides, as it is used, and as it moves across, into, and out of your network. And with integrated deception technology, Fidelis Elevate takes data protection further by automatically generating decoys and breadcrumbs to lure attackers away from your most valuable assets. With Fidelis Elevate, users can:

- Increase network, endpoint, and cloud visibility to protect data wherever it resides.
- Automatically discover and classify data and tag content.
- Understand why and how data moves to detect behavior anomalies faster.
- Stop sessions that violate DLP policies and gain retrospective threat detection to continually fortify defenses against data loss.
- Detect ransomware attempts prior to execution and remove adversaries from the network before damage is done.

Gain an Intelligent Advantage

Counter current threats and better prepare for future attacks with Fidelis Elevate. It enables a continuous process of investigation and discovery that provides insights needed to tune defenses and neutralize threats before they do business damage. Fidelis Elevate delivers intelligence that learns and grows, making it easier for users to:

- Automatically deploy threat intelligence to counter the latest attacks—including zero-day threats.
- Continually alter the deception layer so that it lures even the most sophisticated adversaries.
- Actively analyze decoy activity and understand activity origin and tactics, techniques, and procedures (TTPs).
- Turn detections into indicators of compromise (IOCs) and accelerate response with fewer false positives.
- Easily identify and respond to resurfaced attacks.
- Automate responses to prevent an attack from resurfacing.
- Constantly evaluate the security risk of every asset in your network and cloud infrastructure.

Leverage Existing Security Investments

Fidelis Elevate is an open and active cyber security platform that is made to provide holistic, unified security while also integrating seamlessly with leading solutions. For those who wish to leverage existing investments, Fidelis Elevate integrates with many third-party solutions and provides a full-featured API. As an integrated part of your security stack, Fidelis Elevate helps you find the risks that other tools miss.

See Fidelis Elevate in Action

Learn how Fidelis Elevate helps better protection organizations from endpoints, across networks, and into clouds by [scheduling a demo](#). Learn more about the features and capabilities that make Fidelis Elevate unique by reading the [datasheet](#).

About 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 deep, dynamic visibility and asset discovery, 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

