SOLUTION BRIEF

Fidelis Endpoint®

Shrink the Time Between Detection and Response

Endpoints provide an ever-expanding selection of entry points for adversaries and failure points that are prone to human error. Once a single endpoint is compromised, it gives adversaries a foothold for lateral movement, ransomware, data exfiltration, and deeper compromise. With unknown zero-day threats and vulnerabilities, malware, malicious insiders, and increasingly complex distributed computing environments, endpoint threat detection isn’t enough. Protecting your enterprise requires rapid response to emerging threats through a combination of automated, scripted, and manual methods, along with data-driven intelligence, to uncover vulnerabilities, analyze systems, and thwart attacks at the endpoint before damage is done to your organization.

Fidelis Endpoint

Fidelis Endpoint® provides comprehensive visibility, detection, and response across all endpoints on and off the network to help you get ahead of threats and stop attacks earlier. Fidelis Endpoint’s single-agent architecture features real-time monitoring and response and retrospective analysis of endpoint behaviors for Windows, Mac, and Linux systems to automatically detect and alert on threat indicators and allow you to take decisive action. This way, you can speed investigations and better protect your organization from adversaries, malicious insiders, and malware.

Endpoint Use Cases

- Monitor behavior for suspicious patterns
- Detect and respond proactively to malware and ransomware
- Respond to threats at endpoints manually, scripted, or automatically
- Protect assets on and off the network
- Detect lateral movement originating at the endpoint
- Gain hands-on control of endpoints for investigation
- Unify endpoint security for Windows, MacOS, and Linux
- Scale endpoint protection in rapidly growing environments

Fidelis Endpoint provides detections (red), response (blue), and third-party intelligence and integration (yellow) in a single agent with on/off grid defenses.
SOLUTION BRIEF

Fidelis Endpoint®

How Endpoint Works
Detection without response does not stop the threat. Fidelis Endpoint automates detection and response, while providing secure, remote access into an endpoint’s disk, files, and processes. This shrinks the time between detection and response. At the moment of detection, Fidelis Endpoint can isolate the compromised endpoint, collect comprehensive forensic data, integrate with SOAR platforms, compare against threat intelligence feeds and known vulnerabilities, and give you hands-on endpoint access to put you in proactive control of threat defense.

Extensive and extensible endpoint protection
Anything you can run on an endpoint, you can trigger with manual control, scripts, or through SOAR integration.

- Gain direct, remote access into disks, files, registries, and processes to quickly respond to threats as if you were physically sitting at the endpoint
- Automate responses using the predefined IOC and Yara library or quickly and easily create and customize your own rules
- Update rules on the fly to adapt your response to complex attack TTPs
- Integrate with SOARs and SIEMs to aggregate data from external tools and execute response actions
- Get comprehensive platform visibility and protection by connecting with Fidelis Network and Fidelis Deception

Real-time and retrospective response and forensic analysis
Gather extensive information on running processes, installed software, known vulnerabilities, and system status to automate endpoint isolation and accelerate attack response.

- Get definitive answers to how attackers breached your endpoints, what they did while they were inside, and whether they still have hooks into your systems
- Automatically isolate endpoints and begin collecting forensic data immediately upon threat detection
- Access open threat intelligence feeds from third-party sources, internally developed, and from Fidelis Insight (including sandboxing, machine learning, and threat research) and assign intelligence feed sets to endpoint groups
- Filter and sort on endpoint attributes and get granular intelligence that helps uncover anomalies faster and with greater accuracy
- Safely identify malicious executables with the integrated cloud sandbox
- Determine the extensiveness and risk of present issues by analyzing past behavior patterns, with historical data aggregation for 30-, 60-, or 90-day windows
- Map endpoint behaviors to MITRE ATT&CK to understand attacker TTPs
- Play back key events and review the timeline of suspected incidents

Key Benefits

Detect Faster
Gain active, deep visibility into all endpoint activity in real-time and retrospectively so you can speed investigations and automate response.

Gain Control Over Endpoints
Find and stop adversaries at the point of entry with a single-agent architecture that runs on and off-grid defenses, provides automated, scripted, and manual response, and works seamlessly with integrated deception technology.

Conduct Live Investigations
Use Fidelis Live Console to speed up incident response (IR) and quickly gather information with the click of a button, as if you’re on the endpoint, with full access to registries, processes, files, disks, etc.

Respond with Intelligence
Map endpoint detections to the MITRE ATT&CK framework to understand attacker TTPs, determine the best mitigation strategy, and analyze event data in real-time or retrospectively to improve future responses.

End Alert Fatigue
Automate time-consuming security tasks and common responses with playbooks and scripts and receive high-fidelity alerts for issues that demand immediate attention and pose immediate risk.
Fidelis Endpoint: Proactive Endpoint Response and Detection

Sold alone or as part of the Fidelis Elevate® Active XDR platform, Fidelis Endpoint is part of a proactive cyber defense solution that simplifies threat hunting, detection, and response to neutralize threats faster. With Elevate, Endpoint provides multiple ways to respond to threats at the endpoint, whether they originate from the endpoint itself, or if they’re identified by Fidelis Network or Deception as part of the Fidelis Elevate Active XDR platform.

Fidelis provides contextual visibility across the entire cyber terrain. Fidelis Elevate is an open and extensible Active XDR platform that enables SOC analysts to proactively find and stop threats before they impact business. Elevate unifies deception technologies with detection and response on endpoint (EDR), network (NDR), and cloud applications and services. Aligned with MITRE ATT&CK and Engage (formerly Shield) frameworks, Fidelis Elevate provides contextual visibility and rich cyber terrain mapping across endpoint, network, and cloud. This helps SOC analysts quickly detect and block attacks, perform deep inspection/analysis of the environment to assess whether any systems have been compromised, and return impacted systems to normal business operations as quickly as possible. They form a foundation of intelligence that keeps you ahead of the next attack.