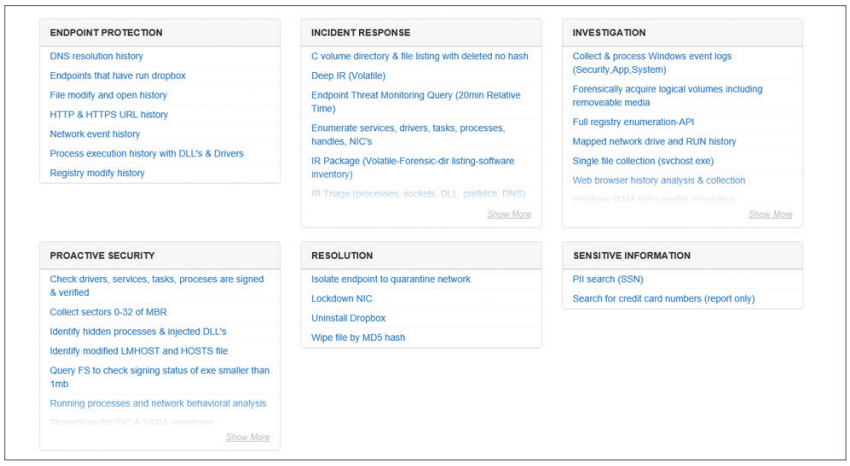
DATASHEET

Fidelis Endpoint™

Identify compromised endpoints and automate your investigation and response.

Focus on the Incidents That Matter

Organisations invest millions to build secure networks and keep highly motivated attackers out of their enterprises. Despite these investments, determined attackers routinely compromise seemingly secure organisations and steal their intellectual property, private data and financial information. Analysts in security operations centres (SOCs) and security teams, tasked with reviewing and prioritising suspected incidents, are overwhelmed by the sheer volume of alerts. They have no way to quickly validate whether a suspected incident is real and receive little context on the potential impact.



Enable front-line security teams to quickly validate a suspected incident and receive context on its severity and potential impact.

Product Overview

Fidelis Endpoint™ equips security-conscious organisations to confidently respond to, validate and resolve security incidents in a fraction of the time it takes using traditional approaches. Security teams receive the visibility, context and automation they need to:

- **Identify and Stop Targeted Attacks Just as They Are Beginning.** Quickly identify malicious behavior, validate threats based on multiple criteria, automate remediation and analysis workflows, and proactively hunt for threats.
- **Correlate Activity With Other Security Tools:** Effectively assess and validate alerts generated by existing security products, such as network-based security solutions or SIEMs, so you can focus on real threats and take action within moments of notification.
- **Make Faster, Better Informed Decisions:** Automate incident response processes, apply threat analytics and get deep visibility into malicious activity wherever it happens.
- **Reduce the Time to Resolve Incidents:** Automate complex and time consuming manual workflows, apply intelligence and context to alerts, and use key security performance metrics — including Mean Time to Validate (MTV) and Mean Time to Respond (MTR) — to track and report on incidents.

Highlights

Advanced Forensic Capability: Capture and analyse live response data, memory and full disk images. Perform in-depth analysis to uncover all the forensic data via the agent.

Endpoint Threat Alerting: Automatically detect when a threat indicator (IP address, DNS, process name, URL, MD5) exists on an endpoint and automatically initiate a pre-configured response action.

Off-Network Support: Monitor endpoints no matter where they are (on or off the network) to ensure all endpoints in your organisation are covered.

Integration with Existing Security Tools: Seamlessly integrate with SIEMs, next-generation firewalls, alerting tools and other monitoring devices to automatically validate alerts and begin remediation activities.

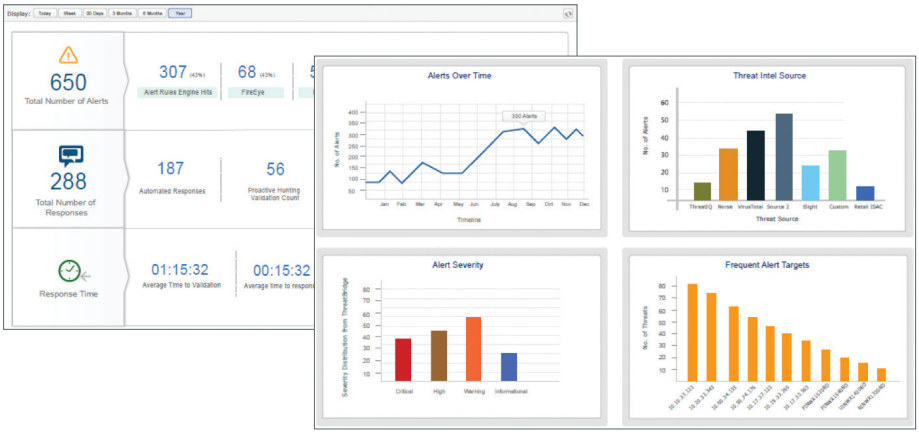
Mobile Threat Detection and Response: Monitor connections to websites and social media and perform real-time metadata collection and analysis on mobile devices (iOS and Android).

Threat Intelligence: Import threat intelligence from commercial feeds, as well as open source and internally developed threat intelligence, to automatically detect and validate threats on endpoints.

Accelerate the triage and validation of suspected incidents by eliminating time-consuming manual investigation steps that require highly skilled and hard-to-find security experts.

About Fidelis Endpoint

- **Eliminate Blind Spots:** Identify threats as they happen no matter where they are in your environment — network, endpoint (on and off the network) or mobile.
- **Respond Immediately:** Integrate SIEMs, next-generation firewalls, alerting tools with endpoints to automatically link disparate information and enable top-to-bottom visibility and effective response.
- **Identify Compromised Endpoints:** Automatically sweep all endpoints for signs of the compromise once an Indicator of Compromise (IOC) has been validated.
- **Proactively Hunt for Threats:** Apply network- or host-based intelligence in any format, from simple to complex, to rapidly identify compromised endpoints and automatically take action.
- **Accelerate Triage and Validation of Suspected Incidents:** Automatically harvest rich system information from endpoints and correlate against threat reputation services, advanced threat detectors and threat intelligence to confirm when endpoints are compromised — without the use of multiple point products or analyst's time.



Use key security performance metrics, such as Mean Time to Validate (MTV) and Mean Time to Respond (MTR), to track and report on incidents.

- **Know What Happened Using Playback:** Fully expose how an attack happened, what was taken and who else was involved — well after the initial compromise has occurred — by recording key events (such as file, processes, registry, network, DNS and URL) and automatically delivering a timeline related to a suspected incident along with the prioritised alerts.
- **Automatically Remediate and Take Action on Impacted Endpoints:** Immediately halt data exfiltration and lateral movement from endpoints using endpoint isolation, process halting, file wiping, kicking off a script to initiate an anti-virus scan or custom scripted routines on the endpoints.
- **Automate Incident Response Workflows:** Easily create and customise response workflows specific to the organisation. Automatically kick off remediation or deep analysis actions by defining trigger rules and actions with the alert response workflow engine.

"A major benefit of introducing Fidelis Endpoint is that we are now able to manage our own incident response in-house. This has enabled us to dramatically improve cyber incident response times from ten days to five hours."

– Director of Forensics and eDiscovery, Top Five Global Bank

Benefits

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

Contact Us Today to Learn More About Fidelis

Fidelis Cybersecurity | +44 (0) 203 021 2500 | info@fidelissecurity.com

Fidelis Cybersecurity protects the world's most sensitive data. We reduce the time it takes to detect attacks and resolve security incidents. With Fidelis you'll know when you're being attacked, you can retrace attackers' footprints and prevent data theft.

