DATASHEET

Fidelis Endpoint®

Shrink the Time Between Detection and Response

Fidelis Endpoint provides deep visibility into managed and unmanaged endpoint activity on the network. It delivers enhanced prevention, effective detection, vulnerability analysis, and automated response, enabling security analysts to remediate threats faster and more effectively. Fidelis allows you to see all endpoint activity across Windows, Mac, and Linux systems, gaining unmatched insight through the collection of all installed software, executable files, and scripts.

How Endpoint Works

Detection without response does not stop a threat. Fidelis Endpoint maximizes efficiency by automating detection and response and providing secure, remote access into an endpoint's disk, files, and processes. Upon detection, Fidelis Endpoint can isolate a compromised endpoint, collect comprehensive forensic data, integrate with SIEM and 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.

Visibility and Detection

Fidelis Endpoint provides deep visibility into all endpoint activity to enable analysts to detect and respond to advanced threats immediately. The Fidelis Endpoint agent is a lightweight process that captures metadata for every process and child process, including behaviors, registry changes, files created, modified, and deleted, and network activity. Detections occur in real time as each process is monitored and can trigger a response which may include termination of malicious
processes, isolation of the endpoint, forensic analysis, and many other actions.

Fidelis gives you access to open threat intelligence feeds from third-party sources, internally developed, and from Fidelis Insight (including sandboxing, machine learning, and threat research) and assigns intelligence feed sets to endpoint groups. The combination of visibility and threat intelligence provides detection of even the most advanced attacks.

Fidelis Endpoint will also create a catalog of all installed software plus any file or script that is executed. This collection of data provides vulnerability analysis, sandboxing of suspicious files, and the ability to hunt for threats across enterprise. Whether your enterprise includes a hundred endpoints or hundreds of thousands, visibility into processes, files, and vulnerabilities is at your fingertips ready to detect threats and trigger a response.

Forensics, Response and Prevention

Fidelis provides real-time and retrospective forensic analysis and response, giving definitive answers to how an adversary breached your endpoints in the first place, their actions once inside, and whether they still have their hooks in your systems. An automated response can be triggered by detections from the endpoint or from external detections when used with the SOAR interface. Fidelis Endpoint ships with well over 100 response scripts that cover Windows, Linux, and Mac. Fidelis Endpoint allows you to customize and add scripts easily to adapt a response to fit your workflow needs.

Response scripts include investigative, forensic, and destructive use cases.

Investigative: Analysis of which users were logged in, process ownership, and log collection. Investigative scripts can collect data immediately following a detection, allowing your analyst to collect information within the seconds between the detection and when the analysts logs into the console.

Forensics: Forensics: Analysis, file collection, and network log collection, providing data at the time of the detection as opposed to minutes later when the attacker may have already removed evidence to cover their tracks.

Destructive: Endpoint isolation (allowing you to investigate while eliminating lateral propagation), file deletion, and registry changes.

When necessary, manual response is easy. Fidelis provides direct, remote access into disks, files, registries, and processes to quickly respond to threats as if you were physically sitting at the endpoint, shrinking the mean time between detection and response.

Response also comes in the form of prevention. By using acombination of known malware file hashes and behaviors, malicious processes can be quarantined before execution and stopped when malicious process behaviors are detected.

Key advantages:

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: Speed up incident response (IR) wtih Fidelis Live Console and quickly gather information with the click of a button, as if you are on the endpoint, with full access to registries, processes, files, disks, etc.

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

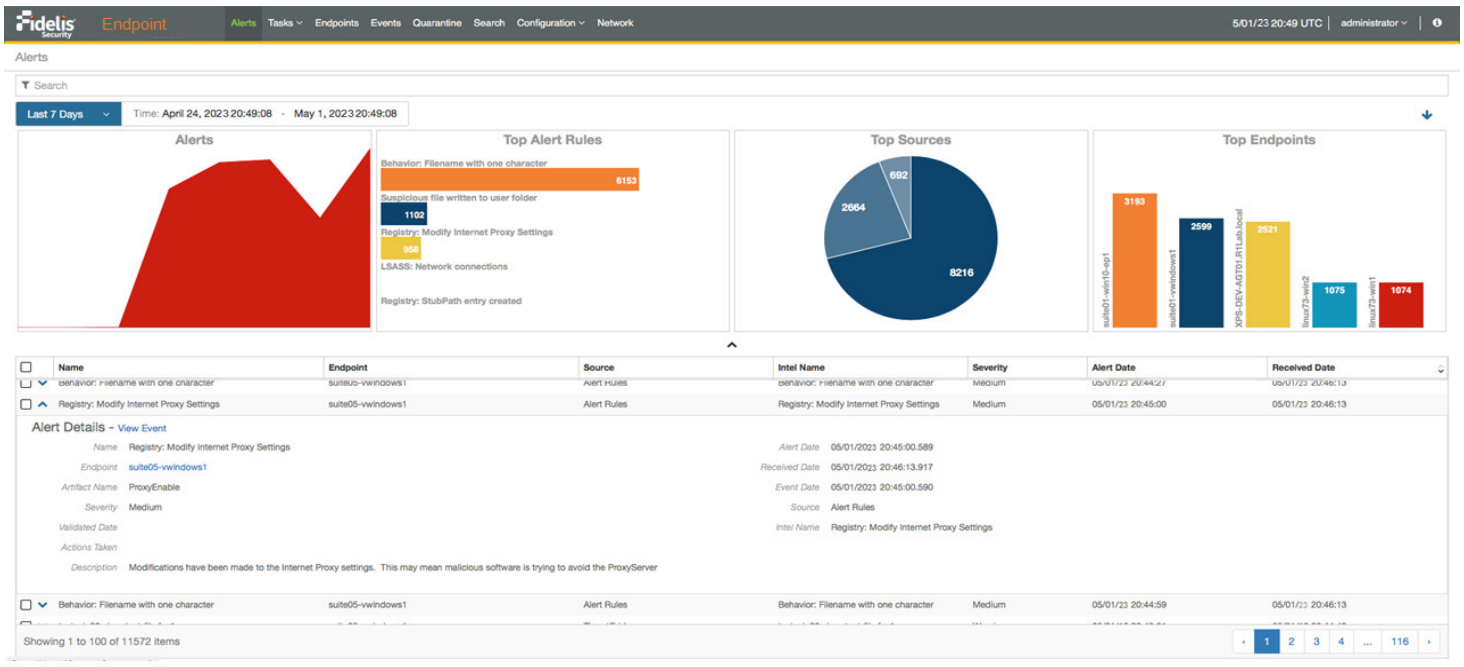
End Alert Fatigue: Automate time-consuming security tasks and common responses with automated scripts and receive high fidelity alerts for issues that demand immediate attention and pose immediate risk.

Understand Vulnerabilities and Detect Malware: Fidelis creates a log of all installed software in the enterprise and performs daily vulnerability analysis, allowing you to correct before engaging in an exploit attempt. Fidelis also collects a copy of every file and script executed in the environment, storing evidence even when an attacker may erase their tools. Use of the Fidelis Sandbox helps to identify malware within the collected set of files and scripts.

Prevent Malware: Quarantine files based on known malware signatures. Stop processes when malicious behaviors are detected.

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
- Detect vulnerabilities
- Collect software, executables, and scripts before



About Fidelis Security®

Fidelis Security® is the industry innovator in proactive cyber defense, safeguarding modern IT for global enterprises with proactive XDR and CNAPP platforms. Fidelis Security consolidates IT security operations to shrink attack surfaces, automate threat detection, and accelerate analysis, forensics, and response so that organizations remain resilient through cyber-attacks and emerge stronger and more secure. Fidelis Security is trusted by top commercial, enterprise, and government agencies worldwide.