Fidelis® Cybersecurity

Fidelis Endpoint®: A Technical Deep Dive

www.fidelissecurity.com

Contents

Endpoint Detection and Response with Fidelis

Modern attacks are a complex and often automated series of processes, steps and interrelated events that penetrate the cybersecurity perimeter. Too often, security teams are forced to rely on strung-together, patchwork systems that create more work and complexity, rather than solve the problems at hand. They lack the complete, unified and automated endpoint detection, response and prevention technology to see and respond to these kinds of attacks.

Fidelis Endpoint® is a key part of the Fidelis Elevate™ platform that is designed for automated detection and response to today's advanced cyber threats. It equips organizations to confidently detect, respond to, and resolve security incidents in a fraction of the time it takes using traditional approaches.

We do this by:

- Rapidly accelerating and automating the validation process
- Cutting down the investigation workflow with automatic collection and correlation of related events, processes and files
- Automating the response processes like endpoint isolation, memory analysis and forensic collection

Unlike other security products, Fidelis Endpoint provides the visibility, context and automation required to identify attacks as they happen and prevent them from becoming breaches. Fidelis Endpoint enables security teams to quickly focus on the incidents that matter. Once a suspected incident is validated, the involved endpoints can be automatically isolated while allowing investigations to continue. With Fidelis Endpoint, security operations teams receive the information they need—when they need it—to make rapid, accurate decisions about potential incidents.

This overview explains how Fidelis Endpoint unifies endpoint detection and response (EDR) and endpoint protection platform (EPP) capabilities traditionally available only as disparate point products, into one powerful solution.

Fidelis Endpoint: Comprehensive, Automated, and Contextual

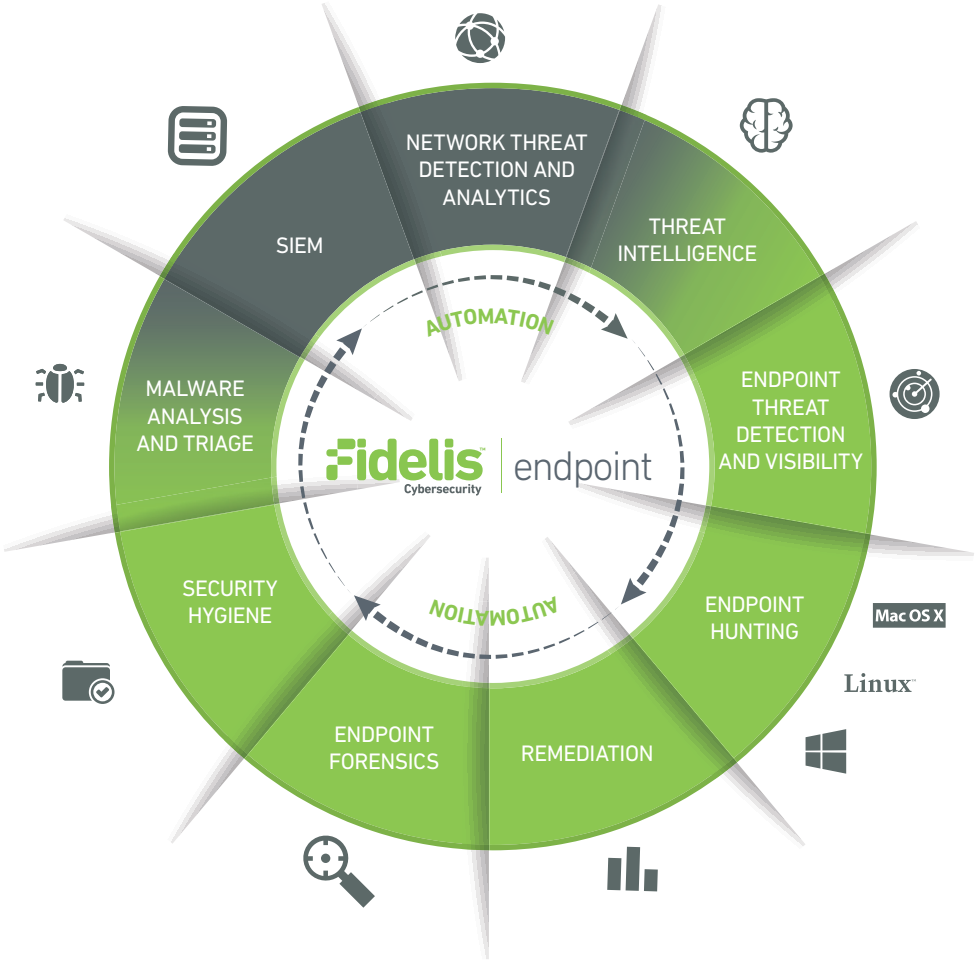
Fidelis Endpoint® enables security teams to focus on and act against real threats by correlating activity between Fidelis Endpoint and existing security products—such as network-based security solutions, next-generation firewall/detection systems, advanced breach detection solutions or security information and event management (SIEMs)—so the teams can effectively assess and validate alerts within seconds of notification. The solution also automates complex, time-consuming, manual workflows and applies intelligence and context to alerts, so analysts can quickly validate, investigate and ultimately resolve incidents.

Fidelis Endpoint reduces risk, improves key metrics, automates manual steps and minimizes clicks in a way that scales, making more effective use of scarce resources.

Unlike standalone solutions, Fidelis Endpoint is a single, combined EDR and EPP solution comprised of:

- Threat intelligence
- Endpoint threat detection and visibility
- Endpoint hunting
- Remediation
- Endpoint forensics
- Security hygiene
- Malware analysis and triage
- SIEM integration
- Network threat detection and analytics

Let's look in more detail at Fidelis' offerings for each of these capabilities.



Threat Intelligence

Today's modern attacks are complex and very targeted. Toolsets for achieving enterprise-persistence and lateral movement have evolved quite rapidly, to where even hacktivists and script-kiddies can access fully autonomous malware that can inflict significant costs on the enterprise. To combat these threats, the Fidelis Threat Research team provides and continually updates threat intelligence (Fidelis Insight) for our customers.

We recognize, however, that reliance on a single source of threat intelligence may limit your ability to detect all malicious activity. For this reason, Fidelis Endpoint® also consumes threat intelligence through multiple, open threat intelligence standards, third-party threat feeds and custom threat intelligence. It aggregates, normalizes and correlates threat intelligence from multiple sources across multiple points of visibility in order to detect suspicious activity. Additionally, Fidelis Endpoint can consume the following types of threat intelligence:

- **Atomic and Multi-dimensional**
  Fidelis Endpoint can easily ingest common indicator terms such as bad IPs, DNS hostnames, URLs and Hashes. Fidelis Endpoint not only consumes threat intelligence from the Fidelis Threat Research Team, but can also utilize threat intelligence from commercial sources and community feeds by normalizing multiple formats (such as STIX, XML, JSON, and delimited files) already supported by the Collective Intelligence Framework (CIF).

- **Behavioral**
  Fidelis Endpoint can use Behavior Rules to identify suspicious or known bad activity on endpoints. Analysts can create and customize Behavior Rules to identify specific activity, such as processes executing from an abnormal directory. Fidelis Threat Research Team actively adds to the detection capabilities by continuously creating new Behavior Rules based on its research and emerging threats.

- **OpenIOC and YARA**
  Fidelis Endpoint has built-in support for OpenIOC and YARA rules. These rules are imported into the database then used in ThreatScan for hunting across the enterprise.

All of this threat intelligence is collected, normalized and made actionable by Fidelis Endpoint. It continuously correlates intelligence against endpoint events and activity, such as process MD5s, network IPs and URLs. In addition, it has a built-in integration with Threat Lookup, enabling lookup of IP addresses, URLs and MD5 hashes to automatically see what's known about these data points. This integration makes it much faster for your analysts to make rapid, accurate decisions by weeding out false positives, confirming suspicious items and gaining additional context.

Endpoint Threat Detection and Visibility

Fidelis Antivirus provides traditional signature and heuristic-based detection of malware on endpoints. Malware detection and remediation is integrated tightly with the Endpoint Collector—the centralized endpoint behavior and historical data store- so your analyst can seamlessly follow the path of the malware back to its origin whenever malware is detected and remediated.

When malware is detected, a sample is automatically sent back to the Global File Quarantine — a central repository of detected malware — so it can easily be used to:

- Jumpstart an investigation into the threat
- View detection information and details from Threat Lookup
- Download the sample for further analysis and investigation

Fidelis Endpoint also provides real-time monitoring of endpoint behaviors. It automatically detects when a threat indicator (IP address, DNS, process name, URL, MD5, etc.) exists on an endpoint or when a process performs certain behavior and can automatically initiate an appropriate response action or generate alerts that are sent to the SIEM.

It monitors endpoints wherever they are—on or off the network—letting you maintain visibility into the endpoint, even when employees work at remote locations.

Endpoint Hunting

Security incidents usually entail multiple actions that can range from simple — a drive-by virus infection — to automated — a lengthy and complicated attack with multiple attacker interactions, such as a targeted hacker intrusion. Regardless of the incident type, there will always be logged events, and alerts usually will be triggered from one system or another. The key to understanding a detected threat is to answer a few basic questions: how did it get there, what has happened since it arrived and what type of threat is it?

The Fidelis Endpoint agent continuously monitors and stores information that's crucial to answering these questions. It collects and stores endpoint behavior data in the Endpoint Collector. Endpoint behavior includes process, network, file, registry, DNS, HTTP/HTTPS and Windows Event Log activity. In addition, it records when processes launch and what changes they make to files and registry entries, as well as network activity. Your analysts can then query the Endpoint Collector to ask, "What happened before and after the alert time?" Fidelis then gives them a recording of endpoint activity they can review to rapidly answer their questions.

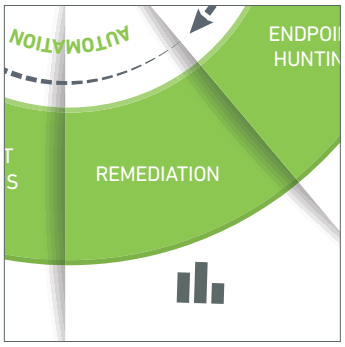
Fidelis Endpoint allows security teams to use both OpenIOC and YARA rules to proactively hunt for artifacts and threats existing on the endpoints across their enterprise. This flexibility allows multi-dimensional rules to detect registry modifications, files and more,

allowing analysts to identify threats that might have existed before the introduction of security tools or to hunt for threats that bypassed existing defenses.

Alerts confirm when an endpoint has been compromised. Fidelis Endpoint's powerful visibility and detection engine combined with Behavior Rules monitor and alert on common activity that indicate malicious events taking place on an endpoint. This continuous monitoring allows playback of attacker command execution, and lets companies automate responses to detected events.

Lastly, contrary to popular belief, it's not enough to simply add an alert to the SIEM—by the time this is done, hackers could have opened another backdoor or moved laterally to other systems within the environment. With the combination of Fidelis Endpoint's Behavior Rules and alert responses, endpoints can be isolated and hackers can be captured "in the box," preventing them from moving to other systems.

Remediation

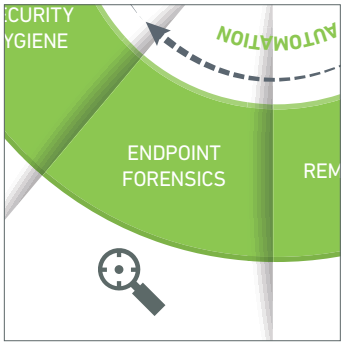


Remediation functions traditionally have been manual and extremely time-consuming, opening organizations up to vulnerability. By automating parts of the process, Fidelis helps shrink the time it takes to remediate an incident, so it can be resolved before an attacker steals valuable IP/assets.

Fidelis Endpoint can automatically remediate and take action on impacted endpoints. For instance, with Fidelis, you can immediately halt data exfiltration and lateral movement from endpoints by using endpoint isolation, process termination or file deletion, or by kicking off a custom-scripted routine on endpoints. Fidelis Endpoint can automatically kick off remediation or deep analysis actions by defining trigger rules and actions with its alert response workflow engine. These incident response workflows are easy to create and customizable to specific organizational needs.

Fidelis Endpoint uses custom scripts that extend its functionality, giving you near-limitless remediation, response and analysis capabilities. Its remediation capabilities also include several systems management functions, such as pushing software, terminating a process, removing a service, rebooting the system, looking for new account creation, volume listing, USB history, software inventory and CVE vulnerability checking.

Endpoint Forensics



Fidelis Endpoint accelerates the triage and validation of alerts by recording and storing endpoint behavior data in a centralized repository, the Endpoint Collector. This historical data remains untouched and can provide valuable clues to help you trace an alert back to its original source. Behavior data, however, only tells part of the story. Sometimes you need to reach out to endpoints to further investigate and respond.

Endpoint includes built-in scripts for collecting live response data, deep forensic data and other information useful to security teams and IT analysts. If your analysts want more granular control—or if there are workflows and standard operating procedures that define which datasets to collect—analysts can choose from a wide variety of options to build new scripts. In addition, data collections can be run against a single system or multiple systems across the enterprise, from one task.

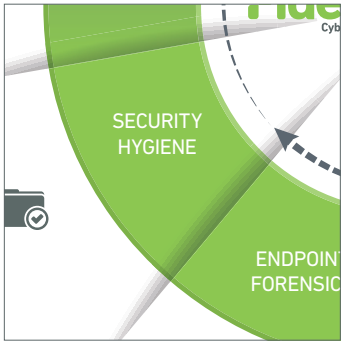
One of the most common procedures in security operations and incident response is performing a "live response" — capturing an initial set of data from a system when it's first flagged as potentially compromised. In this case, only data necessary to perform an initial analysis is collected, such as details on running processes, open network connections, recently contacted DNS hostnames and recently executed applications.

Fidelis collects this kind of data in minutes, saving analysts the hours or days they used to spend collecting and analyzing full system images for alerts that often turn out to be false. By rapidly collecting targeted, live response data, you're much better able to identify threats before clues of their presence fade away. This approach not only ensures threats are identified, it also provides useful information for understanding the threat type and severity.

For systems known to be compromised or for the purpose of internal investigations, you need to collect and analyze much more data in order to thoroughly review it. Fidelis Endpoint lets you collect all the data you need—ranging from simple file and registry listings, to actual files and even full memory dumps and disk images. Additionally, for memory analysis, Fidelis gives you capabilities usually only found in specialized memory analysis tools.

Fidelis Endpoint enables security analysts, incident responders and malware analysts to gather extensive information on running processes. With this approach, your analysts gain access to information difficult to obtain when malware is obfuscated on disk, or avoids residing there altogether.

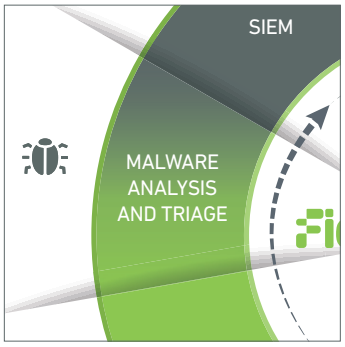
Security Hygiene



Since it's important to not only detect and respond to what occurs in your environment but also take preventive measures to reduce risk, Fidelis Endpoint combines EDR capabilities with security hygiene and systems management.

Fidelis Endpoint can perform software vulnerability correlation and reporting based on the installed software of assets. Found vulnerabilities include links to the MITRE CVE database or Microsoft KB articles, providing background details on the vulnerability. In addition, you can close security gaps and vulnerabilities on endpoints by using custom scripts to deploy software patches and updates across the enterprise. Built-in systems management scripts also provide a current state of the enterprise by showing currently installed patches, software, features, and more.

Malware Analysis and Triage



Besides behavioral detection of malware, Fidelis Endpoint uses several engines to detect and stop malware in other ways.

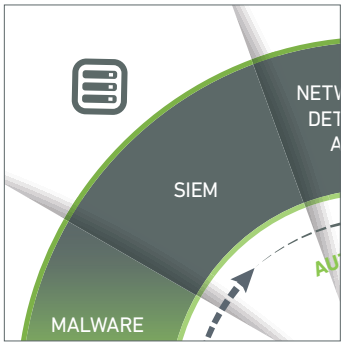
- **Fidelis Antivirus Engine**
  Fidelis Antivirus powered by Bitdefender is able to detect malware through both signatures and heuristics. It is integrated closely with the Endpoint Collector allowing analysts to see exactly what happened prior to the detection and remediation of malware on a system.

- **Process Blocking**
  Fidelis Endpoint makes it easy to add hashes for process blocking in order to prevent execution, but it also supports the use of YARA rules to scan executables prior to allowing execution. This feature allows for creating advanced rules that can use any YARA module, such as the PE module, to look inside an executable and proactively prevent execution. This powerful feature allows security teams to prevent the spread or execution of malware across the enterprise, even if hashes change.

- **Behavior Engine**
  While sandboxes can be easily evaded, Fidelis can detect and act upon malware that executes based upon its behavior. Custom Behavior Rules can be configured to look across multiple dimensions of behavior to identify suspicious process behavior.

- **Cerberus Engine**
  Fidelis also utilizes Cerberus, which employs signatureless malware detection. Cerberus performs a static analysis of the binary and applies a threat score based upon how suspicious each process appears to be, giving the analyst a way to quickly diagnose unknown binaries before sending to a Sandbox or digging deeper.

SIEM Integration



Security information and event management (SIEM) technologies aggregate and correlate events and alerts from multiple sources, then apply intelligence and analytics to help reduce and prioritize the noise. Even a well-maintained SIEM, however, can only do so much because it receives limited information that typically does not tell the whole story. Analysts then have to evaluate and investigate all the alerts presented by the SIEM— manually verifying threats and gathering additional data from multiple sources to build the bigger picture—then remediate all affected endpoints.

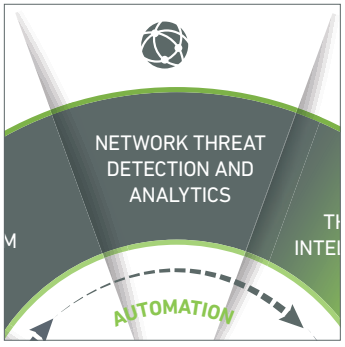
By integrating with SIEMs, Fidelis Endpoint reduces the noise and alert fatigue by automating most of the manual steps taken by analysts. It allows for significant improvements of key metrics—such as alert validation, containment time, forensic data collection time, analysis time and time to incident resolution—by automating actions taken after an alert is received.

Fidelis Endpoint uses syslog export to provide out-of-the-box integrations with many tools—including McAfee Enterprise Security Mangager, HP ArcSight and IBM QRadar—and makes it straightforward to add support for other systems.

Bi-directional integration means you can also trigger pre-defined templates from the SIEM. These templates include live response collections—such as memory analysis, a listing of running processes and open network connections/ sockets—in addition to any other script available in the library. You can easily customize these without scripting.

As Fidelis Endpoint receives the collected data from the agent, it pushes the information back to the SIEM interface.

Network Threat Detection and Analytics



Organizations need visibility into both their network and their endpoints in order to see the full picture of what's going on in their environment. To truly maximize your analysts' time and efforts, you need to automate this process and take away the pain of "alt+tab" and swivel-seating. Through these actions, you'll also speed the detection process.

Fidelis Elevate is the first fully-automated, complete compromise detection and response system designed to improve security center operations. It is engineered to deliver comprehensive visibility and alert validation—and increased response velocity—across both endpoints and networks, in real-time and retrospectively. For this reason, Fidelis Endpoint integrates fully with Fidelis Network, giving you maximum automation in detecting and responding to modern attacks.

With this approach, Fidelis changes the way security teams work. By instantly validating network detections on the endpoint, Fidelis helps security teams prioritize what needs attention now. Only with Fidelis can you drastically reduce response times for investigation and response through automated processes.

Fidelis equips security teams of all sizes to quickly filter through the noise to identify which alerts need action. It delivers automated alert context and one-click automated response actions. Thanks to detection rules

built and fine-tuned by Fidelis' Threat Research Team over the past 15 years, Fidelis Elevate understands the tactics and techniques of threat actors, and knows what to look for. Fidelis uses this in-depth knowledge to validate alerts for suspicious events — solving the problem of knowing "did it happen?" — and delivers rich alert and event context that automates manual investigations and accelerates processes, to answer the question, "what happened?"

Fidelis also provides automated response action from within the alert details, which eliminates manual steps, so security teams can act immediately.

Using Automation to Overcome Security Vulnerabilities

Most security operations center (SOC) analysts and security teams tasked with reviewing and triaging suspected incidents are overwhelmed by alerts, leaving them unable to quickly validate whether a suspected incident is indeed real. They also receive little context on the suspected incident's potential impact.

Manually investigating the incidents to which they do respond is time-consuming, hampered by the lack of qualified security analyst resources. This situation makes it difficult for most organizations to keep pace with attacks that continually increase in volume and complexity.

Fidelis Endpoint alleviates these issues via a maniacal focus on automation. Fidelis automates many time-consuming security tasks, then arms analysts with intelligence, so they quickly can determine an incident's scope and the appropriate response. This accelerated detection and response reduces your risk, improves key metrics and eliminates response fatigue.

Fidelis also automatically makes threat intelligence actionable and applies context. For example, when analysts find a confirmed indicator, they can schedule proactive hunting operations and automatically act, such as:

- First go to a machine and grab a set of volatile data
- Correlate against threat intelligence to see if there are known indicators
- See if it matches any of the Behavior Rules
- Query into Threat Lookup and apply external context
- Highlight any identified risks

Fidelis' automated response engine provides prebuilt rules and responses that can be joined together to automatically trigger specific response actions based on a validated alert — such as "perform triage on the endpoint," "lock down the endpoint" or "perform deep incident response." Fidelis Endpoint also automatically takes action when alerts are sent by SIEM, network threat detection, malware analysis and triage products. And, since every organization has unique needs, Fidelis gives you the flexibility to create custom templates in addition to leveraging its built-in automation capabilities.

A FIDELIS CASE STUDY

Telecommunications company uses automation to isolate endpoints, gather forensic data, analyze malware and remediate incidents 80% faster.

A telecommunications company with a fragmented infrastructure of network, endpoint and SIEM tools deployed Fidelis to improve incident response times.

By integrating Fidelis Endpoint with their SIEM, alerts from the SIEM now trigger Fidelis Endpoint to immediately and automatically isolate suspect endpoints from the rest of the network. Automatically isolating impacted hosts takes only seconds, yet it prevents the threat from spreading through the network — while allowing triage of the threat to continue.

Fidelis Endpoint also empowered the company's security team to quickly, automatically identify all other compromised endpoints — eliminating the time-consuming, manual processes that only exacerbated the company's vulnerability during a security breach.

As a result, the company was able to speed its security operations by 80 percent!

Capability Comparison: Why Fidelis Endpoint Wins

Before Fidelis Endpoint, companies needed to install both EDR and EPP products to protect their endpoints from threats, and manually investigate and remediate any incidents that occurred. This partial list of capabilities highlights what's provided in Fidelis' combined EPP/EDR solution versus what you get with traditional, standalone EPP/anti-virus solutions.

Capability	EPP / AV	Fidelis Endpoint
Detection		
Based on hashes / signatures	●	●
Based on IP addresses	○	●
Based on URLs	○	●
Based on DNS / domain names	○	●
Based on heuristics	●	●
Based on behavior	○	●
Based on IoCs	○	●
Based on YARA rules	○	●
Real-time	●	●
Near-real-time	○	●
Historic	○	●
Response		
Block process execution	○	●
Kill process	○	●
Delete files	○	●
Delete registry entries	○	●
Host isolation	○	●
Notify user / popup	●	●
Automated response	●	●
Automated response on network alert	○	●
System Management		
Hardware inventory	○	●
Software inventory	○	●
With vulnerability reporting	○	●
Computer uptime	○	●
Disk space	○	●
OS details	○	●
WSUS settings	○	●
Windows features enable / disable	○	●

Capability	EPP / AV	Fidelis Endpoint
Investigation		
Global quarantine (central repository)	○	●
Memory analysis	○	●
Address resolution protocol (ARP) cache	○	●
Autoruns	○	●
Disk volumes	○	●
DNS cache	○	●
Drivers	○	●
List user accounts	○	●
File metadata acquisition	○	●
Network interfaces list	○	●
Process dump	○	●
Process list	○	●
Search registry	○	●
Routing table acquisition	○	●
Run Once values	○	●
Scheduled tasks	○	●
List services	○	●
Startup programs	○	●
USB device history	○	●
Login events	○	●
Log acquisition	○	●
Event ID monitoring	○	●
Forensics		
Full disk image acquisition	○	●
File acquisition	○	●
Memory dump acquisition	○	●
Remote memory analysis	○	●
Remote execution of any script	○	●

Appendix: Endpoint Feature Glossary

The below table is a listing of many of Fidelis Endpoint's features along with a category and description. This listing doesn't encompass all capabilities and features, but provides additional context or further definition to items covered in the overview above.

Feature	Category	Description
Endpoint Collector- Centralized endpoint behavior monitoring and alerting	Visibility Detection	The agent collects behaviors from the endpoint such as process starts, registry writes, files written, and windows events like user logon to be checked against threat intelligence and shipped to the central database, Endpoint Collector, for storage.
Behavior Rules feed from Fidelis Insight	Threat Intelligence Detection	A feed from Fidelis Threat Research of behavioral indicators for detection of threats against endpoint events.
Threat Intelligence	Threat Intelligence Detection	Fidelis Endpoint provides the ability to consume 3rd party intelligence feeds containing static indicators such as IP addresses, domain names, and hashes.
Fidelis Insight Feeds	Threat Intelligence Detection	A set of feeds from Fidelis Threat Research are provided and constantly updated with new intelligence from Fidelis Sandbox, Machine Learning, Threat Research, and augmented with intel from other 3rd party sources/ feeds.
Custom searching across current and historical endpoint behaviors	Visibility Hunting	Users can search endpoint behaviors and data stored in the Endpoint Collector to identify suspicious endpoint behaviors and hunt across both recent and historical data retrospectively.
Custom Behavioral Rules for detections	Threat Intelligence Detection	Users can create their own Behavior Rules based on searches performed in the Endpoint Collector, allowing for custom behavioral-based detections.

Feature	Category	Description
Alert Responses	Response	Users can configure responses to alerts in the system allowing for automated actions to take place before an analyst reviews the threat. For example, a critical alert may automatically quarantine an endpoint on the network to prevent a threat from spreading.
Scanning Indicator Library	Threat Intelligence Detection	The Scanning Indicator Library is a central repository of IOCs (Indicator of Compromise) that ships with hundreds of OpenIOC and Yara indicators out of the box from many community sources. Users can also upload new OpenIOC/Yara rules for use. These can be used in ThreatScan jobs to hunt and look for indicators of threats across many machines.
ThreatScan	Hunting Detection	ThreatScan utilizes OpenIOC and Yara rules from the Scanning Indicator Library for threat hunting. It allows for scanning both on the file system and in memory of the endpoints.
Script Library	Management Actions	A library of scripts that can be executed against endpoints. The software comes with hundreds of pre-built scripts covering a range of tasks and categories including: Investigation, Response, Systems Management, and more. Users can create new scripts and easily utilize existing tools in the software.
Notifications and Alert Subscriptions	Management Alerts	The system allows for subscriptions to be configured for new alerts in the system by severity which will be sent to different e-mail addresses, Microsoft Teams, Slack channels, or a combination of all so users never miss an alert.
Integrations and API	Integration	The software comes with the capability to integrate with Fidelis Network, FireEye, and Palo Alto out of the box as well as various SIEMs. This allows for validation of alerts from various systems or execution of tasks on endpoints from SIEM alerts automatically. In addition, the software is designed with a robust REST-based API that can be utilized by custom script and tools for integrations and automation.
Full Disk Imaging and File Collection	Investigation Response	The system is able to perform full disk imaging to a forensic container for traditional forensics and investigation or collect specific files and folders for quick analysis.

Feature	Category	Description
Memory Acquisition and Analysis	Investigation Response	The system is able to perform a full memory capture of the system for traditional memory forensics and investigation or perform quick memory analysis on a live system to provide the user information about processes in memory including details like sockets, handles, DLLs, VADs, and checking for hidden processes.
Installed Software and Vulnerability Report	Investigation Management	This task lists all the installed software and identifies vulnerable software on the endpoint. Software with identified vulnerabilities are listed and provide context about the vulnerability with a description, severity, and links to the MITRE CVE or Microsoft KB article related to the vulnerability for more details.
Isolation and Remediation	Investigation Response	The system is able to isolate endpoints on the network to prevent threats from spreading, while allowing access from the console or other designated systems. While the endpoint is isolated, users can perform investigation or remediation tasks against the endpoint including: terminating processes, collecting or deleting files, restoring to a known good configuration and more.
Threat Lookup	Investigation	Threat Lookup is a service provided by Fidelis to cache and retrieve information from multi-scanners. Processes and malware samples can be checked against the known detections and provide quick context into whether the sample is known in the wild and its detection rate. Note: Only hashes are sent to Threat Lookup to check for results against the cache, no samples or binaries are submitted and customer information is never provided to third-parties.
System Health Page	Management	The System Health Page lets administrators monitor the health of the Endpoint product components running in the system. Users with access can view the status of services and Linux servers, container statistics, collect logs, or start and stop services.
Restore Point Scripts	Response Management	The software ships with scripts for managing windows system restore points, so you can easily create new restore points or revert to a known good restore point in response to threats.
System Management Scripts	Management	The software ships with many scripts that can be used for system management purposes including: gathering hardware and OS information, checking for installed updates and hotfixes or forcing an update, software inventory, and more.

Feature	Category	Description
Connected Agents	Management	The system tracks agents that are online and actively connected so users can filter on agents actively connected to the system for executing jobs quickly against online assets, or find assets that haven't connected in a period of time.
Caching and Offline Agents	Management Detection	Agents cache events and data when they are offline or disconnected from the system and will send cached data back once reconnected. If jobs are executed for agents when offline the system will queue them up for when they come back online. Intelligence and detections are pushed locally to agents so detections can still happen regardless of an internet connection or connection with the console.
Roles and Permissions	Management	The software has extensive role-based access controls allowing administrators to customize user roles to their role in the organization. Users can be limited on what scripts they have access to, endpoints they can perform actions against or view data from, as well as system-level permissions for creating or modifying rules and more.
Lightweight, Encrypted, and Secure Agent Communication	Management	The agent establishes a secure communication channel directly with Endpoint servers using TLS 1.2 encryption over a persistent WebSocket connection. This allows for a lightweight connection to the console for lightning fast communication and responses.
Fidelis Antivirus (optional add-on)	Detection Prevention	Fidelis Antivirus, powered by Bitdefender, adds additional detection and prevention capabilities to the endpoint agent. Fidelis Antivirus adds signature and behavior-based detection/prevention of both known and unknown malware in addition to rootkit detection and boot sector protection. Fidelis Antivirus integrates with the endpoint events so when malware is detected and remediated the user is able to quickly pivot from the alert to the event details providing context into the source of the malware.
Process Blocking (requires Fidelis Antivirus)	Detection Prevention	Users can quickly block processes by hash or leverage the power of Yara rules to block advanced threats from executing and spreading across the enterprise.
Global Quarantine (requires Fidelis Antivirus)	Detection Prevention	Global Quarantine is a centralized location for all detected malware from Fidelis Antivirus. When Fidelis AV detects or prevents a threat on the endpoint it automatically sends a copy of the malware sample to the Global Quarantine where users can pivot to the source event, download a copy of the sample for analysis, or check it against Threat Lookup for scoring information from multi-scanners.

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy.

By integrating bi-directional network traffic analysis across your cloud and internal networks with email, web, endpoint detection and response, and automated deception technology, the Fidelis Elevate™ platform captures rich metadata and content that enables real-time and retrospective analysis, giving security teams the platform to effectively hunt for threats in their environment. Fidelis solutions are delivered as standalone products, an integrated platform, or as a 24x7 Managed Detection and Response service that augments existing security operations and incident response capabilities. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.