white paper

fidelis endpoint®
a technical deep dive

Fidelis Cybersecurity

table of contents

stc

white paper

endpoint detection and response with fidelis

Endpoint prevention is no longer enough as detection and response capabilities are now required. Modern attacks are often file-less using scripts and macros, web drive- by downloads, or social compromise. Detecting unknown intruders or insider threats changes the endpoint security landscape. Security operations desire rich endpoint data on activity and behaviors and the ability to apply multiple threat intelligence feeds to improve detection, plus leverage endpoint forensic investigation capabilities. However, IT endpoint management desires ease of use, minimal impact on end users and devices, security hygiene, and agent consolidation to avoid conflicts.

Fidelis Endpoint® provides a single lightweight agent with on and off grid defences that is easy to manage with dynamic groups and to apply desired actions to endpoints simultaneously. At the same time, it also provides security analysts rich metadata on events, processes, and behaviors supporting advanced queries with Boolean logic, plus a collection of first-time seen file executables and scripts. Companies can leverage their desired AV investment of choice combined with advanced detection and response, including automated responses using playbooks and scripts.

We do this by providing:

- Software inventory and known vulnerability correlation (CVE, KB), plus security hygiene
- Process blocking (hashes, YARA rules) independent of installed AV engine
- First time seen executable file and script collection for investigations and hunting
- Process and event metadata for real-time and retrospective analysis
- Graphical time line to easily follow the actions a process performed
- Indicator library for OpenIOC and YARA rules, plus automated response script library and playbooks
- Hundreds of scripts for investigation and response out of the box, and the ability for analysts to fully customize and create their own
- Ingestion and normalization of third-party and open- source threat intelligence feeds in varying formats, plus inclusion of Fidelis Insight threat intelligence
- Advanced query builder with Boolean logic for investigations and threat hunting
- Unmatched forensic data collection including memory and full disk images
- Dynamic groups to easily manage and maintain policy across different asset types
- Real-time investigation and control through full remote consoles”

Fidelis Endpoint provides the prevention you desire with visibility of your endpoint cyber terrain and security hygiene, plus the details of all endpoint activity including forensic data capture desired by experienced security analysts. Often ease of use comes at the expense of visibility, advanced queries, and applying open threat intelligence, including internally developed indicators and behavior rules. That trade off can be avoided with Fidelis Endpoint, designed by experts in detection, investigations and incident response with an understanding of how endpoint defences are changing.

This overview explains how Fidelis Endpoint .unifies advanced endpoint detection and response (EDR) and forensic capabilities to meet the needs of IT endpoint management and mature security operations.

Fidelis™
Cybersecurity

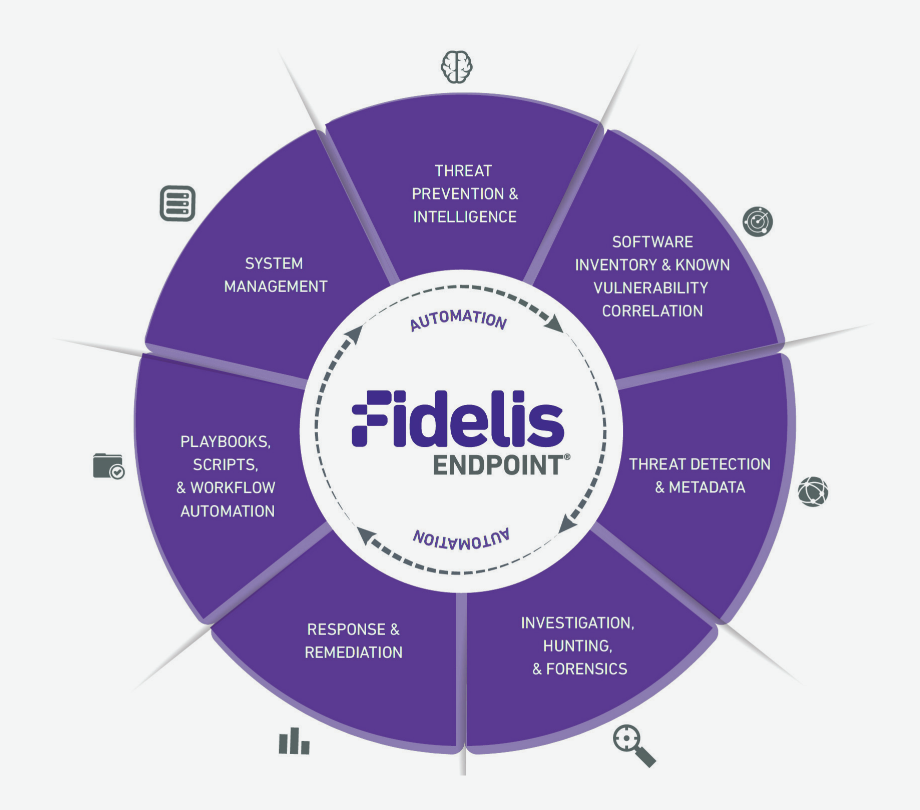
white paper

fidelis endpoint: prevent, detect, and respond

Fidelis Endpoint® enables security teams to focus on and act against 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 threat 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 limited security operation resources.

Consolidate and integrate endpoint defenses to leverage threat intelligence and automate response. Fidelis Endpoint is a prevention, detection and response solution comprised of:

- Threat prevention and intelligence
- Software inventory and known vulnerability correlation
- Threat detection and metadata
- Investigation, hunting, and forensics
- Response and remediation
- Playbooks, scripts, and workflow automation
- System management


THREAT PREVENTION & INTELLIGENCE
SOFTWARE INVENTORY & KNOWN VULNERABILITY CORRELATION
THREAT DETECTION & METADATA
INVESTIGATION, HUNTING, & FORENSICS
RESPONSE & REMEDIATION
PLAYBOOKS, SCRIPTS, & WORKFLOW AUTOMATION
SYSTEM MANAGEMENT
AUTOMATION
Fidelis ENDPOINT®
AUTOMATION

Fidelis Cybersecurity

threat prevention and intelligence

Fidelis Endpoint provides best in class threat prevention with Bitdefender on Windows systems or a customer choice of AV engine investment. Fidelis AV includes behavioral, heuristic and signature defenses, including boot sector protection and a global quarantine of detected malware for analysis. To support a choice of AV engine, process blocking runs independently using hashes or YARA rules to extend prevention defenses. Process blocking also includes the ability to use threat intelligence feeds as a source of hashes to block.

Security analysts can quickly pivot from AV alerts into the endpoint process tree with event details providing context into the source of malware leveraging the value of combined prevention and detection in one agent. Malware detection and remediation is integrated tightly with the Endpoint Collector — the centralized endpoint behavior and historical metadata store - so analysts 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 for each customer — 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 for Windows, Mac, and Linux systems. 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 a SIEM. Endpoints are monitored on and off network letting you maintain visibility even when employees work in remote locations. Besides behavioral detection of malware, Fidelis Endpoint uses several engines to detect and stop malware in other ways.

- Fidelis Antivirus Engine – Fidelis AV powered by Bitdefender detects malware through both signatures and heuristics on Windows systems. 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. Fidelis AV is optional with Fidelis Endpoint supporting an open choice for AV investment.

- Process Behavior Blocking (Advanced Malware Detection) – While sandboxes can be easily evaded, Fidelis Endpoint can detect and act upon malware that executes based upon its behavior. While a process is executing, Advanced Malware Detection will monitor and score the activity across multiple dimensions of behavior to identify malicious process behavior. If the score of the process crosses the threshold for malicious behavior it is terminated. This feature is part of the Fidelis AV option for Windows systems.

- Process Blocking – Fidelis Endpoint makes it easy to add hashes for process blocking in order to prevent execution, and it also supports the use of YARA rules to scan executables prior to allowing execution. Process blocking works independently of AV engine choice. 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. Optionally, analysts may also choose to automatically block any executables deemed malicious by the Fidelis Sandbox

Given today's modern attacks evade basic defenses and are very targeted, the Fidelis Threat Research team provides and continually updates threat intelligence (Fidelis Insight) for our customers leveraging cloud-based sandboxing, machine learning anomaly detection, and
threat research.

We recognize, however, that reliance on a single source of threat intelligence may limit your ability to prevent and 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 internal threat intelligence. It aggregates, normalizes and correlates threat intelligence from multiple sources across multiple points of visibility in order to prevent and detect suspicious activity. Additionally, Fidelis Endpoint can consume the following types of threat intelligence:

- Atomic and Multi-dimensional Indicators – 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 via Fidelis Insight, it can also utilize threat intelligence from commercial sources and community feeds by normalizing multiple formats (such as STIX, XML, JSON, and delimited files).

- Behavior Monitoring – Fidelis Endpoint can use Behavior Rules to identify suspicious or known bad activity on endpoints for detection. Analysts can create and customize Behavior Rules to identify specific activity, such as processes executing from an abnormal directory. The 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 can be imported into the database then used in endpoint ThreatScans or YaraScans for hunting across the enterprise.

- Fidelis Sandbox – The Integration of the Fidelis Sandbox allows for additional identification of malicious executables through both automatic and manual submissions. Automatic submission can be enabled or disabled and is limited to only Windows executable files that are not signed by a trusted vendor. Scripts are omitted from automatic sandbox submission. Optionally, manual sandbox submission of both executables and scripts can be selected for detonation if the analyst so chooses.

All 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 to provide context about a selected process or collected executable making it much faster for your analysts to make rapid, accurate decisions by weeding out false positives, confirming suspicious items and gaining additional details.

Fidelis Endpoint enables you to avoid the false positives and manual tuning of white lists, isolation containers and stand-alone ML anomaly detection for endpoint prevention.

Fidelis Endpoint provides real-time monitoring of endpoint behaviors for Windows, Mac, and Linux systems. It automatically detects when a threat indicator 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 a SIEM.

software inventory and known vulnerability correlation

Fidelis Endpoint helps to map the cyber terrain of the environment by correlating the software installed on assets with known vulnerabilities from the MITRE CVE database and Microsoft KB articles. Endpoint keeps the software inventory lists updated automatically and alerts whenever a new CVE is found affecting software installed in the environment. Being agent based it provides a more comprehensive analysis than external scans, even with authentication, and it consolidates the number of security solutions deployed.

For security hygiene, Fidelis Endpoint provides the operating system status and can apply security patches, plus report on and change the status of the host firewall and AV engine. Alerts on USB insertion are also included along with monitoring and collecting event and process metadata for all endpoint activity. You can close security gaps and vulnerabilities on endpoints by using custom scripts to deploy software patches and updates across the enterprise.

To complement Fidelis Endpoint for software inventory, customers can benefit from Fidelis Network providing asset profiling and classification of all systems and services including enterprise IoT, legacy systems, and shadow IT. A complete cyber terrain mapping is provided with the option of seeding it with deception decoys and breadcrumbs to lure attacks operating within the terrain by adding Fidelis Deception.

threat detection and metadata

Fidelis Endpoint threat detection leverages the threat intelligence feeds and behavior monitoring rules noted above alongside its scanning indicator library of OpenIOC and YARA indicators for on-demand scanning of memory and file systems. The Endpoint Collector provides real-time and retrospective analysis of endpoint process and event metadata for 30, 60, 90 days or longer.

The event timeline provides visibility and context around all endpoint activity including alerts, parent processes, child processes, remote threads, loaded DLL and exe files, files created, files written, files closed, network connections, and a full process tree. For on and off grid support, intelligence and detections are driven locally on the endpoint and any data collected is cached until reconnected and jobs resume.

Taking detection and investigations another step higher, is the new executable file and script collection saving first-time seen copies for analysis, threat hunting, or scoping an incident. Attacks often delete or hide executable files and scripts to evade detection and hide traces. Now your security analysts have a clean copy of these important attack elements to understand the exact details and executable behavior with the option to view the content of the binary in a hex or text view.

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.

investigating, hunting, and forensics

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 metadata in the Endpoint Collector. Endpoint behavior includes process, network, file, registry, DNS, HTTP/ HTTPS and Windows Event Log 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. Investigations also require queries often limited by faceted search capabilities by selecting filters, and in a worst case scenario no ability to save desired searches. Fidelis Endpoint goes a step further with an advanced query builder that leverages Boolean logic for searches with the ability to save advanced queries for frequent monitoring. The advanced query builder supports experienced security analysts alongside faceted search for everyday use. Both aid in threat hunting and creating custom behavior rules.

Fidelis Endpoint also allows security teams to use both OpenIOC and YARA rules to proactively investigate and hunt for artifacts and threats existing on 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. Endpoints can then be isolated on the network for investigation allowing only communication with the Fidelis Endpoint management console or can include additionally specified systems like jump boxes or investigator machines.

Fidelis Endpoint accelerates the triage and validation of alerts by recording and storing endpoint behavior metadata in a centralized repository, the Endpoint Collector. This metadata remains untouched and can provide valuable clues to help you trace an alert back to its original source in real-time or retrospectively. Providing event context of what happened on any endpoint at any time within the time span of Endpoint Collector including system events, files or known bad processes. Behavior meta 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 from the script library 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 for the purpose of internal investigations, you may 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.

In certain situations, it may be necessary for analysts to interact with an endpoint in a real-time fashion. This allows them to quickly identify what is happening on a system at any given point along with taking immediate action. To offer the highest level of endpoint response and control Fidelis Endpoint provides the following Live Investigation options.

- Live Console – The Fidelis Live Console is an interactive command-line console that allows an analyst to interact with any system running the Fidelis Endpoint Agent in real-time over port 443. The Fidelis Live Console is not limited to a series of built in commands, instead allowing analysts the freedom to execute any command that can be interpreted by the endpoint. Default connects are established with System level privileges but there is also the option to impersonate system users.
- Live Process – The Fidelis Live Process tool allows users to interact with a real-time listing of endpoint processes as if they were working directly from the system task manager. From this process listing, analysts the option of a series of actions including ending processes, blocking processes, searching across endpoints for specified processes, and viewing process properties.
- Live Filesystem – Live Filesystem is a capabilityof Fidelis Endpoint that allows analysts to remotely navigate an endpoint's filesystem in real-time. In addition to viewing files residing on endpoints, Live Filesystem also allows the user to Copy, Rename, Move, and Delete target files. On some occasion's analysts made find it necessary to directly interact with remote files. Because of this Live Filesystem allows for files to be both uploaded to and downloaded from the target endpoint.

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

While investigating or triaging a machine there are times when unknown executables are identified. These items may not even have data available from multi-scanners like Virus Total. Fidelis Endpoint includes Cerberus, which can be enabled from within certain investigation scripts to further analyze executables. Cerberus is a "triage" system that looks at the characteristics of a binary on a "first order" level. That is, it looks at things that are immediately apparent about the binary; things like "does this binary contain a valid digital signature", "is this binary packed", and "what OS functions does this binary import". Cerberus creates a score from these characteristics that approximates the "malicious" factor for a binary. This score provides analysts a way to quickly diagnose unknown binaries before sending to a Sandbox or digging deeper.

response and remediation

Response and remediation functions traditionally have been manual and extremely time-consuming. 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 and assets.

Fidelis Endpoint can automatically remediate and act on impacted endpoints. For instance, with Fidelis Endpoint, 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 leveraging playbooks and response scripts. These incident response workflows in playbooks and scripts are easy to customize to specific organizational needs.

Fidelis Endpoint also 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 insertion history, and software inventory with correlation to known CVEs and KBs. Response playbooks and scripts can also return endpoints to a last known good configuration and run triage tasks to collect evidence.

Out of the box integration of Fidelis Endpoint with popular NGFWs and SIEMs provides seamless workflows, plus a REST API for custom 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. However, even a well-maintained SIEM can only do so much because it receives limited information that typically does not tell the whole story. Analysts must then 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 Manager, Micro Focus 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 SIEMs. 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. As Fidelis Endpoint receives the collected data from the agent, it pushes the information back to the SIEM interface. You can easily customize these templates without scripting.

white paper

playbooks, scripts, and workflow automation

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. Plus, 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 leveraging playbooks and scripts. Fidelis Endpoint 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 automated and accelerated detection and response reduces your risk, improves key metrics and eliminates response fatigue.

Fidelis Endpoint also automatically makes threat intelligence actionable and applies context. For example, when analysts find a confirmed indicator through automation, they can proactively collect volatile data from machines. Analysts can also manually detect, investigate, and hunt, such as:

- Checking the executable file and script collection for the endpoint
- Correlating against threat intelligence to see if there are known indicators
- Checking for matches with any of the Behavior Rules
- Queries into Threat Lookup and applying external context
- Highlighting any identified risks, including software inventory and known vulnerabilities
- Retrospectively analyzing endpoint metadata for historical analysis
- Manual submission of scripts and executables to the Fidelis Sandbox for detonation

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 acts when alerts are sent by a 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, playbooks and scripts in addition to leveraging its built-in automation capabilities.

Organizations also need visibility into both their network and their endpoints in order to see the full picture of what's going on in their environment, often referred to as combining network traffic analysis (NTA) with endpoint detection and response (EDR). 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 and response process.

Fidelis Elevate unites network traffic analysis, endpoint detection and response, and deception into a security platform. 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 with Fidelis Network, giving you maximum automation in detecting and responding to modern attacks.

With this approach, Fidelis Elevate changes the way security teams work. By instantly validating network detections on the endpoint, Fidelis helps security teams prioritize what needs attention now. Fidelis can also help you reduce response times for investigation and response through automated processes across network sensor locations (direct, internal, email, web, and cloud VMs) and endpoints.

Fidelis Elevate equips security teams of all sizes to quickly filter through the noise to identify which alerts need action from Fidelis Network, Endpoint and Deception. It delivers automated alert context and one- click automated response actions. Thanks to detection rules built and fine-tuned by Fidelis' Threat Research Team, Fidelis Elevate understands the tactics and techniques of threat actors and knows what to look for in real-time and retrospectively in network and endpoint metadata. 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™
Cybersecurity

system management

Fidelis Endpoint has a new UI for system management with new menu options for artifacts (including behavior, executables, installed software, quarantine, tag search, and reports), and a new intelligence section under the configuration menu (for behavior rules, intelligence feed indicators, intelligence feeds, process blocking rules, and scanning indicator library). An updated alerts page and dashboard also matches the design of Fidelis Network for symmetry in seamless workflows where analysts can view behaviors and quickly pivot to detection with the intelligence source. The updated alerts page enables alert grouping, searching, filtering, and graphical trend analysis, with access to the details of any alert and automated responses executed as the result of a playbook.

The new UI design also includes easy to edit facet filters for searches and task wizard workflows, task queue expiration, and pivoting between task results. A new Reports section is now available to view all behaviors with the same tag in one report. This allows analysts to create a timeline and report across behaviors in more than one process and endpoint allowing for a report about the incident and details of what behaviors were involved.

Command line length has been extended past the previous limit of 512 characters to the maximum length supported by Windows to improve the investigation of PowerShell with encoded commands and processes. Script updates include a new 'YaraScan' script for Windows, macOS, and Linux system to perform YARA scans against the filesystem on endpoints. Renaming and hiding agents enables customers to rename and hide the endpoint agent services with a custom desired name from the newly updated management UI.

New dynamic groups based on endpoint characteristics automatically update and enable improved segmentation, plus easier policy management with Fidelis Endpoint. You can avoid manually maintaining endpoint groups and let the system handle it for you. Also, Fidelis Endpoint alert subscriptions can be configured by severity for email, Microsoft Teams, and Slack where role-based access controls are provided for endpoints, playbooks, scripts and system level permissions. A connected agents status provides a profile of online and active endpoints, or hardly seen endpoints.

System management scripts provide hardware and operating system profiles, software inventory, checking for installed updates and hotfixes, and forcing updates. A system health page provides status of the Fidelis Endpoint backend servers, services, and containers, plus the ability to collect logs and start/stop services. Endpoints use secure agent communications based on a TLS v1.2 encrypted WebSocket connections for lightweight and fast communications and response. Overall, with the new UI and features noted above, systems management is improved based on customer feedback.

a fidelis case study

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 would sacrifice advanced EDR capabilities for AV prevention and ease of use. Most AV solutions remain weak on advanced EDR features and this puts detection and response at risk for security operations. Tightly coupled AV restricts your choice of EDR capabilities, where an open choice for AV investment enables the EDR features you require. Review this list and score your current tools to understand the difference that Fidelis offers.

Capability	Fidelis Endpoint	Other Solutions
Prevention		
AV Prevention for Windows (optional)	●	○
— Signature, heuristic and behavioral defenses	●	○
— Process behavior blocking	●	○
— Boot sector protection	●	○
— Global Quarantine of detected malware	●	○
— Powered by BitDefender	●	○
Open choice for AV engine investment	●	○
Process Blocking (by hashes and YARA rules) independent of AV engine	●	○
Pivot from AV alerts into process tree for event details	●	○
Threat Intelligence (ML behavior models, threat indicators)	●	○

Capability	Fidelis Endpoint	Other Solutions
Detection		
Advanced EDR for Windows, macOS, and Linux	●	○
Open Threat Intelligence feeds	●	○
— Fidelis Insight (ML, Sandbox, Research)	●	○
— Third Party Intelligence	●	○
— Internally Developed Intelligence	●	○
Automatically Apply Threat Intel (Windows)	●	○
Behavior Rules	●	○
— Custom developed internally	●	○
— Fidelis Insight rules	●	○
Scanning Indicator Library (OpenIOC, YARA)	●	○

Capability	Fidelis Endpoint	Other Solutions
On/Off Grid Prevention	●	○
Threat Lookup for cloud-based detection ratings	●	○
Software inventory for endpoints with correlation to known vulnerabilities (CVE, KB)	●	○
Security Hygiene for endpoints	●	○
— OS status and apply patches	●	○
— Report/change AV and FW status	●	○
— USB activity alerts	●	○
On-demand scanning of files and memory	●	○
Investigation and Forensics		
Endpoint Collector	●	○
— 30, 60, 90 days of event & process metadata	●	○
— Any endpoint activity, any time within metadata	●	○
— Easy to use faceted queries and searching	●	○
— Advanced queries using Boolean logic, plus saving searches	●	○
— Investigate, hunt, and develop behavior rules	●	○
Executable File and Script Collection	●	○

Capability	Fidelis Endpoint	Other Solutions
Executable File and Script Collection	●	○
— First time seen clean samples	●	○
Event and Process Metadata	●	○
— 30, 60, or 90 days	●	○
— Real-time & Retrospective Analysis	●	○
— Apply Threat Intel, Search, and Hunt	●	○
Playback analysis and event timelines	●	○
— Restore to a known good configuration	●	○
— Custom and new playbooks & scripts	●	○
Out of the Box Integration	●	○
— Fidelis Elevate (Network, Endpoint & Deception)	●	○
— FireEye and Palo Alto Networks	●	○
— REST API for desired integrations	●	○
System Management		
Dynamic Groups	●	○
— Based on endpoint characteristics	●	○
— Improve group segmentation	●	○
— Automatically update	●	○

Capability	Fidelis Endpoint	Other Solutions
Script Library	●	○
— Pre-built scripts to collect artifacts	●	○
— Custom scripts to automate manual efforts	●	○
System Isolation with console or desired system access	●	○
Installed SW and Known Vulnerabilities (CVE, KB)	●	○
Forensic integrity for evidence or investigation	●	○
— Full disk images into containers	●	○
— File and folder collection	●	○
— Memory capture or live memory analysis	●	○
— Remote execution of any script	●	○
Response		
Automated Playbooks and Script Library	●	○
— Isolate endpoints and access	●	○
— Terminate processes	●	○
— Triage tasks, evidence gathering, memory dumps	●	○
— Collect or delete files	●	○

Capability	Fidelis Endpoint	Other Solutions
Alert subscriptions	●	○
— Configure by severity	●	○
— Email, MS Teams, Slack, etc.	●	○
Role-based Access Controls	●	○
System Management Scripts	●	○
— Hardware and OS profiles	●	○
— Software inventory	●	○
— Installed updates, hotfixes, forcing updates	●	○
Connected Agent Status	●	○
— Online and active	●	○
— Hardly seen	●	○
System Health Page	●	○
— Status of services, servers, and containers	●	○
— Collect logs, plus start-stop services	●	○
Secure Agent Communications	●	○
— Lightweight and fast to/from endpoints	●	○
— Run scripts simultaneously on endpoints	●	○
On-premises system management	●	○
Managed cloud system management	●	○

appendix: fidelis endpoint forensics explained

Beyond detection and response, the role of an EDR product is to provide an analyst quick access to parsed information from an endpoint. Whether the information is a process listing, data from common registry keys and persistence mechanisms, or metadata from files, the EDR product should ease an analyst's workload by quickly returning details without the need for a full forensic collection and analysis of the system.

However, there are times during an investigation or incident response when traditional forensic processing is needed, also known as "dead box" analysis. Typically, this is reserved for key systems and servers that are compromised or when investigating new malware samples, as it can take days to perform this level of analysis. Traditional forensic processing requires dedicated tools, which don't include agents and are usually segregated onto lab networks and utilize servers with the power to process large full disk images quickly. The processing time alone can take hours before a user is able to begin analysis.

Fidelis Endpoint can augment the need for traditional forensics, with a "live machine" forensic approach that provides the ability to capture key artifacts remotely and quickly. In the event a full disk or memory dump is needed for deeper analysis, Fidelis Endpoint can remotely collect images, speeding up the time to collect, analyze, and respond. Forensics has always been a core feature of Fidelis Endpoint, and it was one of the first products on the market to bring live machine forensics and artifact preservation into an EDR and IR workflow.

Fidelis Endpoint provides "live machine" forensics, which should not be confused with traditional or offline "dead box" forensics. The key difference is that live machine forensics collect and analyze data while a machine is still running – this means that artifacts can and will change in memory or on disk while it is collecting. For comparison, offline collections utilize write blockers while acquiring images to prevent writing to disk and tampering with evidence.

Several tasks that assist with forensic workflows are included with Fidelis Endpoint including:

- Full Disk Imaging
- — When needed full disk images can be remotely collected in either E01 or S01 format
- File Collection
- — While investigating it is often beneficial to be able to collect1 files for deeper review and analysis; Fidelis Endpoint can collect single files, or multiple files easily.
- — File collections are based on search filters and can be as specific or broad as needed, including multiple criteria such as file creation dates, paths, extensions, hash, file content, and more.
- — Files can be collected in native format or wrapped in a logical forensic container (AD1) format that preserves all filesystem metadata and is verifiable.
- — Optionally, in lieu of collecting files, a File Metadata collection can be performed. This allows for quickly obtaining data about files matching the filters and can help scope the number of files and data that would be returned prior to a collection.
- Memory Collection
- — If an analyst wants to perform deeper memory analysis and forensics, Fidelis Endpoint can collect the full memory of a system into RAW or AFF4 formats. Analysts can then perform analysis in their tool of choice, such as Volatility.
- Process Dump
- — If additional analysis is needed for a specific process or processes identified on an endpoint, analysts can easily dump the full memory for selected processes or choose to only collect specific items such as Handle Data, Thread Info, and more. These options let you target the specific items you need from the memory of a process and reduce the size of a collection.

- Live Memory Analysis
  - Before collecting or dumping the memory from an endpoint, analysts also have the option to perform live memory analysis. The analysis will return a process listing with additional memory details such as the addresses, privileges, and more. With optional switches the analysis can include additional details for each process such as the sockets, open handles, DLLs, and VADs.
  - Fidelis Endpoint performs the analysis live on the target machine2 , returning the parsed results. This is a quick way to perform an initial triage to identify hidden processes, injected DLLs, and more prior to performing deeper memory analysis from a collection.

In addition to the above forensic tasks, Fidelis Endpoint is able to automatically collect a copy of every binary or script3 executed on an endpoint in an Executable File and Script Collection. The samples are stored centrally allowing for quick analysis via the built-in Hex or Text editor, gaining additional context and details from Threat Lookup, or for downloading a copy of the sample for further analysis. This ensures that even in the event a malicious executable deletes itself, a copy is available for analysis. Analysts can also search for the sample against collected metadata to see every occurrence and the details of its behavior.

The performance impact to systems and users is often of concern when performing any actions against an endpoint. When performing live forensics, a user may notice some spike in resource utilization for example during collections, however the user is still able to continue working. The system uses built-in operating system scheduling techniques to ensure that investigation techniques do not interfere with other uses of the machine. This contrasts with traditional forensic collections where a user is separated from their computer so drives can be imaged manually in order to collect artifacts. The performance impact that may be experienced becomes less of a concern when a user can keep working, and analysts can acquire artifacts faster and more efficiently.

As described above, Fidelis Endpoint can assist with common forensic use cases during an investigation reducing the time to triage and respond to an incident. Advanced users can take advantage of full memory collection or process dumps for deeper analysis in other tools. While Fidelis Endpoint isn't intended to replace or provide all the features of a traditional "dead box" forensic tool, when properly utilized it augments existing capabilities making collection of artifacts faster and easier.

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, however, 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.
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.

Feature	Category	Description
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.
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.

Feature	Category	Description
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.
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.

Feature	Category	Description
Fidelis Antivirus (optional add-on)	Prevention Detection	Fidelis Antivirus, powered by Bitdefender, adds additional prevention and detection capabilities to Windows endpoints. Fidelis Antivirus adds signature, heuristic, and behavior-based prevention of both known and unknown malware in addition to boot sector protection. Security analysts can quickly pivot from AV alerts to process tree event details to learn the context and source of the malware. Fidelis Antivirus is optional enabling customers an open choice of AV for endpoints.
Process Behavior Blocking (requires Fidelis AV)	Prevention Detection	Process behavior blocking is included with Fidelis Antivirus and uses machine learning models to analyze process behaviors for malicious activity. Threat intelligence updates for AV indicators also include behavior model updates.
Global Quarantine (requires Fidelis AV)	Prevention Detection	Global Quarantine is a centralized location for all detected malware from Fidelis Antivirus for customer deployments. When Fidelis AV detects or prevents a threat on the endpoint it automatically sends a copy of the malware sample to the customer's Global Quarantine where security analysts 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.
Process Blocking	Prevention Detection	Customers can quickly block processes by IOC hash or leverage the power of YARA rules from threat intelligence feeds to block advanced threats from executing and spreading across the enterprise. Process blocking runs independent of AV engine choice on endpoints for added prevention.

about fidelis security

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.

Fidelis™ Cybersecurity