Fidelis Cybersecurity

DATASHEET

Fidelis Endpoint®

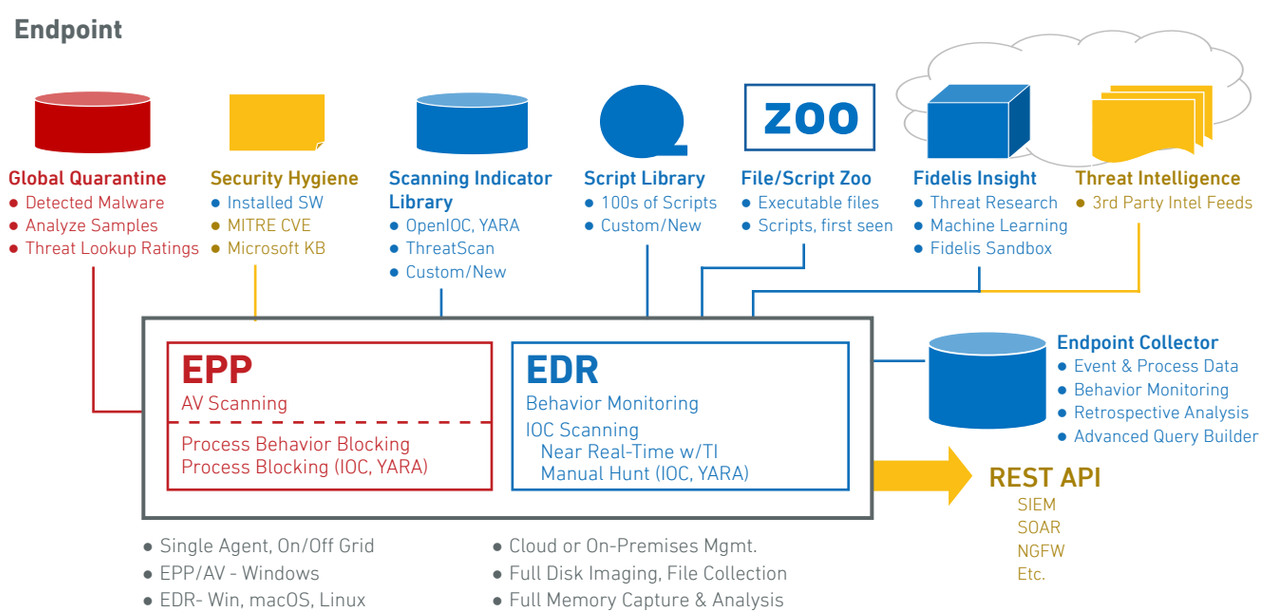
Single Agent Prevention, Detection, Investigation and Response

Fidelis Endpoint combines robust capabilities across endpoint protection, EDR, forensics and investigation and system management, all in one agent.

Fidelis Endpoint has a single agent architecture that runs on and off grid defenses supported by cloud or on-premises management. It provides powerful features for the most advanced and mature security operations and is scalable to 100,000s of endpoints.

Fidelis Endpoint uniquely provides the following:

- Single AV and EDR Windows agent with best in class AV and unmatched EDR features
- Advanced EDR features with IOC and YARA indicators for Windows, macOS, and Linux systems
- Event and process metadata for real-time and retrospective analysis, plus a file/script zoo
- Open threat intelligence feeds (Fidelis Insight, Open Source & 3rd Party, Internally Developed)
- Automated prevention, detection, investigation and response functions, plus custom scripts
- Optional MDR service for 24/7 coverage with detection, response, and analyst communications



Fidelis Endpoint provides prevention (red), detection and response (blue), and third-party intelligence and integration (tan) in a single agent with on/off grid defenses.

Prevention

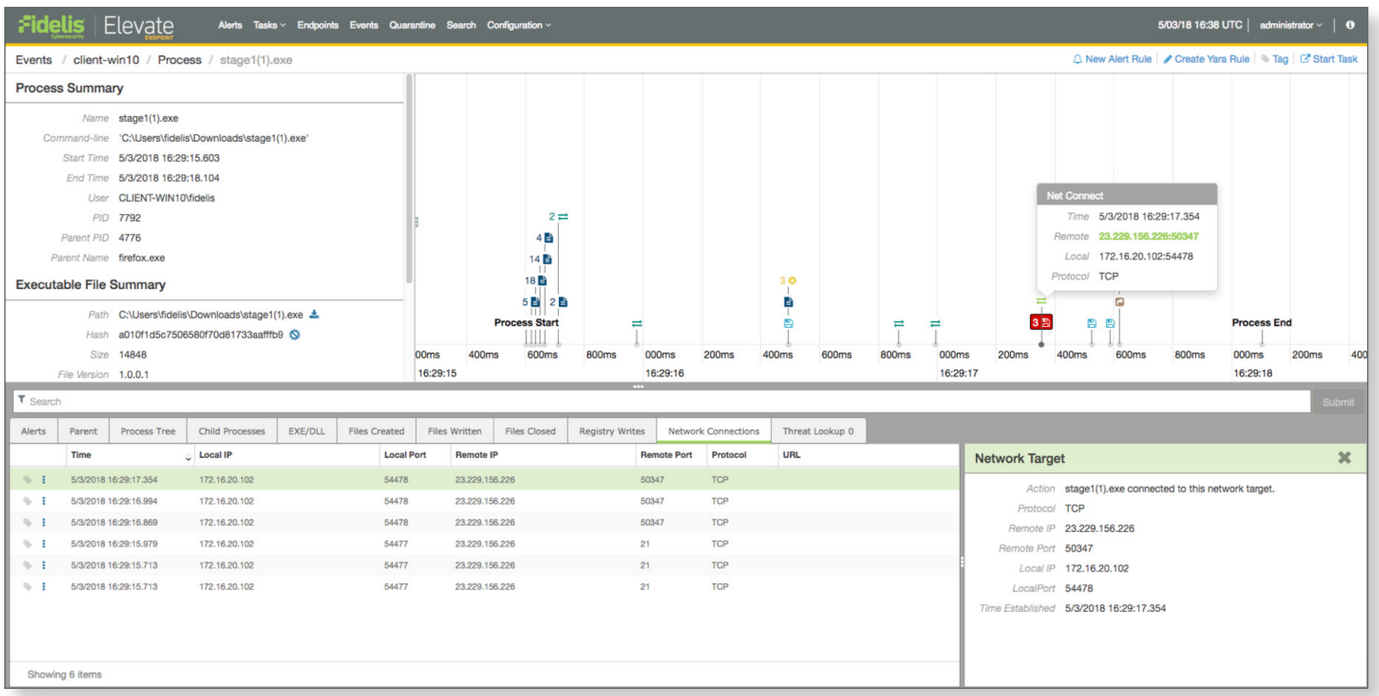
- **Best in class AV prevention** for Windows from BitDefender using behavioral, heuristic and signature defenses, including boot sector prevention and a global quarantine of detected malware for analysis
- **Threat Lookup** provides cloud-based detection ratings from multiple scanners
- **Threat intelligence** updates include ML behavior models and AV file indicators for on or off grid prevention for endpoints
- **Process behavior blocking** along with using IOCs and YARA rules to block processes across the enterprise for endpoints function independently of customer choice for AV engine
- **Installed software reporting** for endpoints with known vulnerabilities and links to MITRE CVE or Microsoft KB reports
- **Security hygiene for endpoints** including operating system status and applying patches, ability to report and change host FW and AV status, plus alerts for USB insertions
- **Quickly pivot from AV alerts into the process tree** with event details providing context into the source of malware leveraging the value of combined prevention and detection
- **Avoid the false positives and manual tuning** of white lists, isolation containers and stand-alone ML anomaly detection for prevention

Detection

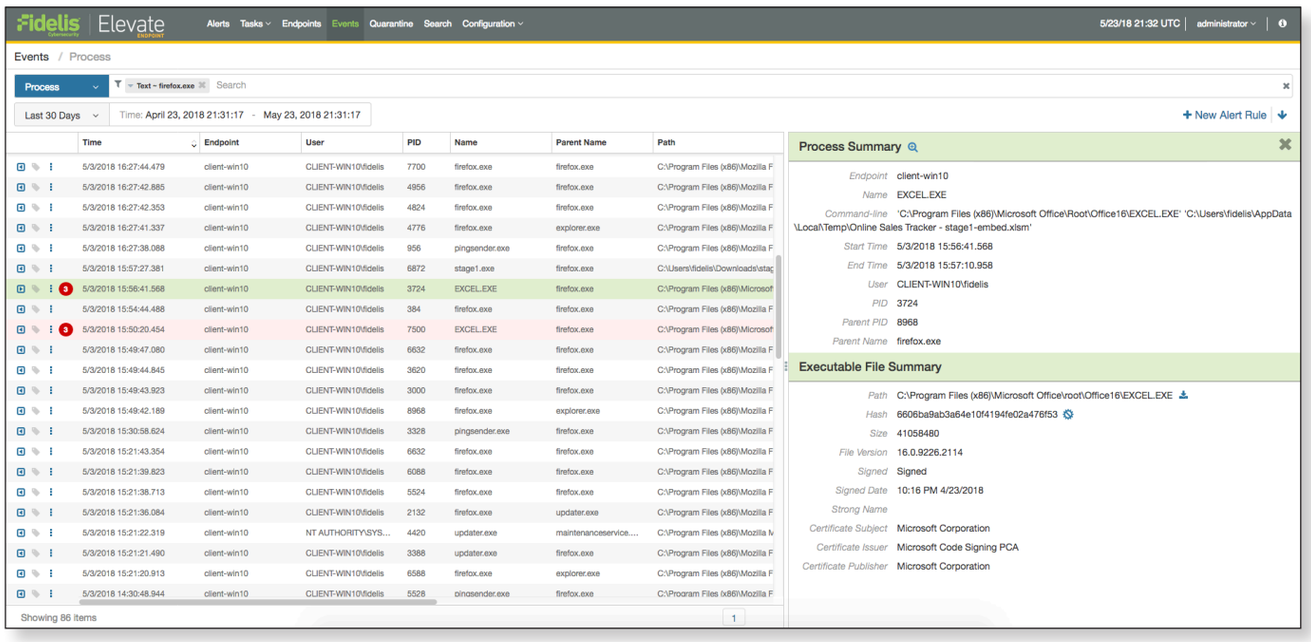
- **Advanced EDR features** for Windows, macOS and Linux systems
- **Open threat intelligence feeds** from third-party sources, internally developed, and from Fidelis Insight (including sandboxing, machine learning, and threat research)
- **Custom behavioral rules** using behavioral indicators alongside Fidelis provided behavioral rules
- **Scanning Indicator Library** fully stocked with IOC and YARA indicators out of the box, plus the ability to upload new OpenIOC and YARA indicators
- **30, 60 or 90 days of rich event and process metadata** for real-time and retrospective analysis using threat intelligence feeds, plus supporting custom searches and hunting
- **Automatically apply threat intelligence** to detect threats from system events on Windows systems
- **Playback analysis** enables recording of key events and automatically delivers a timeline related to suspected incidents, along with the prioritized alerts
- **On-demand scanning** of file systems and memory using the Scanning Indicator Library
- **On/off grid support** where intelligence and detection are local and data is cached until reconnected and jobs resume

NEW — Executable File and Script Zoo

- Collects a first time copy of executable files and scripts from endpoint
- Addresses the problem of malicious software deleting files or hiding traces



The event timeline provides visibility and context around all endpoint activity including alerts, parent processes, the process tree, child processes, loaded DLL and exe files, files created, files written, files closed, network connections, and threat lookup.



Fidelis Endpoint captures and stores event and alert data to enable threat hunters to easily search for, identify, and investigate threats and adversaries.

Investigation

- **Proven forensic integrity** with full disk imaging to forensic containers, plus file and folder collection, memory capture, and live memory analysis
- **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
- **Endpoint Collector** provides real-time and retrospective investigations, plus supports custom searches and hunting
- **Advanced Query Builder** goes beyond faceted searches with Boolean logic for investigation, behavior rule creation, and threat hunting
- **Installed software report** for endpoints including known vulnerabilities with links to MITRE CVE and Microsoft KB reports
- **Endpoint system isolation** for investigations with access to the console or a desired specific system
- **Script Library** includes pre-built scripts to collect artifacts for investigation automation, plus custom created scripts so manual efforts become automated going forward for investigations

Response

- **Automated playbooks and custom alert responses** can isolate endpoints to console access and running playbooks, or running triage tasks for evidence gathering and memory dumps
- **Scripts** can restore endpoints to a known good configuration
- **Built in responses** include terminating processes, collecting or deleting files where the Script Library provides pre-built response scripts, plus supporting new and custom scripts for response
- **Out of the box integration** with FireEye, Palo Alto Networks and SIEMs and NGFWs of choice is supported by REST API

Management

- ✓ Dynamic groups based on characteristics automatically update and enable improved segmentation, plus easier policy management
- ✓ Alert subscriptions can be configured by severity for email, Microsoft Teams, Slack, etc.
- ✓ System management scripts provide hardware and operating system profiles, software inventory, checking for installed updates and hotfixes, and forcing updates
- ✓ Connected Agents status provides a profile of online and active, or hardly seen endpoints
- ✓ System health page provides status of services, servers, and containers, plus the ability to collect logs and start/stop services
- ✓ Role-based access controls are provided for endpoints, scripts and system level permissions
- ✓ Endpoints use secure agent communications based on a TLS v1.2 encrypted WebSocket connection for lightweight and fast communications and responses

Deployment Options

On-Premise:

- You maintain and manage all software
- Fidelis professional services assists with deployment and training
- Maintenance fees includes intelligence updates from Fidelis Threat Research Team
- License additional agents as your needs grow

Cloud:

- Infrastructure maintained by Fidelis, so you can focus on security
- Rapid deployment and immediate implementation
- Scale up as you grow with as many endpoint agents as you need
- Uninterrupted service as you transition from a trial to production
- Simplified subscription pricing based on number of agents and storage needs

Fidelis Elevate Integration Advantages

- Fidelis Endpoint and Network are fully integrated for a single pane of glass to validate alerts from network to endpoints, plus understand the wider scope of threats from endpoints into network cross session and multifaceted analysis
- Fidelis Deception alerts seamlessly flow into Fidelis Endpoint to investigate compromised hosts where breadcrumbs on endpoints act as lures to decoys for post breach detection
- Fidelis Endpoint also automates breadcrumb distribution and freshness cycles for deterministic and effective deception

Optional Managed Detection and Response (MDR) Services

Fidelis Endpoint is a powerful surgeon's tool for prevention, detection, investigation and response with high degrees of automation through scripting, plus open threat intelligence and customization. Achieving 24/7 coverage with a thinly stretched security team can be challenging, that's why we offer an MDR service, leveraging our security experts with experience of over 4,000 cases.

Fidelis provides the advanced solutions, threat intelligence and managed services, including proactive incident response (IR) retainers.

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

– Director of Forensics and eDiscovery, Top Five Global Bank

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

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. 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.

