

Fidelis Endpoint®

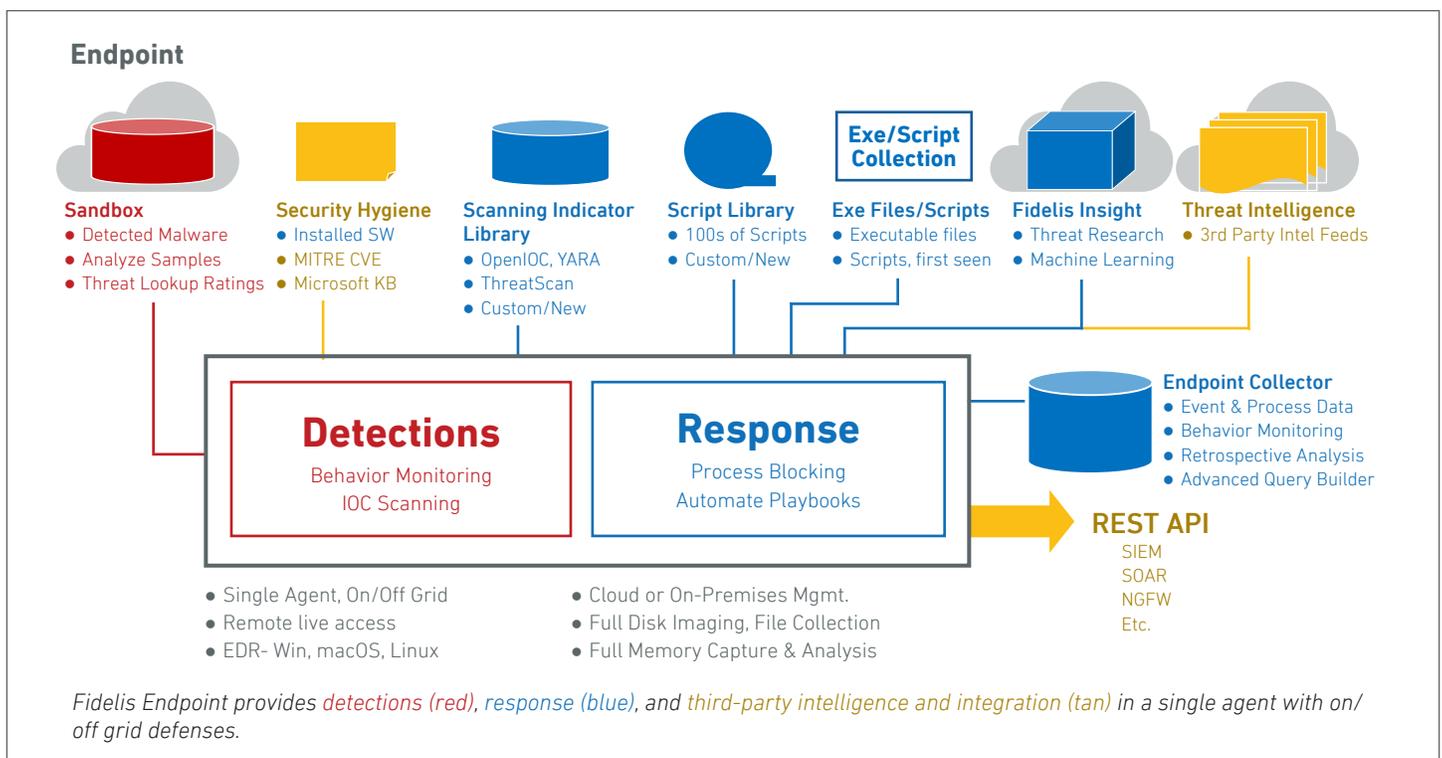
Speed Digital Forensics, Investigation and Response to Advanced Threats through a Single Agent and Console

Powerful Endpoint Detection and Response

Fidelis Endpoint provides deep visibility into all endpoint activity to enable analysts to detect, investigate, hunt and respond to advanced threats within minutes. Fidelis arms analysts to detect threats in real time and retrospectively, simplify threat hunting, prevent threats through process blocking that coexists with any AV solution, conduct deep forensic analysis, and automate responses with an Advanced Scripting Engine for limitless response options. Fidelis Endpoint has a single agent architecture that runs on and off grid defenses supported by cloud or on-premises management, and is scalable to 100,000s of endpoints.

Fidelis Endpoint enables analysts and incident responders to:

- **Map endpoint detections** to the MITRE ATT&CK™ framework to understand attacker TTPs and determine the proper response
- **Hunt for threats** via advanced EDR features with IOC and YARA indicators - across Windows, macOS, and Linux systems
- **Analyze event and process metadata** in real-time or retrospectively, and identify suspicious files/scripts seen for the first time
- **Remote access** into an endpoint's disk, files, and processes for faster response
- **Open threat intelligence feeds** (Fidelis Insight, Open Source & 3rd Party, Internally Developed)
- **Full software inventory and identification** of vulnerabilities with links to MITRE CVEs or Microsoft KB Reports
- **Automated protection, detection, investigation and response functions**, plus custom scripts
- **Optional MDR service** for 24/7 coverage with detection, response, and analyst communications



Visibility and Detection

- Advanced EDR features support Windows, macOS, and Linux systems
- Map endpoint behaviors to MITRE ATT&CK to understand attacker TTPs
- Access open threat intelligence feeds from third-party sources, internally developed, and from Fidelis Insight (including sandboxing, machine learning, and threat research)
- Automate responses using a library of predefined behavioral rules and the ability to create and customize your own
- IOC and YARA library that can be expanded and customized
- 30, 60, or 90 days of rich event and process metadata for real-time and retrospective analysis and hunting against the most current threat intelligence
- Automatically apply threat intelligence to detect threats from system events
- Playback key events and review the timeline of suspected incidents
- On-demand scanning of file systems and memory using the Scanning Indicator Library
- Detects executable files and scripts seen for the first time – critical for visibility of files being deleted or hidden attacker traces

- Automatic submittal of untrusted executables to cloud sandbox for analysis
- On/off grid support where intelligence and detections are local and data is cached until reconnected and jobs resume

Forensics, Response and Prevention

- Take actions and collect data with a customizable library of scripts and playbooks
- Speed investigations and analysis with remote access into endpoint disks, files, and processes
- Remotely collect forensically sound data memory captures and full disk images
- Integrate with SIEMs, NGFWs, and more to execute response actions
- Automate remediation, deep analysis, or custom actions with response playbooks
- Threat Lookup provides cloud-based detection ratings from multiple scanners
- Block processes across enterprise endpoints using IOCs and YARA rules
- Identify vulnerabilities with installed software reporting for endpoints
- Manage security hygiene with reporting on system status patches, AV status, and USB utilization

Information Alerts 1679 Installed Software Task History USB Behaviors Live									
Search...									
	Name	PID	CPU %	Memory	Priority	User	Elevated	MD5	
	abrt-watch-log	768	0	4.41MB		root		6b893c479f180c5be0e632def0e81e7	
	abrt-watch-log	778	0	4.41MB		root		6b893c479f180c5be0e632def0e81e7	
File System	Actions			0	5.28MB	root		bf7fe0776ada30d5085cdfd5a1c73a7	
	End Process			0	3.61MB	root		45e17648ea20943dd032d1101749b9	
	End Process Tree			0	0.98MB	root		d8a9ebf94b8251123a71f49160e6e11	
	End Process on Multiple Endpoints			0	3.25MB	gdm		0318d47f45bc437f1504a39579d513	
	Search/End Process on Multiple Endpoints			0	3.32MB	gdm		10f84d430f3d03e572abd8848ea7f34	
	Add Hash to Process Blocking			0	0B	root		23dcc43ae6757a30d115771f4623cf	
	Open File Location			0	964KB	root		d22eefc1f44f73dfb721d84da86e095	
	Create Dump File			0	828KB	root		8c2be7568ae11bde1ded6a237ead03	
	View Behaviors			0	1.76MB	root		8c2be7568ae11bde1ded6a237ead03	
	View Behaviors On All Endpoints			0	1.68MB	avahi		6cd98259caaf9a9080040ed794eb56	
Processes	View Behaviors On All Endpoints			0	244KB	avahi		6cd98259caaf9a9080040ed794eb56	
	View Executable			0	2.92MB	root		8aea7ca46ed391c2e0a4da90d8c725	
	Properties			0	0B	root			
	bioset	475	0	0B		root			
	caribou	2958	0	7.09MB		gdm		d0a71632262f52a6a13fe63c6466e0f	
	chronyd	786	0	1.59MB		chrony		2c6726457d55372f200360a24c03df	
	colord	2902	0	7.76MB		colord		4e1d8c63b9ee31924aa6c5ffb2b640f	
	cron	1437	0	1.65MB		root		7cca078ca111b74597922f14154a57	
	crypto	38	0	0B		root			
	cupsd	1420	0	3.93MB		root		05e6573c8f36a5ce6a6128e273ae9a	

With Live Console, users gain direct, remote access into an endpoint's disk, files and processes, to more quickly mitigate threats found on an asset.