Fidelis Cybersecurity

DATASHEET

Fidelis Sandbox

A Key Method of Malware Detection in the Cloud or On-Prem

Overview

The Fidelis Sandbox is a critical component of Fidelis Elevate™ — available via the cloud or on-premises — providing an isolated virtual execution environment for the detonation of suspicious objects. By observing execution behaviors of suspicious objects, the Sandbox detects malware that is difficult to find using only static analysis.

Fidelis Elevate™ monitors an organization's network in real - time by reassembling, decoding, and analyzing network traffic to detect advanced attacks and prevent data theft. At the core of Fidelis Elevate's operations is the Malware Detection Stack - consisting of Deep Session Inspection, the Malware Detection Engine and Sandbox components. Deep Session Inspection extracts artifacts through a deep decoding tree, while the Malware Detection Engine uses static and emulation analysis as the second layer of detection. Fidelis Sandbox conducts the third layer of detection in an isolated virtual execution environment that allows samples to call out as they would in normal operations.

Fidelis Sandbox Analysis

Analysis is performed on execution behavior such as: writes to the file system, registry modifications, and network activity. Analysis is also performed on all dropped objects written to disk or memory. Fidelis Elevate sensors are placed on the active call out network and full analysis of all network activity is conducted. The results of all analysis are displayed in the Sandbox report that carries a malware score, and the results are associated with the alert created because of the malicious file or site. Each file and URL is stored along with the Sandbox Report within the Fidelis platform. This data is used to drive malware detection and prevention:

- If the file or site is submitted again, the report can be returned immediately.
- IOCs can be extracted from the reports and added to Fidelis IOC feeds, completing the loop so that everyone in the Fidelis community becomes protected soon after the first detection. IOC feeds can be applied to Fidelis Elevate sensors and Fidelis Endpoint® agents for future detections, as well as to detect indicators that may have been present before the first detection.
- Detections are used to feed Fidelis' malware prevention feed. Once malware has been detected, a file hash can be created in a Fidelis proprietary format to detect the file in transit and prevent successful transmission.
- Machine learning algorithms are performed against the stored database of files, URLs, and reports, with analysis results providing a rich set IOCs that lead to improvements in Fidelis policies to better detect future malicious and suspicious files and sites.

Key Features

- ✓ Observe malware execution in mutex, registry, API call, file system access, network behavior and artifacts
- ✓ Understand malware behavior by observing malware's Internet access behavior in its full life cycle or simulating interaction with malware execution and recording the network behavior
- ✓ Identify malware evasion behaviors such as delayed execution, environment diagnostics and checking human interaction
- ✓ Share malware forensics with other Fidelis components for immediate prevention and used to protect against future attacks

Submitting Suspicious Files to the Fidelis Sandbox

Submissions to the Fidelis Sandbox includes the following methods:

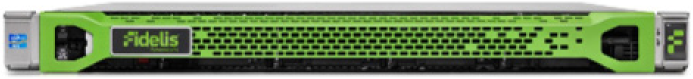
- Files and URLs detected as malicious by the Malware Detection Engine on Network sensors are submitted for analysis. The result is a Sandbox Report that provides a detailed analysis of the execution of the file or the URL when visited by a browser.
- Files and URLs deemed suspicious by the Network sensor are submitted for analysis. These files and URLs were not detected as malicious by the real-time analysis on the agent or sensor, but were submitted due to suspicion raised based on the content of the file or the context of the file or the content under which the file or URL was detected. A Network Alert or Alert will only be generated if the Sandbox Report indicates high confidence of malicious activity
- Files and URLs may be manually submitted by a CommandPost user. This process will generate a Fidelis Elevate alert regardless of the content of the Sandbox Report. The generated alert can be visited to view the report.
- Any file written to a decoy is automatically submitted for analysis.

Fidelis Sandbox Appliance Technical Specifications

The Fidelis Sandbox appliance is available to customers unable to submit files to Fidelis Insight. Care must be taken if the appliance is used to fully execute samples including the ability to make network calls. The network calls can be disabled if it is not possible to instrument the appliance properly in your environment.

The appliance can execute approximately 20,000 samples per day and can be shared by multiple Fidelis CommandPosts within your enterprise. File submissions are based on the Malware Detection Engine and can be augmented by custom rules using the Sandbox rule action.

Note: The sandbox rule action is only available on a CommandPost that includes a Fidelis Sandbox component.



Fidelis Sandbox 20 / Collector SA2 Appliance	
Form Factor	1U HPE ProLiant DL360 Gen10 Chassis
CPU	Dual Gold 6246 12/24-core 3.3Ghz
TPM	No
Memory	192 GB ECC DDR4 2933Mhz
Storage Capacity & Configuration	300 GB 2x HDD RAID-1 1.2 TB (3.6 TB Effective) 6x HDD, RAID-10
Network Adapters	4x 1GbE
Out of Band Management	3 Year ILO- HPE Advanced 24x7 Tech Support and Updates
Dimensions	H: 4.29 cm (1.69 in) W: 43.46 cm (17.11 in) D: 70.7 cm (27.83 in)
Weight (appx.)	16.27 kg (35.86 lb)
Power Supply	Dual hot-swap 800W High Efficiency AC power supplies
Operating Temperature	10° to 35°C (50° to 95°F) at sea level
AC Input Requirements	100 - 120 VAC 200 - 240 VAC
BTU Rating (max)	3067 BTU/hr (100 VAC) 2958 BTU/hr (200 VAC) 2949 BTU/hr (240 VAC)

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.