DATASHEET

Fidelis Sandbox

A Key Method of Malware Detection n the Cloud or On Premise

Overview

The Fidelis Sandbox is a critical component of Fidelis Elevate® that provides an isolated virtual execution environment, either on-premises or in the cloud, 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 and signatures.

Fidelis Elevate is an extended Detection and Response (XOR) platform that monitors an organization's environment using a combination of network sensors, endpoint agents, and deceptive decoys. The Fidelis Cloud Sandbox is included for all Fidelis Elevate customers. The Fidelis Sandbox Appliance is available for Fidelis Network customers who cannot use the cloud.

Fidelis Network® sensors work in real-time by reassembling, decoding, and analyzing network traffic to detect advanced attacks and data theft. Fidelis Endpoint® agents monitor every process and user behavior on managed systems. Fidelis Deception® decoys are placed in the environment to lure and attract attackers. In each case, suspicious files and web site URLs are sent to the sandbox for detonation and determination.

With Fidelis Deception in place, any file written to a decoy is considered highly suspicious and is sent to the sandbox for analysis. The Fidelis Network sensors and Fidelis Endpoint agents have embedded AV engines, signatures, and static file analysis components that may detect malware and prevent the network transfer or the execution of the file. In this case, Fidelis Sandbox provides execution forensics for the Fidelis Elevate user. Sensors and agents can also detect suspicious files based on network or file characteristics, which are also sent to the sandbox and will generate an alert if found to be malicious.

Fidelis Sandbox Analysis

Fidelis Sandbox 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. The results of all analysis are displayed in the Fidelis Sandbox report that carries a malware score. The report is associated with the alert created due to the malicious file or web site. Each file and URL is stored along with the report within the sandbox. This data is used to drive malware detection and prevention:

- If the file or site is submitted again, the report can be returned immediately
- Indicators of compromise (IOC) can be extracted from the reports and added to Fidelis Security IOC feeds, completing the loop so that everyone in the Fidelis Security 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 Security's malware prevetion feed. Once malware has been detected, a file hash can be created in a Fidelis Security 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 of IOCs that lead to improvements in Fidelis Security 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 lifecycle 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 Security components for immediate prevention and use to protect against future attacks
- Perform machine learning modeling on the execution results to detect new strains of malware that are undetectable by other methods

Submitting Suspicious Files to the Fidelis Sandbox

Submissions to the Fidelis Sandbox includes the following methods:

- Files and URLs detected as malicious by Fidelis Network sensors are submitted for analysis. The result is a Fidelis 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 Fidelis Network sensor are submitted for analysis. These files and URLs were not detected as malicious by the real-time analysis on the sensor, but they 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 Fidelis Network alert will only be generated if the Fidelis 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 Fidelis Sandbox report. The generated alert can be visited to view the report.
- Fidelis Endpoint collects and examines several data points from the execution of every installed software, file, or script across the environment. Suspicious files are automatically sent to the sandbox for analysis, and the reports and malware scores are made available on the Executables UI page.
- Fidelis Network and Fidelis Endpoint are configurable for determining which files are sent to the sandbox.
- For Fidelis Deception, any file written to a emulation decoy is suspicious and is automatically submitted for sandbox analysis
- Analysts may submit files manually, either from the Fidelis Endpoint Executables page, or through the UI or API interface.

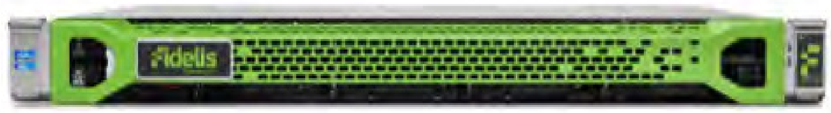
Fidelis Sandbox Appliance Technical Specifications

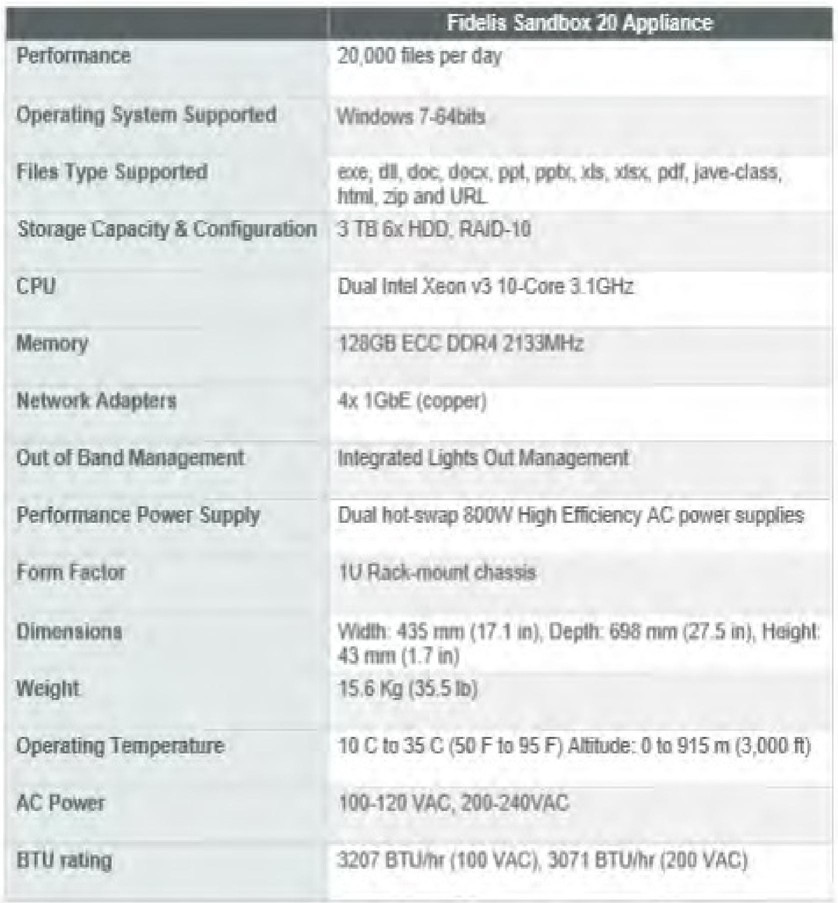
The Fidelis Sandbox appliance is available to Fidelis Network customers who are unable to submit files to the cloud sandbox. Care must be taken if the appliance is used to fully execute samples including the ability to make network calls. Network calls can be disabled if it is not possible to instrument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

The appliance works with Fidelis Network and can execute approximately 30,000 Linux or Windows 7 samples per day, or approximately 25,000 Windows 10 samples per day. It can be shared by multiple Fidelis CommandPosts within your enterprise. File submissions can be augmented by custom rules using the Fidelis Sandbox rule action for customer Fidelis Network rules. A single Fidelis Sandbox appliance can execute files from different operating systems concurrently. Multiple appliances can be registered to a CommandPost to scale horizontally.

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

Technical Specifications





	Fidelis Sandbox 20 Appliance
Performance	20,000 files per day
Operating System Supported	Windows 7-64bits
Files Type Supported	exe, dll, doc, docx, ppt, pptx, xls, xlsx, pdf, jave-class, html, zip and URL
Storage Capacity & Configuration	3 TB 6x HDD, RAID-10
CPU	Dual Intel Xeon v3 10-Core 3.1GHz
Memory	128GB ECC DDR4 2133MHz
Network Adapters	4x 1GbE (copper)
Out of Band Management	Integrated Lights Out Management
Performance Power Supply	Dual hot-swap 800W High Efficiency AC power supplies
Form Factor	1U Rack-mount chassis
Dimensions	Width: 435 mm (17.1 in), Depth: 698 mm (27.5 in), Height: 43 mm (1.7 in)
Weight	15.6 Kg (35.5 lb)
Operating Temperature	10 C to 35 C (50 F to 95 F) Altitude: 0 to 915 m (3,000 ft)
AC Power	100-120 VAC, 200-240VAC
BTU rating	3207 BTU/hr (100 VAC), 3071 BTU/hr (200 VAC)

About Fidelis Security®

Fidelis Security® is the industry innovator in proactive cyber defense, safeguarding modern IT for global enterprises with proactive XDR and CNAPP platforms. Fidelis Security consolidates IT security operations to shrink attack surfaces, automate threat detection, and accelerate analysis, forensics, and response so that organizations remain resilient through cyber-attacks and emerge stronger and more secure. Fidelis Security is trusted by top commercial, enterprise, and government agencies worldwide.