

## Fidelis Sandbox Appliance

The Fidelis Sandbox appliance is a virtual execution and determination environment and is an integrated component of the Network Detection Stack. By integrating the Virtual Execution Environment with Deep Session Inspection® and the Malware Detection Engine, Fidelis Network™ enables organizations to identify when they're being attacked, retrace the attackers' footprints and prevent data theft at every stage of the attack lifecycle.

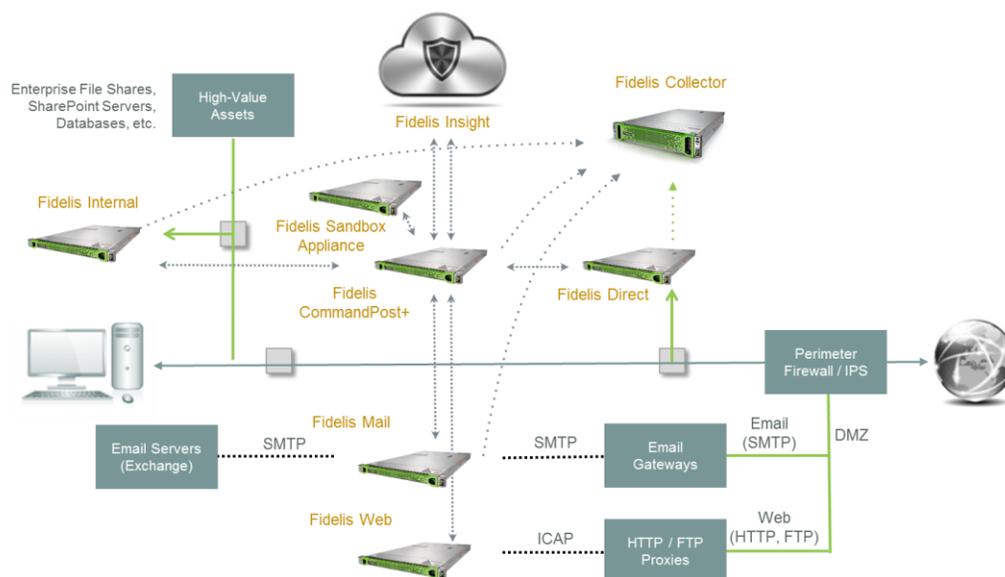
## Fidelis Network™ Advanced Malware Protection Architecture

The **Fidelis Sandbox Appliance** is 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 Network monitors your network in real-time by reassembling, decoding, and analyzing network traffic using patented Deep Session Inspection technology to detect advanced attacks and prevent data theft. At the core of Fidelis Network'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. The Malware Detection Engine uses static and emulation analysis in the second layer of detection. And the Sandbox conducts the third layer of detection in an isolated virtual execution environment.

### Key Features:

- Observe malware execution in mutex, registry, API call, file system access, network behavior and artifacts.
- Routed mode observes malware's Internet access behavior in its full life cycle. In isolated mode, the network simulator interacts with malware execution and records network behavior.
- Malware evasion behaviors such as delayed execution, environment diagnostics and checking human interaction are seen and used to detect malware.
- Malware forensics are shared with other Fidelis Network components for immediate prevention. Threat data is shared via Fidelis Insight to all Fidelis customers to protect against future attacks.



Fidelis Network Product Architecture

## Technical Specifications



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