Fortinet

BREACH DETECTION SYSTEM

AUTHOR: Jason Pappalexis CONTRIBUTORS: Andrew Braunberg, Paula Musich

Fortinet has built its reputation in the network security space on high performance and competitive pricing, themes that continued with the 2013 release of its breach detection system (BDS), FortiSandbox. Available first as a cloud service (within the FortiCloud offering) and then as local appliances, FortiSandbox provides sandbox-based malware detection to the Fortinet suite of products. A succession of updates within the last six months illustrates Fortinet's commitment to feature enhancement and product stability. In May 2015, Fortinet announced the integration of FortiMail v5.2.4 with FortiSandbox 1.4, and in July 2015, the vendor released v2.1 of FortiSandbox, which includes automated signature generation. Fortinet has recently released v5.4 of FortiClient, which is designed to dynamically accept automated FortiSandbox updates.

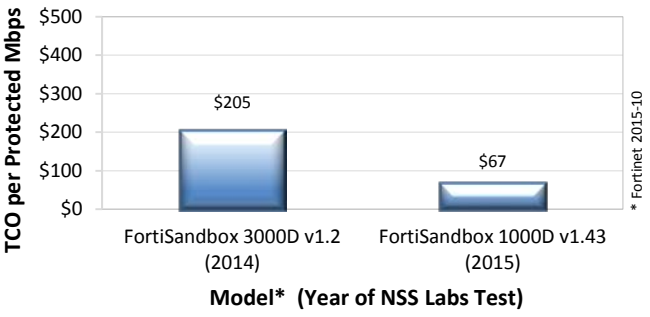
Portfolio

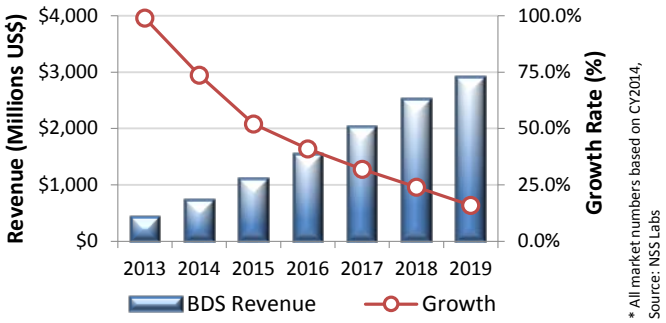
DEPLOYMENT OPTIONS	Physical appliance, virtual appliance, cloud service	
PRODUCT	**FSA-1000D** • Sandboxing 160 files per hour • Antivirus scanning 6,000 files per hour • 8 virtual machines	**FSA-3000D** • Sandboxing 560 files per hour • Antivirus scanning 15,000 files per hour • 28 virtual machines

*Models listed are available at time of publication.

- The following products can send files to FortiSandbox for inspection: the FortiGate firewall, next generation firewall (NGFW), intrusion prevention system (IPS), secure web gateway (SWG), and unified threat management (UTM) products; the FortiMail secure email gateway (SEG), the FortiClient endpoint, the FortiWeb web application firewall (WAF), and the FortiSwitch products.
- The FSA-3000D hardware was upgraded in early 2015.

Total Cost of Ownership and Market Summary





- At US$67, the *TCO per Protected Mbps* for the FortiSandbox 1000D was better than the average *TCO per Protected Mbps* for the 2015 NSS Labs BDS group test (US$169).
- The BDS market is expected to grow by 41 percent in 2016 and is projected to have a compound annual growth rate (CAGR) of 32 percent over the forecast period.
- A strong interest in post-incident forensics is driving the market.

Recent Developments

July 2015

FortiSandbox v2.1 released; automated local updates permitted to integrated products; FortiSwitch v3.3 released

August 2015

Rated as *Recommended* in NSS' BDS v2.0 group test; FortiWeb 5.4 integrated with FortiSandbox

September 2015

FortiClient 5.4 released, dynamically utilizes FortiSandbox updates

Buyer Considerations

FACTORS	OVERALL	SIX-MONTH TREND	
Product Innovation	NEUTRAL	POSITIVE	• Released FortiSandbox v2.1, which includes the ability to deliver automated local updates to integrated products, updated malware, and malicious URL detection • Leverages Fortinet's more mature security products (for example, widget-based administrative console)
Product Features	POSITIVE	POSITIVE	• Dynamically generated threat intelligence delivered to integrated products • Supports custom application control and IPS signature capabilities • Incorporates FortiGuard technology
Integrations and Third-Party Support	NEUTRAL	NO CHANGE	• Integrates with security information and event management (SIEM) vendors (such as HP ArcSight, IBM Security's Q1 Labs, and LogRhythm) when used with FortiAnalyzer • JSON API available
TCO	NEUTRAL	POSITIVE	• Fortinet products perceived as cost-effective, although FortiSandbox hardware may be out of reach of some SMBs; virtual appliances are lower-cost options

COMPETITIVE FEATURES	
Platform	Stand-alone product that can integrate with other Fortinet products
Form Factor	Cloud service, physical appliance, virtual appliance
Deployment Mode	Network (out of band), integration with FortiGate (NGFW, NGIPS, SWG, UTM), FortiClient, FortiMail, FortiSwitch, FortiWeb
Scanning	Focus on primary protocols (for example, HTTP, SMTP, SMB, FTP), including SSL-encrypted protocols
Sandbox Location	Local appliance and cloud service
Customizable Sandbox	Feature not available
Host Remediation	FortiClient 5.4 permits devices to be quarantined or removed

STRENGTHS

- During the 2015 NSS BDS group test, the FortiSandbox 1000D achieved a 97.3 percent breach detection rate and demonstrated a *TCO per Protected Mbps* of US$67. Both scores resulted in the product receiving a *Recommended* rating. During the test, the device:
  - Detected 98.7 percent of all HTTP malware, 99.1 percent of all email malware, 94.5 percent of drive-by exploits, and 96.3 percent of social exploits, which resulted in its overall rating of 97.3 percent
  - Passed all stability and reliability tests
- Fortinet offers a file testing service that allows companies to evaluate sandboxing and advanced threat detection within FortiSandbox prior to purchasing.
- The new FortiSandbox-VM with API expands deployment options, for example, within virtual data centers.
- Fortinet has received an NSS *Recommended* rating for perimeter and endpoint security products (NGFW/NGIPS/WAF/EPP), including BDS.

WEAKNESSES

- In the 2015 NSS BDS group test, Fortinet FortiSandbox 1000D detected 66.7 percent of all evasions.

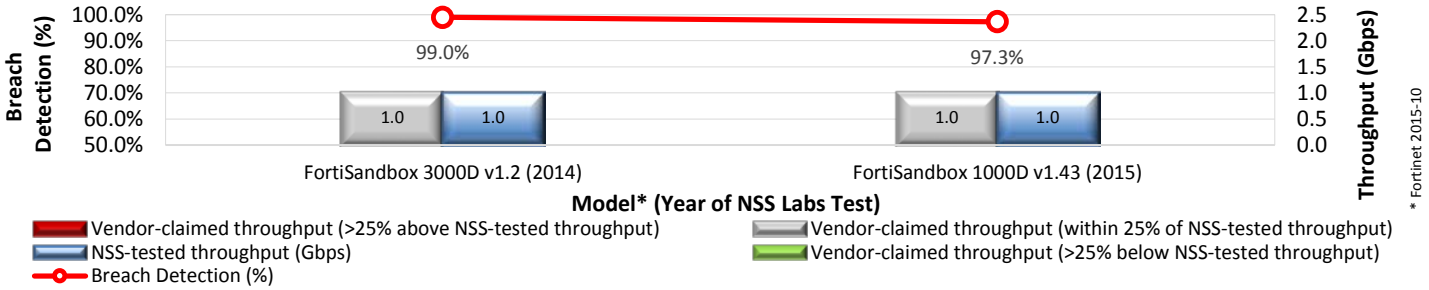
OPPORTUNITIES

- Fortinet has growth opportunity moving upmarket. The company traditionally has had a beachhead in the SMB segment and has steadily evolved its technologies. The introduction of FortiSandbox provides a way to address the needs of enterprise and service provider customers.
- FortiSandbox technology is being integrated into Fortinet's current product line, which provides additional upsell opportunities for the company.
- The ability to utilize custom virtual machines would increase the relevance of FortiSandbox.

THREATS

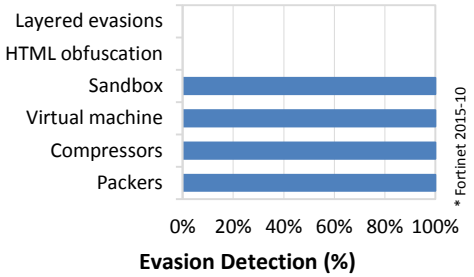
- While FortiSandbox is competitively priced for enterprises, the physical appliances may be expensive for many SMBs.

NSS Labs Group Test Results



At NSS, *Security Effectiveness* and throughput are critical metrics by which security devices are measured. NSS testing has shown:

- Fortinet's breach detection rate reached 97.3 percent overall, which was above the average of the 2015 NSS BDS group test.
- Vendor-claimed throughput aligned with NSS-tested throughput in 2014 and 2015.



- The 1000D detected:
  - 100.0 percent of sandbox evasions, virtual machine evasions, compressor evasions, and packer evasions
  - Zero layered evasions and zero HTML obfuscation evasions

Product	NSS Methodology Version	NSS-Tested Throughput	Breach Detection	TCO per Protected Mbps ($US)	NSS Labs SVM Rating
FortiSandbox 1000D (v2.10 build 0081)	Breach Detection Systems v2.0	1,000 Mbps	97.3%	$67	Evasion Retest
FortiSandbox 1000D (v1.43)	Breach Detection Systems v2.0	1,000 Mbps	97.3%	$67	**Recommended**
FortiSandbox 3000D (v1.2)	Breach Detection Systems v1.5	1,000 Mbps	99.0%	$205	**Recommended**

Test methodologies are found on the NSS Labs website at www.nsslabs.com.

NSS-tested throughput for the *NSS Labs Breach Detection Systems Methodology v1.5* was capped at 1,000 Mbps, and may not reflect the true maximum capabilities of the tested product. TCO per Protected Mbps corresponds to single sensor costs over a 3-year period.