BREACH DETECTION SYSTEMS COMPARATIVE REPORT

Security Value Map™ (SVM)

OCTOBER 19, 2017

Author – Thomas Skybakmoen

Tested Products

Check Point Software Technologies 15600 Next Generation Threat Prevention & SandBlast™ (NGTX) Appliance R77.30

Cisco FirePower 8120 v.6 & Cisco AMP v.5.1.9.10430

FireEye Network Security NX 10450 v7.9.2 & EX 8400 v7.9.0

FireEye Network Security 6500NXES-VA v7.9.2

Fortinet FortiSandbox-2000E v.FSA 2.4.1 & FortiClient (APT Agent) v.5.6.0.1075

Lastline Enterprise v7.25

Trend Micro Deep Discovery Inspector Model 4000 v3.8 SP5 & OfficeScan (OSCE) v.12.0.1807

Environment

Breach Detection Systems Test Methodology v4.0

Overview

Empirical data from individual Test Reports and Comparative Reports is used to create NSS Labs' unique Security Value Map™ (SVM). The SVM illustrates the relative value of security investment options by mapping the *Security Effectiveness* and the *Total Cost of Ownership (TCO) per Protected Mbps* (*Value*) of tested product configurations. The terms *TCO per Protected Mbps* and *Value* are used interchangeably throughout the Comparative Reports.

The SVM provides an aggregated view of the detailed findings from NSS' group tests. Individual Test Reports are available for each product tested. Comparative Reports provide detailed comparisons across all tested products in the areas of security, performance, and TCO.

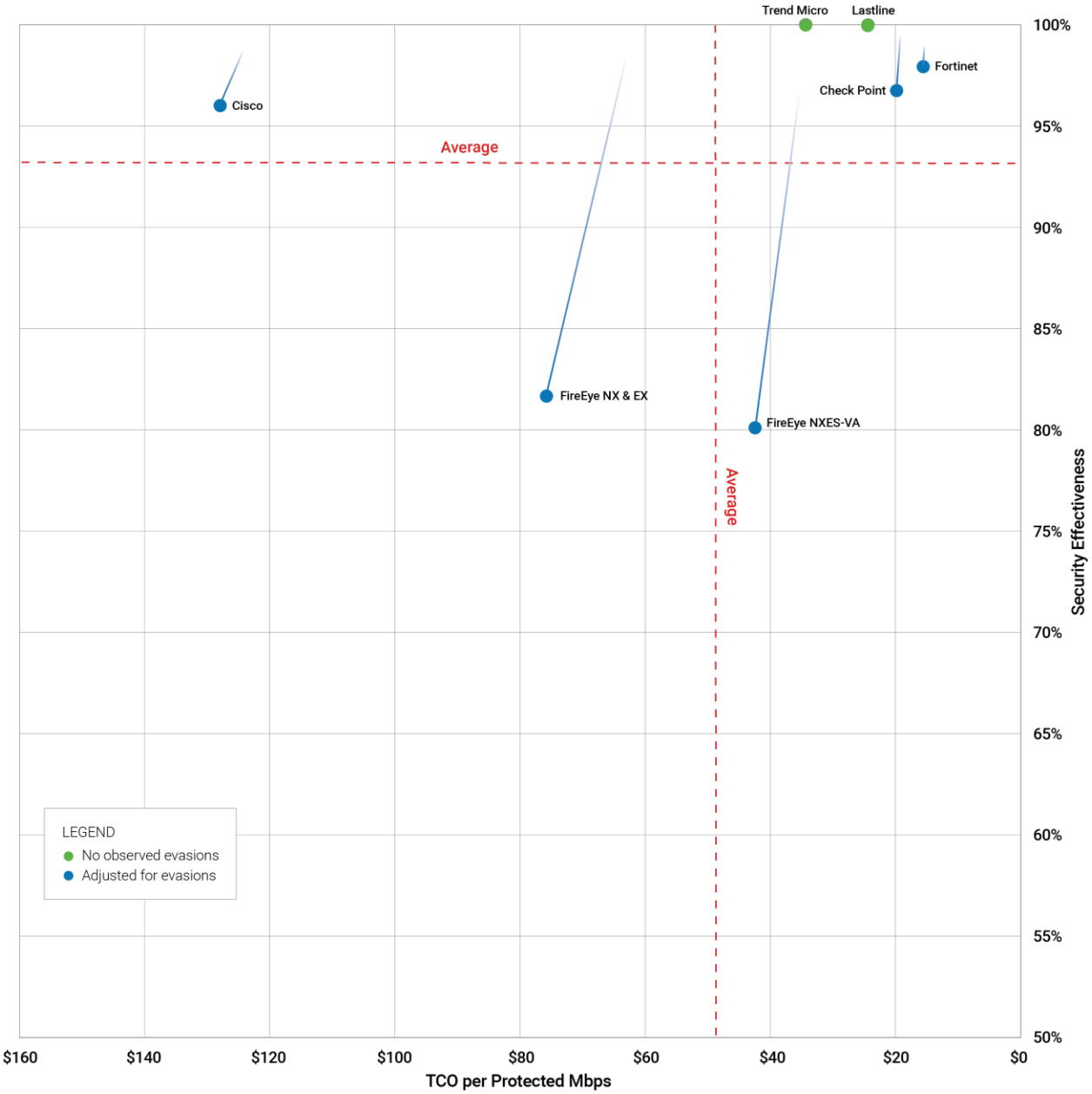

Figure 1 – NSS Labs 2017 Security Value Map (SVM) for Breach Detection Systems (BDS)

Key Findings

- Four products achieved a *Recommended* rating; one product received a *Neutral* rating; one product received a *Security Recommended* rating; and one product received a *Caution* rating.
- Five out of the seven products tested missed evasions.
- Overall *Security Effectiveness* ranged between 80.2% and 100.0%.
- The average *Security Effectiveness* rating was 93.2%; five products received a *Security Effectiveness* rating above the average, and two received a *Security Effectiveness* rating below the average.
- False positive rates ranged from 0% to 0.36%.
- *TCO per Protected Mbps* ranged between US$16 and US$128, with most tested products costing less than US$44 per protected Mbps.
- The average *TCO per Protected Mbps* (*Value*) was US$48.82; five products demonstrated value above the average, and two demonstrated value below the average.

Product Rating

The Overall Rating in Figure 2 is determined by which section of the SVM the product falls within: *Recommended* (top right), *Neutral* (top left or bottom right), or *Caution* (bottom left). For more information on how the SVM is constructed, see the *How to Read the SVM* section of this document.

Product	Security Effectiveness		Value in US$ (TCO per Protected Mbps)		Overall Rating
Check Point	96.7%	Above average	$20	Above average	Recommended
Cisco	96.0%	Above average	$128	Below average	Neutral (Security Recommended)
FireEye NX & EX	81.7%	Below average	$76	Below average	Caution
FireEye NXES-VA	80.2%	Below average	$43	Above average	Neutral
Fortinet	98.0%	Above average	$16	Above average	Recommended
Lastline	100.0%	Above average	$25	Above average	Recommended
Trend Micro	100.0%	Above average	$35	Above average	Recommended

Figure 2 – NSS Labs' 2017 Recommendations for Breach Detection Systems (BDS)

This report is part of a series of Comparative Reports on security, performance, TCO, and the SVM. In addition, NSS clients have access to an NSS Labs *SVM Toolkit™* that allows for the incorporation of organization-specific costs and requirements to create a completely customized SVM. For more information, visit www.nsslabs.com.

Table of Contents

Table of Figures

How to Read the SVM

The SVM depicts the value of a typical deployment of four BDS products plus one central management unit (and where necessary, a log aggregation and/or event management unit). Running a multi-device deployment provides a more accurate reflection of cost than running only a single BDS.

In procuring a BDS solution for the enterprise, it is essential to factor in both bandwidth and the number of users. NSS has found that the malware detection rates of some BDS network devices drop when they operate at maximum capacity. NSS research has shown that, in general, enterprise network administrators architect their networks for up to 2 Mbps of sustained throughput per employee. For example, to support 500 users, an enterprise must deploy 500 agents and/or one network device of 1,000 Mbps capacity.

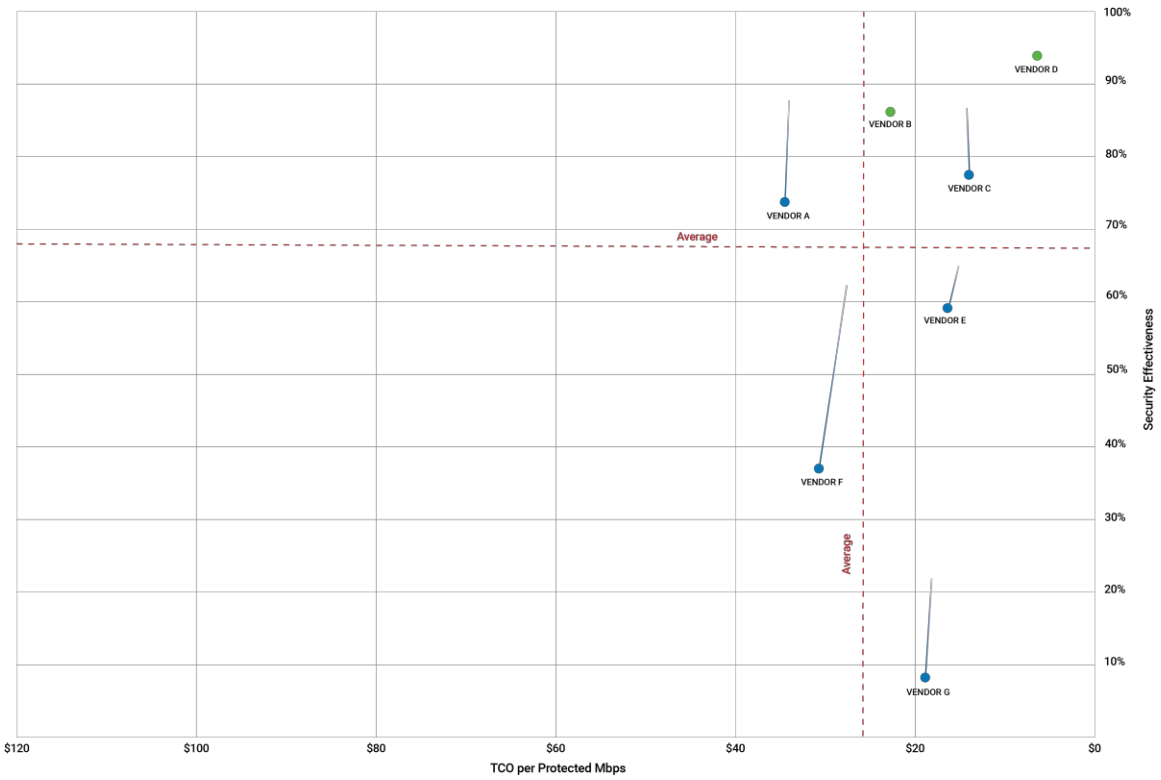

Figure 3 – Example SVM

No two security products deliver the same security effectiveness or performance, making precise comparisons extremely difficult. In order to enable value-based comparisons of BDS products on the market, NSS has developed a unique metric: *TCO per Protected Mbps.*

The *x* axis displays the *TCO per Protected Mbps* in US dollars, which decreases from left to right. This metric incorporates the 3-Year TCO with the *Security Effectiveness* score to provide a data point with which to compare the actual value of each product tested. The formula used is as follows: 3-Year TCO/ (*Security Effectiveness* x *NSS-Tested Throughput*). The TCO incorporates capital expenditure (capex) costs over a three-year period, including initial acquisition and deployment costs and annual maintenance and update costs (software and hardware updates). For more details on *Security Effectiveness* and TCO, see the Security and TCO comparative reports at www.nsslabs.com.

The *y* axis displays the *Security Effectiveness* score as a percentage. *Security Effectiveness* is greater toward the top of the *y* axis. Devices that are missing critical security capabilities will have a reduced *Security Effectiveness* score.

The *Security Effectiveness* score of some products is represented by two data points (a blue dot and a gradient line). The highest point of the gradient line represents *Security Effectiveness* based solely on block rate. However, this is not the only measure of S*ecurity Effectiveness*—NSS also factors in evasions. Incorporating this additional information allows NSS to calculate a second, lower score (represented by the blue dot), which more realistically depicts the actual *Security Effectiveness* of a product.

The *Security Effectiveness* score of products that did not miss any evasions is represented by a single green dot.

The SVM displays two dotted lines that represent the average for the *Security Effectiveness* and *TCO per Protected Mbps* ratings of all the tested products. These lines divide the SVM into four unequally sized sections. Where a product's *Security Effectiveness* and *TCO per Protected Mbps* scores map on the SVM will determine which section it falls into:

- **Recommended**: Products that map into the upper-right section of the SVM score well for both *Security Effectiveness* and *TCO per Protected Mbps***.** These products provide a high level of detection and value for money.
- **Caution:** Products that map into the lower-left section of the SVM offer limited value for money given their 3-Year TCO and measured *Security Effectiveness*.
- **Neutral:** Products that map into either the upper-left or lower-right sections may be good choices for organizations with specific security or budget requirements.

Neutral products in the upper-left section score above the average for *Security Effectiveness* but below the average for *TCO per Protected Mbps* (*Security Recommended).* These products are suitable for environments requiring a high level of detection, albeit at a higher-than-average cost.

Conversely, *Neutral* products in the lower-right section score below the average for *Security Effectiveness* but above the average for *TCO per Protected Mbps*. These products would be suitable for environments where a slightly lower level of detection is acceptable in exchange for a lower TCO.

In all cases, the SVM should only be a starting point. NSS clients have access to the *SVM Toolkit*, which allows for the incorporation of organization-specific costs and requirements to create a custom SVM. Clients can also meet with NSS analysts if they wish to develop a custom SVM.

Analysis

Each product may fall into one of three categories based on its rating in the SVM: *Recommended*, *Neutral*, or *Caution*. Each of the tested products receives only a single rating. Vendors are listed alphabetically within each section.

Recommended

Check Point Software Technologies 15600 Next Generation Threat Prevention & SandBlast™ (NGTX) Appliance R77.30

Detection Rate	The Check Point 15600 Next Generation Threat Prevention & SandBlast™ (NGTX) Appliance received a breach detection rating of 99.7%.
Stability and Reliability	The product passed all stability and reliability tests.
Evasions	The device failed to detect 50% of the web socket connection evasions it was tested against. Please see the Test Report for additional details.
Performance Rating	During performance testing, the product was rated by NSS at 5,667 Mbps.

Fortinet FortiSandbox-2000E v.FSA 2.4.1 & FortiClient (APT Agent) v.5.6.0.1075

Detection Rate	The Fortinet FortiSandbox-2000E & FortiClient (ATP Agent) received a breach detection rating of 99.0%.
Stability and Reliability	The product passed all stability and reliability tests.
Evasions	The product failed to detect 2% of the sandbox evasions it was tested against. Please see the Test Report for additional details.
Performance Rating	During performance testing, the product was rated by NSS at 8,667 Mbps.

Lastline Enterprise v7.25

Detection Rate	The Lastline Enterprise received a breach detection rating of 100%.
Stability and Reliability	The product passed all stability and reliability tests.
Evasions	The product proved effective against all evasion techniques it was tested against.
Performance Rating	During performance testing, the product was rated by NSS at 3,000 Mbps.

Trend Micro Deep Discovery Inspector Model 4000 v3.8 SP5 & (OfficeScan) OSCE v.12.0.1807

Detection Rate	The Trend Micro Deep Discovery Inspector Model 4000 and OSCE received a breach detection rating of 100.0%.
Stability and Reliability	The product passed all stability and reliability tests.
Evasions	The product proved effective against all evasion techniques it was tested against.
Performance Rating	During performance testing, the product was rated by NSS at 8,667 Mbps.

Neutral

Cisco FirePower 8120 v.6 & Cisco AMP v.5.1.9.10430

Detection Rate	The Cisco FirePower 8120 & Cisco AMP received a breach detection rating of 99.0%.
Stability and Reliability	The product passed all stability and reliability tests.
Evasions	The product failed to detect 5.9% of the sandbox evasions it was tested against. Please see the Test Report for additional details.
Performance Rating	During performance testing, the product was rated by NSS at 750 Mbps.

FireEye Network Security 6500NXES-VA v7.9.2

Detection Rate	The FireEye Network Security 6500NXES-VA received a breach detection rating of 96.6%.
Stability and Reliability	The product passed all stability and reliability tests.
Evasions	The product failed to detect 2% of packer & compressor evasions, 100% of web socket connection evasions, and 20% of the HTTP evasions it was tested against. Please see the Test Report for additional details.
Performance Rating	During performance testing, the product was rated by NSS at 1,667 Mbps.

Caution

FireEye Network Security NX 10450 v7.9.2 & EX 8400 v7.9.0

Detection Rate	The FireEye Network Security NX 10450 & EX 8400 received a breach detection rating of 98.4%.
Stability and Reliability	The product passed all stability and reliability tests.
Evasions	The product failed to detect 2% of packer & compressor evasions, 100% of web socket connection evasions, and 20% of the HTTP evasions it was tested against. Please see the Test Report for additional details.
Performance Rating	During performance testing, the product was rated by NSS at 5,000 Mbps.

Test Methodology

Breach Detection Systems: Test Methodology v4.0

A copy of the test methodology is available on the NSS Labs website at www.nsslabs.com.

Contact Information

NSS Labs, Inc.
3711 South MoPac Expressway
Building 1, Suite 400
Austin, TX 78746-8022
USA
info@nsslabs.com
www.nsslabs.com