BREACH DETECTION SYSTEMS COMPARATIVE REPORT

Total Cost of Ownership (TCO)

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

The implementation of breach detection systems (BDS) can be a complex process, with multiple factors affecting the overall cost of deployment, maintenance, and upkeep. Enterprises should include the total cost of ownership (TCO) as part of their evaluations, focusing on the following at a minimum:

- Acquisition costs for the BDS and a central management system (CMS)
- Fees paid to the vendor for annual maintenance, support, and signature updates
- Labor costs for installation, maintenance, and upkeep

NSS Labs invited all BDS vendors to submit their products for testing at no cost. Throughput for the submitted products ranged from 1 Gbps to 10 Gbps, which would account for differences in TCO. No two network security systems 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 formula: *TCO per Protected Mbps*. Using this formula, NSS is able to normalize data and account for wide-ranging differences in TCO and performance among products. See Figure 1 for details.

Within a given performance range (*NSS-Tested Throughput*), the *TCO per Protected Mbps* metric provides clear guidance as to whether a product's price is higher or lower than the majority of its competitors. A high price could indicate a premium based on security effectiveness, brand recognition, or level of customer service. Conversely, a high price could also be a penalty for purchasing an underperforming product.

***Security Effectiveness* =** Breach Detection Score[1] x Evasion Score x Stability & Reliability Score

TCO per Protected Mbps = 3-Year TCO/((*Security Effectiveness* x (1- False Positives)) x NSS-Tested Throughput)

Figure 1 – Security Effectiveness and TCO per Protected Mbps Formulas

For the purposes of this analysis, NSS developed an enterprise use case with one CMS and four devices deployed across multiple remote locations.

Product	NSS-Tested Throughput (Mbps)	3-Year TCO (USS) (four devices + CMS)	Security Effectiveness	TCO per Protected Mbps
Check Point	5,667	$435,521	96.7%	$20
Cisco	750	$368,356	96.0%	$128
FireEye NX & EX	5,000	$1,240,156	81.7%	$76
FireEye NXES-VA	1,667	$228,424	80.2%	$43
Fortinet	8,667	$533,211	98.0%	$16
Lastline	3,000	$294,900	100.0%	$25
Trend Micro	8,667	$1,197,600	100.0%	$35

Figure 2 – TCO per Protected Mbps Results for Tested Products

[1] The breach detection rate is calculated as the percentage of all malware and exploits that were detected under test (drive-by exploits, social exploits, HTTP malware, SMTP malware, and offline infections).

Table of Contents

Table of Figures

Total Cost of Ownership

Tuning

BDS products are complex. With a shortage of skilled and experienced security professionals, enterprises should consider the time and resources required to properly install and maintain the solution. Failure to do so could result in products not achieving their full security potential.

Figure 3 depicts the labor required to take the device out of the box, configure it, deploy it in the network, apply updates and patches, perform initial tuning, and set up desired logging and reporting.

Labor for Device Setup

Costs are based on the time that would be required by an experienced security engineer to perform the setup tasks listed above. The calculations assume a rate of US$75 per hour. Clients can use the Security Value Map™ (SVM) Toolkit and substitute their own costs to get accurate TCO figures.

Product	Installation (Hours)
Check Point	8
Cisco	8
FireEye NX & EX	8
FireEye NXES-VA	8
Fortinet	8
Lastline	8
Trend Micro	8

Figure 3 – Labor Cost per BDS (Hours)

Labor for Central Management

Enterprises should include labor costs for operational expenditures (opex) when evaluating BDS devices. These costs would include day-to-day management tasks such as administration, policy and configuration handling, log handling, alert handling, monitoring, reporting, analysis, auditing and compliance, maintenance, software updates, and troubleshooting.

NSS does not include opex in this analysis. NSS clients can model these costs using the SVM Toolkit or they can schedule an inquiry call with NSS analysts.

Equipment and Software Costs

All capital expenditure (capex) costs are based on street prices that are provided by vendors and then validated by value-added resellers (VARs) at the time of the test. The actual cost to end users may be lower depending on the negotiated discount. However, it is fair to assume that all vendors will provide a similar discount, resulting in a relatively constant cost ratio. Costs for a single BDS and CMS are depicted in Figure 4.

	Initial Purchase		Annual Cost	
Product	Device as Tested	Price (CMS)	Maintenance and Support (Hardware/Software)	Maintenance and Support (CMS)
Check Point	$49,390	$7,500	$18,461	$2,175
Cisco	$52,413	$2,000	$12,759	$400
FireEye NX & EX	$150,900	$10,000	$51,608	$1,620
FireEye NXES-VA	$26,058	$10,000	$8,911	$1,620
Fortinet	$52,000	$6,998	$25,935	$1,531
Lastline	$67,500	$22,500	$0	$0
Trend Micro	$166,000	$0	$66,400[2]	$0

Figure 4 – Equipment and Software Costs (US$)

NSS clients can use the SVM Toolkit to model actual negotiated prices, labor costs, and upkeep times.

TCO Calculations

The TCO incorporates capex over a three-year period, including initial acquisition and deployment costs and annual maintenance and update costs (software and hardware updates). Calculations are as follows:

Value	Description of Calculation
Year 1 Cost	Initial Purchase Price + Maintenance Cost + (Installation x Labor rate $/hr)
Year 2 Cost	Maintenance Cost
Year 3 Cost	Maintenance Cost
3-Year TCO	Year 1 Cost + Year 2 Cost + Year 3 Cost

Figure 5 – TCO Calculations

Calculations are based on a labor rate of US$75 per hour and vendor-provided pricing information. Where possible, the 24/7 maintenance and support option with 24-hour replacement is used, since enterprise customers typically select that option.

[2] Maintenance and support for the first year are included in the initial purchase price and are not counted again in Year 1 Cost.

Pricing in Figure 6 is for four devices and one CMS.

Product	Purchase Price	Maintenance per Year	Year 1 Product Cost	Year 1 Labor Cost	1-Year TCO
Check Point	$205,060	$76,020	$281,080	$2,400	$283,480
Cisco	$211,652	$51,435	$263,087	$2,400	$265,487
FireEye NX & EX	$613,600	$208,052	$821,652	$2,400	$824,052
FireEye NXES-VA	$114,232	$37,264	$151,496	$2,400	$153,896
Fortinet	$214,998	$105,271	$320,269	$2,400	$322,669
Lastline	$292,500	$0	$292,500	$2,400	$294,900
Trend Micro	$664,000	$265,600	$664,000	$2,400	$666,400

Figure 6 – Year 1 TCO (US$)

Note that opex is excluded from TCO calculations for the purposes of this report, but NSS clients can model these costs using the SVM Toolkit.

Normalizing TCO Data

The benefit of normalization is that, within a given performance range (*NSS-Tested Throughput*), the *TCO per Protected Mbps* metric provides clear guidance as to whether a product's price is higher or lower than the majority of its competitors. A high price could indicate a premium based on security effectiveness, brand recognition, or level of customer service. Conversely, a high price could also be a penalty for purchasing an underperforming product.

There are multiple methods by which *Value* can be determined:

Purchase Price Based on Vendor-Claimed Throughput

The simplest means of determining *Value*, but also the most misleading, is to determine the purchase price per Mbps, based on the vendor-claimed throughput and the initial purchase price of the product.

TCO Based on Vendor-Claimed Throughput

A more accurate calculation would be to determine the TCO per vendor-claimed throughput (in the case of BDS, this would be Mbps). This calculation is performed in many purchasing departments. Unfortunately, this approach is as flawed as the first approach, since it relies on the vendor-claimed throughput without performing independent tests to determine the *actual* throughput of the device under real-world conditions.

TCO Based on NSS-Tested Throughput

Vendor throughput claims are frequently exaggerated in marketing materials, or they simply fail to take into account real-world deployment conditions. Knowing this, many enterprise IT professionals will over-purchase based on throughput to ensure adequate performance headroom. *NSS-Tested Throughput* is a real-world representation of a product's performance. *NSS-Tested Throughput* is often significantly different from vendor-claimed throughput (see Figure 7). For more information on *NSS-Tested Throughput*, see the Comparative Report on performance at www.nsslabs.com.

Product	Vendor-Claimed Throughput (Mbps)	NSS-Tested Throughput (Mbps)	% Delta
Check Point	3,000	5,667	89%
Cisco	1,000	750	-25%
FireEye NX & EX	4,000	5,000	25%
FireEye NXES-VA	1,000	1,667	67%
Fortinet	4,000	8,667	117%
Lastline	5,000	3,000	-40%
Trend Micro	4,000	8,667	117%

Figure 7 – Vendor-Claimed vs. NSS-Tested Throughput

TCO Based on Security Effectiveness

Determining value solely based on TCO and throughput is acceptable when dealing with a pure networking device. However, for security devices, *Security Effectiveness* must also be factored into the equation. *The Security Effectiveness* of a device factors in detection rate, evasions, and stability and reliability scores (see Figure 1). Each of these factors can have a serious impact on *Security Effectiveness*. See Figure 1 for details.

Figure 8 depicts the calculations for *TCO per Protected Mbps*, which is based on the product's three-year TCO and *Security Effectiveness* ratings. For more information on these calculations, schedule an inquiry call with NSS analysts or refer to the SVM Toolkit.

Product	NSS-Tested Throughput (Mbps)	3-Year TCO (US$) (four devices + CMS)	Security Effectiveness	TCO per Protected Mbps
Check Point	5,667	$435,521	96.7%	$20
Cisco	750	$368,356	96.0%	$128
FireEye NX & EX	5,000	$1,240,156	81.7%	$76
FireEye NXES-VA	1,667	$228,424	80.2%	$43
Fortinet	8,667	$533,211	98.0%	$16
Lastline	3,000	$294,900	100.0%	$25
Trend Micro	8,667	$1,197,600	100.0%	$35

Figure 8 – TCO per Protected Mbps

Security Effectiveness and Value

Value is a metric that is distinct from both purchase price and TCO. Figure 9 and Figure 10 demonstrate the ways in which the actual value of a product can change significantly as *NSS-Tested Throughput* and *Security Effectiveness* are factored in.

In Figure 9, reading from left to right, the value changes as additional test metrics are introduced. The value in the final column incorporates the three-year TCO, the *NSS-Tested Throughput*, and *Security Effectiveness* as determined by NSS testing.

	Vendor-Claimed Throughput (Mbps)	Vendor-Claimed Throughput (Mbps) + Detection Rate	NSS-Tested Throughput (Mbps) + Detection Rate	NSS-Tested Throughput (Mbps) + Security Effectiveness
Product	TCO per Mbps	TCO per Protected Mbps	TCO per Protected Mbps	TCO per Protected Mbps
Check Point	$36	$36	$19	$20
Cisco	$92	$93	$124	$128
FireEye NX & EX	$78	$79	$63	$76
FireEye NXES-VA	$57	$59	$35	$43
Fortinet	$33	$34	$16	$16
Lastline	$15	$15	$25	$25
Trend Micro	$75	$75	$35	$35

Figure 9 – Value Based on TCO per Protected Mbps

Figure 10 compares the vendor-claimed *Value* metric with the metric generated from NSS test results. The *Security Effectiveness* value indicates whether a product is underpriced, overpriced, or priced accurately depending on the *NSS-Tested Throughput* and overall *Security Effectiveness*.

A product with a *Security Effectiveness* value that is higher than its purchase price can be considered good value. A product with a purchase price that is higher than its *Security Effectiveness* value can be considered overpriced.

Product	Purchase Price	Security Effectiveness Value	Delta	% Delta
Check Point	$205,060	$413,489	$208,429	102%
Cisco	$211,652	$136,747	($74,905)	-35%
FireEye NX & EX	$613,600	$465,573	($148,027)	-24%
FireEye NXES-VA	$114,232	$114,232	$0	0%
Fortinet	$214,998	$558,268	$343,270	160%
Lastline	$292,500	$712,323	$419,823	144%
Trend Micro	$664,000	$569,858	($94,142)	-14%

Figure 10 – Purchase Price vs. Security Effectiveness Value

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

This and other related documents are available at: **www.nsslabs.com.** To receive a licensed copy or report misuse, please contact NSS Labs

Please read the disclaimer in this box because it contains important information that binds you. If you do not agree to these conditions, you should not read the rest of this report but should instead return the report immediately to us. "You" or "your" means the person who accesses this report and any entity on whose behalf he/she has obtained this report.

1. The information in this report is subject to change by us without notice, and we disclaim any obligation to update it.

2. The information in this report is believed by us to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at your sole risk. We are not liable or responsible for any damages, losses, or expenses of any nature whatsoever arising from any error or omission in this report.

3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY US. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, ARE HEREBY DISCLAIMED AND EXCLUDED BY US. IN NO EVENT SHALL WE BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and/or software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet your expectations, requirements, needs, or specifications, or that they will operate without interruption.

5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.

6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.