ADVANCED ENDPOINT PROTECTION COMPARATIVE REPORT

Total Cost of Ownership (TCO)

MARCH 10, 2017

Authors – Jason Brvenik, Thomas Skybakmoen, Morgan Dhanraj

Tested Products

Carbon Black Cb Protection v7.2.3.3106[1]

CrowdStrike Falcon Host[2]

CylancePROTECT v1.2.1410

ESET Endpoint Security v6.4.2014.0

Fortinet FortiClient v5.4.1.0840

X by Invincea v4.2.0-387

Kaspersky Endpoint Security 10

Malwarebytes Endpoint Security v1.7.4.0000

McAfee Endpoint Security v10.5

SentinelOne Endpoint Protection Platform v1.8.3#31

Sophos Central Endpoint Advanced & Sophos InterceptX

Symantec Endpoint Protection 14 with ATP Endpoint (EDR) V2.2

Trend Micro OfficeScan XGEN v12.0.1851

Environment

Advanced Endpoint Protection: Test Methodology v1.0

---

[1] Carbon Black's 100% security score is a result of its whitelisting technology. While this is an excellent security score, enterprises must factor in the ongoing operational overhead that accompanies whitelisting, which means it may not be appropriate for all deployments. As seen in NSS' Security Value Map™, Carbon Black has a higher than average total cost of ownership (TCO).

[2] The Falcon Host's final rating may have been different had it completed the test. We were unable to complete testing due to remotely disabled access.

Overview

This report provides an overview of the NSS Labs Total Cost of Ownership (TCO) formula and discusses how enterprises should apply the formula when budgeting for a security technology. In past NSS group tests, TCO calculations included only the cost and maintenance of a product, and this was normalized against appropriate metrics, such as performance and security effectiveness. While this formula varied from test to test, the principles remained the same. Figure 1 is a typical example.

$$\textbf{TCO per Protected Mbps} = \frac{3\text{–}Year\ TCO}{(Security\ effectiveness) * (NSS\text{–}Tested\ Throughput)}$$

Figure 1 – Example of Past Formula

However, from a financial perspective, the formula in Figure 1 failed to represent to an enterprise the return on investment (ROI) a security product yielded, as well as the operational cost of deploying the product, given its effectiveness. The formula in Figure 2 presents a scenario in which there is no security protection (Base Operational Expense), and it calculates the Security Savings associated with breaches and remediation (Security Effectiveness).

Security Effectiveness = (Block Rate[3] + Additionally Detected) – Impact of Evasions

$$\textbf{TCO per Protected Agent} = \frac{= (\text{Product/s Cost}) + (\text{Base Operational Expense}) - (\text{Security Savings})}{Number\ of\ Agents\ purchased[4]}$$

Figure 2 – Security Effectiveness and TCO per Protected Agent Formulas

Product	Security Effectiveness	Security Savings	Cost of Responding to Infections/Incidents	TCO	TCO per Protected Agent	ROI
Carbon Black[1]	100.0%	$1,081,000	$0	$269,000	$538	401.9%
CrowdStrike[2]	73.2%	$648,091	$530,909	$701,909	$1,404	92.3%
Cylance	97.7%	$1,284,257	$4,243	$65,743	$131	1953.4%
ESET	89.5%	$1,208,242	$81,788	$141,758	$284	852.3%
Fortinet	95.9%	$1,137,300	$205,350	$212,700	$425	534.7%
Invincea	97.5%	$1,292,088	$39,072	$57,912	$116	2231.1%
Kaspersky	93.6%	$1,239,023	$86,677	$110,977	$222	1116.5%
Malwarebytes	57.9%	$732,369	$581,196	$617,631	$1,235	118.6%
McAfee	99.0%	$1,250,629	$13,776	$99,371	$199	1258.6%
SentinelOne	97.8%	$1,305,994	$3,161	$44,006	$88	2967.8%
Sophos	94.7%	$1,228,686	$58,054	$121,314	$243	1012.8%
Symantec	98.7%	$1,208,233	$ 56,172	$141,767	$284	852.3%
Trend Micro	98.3%	$1,216,068	$109,887	$133,932	$268	908.0%

Figure 3 – TCO per Protected Agent Results for Tested Products

[1] Carbon Black's 100% security score is a result of its whitelisting technology. While this is an excellent security score, enterprises must factor in the ongoing operational overhead that accompanies whitelisting, which means it may not be appropriate for all deployments. As seen in NSS' Security Value Map™, Carbon Black has a higher than average total cost of ownership (TCO).

[2] The Falcon Host's final rating may have been different had it completed the test. We were unable to complete testing due to remotely disabled access.

[3] Block Rate and Additional Detection Rate are defined as the number of exploits and malware blocked and detected under test within the 2-hour window.

[4] The impact of evasions was not included in this TCO model. Future versions of the TCO model will incorporate the impact of evasions.

Table of Contents

Table of Figures

Total Cost of Ownership Model

Normalizing Operational Burden

Previously, the TCO was computed as the fixed cost of owning a security product and did not provide additional validation for that quoted price. A high price could be justified due to positive brand recognition, a premium based on security effectiveness, or superior customer service. NSS' updated formula captures the intrinsic value of a security product by factoring in the higher impact the key variables previously listed have on the overall costs. This more comprehensive TCO metric, in conjunction with the security effectiveness value, provides organizations with broader insight into which purchasing decision will yield the best returns on their investments.

The updated TCO model conveys to the enterprise a full range of use cases, starting with the costs of not having any security protection to calculating the potential value of deploying a security technology based on overall cost, security effectiveness and internal needs for such a security product. The foundation of the TCO model relies on two core assumptions:

- Without security:
  - Compromises will occur
  - Incidents will occur
  - Additional operational overhead is needed to remedy the effects of a compromised system and protect the business user
- With security:
  - Compromises will occur less often
  - Incidents will occur less often
  - The operational burden should be reduced and organizations will be able to realize this reduction

Since each AEP product has a unique set of capabilities, the TCO metric assigns a value that normalizes the operational overhead, potential consequences, and associated costs a security breach can have on an organization. This allows decision makers to better analyze risk and make calculated choices that are ideal for their organizations.

Assumptions for TCO Model

NSS assumes the following when calculating TCO:

- An infection requires an IT response, which increases operational costs.
- An incident requires an incident response, which increases operational costs.
- Blocking an infection removes the need to perform either of the first two actions, and this lack of required response increases operational savings.
- Detection of an infection reduces the attacker's dwell time and thus the potential of an incident occurring
- If an infection is neither blocked nor detected, this may result in an incident, which would result in increased operational and marginal costs.
- All costs and assumptions are calculated over a three-year period.

Key Terms Used in TCO Calculations

- **Infection Response**: An infection that requires an IT team's response
- **Fixed Cost:** Cost of labor (IT team's response)
- **Infection Response Cost**: The cost to remediate infections
- **Incident (Breach)**: A company is fully compromised
- **Incident Response**: An incident that requires an incident response
- **Incident Response Cost**: The total cost to remediate an incident
- **Incident Conversion Rate**: The percentage of infections that will turn into incidents
- **Base Operational Expense**: The total projected cost to operate a business without a security product
- **Security Savings**: The projected savings realized from blocking or detecting an infection and/or incident
- **Product Cost**: The cost to own a security product for three years including maintenance and support
- **Total Cost of Ownership**: The aggregate cost of owning a security device

Mathematical Formulas

NSS uses the following formulas to calculate TCO:

Infection Response Cost

Without any security protection, a business will incur an operational expense. Once an infection is discovered, it must be remediated by the IT team at a fixed cost, which varies from one enterprise to the next. The Infection Response Cost formula is used to calculate the total cost to remediate infections.

Infection Response Cost *= (Number of Infections) * (Fixed Cost)*

Figure 4 – Infection Response Cost

Incident Response Cost

A percentage of those infections will likely lead to incidents (breaches). NSS defines this as the Incident Conversion Rate, which calculates the percentage of infections that convert to incidents. One incident equals one incident response, and each incident response has an associated cost.

Incident Response Cost *= (Number of Infections) * (Incident Conversion Rate) * (Incident Cost)*

Figure 5 – Incident Response Cost

Base Operational Expense

The consequences of ***not*** protecting your enterprise become evident. Your operational expenses are greatly increased if you are unable to protect your business. Base Operational Expense represents the total amount an unprotected business would have to allocate in its budget in order to decrease its likelihood of compromise.

Base Operational Expense *= (Infection Response Cost) + (Incident Response Cost)*

Figure 6 – Base Operational Expense

Block Savings

An unprotected business can now make an informed decision to invest in a security technology that mitigates its base operational expenses, and it can project the associated potential savings. Since blocking an infection is preventative, this means there is no infection or corresponding incident cost. Block Savings are defined as the savings a business achieves as a result of incidents being blocked.

Block Savings *= (Number of Blocked Infections * Fixed Cost) + (Number of Blocked Incidents * Incident Conversion Rate * Incident Cost)*

Figure 7 – Block Savings

Detect Savings

If a product does not block an infection initially, an additional detection can reduce the risk—and thus the associated costs—of an incident. This is reflected in a reduced incident conversion rate. Detection reduces the chance that there will be an incident and thus it reduces the chance of an associated incident response cost; however, there will still be the associated cost of fixing the infection. The model assumes that anything that is blocked is also detected. The additional detection component calculates the incidents that were only detected. This reduction is calculated using the Reduced Incident Conversion Rate.

Detect Savings *= (Number of Detected Infections * Reduced Incident Conversion Rate * Incident Cost)*

Figure 8 – Detect Savings

Security Savings

From a value perspective, blocking an infection is more valuable than detecting it, and detecting an infection is clearly more valuable than missing it completely—which could result in an incident. The Security Savings formula calculates the total amount of savings a business can accumulate by having a security product that can block and detect an infection.

Security Savings *= (Detect Savings) + (Block Savings)*

Figure 9 – Security Savings

TCO

We can calculate TCO by deducting the Security Savings an organization will derive from deploying a security product from the security product's cost and from its Base Operational Expense. The Product Cost is calculated assuming a three-year commitment, which includes maintenance, support, and operational expenses.

Product Cost = (Acquisition) + (Deployment Costs) + (Annual Maintenance and Support) + (Update Costs) + (Operational Expenses)

Total Cost of Ownership = (Product Cost) + (Base Operational Expense) – (Security Savings)

Figure 10 – TCO

If your security product is not blocking or detecting any infections, you will incur Infection Response Costs and possibly also Incident Response Costs. The opportunity cost of purchasing and deploying a security product is greater than the cost of not having a security product.

ROI

Ultimately, a company will invest in a security product that increases efficiency, reduces costs, and maximizes its return. The initial investment in a security product can yield a positive Return on Investment (ROI). The ROI is an additional measurement that enterprises can utilize to compare the profitability of investing in a specific security product versus other products in its peer group.

$$\textit{Return on Investment} = \frac{Security\ Savings}{(Product\ Cost) + (Base\ Operational\ Expense - Security\ Savings)}$$

Figure 11 – ROI

Use Cases

To illustrate how these formulas work, NSS has modeled three different enterprise use cases, starting with 500 users/agents, then increasing this number to 5,000 users/agents, and finally increasing the number to 40,000 users/agents. NSS has assumed the same variables for all use cases. NSS subscribers will be able to alter the variables using the SVM Toolkit™.

- Product acquisition cost = US$200 per agent
- Fixed IT cost per infection = US$300
- Incident (breach) cost = US$20,000
- Incident conversion rate = 3%
- Reduced incident conversion rate = 2% (Only 1% of detected incidents will convert.)

Use Case #1

- Enterprise: 500 employees
- Number of Infections: 1,500 infections (one infection per employee per year)

Number of Infections Blocked	Number of Infections Detected	Security Savings	Cost of Responding to Infections/Incidents	TCO	TCO per Protected Agent	ROI
100%	0%	$1,250,000	$0	$100,000	$200	1250.0%
90%	10%	$1,175,000	$75,000	$175,000	$350	671.4%
50%	50%	$875,000	$375,000	$475,000	$950	184.2%
0%	100%	$500,000	$750,000	$850,000	$1,700	58.8%

Figure 12 – Use Case #1

Use Case #2

- Enterprise: 5,000 employees
- Number of Infections: 15,000 infections (one infection per employee per year)

Number of Infections Blocked	Number of Infections Detected	Security Savings	Cost of Responding to Infections/Incidents	TCO	TCO per Protected Agent	ROI
100%	0%	$12,500,000	$0	$1,000,000	$200	1250.0%
90%	10%	$11,750,000	$750,000	$1,750,000	$350	671.4%
50%	50%	$8,750,000	$3,750,000	$4,750,000	$950	184.2%
0%	100%	$5,000,000	$7,500,000	$8,500,000	$1,700	58.8%

Figure 13 – Use Case #2

Use Case #3

- Enterprise: 40,000 employees with a security perspective/budget
- Number of Infections: 120,000 infections (one infection per employee per year)

Number of Infections Blocked	Number of Infections Detected	Security Savings	Cost of Responding to Infections/Incidents	TCO	TCO per Protected Agent	ROI
100%	0%	$100,000,000	$0	$8,000,000	$200	1250.0%
90%	10%	$94,000,000	$6,000,000	$14,000,000	$350	671.4%
50%	50%	$70,000,000	$30,000,000	$38,000,000	$950	184.2%
0%	100%	$40,000,000	$60,000,000	$68,000,000	$1,700	58.8%

Figure 14 – Use Case #3

AEP Group Test Results

Once NSS' updated TCO formula is applied to the AEP group test results, we see the following results:

Product	Security Effectiveness	Security Savings	Cost of Responding to Infections/Incidents	TCO	TCO per Protected Agent	ROI
Carbon Black[1]	100.0%	$1,081,000	$0	$269,000	$538	401.9%
CrowdStrike[2]	73.2%	$648,091	$530,909	$701,909	$1,404	92.3%
Cylance	97.7%	$1,284,257	$4,243	$65,743	$131	1953.4%
ESET	89.5%	$1,208,242	$81,788	$141,758	$284	852.3%
Fortinet	95.9%	$1,137,300	$205,350	$212,700	$425	534.7%
Invincea	97.5%	$1,292,088	$39,072	$57,912	$116	2231.1%
Kaspersky	93.6%	$1,239,023	$86,677	$110,977	$222	1116.5%
Malwarebytes	57.9%	$732,369	$581,196	$617,631	$1,235	118.6%
McAfee	99.0%	$1,250,629	$13,776	$99,371	$199	1258.6%
SentinelOne	97.8%	$1,305,994	$3,161	$44,006	$88	2967.8%
Sophos	94.7%	$1,228,686	$58,054	$121,314	$243	1012.8%
Symantec	98.7%	$1,208,233	$ 56,172	$141,767	$284	852.3%
Trend Micro	98.3%	$1,216,068	$109,887	$133,932	$268	908.0%

Figure 15 – TCO per Protected Agent

[1] Carbon Black's 100% security score is a result of its whitelisting technology. While this is an excellent security score, enterprises must factor in the ongoing operational overhead that accompanies whitelisting, which means it may not be appropriate for all deployments. As seen in NSS' Security Value Map™, Carbon Black has a higher than average total cost of ownership (TCO). For additional information, please see the TCO Comparative Report.

[2] The Falcon Host's final rating may have been different had it completed the test. We were unable to complete testing due to remotely disabled access.

Test Methodology

Advanced Endpoint Protection: Test Methodology v1.0

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

Contact Information

NSS Labs, Inc.
206 Wild Basin Road
Building A, Suite 200
Austin, TX 78746
info@nsslabs.com
www.nsslabs.com