ADVANCED ENDPOINT PROTECTION COMPARATIVE REPORT

Total Cost of Ownership (TCO)

MARCH 5, 2019

Authors – Thomas Skybakmoen, Scott Robin

Tested Products

Bitdefender GravityZone Ultra v6.6.7.106

Carbon Black CB Defense 3.2.10105

Check Point Software Technologies Check Point SandBlast Agent Next Generation AV E80.82.1

Cisco Advanced Malware Protection (AMP) for Endpoints 6.2.3.10807

Comodo Client Security 10.8.0.7053

Cylance CylancePROTECT + CylanceOPTICS v2.0.1500

Endgame Endpoint Security v3.3

enSilo Endpoint Security Platform v3.0

F-Secure Computer Protection Premium v18.14

Fortinet FortiClient v6.0.3

Kaspersky Lab Kaspersky Endpoint Security v11.0.1.90

Malwarebytes Endpoint Protection and Response v1.2.0.632

Panda Security Panda Adaptive Defense 360 v3.40.00

Sophos Intercept X Advanced v2.0.10

Symantec Endpoint Protection and Advanced Threat Protection (ATP) v14.2.1023.0100

Trend Micro Smart Protection for Endpoints v12.0.5024

Vendor A

Vendor B

Vendor C

Environment

NSS Labs Advanced Endpoint Protection (AEP) Test Methodology v3.0

NSS Labs Evasions Test Methodology v1.2

Overview

This report uses the NSS Labs Total Cost of Ownership (TCO) model to calculate TCO for advanced endpoint protection (AEP) products in the NSS Labs 2019 AEP Group Test (AEP Test Methodology v3.0). The model assumes that enterprises that do not deploy AEP security, or that deploy an AEP security product with low protection, will incur less security savings in the event of a breach, since additional operational overhead will be required to remediate the effects of a compromised system and protect the business. From a security perspective, the projected cost of operating a business has three primary components:

Figure 1 – Effect of Security Savings on TCO

From a financial perspective, a TCO model should represent purchase costs; the return on investment (ROI) a security product yields; and the operational cost of deploying and managing the product, given its overall effectiveness (*Overall Capability Score*). Figure 2 depicts the *TCO per Protected Agent* and ROI for each product.

Vendor	Overall Capability Score	Product Operational Savings	Total Savings	Cost of Infections & Incidents	TCO (US$)	TCO per Protected Agent	ROI
Bitdefender	97.5%	Yes	$6,893,131	$164,694	$456,869	$183	1509%
Carbon Black	98.0%	Yes	$7,082,911	$98,072	$267,089	$107	2652%
Check Point	97.4%	Yes	$7,029,917	$193,483	$320,083	$128	2196%
Cisco	97.9%	Yes	$7,025,387	$233,289	$324,613	$130	2164%
Comodo	98.5%	No	$6,474,135	$99,765	$875,865	$350	2347%
Cylance	96.8%	Yes	$6,745,481	$217,669	$604,519	$242	1116%
Endgame	98.9%	Yes	$7,119,826	$74,824	$230,174	$92	3093%
enSilo	97.4%	Yes	$6,988,960	$172,340	$361,040	$144	1936%
Fortinet Technologies	97.5%	Yes	$7,117,042	$188,949	$232,958	$93	3055%
F-Secure	96.6%	No	$6,461,464	$113,711	$888,536	$355	2239%
Kaspersky Lab	96.8%	Yes	$7,053,786	$213,134	$296,214	$118	2381%
Malwarebytes	93.3%	Yes	$6,719,100	$463,050	$630,900	$252	1065%
Panda Security	98.3%	Yes	$7,023,188	$104,212	$326,812	$131	2149%
Sophos	99.1%	Yes	$7,190,070	$57,963	$159,930	$64	4496%
Symantec	96.5%	Yes	$6,681,758	$227,192	$668,242	$267	1000%
Trend Micro	97.9%	Yes	$7,116,674	$149,326	$233,326	$93	3050%
Vendor A	90.7%	No	$6,050,617	$573,283	$1,299,383	$520	865%
Vendor B	88.4%	Yes	$6,459,458	$736,942	$890,542	$356	725%
Vendor C	87.8%	Yes	$6,409,974	$819,426	$940,026	$376	682%

Figure 2 –TCO per Protected Agent and ROI of Tested Products

Table of Contents

Table of Figures

Total Cost of Ownership Model

Normalizing Operational Burden

Enterprises that do not deploy an AEP product, or that deploy an AEP product with low protection, will incur less security savings in the event of a breach since additional operational overhead will be required to remediate the effects of a compromised system and protect the business. Furthermore, security products that do not provide visibility and forensic detail will realize less security savings because compromises will have to be investigated manually, which would increase operational cost. Therefore, for the purposes of this TCO model, management (of security products) and investigation (of breaches) is conservatively estimated as requiring two full-time employees at $100,000 per year (*Product Operational Cost*).

The NSS TCO model calculates the projected cost of operating a business without deploying an endpoint security product as well as the potential value of deploying an endpoint security product. This potential value is based on product cost, *Product Operational Cost*, and the *Overall Capability* score of a product. The TCO model makes these core assumptions:

- Without security:
  - Infections 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:
  - Infections 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:

- Headcount is required to operate the business securely.
- An infection requires an IT response, which increases operational costs.
- An incident requires an incident response, which increases operational costs.
- Blocking an infection can reduce the need to respond to infections and incidents, which increases operational savings.
- Early 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 are assumed to be over a three-year period.

Key Terms Used in TCO Calculations

- **Infection Response**: An infection requires an IT team's response
- **Fixed Cost:** Cost of labor (IT team's response) varies if infection requires manual investigation
- **Infection Response Costs**: Cost to remediate infections
- **Incident (Breach)**: Organization is fully compromised
- **Incident Response**: An incident requires an IT team's response
- **Incident Response Costs**: Total cost to remediate incidents
- **Incident Conversion Rate**: Percentage of infections that will turn into incidents
- **Base Operational Expense**: Total projected cost to operate a business without a security product
- **Overall Capability Score:** A percentage score that represents a vendor's overall security capabilities
- **Security Savings**: Projected savings realized from blocking or detecting an infection and/or incident
- **Product Operational Costs:** The cost of management (of security products) and investigation (of breaches)
- **Product Operational Savings:** Projected savings realized through *Product Operational Costs*
- **Product Cost**: Cost to own a security product for three years including maintenance and support
- **Total Cost of Ownership**: Aggregate cost of owning a security product
- **Total Savings**: The total savings achieved once a product's cost, product operational costs, and security savings are subtracted from its base operational expense
- **TCO per Protected Agent**: The total cost per endpoint (agent), once all costs and savings are factored in

Mathematical Formulas

Figure 3 details NSS' formula for calculating *TCO per Protected Agent*. The formula includes the projected cost of operating a business without deploying an endpoint security product (*Base Operational Expense*) as well as the actual cost *(Product Cost)* of acquiring a security product. The formula also includes the projected savings realized through *Product Operational Costs* and blocking or detecting an infection and/or incident *(Security Savings).* This allows NSS to calculate a more realistic cost per agent/user as opposed to the cost of having no AEP security product at all.

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

Figure 3 – *TCO per Protected Agent* Formula

Infection Response Costs

Without any security protection, a business will incur operational expenses. Once an infection is discovered, it must be remediated by the IT team at a fixed cost. The *Infection Response Costs* formula is used to calculate the total cost to remediate infections.

$$\textit{Infection Response Costs} = (\textit{Number of Infections}) * (\textit{Fixed Cost})$$

Figure 4 – Infection Response Costs

Incident Response Costs

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

Figure 5 – Incident Response Costs

Base Operational Expense

The consequences of not protecting an enterprise become evident. The enterprise's operational expenses are greatly increased if it is unable to protect its assets. *Base Operational Expense* represents the total amount an unprotected enterprise would have to allocate in its IT budget in order to decrease its likelihood of compromise.

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

Figure 6 – Base Operational Expense

Block Savings

An unprotected enterprise can use its projected cost (*Base Operational Expense)* to make an informed decision to invest in a security technology that will mitigate its operational expenses, and it can project the associated potential savings. Since blocking an infection is preventative, there is less chance of an infection or corresponding incident cost; however, there might still be the associated cost of investigating and managing possible compromises if the product does not provide visibility and forensic detail because possible compromises will have to be investigated manually. *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 initially block an infection, detection of the infection is another way to reduce the risk—and thus the associated costs—of an incident. This would result 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 *Additional Detection Rate* depicts the incidents that were detected but not blocked. This reduction is calculated using the *Reduced Incident Conversion Rate.* The TCO model assumes that anything that is blocked is also detected, but this may not always be the case since some AEP products provide little to no information on how attacks were blocked.

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

Figure 8 – Detect Savings

Security Savings

It is more valuable to block an infection than it is to detect it—and it is more valuable to detect an infection than it is to miss it completely, which could result in an incident. The *Security Savings* formula calculates the total amount of savings a business can accumulate by deploying a security product that can block and detect an infection.

Security Savings = *(Detect Savings + Block Savings)-(False Positives)*

Figure 9 – Security Savings

TCO per Protected Agent

NSS calculates *TCO per Protected Agent* by deducting the *Security Savings* an organization will derive from deploying a security product from the *Product Cost*, *Product Operational Cost*, and *Base Operational Expense*. *Product Cost* is calculated assuming a three-year commitment, which includes maintenance, support, and operational expenses.

$$\textbf{TCO per Protected Agent} = \frac{(\text{Product(s)Cost}) + (\text{ Product Operational Cost}^{1}) + (\text{Base Operational Expense} - \text{Security Savings})}{Number\ of\ Agents\ purchased}$$

Figure 10 – TCO per Protected Agent

If a security product is not blocking or detecting any infections, the business 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, businesses 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 ROI, which is an additional measurement that enterprises can utilize to compare the profitability of investing in a specific security product versus peer products.

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

Figure 11 – ROI

Overall Capability Score

The *Overall Capability Score* is used to calculate *TCO per Protected Agent*, which in turn is used to plot a product's value on the x axis in the NSS Labs Security Value Map™ (SVM).

$$\textbf{\textit{Overall Capability Score}} = (\text{Block Rate} + \text{Additional Detection Rate}) - (\text{False Positives})$$

Figure 12 – Overall Capability Score

[1] For the purposes of this TCO model, management and investigation is conservatively estimated as requiring two full-time employees at $100,000 per year (modeled at $80 per agent).

Vendor	Overall Capability Score
Bitdefender	97.5%
Carbon Black	98.0%
Check Point	97.4%
Cisco	97.9%
Comodo	98.5%
Cylance	96.8%
Endgame	98.9%
enSilo	97.4%
Fortinet Technologies	97.5%
F-Secure	96.6%
Kaspersky Lab	96.8%
Malwarebytes	93.3%
Panda Security	98.3%
Sophos	99.1%
Symantec	96.5%
Trend Micro	97.9%
Vendor A	90.7%
Vendor B	88.4%
Vendor C	87.8%

Figure 13 – Overall Capability Score

Use Cases

To illustrate how these TCO formulas work in the real world, NSS has modeled three different enterprise use cases:

- 500 users/agents
- 2,500 users/agents
- 50,000 users/agents

The same variables are assumed for all use cases. Enterprise customers can contact NSS to model their own SVM in order to better understand which products might be best for them.

- *Product Cost* = US$200 per agent
- One attack per user/agent per year over a three-year period
- Cost Saving per infection = US$300
- Incident (breach) cost = US$20,000
- Incident conversion rate = 3%
- Reduced incident conversion rate (no/low centralized management and automation) = Only 1% of detected incidents will convert to a breach
- Reduced incident conversion rate (with centralized management and automation) = Only 0.25% of detected incidents will convert to a breach

Use Case #1

- Enterprise: 500 employees
- Number of infections over three years: 1,500

Infections Blocked (%)	Infections Detected (%)	Total Savings ($)	Cost of Infections & Incidents ($)	TCO ($)	TCO per Protected Agent ($)	ROI (%)
100.0	0.0	1,250,000	0	100,000	200	1,250
95.0	0.0	1,182,500	67,500	167,500	335	706
95.0	2.5	1,197,500	52,500	152,500	305	785
90.0	0.0	1,115,000	135,000	235,000	470	474
90.0	5.0	1,145,000	105,000	205,000	410	559

Figure 14 – Use Case #1

Use Case #2

- Enterprise: 2500 employees
- Number of infections over three years: 7,500

Infections Blocked (%)	Infections Detected (%)	Total Savings ($)	Cost of Infections & Incidents ($)	TCO ($)	TCO per Protected Agent ($)	ROI (%)
100.0	0.0	6,250,000	0	500,000	200	1,250
95.0	0.0	5,912,500	337,500	837,500	335	706
95.0	2.5	5,987,500	262,500	762,500	305	785
90.0	0.0	5,575,000	675,000	1,175,000	470	474
90.0	5.0	5,725,000	525,000	1,025,000	410	559

Figure 15 – Use Case #2

Use Case #3

- Enterprise: 50,000 employees
- Number of infections over three years: 150,000

Infections Blocked (%)	Infections Detected (%)	Total Savings ($)	Cost of Infections & Incidents ($)	TCO ($)	TCO per Protected Agent ($)	ROI (%)
100.0	0.0	125,000,000	0	10,000,000	200	1,250
95.0	0.0	118,250,000	6,750,000	16,750,000	335	706
95.0	2.5	119,750,000	5,250,000	15,250,000	305	785
90.0	0.0	111,500,000	13,500,000	23,500,000	470	474
90.0	5.0	114,500,000	10,500,000	20,500,000	410	559

Figure 16 – Use Case #3

Product Costs

All capital expenditure (capex) costs are based on quotes obtained at the time of testing. 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.

Where possible, the 24/7 maintenance and support option with 24-hour replacement is utilized, since this is the option typically selected by enterprise customers. Prices depicted include the purchase and maintenance costs for 2,500 software agents only. Please contact NSS for additional detail. Year 1 Cost includes an additional $600 installation cost that was applied to all products in the test.

Product	1-Year Product Cost	2-Year Product Cost	3-Year Product Cost
Bitdefender	$97,792	$194,983	$292,175
Carbon Black	$56,739	$112,878	$169,017
Check Point	$42,600	$84,600	$126,600
Cisco	$30,842	$61,083	$91,325
Comodo	$59,100	$117,600	$176,100
Cylance	$129,350	$258,100	$386,850
Endgame	$52,183	$103,767	$155,350
enSilo	$63,300	$126,000	$188,700
Fortinet Technologies	$15,070	$29,540	$44,009
F-Secure	$58,675	$116,750	$174,825
Kaspersky Lab	$28,093	$55,587	$83,080
Malwarebytes	$56,350	$112,100	$167,850
Panda Security	$74,600	$148,600	$222,600
Sophos	$34,389	$68,178	$101,967
Symantec	$147,417	$294,233	$441,050
Trend Micro	$28,400	$56,200	$84,000
Vendor A	$42,433	$84,267	$126,100
Vendor B	$51,600	$102,600	$153,600
Vendor C	$40,600	$80,600	$120,600

Figure 17 – Three-Year Product Cost (US$)

Figure 18 displays the results once the NSS formula for calculating ROI and *TCO per Protected Agent* is applied.

Vendor	Overall Capability Score	Product Operational Savings	Total Savings	Cost of Infections & Incidents	TCO (US$)	TCO per Protected Agent	ROI
Bitdefender	97.5%	Yes	$6,893,131	$164,694	$456,869	$183	1509%
Carbon Black	98.0%	Yes	$7,082,911	$98,072	$267,089	$107	2652%
Check Point	97.4%	Yes	$7,029,917	$193,483	$320,083	$128	2196%
Cisco	97.9%	Yes	$7,025,387	$233,289	$324,613	$130	2164%
Comodo	98.5%	No	$6,474,135	$99,765	$875,865	$350	2347%
Cylance	96.8%	Yes	$6,745,481	$217,669	$604,519	$242	1116%
Endgame	98.9%	Yes	$7,119,826	$74,824	$230,174	$92	3093%
enSilo	97.4%	Yes	$6,988,960	$172,340	$361,040	$144	1936%
Fortinet Technologies	97.5%	Yes	$7,117,042	$188,949	$232,958	$93	3055%
F-Secure	96.6%	No	$6,461,464	$113,711	$888,536	$355	2239%
Kaspersky Lab	96.8%	Yes	$7,053,786	$213,134	$296,214	$118	2381%
Malwarebytes	93.3%	Yes	$6,719,100	$463,050	$630,900	$252	1065%
Panda Security	98.3%	Yes	$7,023,188	$104,212	$326,812	$131	2149%
Sophos	99.1%	Yes	$7,190,070	$57,963	$159,930	$64	4496%
Symantec	96.5%	Yes	$6,681,758	$227,192	$668,242	$267	1000%
Trend Micro	97.9%	Yes	$7,116,674	$149,326	$233,326	$93	3050%
Vendor A	90.7%	No	$6,050,617	$573,283	$1,299,383	$520	865%
Vendor B	88.4%	Yes	$6,459,458	$736,942	$890,542	$356	725%
Vendor C	87.8%	Yes	$6,409,974	$819,426	$940,026	$376	682%

Figure 18 – ROI and TCO per Protected Agent of Tested Products

Test Methodology

NSS Labs Advanced Endpoint Protection (AEP) Test Methodology v3.0

NSS Labs Evasions Test Methodology v1.2

Copies of the test methodologies are available at www.nsslabs.com.

Contact Information

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