ADVANCED ENDPOINT PROTECTION COMPARATIVE REPORT

Security Value Map™ (SVM)

APRIL 17, 2018

Authors – Thomas Skybakmoen, Morgan Dhanraj

Tested Products

Bitdefender GravityZone Elite v6.2.31.985
Carbon Black Cb Defense v3.0.2.2
Cisco AMP for Endpoints v6.0.5
Comodo Advanced Endpoint Protection v3.18.0
Cylance CylancePROTECT + OPTICS v2.0.1450
Endgame Endpoint Security v2.5
enSilo Endpoint Security Platform v2.7
ESET Endpoint Protection Standard v6.5.522.0
FireEye Endpoint Security v4
Fortinet FortiClient v5.6.2
G DATA EndPoint Protection Business v14.1.0.67
Kaspersky Lab Kaspersky Endpoint Security v10
Malwarebytes Endpoint Protection v1.1.1.0
McAfee Endpoint Security v10.5
Palo Alto Networks Traps v4.1
Panda Security Panda Adaptive Defense 360 v2.4.1
SentinelOne Endpoint Protection Platform (EPP) v2.0.1.10548
Sophos Endpoint Protection 10.7.6 VE3.70.2
Symantec Endpoint Protection and Advanced Threat Protection (ATP) Platform v14.0.3876.1100
Trend Micro Smart Protection for Endpoints v12.0.1864

Unverified Products[1]

CrowdStrike

Environment

Advanced Endpoint Protection (AEP) Test Methodology v2.0

[1] NSS was unable to measure the effectiveness and determine the suitability of CrowdStrike advanced endpoint protection products and therefore cautions against their deployment without a comprehensive evaluation.

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 by mapping the *Security Effectiveness* and the *Total Cost of Ownership (TCO) per Protected Agent* (*Value*) of tested product configurations. The terms *TCO per Protected Agent* 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 and can be found at www.nsslabs.com. Comparative Reports provide detailed comparisons across all tested products in the following areas:

- Security
- TCO

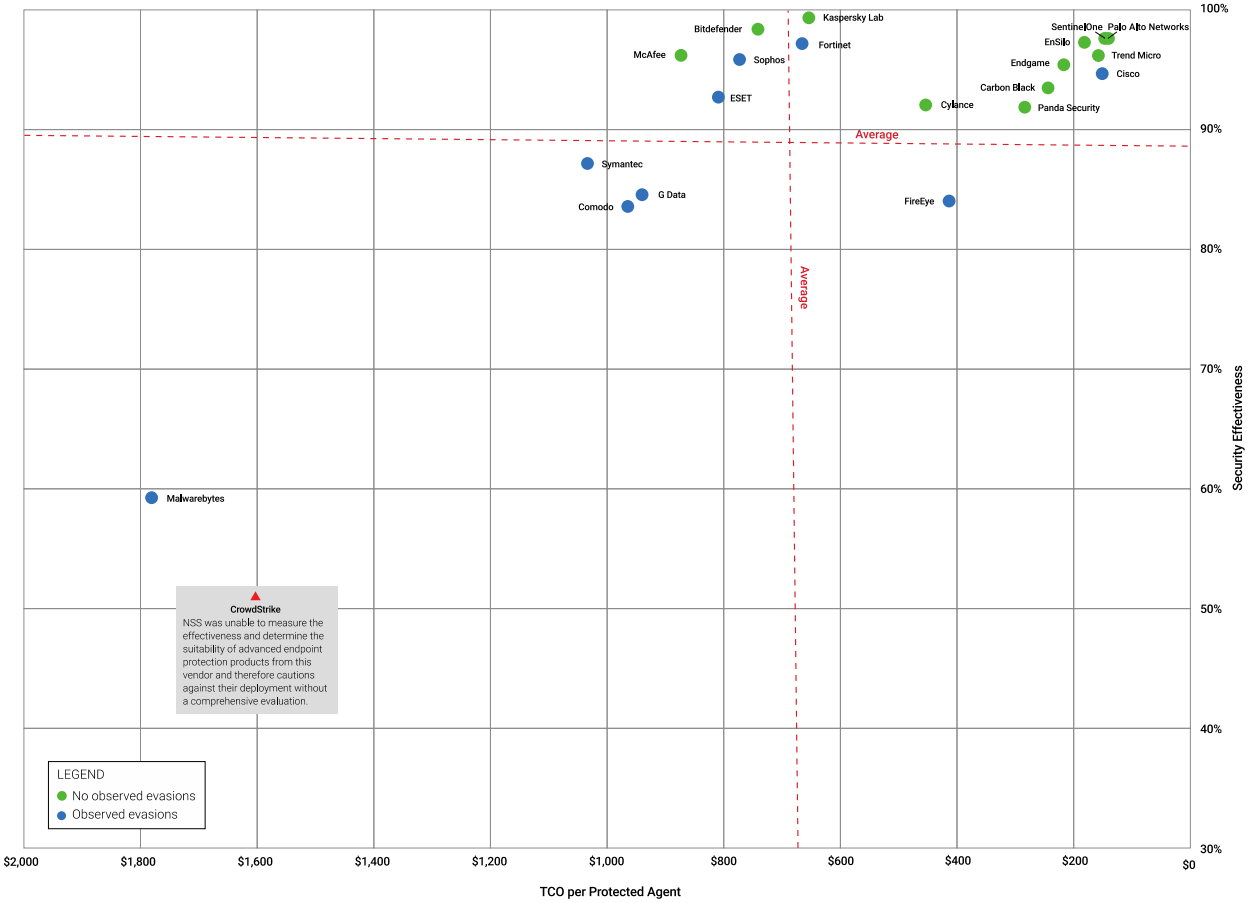

Figure 1 – NSS Labs' 2018 Security Value Map (SVM) for Advanced Endpoint Protection (AEP)

Key Findings

- Eleven products were rated as *Recommended;* four products were rated as *Security Recommended;* one *product was rated as Neutral;* and five products were rated as *Caution*.
- The *Security Effectiveness* of verified products ranged between 59.4% and 99.4% with ten of the twenty verified products achieving a rating greater than 95%.
- The average *Security Effectiveness* rating was 88.6%; fifteen of the verified products received an above-average *Security Effectiveness* rating, and five received a below-average *Security Effectiveness* rating.
- Nine verified products missed at least one evasion.
- The *TCO per Protected Agent* for verified products ranged between US$146 and US$1,783, with most tested products costing less than US$750 per protected agent.
- The average *TCO per Protected Agent* (*Value*) was US$690; twelve products demonstrated value above the average, and nine 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), *Security Recommended* (top left), *Neutral* (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 Agent)		Overall Rating
Bitdefender	98.5%	Above Average	$744	Below Average	Security Recommended
Carbon Black	93.6%	Above Average	$245	Above Average	Recommended
Cisco	94.7%	Above Average	$151	Above Average	Recommended
Comodo	83.7%	Below Average	$966	Below Average	Caution
Cylance	92.1%	Above Average	$455	Above Average	Recommended
Endgame	95.5%	Above Average	$218	Above Average	Recommended
enSilo	97.4%	Above Average	$184	Above Average	Recommended
ESET	92.8%	Above Average	$812	Below Average	Security Recommended
FireEye	84.2%	Below Average	$415	Above Average	Neutral
Fortinet	97.3%	Above Average	$667	Above Average	Recommended
G DATA	84.7%	Below Average	$941	Below Average	Caution
Kaspersky Lab	99.4%	Above Average	$656	Above Average	Recommended
Malwarebytes	59.4%	Below Average	$1,783	Below Average	Caution
McAfee	96.2%	Above Average	$874	Below Average	Security Recommended
Palo Alto Networks	97.7%	Above Average	$146	Above Average	Recommended
Panda Security	91.9%	Above Average	$286	Above Average	Recommended
SentinelOne	97.7%	Above Average	$148	Above Average	Recommended
Sophos	95.9%	Above Average	$775	Below Average	Security Recommended
Symantec	87.2%	Below Average	$1,036	Below Average	Caution
Trend Micro	96.2%	Above Average	$160	Above Average	Recommended
Crowdstrike	NA	NA	NA	NA	Caution

Figure 2 – NSS Labs' 2018 Recommendations for Advanced Endpoint Protection (AEP) Products

Table of Contents

Tested Products 1

Unverified Products 1

Environment 1

Overview 2

Key Findings 3

Product Rating 3

How to Read the SVM 6

The x axis 6

The y axis 6

Analysis 8

Recommended 8

Carbon Black Cb Defense v3.0.2.2 8

Cisco AMP for Endpoints v6.0.5 8

Cylance CylancePROTECT + OPTICS v2.0.1450 8

Endgame Endpoint Security v2.5 8

enSilo Endpoint Security Platform v2.7 9

Fortinet FortiClient v5.6.2 9

Kaspersky Lab Kaspersky Endpoint Security v10 9

Palo Alto Networks Traps v4.1 9

Panda Security Panda Adaptive Defense 360 v2.4 9

SentinelOne Endpoint Protection Platform (EPP) v2.0.1.10548 10

Trend Micro Smart Protection for Endpoints v12.0.1864 10

Security Recommended 10

Bitdefender GravityZone Elite v6.2.31.985 10

ESET Endpoint Protection Standard v6.5.522.0 10

McAfee Endpoint Security v10.5 10

Sophos Endpoint Protection 10.7.6 VE3.70.2 11

Neutral 11

FireEye Endpoint Security v4 11

Caution 11

Comodo Advanced Endpoint Protection v3.18.0 11

G DATA Endpoint Protection Business v14.1.0.67 11

Malwarebytes Endpoint Protection v1.1.1.0 12

Symantec Endpoint Protection and Advanced Threat Protection (ATP) Platform v14.0.3876.1100 12

CrowdStrike 12

Test Methodology 13

Contact Information 13

Table of Figures

Figure 1 – NSS Labs' 2018 Security Value Map (SVM) for Advanced Endpoint Protection (AEP) 2
Figure 2 – NSS Labs' 2018 Recommendations for Advanced Endpoint Protection (AEP) Products 3
Figure 3 – Example SVM 6

How to Read the SVM

The SVM depicts the value of a typical deployment of 500 agents.

This report is part of a series of Comparative Reports on security, 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.

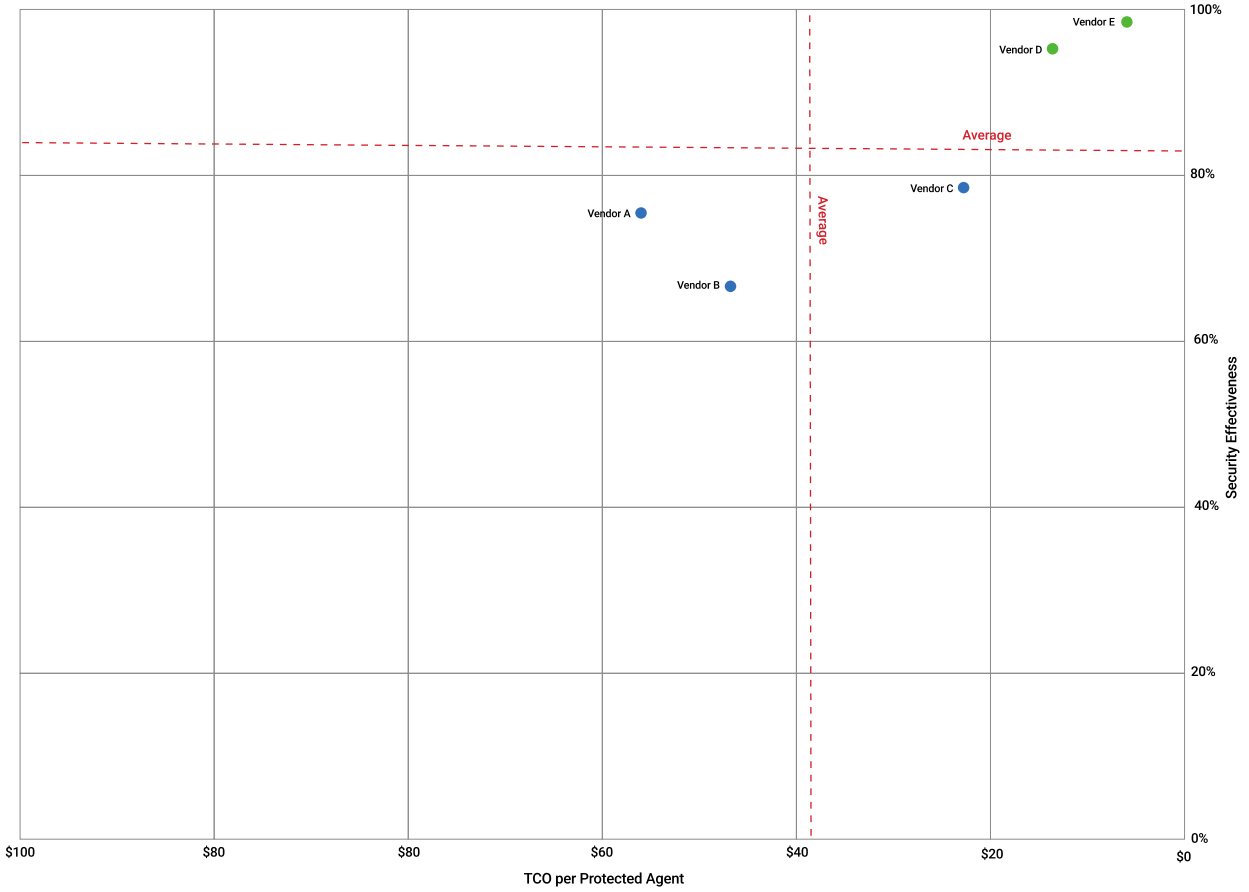

Figure 3 – Example SVM

No two security products deliver the same security effectiveness or TCO, making precise comparisons extremely difficult. In order to enable value-based comparisons of AEP products on the market, NSS has developed a unique metric: *TCO per Protected Agent*. For additional information, please see the TCO Comparative Report.

The *x* axis displays the *TCO per Protected Agent* in US dollars, which decreases from left to right. This metric incorporates the 3-Year TCO and operational expenditure (opex) savings with a calculated security score (*Overall Capability* score*)* to provide a data point by which to compare the actual value of each product tested. For more details on security and how it relates to *TCO per Protected Agent*, see the TCO comparative report 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. Products that are missing critical security capabilities will have a reduced *Security Effectiveness* score.

The SVM displays two dotted lines that represent the average *Security Effectiveness* and *TCO per Protected Agent* 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 Agent* 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 Agent***.** These products provide a high level of detection and value for money.
- **Security Recommended:** Products that map into the upper-left section of the SVM are suitable for environments requiring a high level of detection, albeit at a higher-than-average cost.
- **Neutral:** Products that map into the lower-right section of the SVM may be good choices for organizations where a slightly lower level of detection is acceptable in exchange for a lower TCO.
- **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*.

In all cases, the SVM should only be a starting point. Enterprise customers can contact NSS to model their own SVM in order to better understand which products might be best for them.

To establish TCO, *Block Rate* and *Additional Detection Rate* are included in the *Overall Capability* score calculations. These calculations are used to determine the *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). A product's capability to detect threats that were not blocked reduces the operational burden and cost of remediating infections and incidents (breaches).

The *Security Effectiveness* score, which is represented on the *y* axis of the SVM, does not include the *Additional Detection Rate* since the focus of an advanced endpoint protection (AEP) product is on blocking threats.

The *Security Effectiveness* score of some products is represented either by a blue or green dot. A green dot depicts products with no missed evasions, whereas a blue dot represents missed evasions.

Analysis

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

Recommended

Carbon Black Cb Defense v3.0.2.2

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 93.6%.
Evasions	The product received a score of 100% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product alerted on 0.6% false positives during testing.

Cisco AMP for Endpoints v6.0.5

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 94.7%.
Evasions	The product received a score of 97% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After the initial tuning, the product did not alert on any false positives during testing.

Cylance CylancePROTECT + OPTICS v2.0.1450

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 92.1%.
Evasions	The product received a score of 100% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After the initial tuning, the product did not alert on any false positives during testing.

Endgame Endpoint Security v2.5

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 95.5%.
Evasions	The product received a score of 100% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After the initial tuning, the product did not alert on any false positives during testing.

enSilo Endpoint Security Platform v2.7

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 97.4%.
Evasions	The product received a score of 100% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After the initial tuning, the product alerted on 0.1% false positives during testing.

Fortinet FortiClient v5.6.2

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 97.3%.
Evasions	The product received a score of 99% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After the initial tuning, the product did not alert on any false positives during testing.

Kaspersky Lab Kaspersky Endpoint Security v10

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 99.4%.
Evasions	The product received a score of 100% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product did not alert on any false positives during testing.

Palo Alto Networks Traps v4.1

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 97.7%.
Evasions	The product received a score of 100% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product did not alert on any false positives during testing.

Panda Security Panda Adaptive Defense 360 v2.4

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 91.9%.
Evasions	The product received a score of 100% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product alerted on 0.1% false positives during testing.

SentinelOne Endpoint Protection Platform (EPP) v2.0.1.10548

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 97.7%.
Evasions	The product received a score of 100% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product did not alert on any false positives during testing.

Trend Micro Smart Protection for Endpoints v12.0.1864

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 96.2%.
Evasions	The product received a score of 100% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product did not alert on any false positives during testing.

Security Recommended

Bitdefender GravityZone Elite v6.2.31.985

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 98.5%.
Evasions	The product received a score of 100% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product did not alert on any false positives during testing.

ESET Endpoint Protection Standard v6.5.522.0

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 92.8%.
Evasions	The product received a score of 96% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product did not alert on any false positives during testing.

McAfee Endpoint Security v10.5

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 96.2%.
Evasions	The product received a score of 100% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product did not alert on any false positives during testing.

Sophos Endpoint Protection 10.7.6 VE3.70.2

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 95.9%.
Evasions	The product received a score of 98% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product did not alert on any false positives during testing.

Neutral

FireEye Endpoint Security v4

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 84.2%.
Evasions	The product received a score of 96% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product did not alert on any false positives during testing.

Caution

Comodo Advanced Endpoint Protection v3.18.0

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 83.7%.
Evasions	The product received a score of 95% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product did not alert on any false positives during testing.

G DATA Endpoint Protection Business v14.1.0.67

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 84.7%.
Evasions	The product received a score of 95% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product did not alert on any false positives during testing.

Malwarebytes Endpoint Protection v1.1.1.0

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 59.4%.
Evasions	The product received a score of 93% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product did not alert on any false positives during testing.

Symantec Endpoint Protection and Advanced Threat Protection (ATP) Platform v14.0.3876.1100

Security Effectiveness	The product received an overall *Security Effectiveness* rating of 87.2%.
Evasions	The product received a score of 97% for evasions. Refer to the Comparative Report on Security for more on how evasions are factored into the *Security Effectiveness* score.
False Positives	After initial tuning, the product did not alert on any false positives during testing.

CrowdStrike

NSS was unable to measure the effectiveness and determine the suitability of advanced endpoint protection products from CrowdStrike and therefore cautions against their deployment without a comprehensive evaluation.

Test Methodology

Advanced Endpoint Protection (AEP) Test Methodology v2.0

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