ADVANCED ENDPOINT PROTECTION COMPARATIVE REPORT

Security Value Map™ (SVM)

FEBRUARY 14, 2017

Authors – Thomas Skybakmoen, Scott Marcks

Tested Products

Carbon Black Cb Protection v7.2.3.3106

CrowdStrike Falcon Host[1]

CylancePROTECT 1.2.1410

ESET Endpoint Security 6.4.2014.0

Fortinet FortiClient v5.4.1.0840

X by Invincea v4.2.0-387

Kaspersky Endpoint Security 10

Malwarebytes Endpoint Security v.1.7.4.0000

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 (AEP) Test Methodology v1.0

[1] 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

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

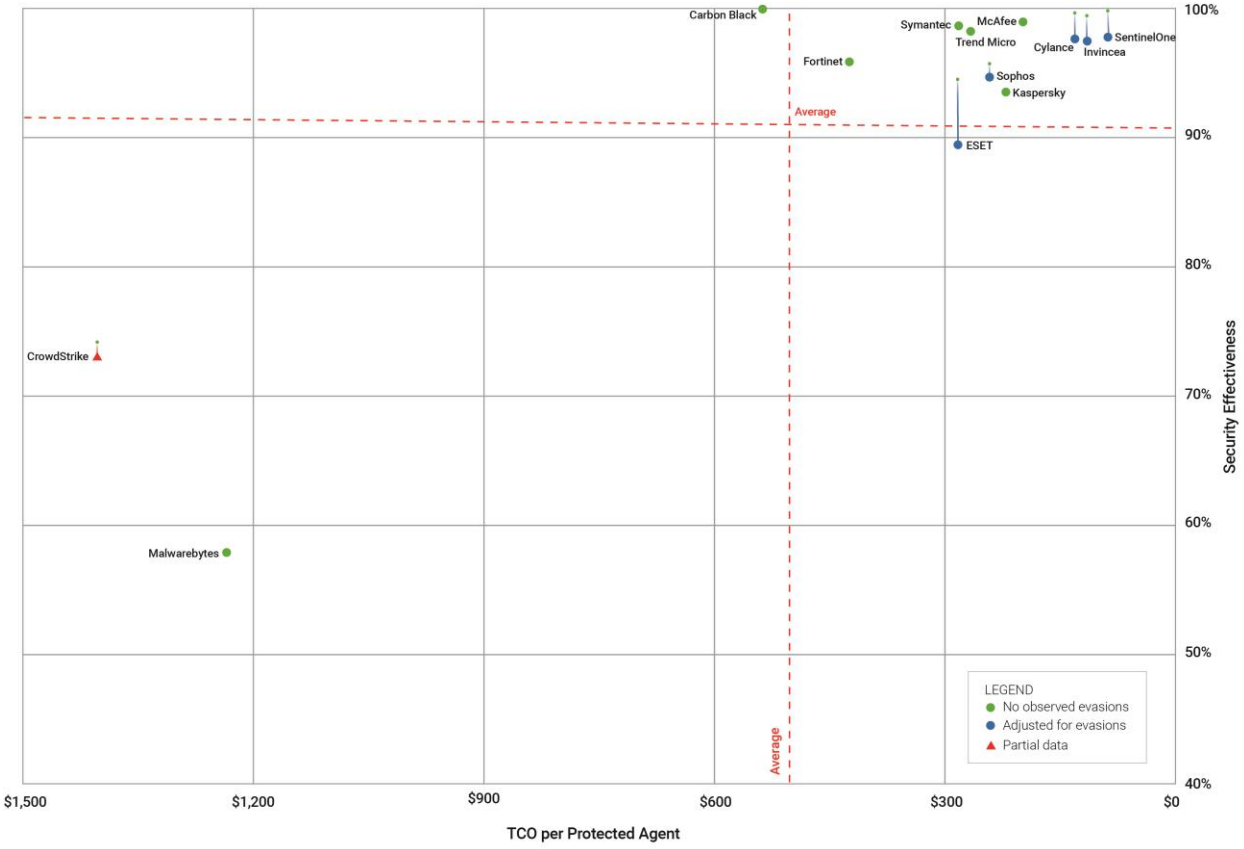

Figure 1 – NSS Labs' 2017 Security Value Map (SVM) for Advanced Endpoint Protection (AEP)

Key Findings

- Overall *Security Effectiveness* ranged from 57.9% to 100.0%, with 8 of the 13 tested products achieving a rating greater than 95%.
- The *TCO per Protected Agent* ranged from US$88 to US$1,404, with most tested products costing less than US$537 per protected agent.
- The average *Security Effectiveness* rating was 90.8%; 10 devices received an above-average *Security Effectiveness* rating, and 3 received a below-average *Security Effectiveness* rating.
- The average *TCO per Protected Agent* was US$502.67; 11 products were rated as having above-average value, 2 were rated as having below-average value.

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 Agent)		Overall Rating
Carbon Black	100.0%	Above Average	$538	Below Average	Security Recommended
CrowdStrike[2]	73.2%	Below Average	$1,404	Below Average	Caution[2]
CylancePROTECT	97.7%	Above Average	$131	Above Average	Recommended
ESET	89.5%	Below Average	$284	Above Average	Neutral
Fortinet	95.9%	Above Average	$425	Above Average	Recommended
Invincea	97.5%	Above Average	$116	Above Average	Recommended
Kaspersky	93.6%	Above Average	$222	Above Average	Recommended
Malwarebytes	57.9%	Below Average	$1,235	Below Average	Caution
McAfee	99.0%	Above Average	$199	Above Average	Recommended
SentinelOne	97.8%	Above Average	$88	Above Average	Recommended
Sophos	94.7%	Above Average	$243	Above Average	Recommended
Symantec	98.7%	Above Average	$284	Above Average	Recommended
Trend Micro	98.3%	Above Average	$268	Above Average	Recommended

Figure 2 – NSS Labs' 2017 Recommendations for Advanced Endpoint Protection (AEP)

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.

[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.

Table of Contents

Table of Figures

How to Read the SVM

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

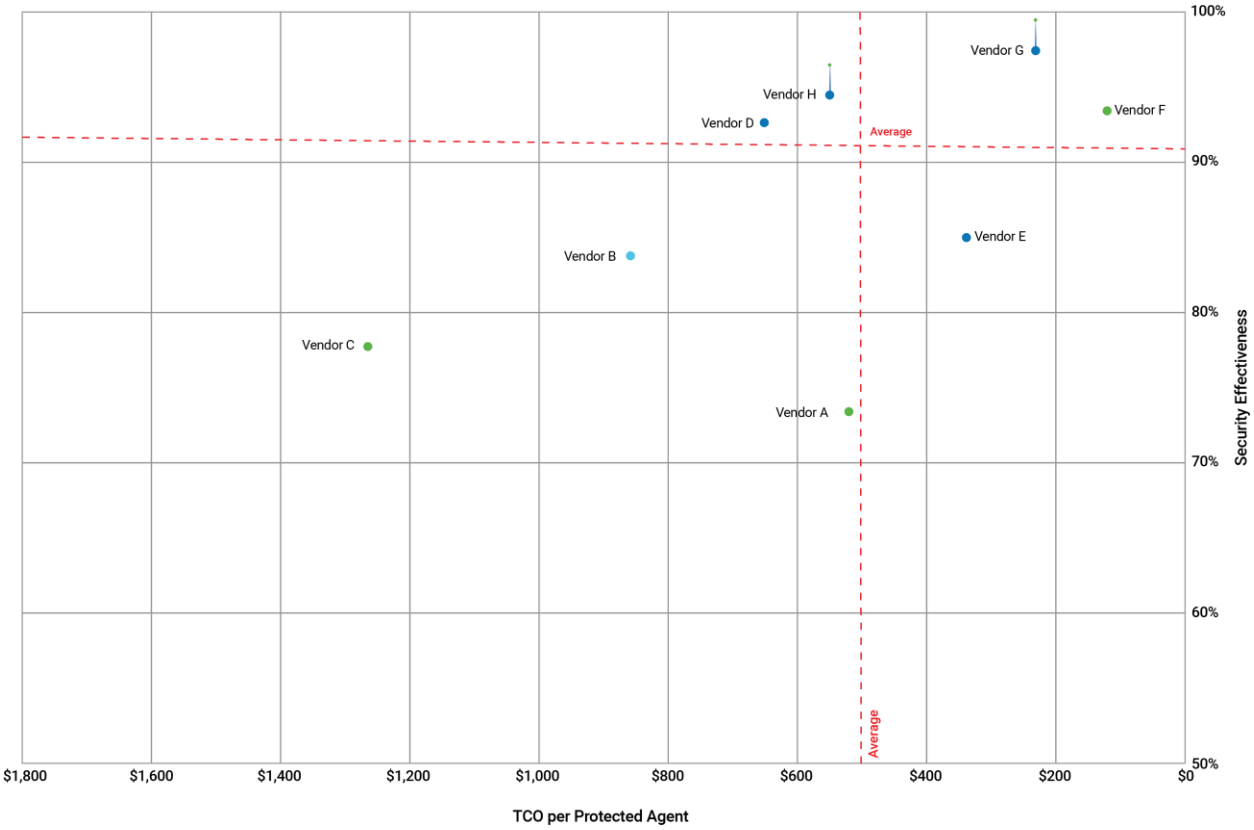

Figure 3 – Example SVM

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 the *Security Effectiveness* score to provide a data point by which to compare the actual value of each product tested. 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. Products that are missing critical security capabilities will have a reduced *Security Effectiveness* score.

Some products may have two data points, which represent two different scores. The higher score represents security effectiveness based solely on block rate and additional detection rate. However, this is not the only measure of security effectiveness; NSS also factors in evasions. This additional information allows NSS to calculate a second, lower score that more realistically depicts the actual security effectiveness of a product.

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.
- **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 as above average for *Security Effectiveness* but below average for *TCO per Protected Agent (Value)*. 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 as below average for *Security Effectiveness* but above average for *TCO per Protected Agent (Value)*. 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

CylancePROTECT 1.2.1410

Security Effectiveness	CylancePROTECT received an overall Security Effectiveness rating of 97.7%.
Evasions	CylancePROTECT received a score of 98.0% for evasions techniques tested. Please refer to the Security Comparative Report for additional information on how evasions are factored into the Security Effectiveness score.
False Positives	After the initial tuning, CylancePROTECT did not alert on any false positives during testing.

Fortinet FortiClient v5.4.1.0840

Security Effectiveness	Fortinet FortiClient received an overall Security Effectiveness rating of 95.9%.
Evasions	Fortinet FortiClient detected 100.0% of the evasions techniques tested.
False Positives	After the initial tuning, the Fortinet FortiClient did not alert on any false positives during testing.

X by Invincea v4.2.0-387

Security Effectiveness	X by Invincea received an overall Security Effectiveness rating of 97.5%.
Evasions	X by Invincea received a score of 98.0% for evasions techniques tested. Please refer to the Security Comparative Report for additional information on how evasions are factored into the Security Effectiveness score.
False Positives	After the initial tuning, the X by Invincea did not alert on any false positives during testing.

Kaspersky Endpoint Security 10

Security Effectiveness	Kaspersky Endpoint Security received an overall Security Effectiveness rating of 93.6%.
Evasions	Kaspersky Endpoint Security detected 100.0% of the evasions techniques tested.
False Positives	After the initial tuning, the Kaspersky Endpoint Security did not alert on any false positives during testing.

McAfee Endpoint Security v10.5

Security Effectiveness	McAfee Endpoint Security received an overall Security Effectiveness rating of 99.0%.
Evasions	McAfee Endpoint Security detected 100.0% of the evasions techniques tested.
False Positives	After the initial tuning, the McAfee Endpoint Security did not alert on any false positives during testing.

SentinelOne Endpoint Protection Platform v1.8.3#31

Security Effectiveness	SentinelOne Endpoint Protection Platform received an overall Security Effectiveness rating of 97.8%.
Evasions	SentinelOne Endpoint Protection Platform received a score of 98.0% for evasions techniques tested. Please refer to the Security Comparative Report for additional information on how evasions are factored into the Security Effectiveness score.
False Positives	After the initial tuning, the SentinelOne Endpoint Protection Platform did not alert on any false positives during testing.

Sophos Central Endpoint Advanced & Sophos InterceptX

Security Effectiveness	Sophos Central Endpoint Advanced & Sophos InterceptX received an overall Security Effectiveness rating of 94.7%.
Evasions	Sophos Central Endpoint Advanced & Sophos InterceptX received a score of 99.0% for evasions techniques tested. Please refer to the Security Comparative Report for additional information on how evasions are factored into the Security Effectiveness score.
False Positives	After the initial tuning, the Sophos Central Endpoint Advanced & Sophos InterceptX alerted on no false positives during testing.

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

Security Effectiveness	Symantec Endpoint Protection 14 with ATP Endpoint received an overall Security Effectiveness rating of 98.7%.
Evasions	Symantec Endpoint Protection 14 with ATP Endpoint detected 100.0% of the evasions techniques tested.
False Positives	After the initial tuning, the Symantec Endpoint Protection 14 with ATP Endpoint (EDR) V2.2 did not alert on any false positives during testing.

Trend Micro OfficeScan XGEN v12.0.1851

Security Effectiveness	Trend Micro OfficeScan XGEN received an overall Security Effectiveness rating of 98.3%.
Evasions	Trend Micro OfficeScan XGEN detected 100.0% of the evasions techniques tested.
False Positives	After the initial tuning, the Trend Micro OfficeScan XGEN did not alert on any false positives during testing.

Neutral

Carbon Black Cb Protection v7.2.3.3106

Security Effectiveness	Carbon Black Cb Protection received an overall Security Effectiveness rating of 100.0%. This 100% security effectiveness is a result of its whitelisting technology.
Evasions	Carbon Black Cb Protection detected 100.0% of the evasions techniques tested.
False Positives	After the initial tuning, the Carbon Black Cb Protection alerted on no false positives during testing.

NOTE: Enterprises must factor in the ongoing operational overhead that often accompanies whitelisting, which means it may not be appropriate for all deployments. As seen in NSS' Security Value Map TM, Carbon Black has a higher than average total cost of ownership (TCO). For additional information, please see the Security and TCO Comparative Reports.

ESET Endpoint Security 6.4.2014.0

Security Effectiveness	ESET Endpoint Security received an overall Security Effectiveness rating of 89.5%.
Evasions	ESET Endpoint Security received a score of 95.0% for evasions techniques tested. Please refer to the Security Comparative Report for additional information on how evasions are factored into the Security Effectiveness score.
False Positives	After the initial tuning, the ESET Endpoint Security did not alert on any false positives during testing.

Caution

CrowdStrike Falcon Host

Security Effectiveness	CrowdStrike Falcon Host[3] received an overall Security Effectiveness rating of 73.2%.
Evasions	CrowdStrike Falcon Host received a score of 99.0% for evasions techniques tested. Please refer to the Security Comparative Report for additional information on how evasions are factored into the Security Effectiveness score.
False Positives	After the initial tuning, CrowdStrike Falcon Host did not alert on any false positives during testing.

Malwarebytes Endpoint Security v.1.7.4.0000

Security Effectiveness	Malwarebytes Endpoint Security received an overall Security Effectiveness rating of 57.9%.
Evasions	Malwarebytes Endpoint Security detected 100.0% of the evasions techniques tested.
False Positives	After the initial tuning, Malwarebytes Endpoint Security did not alert on any false positives during testing.

[3] NSS Labs was unable to complete testing due to remotely disabled access. The Falcon Host's final rating may have been different had it completed the test.

Test Methodology

Advanced Endpoint Protection (AEP) 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