ADVANCED ENDPOINT PROTECTION COMPARATIVE REPORT

Security

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

Implementation of advanced endpoint protection (AEP) products can be complex, with multiple factors affecting security effectiveness. The following factors should be considered when evaluating these products:

- Blocking capabilities
- Detection capabilities
- Resistance to evasions
- Manageability and forensics capabilities

The *Security Effectiveness* score, which is represented on the y axis of the SVM, does not include the *Additional Detection Rate*, since an AEP product's focus is on blocking threats. However, to establish total cost of ownership (TCO), *Block Rate* and *Additional Detection Rate* are included in the *Overall Capability Score* calculations. The *Overall Capability Score* 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). For additional information on TCO, please see the Comparative Report on TCO at www.nsslabs.com.The security effectiveness of a product is determined primarily by its block rate, but calculations also take into consideration the severity of each attack used in the test. Figure 1 presents the results of *Security Effectiveness* testing.

Vendor	Security Effectiveness
Bitdefender	97.2%
Carbon Black	96.9%
Check Point	96.6%
Cisco	94.5%
Comodo	98.5%
Cylance	96.8%
Endgame	98.9%
enSilo	97.4%
Fortinet Technologies	96.7%
F-Secure	98.3%
Kaspersky Lab	96.8%
Malwarebytes	92.8%
Panda Security	98.4%
Sophos	99.1%
Symantec	96.2%
Trend Micro	97.1%
Vendor A	90.8%
Vendor B	87.4%
Vendor C	87.8%

Figure 1 – Security Effectiveness

Table of Contents

Table of Figures

Analysis

The threat landscape is evolving constantly; attackers are refining their strategies and increasing both the volume and the sophistication of their attacks. Additionally, enterprises now must defend against targeted persistent attacks. In the past, servers were the main target; however, attacks against desktop client applications are now mainstream and present a clear danger to organizations as an initial infection vector.

As part of the initial AEP group test setup, 96 instances of the endpoint product were deployed on Windows 7 and Windows 10 operating systems. All product configurations were reviewed, validated, and approved by NSS prior to the test.

Block Rate

Block Rate is defined as the percentage of exploits and malware blocked within 15 minutes of attempted execution. *Block Rate* measures a product's ability to block malware and exploits during download, on access, and during execution. Products use various methods, including reputation, application whitelisting, behavior-based blocking, and/or signatures to block threats.

Additional Detection Rate

The *Additional Detection Rate* is defined as the percentage of exploits and malware detected but not blocked within 15 minutes of attempted execution. The ability of the product to detect and report on successful infections in a timely manner is critical to maintaining the security and functionality of the monitored network. Infection and transmission of malware should be reported quickly and accurately, giving administrators the opportunity to contain the infection and minimize impact on the network.

False Positives

The ability of an AEP product to correctly identify and allow benign content is as important as its ability to provide protection against malicious content. NSS ran various samples of legitimate application files and documents, all of which products were required to properly identify and allow. If any legitimate files could not be opened or executed immediately, these were recorded as a false positives. For additional information on false positives, please see the individual test reports, available at www.nsslabs.com.

Test Categories

- **Malware Delivered over HTTP:** In these web-based attacks, users click on malicious links to download and execute malware.
- **Malware Delivered over Email:** In these inbound, email-based attacks, users are deceived into downloading malicious attachments in emails to execute malware.
- **Malware Delivered by Docs and Scripts**: In these attacks, malware is delivered via documents and scripts. Such attacks could be as simple as delivering malware using macros.
- **Offline Threats:** These attacks are performed on victim machines that are disconnected from the Internet. Attacks are delivered and executed with no cloud or backend connectivity or support. Victim machines are later reconnected to the network.

- **Unknown Threats:** These threats have not previously been seen in the wild. They are either samples created by NSS, or they are pre-existing samples that have been modified.
- **Exploits:** These are defined as malicious software that is designed to take advantage of existing deficiencies in hardware or software systems, such as vulnerabilities or bugs. In some cases, a user merely needs to visit a web page hosting malicious code in order to be infected via exploits.
- **Blended Threats**: These threats possess the characteristics of both exploits and socially engineered malware. They attempt to make it difficult to distinguish between what is malicious and what is legitimate activity.
- **Evasions**: These techniques include packers, crypters, and other types of evasive techniques used to bypass traditional antivirus signature detection.

Test Composition

Each product was initially tested against 1,629 unique malicious samples and 1,061 unique false positive samples. Ultimately, 897 unique malicious samples and 1,053 unique false positive samples met NSS' validation criteria and were included as part of the test. Figure 2 depicts the percentage of samples used in each test category.

Tests	Samples[1]
Malware (various delivery mechanisms)	Percentage of Total Samples
HTTP	29.1%
Email	50.5%
Documents and Scripts	6.9%
Offline Threats	1.7%
Unknown Threats	2.5%
Exploits	1.9%
Blended Threats	2.9%
Evasions	4.6%

Figure 2 – Test Composition

[1] No product is able to provide 100% protection against attacks. A single successful attack is often all an attacker needs to gain unauthorized access, infiltrate an organization, and steal or destroy data.

Block Rate

Figure 3 displays each product's block rate for all test categories.

Vendor	HTTP	Email	Docs & Scripts	Offline Threats	Unknown Threats	Exploits	Blended Threats	Evasions
Bitdefender	100.0%	97.9%	87.1%	100.0%	100.0%	88.2%	88.5%	100.0%
Carbon Black	99.1%	100.0%	91.9%	100.0%	95.5%	94.1%	46.2%	97.6%
Check Point	100.0%	100.0%	90.3%	100.0%	81.8%	88.2%	50.0%	100.0%
Cisco	98.7%	99.7%	85.5%	93.3%	95.5%	76.5%	15.4%	97.6%
Comodo	100.0%	100.0%	100.0%	100.0%	100.0%	58.8%	84.6%	100.0%
Cylance	98.7%	99.5%	100.0%	80.0%	95.5%	88.2%	50.0%	100.0%
Endgame	99.6%	99.7%	98.4%	100.0%	100.0%	70.6%	100.0%	100.0%
enSilo	99.6%	99.7%	96.8%	100.0%	100.0%	64.7%	65.4%	100.0%
Fortinet Technologies	100.0%	98.5%	91.9%	93.3%	100.0%	100.0%	50.0%	100.0%
F-Secure	100.0%	98.5%	91.9%	86.7%	100.0%	100.0%	100.0%	100.0%
Kaspersky Lab	99.7%	98.7%	83.9%	100.0%	100.0%	88.2%	76.9%	100.0%
Malwarebytes	98.4%	99.0%	83.9%	100.0%	50.0%	76.5%	19.2%	100.0%
Panda Security	99.6%	99.4%	96.8%	100.0%	100.0%	76.5%	88.5%	100.0%
Sophos	100.0%	99.5%	96.8%	100.0%	100.0%	100.0%	88.5%	100.0%
Symantec	99.0%	100.0%	98.4%	80.0%	95.5%	82.4%	30.8%	68.3%
Trend Micro	99.5%	99.7%	88.7%	53.3%	95.5%	76.5%	100.0%	90.2%
Vendor A	99.1%	97.2%	80.6%	100.0%	95.5%	82.4%	11.5%	92.7%
Vendor B	92.4%	96.4%	100.0%	26.7%	68.2%	47.1%	53.8%	75.6%
Vendor C	88.9%	88.4%	100.0%	93.3%	95.5%	47.1%	57.7%	100.0%

Figure 3 – Block Rate

Once a product's block rate has been determined and once the severity of each attack has been factored in, security effectiveness can be calculated. See Figure 1 for the results of the security effectiveness testing.

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

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