ADVANCED ENDPOINT PROTECTION TEST REPORT

Carbon Black Cb Protection v7.2.3.3106

FEBRUARY 14, 2017

Authors – Thomas Skybakmoen, Morgan Dhanraj

Overview

NSS Labs performed an independent test of the Carbon Black Cb Protection product. The product was subjected to thorough testing at the NSS facility in Austin, Texas, based on the Advanced Endpoint Protection (AEP) Test Methodology v1.0, which is available at www.nsslabs.com. This test was conducted free of charge and NSS did not receive any compensation in return for Carbon Black's inclusion.

This report provides detailed information about this product and its security effectiveness. Additional comparative information is available at www.nsslabs.com.

As part of the initial AEP test setup, products were configured in a deployment mode typical to enterprises. As such, products were configured to mimic an enterprise environment by applying typical applications such as exclusion policies and tuning requirements. All product-based configurations are reviewed, validated, and approved by NSS prior to the test. Every effort is made to ensure optimal security effectiveness, as would be the aim of a typical customer deploying the product in a live environment. Figure 1 presents the overall results of the tests.

Product						Security Effectiveness[1]	
Carbon Black Cb Protection v7.2.3.3106						100.0%	
HTTP	HTTPS	Email	P2P Applications	Local Intelligence	Blended Threats	Exploits	Various Evasions
100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Figure 1 – Overall Test Results

The Cb Protection achieved a Security Effectiveness rating of 100.0%. The Cb Protection did not block any false positive samples after the initial tuning. The Cb Protection blocked all of the tested evasions.

[1] Security effectiveness is defined as the number of exploits and malware blocked and detected under test within the 2-hour window.

Table of Contents

Table of Figures

Security Effectiveness

The aim of this section is to verify that the advanced endpoint product is capable of detecting, preventing, and continuously logging threats accurately, whilst remaining resistant to false positives. This section utilizes real threats and attack methods that exist in the wild and that are being used by cybercriminals and other threat actors, based on attacks collected from NSS' global threat intelligence network.

The ultimate goal of any attack on a computer system is to gain access to a target host and perform an unauthorized action, which results in the compromise of an asset or data. Computer systems are designed with many levels of protection to prevent unauthorized access. However, intruders may use several techniques to circumvent these levels of protection, such as targeting vulnerable services, invoking backdoor privilege escalation, or replacing key operating system files. AEP products protect against automated and manual threats by leveraging the following key capabilities:

- Inbound threat detection and prevention (prior to execution)
- Execution-based threat detection and prevention (during execution)
- Continuous monitoring post-infection and ability to act in the event of compromise (post-execution)

NSS has created a unique testing infrastructure—the NSS Labs Live Testing™ harness, which incorporates multiple product combinations, or "stacks," within the attack chain. Each stack consists of either an OS alone, or of an OS with additional applications installed (e.g., a browser, Java, and Adobe Acrobat). These stacks make up the BaitNET™ test harness, which is also the primary engine for NSS' Cyber Advanced Warning System™ (CAWS). This test harness continuously captures suspicious URLs from threat data generated from NSS and its customers, as well as data from open-source and commercial threat feeds.

An AEP product must be able to detect, prevent, continuously monitor, and take action against threats while providing end-to-end visibility through event logs generated by the endpoint product. Each of the above threat categories contains unique infection vectors, and the test aims to determine how effective the AEP product is at protecting against a threat, regardless of the infection vector or method of obfuscation. The term "threat" used within this report refers to malware, exploits, or blended threats that are able to successfully access, download, and execute on a target system, with or without subsequent post-infection compromise and/or outbound communication attempts.

AEP products were tested against the following threat categories in NSS' AEP Group Test:

- Malware
- Exploits
- Blended threats

Each type of threat is deployed via one of the following infection vectors:

- **HTTP**: These attacks are web-based, where the user is deceived into clicking on a malicious link to download and execute malware, or where the user merely needs to visit a web page hosting malicious code in order to be infected via exploits.
- **HTTPS**: These attacks occur when attackers compromise high-profile websites or websites with a specific clientele in order to serve exploits from a trusted source.
- **Email** (IMAP4/POP3): These are inbound, email-based attacks where the user is deceived into clicking on a malicious link to download and execute malware, or where the user merely needs to visit a web page hosting

malicious code in order to be infected via exploits. A user can also be deceived into downloading and executing malicious attachments.

- **Productivity software**: These applications are used for file sharing, collaboration, and/or social networking; common examples include Skype, Dropbox, Google Drive, Facebook, and Bitcasa.
- **P2P applications**: These applications allow the user to download parts of files from multiple sources on the Internet at the same time. Common examples include BitTorrent, Gnutella, Pando, BearShare, and Vuze.

False Positives

The ability of the AEP product to correctly identify and allow benign traffic is as important as its ability to provide protection against malicious content. The AEP product accomplishes this by detecting, preventing, and continuously monitoring threats, while at the same time allowing non-malicious traffic to pass. As part of initial setup and tuning, NSS ran various samples of legitimate application traffic, which were properly identified and allowed by the product. If legitimate traffic had not been not allowed, NSS would have measured it as a false positive alert. After initial tuning, the Cb Protection did not alert on any false positives during testing.

Product	False Positive Rate
Carbon Black Cb Protection v7.2.3.3106	0.0%

Figure 2 – Malware Delivered by False Positives

Malware

One of the most common ways in which systems are compromised is through socially engineered malware. This section focuses on social engineering techniques that deceive users into downloading malicious files that are delivered via the following infection vectors:

- HTTP
- HTTPS
- Email (IMAP4/POP3)
- Productivity software
- P2P applications

Malware Delivered by HTTP

Figure 3 depicts malware delivered using HTTP. Over the course of the test, the Cb Protection blocked 100.0% of malware delivered by HTTP. It did not detect any additional malware. This resulted in an overall score of 100.0%.

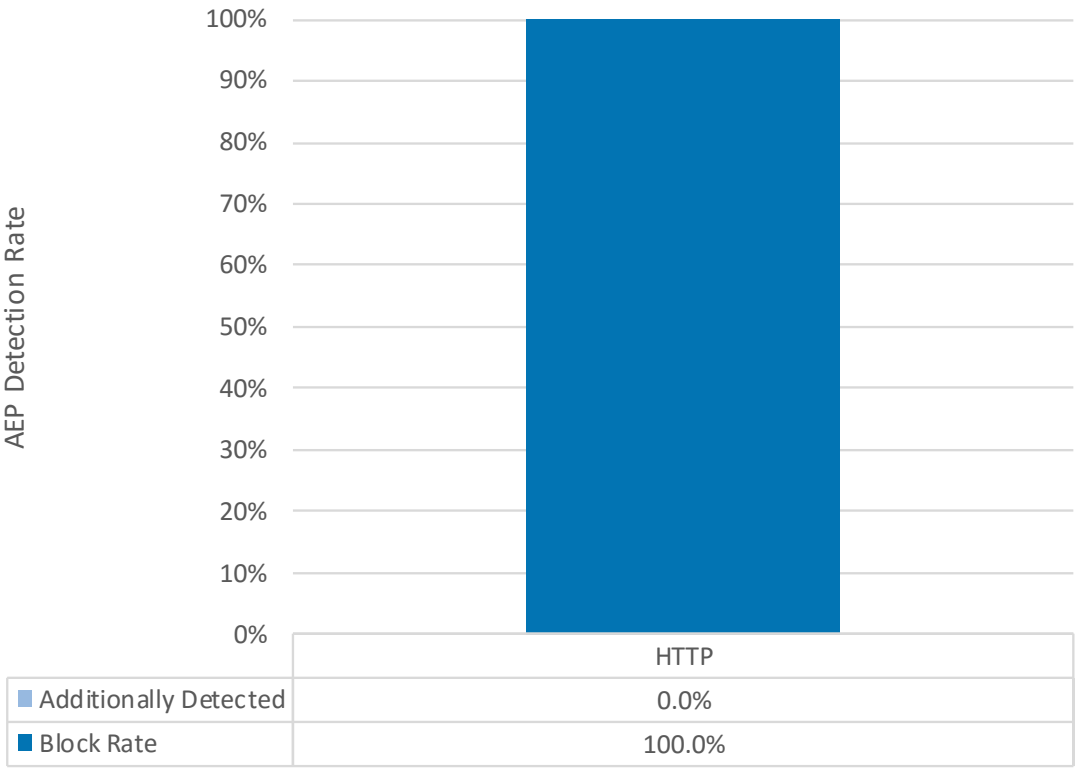

Figure 3 – Malware Delivered by HTTP

Malware Delivered by HTTPS

Figure 4 depicts malware delivered using HTTPS. Over the course of the test, the Cb Protection blocked 100.0% of malware delivered by HTTPS. It did not detect any additional malware. This resulted in an overall score of 100.0%.

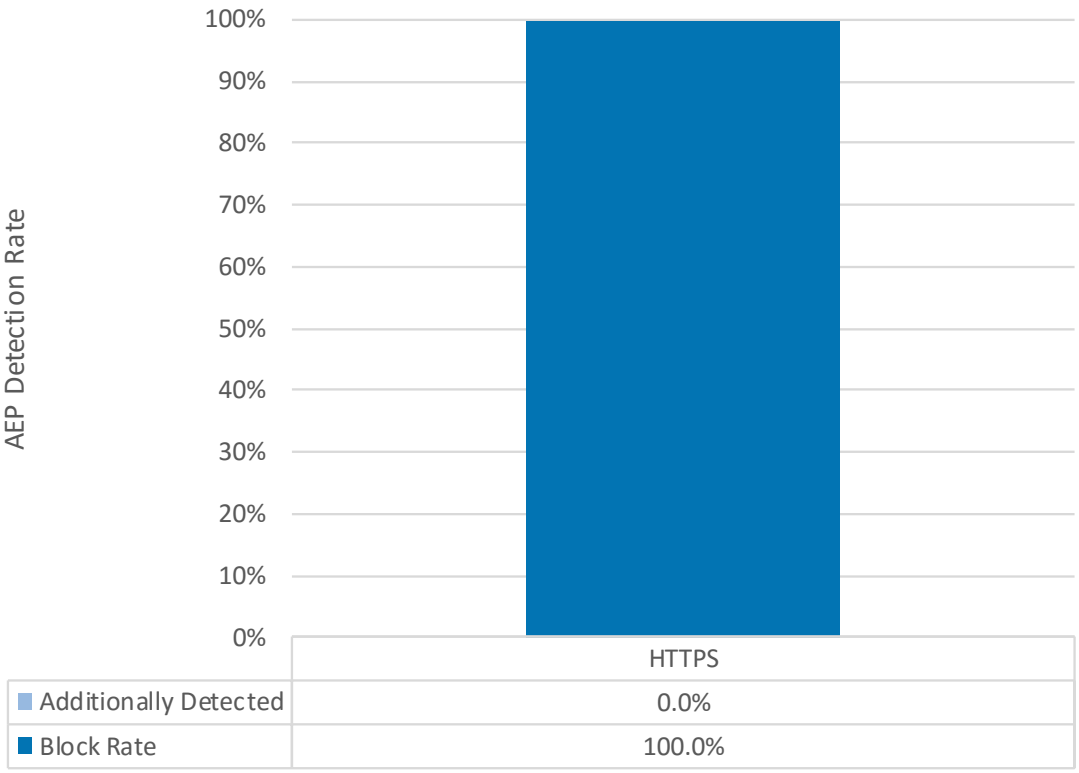

Figure 4 – Malware Delivered by HTTPS

Malware Delivered over Email

Figure 5 depicts malware that uses email (IMAP4/POP3) as its transport mechanism (e.g., a malicious email attachment). Over the course of the test, the Cb Protection blocked 100.0% of malware delivered over email. It did not detect any additional malware. This resulted in an overall score of 100.0%.

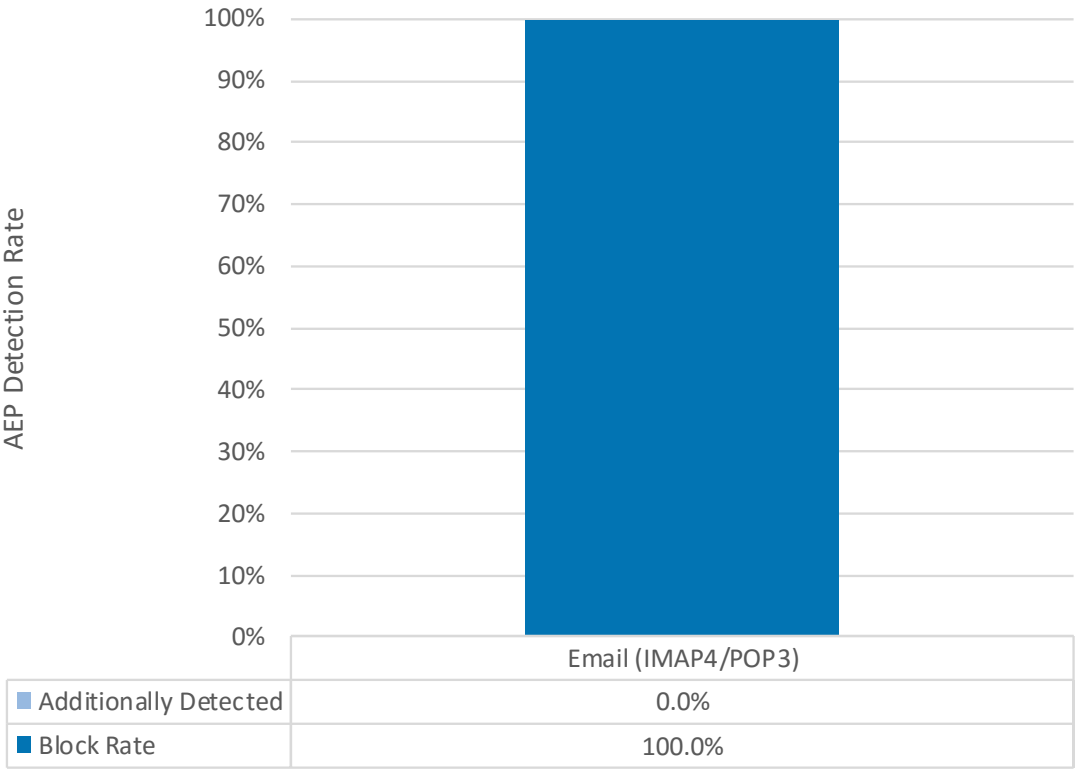

Figure 5 – Malware Delivered by Email

Malware Delivered over P2P

Figure 6 depicts malware that uses P2P as its transport mechanism. Over the course of the test, the Cb Protection blocked 100.0% of malware using P2P as its transport mechanism. It did not detect any additional malware. This resulted in an overall score of 100.0%.

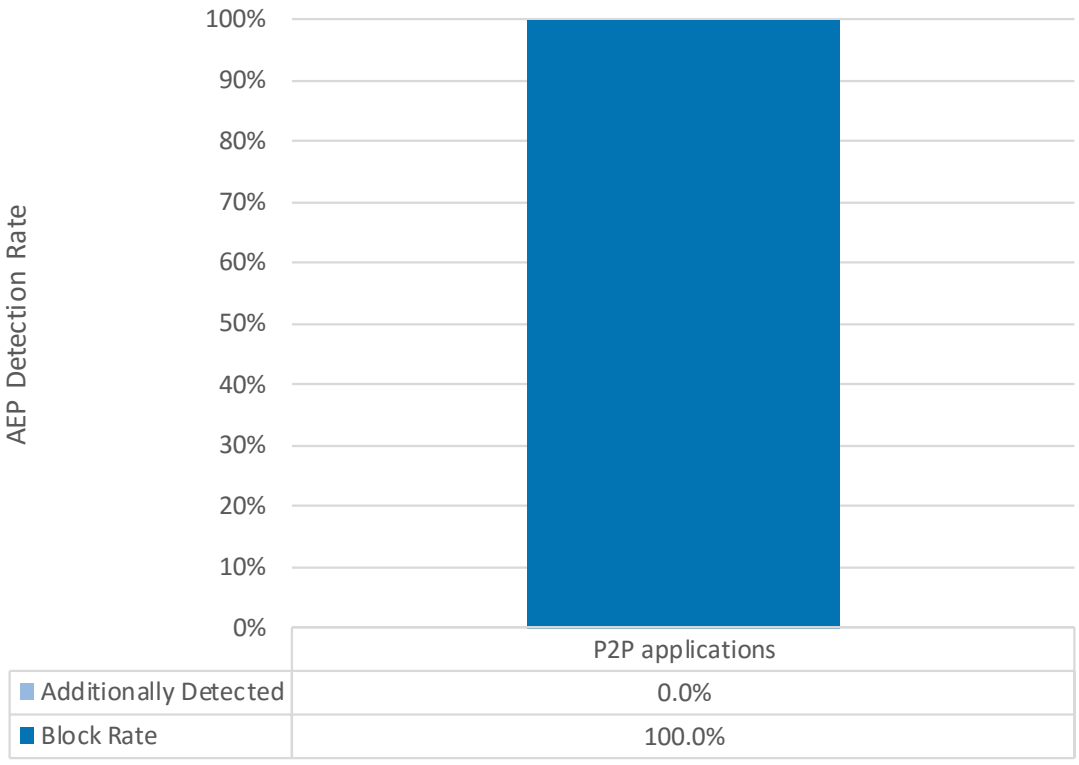

Figure 6 – Malware Delivered over P2P Applications

Local Intelligence Evaluation

This test evaluated local endpoint intelligence. Hosts without cloud connectivity may be infected outside the corporate network with or without an endpoint product installed.

Figure 7 depicts the results of the local intelligence test. Over the course of the test, the Cb Protection blocked 100.0% of attacks. It did not detect any additional attacks. This resulted in an overall score of 100.0%.

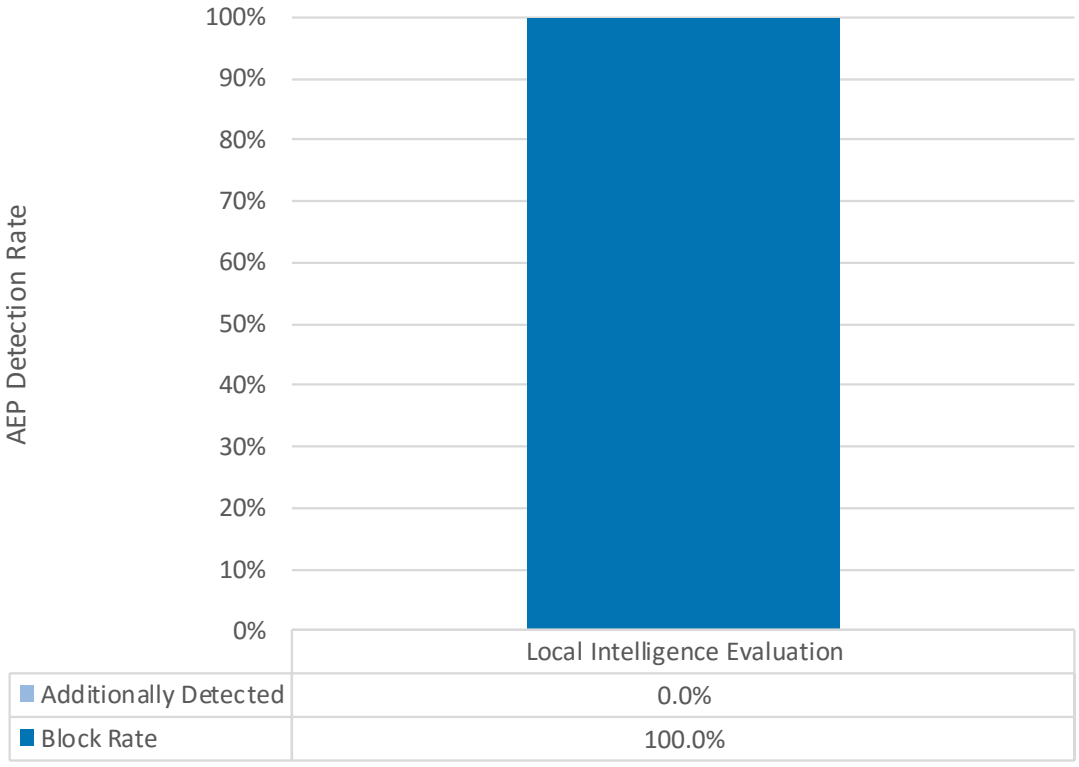

Figure 7 – Malware Delivered by Local Intelligence

Exploits

Figure 8 depicts exploits. These are defined as malicious software designed to take advantage of existing deficiencies in hardware or software systems, such as vulnerabilities or bugs. Over the course of the test, the Cb Protection blocked 100.0% of exploits. It did not detect any additional exploits. This resulted in an overall score of 100.0%.

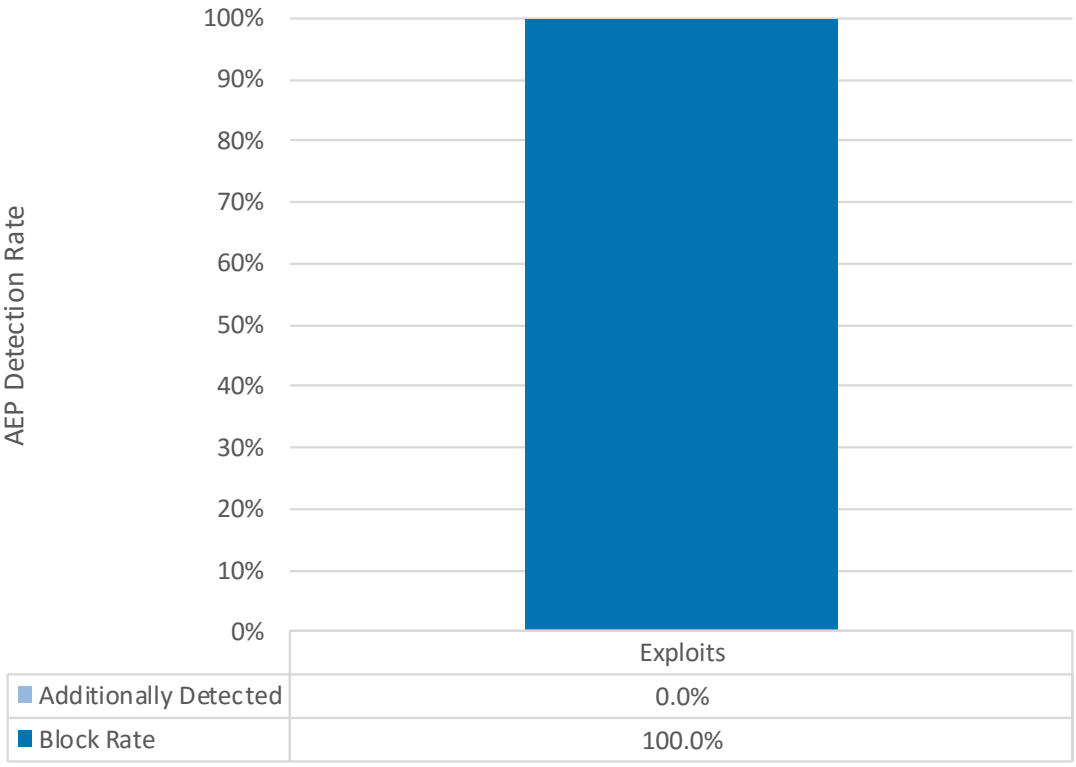

Figure 8 – Exploits

Blended Threats

Blended threats possess the characteristics of both exploits and socially engineered malware. Enterprises expect most AEP products to be able to address these types of threats. Some examples of blended threats include unknown threats, ransomware, kernel-mode exploits, chained exploits, rootkits, and Trojans.

Figure 9 depicts blended threats. Over the course of the test, the Cb Protection blocked 100.0% of blended threats. It did not detect any additional blended threats. This resulted in an overall score of 100.0%.

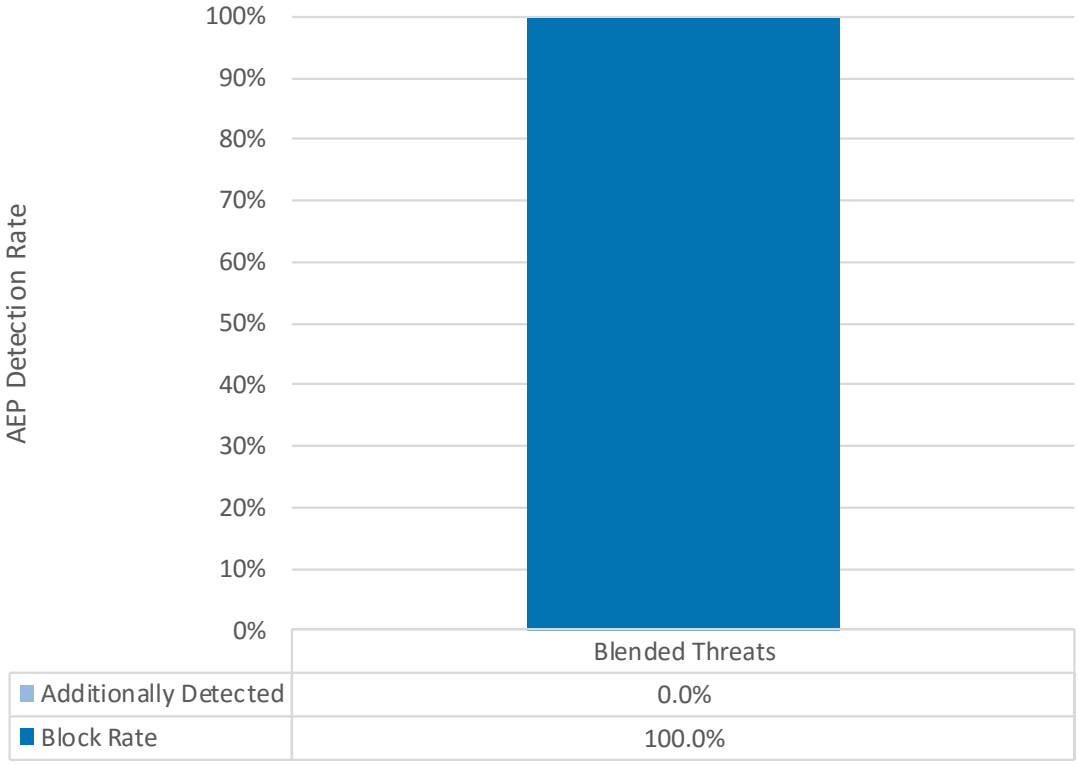

Figure 9 – Blended Threats

Resistance to Evasion Techniques

Cybercriminals deploy evasion techniques to disguise and modify attacks at the point of delivery in order to avoid detection by AEP products. If an AEP product fails to correctly identify a specific type of evasion, an attacker can potentially deliver malware that the AEP would normally detect. Attackers can modify attacks and malicious code in order to evade detection in a number of ways.

In this section, NSS verifies that the AEP product is capable of detecting, preventing, and continuously monitoring threats and that it is able to take action against malware, exploits, and blended threats when subjected to various common evasion techniques. Please contact NSS Labs for additional information on the evasions utilized.

Figure 10 provides the results of the evasion tests for the Cb Protection.

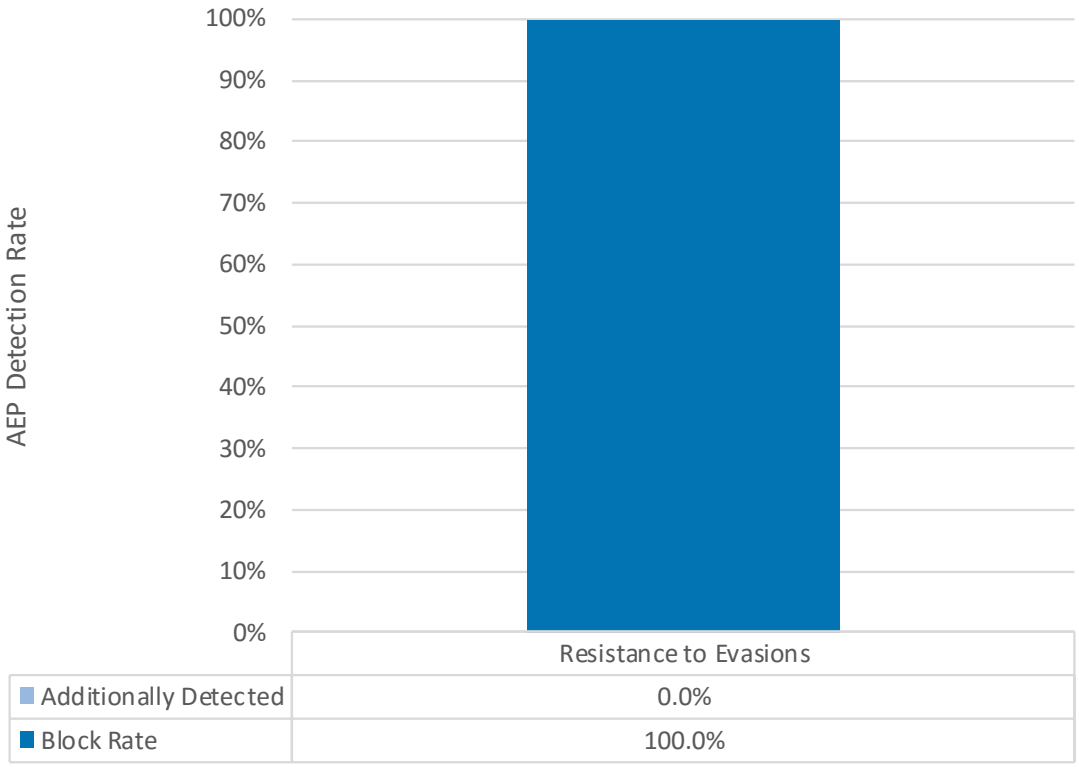

Figure 10 – Resistance to Evasions

Total Cost of Ownership (TCO)

Implementation of AEP products can be complex, with several factors affecting the overall cost of deployment, maintenance, and upkeep. All of these factors should be considered over the course of the useful life of the product, as well as any component of the AEP product under test and any application/service that is leveraged in the public or private cloud during testing.

- Product purchase – The cost of acquisition
- Product maintenance – The fees paid to the vendor (including software, maintenance, and updates)
- Installation – The time required to configure the security product, deploy it in the network, apply updates and patches, and set up desired logging and reporting
- Threat alerting and monitoring – The time required to review and act upon alerts and other threat information generated by the AEP product during testing
- Upkeep – The time required to apply periodic updates and patches from vendors, including software updates

For TCO analysis, refer to the TCO Comparative Report, which is available at www.nsslabs.com.

Appendix A: Product Scorecard

Security Effectiveness		100.0%	
False positives (detection accuracy)		0.0%	
Malware	Block rate	Additional detection rate	Security Effectiveness
HTTP	100.0%	0.0%	100.0%
HTTPS	100.0%	0.0%	100.0%
Email (IMAP4/POP3)	100.0%	0.0%	100.0%
P2P applications	100.0%	0.0%	100.0%
Local intelligence evaluation	100.0%	0.0%	100.0%
Exploits	Block rate	Additional detection rate	Security Effectiveness
Exploits	100.0%	0.0%	100.0%
Blended threats	100.0%	0.0%	100.0%
Evasions	Block rate	Additional detection rate	Security Effectiveness
Evasions	100.0%	0.0%	100.0%

Figure 11 – Scorecard

Appendix B: Acknowledgement

NSS Labs would like to thank its partners for their support during this group test.

Test Methodology

Advanced Endpoint Protection (AEP) Test Methodology v1.0

A copy of the test methodology is available at www.nsslabs.com.

Contact Information

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