ADVANCED ENDPOINT PROTECTION TEST REPORT

Palo Alto Networks Traps v4.1

APRIL 17, 2018

Authors – Rabin Bhattarai, Edsel Valle, Morgan Dhanraj, Ryan Kelly

Overview

NSS Labs performed an independent test of the Palo Alto Networks Traps v4.1. The product was subjected to thorough testing at the NSS facility in Austin, Texas, based on the Advanced Endpoint Protection (AEP) Test Methodology v2.0, which is available at www.nsslabs.com. This test was conducted free of charge and NSS did not receive any compensation in return for Palo Alto Networks' 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 test.

Product						3-Year TCO – 500 Agents (US$)		
Palo Alto Networks Traps v4.1						$36,000		
	HTTP	Email	Docs & Scripts	Offline Threats	Unknown Threats	Exploits	Blended Threats	Evasions
Block Rate	99.6%	99.4%	100%	92.3%	83.3%	100%	36.4%	100%
Additional Detection Rate	0.0%	0.0%	0.0%	0.0%	0.0%	0%	0.0%	0.0%

Figure 1 – Overall Test Results

Block Rate is defined as the percentage of exploits and malware blocked within 15 minutes. The *Additional Detection Rate* depicts the percentage of exploits and malware detected but not blocked within 30 minutes.

An AEP product with a low block rate 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. For detailed TCO analysis, please see the TCO Comparative Report at www.nsslabs.com.

Table of Contents

Table of Figures

Security Effectiveness

The aim of this section is to verify that the AEP 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 that 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 protections, 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 operating system alone or an operating system with additional applications installed (e.g., a browser, Java, and Adobe Acrobat). These stacks make up NSS' Continuous Security Validation Platform. This test harness continuously captures suspicious URLs, exploits, and malicious files from threat data generated from NSS and its customers, as well as data from open-source and commercial threat feeds. Captured malicious samples are then further validated to confirm that they are malicious in nature. During testing, NSS combines its knowledge of a product's offensive capabilities with these samples.

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 type of threat (malware, exploits, blended threats, and evasions) contains unique infection vectors. This test aims to determine how effectively the AEP product can protect against a threat, regardless of the infection vector or method of obfuscation. The term "threat" is used within this report to refer 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:

- Malware
- Exploits
- Blended threats
- Evasions

Each category 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 (on, for example, a web page or a banner advertisement) 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.
- **Email (IMAP4/POP3)**: These are inbound, email-based attacks where the user is deceived into clicking on a malicious link within an email to download and execute malware, or where the user is asked to visit a web page that hosts malicious code in order to be infected via exploit.

False Positives

The ability of the AEP product to correctly identify and allow benign content is as important as its ability to provide protection against malicious content. As part of initial setup and tuning, NSS ran various samples of legitimate application traffic, files, and documents, all of which the product was required to properly identify and allow. If any legitimate traffic was not allowed, this was recorded as a false positive. Figure 2 depicts the false positive results of the Traps after initial tuning.

Product	False Positive Rate
Palo Alto Networks Traps v4.1	0.0%

Figure 2 – False Positive Rate

Malware

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

- HTTP
- Email (IMAP4/POP3)
- Offline threats
- Docs and scripts
- Unknown threats

Malware Delivered Using HTTP

Figure 3 depicts test results for malware delivered using HTTP. During the test, the Traps's block rate for malware delivered over HTTP was 99.6%, and its additional detection rate was 0.0%.

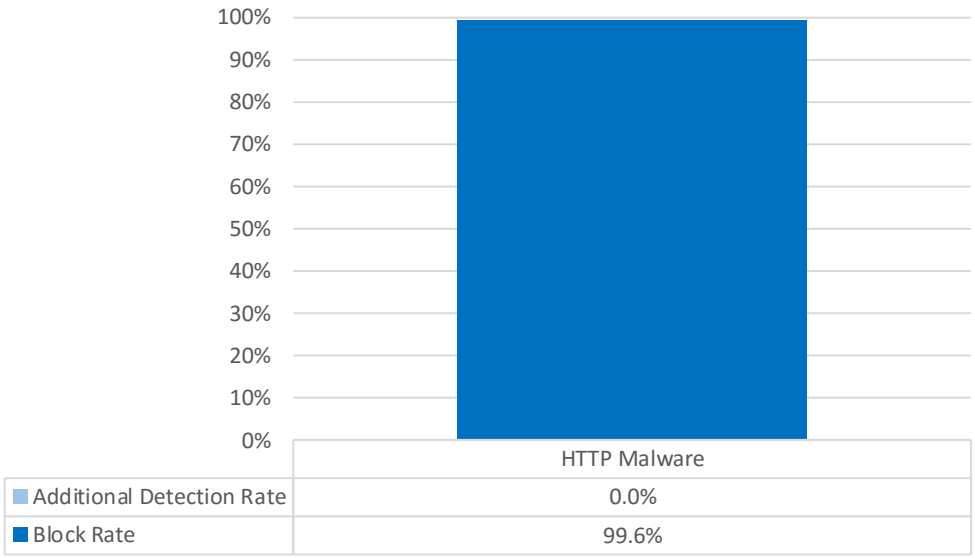

Figure 3 – Malware Delivered by HTTP

Malware Delivered Using Email

Figure 4 depicts test results for malware delivered using email (IMAP4/POP3) as its transport mechanism (e.g., a malicious email attachment). During the test, the Traps's block rate for malware delivered over email was 99.4%, and its additional detection rate was 0.0%.

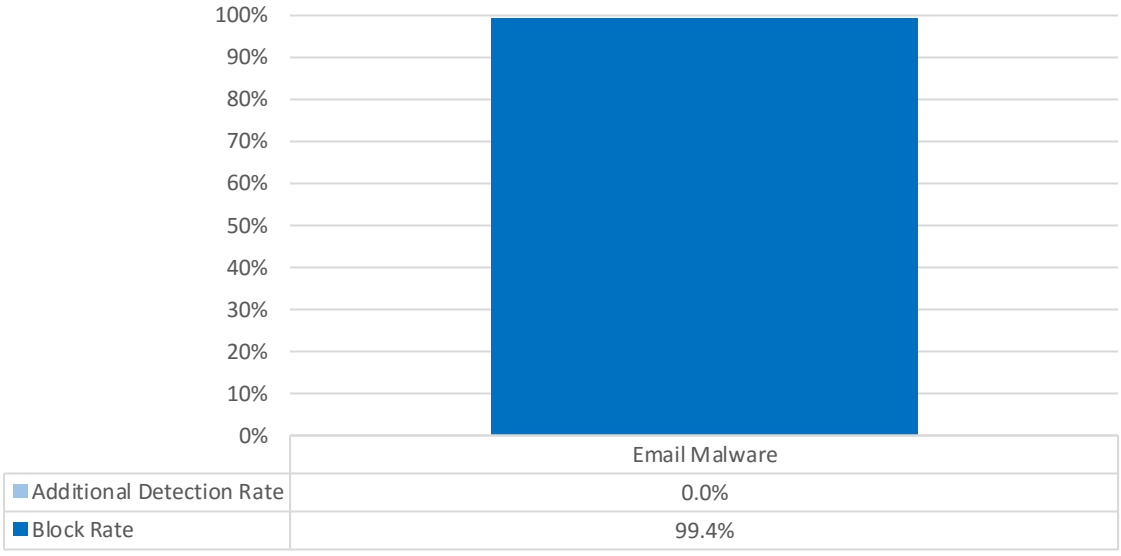

Figure 4 – Malware Delivered by Email

Malware Delivered via Docs and Scripts

Figure 5 depicts test results for malware delivered via docs and scripts. During the test, the Traps's block rate for malware delivered via docs and scripts was 100.0%, and its additional detection rate was 0.0%.

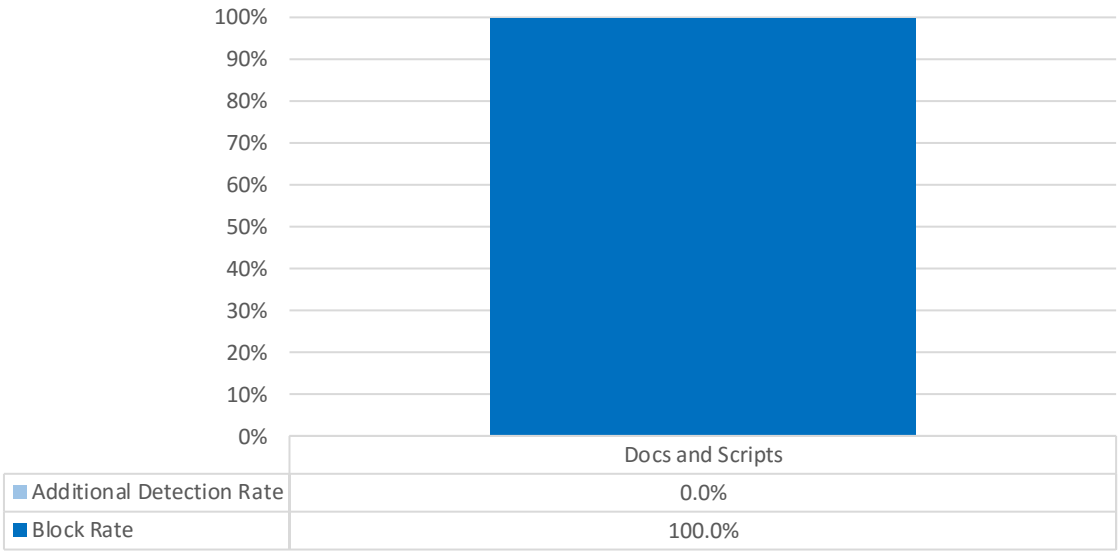

Figure 5 – Malware Delivered via Docs and Scripts

Malware Delivered via Offline Mechanism

Figure 6 depicts test results for malware delivered via an offline mechanism. During the test, the Traps's block rate for malware delivered via an offline mechanism was 92.3%, and its additional detection rate was 0.0%.

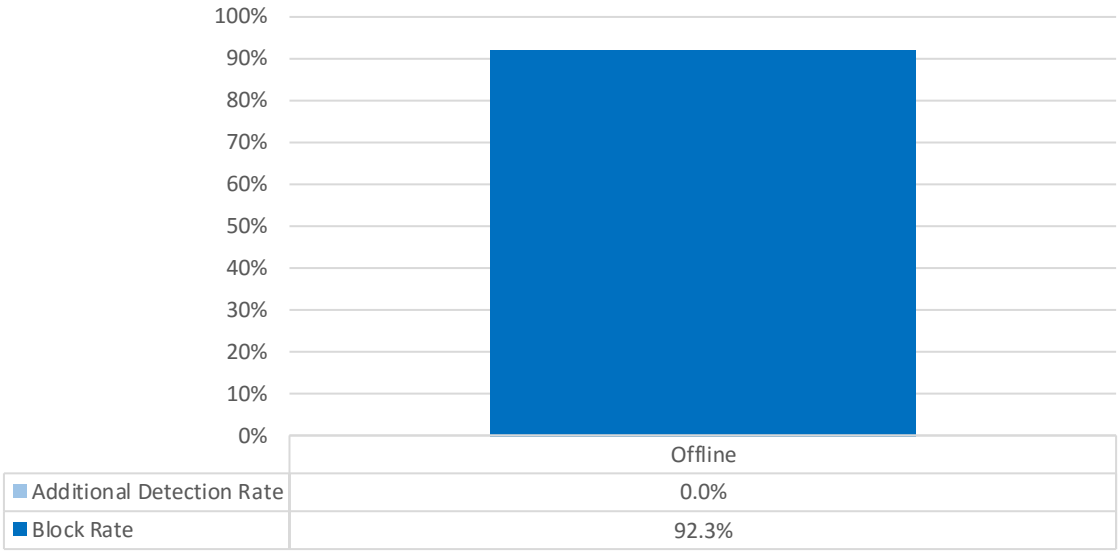

Figure 6 – Malware Delivered via Offline Mechanism

Unknown Threats

Figure 7 depicts test results for previously unknown malware introduced into the environment. During the test, the Traps's block rate for previously unknown threats was 83.3%, and its additional detection rate was 0.0%.

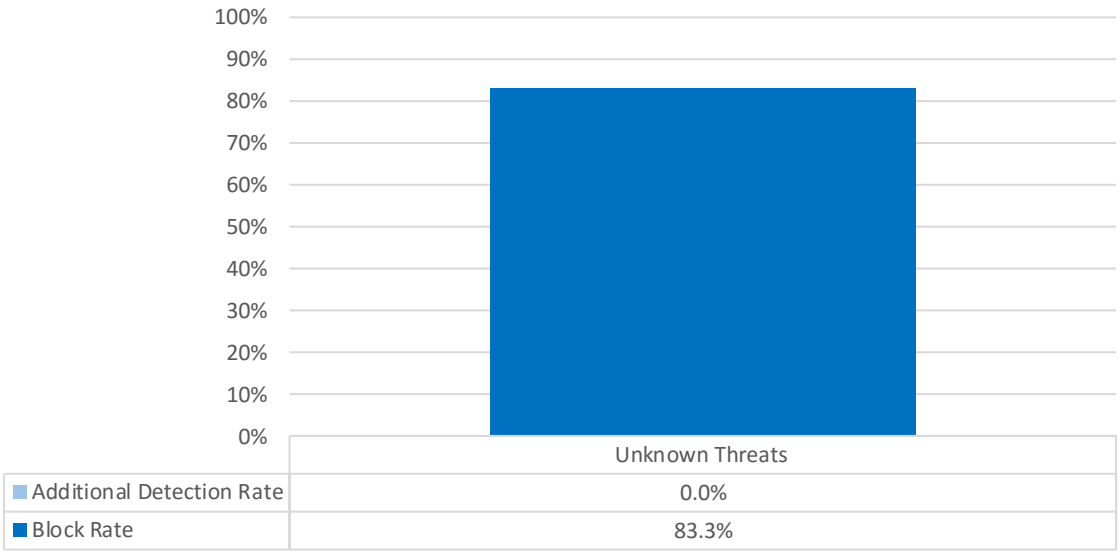

Figure 7 –Unknown Threats

Exploits

Figure 8 depicts the results of exploits testing for the Traps. Exploits are defined as malicious software designed to take advantage of existing deficiencies, such as vulnerabilities or bugs, in hardware or software systems. During the test, the Traps's block rate for exploits was 100%, and its additional detection rate was 0%.

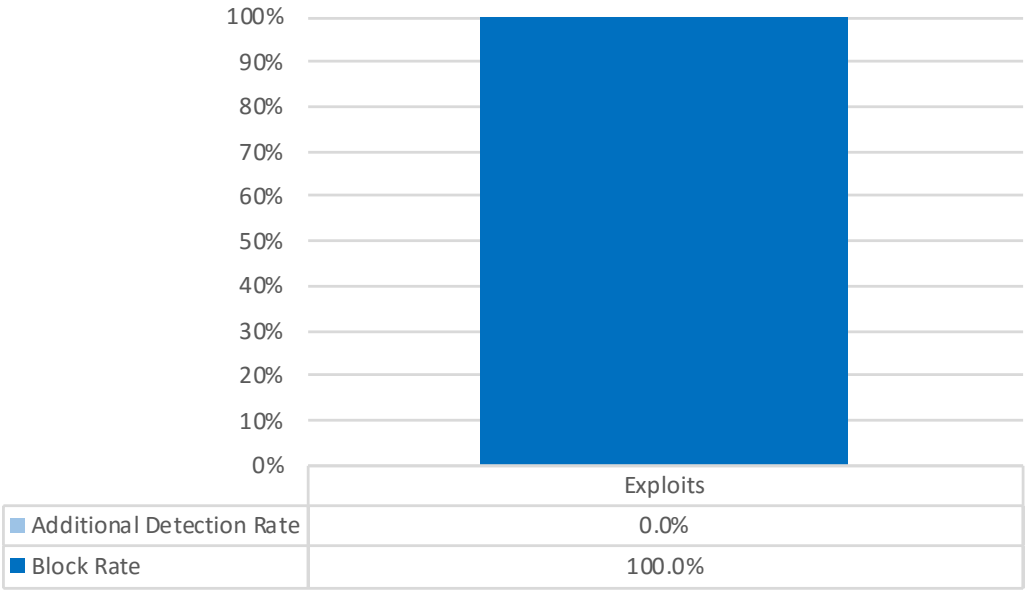

Figure 8 – Exploits

Blended Threats

Figure 9 depicts the results of blended threats testing for the Traps. These threats possess the characteristics of both exploits and socially engineered malware. These threats attempt to make it difficult to distinguish between what is malicious and what is legitimate activity. They are executed by backdooring commonly used system administration tools such as PuTTy, or by executing remote commands using day-to-day sysadmin tools such as PsExec. Enterprises expect AEP products to be able to address this type of threat.

During the test, the Traps's block rate for blended threats was 36.4%, and its additional detection rate was 0.0%.

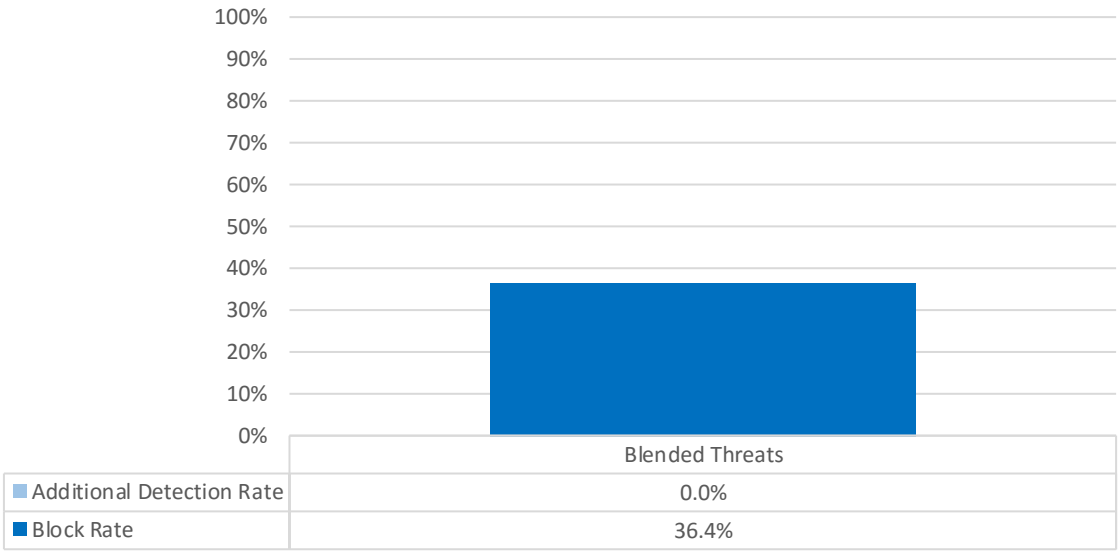

Figure 9 – Blended Threats

Resistance to Evasion Techniques

Figure 10 depicts the results of evasions testing for the Traps. 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 product would normally detect. Attackers can modify attacks and malicious code in order to evade detection in a number of ways.

In this test, 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 common evasion techniques. Please contact NSS for information on the evasions utilized.

During the test, the Traps's block rate for evasion techniques was 100.0%, and its additional detection rate was 0.0%.

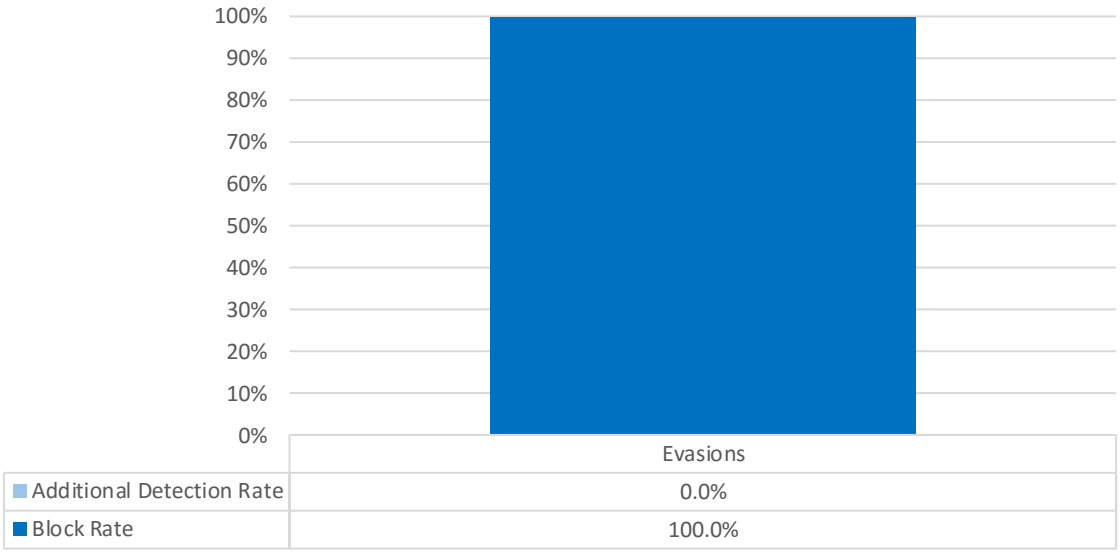

Figure 10 – Resistance to Evasions

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 of its components and any application/service that is leveraged 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 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 on alerts and other threat information generated by the product during testing
- Upkeep – The time required to apply periodic updates and patches from vendors, including software updates

Calculating the Total Cost of Ownership (TCO)

Calculations are based on vendor-provided pricing information. 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 500 software agents only; costs for central management solutions (CMS) may be extra.

Product	Year 1 Cost	Year 2 Cost	Year 3 Cost	3-Year TCO
Palo Alto Networks Traps v4.1	$36,000	$0	$0	$36,000

Figure 11 –3-Year TCO (US$)

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

Appendix A: Product Scorecard

Test Results		
False Positives (detection accuracy)	0.0%	
Malware (various delivery mechanisms)	Block Rate	Additional Detection Rate
HTTP	99.6%	0.0%
Email	99.4%	0.0%
Docs and Scripts	100.0%	0.0%
Offline Threats	92.3%	0.0%
Unknown Threats	83.3%	0.0%
Exploits	100.0%	0.0%
Blended Threats	36.4%	0.0%
Evasions	100.0%	0.0%

Figure 12 – Scorecard

Test Methodology

NSS Labs Advanced Endpoint Protection (AEP) Test Methodology v2.0

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

Contact Information

NSS Labs, Inc.
3711 South MoPac Expressway
Suite 400
Austin, TX 78735 USA
info@nsslabs.com
www.nsslabs.com