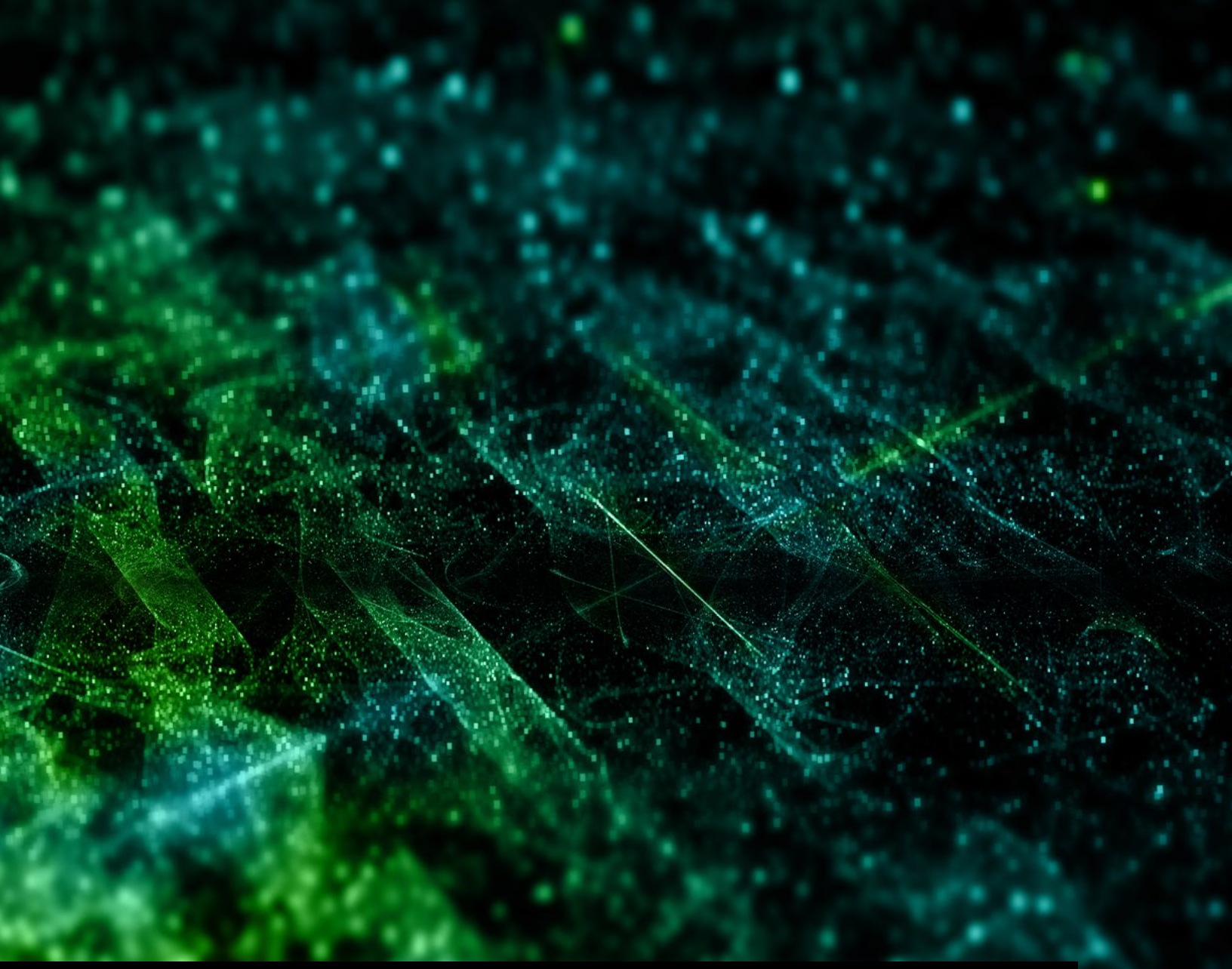

Advanced Endpoint Protection Comparative Report

NSS Labs' Summary of Tests for CylancePROTECT®

CYLANCE™

In February 2017, 14 enterprise anti-malware products were evaluated in NSS Labs' Advanced Endpoint Protection Comparative Report, a non-commissioned test. Products ranged from traditional AV products to a majority of the next-generation vendors.

The aim of this test was to verify that CylancePROTECT is capable of detecting, preventing, and continuously logging threats accurately prior to, during, and after execution while remaining resistant to false positives.

In addition to exceptionally high marks for efficacy, CylancePROTECT was also recognized as a leader in total cost of ownership (TCO) for value in efficacy, ease of management, and the least intensive operational burden across the products tested. In all, CylancePROTECT achieved 99.69% effectiveness and achieved 100% scores across the categories of exploit prevention, blended threats (exploits + social engineering), local intelligence (the endpoint has no cloud or network connection), P2P applications exploitation, and HTTPS attacks.

Product						Security Effectiveness[1]	
CylancePROTECT v1.2.1410						99.69%	
HTTP	HTTPS	Email	P2P Applications	Local Intelligence	Blended Threats	Exploits	Various Evasions
98.0%	100.0%	99.8%	100.0%	100.0%	100.0%	100.0%	87.5%

Figure 1 – NSS Labs' 2017 Security Value Map™ for Advanced Endpoint Protection CylancePROTECT detail

Security Effectiveness

The aim of this test was to verify that each advanced endpoint product (AEP) was capable of detecting, preventing, and continuously logging threats accurately, while remaining resistant to false positives. The tests utilized real threats and attack methods that existed at the time in the wild and that were being used by cybercriminals and other threat actors, based on attacks collected from NSS Labs' global threat intelligence network.

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

- Malware
- Exploits
- Blended threats

Each type of threat was 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.

Security Effectiveness		99.69%	
False Positives (detection accuracy)		0.0%	
Malware	Block Rate	Additional Detection Rate	Security Effectiveness
HTTP	98.0%	0.0%	98.0%
HTTPS	100.0%	0.0%	100.0%
Email (IMAP4/POP3)	99.8%	0.0%	99.8%
P2P Applications	100.0%	0.0%	100.0%
Local IntelligenceEvaluation	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	87.5%	0.0%	87.5%

Figure 2 – NSS Labs' 2017 Security Value Map for Advanced Endpoint Protection CylancePROTECT Security Effectiveness Scorecard

A few elements we believe are worthy of particular note:

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. Over the course of the test, CylancePROTECT blocked 100.0% of attacks.

Exploits Evaluation

Exploits 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, CylancePROTECT blocked 100.0% of exploits.

Blended Threats Evaluation

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. Over the course of the test, CylancePROTECT blocked 100.0% of 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.

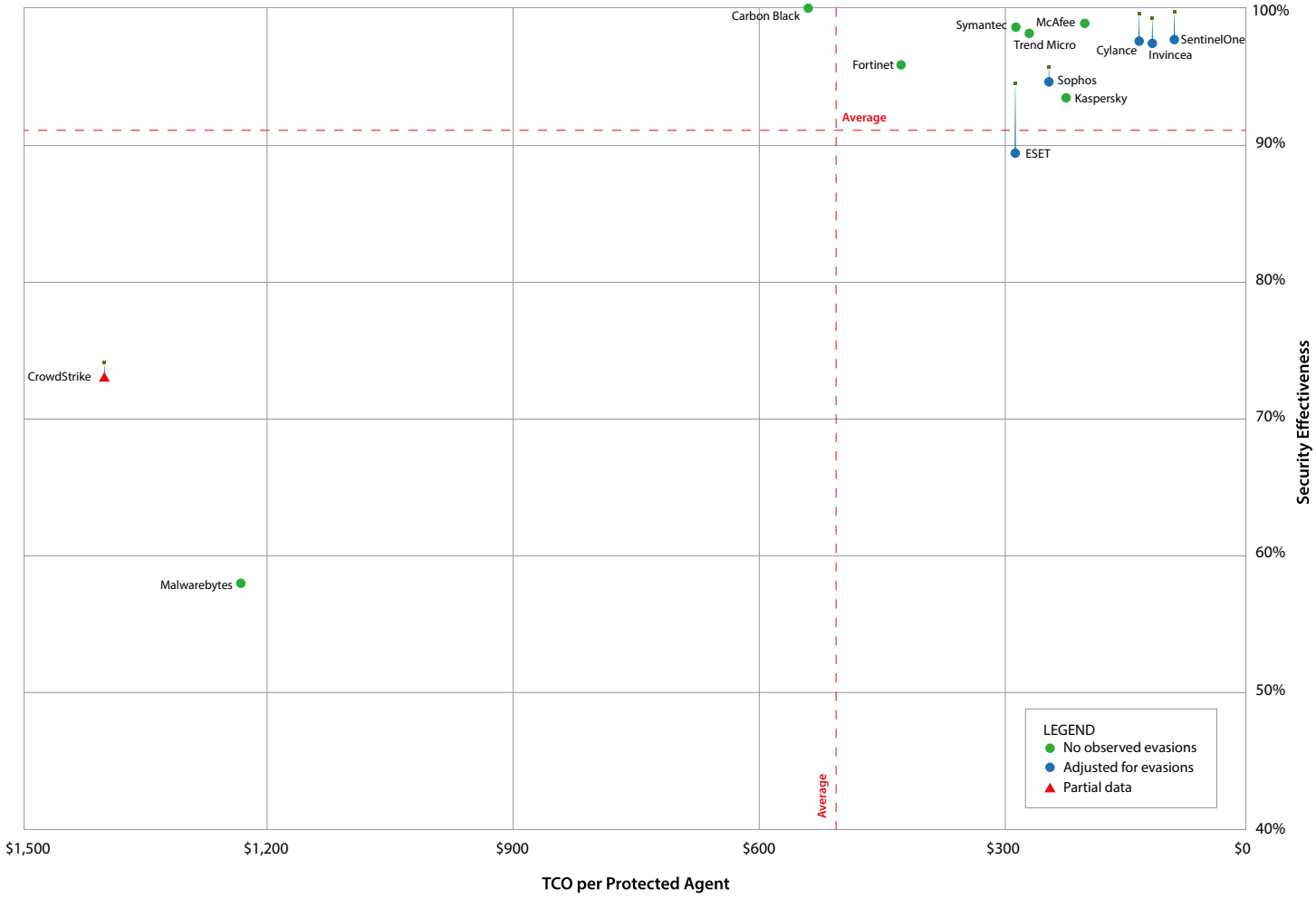

Figure 3 – NSS Labs' 2017 Security Value Map for Advanced Endpoint Protection

NSS Labs evaluated whether the AEP products were capable of detecting, preventing, and continuously monitoring threats and whether they could take action against malware, exploits, and blended threats when subjected to various common evasion techniques. Cylance has addressed the evasions identified by NSS Labs, and is no longer vulnerable to the evasion techniques discovered by NSS Labs.

The empirical data from the individual test reports and comparative reports is used to create NSS Labs' unique Security Value Map (SVM). The SVM illustrates the relative value of a security investment by mapping the security effectiveness and the TCO per protected agent (value) of tested product configurations. The SVM provides an aggregated view of the detailed findings from NSS Labs' group tests. Cylance is listed in the far upper right of the SVM, demonstrating exceptional security effectiveness and TCO.

For more information:

- Check out the full CylancePROTECT report here
- Review the individual test reports for each vendor evaluated at www.nsslabs.com
- Make sure you also don't miss the chance to review our 2017 AV-TEST Advanced Threat Prevention Test Results

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612