ADVANCED ENDPOINT PROTECTION COMPARATIVE REPORT

Security

FEBRUARY 21, 2017

Authors – Thomas Skybakmoen, Morgan Dhanraj

Tested Products

Carbon Black Cb Protection v7.2.3.3106[1]

CrowdStrike Falcon Host[2]

CylancePROTECT v1.2.1410

ESET Endpoint Security v6.4.2014.0

Fortinet FortiClient v5.4.1.0840

X by Invincea v4.2.0-387

Kaspersky Endpoint Security 10

Malwarebytes Endpoint Security v1.7.4.0000

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] Carbon Black's 100% security score is a result of its whitelisting technology. While this is an excellent security score, enterprises must factor in the ongoing operational overhead that accompanies whitelisting, which means it may not be appropriate for all deployments. As seen in NSS' Security Value Map™, Carbon Black has a higher than average total cost of ownership (TCO). For additional information, please see the TCO Comparative Report.

[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.

Overview

Implementation of advanced endpoint protection (AEP) products can be a complex process, with multiple factors affecting the overall *Security Effectiveness* of the system. The following factors should be considered while evaluating the useful life of the AEP product:

- Blocking capabilities
- Detection capabilities
- Anti-evasion capabilities (resistance to common evasion technique)

In order to determine the relative *Security Effectiveness* of AEP products on the market and to facilitate accurate product comparisons, NSS Labs has developed a unique metric:

Security Effectiveness = *(Block Rate +* Additional Detection Rate[3]) *- Evasions*

Figure 1 – Security Effectiveness Formula

By focusing on *Security Effectiveness* as a whole instead of on block rate alone, NSS is able to factor in the ease with which defenses can be bypassed. 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 2 presents the overall results of the tests.

Product	Block Rate	Additional Detection Rate	Total Coverage	Evasion Rating	Security Effectiveness
Carbon Black[1]	100.0%	0.0%	100.0%	100.0%	100.0%
CrowdStrike[2]	39.5%	34.7%	74.2%	99.0%	73.2%
Cylance	99.7%	0.0%	99.7%	98.0%	97.7%
ESET	93.5%	1.0%	94.5%	95.0%	89.5%
Fortinet	75.9%	20.0%	95.9%	100.0%	95.9%
Invincea	93.4%	6.1%	99.5%	98.0%	97.5%
Kaspersky	93.6%	0.0%	93.6%	100.0%	93.6%
Malwarebytes	56.2%	1.7%	57.9%	100.0%	57.9%
McAfee	99.0%	0.0%	99.0%	100.0%	99.0%
SentinelOne	99.8%	0.0%	99.8%	98.0%	97.8%
Sophos	95.7%	0.0%	95.7%	99.0%	94.7%
Symantec	93.6%	5.1%	98.7%	100.0%	98.7%
Trend Micro	86.7%	11.6%	98.3%	100.0%	98.3%

Figure 2 – Security Effectiveness

[1] Carbon Black's 100% security score is a result of its whitelisting technology. While this is an excellent security score, enterprises must factor in the ongoing operational overhead that accompanies whitelisting, which means it may not be appropriate for all deployments. As seen in NSS' Security Value Map™, Carbon Black has a higher than average total cost of ownership (TCO). For additional information, please see the TCO Comparative Report.

[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.

[3] Block Rate and additional detection rate are defined as the number of exploits and malware blocked and detected under test within the 2-hour window.

Table of Contents

Tested Products 1

Environment 1

Overview 2

Analysis 4

Block Rate 4
Additional Detection Rate 4
Scoring 4
False Positives 4
Malware Delivered by HTTP 5
Malware Delivered over HTTPS 5
Malware Delivered over Email 6
Malware Delivered by P2P 6
Local Intelligence Evaluation 7
Exploits 7
Blended Threats 8
Resistance to Evasion Techniques 9

Security Effectiveness 10

Test Methodology 11

Contact Information 11

Table of Figures

Figure 1 – Security Effectiveness Formula 2
Figure 2 – Security Effectiveness 2
Figure 3 – Malware Delivered by HTTP 5
Figure 4 – Malware Delivered over HTTPS 5
Figure 5 — Malware Delivered over Email 6
Figure 6 – Malware Delivered by P2P 6
Figure 7 — Local Intelligence Evaluation 7
Figure 8 — Exploits 7
Figure 9 — Blended Threats 8
Figure 10 – Evasion Resistance 9
Figure 11 – Security Effectiveness 10

Analysis

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

Block Rate

The block rate measured 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 measured a product's ability to detect the threats the product was not able to block.

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.

Scoring

As response time is critical in halting the damage caused by malware infections, the AEP product should be able to detect known samples, or analyze unknown samples, and report on them within 2 hours of initial infection and command and control (C&C) callback. Any product that did not block or detect (log) an attack, infection, or C&C callback within the detection window did not receive credit for the detection.

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 applications and traffic, which were expected to be properly identified and allowed by each product. If any product had not allowed legitimate traffic, NSS would have measured this as a false positive alert. Please see the individual Test Reports at www.nsslabs.com for more information.

Malware Delivered by HTTP

Figure 3 displays each product's combined block and detection score for malware that uses the HTTP protocol as its transport mechanism, i.e., malware delivered through a web browser.

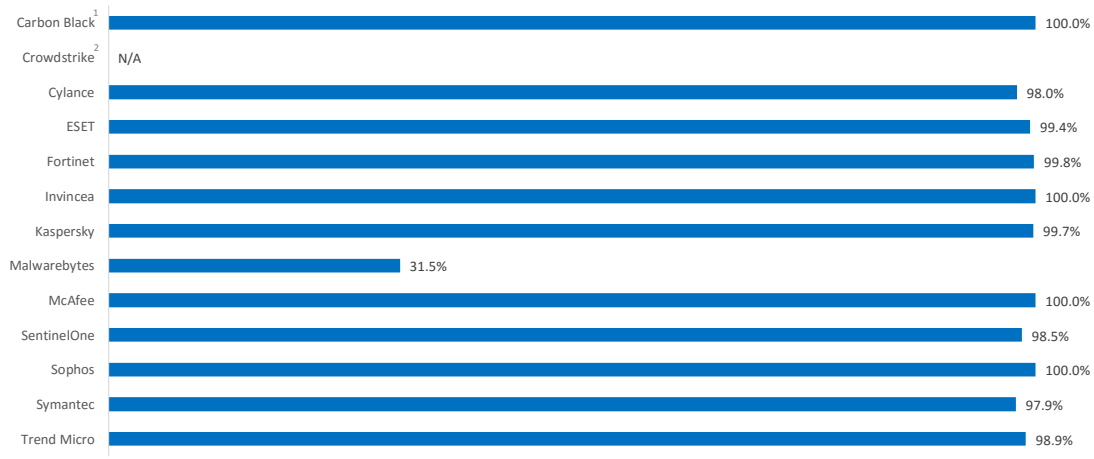

Figure 3 – Malware Delivered by HTTP

Malware Delivered over HTTPS

Figure 4 displays each product's combined block and detection score for malware that uses the HTTPS protocol as its transport mechanism, i.e., malware delivered through a web browser over TLS-encrypted channels.

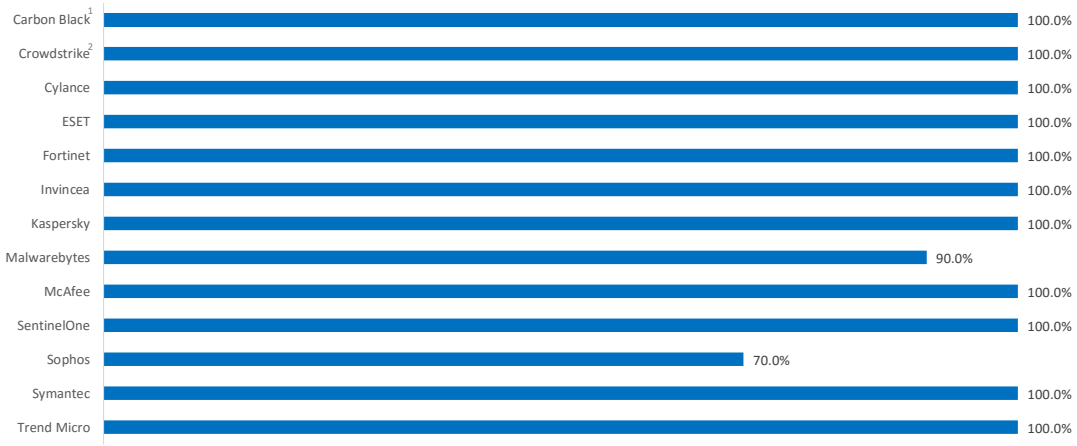

Figure 4 – Malware Delivered over HTTPS

[1] Carbon Black's 100% security score is a result of its whitelisting technology. While this is an excellent security score, enterprises must factor in the ongoing operational overhead that accompanies whitelisting, which means it may not be appropriate for all deployments. As seen in NSS' Security Value Map™, Carbon Black has a higher than average total cost of ownership (TCO). For additional information, please see the TCO Comparative Report.

[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.

Malware Delivered over Email

Figure 5 displays each product's combined block and detection score for malware that uses email (IMAP4/POP3) as a transport mechanism, such as a malicious email attachment.

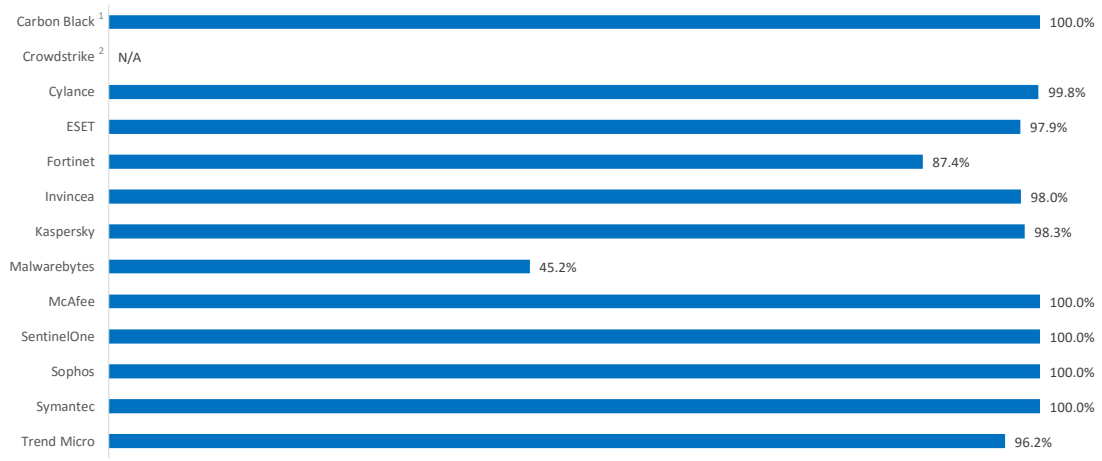

Figure 5 — Malware Delivered over Email

Malware Delivered by P2P

Figure 6 displays each product's combined block and detection score formalware that uses the P2P protocol as its transport mechanism.

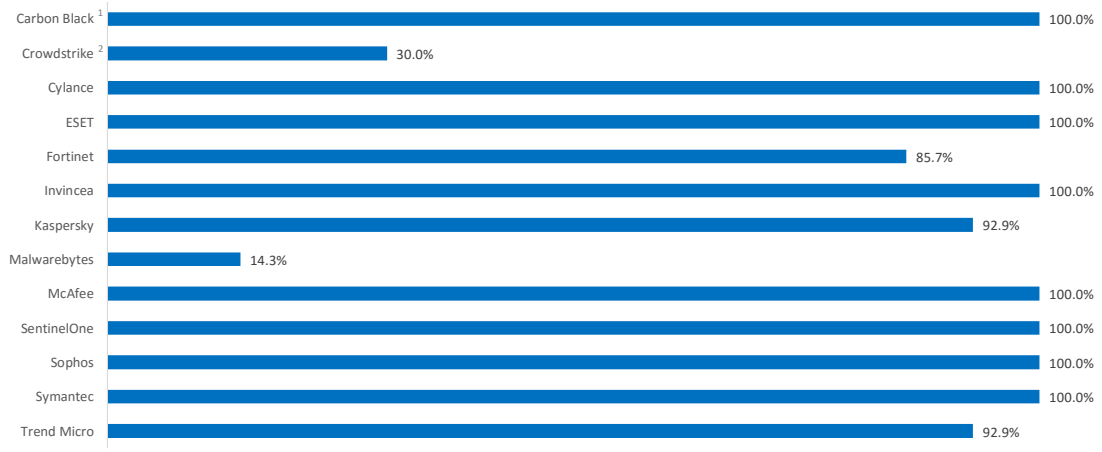

Figure 6 – Malware Delivered by P2P

[1] Carbon Black's 100% security score is a result of its whitelisting technology. While this is an excellent security score, enterprises must factor in the ongoing operational overhead that accompanies whitelisting, which means it may not be appropriate for all deployments. As seen in NSS' Security Value Map™, Carbon Black has a higher than average total cost of ownership (TCO). For additional information, please see the TCO Comparative Report.

[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.

Local Intelligence Evaluation

Figure 7 displays each product's combined block and detection score for malware that uses the local Intelligence vector as its transport mechanism. Hosts that have zero cloud connectivity may be infected outside the corporate network with or without an endpoint product installed.

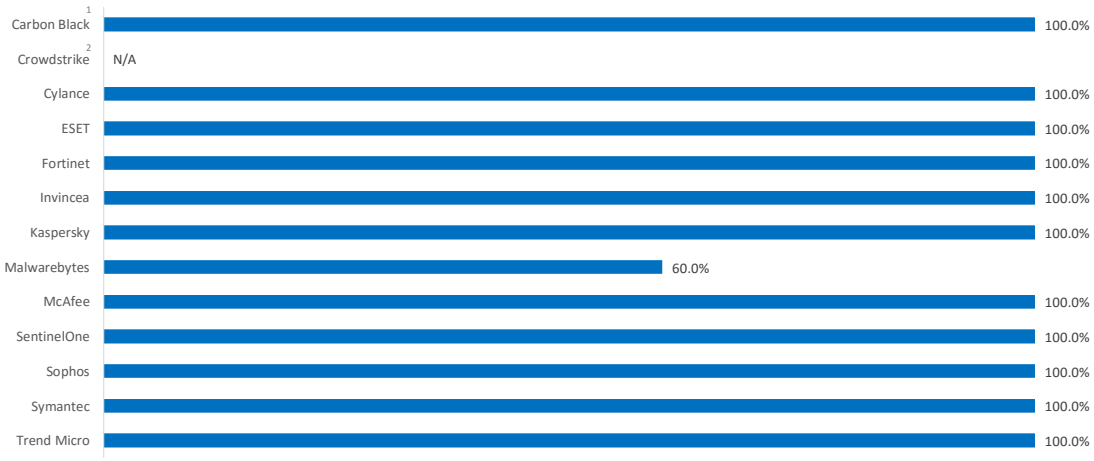

Figure 7 — Local Intelligence Evaluation

Exploits

Exploits are defined as malicious software that is designed to take advantage of existing deficiencies in hardware or software systems, such as vulnerabilities or bugs. Figure 8 displays each product's combined block and detection score for exploits.

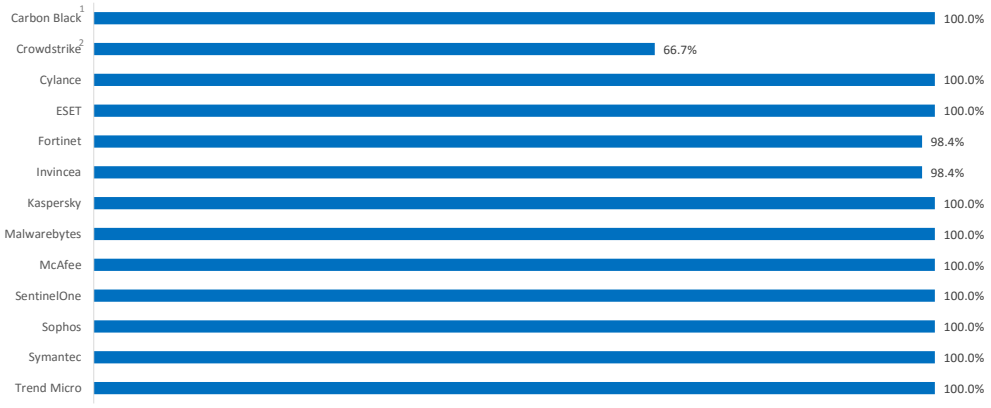

Figure 8 — Exploits

[1] Carbon Black's 100% security score is a result of its whitelisting technology. While this is an excellent security score, enterprises must factor in the ongoing operational overhead that accompanies whitelisting, which means it may not be appropriate for all deployments. As seen in NSS' Security Value Map™, Carbon Black has a higher than average total cost of ownership (TCO). For additional information, please see the TCO Comparative Report.

[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.

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. Examples of blended threats include, but are not limited to, unknown threats, ransomware, kernel-mode exploits, chained exploits, rootkits, and Trojans.

Figure 9 displays each product's combined block and detection score for blended threats.

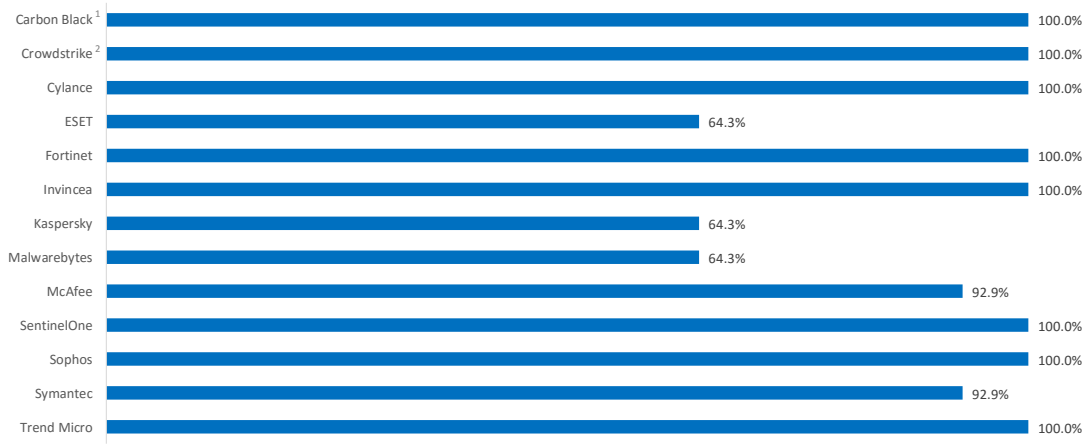

Figure 9 — Blended Threats

[1] Carbon Black's 100% security score is a result of its whitelisting technology. While this is an excellent security score, enterprises must factor in the ongoing operational overhead that accompanies whitelisting, which means it may not be appropriate for all deployments. As seen in NSS' Security Value Map™, Carbon Black has a higher than average total cost of ownership (TCO). For additional information, please see the TCO Comparative Report.

[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.

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 otherwise normally detect. Attackers can and do 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. Products that missed one or more evasion per category were given a one percent reduction per category.

Figure 10 provides evasion resistance scores for each of the tested products.

Product	Final Evasion Score
Carbon Black[1]	100%
CrowdStrike[2]	99%
Cylance	98%
ESET	95%
Fortinet	100%
Invincea	98%
Kaspersky	100%
Malwarebytes	100%
McAfee	100%
SentinelOne	98%
Sophos	99%
Symantec	100%

Figure 10 – Evasion Resistance

[1] Carbon Black's 100% security score is a result of its whitelisting technology. While this is an excellent security score, enterprises must factor in the ongoing operational overhead that accompanies whitelisting, which means it may not be appropriate for all deployments. As seen in NSS' Security Value Map™, Carbon Black has a higher than average total cost of ownership (TCO). For additional information, please see the TCO Comparative Report.

[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.

Security Effectiveness

The *Security Effectiveness* of a product is determined by factoring the results of evasions testing into the detection rate.

Product	Block Rate	Additional Detection Rate	Total Coverage	Evasion Rating	Security Effectiveness
Carbon Black[1]	100.0%	0.0%	100.0%	100.0%	100.0%
CrowdStrike[2]	39.5%	34.7%	74.2%	99.0%	73.2%
Cylance	99.7%	0.0%	99.7%	98.0%	97.7%
ESET	93.5%	1.0%	94.5%	95.0%	89.5%
Fortinet	75.9%	20.0%	95.9%	100.0%	95.9%
Invincea	93.4%	6.1%	99.5%	98.0%	97.5%
Kaspersky	93.6%	0.0%	93.6%	100.0%	93.6%
Malwarebytes	56.2%	1.7%	57.9%	100.0%	57.9%
McAfee	99.0%	0.0%	99.0%	100.0%	99.0%
SentinelOne	99.8%	0.0%	99.8%	98.0%	97.8%
Sophos	95.7%	0.0%	95.7%	99.0%	94.7%
Symantec	93.6%	5.1%	98.7%	100.0%	98.7%
Trend Micro	86.7%	11.6%	98.3%	100.0%	98.3%

Figure 11 – Security Effectiveness

[1] Carbon Black's 100% security score is a result of its whitelisting technology. While this is an excellent security score, enterprises must factor in the ongoing operational overhead that accompanies whitelisting, which means it may not be appropriate for all deployments. As seen in NSS' Security Value Map™, Carbon Black has a higher than average total cost of ownership (TCO). For additional information, please see the TCO Comparative Report.

[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.

Test Methodology

Advanced Endpoint Protection 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