BREACH DETECTION SYSTEM TEST REPORT

Cisco Advanced Malware Protection v5.2.2015072320

Authors – Dipti Ghimire, Bhaarath Venkateswaran, Ahmed Garhy, Mohamed Saher

Overview

NSS Labs performed an independent test of the Cisco Advanced Malware Protection v5.2.2015072320. The product was subjected to thorough testing at the NSS facility in Austin, Texas, based on the Breach Detection System (BDS) Methodology v2.0 available at www.nsslabs.com. This test was conducted free of charge and NSS did not receive any compensation in return for participation.

While the companion comparative reports on security, performance, and total cost of ownership (TCO) will provide information about all tested products, this individual test report provides detailed information not available elsewhere.

As part of the initial BDS test setup, devices are tuned as deemed necessary by the vendor. Every effort is made to ensure the optimal combination of *Security Effectiveness* and performance, as would be the aim of a typical customer deploying the device in a live network environment. Figure 1 presents the overall results of the tests.

Product				Detection Rate[1]	NSS-Tested Throughput
Cisco Advanced Malware Protection v5.2.2015072320				99.2%	1,000 Mbps
HTTP Malware	**Email Malware**	**SMB Malware**	**Drive-by Exploits**	**Social Exploits**	**Evasions**
100%	100%	100%	96.7%	100.0%	100.0%

Figure 1 – Overall Test Results

The Cisco Advanced Malware Protection v5.2.2015072320 received an overall detection rating of 99.2%. The Advanced Malware Protection proved effective against all evasion techniques tested. The solution also passed all stability and reliability tests.

The solution was tested and rated by NSS at 1,000 Mbps. *NSS-Tested Throughput* is calculated as an average of the "real-world" protocol mixes (Enterprise Perimeter and Education), and the 21 KB HTTP response-based tests.

[1] Detection rate is defined as the average percentage of malware and exploits detected under test.

Table of Contents

Table of Figures

Security Effectiveness

This section aims to verify that the product can detect and log breaches and attempted breaches accurately. All tests in this section are completed with no background network load.

This test utilizes threats and attack methods that exist in the wild and are currently being used by cybercriminals and other threat actors, based on attacks collected from NSS' global threat intelligence network. For details on live testing, refer to the Security Stack Methodology v1.5.[2]

The ability of the product to detect and report 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.

As response time is critical in halting the damage caused by malware infections, the system under test (SUT) should be able to detect known samples, or analyze unknown samples, and report on them within 48 hours of initial infection and command and control (C&C) callback. Any SUT that does not alert on an attack, infection, or C&C callback within the detection window will not receive credit for the detection.

The following use cases may be examined to determine if the SUT can identify a security risk within each scenario.

- **Web-based malware attacks that rely on social engineering** – The user is deceived into clicking a malicious link to download and execute malware.
- **Web-based exploits** – Also known as "drive-by downloads," these occur when the user is infected merely by visiting a web page that hosts malicious code.
- **Socially engineered malware delivered via non-HTTP traffic** – Malware is delivered by other common means such as email, a cloaked executable (.jpeg, .exe, .zip), FTP, or an infected USB drive.
- **Blended exploits** – Also known as "doc-jacking," these are typically delivered via common documents, such as Microsoft Word documents or Excel spreadsheets, containing exploits. These exploits are typically delivered via network protocols.
- **Offline infections** – Remote users with mobile devices can become infected while outside the protection of the corporate network security. When infected devices are subsequently reattached to the corporate network, the infection can spread.

[2] https://www.nsslabs.com/reports/security-stack-test-methodology-v15

Exploit and Malware Detection

Figure 2 depicts the percentage of malware and exploits detected by Cisco Advanced Malware Protection for each of the delivery mechanisms used in the test:

- **Drive-by and social exploits** – Malicious software that is designed to take advantage of existing deficiencies in hardware or software systems, such as vulnerabilities or bugs
- **HTTP protocol** – Malware using HTTP protocol as its transport mechanism; that is, the malware is downloaded through a web browser
- **SMTP/IMAP** – Malware that uses email (SMTP/IMAP) as its transport mechanism; for example, a malicious email attachment
- **SMB** – Malware that uses the server message block (SMB) protocol as its transport mechanism

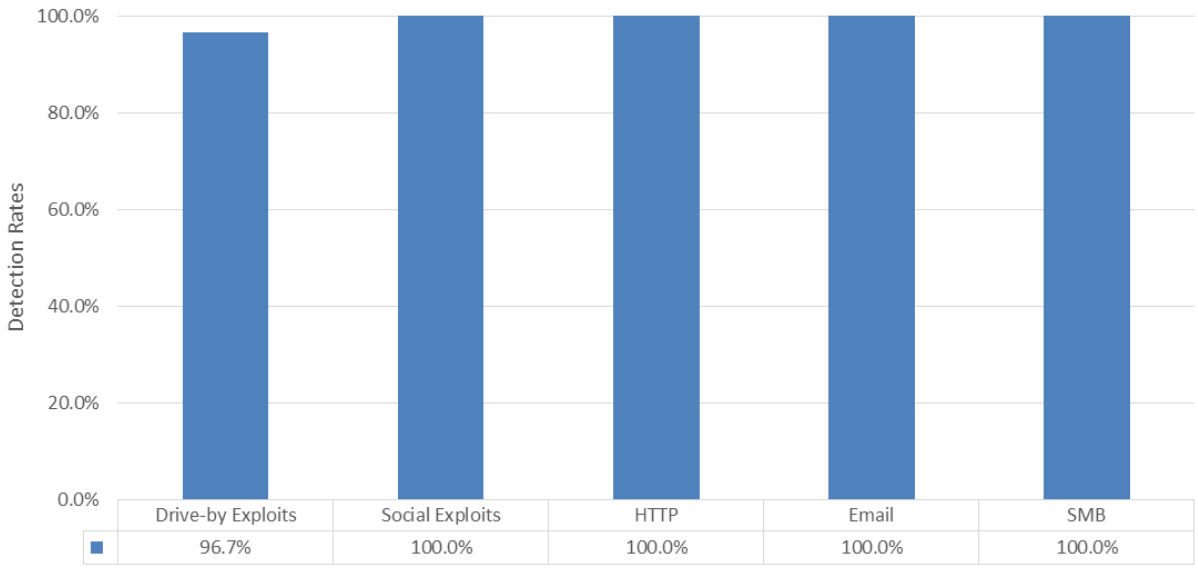

Figure 2 – Exploit and Malware Detection Rates

Resistance to Evasion Techniques

Evasion techniques are a means of disguising and modifying attacks at the point of delivery in order to avoid detection by security products. If a security device fails to correctly identify a specific type of evasion, an attacker could potentially deliver malware that the device normally would detect. Figure 3 provides the results of the evasion tests for Cisco Advanced Malware Protection.

Evasions	Result
Packers	100%
Compressors	100%
Virtual machine	100%
Sandbox	100%
HTML obfuscation	100%
Layered evasions	100%

Figure 3 – Resistance to Evasion Results

Network Device Performance

There is frequently a trade-off between *Security Effectiveness* and performance; a product's *Security Effectiveness* should be evaluated within the context of its performance, and vice versa. This ensures that detection does not adversely impact performance and that no security shortcuts are taken to maintain or improve performance. The NSS performance tests are designed to validate that a network device inspection engine can maintain its detection rate as background traffic increases.

Raw Packet Processing Performance (UDP Traffic)

This section uses UDP packets of varying sizes generated by test equipment. A constant stream of the appropriate packet size — with variable source and destination IP addresses transmitting from a fixed source port to a fixed destination port — is transmitted bidirectionally over the monitored network.

Each packet contains dummy data and is targeted at a valid port on a valid IP address on the target subnet. The percentage load and frames per second (fps) figures across each inline port pair are verified by network monitoring tools before each test begins. Multiple tests are run and averages are taken where necessary.

This traffic does not attempt to simulate any real-world network. No TCP sessions are created during this test, and there is very little for the detection engine to do. However, each vendor will be required to write a signature to detect the test packets in order to ensure that they are being passed through the detection engine and not "fast-tracked" through the network device. The first stage at which one or more attacks is not detected is recorded as the maximum raw packet processing capacity for the network device.

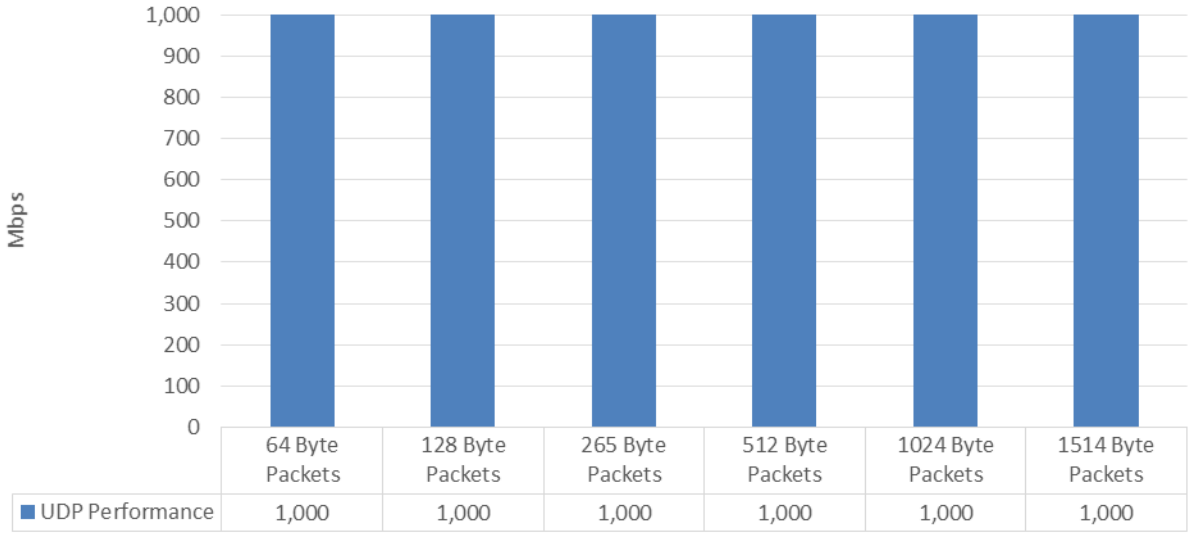

Figure 4 – Raw Packet Processing Performance (UDP Traffic)

Maximum Capacity

The use of automated testing and traffic generation appliances allows NSS engineers to create "real-world," high-speed traffic as the background load for the tests.

These tests aim to stress the network device inspection engine and determine how it copes with high volumes of concurrent transmission control protocol (TCP) open connections and TCP connections per second. All tests in this section are repeated at 25%, 50%, 75%, and 100%[3] of the maximum rated throughput of the SUT. At each stage, multiple instances of malicious traffic are passed and the number detected is logged. The first stage at which one or more attacks is not detected is recorded as the maximum capacity for that response size/traffic mix.

- **Maximum concurrent TCP connections** – This test determines the maximum concurrent TCP connections of the SUT with no data passing across the connections. This type of traffic is not typically found on a normal network, but it provides the means to determine the maximum possible concurrent connections figure. The first stage at which one or more attacks is not detected is recorded as the maximum concurrent TCP open connections.
- **Maximum TCP connections per second** – This test determines the maximum TCP connection rate of the SUT with one byte of data passing across the connections. This type of traffic is not typically found on a normal network, but it provides the means to determine the maximum possible TCP connection rate. The first stage at which one or more attacks is not detected is recorded as the maximum TCP connections.
- **Maximum HTTP connections per second** – This test determines the maximum TCP connection rate of the network device with a 1-byte HTTP response size. The response size defines the number of bytes contained in the body, excluding any bytes associated with the HTTP header. A 1-byte response size is designed to provide a theoretical maximum HTTP connections per second rate. The first stage at which one or more attacks is not detected is recorded as the maximum HTTP connections.

Results for the maximum concurrent TCP connections per second, maximum TCP connections, and maximum HTTP connections per second tests are provided in Figure 5.

[3] The 100% load will actually be less than 100% to allow headroom for malicious traffic.

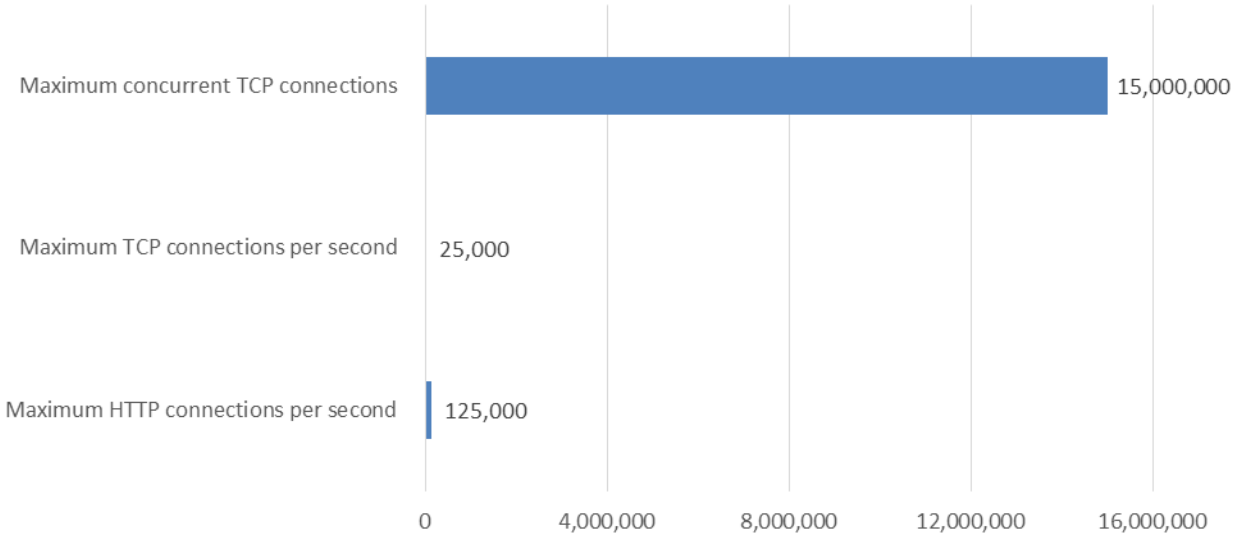

Figure 5 – Maximum Concurrent TCP Connections and Maximum TCP Connections per Second

HTTP Capacity with No Transaction Delays

These tests stress the HTTP detection engine and determine how the SUT copes with network loads of varying average packet size and varying connections per second. By creating genuine session-based traffic with varying session lengths, the SUT is forced to track valid TCP sessions, thus ensuring a higher workload than for simple packet-based background traffic. This provides a test environment that is as close to "real world" as it is possible to achieve in a lab environment, while also ensuring absolute accuracy and repeatability.

Each transaction consists of a single HTTP GET request with no transaction delays (that is, the web server responds immediately to all requests). All packets contain valid payload (a mix of binary and ASCII objects) and address data. This test provides an excellent representation of a live network (albeit one biased toward HTTP traffic) at various network loads.

All tests in this section are repeated at 25%, 50%, 75%, and 100%[4] of the maximum rated throughput of the SUT. At each stage, multiple instances of malicious traffic are passed and the number detected is logged. The first stage at which one or more attacks is not detected is recorded as the maximum HTTP capacity for that response size/traffic mix.

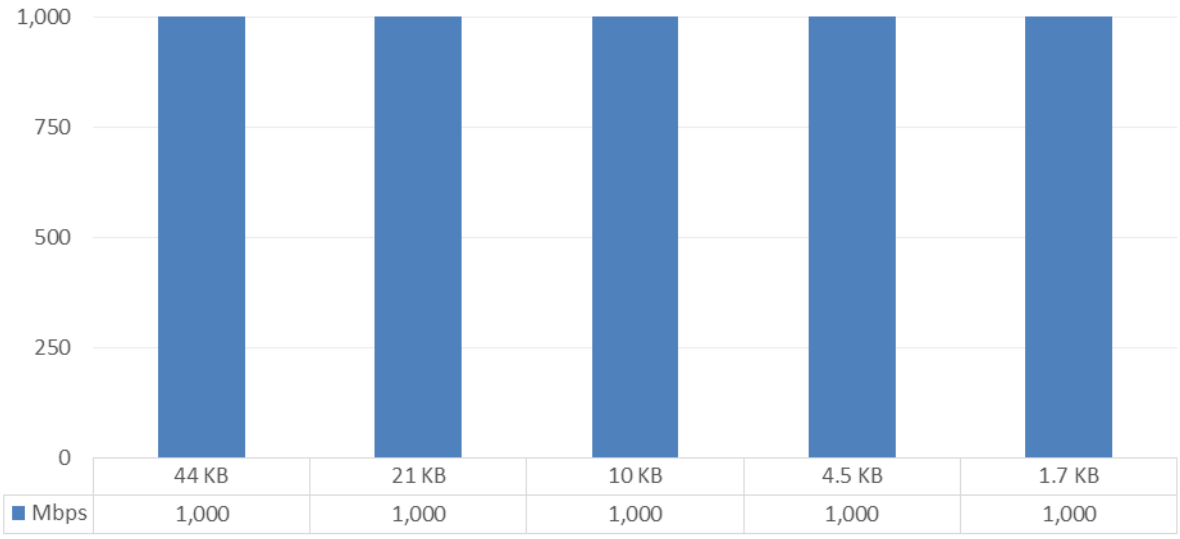

Figure 6 – Detection under Load (HTTP Capacity with No Transaction Delay)

[4] The 100% load will actually be less than 100% to allow headroom for malicious traffic.

HTTP Capacity with Transaction Delays

Typical user behavior introduces delays between requests and reponses; for example, "think time," as users read web pages and decide which links to click next. This group of tests is identical to the previous group except that these tests include a five-second delay in the server response for each transaction. This delay has the effect of maintaining a high number of open connections throughout the test, thus forcing the sensor to utilize additional resources to track those connections.

As with the tests that employ HTTP capacity with no transaction delays, tests are repeated at 25%, 50%, 75%, and 100%[5] of the maximum rated throughput of the BDS. In order to highlight any differences in performance, Figure 7 presents the results for HTTP capacity both with and without transaction delays.

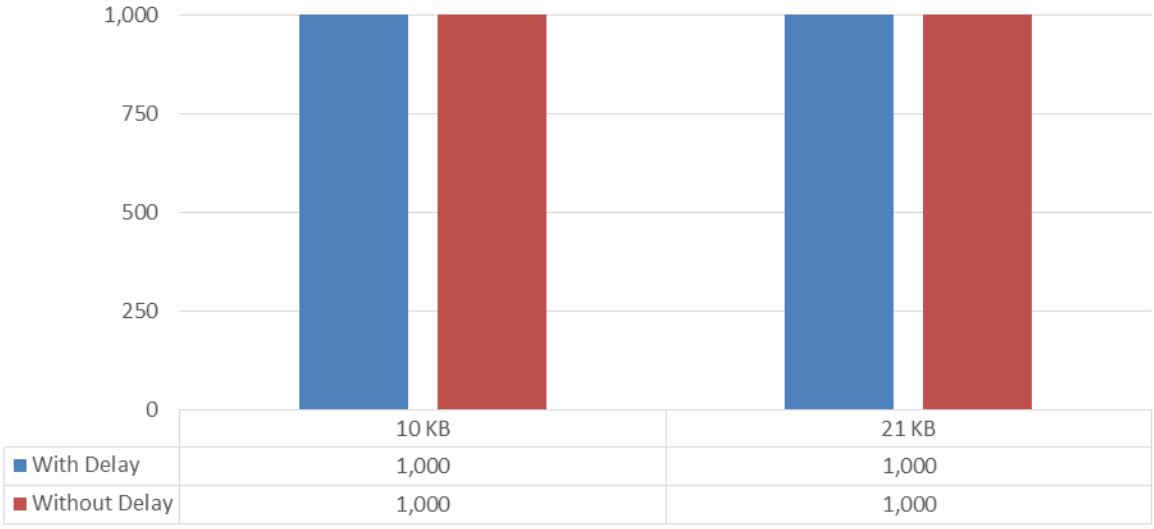

Figure 7 – Detection under Load (HTTP Capacity with Transaction Delay)

[5]The 100% load will actually be less than 100% to allow headroom for malicious traffic.

"Real-World" Traffic Mixes

This test measures the performance of the network device under test in a "real-world" environment by introducing additional protocols and real content while still maintaining a precisely repeatable and consistent background traffic load. The average result is a background traffic load that is closer to what may be found on a heavily utilized "normal" production network. All tests are repeated at 25%, 50%, 75%, and 100%[6] of the maximum rated throughput of the SUT. At each stage, multiple instances of malicious traffic are passed and the number detected is logged. The first stage at which one or more attacks is not detected is recorded as the maximum rated throughput of the BDS. Results are presented in Figure 8.

The Advanced Malware Protection performed in line with the throughput claimed by the vendor.

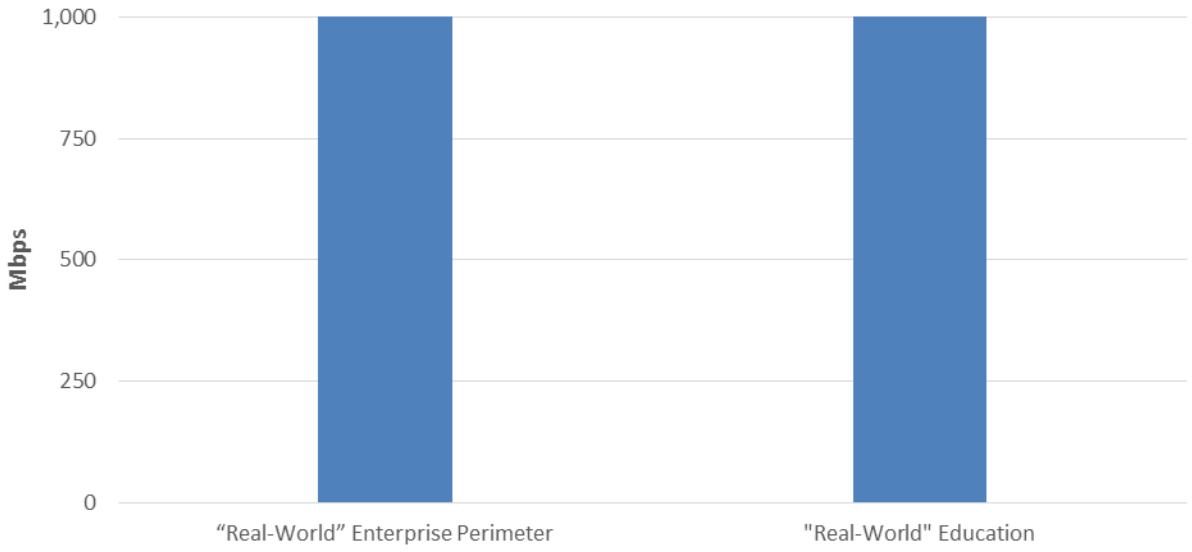

Figure 8 – Detection under Load ("Real World" Traffic)

[6] The 100% load will actually be less than 100% to allow headroom for malicious traffic.

Stability and Reliability

Long-term stability is important, since a failure can result in serious breaches remaining undetected and thus not remediated. These tests verify the stability of a network device, along with its ability to maintain a minimum level of detection while under normal load and while identifying malicious traffic. Products that cannot sustain logging of legitimate traffic or that crash while under hostile attack will not pass.

The Advanced Malware Protection is required to remain operational and stable throughout these tests and to operate at 100% scanning capability, raising an alert each time malicious traffic is detected. If any malicious traffic passes undetected, caused by either the volume of traffic or by the BDS failing for any reason, the product will fail.

Figure 9 presents the results of the stability and reliability tests for the Cisco Advanced Malware Protection.

Stability and Reliability	Result
Detection under extended attack	PASS
Attack detection – normal load	PASS
Protocol fuzzing and mutation – detection ports	PASS
Persistence of data	PASS

Figure 9 – Stability and Reliability Results

Management and Configuration

Security devices are complicated to deploy, and essential components such as centralized management console options, log aggregation, and event correlation/management systems further complicate the purchasing decision.

Understanding key comparison points will allow customers to model the overall impact on network service level agreements (SLAs), estimate operational resource requirements to maintain and manage the systems, and better evaluate the required skill and competencies of staff.

Enterprises should include management and configuration during their evaluation, focusing on the following at minimum:

- **General management and configuration –** How easy is it to install and configure network devices and/or agents, and how easy is it to deploy multiple devices throughout a large enterprise network?
- **Product customization –** How easy is it to create custom configurations, edit them, and deploy them across an enterprise? Configurations may be policies, alert settings, and so on, depending on the product.
- **Alert handling –** How accurate and timely is the alerting, and how easy is it to drill down to locate critical information needed to remediate a security problem?
- **Reporting –** How effective is the reporting capability, and how readily can it be customized?

Total Cost of Ownership (TCO)

Implementation of security solutions can be complex, with several factors affecting the overall cost of deployment, maintenance fees, and upkeep.

The following factors should be considered over the course of the useful life of the solution:

- **Product purchase** – The cost of acquisition.
- **Product maintenance fees** – The recurring fees paid to the vendor (including software and hardware support, maintenance, and other updates).
- **Installation time** – The time required to take the device out of the box, configure it, put it into the network, apply updates and patches, and set up desired logging and reporting.
- **Upkeep** – The time required to apply periodic updates and patches from vendors, including hardware, software, and other updates.
- **Management** – Day-to-day management tasks including device configuration, policy updates, policy deployment, alert handling, and so on.

For the purposes of this report, capital expenditure (capex) items are included for a single product only (the cost of acquisition and installation).

Calculating the Total Cost of Ownership (TCO)

In procuring a BDS solution for the enterprise, it is essential to factor in both bandwidth and the number of users. NSS has found that the malware detection rates of some BDS network devices drop when they operate at maximum capacity. NSS research has shown that, in general, enterprise network administrators architect their networks for up to 2 Mbps per employee of sustained throughput. Consequently, an enterprise must deploy 500 agents and/or one network device of 1,000 Mbps capacity to support 500 users.

Users	Mbps per User	Network Device Throughput	Centralized Management
500	2 Mbps	1,000 Mbps	1

Figure 10 – Number of Users

Installation Time

This table depicts the number of hours of labor required to install each breach detection solution. The table accurately reflects the amount of time that NSS engineers, with the help of vendor engineers, needed to install and configure the BDS to the point where it operated successfully in the test harness, ignored legitimate traffic, and detected prohibited or malicious traffic. This closely mimics a typical enterprise deployment scenario for a single product.

The installation cost is based on the time that an experienced security engineer would require to perform the installation tasks described above. This approach allows NSS to hold constant the talent cost and measure only the difference in time required for installation. Readers should substitute their own costs to obtain accurate TCO figures.

Product	Installation
Cisco Advanced Malware Protection v5.2.2015072320	8 hours (sensor) + 5 min (per agent)

Figure 11 – Installation Time (Hours)

Purchase Price And Total Cost Of Ownership

Calculations are based on vendor-provided pricing. 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 are for a 1000 Mbps single network BDS and/or 500 software agents, and maintenance only; the cost for a central management system (CMS) may be extra. For additional TCO analysis, including the CMS, refer to the TCO Comparative Report.

Product	Purchase	Maintenance /Year	Year 1 Cost	Year 2 Cost	Year 3 Cost	3-Year TCO
Cisco Advanced Malware Protection v5.2.2015072320	$77,995	$24,574	$125,456	$43,736	$43,736	$212,928

Figure 12 – Total Cost of Ownership (TCO)

- **Year 1 Cost** is calculated by adding installation costs (US$75 per hour fully loaded labor x installation time) + purchase price + first-year maintenance/support fees.
- **Year 2 Cost** consists only of maintenance/support fees and cost of FireAMP agent.
- **Year 3 Cost** consists only of maintenance/support fees**.**

This formula provides a TCO consisting of software, hardware, installation, and maintenance costs for a BDS that includes 1,000 Mbps of bandwidth and/or 500 agents. Additional management and labor costs are excluded, as are TCO calculations for additional devices or agents, since they are modeled extensively in the TCO Comparative Report.

Value: Total Cost of Ownership per Protected Mbps

There is a clear difference between price and value. The least expensive product does not necessarily offer the greatest value if it offers significantly lower performance than only slightly more expensive competitors. The best value is a product with a low TCO and high level of secure throughput (Detection Rate x *NSS-Tested Throughput*).

Figure 13 depicts the relative cost per unit of work performed, described as TCO per Protected Mbps.

Product	Detection Rate	3-Year TCO	NSS-Tested Throughput	TCO per Protected Mbps
Cisco Advanced Malware Protection v5.2.2015072320	99.2%	$212,928	1,000 Mbps	$215

Figure 13 – Total Cost of Ownership per Protected Mbps

The *TCO per Protected Mbps* was calculated by taking the 3-Year TCO and dividing it by the product of the detection rate multiplied by the *NSS-Tested Throughput*. Therefore, 3-Year TCO/ (Detection Rate x *NSS-Tested Throughput*) = TCO per Protected Mbps.

Appendix: Product Scorecard

Description	Result
Security Effectiveness	
Detection Rate	**99.2%**
Exploits	**98.4%**
Drive-by Exploits	96.7%
Social Exploits	100.0%
Malware (various delivery mechanisms)	**100.0%**
HTTP	100.0%
Email	100.0%
SMB	100.0%
Evasions	**100.0%**
Packers	100.0%
Compressors	100.0%
Virtual Machine	100.0%
Sandbox	100.0%
HTML Obfuscation	100.0%
Layered Evasions	100.0%
Performance	
Raw Packet Processing Performance (UDP Traffic)	Max Capacity (Mbps)
64 Byte Packets	1,000
128 Byte Packets	1,000
265 Byte Packets	1,000
512 Byte Packets	1,000
1024 Byte Packets	1,000
1514 Byte Packets	1,000
Maximum Capacity	Max Capacity
Maximum Concurrent TCP Connections	15,000,000
Maximum TCP Connections per Second	25,000
Maximum HTTP Connections per Second	125,000
HTTP Capacity with No Transaction Delays	Max Capacity (Mbps)
44 KB HTTP Response Size – 2,500 Connections per Second	1,000
21 KB HTTP Response Size – 5,000 Connections per Second	1,000
10 KB HTTP Response Size – 10,000 Connections per Second	1,000
4.5 KB HTTP Response Size – 20,000 Connections per Second	1,000
1.7 KB HTTP Response Size – 40,000 Connections per Second	1,000
HTTP Capacity With Transaction Delays	Max Capacity (Mbps)
21 KB HTTP Response Size with Delay	1,000
10 KB HTTP Response Size with Delay	1,000

Real-World Traffic	Max Capacity (Mbps)
Real-World Protocol Mix (Enterprise Perimeter)	1,000
Real-World Protocol Mix (Education)	1,000
Stability & Reliability	
Detection Under Extended Attack	PASS
Attack Detection – Normal Load	PASS
Protocol Fuzzing and Mutation – Detection Ports	PASS
Persistence of Data	PASS
TCO	
Ease of Use	
Initial Setup (Hours) – Hardware	8
Initial Setup (Hours) – Software	0.08333
Expected Costs	
Initial Purchase (hardware as tested)	$77,995
Initial Purchase (software as tested – per agent)	$0
Setup Cost ($75 Hour)	$3,725
Initial Purchase (enterprise management system)	See Comparative
Annual Cost of Maintenance & Support (hardware)	$24,536
Annual Cost of Maintenance & Support (software – per agent)	$38
Annual Cost of Maintenance & Support (enterprise management)	See Comparative
Total Cost of Ownership (TCO)	
Year 1	$125,456
Year 2	$43,736
Year 3	$43,736
3-Year TCO	$212,928

Figure 14 – Scorecard

Test Methodology

Breach Detection Systems (BDS): v2.0

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 USA
info@nsslabs.com
www.nsslabs.com