BREACH DETECTION SYSTEMS TEST REPORT

Trend Micro Deep Discovery Inspector Model 4000 (Hardware model 4100) v5.0 & OfficeScan XG SP1

OCTOBER 11, 2018

Authors – Dipti Ghimire, James Hasty

Overview

NSS Labs performed an independent test of the Trend Micro Deep Discovery Inspector Model 4000 (Hardware model 4100) v5.0 & OfficeScan XG SP1. The product was subjected to thorough testing at the NSS facility in Austin, Texas, based on the Breach Detection Systems (BDS) Test Methodology v5.0 and the NSS Labs Evasions Test Methodology v1.1, both available at www.nsslabs.com. This test was conducted free of charge and NSS did not receive any compensation in return for Trend Micro's participation.

As part of the initial BDS test setup, systems 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			Breach Detection Rate[1]	NSS-Tested Throughput	3-Year TCO (US$)
Trend Micro Deep Discovery Inspector Model 4000 (Hardware model 4100) v5.0 & OfficeScan XG SP1			98.7%	9,000 Mbps	$299,400
False Positives	Drive-by Exploits	Social Exploits	HTTP Malware (Executables)	HTTP Malware (Docs & Scripts)	SMTP Malware
0.93%	100.0%	100.0%	100.0%	100.0%	100.0%
Offline Infections		Stability & Reliability		Evasions Detected	
100.0%		PASS		371/374	

Figure 1 – Overall Test Results

The Deep Discovery Inspector Model 4000 (Hardware model 4100) achieved a breach detection rating of 98.7% after 20 hours and 48 minutes. The device proved effective against 371 out of 374 evasions tested. The device passed all stability and reliability tests.

The Deep Discovery Inspector Model 4000 (Hardware model 4100) was tested and rated by NSS at 9,000 Mbps (Trend Micro rates this device at 4,000 Mbps). *NSS-Tested Throughput* is calculated as an average of the "real-world" protocol mixes (Enterprise Perimeter and Financial) and the 21 KB HTTP response-based tests.

[1] Breach Detection Rate is defined as the percentage of all attacks 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 test cases in this section are completed with background network load.

This test utilizes threats and attack methods that exist in the wild and that are currently being used by cybercriminals and other threat actors. For live testing, NSS employs a unique live test harness, NSS' global threat intelligence network, to measure how well security products protect against "drive-by" exploits that target client applications.

NSS' global threat intelligence network captures thousands of suspicious URLs per day from threat data generated by NSS and its customers, as well as data from open-source and commercial threat feeds. This list of URLs is optimized and assigned to victim machines, each of which has a unique combination of operating system (including service pack/patch level), browser, and client application. For details on live testing, please refer to the latest Security Stack (Network) Test Methodology, which can be found at www.nsslabs.com.

The ability of the product to detect and report on successful breaches in a timely manner is critical to maintaining the security and functionality of the monitored network. Any malicious traffic should be detected and reported on 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 attempted breaches, the system under test should be able to detect known samples, or analyze unknown samples, and report on them as quickly as possible within 24 hours of initial exposure. Any system that does not alert on an attack, breach, or C&C callback within the detection window will not receive credit for the detection.

The following use cases were examined to determine whether or not the system could 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** – 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** – These samples can utilize varied and layered evasion and obfuscation techniques
- **Offline infections** – Remote users with mobile devices can become infected while outside the protection of the corporate network security. Once infected devices are reattached to the corporate network, the infection can spread.

False Positives

The ability of the BDS to identify legitimate traffic while maintaining detection of threats and breaches is as important as its ability to detect malicious content. This test includes a varied sample of legitimate application traffic that may be falsely identified as malicious (also known as false positives).

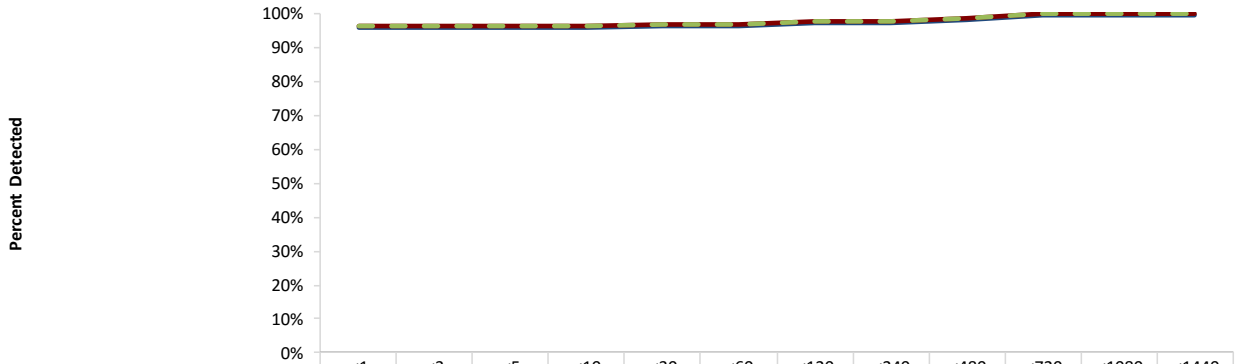
Figure 2 depicts the percentage of non-malicious traffic mistakenly identified as malicious. A lower score is better. The Deep Discovery Inspector Model 4000 (Hardware model 4100) demonstrated a false positive rate of 0.93%.

Product	Total Number of False Positives Run	Total Number of False Positives Detected	Detect Percentage
Trend Micro Deep Discovery Inspector Model 4000 (Hardware model 4100) v5.0 & OfficeScan XG SP1	540	5	0.93%

Figure 2 – False Positive Rate

Malware Delivered by Drive-by Exploits

Figure 3 depicts malware delivered using drive-by exploits. Drive-by exploits are defined as malicious software designed to take advantage of existing deficiencies in hardware or software systems such as vulnerabilities or bugs. During the test, the Deep Discovery Inspector Model 4000 (Hardware model 4100) detected 99.5% of the drive-by exploits on initial compromise and 100.0% on callback, resulting in an overall detection rate of 100.0%. Figure 3 provides a histogram of detection over time. Earlier detection is better.

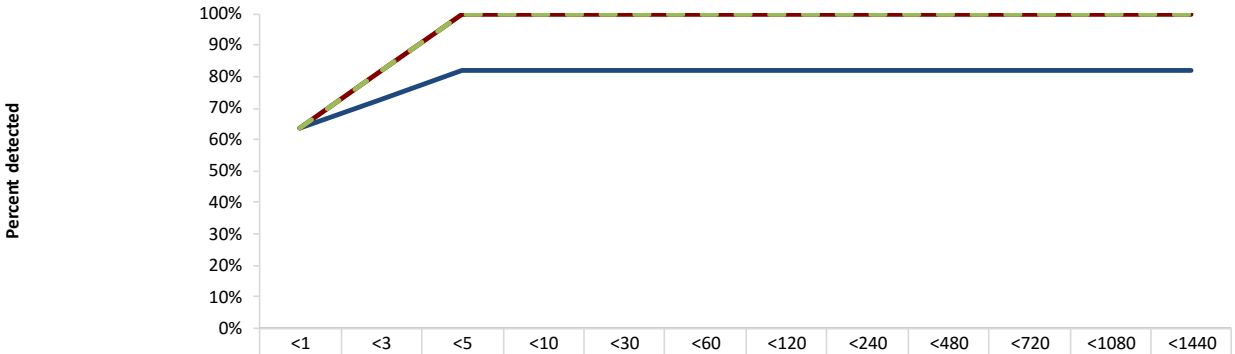


	<1	<3	<5	<10	<30	<60	<120	<240	<480	<720	<1080	<1440
Initial Compromise	95.9%	95.9%	95.9%	95.9%	96.4%	96.4%	97.3%	97.3%	98.2%	99.5%	99.5%	99.5%
Initial Compromise + Callback	96.4%	96.4%	96.4%	96.4%	96.8%	96.8%	97.7%	97.7%	98.6%	100.0%	100.0%	100.0%
Overall	96.4%	96.4%	96.4%	96.4%	96.8%	96.8%	97.7%	97.7%	98.6%	100.0%	100.0%	100.0%

Figure 3 – Malware Delivered by Drive-by Exploits: Detection over Time (Minutes)

Malware Delivered by Social Exploits

Figure 4 depicts malware delivered using social exploits. Social exploits are defined as malicious software designed to take advantage of existing deficiencies in hardware or software systems, such as vulnerabilities or bugs. During the test, the Deep Discovery Inspector Model 4000 (Hardware model 4100) detected 81.8% of the exploits on initial compromise and 100.0% on callback, resulting in an overall detection rate of 100.0%. Figure 4 provides a histogram of detection over time. Earlier detection is better.

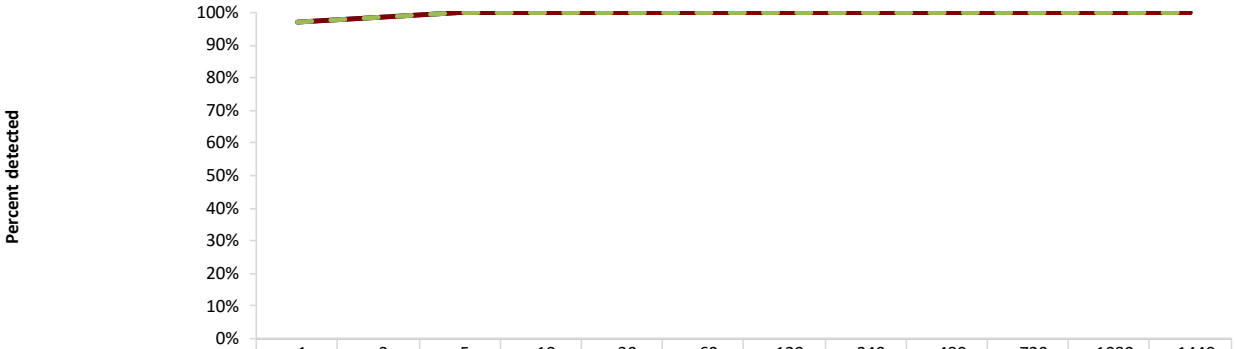


	<1	<3	<5	<10	<30	<60	<120	<240	<480	<720	<1080	<1440
Initial Compromise	63.6%	72.7%	81.8%	81.8%	81.8%	81.8%	81.8%	81.8%	81.8%	81.8%	81.8%	81.8%
Download + Callback	63.6%	81.8%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Overall	63.6%	81.8%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Figure 4 – Malware Delivered by Social Exploits: Detection over Time (Minutes)

Malware Delivered over HTTP (Executables)

Figure 5 depicts .exe malware using the HTTP protocol as its transport mechanism; that is, the malware is downloaded through a web browser. During the test, Deep Discovery Inspector Model 4000 (Hardware model 4100) detected 100.0% of the malware on download and 100.0% on callback, resulting in an overall detection rate of 100.0%. Figure 5 provides a histogram of detection over time. Earlier detection is better.

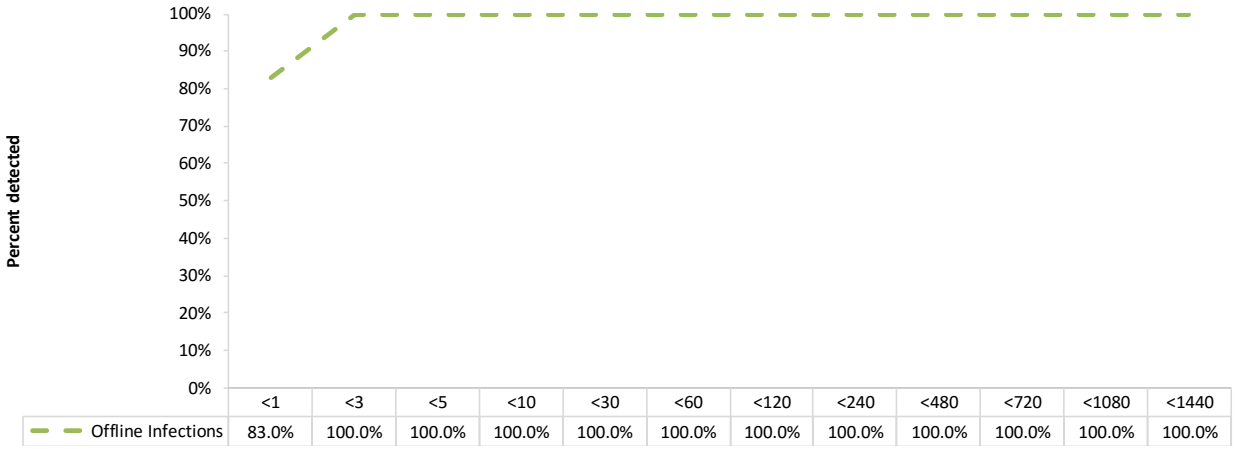


	<1	<3	<5	<10	<30	<60	<120	<240	<480	<720	<1080	<1440
Download	97.0%	98.7%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Download + Callback	97.0%	98.7%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Overall	97.0%	98.7%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Figure 5 – Malware Delivered over HTTP (Executables): Detection over Time (Minutes)

Malware Delivered over HTTP (Docs and Scripts)

Figure 6 depicts docs and scripts malware using the HTTP protocol as its transport mechanism; that is, the malware is downloaded through a web browser. During the test, Deep Discovery Inspector Model 4000 (Hardware model 4100) detected 100.0% of docs and scripts. Figure 6 provides a histogram of detection over time. Earlier detection is better.

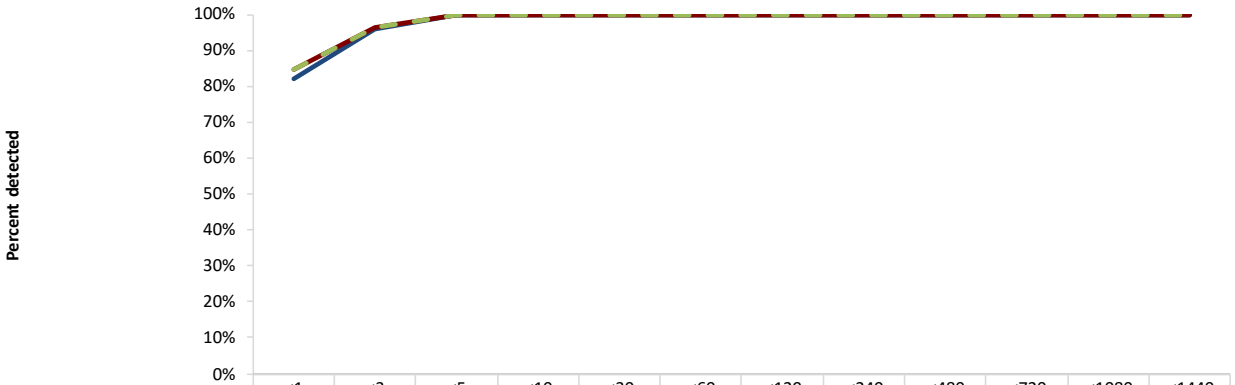


	<1	<3	<5	<10	<30	<60	<120	<240	<480	<720	<1080	<1440
Offline Infections	83.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Figure 6 – Malware Delivered over HTTP (Docs and Scripts): Detection over Time (Minutes)

Malware Delivered over Email

Figure 7 depicts malware that uses email (SMTP) as its transport mechanism; for example, a malicious email attachment. During the test, the Deep Discovery Inspector Model 4000 (Hardware model 4100) detected 99.9% of the malware on download and 100.0% on callback, resulting in an overall detection rate of 100.0%. Figure 7 provides a histogram of detection over time. Earlier detection is better.

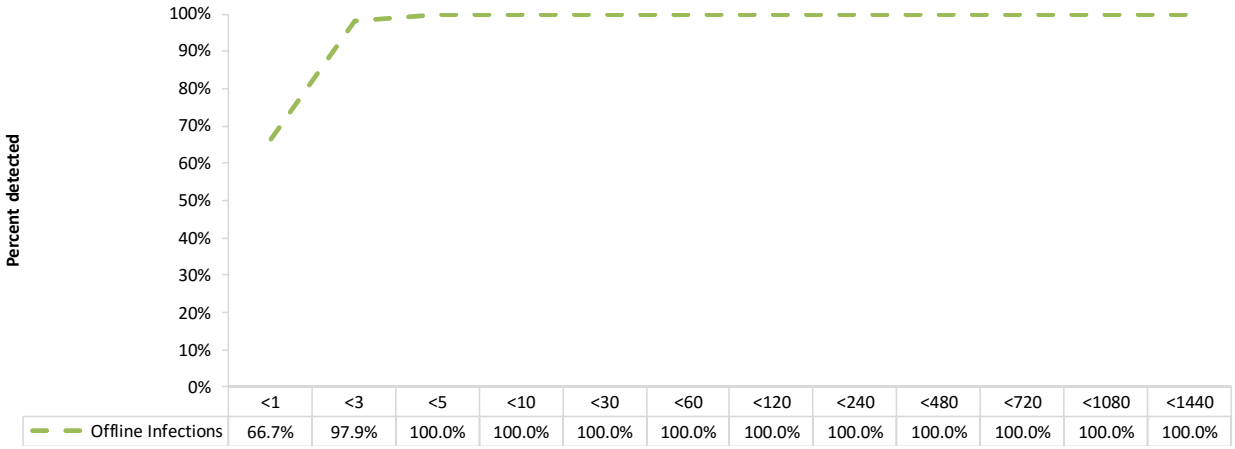


	<1	<3	<5	<10	<30	<60	<120	<240	<480	<720	<1080	<1440
Download	82.3%	95.8%	99.7%	99.7%	99.7%	99.7%	99.7%	99.7%	99.8%	99.9%	99.9%	99.9%
Download + Callback	84.6%	96.2%	99.8%	99.8%	99.8%	99.8%	99.8%	99.8%	99.9%	100.0%	100.0%	100.0%
Overall	84.6%	96.2%	99.8%	99.8%	99.8%	99.8%	99.8%	99.8%	99.9%	100.0%	100.0%	100.0%

Figure 7 – Malware Delivered over Email: Detection over Time (Minutes)

Offline Infections

Offline infections are defined as situations where hosts are infected with malware outside the corporate network and subsequently attached to the network. During the test, the Deep Discovery Inspector Model 4000 (Hardware model 4100) detected 100.0% of the offline infections. Figure 8 provides a histogram of detection over time. Earlier detection is better.



	<1	<3	<5	<10	<30	<60	<120	<240	<480	<720	<1080	<1440
Offline Infections	66.7%	97.9%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Figure 8 – Offline Infections: Detection over Time (Minutes)

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 samples that the device normally would detect. The resiliency of a system can be defined as its ability to absorb an attack and reorganize around a threat.

When an attacker is presented with a vulnerability, the attacker can select one or more paths to trigger the vulnerability. NSS measured the BDS' resiliency by introducing a vulnerability along with its triggers and then asking the device to protect against the vulnerability. Various previously unseen variations of exploits were introduced to exploit the vulnerability and measure the device's effectiveness against them. A resilient device is able to detect and prevent against different variations of an exploit.

For more, see the Evasions Test Methodology v1.1 at www.nsslabs.com. Figure 9 provides the results of the evasion tests for the Deep Discovery Inspector Model 4000 (Hardware model 4100).

Test Procedure	Result
Binary Obfuscation	100.0%
Packers	100.0%
Compressors	100.0%
Virtual Machine	100.0%
Sandbox	100.0%
HTML Obfuscation	100.0%
Anti-Debugging and Monitoring	100.0%
Metamorphic and Polymorphic	91.7%
HTTP Evasion	100.0%
Layered Evasions	93.3%
Resiliency[2]	
Attacks on nonstandard ports[3]	PASS

Figure 9 – Resistance to Evasion Results

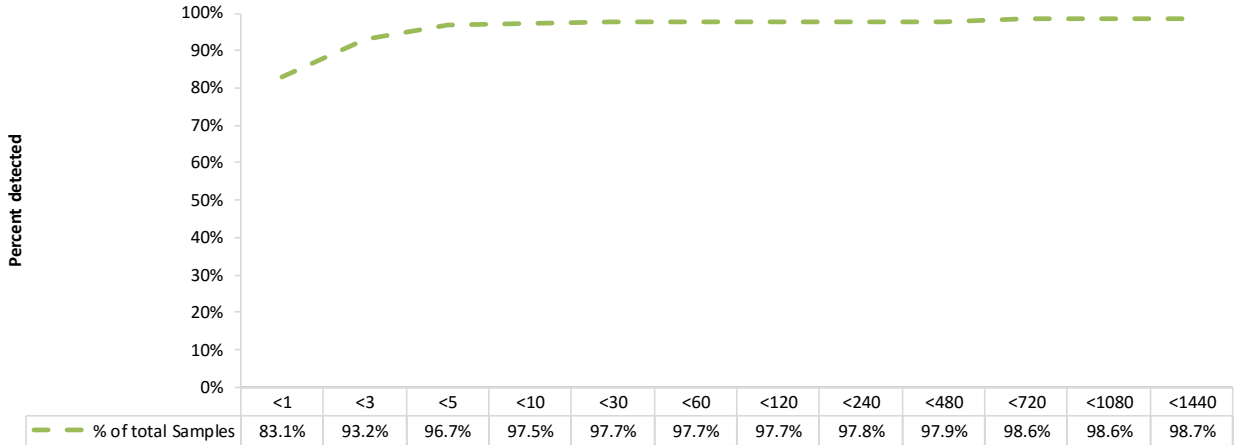
[2] The results of resiliency testing are included in the Breach Detection Rate calculations.

[3] Enterprises should be aware of the importance of egress filtering and should ensure their configurations mitigate these risks.

Time to Detect

As response time is critical in halting the damage caused by a breach, the BDS should be able to detect known samples, or analyze unknown samples, and report on it within 24 hours of initial infection, command and control (C&C) callback, or other malicious outbound traffic. Any BDS that cannot, or does not, log an attack, infection, or C&C callback within this detection window will not receive credit for the detection.

Over the course of the test, the Deep Discovery Inspector Model 4000 (Hardware model 4100) reached its maximum detection rate of 98.7 % of all attacks[4] after 20 hours and 47 minutes. Figure 10 provides a histogram of detection over time. Earlier detection is better.



	<1	<3	<5	<10	<30	<60	<120	<240	<480	<720	<1080	<1440
% of total Samples	83.1%	93.2%	96.7%	97.5%	97.7%	97.7%	97.7%	97.8%	97.9%	98.6%	98.6%	98.7%

Figure 10 – Time to Detect

[4] The Time to Detect score includes evasions.

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. All tests in this section are repeated at 25%, 50%, 75%, and 100% of the maximum rated throughput of the system under test (note that the 100% load is actually less than 100% to allow headroom for malicious traffic). 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 test.

HTTP Capacity

These tests stress the HTTP detection engine and determine how the system 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 system 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 conditions as can be achieved in a lab environment, while also ensuring absolute accuracy and repeatability.

Each transaction consists of a single HTTP GET request. 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.

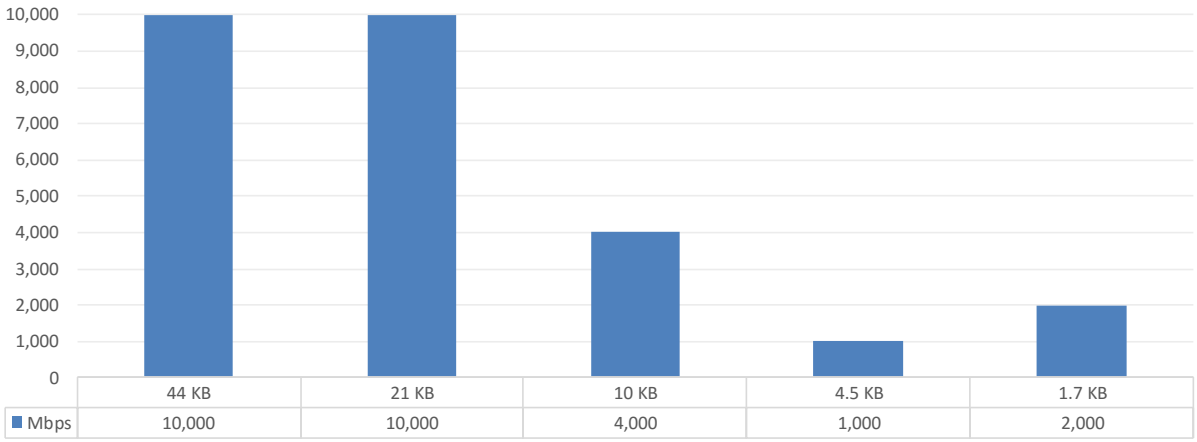


Figure 11 – Detection under Load (HTTP Capacity)

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 that which may be found on a heavily utilized "normal" production network. Results are presented in Figure 12.

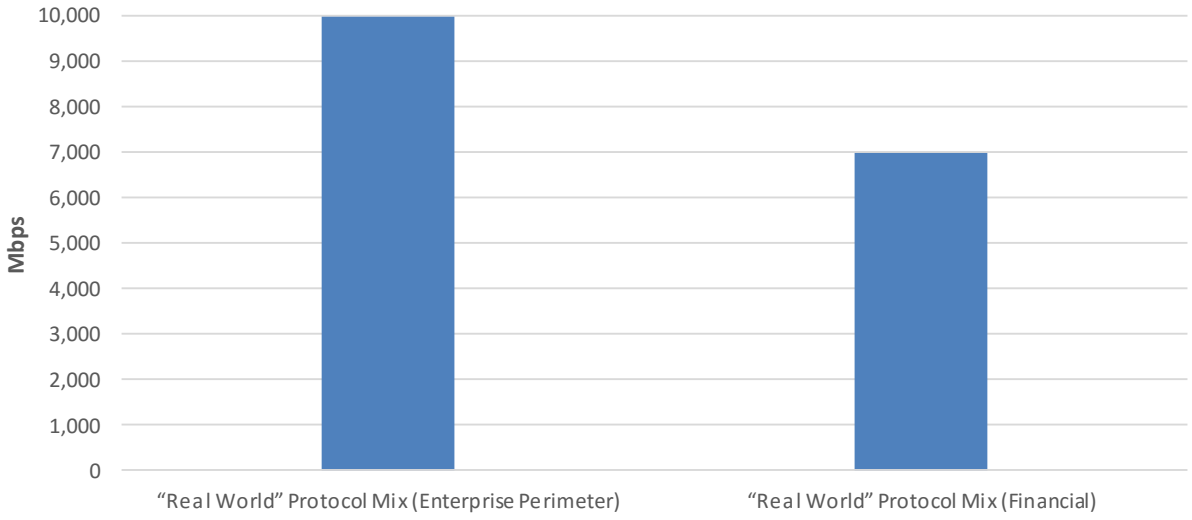


Figure 12 – Detection under Load ("Real-World" Traffic)

Stability and Reliability

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

The system is required to remain operational and stable throughout these tests and to detect 100% of previously detected traffic, raising an alert for each. If any malicious traffic passes undetected—caused by either the volume of traffic or by the system failing for any reason—this will result in a fail.

Figure 13 presents the results of the stability and reliability tests for the Deep Discovery Inspector Model 4000 (Hardware model 4100).

Stability and Reliability	Result
Detection under extended attack	PASS
Power failure and persistence of data	PASS

Figure 13 – Stability and Reliability Results

Total Cost of Ownership (TCO)

Implementation of security products can be complex, with several factors affecting the overall cost of deployment, maintenance, and upkeep. All of the following should be considered over the course of the useful life of the product:

- **Product Purchase** – The cost of acquisition
- **Product Maintenance** – The fees paid to the vendor, including software and hardware support, maintenance, and other updates
- **Installation** – The time required to take the device out of the box, configure it, install it in 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 device only (the cost of acquisition and installation).

Calculating the Total Cost of Ownership (TCO)

When procuring a BDS for the enterprise, it is essential to factor in both bandwidth and number of users. NSS has found that the 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 of sustained throughput per employee. For example, to support 500 users, an enterprise must deploy 500 agents and/or one network device of 1,000 Mbps capacity.

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

Figure 14 – Number of Users

Installation Time

Figure 15 depicts the number of hours of labor required to install each system using only local device management options. The table accurately reflects the amount of time that NSS engineers, with the help of vendor engineers, needed to install and configure the system to the point where it operated successfully in the test harness, passed legitimate traffic, and detected any prohibited or malicious traffic. This closely mimics a typical enterprise deployment scenario for a single system.

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
Trend Micro Deep Discovery Inspector Model 4000 (Hardware model 4100) v5.0 & OfficeScan XG SP1	8 hours

Figure 15 – Installation Time (Hours)

Total Cost of Ownership

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 are for a 1,000 Mbps single-network BDS and/or 500 software agents and maintenance only; costs for central management solutions (CMS) may be extra.

Product	Purchase	Maintenance /Year	Year 1 Cost	Year 2 Cost	Year 3 Cost	3-Year TCO
Trend Micro Deep Discovery Inspector Model 4000 (Hardware model 4100) v5.0 & OfficeScan XG SP1	$166,000	$66,400	$166,600	$66,400	$66,400	$299,400

Figure 16 –3-Year TCO (US$)

- **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.
- **Year 3 Cost** consists only of maintenance/support fees.

For additional TCO analysis, including for the CMS, refer to the TCO Comparative Report.

Appendix: Product Scorecard

Security Effectiveness			
False Positives	0.93%		
Exploits	Download/Drop	Download/Callback	Overall
Drive-by Exploits	99.5%	12.2%	100.0%
Social Exploits	81.8%	72.7%	100.0%
Malware (various delivery mechanisms)	Download/Drop	Download/Callback	Overall
HTTP (Executables)	100.0%	17.8%	100.0%
SMTP	99.9%	24.5%	100.0%
HTTP (Docs and Scripts)	100.0%		
Off-Line Infections	100.0%		
Evasions			
Binary Obfuscation	100.0%		
Packers	100.0%		
Compressors	100.0%		
Virtual Machine	100.0%		
Sandbox	100.0%		
HTML Obfuscation	100.0%		
Anti-Debugging and Monitoring	100.0%		
Metamorphic and Polymorphic	91.7%		
HTTP Evasion	100.0%		
Layered Evasions	93.3%		
Resiliency	47.4%		
Performance			
Maximum Capacity (HTTP Capacity)	Max Capacity (Mbps)		
44 KB HTTP Response Size – 2,500 Connections per Second	10,000		
21 KB HTTP Response Size – 5,000 Connections per Second	10,000		
10 KB HTTP Response Size – 10,000 Connections per Second	4,000		
4.5 KB HTTP Response Size – 20,000 Connections per Second	1,000		
1.7 KB HTTP Response Size – 40,000 Connections per Second	2,000		
“Real-World” Traffic	Max Capacity (Mbps)		
“Real-World” Protocol Mix (Enterprise Perimeter)	10,000		
“Real-World” Protocol Mix (Financial)	7,000		
Stability & Reliability			
Detection Under Extended Attack	PASS		
Power Failure and Persistence of Data	PASS		
Total Cost of Ownership			
Ease of Use			
Initial Setup (Hours)	8		
Time Required for Upkeep (Hours per Year)	Contact NSS Labs		
Time Required to Tune (Hours per Year)	Contact NSS Labs		
Expected Costs			
Initial Purchase (hardware as tested)	$166,000		
Installation Labor Cost (@$75/hr)	$600		
Annual Cost of Maintenance & Support (hardware/software)	$66,400		

Annual Cost of Updates (IPS/AV/etc.)	Included
Initial Purchase (centralized management system)	Contact NSS Labs
Annual Cost of Maintenance & Support (centralized management)	Contact NSS Labs
Management Labor Cost (per Year @$75/hr)	Contact NSS Labs
Tuning Labor Cost (per Year @$75/hr)	Contact NSS Labs
Total Cost of Ownership	
Year 1	$166,600
Year 2	$66,400
Year 3	$66,400
3 Year Total Cost of Ownership	$299,400

Figure 17 – Scorecard

Test Methodology

NSS Labs Breach Detection Systems (BDS) Test Methodology v5.0

NSS Labs Evasions Test Methodology v1.1

A copy of the test methodology is available on the NSS Labs website at www.nsslabs.com.

Contact Information

3711 South Mopac Expressway
Building 1, Suite 400
Austin, TX 78746
info@nsslabs.com
www.nsslabs.com