



# ENTERPRISE EPP COMPARATIVE REPORT

## Security Stack: Socially Engineered Malware

**Authors – Bhaarith Venkateswaran, Randy Abrams, Thomas Skybakmoen**

### Tested Products

Bitdefender Endpoint Security v5.3.15.539

ESET Endpoint Security v 6.1.2109.0

Fortinet FortiClient v5.2.3.0633

F-Secure Client Security Premium 11.60 build 284

G DATA Security Client v13.1.0.224

Kaspersky Endpoint Security v10.2.2.10535

McAfee Endpoint Protection v8.0

Panda Endpoint Security v7.20.0

Sophos Endpoint Security v10.3

Symantec Endpoint Security v12.1.4112.4156

Trend Micro Endpoint Security v11.0.1057

### Environment

Windows 7 SP1 32-Bit

- Windows Firewall disabled
- Windows automatic updates disabled

Internet Explorer 10

## Overview

The endpoint user creates a broad attack surface that is difficult to defend. Socially engineered malware (SEM) and the exploitation of software vulnerabilities are among the most common and effective cyberattacks that enterprises face today. Endpoint protection (EPP) products must provide robust defenses against these threats. NSS tested 11 enterprise-class EPP products for their ability to protect against exploits and SEM. The results presented in this report were obtained via 24x7 continuous testing over a period of 24 days.

### Average Block Rate

Figure 1 depicts the number of SEM samples blocked throughout the test. EPP product updates may contain new engine updates, heuristic updates, and malware-specific detection updates, all of which affect the quality of protection against exploits and malware. This test focuses on SEM. Tests for exploit protection are published at [www.nsslabs.com](http://www.nsslabs.com).

Product	Average Block Rate	NSS Rating
Kaspersky Endpoint Security v10.2.2.10535	100.0%	<b>Recommended</b>
McAfee Endpoint Protection v8.0	100.0%	<b>Recommended</b>
Symantec Endpoint Security v12.1.4112.4156	100.0%	<b>Recommended</b>
ESET Endpoint Security v6.1.2109.0	99.9%	<b>Recommended</b>
Fortinet FortiClient v5.2.3.0633	99.9%	<b>Recommended</b>
Sophos Endpoint Security v10.3	99.0%	<b>Recommended</b>
Trend Micro Endpoint Security v11.0.1057	99.0%	<b>Recommended</b>
F-Secure Client Security Premium 11.60 build 284	98.1%	Neutral
G DATA Security Client v13.1.0.224	94.8%	Neutral
Bitdefender Endpoint Security v5.3.15.539	92.8%	Neutral
Panda Endpoint Security v7.20.0	82.8%	Caution

Figure 1 – Average Block Rate

This test was composed of over 1,700 test cases that included 400 unique attacks (URLs) and 304 unique SEM samples (hashes). A unique SEM sample has a unique hash. A unique attack URL may contain duplicate SEM samples that are part of a unique URL; <http://a.edu/abc/malware.exe> and <http://a.edu/malware.exe> are unique URLs.

## Response Times

New SEM is continuously added to the harness throughout the test. Most EPP products are able to block many samples at zero hour. Figure 2 depicts the average percentage of new samples blocked during the first seven days after they are discovered. When products achieve equal maximum protection rates, response time becomes a differentiator. The products are ranked in the order of zero-hour protection.

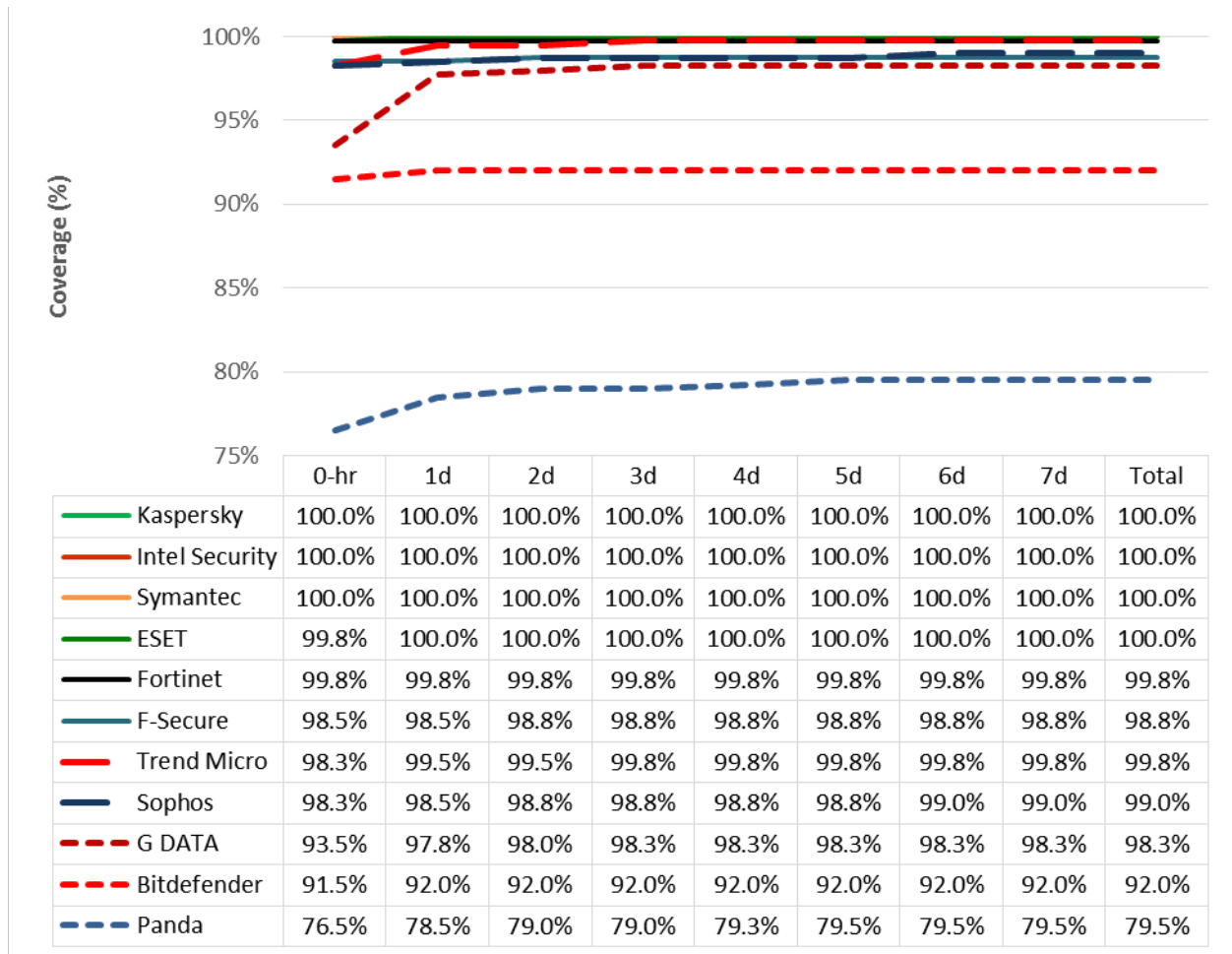


Figure 2 – Seven-Day Response Histogram

## Average Time to Add Protection

Figure 3 reports the average amount of time required to add protection for all attacks throughout the test.

Vendor	Hours
Fortinet	0.00
Kaspersky	0.00
Intel Security	0.00
Symantec	0.00
ESET	0.03
Bitdefender	0.05
F-Secure	0.09
Trend Micro	0.28
Sophos	0.42
G DATA	0.64
Panda	1.17

Figure 3 – Average Time to Add Protection

## Consistency of Protection

It is important to maintain a consistent SEM protection rate throughout the test. Negative fluctuations can indicate decreased protection rates for new samples, erratic protection for new and existing samples, or both. Details on how each vendor performed can be found in individual test reports, published at [www.nsslabs.com](http://www.nsslabs.com).

## Test Methodology

Security Stack: Test Methodology v1.5

A copy of the test methodology is available at [www.nsslabs.com](http://www.nsslabs.com).

## Contact Information

NSS Labs, Inc.  
206 Wild Basin Rd  
Building A, Suite 200  
Austin, TX 78746  
[info@nsslabs.com](mailto:info@nsslabs.com)  
[www.nsslabs.com](http://www.nsslabs.com)

This and other related documents available at: [www.nsslabs.com](http://www.nsslabs.com). To receive a licensed copy or report misuse, please contact NSS Labs.

© 2015 NSS Labs, Inc. All rights reserved. No part of this publication may be reproduced, copied/scanned, stored on a retrieval system, e-mailed or otherwise disseminated or transmitted without the express written consent of NSS Labs, Inc. (“us” or “we”).

Please read the disclaimer in this box because it contains important information that binds you. If you do not agree to these conditions, you should not read the rest of this report but should instead return the report immediately to us. “You” or “your” means the person who accesses this report and any entity on whose behalf he/she has obtained this report.

1. The information in this report is subject to change by us without notice, and we disclaim any obligation to update it.
2. The information in this report is believed by us to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at your sole risk. We are not liable or responsible for any damages, losses, or expenses of any nature whatsoever arising from any error or omission in this report.
3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY US. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, ARE HEREBY DISCLAIMED AND EXCLUDED BY US. IN NO EVENT SHALL WE BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and/or software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet your expectations, requirements, needs, or specifications, or that they will operate without interruption.
5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.
6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.