CONSUMER ANTI-MALWARE PRODUCTS

GROUP TEST REPORT

AVG Internet Security 9
ESET Smart Security 4
F-Secure Internet Security 2010
Kaspersky Internet Security 2011
McAfee Internet Security
Microsoft Security Essentials

Norman Security Suite
Panda Internet Security 2011
Sunbelt VIPRE Antivirus Premium 4
Symantec Norton Internet Security 2010
Trend Micro Titanium Maximum Security

METHODOLOGY VERSION: 1.5
SEPTEMBER 2010

All testing was conducted independently and without sponsorship.

For expert, independent advice on corporate products, contact us at
+1 (760) 412-4627 or advisor@nsslabs.com.

Please note that access to or use of this report is conditioned on the following:

1. The information in this report is subject to change by NSS Labs without notice.

2. The information in this report is believed by NSS Labs to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at the reader's sole risk. NSS Labs is not liable or responsible for any damages, losses, or expenses arising from any error or omission in this report.

3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY THE NSS LABS. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY NSS LABS. IN NO EVENT SHALL NSS LABS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL 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 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 the reader's 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.

CONTACT INFORMATION

NSS Labs, Inc.
P.O. Box 130573
Carlsbad, CA 92013 USA
+1 (760) 412-4627
www.nsslabs.com

TABLE OF CONTENTS

Summary of Findings

Based on these latest test results, cybercriminals are becoming more effective. Consumers are facing a dizzying array of threats that are not completely addressed by even the best performing products. Products need to improve – some more dramatically than others. Tested products slipped by 6% on average from 2009 to 2010. And the notion that "you're fine as long as you keep your AV updated" is completely false. To be clear, consumers need protection and should pick one of the products that scored best in our testing. Note that in most cases we found considerable differences between a vendor's corporate product and their consumer version. It is not safe to assume the results are identical.[1]

Product	Malware Blocking%	Exploit Blocking %	Performance Impact
Trend Micro	90.1%	**19%**	0.21
McAfee	85.2%	**73%**	0.67
F-Secure	80.4%	**75%**	1.17
Norman	77.2%	**25%**	0.05
Sunbelt	75.3%	**3%**	0.37
Microsoft	75.0%	**60%**	0.05
Panda	73.1%	**10%**	0.17
Symantec	72.3%	**64%**	0.09
Kaspersky	71.3%	**75%**	0.38
Eset	60.0%	**44%**	0.09
AVG	54.8%	**15%**	0.58

TABLE 1: PRODUCT GUIDANCE

Overall Results & Findings

- Malware protection is far from commodity, with effectiveness ranging between 54% and 90%, a 36% spread.
- Cybercriminals have between a 10% - 45% chance of getting past your AV with Web Malware (depending on the product).
- Cybercriminals have between 25% - 97% chance of compromising your machine using exploits (depending on the product).
- Expect use of exploits to increase since it is far more effective than traditional malware.

The overall findings from the study underscore the need to choose wisely based on technical evaluations. Our assessment places a slightly higher importance on the malware protection over time, since that best reflects long-term averages of real-world usage. Currently, web-delivered malware is a more prevalent attack against consumers than exploits, although the

[1] For corporate security product testing and research, consult our paid reports by contacting us at www.nsslabs.com

latter is quickly rising. As the use of exploits increases, this will factor greater into our weighting.

PRODUCT GUIDANCE

Trend Micro offers the best protection against Web Malware, and excellent performance (i.e. minimal impact). However, its lack of exploit protection is a considerable impediment. McAfee and F-Secure also offer good protection from Web Malware. F-Secure, Kaspersky, and McAfee offer the best protection against exploits. However, McAfee and F-Secure had the largest performance impact. In our opinion, the performance impact is far outweighed by the security imperative, and users should prioritize security over performance.

Rating	Products *(alphabetically)*
Recommend	F-Secure McAfee Trend Micro
Neutral	Kaspersky Microsoft Norman Panda Sunbelt Symantec
Caution	AVG ESET

TABLE 2: PRODUCT GUIDANCE

1 Introduction

Today's cybercriminals have vast resources and advantages over end-users of personal computers. Their ability to develop, mutate and launch a myriad of attacks – ranging from phishing and malware, exploits – appears significant. Detecting and preventing these threats continues to be a challenge as criminals remain aggressive. Malware proliferation statistics for 2009 and 2010 show an acceleration of this trend. And all evidence suggests that this gap between attacker and attacked is widening.

Meanwhile, consumers are besieged with a plethora of security products which profess to protect them from these attacks. Some even claim to 'catch every threat', or offer 'total protection', 'maximum protection' etc. With more than 40 antivirus vendors, each with several product versions, it's easy for consumers to be confused about which product to purchase, and make the wrong choice.

To help consumers make better, empirically informed, decisions about how to protect themselves, NSS Labs has conducted an anti-malware product group test free of charge as a public service. This test at once demonstrates the threat landscape, and state of security software (not to mention our testing capabilities).

This test examines multiple threat types and vectors from end-to-end, all the while, replicating how real people access the internet. This whole product test report examines protection from the following threats and vectors:

- Malware Downloaded from web sites on the internet through social engineering tricks
- Client-side exploits against applications such as Windows® Internet Explorer®, Mozilla® Firefox®, Apple® Quicktime®, and Adobe® Acrobat®.

In addition, we measured several key performance metrics, such as increase in memory, CPU, boot time, and application load time.

Security software used in the test was either provided by the vendor or generally available from their public website for purchase. All software was installed on identical machines, with the following specifications:

- Microsoft® Windows 7 operating system
- 2 GB RAM
- 20 GB HD

Test machines were verified prior to and during the experiment to ensure proper functioning, and were given full access to the Internet so they could visit the actual live sites. SmartScreen® was disabled within Windows Internet Explorer 8 so that no other reputation services in the browser would interfere with the product under test.

1.1 The Internet Security Suite Functionality

Most antivirus vendors offer several product options, ranging from basic antivirus to more feature-rich internet security suites. The main goal of these products is to protect against socially-engineered malware; malicious files that a user unwittingly chooses to execute. Another growing threat that must be countered are client-side exploits, sometimes referred to as ‘drive-by downloads’. In these cases, vulnerabilities in a PC’s software can be exploited when a user visits an infected web site – silently, without the user’s knowledge.

Internet Security Suites must catch these sophisticated attacks while not mistaking legitimate programs for bad ones. Meanwhile, users are demanding solutions that don’t slow their systems down.

2 Malware Protection

The Socially-Engineered Malware Threat

Socially-engineered malware attacks trick users into downloading and running malicious programs disguised as movie files, codecs, and other utilities. This web-based vector represents over 50% of the malware in circulation today. Detecting and preventing these threats continues to be a challenge as criminals become more aggressive. Anti-virus researchers detect 50,000 new malicious programs per day on average, and malware proliferation statistics for 2009 and 2010 show an acceleration of this trend.

2.1 Proactive and Execution Protection

Two important factors in any endpoint protection product are proactive and total protection. “Blocked on download” means malware has been kept off the machine entirely. For malware that made it past this first line of defense, we also measured the percentage “Blocked on execution.” Total protection includes both download and execution layers. In the graph below, farther up and right is best. The average block rate on download was 56%, and 74% overall.

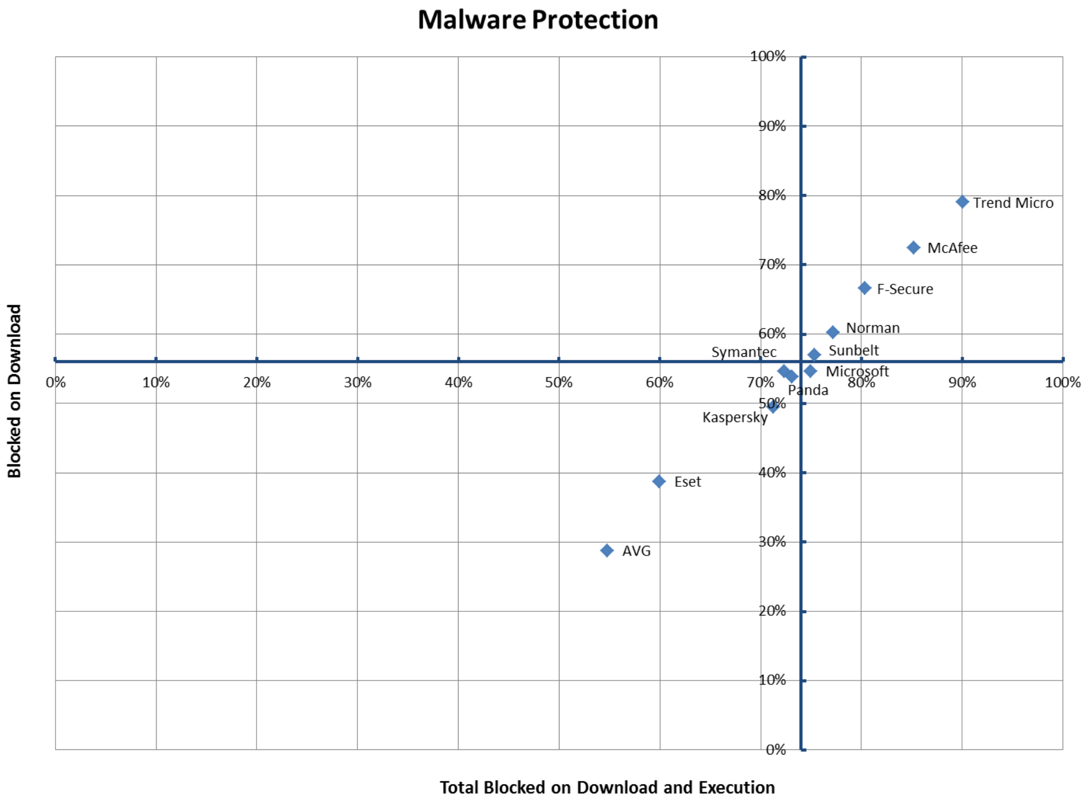


FIGURE 1: AVERAGE PROTECTION FROM SOCIALLY-ENGINEERED MALWARE

2.2 Blocking URLs with Socially Engineered Malware Over Time

The metrics for blocking individual URLs represent just one perspective. When it comes to daily usage scenarios, users are visiting a wide range of sites which may change quickly. Thus, at any given time, the available set of malicious URLs is revolving; continuing to block these sites is a key criterion for effectiveness. Therefore, NSS Labs tested a set of live URLs every six hours. The following tables and graphs show the repeated evaluations of blocking over the course of the entire test period. Each score represents protection at a given point in time. The protection ratings answer the question: "what kind of protection can I expect from my product at any given time?"

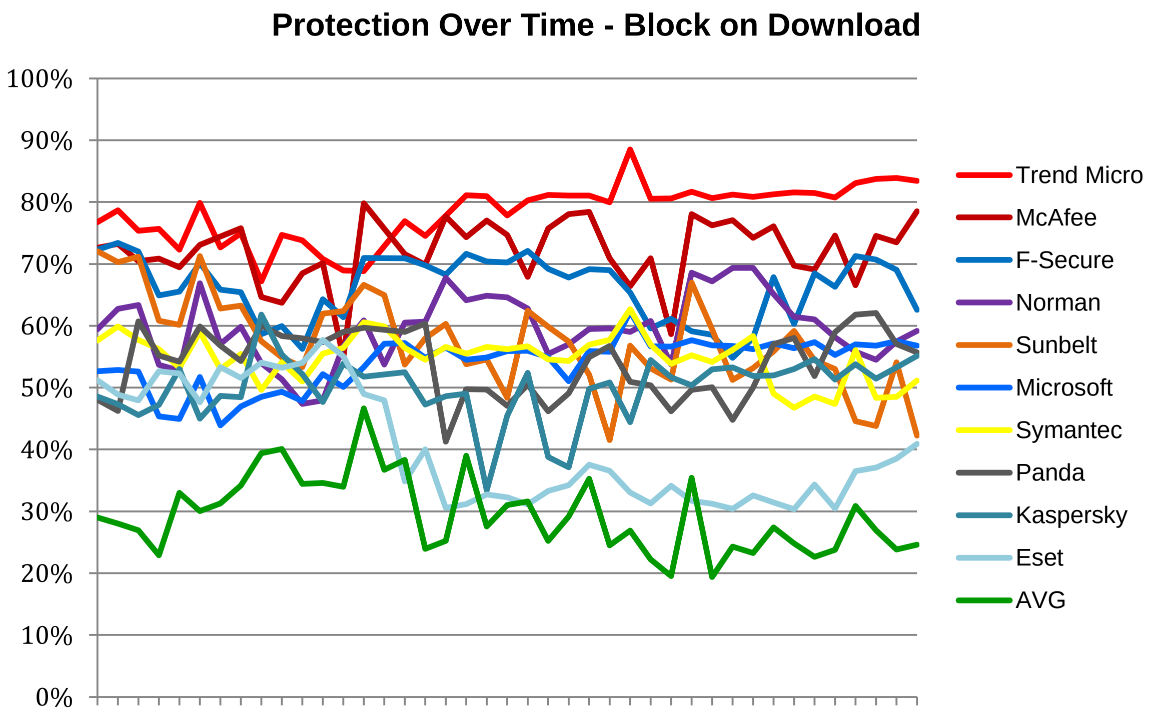


FIGURE 2: SOCIALLY-ENGINEERED MALWARE PROTECTION OVER TIME

Note that the average protection percentage will deviate from the unique URL results for several reasons. First, this data includes multiple tests of a URL. So if it is blocked early on, it will improve the score. If it continues to be missed, it will detract from the score. This method provides a reasonable estimate of expected protection at any given time.

On the proactive measurement, Trend Micro, McAfee and F-Secure prevented significantly more malware from being downloaded than other products.

2.3 Download + Execution

If a malicious file is downloaded, then the goal is to prevent code execution. In our dynamic execution test, we ran the malware and allowed all facilities of the software to attempt to block it.

Table 1 below provides detailed results used in Figure 1 above, as well as the Protection Over Time results from Figure 2 above. Products are sorted by Total Blocked.

Product	Blocked on Download (A+B)	Additional Blocked on Execution (C)	Total Blocked
Trend Micro	79.0%	11.1%	90.1%
McAfee	72.4%	12.8%	85.2%
F-Secure	66.6%	13.8%	80.4%
Norman	60.3%	16.9%	77.2%
Sunbelt	57.0%	18.3%	75.3%
Microsoft	54.6%	20.3%	75.0%
Panda	53.8%	19.3%	73.1%
Symantec	54.6%	17.7%	72.3%
Kaspersky	49.5%	21.8%	71.3%
Eset	38.7%	21.3%	60.0%
AVG	28.7%	26.1%	54.8%

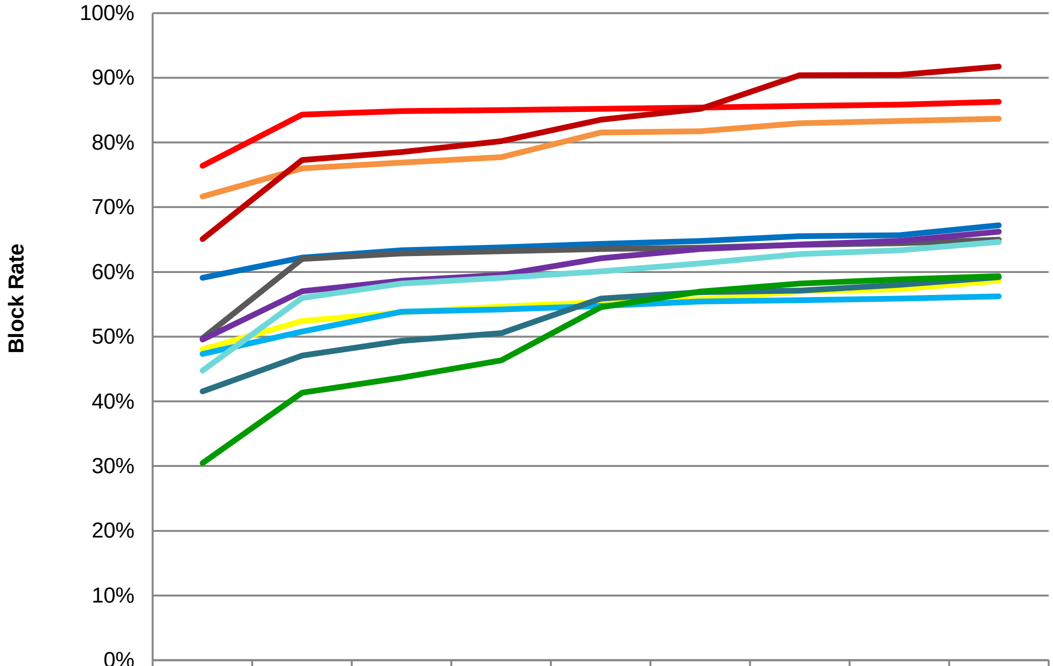
TABLE 3: PERCENTAGE OF MALWARE CAUGHT BY PRODUCT

Overall, the Trend Micro and McAfee products are well ahead of most of the competition in protecting against web-based socially-engineered malware. F-Secure also ranked fairly high. Perhaps surprisingly, Microsoft Security Essentials, a free product, ranked higher than half of the competition (paid products), including Symantec’s market leading product.

2.4 Time to Protect Histogram

Approximately half of the products tested caught less than half of the malware upon first introduction to the test. For all malware that was not caught initially, we measured the time to add protection for each sample. This was achieved by continuing to test each sample every 6 hours throughout the test and noting when protection was added. The “Time-to-Protect” graph represents an important metric of how quickly vendors are able to add protection for a threat once it has been introduced into the test cycle.

Re-sampling malware protection levels like this is a unique feature of NSS Labs’ Live Testing. It is also worth noting that traditional AV tests do not test malware as quickly as with our testing. This accounts for some fairly high scores which can be misleading in those tests. If samples are held for days, weeks or months prior to testing, this can skew results higher than a consumer would experience in the real world. The skew can be even higher when samples are shared between testers and vendors prior to the test.


Histogram - Block on Download (Over Time)

	0-hr	1d	2d	3d	4d	5d	6d	7d	Total
▬ Trend Micro	76.4%	84.3%	84.8%	85.0%	85.2%	85.4%	85.7%	85.8%	86.3%
▬ Sunbelt	71.7%	76.0%	76.9%	77.7%	81.6%	81.7%	83.0%	83.3%	83.7%
▬ McAfee	65.1%	77.3%	78.5%	80.2%	83.5%	85.2%	90.4%	90.5%	91.7%
▬ F-Secure	59.1%	62.2%	63.4%	63.8%	64.3%	64.8%	65.5%	65.7%	67.2%
▬ Panda	49.7%	62.0%	62.8%	63.2%	63.5%	63.7%	64.2%	64.4%	65.0%
▬ Norman	49.6%	57.0%	58.6%	59.5%	62.1%	63.5%	64.3%	64.8%	66.2%
▬ Symantec	48.0%	52.4%	53.7%	54.6%	55.3%	55.8%	57.0%	57.3%	58.6%
▬ Microsoft	47.3%	50.8%	53.8%	54.2%	54.7%	55.4%	55.6%	55.9%	56.2%
▬ Eset	44.7%	56.0%	58.2%	59.1%	60.1%	61.3%	62.7%	63.4%	64.6%
▬ Kaspersky	41.5%	47.1%	49.4%	50.5%	55.9%	56.9%	57.1%	58.0%	59.2%
▬ AVG	30.5%	41.4%	43.7%	46.3%	54.5%	57.0%	58.2%	58.8%	59.4%

FIGURE 3: TIME TO PROTECT HISTOGRAM

Cumulative protection rates are listed for the "zero hour" and then daily until blocked or the test ended. Final protection scores for the URL test duration are summarized under the "Total" column. Generally, at least half of a product's total protection was achieved in the zero hour, and better products had a higher percentage of zero-hour blocks. The lowest performing product stopped just 30% of 0-hr malware (AVG), while the highest performing stopped 76.4% (Trend Micro).

2.5 Average Response Time to Block Malware

In order to protect the most people, a security product must be both fast (i.e. quick to react) and accurate. The graph below answers the question: How long on average must a user wait before a visited malicious site is blocked? The results show a range between 3.3 and 28.5 hours for the 11 tested vendors.

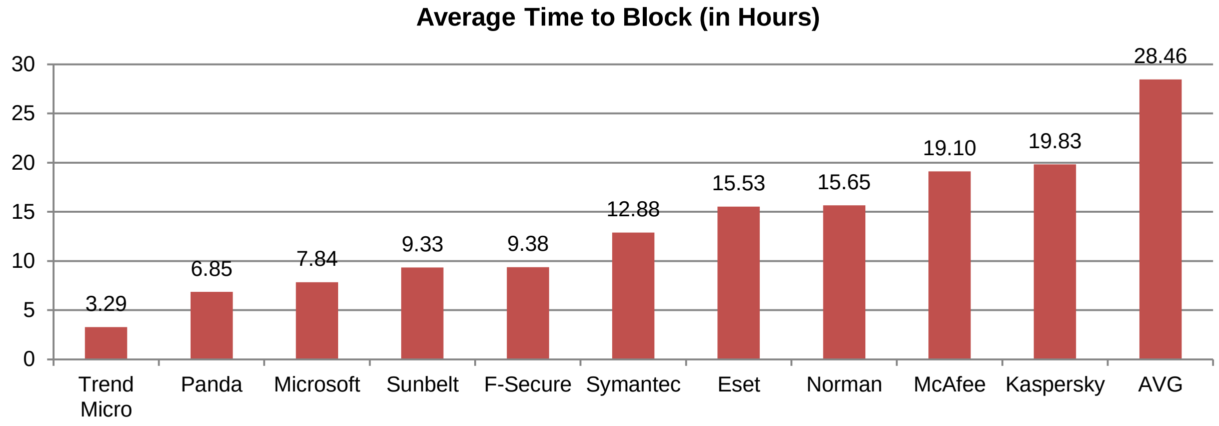


FIGURE 4: AVERAGE TIME TO BLOCK MALICIOUS SITES

The mean time to add protection for a malicious site (if it was blocked at all) was 13.5 hours. Smaller numbers are better. Note that the Average Time to Block (Figure 4) should be read in conjunction with the Histogram (Figure 3) to interpret the results within the correct context.

2.6 Comparing Results from Last Year

Are security products keeping up with cybercriminals? The table below shows the block on download and execution results from the current Q3 2010 test vs. our Q3 2009 test, as well as the net change. It seems the cybercriminals are pulling ahead of the defenders. Indeed, our findings reflect the growing trends in the explosion of malware that have been chronicled by the same vendors under test.

Malware Prevention Over Time

Product	Q3 2009	Q3 2010	Change
Trend Micro	96.4%	90.1%	-6.3%
McAfee	81.6%	85.2%	3.6%
F-Secure	80.0%	80.4%	0.4%
Norman	81.2%	77.2%	-4.0%
Sunbelt	NA	75.3%	NA
Microsoft	NA	75.0%	NA
Panda	72.0%	73.1%	1.1%
Symantec / Norton	81.8%	72.3%	-9.5%
Kaspersky	87.8%	71.3%	-16.5%
Eset	67.9%	60.0%	-7.9%
AVG	73.3%	54.8%	-18.5%
Average	*80.2%*	*74.1%*	*-6.4%*

TABLE 4: BLOCK ON DOWNLOAD AND EXECUTION RATE—Q3 2010 VS. Q3 2009 TEST RESULTS

In general most products protection declined slightly over the last twelve months, with a couple exceptions. McAfee was the only product to significantly improve (+3.6%). The biggest declines were posted by AVG and Kaspersky at 18.5% and 16.5%, respectively. Even top performer Trend Micro slipped 6%.

2.7 METHODOLOGY

NSS Labs has developed a unique "Live in-the-Cloud" testing framework that emulates the experience of average users. The earlier the protection, the more proactive it can be considered. Thus, NSS Labs tests malware protection at each of three unique stages as follows.

Stages of Prevention	% Blocked
1. URL/File Access (Reputation)	A
2. Download	B
3. Execution	C
Overall Protection	A+B+C = 100% maximum

TABLE 5: STAGES OF PREVENTION

Our Live Testing framework focuses on threats currently active on the Internet gathered from our extensive global intelligence network. Recurring testing introduces malware into the test harness within minutes of discovery and repeats the testing cumulatively every 6 hours, each time adding newly found malicious sites. Over a period of 11 days, from August 22, 2010 to September 1, 2010, NSS Labs engineers ran 57,000 tests of 3,433 unique malicious URLs. Removing clean URLs from the mix, the following results are based on 1,122 malicious sites.

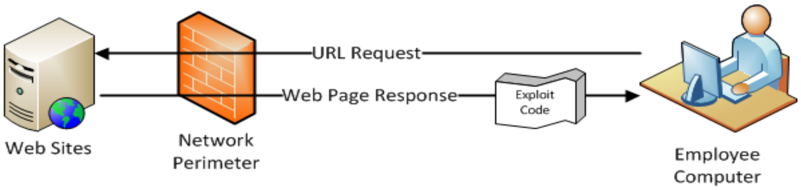
False positive testing: It is important that security products do not block legitimate content. In our testing we subjected the products to 1,000 different clean URLs and file downloads. Using default settings, typical of consumer environments, we did not register any false positive alarms. However, it is possible that more aggressive settings could generate false positives, but that was beyond the scope of this analysis.

3 Exploit Protection

There is a widely-held belief that as long as a user does not visit the "shady" parts of the Internet, he/she is not at risk from attacks. This is patently false; End users are at risk no matter where they surf. Even sites like the *Wall Street Journal*, the *New York Times*, and MLB.com have served up malicious content to their readers.

3.1 The Threat

Client-side exploits. These attacks rely upon users visiting infected websites in order to exploit web browsers, browser plug-ins, and add-on applications such as Adobe Acrobat and Flash. Once the desktop PC has been compromised, the attacker uses that machine to attack others—either remotely as part of a "bot" or locally to gain corporate secrets including personal and financial information, such as credit cards, bank account access, passwords, social security numbers, etc.



These exploits represent the newest and most serious threats, since they occur silently, without user awareness, when a user visits a malicious website. However, they are currently in the minority, but growing at a fast pace.

3.2 Results

Exploit protection amongst the products ranged between 3.4% and 74.6% - in other words, generally poor. Over half of the AV products stop less than 50% of the exploit attacks. Put differently, a cybercriminal would have between 25% and 97% chance of successfully attacking your machine.

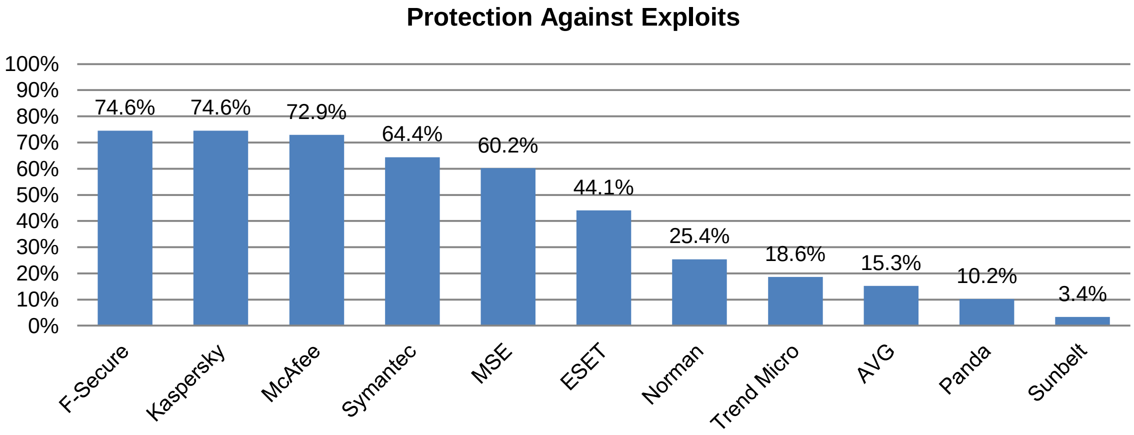


FIGURE 6: EXPLOIT BLOCK RATE

Given these results, users should adamantly apply the latest available patches to their operating system and applications. Disable or uninstall applications that you do not use or absolutely require, as these can provide unnecessary openings to attackers.

3.3 METHODOLOGY

These tests were performed using state-of-the-art penetration testing tools such as Metasploit in a controlled environment. They are designed to assess the raw exploit detection capabilities of the products, regardless of where the attacks are launched from. It should be noted that some vendors have reputation systems, which can block access to infected websites. While this technology may protect against certain specific sites, it will not protect against the raw type of attack, which can be delivered from billions of different internet addresses.

All 118 exploits were validated against live target systems and vulnerable applications. This is the largest test of its kind that has ever been publicly performed on consumer products. The samples include vulnerabilities such as:

- CVE-2010-0806: IEPeers.dll attack, which is used by Zeus, Stuxnet, and others.
- CVE-2010-0249: Internet explorer use-after-free attack, made popular in the Operation Aurora attack against Google and 100 other defense companies.
- CVE-2009-0927: Adobe Reader.
- CVE-2007-0015: Quicktime buffer overflow.

No evasions were used in this testing. In reality, cybercriminals use evasions actively to circumvent security products. Thus, the real-world results should be considerably worse.[2]

[2] Evasions are methods by which attacks can be made successful through disguise and obfuscation.

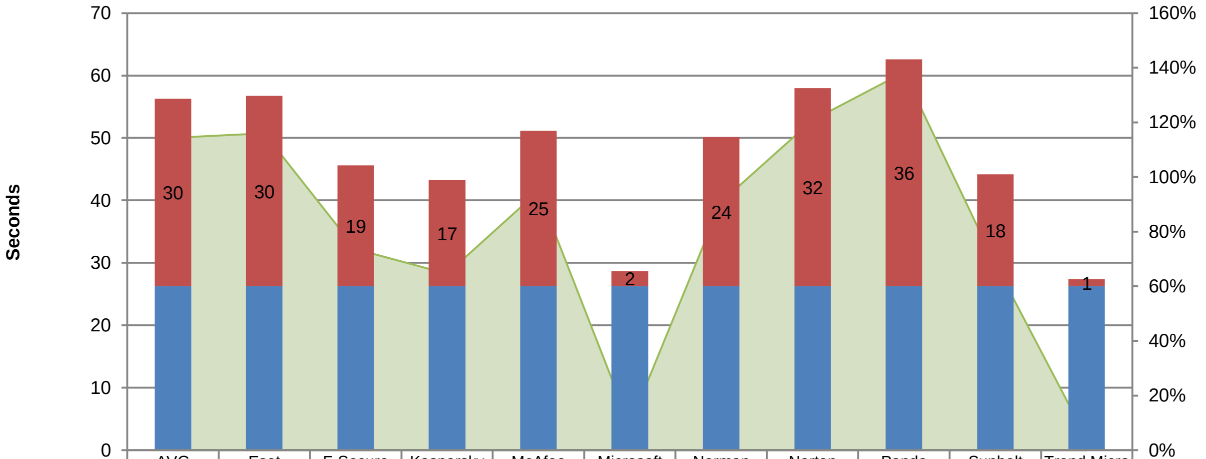
4 Performance Impact

Security products impact performance by slowing down the system and consuming memory that could be used for other applications. This is a necessary trade-off since some security processing must be performed. Some security products impacted certain applications more, and others less. While more effective solutions generally had a higher system impact, the reverse was not necessarily true; i.e. don’t assume that poor performance means you are getting better security.

We performed 500 warm starts for each application to ensure our results were accurate. The associated margin of error is 4.38% with 95% confidence. Thus, if our results show a 1 second increase, then 95 times out of 100, the results will be between 0.9562 and 1.0438 seconds.

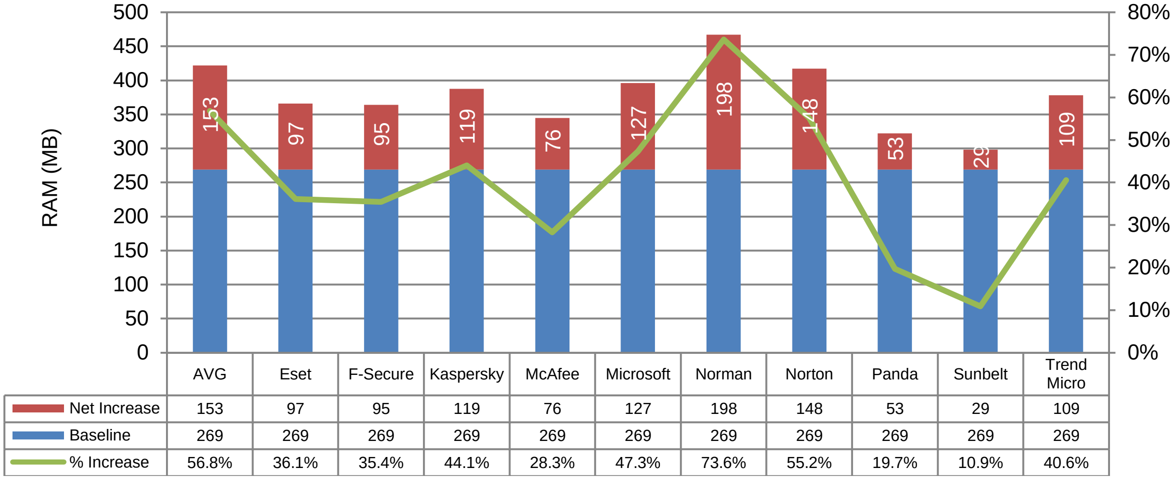
The following graphs show the baseline measurements with no security software installed, the net increase in time, and the % increase. Generally, differences less than half a second are difficult for users to perceive and should have minimal impact.

4.1 Boot Time



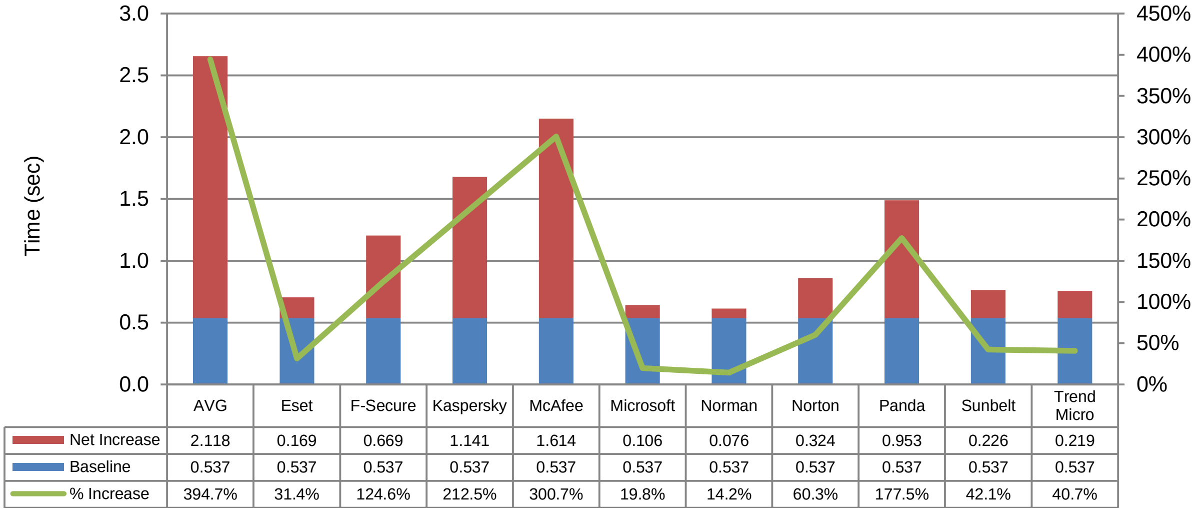
	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	Trend Micro
🟩 % Increase	114.3%	116.0%	73.6%	64.6%	94.8%	9.3%	90.9%	120.8%	138.3%	68.1%	4.3%
🟥 Net Increase	30.0	30.5	19.3	17.0	24.9	2.4	23.9	31.7	36.3	17.9	1.1
🟦 Baseline	26.3	26.3	26.3	26.3	26.3	26.3	26.3	26.3	26.3	26.3	26.3

4.2 Memory Utilization When Idle



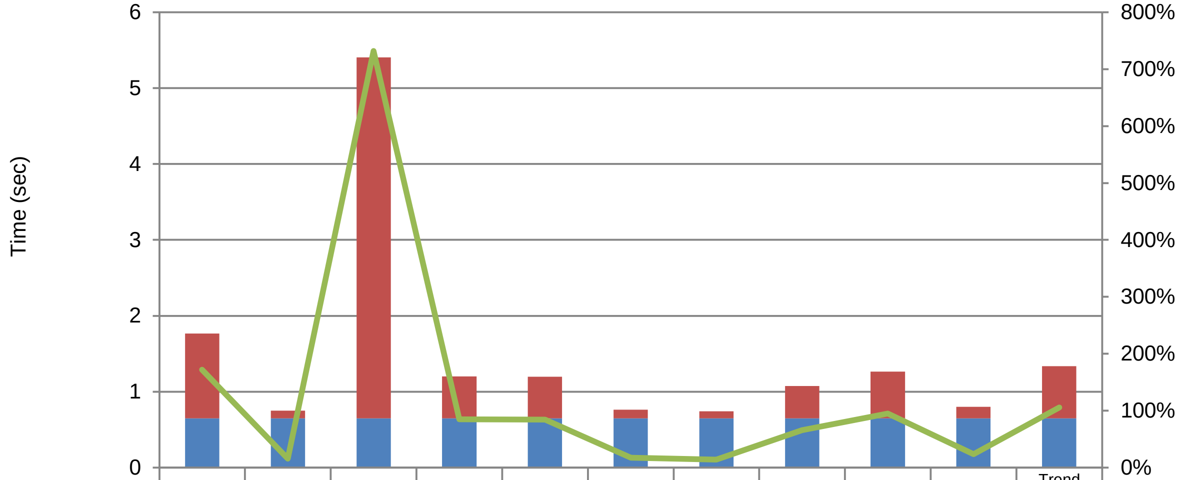
	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	Trend Micro
🟥 Net Increase	153	97	95	119	76	127	198	148	53	29	109
🟦 Baseline	269	269	269	269	269	269	269	269	269	269	269
🟩 % Increase	56.8%	36.1%	35.4%	44.1%	28.3%	47.3%	73.6%	55.2%	19.7%	10.9%	40.6%

4.3 Outlook 2007



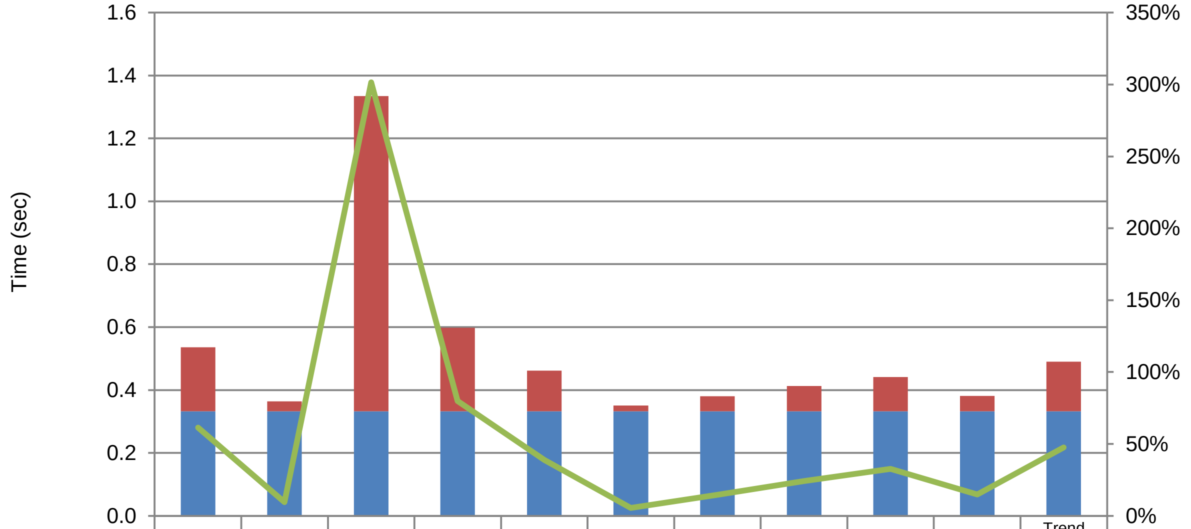
	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	Trend Micro
🟥 Net Increase	2.118	0.169	0.669	1.141	1.614	0.106	0.076	0.324	0.953	0.226	0.219
🟦 Baseline	0.537	0.537	0.537	0.537	0.537	0.537	0.537	0.537	0.537	0.537	0.537
🟩 % Increase	394.7%	31.4%	124.6%	212.5%	300.7%	19.8%	14.2%	60.3%	177.5%	42.1%	40.7%

4.4 Internet Explorer 8



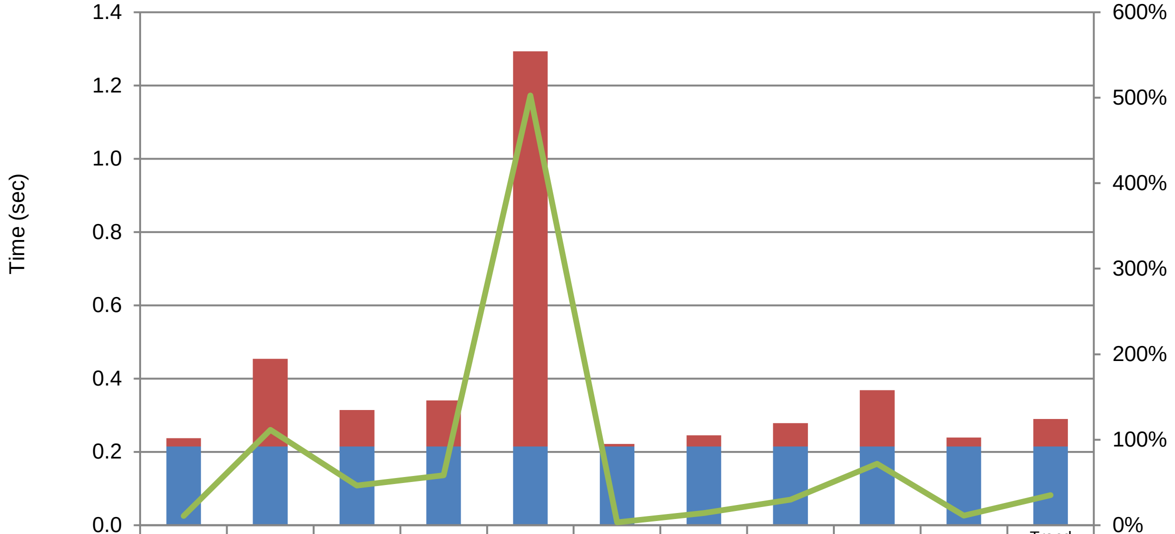
	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	Trend Micro
🟥 Net Increase	1.117	0.100	4.758	0.553	0.549	0.114	0.091	0.426	0.616	0.151	0.687
🟦 Baseline	0.650	0.650	0.650	0.650	0.650	0.650	0.650	0.650	0.650	0.650	0.650
🟩 % Increase	171.8%	15.5%	732.0%	85.0%	84.4%	17.5%	14.0%	65.5%	94.8%	23.3%	105.8%

4.5 Firefox 3.6



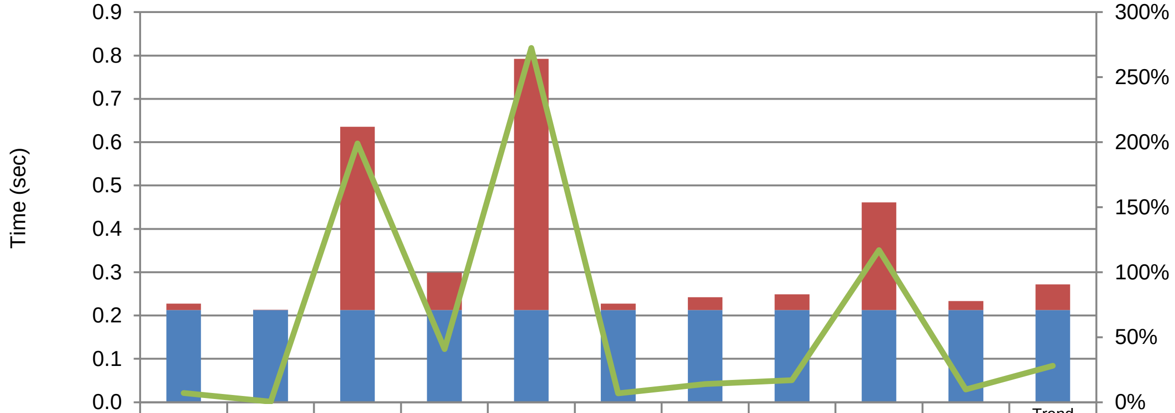
	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	Trend Micro
🟥 Net Increase	0.204	0.031	1.002	0.266	0.129	0.018	0.048	0.081	0.109	0.049	0.158
🟦 Baseline	0.332	0.332	0.332	0.332	0.332	0.332	0.332	0.332	0.332	0.332	0.332
🟩 % Increase	61.4%	9.5%	301.5%	79.9%	38.8%	5.4%	14.5%	24.3%	32.7%	14.9%	47.6%

4.6 Word 2007



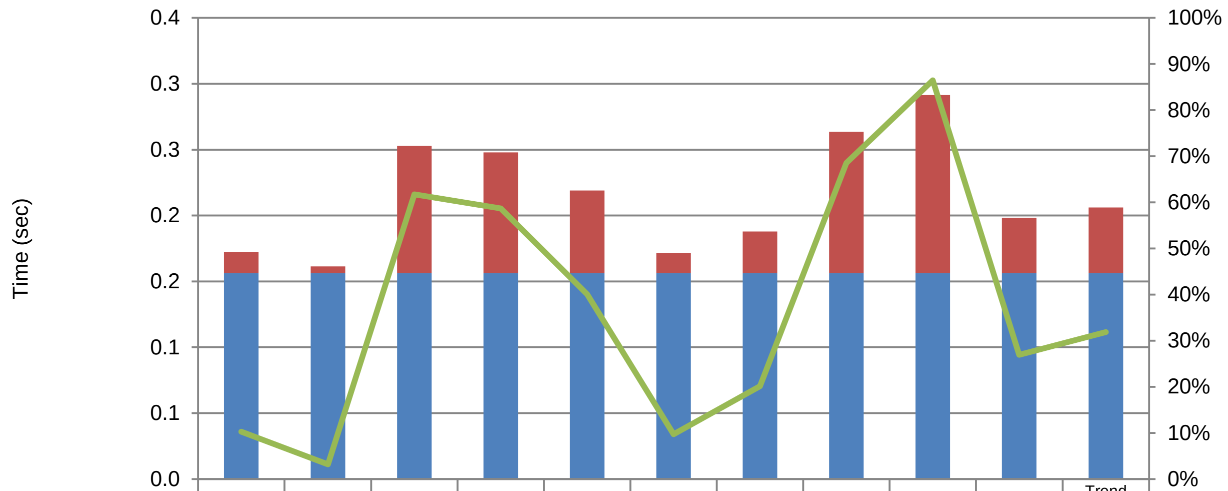
	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	Trend Micro
🟥 Net Increase	0.023	0.240	0.099	0.125	1.079	0.007	0.031	0.064	0.154	0.024	0.075
🟦 Baseline	0.215	0.215	0.215	0.215	0.215	0.215	0.215	0.215	0.215	0.215	0.215
🟩 % Increase	10.6%	111.6%	46.2%	58.4%	502.7%	3.4%	14.2%	29.8%	71.8%	11.2%	35.1%

4.7 Excel 2007



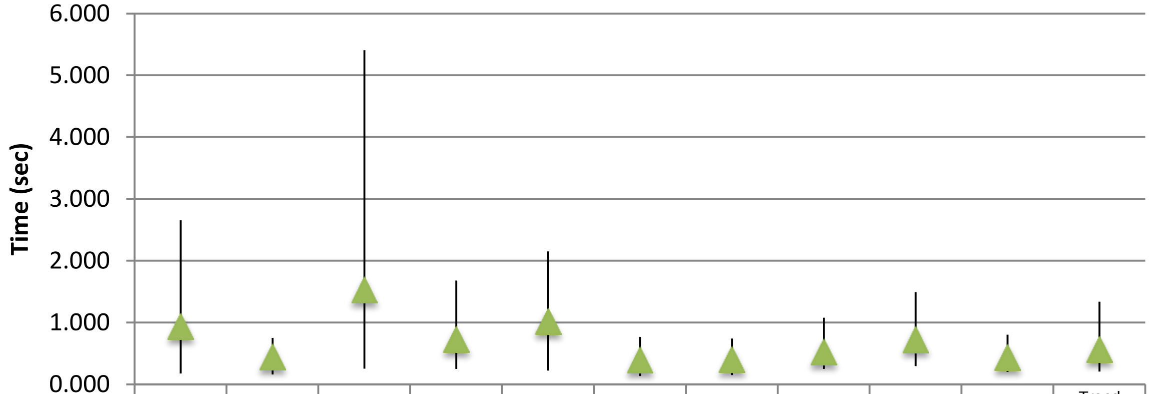
	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	Trend Micro
🟥 Net Increase	0.015	0.001	0.423	0.087	0.579	0.015	0.030	0.036	0.249	0.021	0.059
🟦 Baseline	0.213	0.213	0.213	0.213	0.213	0.213	0.213	0.213	0.213	0.213	0.213
🟩 % Increase	7.0%	0.4%	198.9%	40.8%	272.5%	6.9%	14.1%	17.0%	116.9%	9.8%	27.9%

4.8 Adobe Acrobat Reader 9



	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	Trend Micro
🟥 Net Increase	0.016	0.005	0.097	0.092	0.063	0.015	0.031	0.107	0.135	0.042	0.050
🟦 Baseline	0.156	0.156	0.156	0.156	0.156	0.156	0.156	0.156	0.156	0.156	0.156
━ % Increase	10.3%	3.2%	61.8%	58.7%	40.1%	9.7%	20.1%	68.5%	86.5%	26.9%	31.9%

4.9 Average net time increase to start an application



	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	Trend Micro
Hi	2.655	0.750	5.408	1.677	2.151	0.764	0.741	1.076	1.490	0.801	1.337
Low	0.172	0.161	0.253	0.248	0.219	0.171	0.188	0.249	0.291	0.198	0.206
▲Average	0.933	0.441	1.525	0.728	1.019	0.396	0.402	0.523	0.720	0.436	0.559
% Increase	166.1%	26.0%	335.2%	107.6%	190.8%	13.1%	14.6%	49.3%	105.4%	24.4%	59.4%

Warm Start Applications

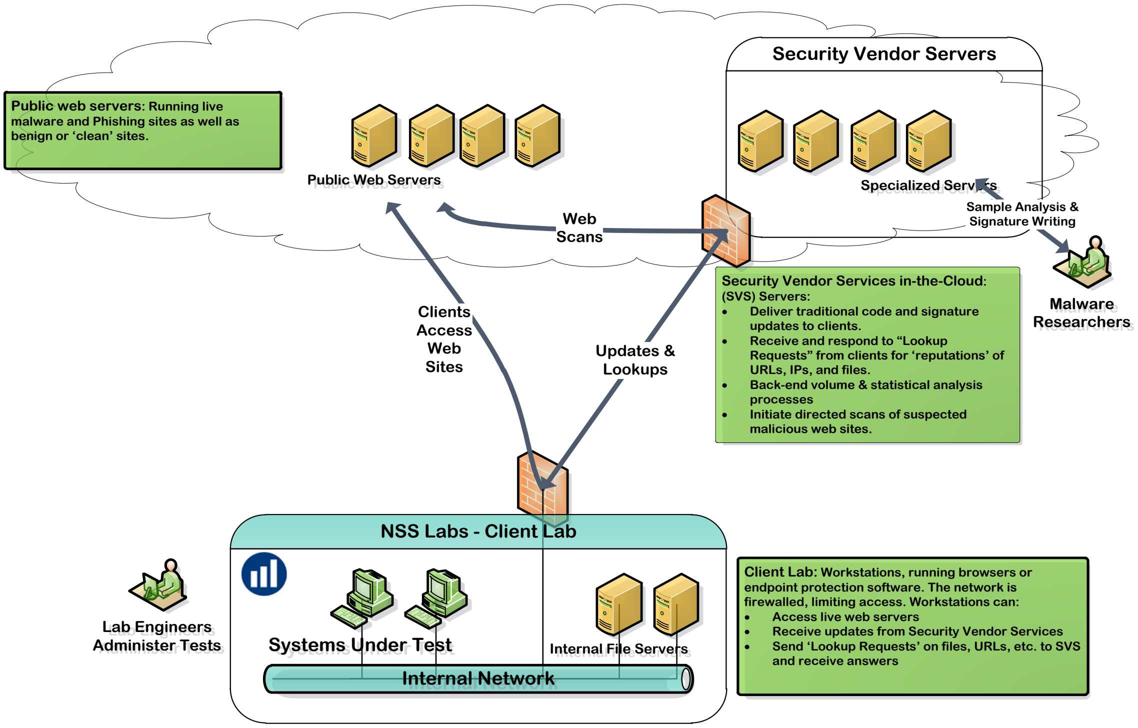
Several products demonstrated minimal levels of system impact. In order of impact, starting with the least: Microsoft, Norman, Sunbelt, Eset, Symantec, Trend Micro, Panda, Kaspersky, AVG, McAfee, F-Secure.

However, remember that security is the primary purchasing criteria. Of the most effective products, those in our 'Recommended' category, Trend Micro had the lowest impact.

APPENDIX A: MALWARE TEST ENVIRONMENT

Given the rapid rate and aggressiveness with which criminals propagate malware across the web, testing must occur quickly in order to reflect true user experiences. NSS Labs has developed a unique proprietary "Live Testing" harness and methodology.

All products were connected to the live internet and able to receive signature, software, and reputation updates or otherwise as delivered by the vendor. Products under test are subjected to live malware that is introduced into the test network via a URL request made via a web browser. All tests were executed in a highly controlled manner and results were meticulously recorded and archived at each interval of the test.



Public web servers: Running live malware and Phishing sites as well as benign or 'clean' sites.

Security Vendor Services in-the-Cloud: (SVS) Servers:

- Deliver traditional code and signature updates to clients.
- Receive and respond to "Lookup Requests" from clients for 'reputations' of URLs, IPs, and files.
- Back-end volume & statistical analysis processes
- Initiate directed scans of suspected malicious web sites.

Client Lab: Workstations, running browsers or endpoint protection software. The network is firewalled, limiting access. Workstations can:

- Access live web servers
- Receive updates from Security Vendor Services
- Send 'Lookup Requests' on files, URLs, etc. to SVS and receive answers

FIGURE 5: THE NSS LABS LIVE-IN-THE-CLOUD FRAMEWORK

Scoring of the products was measured at multiple stages of the user experience, as either blocked or not blocked. These stages are:

1. Reputation – is the user allowed to access the site
2. Download – is the malicious content blocked during download
3. Execution – should any malicious content be saved on the PC, is it prevented from executing

This test was performed continuously (24x7), every 6 hours, for a total of nine days. New samples were added as they were discovered, and previously discovered samples were retested.

False positive testing was also performed to ensure legitimate applications were not flagged as malicious by any of the anti-malware products. Periodically clean URLs were run through the system to verify that the products were not over-blocking.

Each threat is archived to ensure proper analysis before, during, and after the test. Illegitimate samples are removed from the final test results. A key innovation in anti-malware testing, NSS Labs performs sample validation (to ensure it is either malicious or clean) continually throughout the test. Multiple analysis techniques are utilized, including automated sandboxes, proprietary tools, and manual reverse engineering and analysis. This proprietary technique ensures the freshest malware can be included in our test, even before some vendors have enabled protection. Just like in the real world.

APPENDIX B: ABOUT NSS LABS, INC.

NSS Labs, Inc. is the world's leading independent information security research and testing organization. Its expert analyses provide information technology professionals with the unbiased data they need to select the right product for their organizations. Pioneering intrusion detection and prevention system testing with the publication of the first such test criteria in 1991, NSS Labs also evaluates firewall, unified threat management, anti-malware, encryption, web application firewall, and other technologies on a regular basis. The firm's real-world test methodology is the only one to assess security products against live Internet threats.

NSS Labs tests are considered the most aggressive in the industry and its recommendations are highly regarded by enterprises. Founded in 1991, the company has offices in Carlsbad, California and Austin, Texas.

Find out how NSS Labs can help your organization:

- Identify the best products at the best prices
- Optimize your security posture

Call: 760-412-4627

Email: advisor@nsslabs.com