TEST REPORT
Tolly.

#211133
November 2011
Commissioned by
Trend Micro, Inc.

Trend Micro Titanium Maximum Security 5.0

Consumer Endpoint Security Performance vs. K7 Computing, Kaspersky, McAfee & Symantec

Executive Summary

Endpoint security is an essential element of any Windows PC. As an "always-on" service, its resource requirements have the potential to impact and degrade user experience. Furthermore, the complexities of security configuration can be confusing to consumers, the vast majority of whom are non-technical.

Trend Micro has focused its Titanium Maximum Security 5.0 offering on providing effective endpoint security without requiring user configuration and without degrading the user experience.

Trend Micro, Inc. commissioned Tolly to benchmark the performance of Titanium Maximum Security 5.0 vs. consumer-class, Windows 7 32-bit security solutions from K7 Computing, Kaspersky, McAfee and Symantec. Specifically, this testing evaluated the impact each solution had on system resources and user experience in a number of common usage scenarios.

Testing showed that Trend Micro Titanium consistently scored at or near the top of the rankings in a series of tests that involved boot times, on-demand scanning, memory, CPU usage, and installation functions.

TEST HIGHLIGHTS

Trend Micro Titanium 5.0:

1 Demonstrated consistently efficient usage of system resources

2 Implemented the smallest installer among the products tested

3 Delivered the fastest boot and shutdown time of all products tested

4 Demonstrated the lowest memory and fastest completion time when performing a full scan

5 Showed the lowest impact on installing third-party programs

6 Implemented easy-to-use, rich feature set in addition to essential threat protection

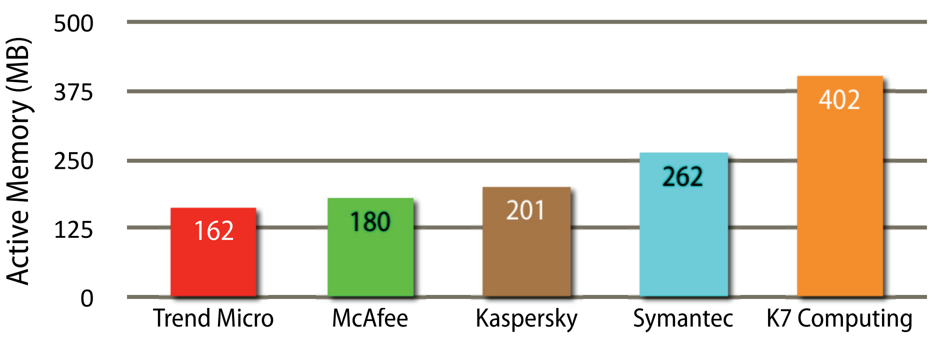
Introduction

In order to determine the system resource impact, and consequently, the impact on the end-user experience over the course of a product's lifetime, Tolly engineers put each endpoint security offering through a battery of tests.

Tests included one-time tasks such as the installation of both the endpoint security system and third-party software, as well as common tasks such as system booting/shutdown and manual disk scans.

<continued on next page...>

Endpoint Security Systems: Full Scan Memory Usage
(Lower numbers are better)



Note: Active memory was measured using the Poolmon utility, configured to monitor the unique kernel tags of each individual product, added to the perfmon counter for the applicable system services.

Source: Tolly, October 2011

Figure 1

Introduction (Cont'd)

Trend Micro Titanium consistently ranked at or near the top performers in each of the reported tests, supporting the company's claim that Titanium has been designed to deliver optimal performance to the user.

In addition, Trend Micro continues to offer a rich and user-friendly feature set, protecting users from many angles of attack while optimizing user experience with both quick and easy defaults, and a suite of advanced yet essential tools.

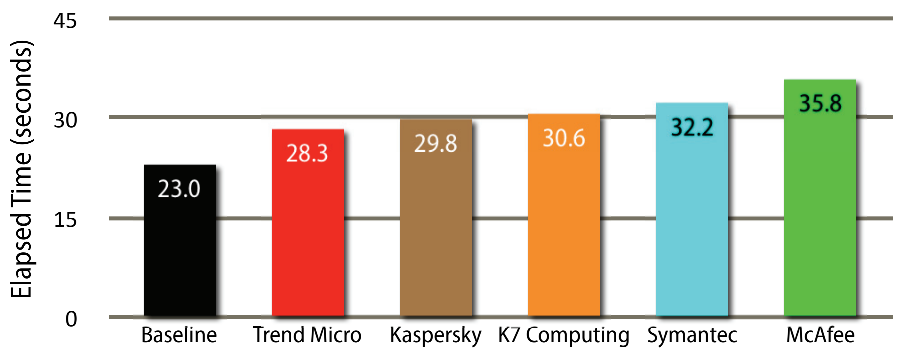
Boot Time

In order to provide effective protection, security software needs to load several components during the boot sequence. Loading additional modules, however, can extend the time required to complete the system boot and make the system available to the user.

This test measured the time required to boot the computer from an "Off" state, up to the point where the Windows 7 was fully initialized and the desktop could accept user input.

Measured using the Microsoft Velocity Test Suite, Trend Micro Titanium completed the boot process in the least time of any products tested in just over 28 seconds, compared to the baseline (no endpoint security installed) time of 23 seconds. See Figure 2.

Endpoint Security Systems: Windows 7 Boot Complete
As Reported by Microsoft's Velocity Test Suite
(Lower numbers are better)



Source: Tolly, October 2011

Figure 2

Products such as Kaspersky and K7 Computing increase the boot time to 29.8 seconds and 30.6 seconds, respectively. McAfee's Total Protection impacted the baseline time by 56%, more than any product tested.

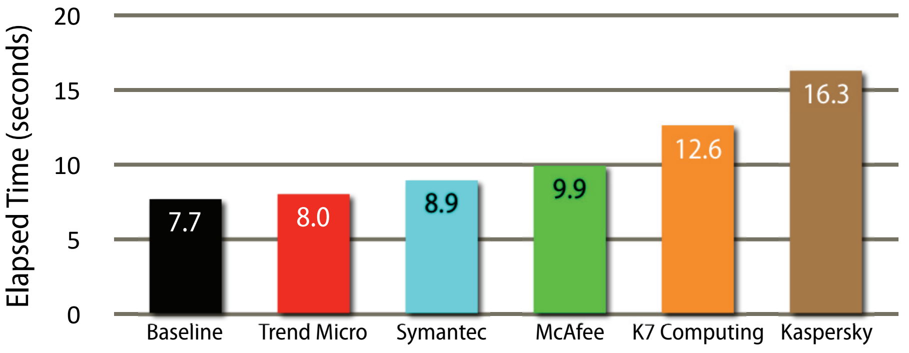
Shutdown Time

Just as starting all applicable product services on a PC will influence boot times, shutdown requires the graceful termination of all the program's components to ensure there is no data corruption, the duration of which typically depends on the number of services associated with a solution.

Again run as part of Microsoft's Velocity Test Suite, the test measured the time needed to shutdown the machine completely from an idle state. With the baseline set at 7.7 seconds, Trend Micro Titanium 5.0 only required an additional 0.3 seconds, completing the operation in 8.0 seconds.

In 2nd place, Symantec Norton 360 impacted the baseline performance by 1.2 seconds, a 15% increase. On the other end of the spectrum, Kaspersky PURE, the second fastest solution in the boot tests, more than doubled the shutdown time, clocking in at 16.3 seconds. See Figure 3.

Endpoint Security Systems: Windows 7 Shutdown
As Reported by Microsoft's Velocity Test Suite
(Lower numbers are better)



Source: Tolly, October 2011

Figure 3

Solution Footprint - Idle Memory

Even when the security solution is idle, it is active in the system and using system resources - and the most precious of these resources is system memory. While disk sizes have grown dramatically and multi-core processors are increasingly common, system random access memory (RAM) is still relatively limited. Memory actively occupied by the security solution is unavailable for application use.

Results across vendors varied by almost a factor of 5 with the Trend Micro solution using the least amount of RAM at 33MB, followed by Kaspersky at 39.5MB. Results are the sum of all active memory consumed by all system processes and the non-paged memory allocated by each of the applicable kernel processes. See Figure 4.

McAfee, Symantec and K7 Computing required increasingly larger amounts of memory with K7 requiring the most at nearly 160MB, a significant amount of the installed memory of the test system.

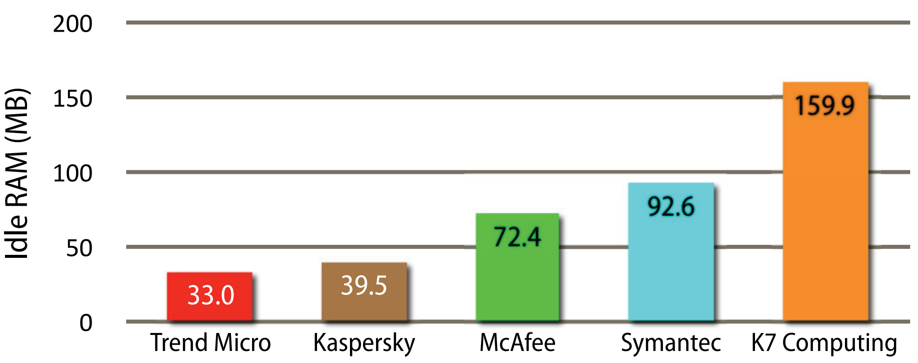
Solution Footprint - Idle CPU

While memory consumption is important, a solution's idle CPU utilization is also an important consideration. Even with multi-core CPUs becoming commonplace, non-optimized processes can decrease responsiveness of other applications and even cause increased power usage.

On an idle machine equipped with an Intel Core 2 Quad processor (four core), engineers observed the CPU utilization at 0.1%. Trend Micro increased this by a modest 0.1%, taking a total of 0.2% of the CPU. Likewise Kaspersky required just 0.3% of the CPU when at idle. See Figure 5.

Symantec and K7 Computing, on the other hand, required 1.6% and 1.7%, respectively, of the CPU when idle. While this may not seem like a dramatic increase in the test system, it would translate to a sizable impact if attempted on an older, single core system.

Endpoint Security Systems: Solution Idle Memory Footprint
(Lower numbers are better)



Note: Idle memory was gathered using the Poolmon utility, configured to monitor the unique kernel tags of each individual product, added to the perfmon counter for the product services.

Source: Tolly, October 2011

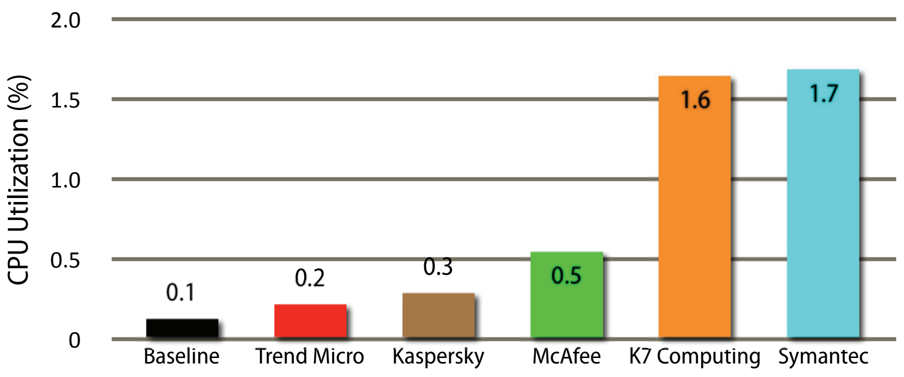
Figure 4

Full Scan Performance/Memory Footprint

While all of the solutions tested provide for scheduled scans of the system, there are times when users will require an on-demand (manual) scan. It is useful to understand the demands that the security solution makes on the system during such a scan because a lower scan time and busy memory usage during a scan means more of both are available to do multiple things simultaneously with your PC.

Each of the solutions tested offered an option for a full system scan but as the scope of such scans varied across systems,

Endpoint Security Systems: CPU at Idle
As Reported by Microsoft's Velocity Test Suite
(Lower numbers are better)



Source: Tolly, October 2011

Figure 5

testers configured each solution to run a full scan of the two installed drives.

Testers gathered memory usage for all products by running the product's full scan function for the entire duration, recording user memory with Performance Monitor, using the kernel tag method to extract more granular memory utilization data.

The full scan test was the most complex of the series as results were measured in multiple ways that included the time to complete and memory utilization.

Figures 1, 6, and 7 illustrate summary results for separate but related tests.

The data in Figure 1 (page 1) represents the average memory usage of each product during the full scan - the scope and duration of which, as noted earlier, varied across products.

The first full scan, illustrated in Figure 6 was focused on determining the amount of time required to scan the client machine when there was no preexisting cache.

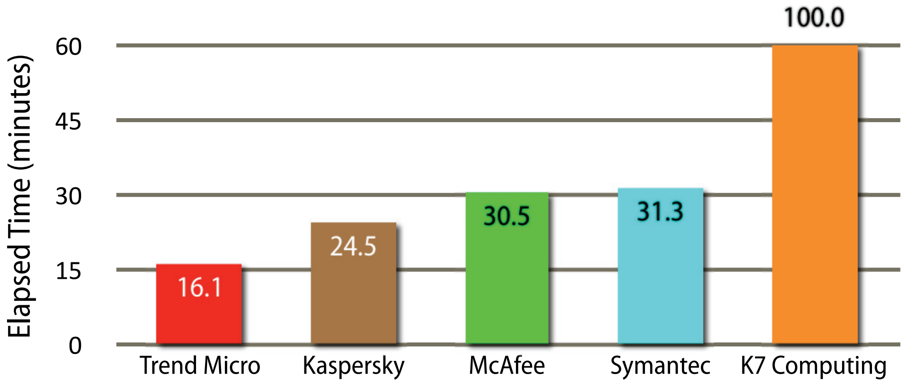
Results show that Trend Micro has the lowest memory utilization and run time for the first full-drive scan. The first scan is important in allowing many programs to build a cache of the file system, optimizing future scans. Trend Micro completed the initial scan in just over 16 minutes, the closest competitor, Kaspersky, required 52% longer. K7 Computing took the longest by far, requiring an hour and forty minutes to complete the initial scan, while consuming more than twice the active memory of the Trend Micro solution.

In addition to scanning the approximately 75,000 files residing on the drives, the security products automatically include other objects in the custom scan, such as registry entries, DLL files, etc.

Irrespective of scope, it can be seen that all of the other offerings consume from 18 to over 200MB more active RAM when running a full scan than Trend Micro, and take considerably longer.

Endpoint Security Systems: First Full System Scan Time

(Lower numbers are better)



Note: In order to better view the differences among products, the Y-axis range has been set to 60 minutes. K7 Computing required 100 minutes to finish the test.

Source: Tolly, October 2011

Figure 6

During the subsequent full scans, Trend Micro once again completed swiftly, requiring only 27 seconds to check-up on the system. This is possible due to the aforementioned caching mechanisms in place.

All but one vendor incorporated this functionality, resulting in significantly shorter scans, with the exception of K7 Computing, which needed another full hour and forty minutes to complete each subsequent scan.

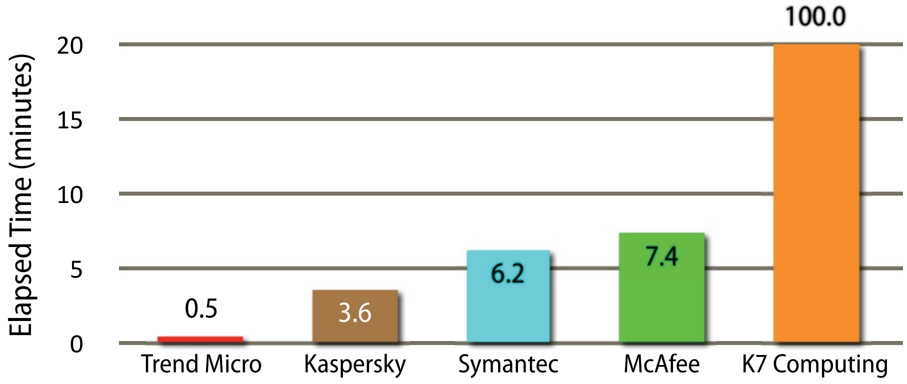
Third-Party Application Installation

Engineers also benchmarked the run time of installing and then removing a Microsoft .Net framework component that was packaged using that Microsoft Installer (MSI) utility.

Against a baseline measurement of 25.5 seconds for the install process, Trend Micro

Endpoint Security Systems: Repeated Full System Scan Time

(Lower numbers are better)



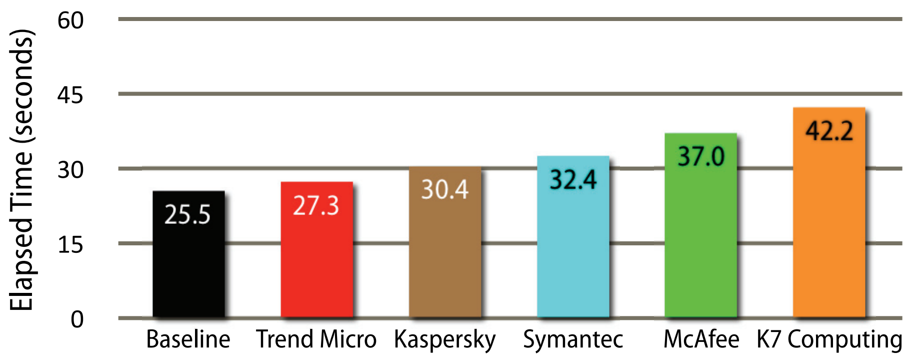
Note: In order to better view the differences among products, the Y-axis range has been set to 60 minutes. K7 Computing required 100 minutes to finish the test.

Source: Tolly, October 2011

Figure 7

Endpoint Security Systems: MSI Installation Time

(Lower numbers are better)



Source: Tolly, October 2011

Figure 8

Trend Micro, Inc.

Titanium Maximum Security 5.0

Endpoint Security Performance

Tolly. Certified

Tested October 2011

delivered the best result adding less than two seconds of overhead to the process. Most of the other vendors results were in the range of 30 to 37 seconds for the install. K7 Computing took longest to complete this process, requiring 42.2 seconds for the full installation. See Figure 8.

While the elapsed times were relatively short, testers note that install overhead could become a bigger issue when installing a complex product that would have a much longer baseline install time.

Installation and Disk Usage

Tolly engineers noted the installer size and disk requirements for the solutions under test. Trend Micro packages Titanium as a small downloader program that, when run, initiates a download of install packages, the combined size of which was 62.3MB, the smallest among the solutions. Other solutions, such as McAfee and Symantec also deliver a downloader, but the totals are much larger, taking 126MB for Symantec and 187MB for McAfee. See Figure 9.

The actual installation time varied for all products, but as a one-time operation, the impact to the end-user is limited. Engineers timed the installation of each solution. In the event that a product was provided as a downloader, the installation download was added to the total time needed to complete the install, assuming a download speed of 5Mbps for all vendors. See Figure 10.

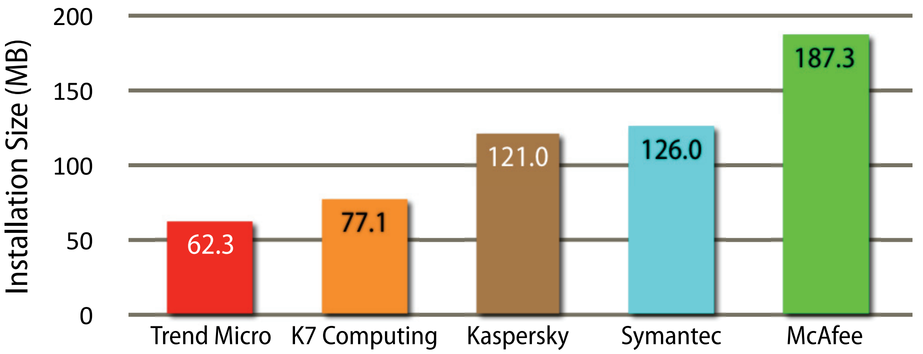
The K7 Computing solution required the least combined download and install time, completing the process in under 3 minutes, primarily due to the inclusion of the whole product package and small installer size, as opposed to needing to download the files inside the installer. Likewise Kaspersky does not need to download any files during the actual product install. However, a larger initial download size, combined with a lengthier install process, landed it in second-to-last place, at approximately 6 minutes.

Of the products that offered an up-to-date downloader, Trend Micro offered the lowest total installation time, requiring just over three and a half minutes. McAfee, using this same up-to-date delivery method, needed over seven minutes to fully install the product, the majority spent downloading the current packages.

Once installed, the solutions require between 250MB to 1300MB of disk space

Endpoint Security Systems: Solution Installer Size

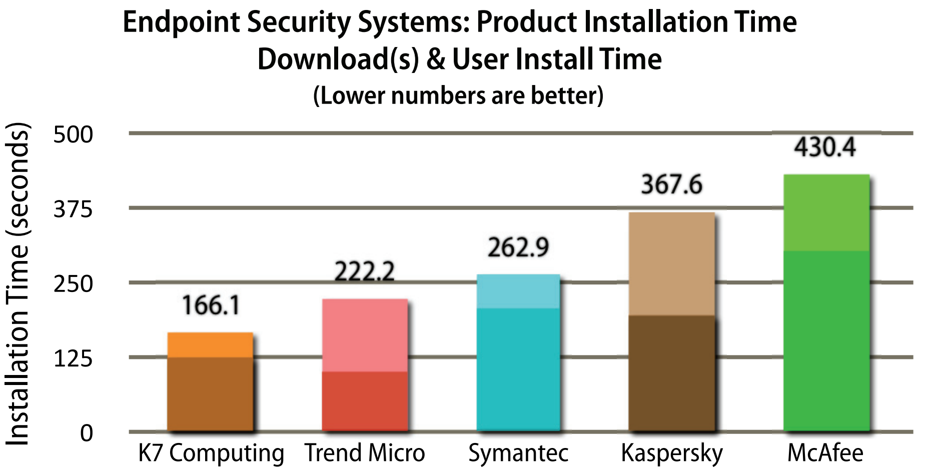
(Lower numbers are better)



Note: Where product installers consisted of downloaders, the initial package size plus the downloaded data size is reported.

Source: Tolly, October 2011

Figure 9



Notes: Total time taken to download and install product fully is reported above product. Product two-step and three-step download and install times are indicated by different shades. The darker shade indicates the time needed to download all installation files at a rate of 5Mbps. The lighter shade represents the actual time to install the solution to disk.

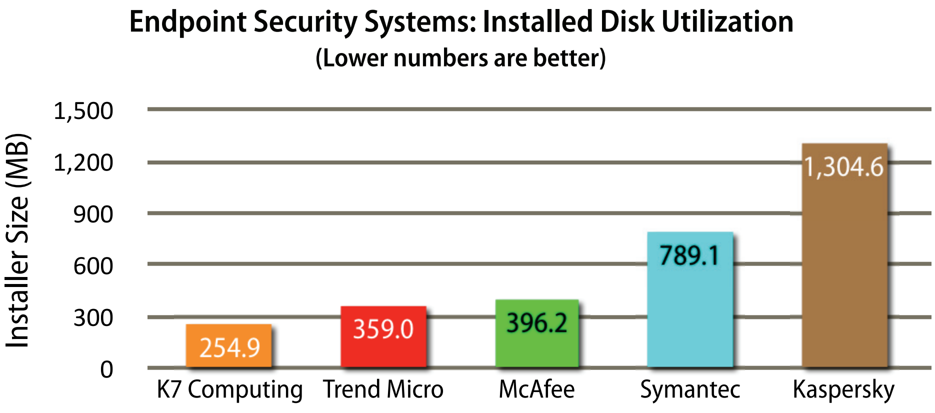
Source: Tolly, October 2011

Figure 10

with Trend Micro in second place, requiring 359MB, K7 Computing the lowest and Kaspersky the highest by far, using over 1GB of disk space on the client. See Figure 11.

Endpoint Security Feature Comparison

Endpoint security has evolved immensely since its start as standalone anti-virus (AV), its only purpose being to scan a user's computer for malware, and little else. Since these humble beginnings, AV vendors have been called upon to mitigate the ever-increasing risks posed to consumers, adding real-time and rootkit scanning, advanced firewalls and Intrusion Prevention Systems (IPS), and finally leveraging the cloud to deliver real-time protection to users around the globe.



Note: System was snapshotted immediately prior to the product installation, where the installer had already been downloaded. After installation, the systems were rebooted, left idle for 5 minutes, then differenced.

Source: Tolly, October 2011

Figure 11

Basic Functions

In the past two years, many vendors in this space have debuted services which provide security products with constantly-updated information to keep users safe, even in the event of a new virus outbreak. The global protection network, implemented by all vendors to some extent, continually gathers threat data from endpoints, identifying new threats and pushes updated information to the entire installed base. Expanding on this functionality, Trend Micro, Symantec, McAfee, and Kaspersky have created online repositories, consisting of billions of files, from which the reputation (integrity) of any given file can be queried. Products which implement both technologies lend to the creation of a global shield which protects each and every endpoint.

All Endpoint security products tested provide the basic full and real-time scan tasks; however vendors will implement these in different ways. While the most thorough scan involves checking each and every file on the system, this is usually unnecessary, as not every file has been modified since the last scan. To increase efficiency and performance when scanning, vendors have implemented caching to keep track of and skip unchanged files, cutting back on system resource usage while providing the same protection. K7 Computing was the only product which did not implement caching for on-demand scans.

Internet Security

The most common way for a user to access the Internet is through a web browser, email, or a chat client (AIM, Skype, etc). That being the case, vendors must be able to protect users from any malicious files delivered over this medium. All security products tested automatically scan all file downloads, attachments, and file transfers for malicious content, as well as guarding against spam and phishing attacks.

When navigating with a web browser, users need to be protected from fraudulent or untrusted sites, and while many browsers today implement this security, Trend Micro, Symantec, McAfee, and Kaspersky include a page rating service, which automatically scores a site with regards to its security. Trend Micro supplements this with its Web Reputation Service, which is capable of evaluating URLs in searches or while browsing, in emails or instant messages, providing the same web threat protection, and blocking access to known malicious sites.

On the other end, these security suites also protect against hackers actively trying to break in to a system, and keep users protected by verifying the integrity of the local network. Taking the form of an Intrusion Defense System (IDS) and Firewall, all security products tested incorporate both of these, all fully-customizable to the user. While Trend Micro does not integrate a standalone firewall implementation, it leverages the existing Windows Firewall, adding Behavior Monitoring, IDS, and Exploit detection while minimizing the system impact.

Malware Protection

Advanced mechanisms for malware detection include behavior monitoring, sandboxing (or emulation), and rootkit detection. These features allow security products to identify a threat, even if no preexisting record exists. With behavior monitoring, security products monitor the system, looking for any abnormal changes, identifying and blocking the process or program responsible, while the rootkit detection scans for any malware which has manifested in the system registry. All security suites tested incorporate support for behavior monitoring and rootkit detection.

Another feature which has made its way into endpoint security products lately is sandboxing. This allows the computer to open a file or application in a quasi-virtual environment on top of the OS, protecting system files from being altered by potentially-malicious programs. Kaspersky features sandboxing as part of its suite, allowing users to choose applications which run in a protected virtual environment, while Trend Micro incorporates a lightweight emulation of this technology.

Despite the focus on internet security, not all threats arrive this way. A USB drive, for example, used on an infected host, can be used as a carrier, delivering its payload wherever it may be plugged in. While this used to be a problem, all vendors now host autorun protection, and include tools to clean harmful files from removable media.

Data Protection

Data security is one of the most important aspects a security solution can provide, especially with the recent explosion of identity theft. Even in the event of a user's system being compromised, the data it contains must remain off-limits to prying eyes. Security vendors have devised several ways to mask user input, through keystroke encryption (Trend Micro) or a virtual keyboard (K7 Computing and Kaspersky), and full online credential management (Symantec and Kaspersky).

In the event that a user's system is compromised or stolen, and has sensitive data on it, a user will want to protect that data from being accessed at all. Trend Micro, McAfee, and Kaspersky all facilitate the creation of locally-encrypted files and folders for protecting sensitive data. However, Trend Micro takes this functionality a step further, allowing users the capability of locking their vault (encrypted folder) remotely in the event of a theft. Additionally, all the products tested, with the exception of Symantec, include a means of securely deleting files and folders, such that they cannot be recovered.

Supplementary Features

In the past year, many products have debuted new features to stay current with consumer habits and maintain security effectiveness against the ever-evolving virus threat. Trend Micro has implemented a "social media scanner", capable of checking the reputation of links embedded in a variety of social networking sites, which supplements the suite of advanced browser tools already present in the solutions. Symantec implements similar functionality, however it is more closely related to page rankings and needs to be invoked by the user. All products, with the exception of K7 Computing, are equipped with a browser toolbar to facilitate security functions when online.

Parental controls have come a long way in the past few years with the incorporation of web reputation and page ranking services into the security suites, many vendors are now able to easily classify content, restricting it based on a set of categories. Trend Micro and McAfee can define website filters by content categories, easily creating customized policies for different family members. Symantec and Kaspersky incorporate a subset of these categories, but also allow for a detailed log of online interactions and chats. Trend Micro also offers this feature as part of its Online Guardian product. Additionally, Kaspersky can allow/block communications to contacts in both IM applications and online social networks. It is important to note that K7 Computing has parental controls, but it is based on blocking a list of URLs, which the user must enter manually.

While all solutions tested facilitate local backups, only Trend Micro, McAfee, and Symantec are complemented with online backup services, allowing users to maintain current backups of sensitive information while untethered from an external hard drive. K7 Computing only provides local backups, a largely redundant capability, since Windows Backup already provides this. Additionally, Kaspersky supports backup to a FTP server, but is not configured with a backup service out-of-box.

Other useful tools include the creation of a system rescue disk (Symantec and Kaspersky), a rootkit-check/clean disk (Trend Micro), and a system tuner (all products), which optimizes system performance and security to an extent. Kaspersky includes only a browser tuneup and a gaming mode (to reduce notifications), while Trend Micro, K7 Computing, McAfee, and Symantec offer built-in disk and registry optimization.

As the way we access the Internet continues to evolve, vendors must be conscious of threats beginning to target smartphones and tablet computers, to name a few. Trend Micro, McAfee, and Symantec all have security products which protect both Android and iOS platforms, and Kaspersky currently only supports Android, while K7 Computing has no support for either.

Reporting

While the majority of users will not need to utilize in-depth product reporting, it is important to provide detailed reporting in places such as parental controls, detection history, and an overall system status that the typical user can understand. All the products reviewed utilize a simplistic dashboard, providing an at-a-glance system status and recommended actions for maintaining system integrity. In addition, any user implementing parental controls will want an easy-to-digest summary of a child's online activity (Kaspersky and Symantec).

Kaspersky and McAfee also include a means of viewing the status of other installations on the network from a single machine. Kaspersky expands upon this, allowing a single machine to manage others, eliminating the need for independent management in a multi-PC home network.

Trend Micro boasts a unique feature called Root Cause Analysis Report. From any detection event, the built-in tool can trace the source of the infection, a useful tool for any advanced user.

Ease-of-Use

Each product's interface is more-than-adequate for the typical consumer, all the basic anti-virus functions are preconfigured with set tasks, allowing users to perform common activities with a few clicks. Advanced functions however, like defining parental controls or firewall exceptions are difficult to do in K7 Computing. The interface is designed for advanced users, requiring a user manually define each and every exception.

The breadth of configuration options varies considerably between products. While McAfee has very detailed logs and a wide feature set, the amount of customization is kept to a minimum. On the other end, K7 Computing supports very fine tuning, but is outside what the typical user can configure. This is not limited to these two products however, as vendors often face the challenge of expanding the feature set, without detracting from the overall usability of the solution.

That being said, Trend Micro, Kaspersky, Symantec and McAfee appear to be on relatively equal footing feature-wise, as each has gone above and beyond the basic requirements of security software, while allowing the user to interact and configure relevant aspects in an intuitive way.

Trend Micro has demonstrated its superior performance, partly due to the integration of smart scanning and its reputation services system-wide, while Kaspersky's parental control is unmatched in both ease-of-use and protection. Symantec has Identity Safe to easily protect all online transactions, with its Insight network gaining momentum, and McAfee, which, despite its simplistic appearance, contains a wealth of useful information just below its surface. K7 Computing is a special case. Although it may provide adequate protection from threats, it lacks many of the amenities consumers have come to expect from endpoint protection suites.

Endpoint security has become the quintessential companion for any PC. The leveraging of Trend Micro's Smart Scan against a cloud database has landed Enterprise-class security squarely in the hands of the consumer. That, combined with extensive and intuitive features opens up the internet more than ever before for the typical user.

Test Methodology

All performance tests were conducted using a single Windows system image that was created prior to the installation of any endpoint security solution and restored before installing each solution under test. All performance testing was conducted on a single physical machine with no hardware or BIOS changes across the solutions tested. The image consisted of the Windows 7 Home Premium 32-bit OS plus several measurement utility programs. The only other applications installed were AutoIT v3 (for scripting of tests), and Teamviewer (used to enable remote access on the machine after the completion of tests). See Tables 1 and 2 for details of the endpoint security solutions under test and the hardware platforms used.

All reported data is the average of three or more iterations of a given test. In all cases where a baseline is referenced, those results were gathered from the Windows 7 system without any endpoint security software installed.

Velocity Test Suite

Tolly engineers utilized Microsoft's Velocity Test Suite to measure certain aspects of the machine's startup and shutdown. Each iteration of the test involved timing three

Performance Endpoint OS, Platform and Network Summary

Operating System	Microsoft Windows 7 Home Premium 32-bit (System maintenance current as of 17 September 2011. After install, system update was turned off.)
Hardware	Intel Core2 Quad CPU Q8400 @ 2.66 GHz (Windows Experience Index 3.5), 3GB RAM. C: Western Digital Caviar Blue, SATA, 7200 RPM, 320GB, 8MB Cache,. Approximately 160 GB of disk used by OS, benchmarking applications and user data. D: Western Digital Caviar Blue, SATA, 7200 RPM, 320GB, 8MB Cache. Both drives verified virus-free and had 0% fragmentation prior to each test.
LAN	1 GbE Atheros AR8121/AR8113/AR8114 PCI-E Controller (NDIS6.20)
LAN Switch	3Com SuperStack3 Baseline Switch 2808. All ports Gigabit Ethernet.

Source: Tolly, October 2011 Table 1

Vendor	Product	Version
Trend Micro, Inc.	Titanium Maximum Security	5.0.1280
K7 Computing Private Ltd.	K7 Computing Ultimate Security	11.1.0057
Kaspersky Lab	PURE	9.1.0.124
McAfee	Total Protection 2012	11.0.623
Symantec	Norton 360	5.1.0.29

Source: Tolly, October 2011 Table 2

complete boots of the system (until Windows reports a steady state), and three complete shutdowns from an idle state. Engineers ran each iteration three times and averaged the results.

Solution Idle Footprint

Tolly engineers used two separate mechanisms to arrive at the reported memory and CPU utilization metrics. The Windows Performance Monitor utility was used to gather user memory by process (which was narrowed down to the services of a single product), as well as the total CPU usage for a user over a five minute interval, started five minutes after the system boot.

Since security products embed themselves deep into the system, Tolly engineers used Microsoft's Memory Pool Monitor (Poolmon) to report on the utilization of each product-specific kernel tag, providing an exact tally of all paged and non-paged bytes in use by the solution.

Scripts incorporating these functions were provided to Tolly to facilitate the data collection, and results were verified independently to ensure accuracy. This test was run four times for each solution and the average results were used. For Baseline (no security product installed) utilization, engineers reported only the idle CPU.

Full Scan Performance

Two related tests were run to benchmark the speed and resource utilization of the various solutions when running on-demand scans. Both tests used on-demand scans and gauged scanning speed and resource utilization. In order to gauge scanning speed, all products were configured to conduct a custom scan of the two drives with no other options selected. The drives contained the base system image plus a mix of files to emulate a typical user environment. The second drive contained a full image of the machine, as well as other miscellaneous files.

To determine "busy" memory usage, engineers utilized the same method as for the idle resource consumption, the perfmon utility to gather memory statistics for processes, and poolmon for the kernel tags. Engineers started the recording process, then initiated a full scan for each product, capturing the memory utilization for the duration of the full scan.

For the initial scan, the test was run twice, for validation purposes, as each run required uninstalling and re-imaging the client machine. Tests were run three or more times for the repeated full scan and the results were averaged.

Third-party Application Installation

Tolly engineers selected a publicly available installable component of Microsoft's .Net Framework 2.0 Express SP2 and measured the amount of time required to install and then uninstall the component. Each omitted the user action required in order to go through the process of installation/ uninstallation, and instead measured only the time when the components were actually installing.

Installation and Disk Usage

Tolly engineers noted the size of each solutions installer. For solutions that involved downloading the current software during the installation procedure, engineers noted the size of the download file.

Engineers installed Epsilon Squared's InstallRite utility to create a snapshot of the baseline system before each solution was installed. After installation and a system reboot, InstallRite was run to create another list which identified files added to the baseline system. Engineers calculated the disk usage from this list. For those products that downloaded to the C: drive and/or failed to delete their install files after installation, the additional files are included in the final results.

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by email at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Interaction with Competitors

In accordance with our process for conducting comparative tests, The Tolly Group contacted the competing vendors inviting them to review the test methodology and their results prior to publication. Kaspersky declined to participate in the evaluation. K7 Computing did not respond to our invitation. McAfee and Symantec accepted the invitation to participate in the evaluation. Comments from McAfee and Symantec are included in the main document as appropriate.

Tolly. Fair Testing Charter

For more information on the Tolly Fair Testing Charter, visit:
http://www.tolly.com/FTC.aspx

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.