TEST REPORT

Tolly.

#210142

September 2010

Commissioned by Trend Micro, Inc.

Trend Micro Titanium Maximum Security 3.0

Consumer Endpoint Security Performance vs K7, 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 applications. 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 3.0 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 3.0 vs. consumer-class, Windows 7 32-bit security solutions from K7, 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 and CPU usage, installation and network copy functions.

Introduction

In order to determine the system resource impact, and consequently, the impact on the end-user experience, 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 reboot and manual disk scans. Additionally, engineers tested the ongoing impact of the security endpoint working in the background when the system is idle and when running common tasks such as on-access scans of files being copied to the endpoint from a file server.

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

TEST HIGHLIGHTS

Trend Micro Titanium 3.0:

1. Demonstrated consistently optimal usage of system resources
2. Implemented the smallest installer among the products tested
3. Delivered the fastest boot time of all products tested
4. Delivered the fastest network file copy of all products tested
5. Demonstrated the lowest memory and CPU usage when performing a full scan of the C: drive
6. Showed the lowest combined impact on installing and uninstalling programs

Boot Time

In order to provide effective protection, security software needs to load during the boot sequence. Loading additional software 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 from the first text displayed after power-on by the system BIOS, up to the point where the Windows 7 was fully initialized and the desktop could accept user input.

Boot Time (cont.)

Trend Micro Titanium and McAfee Total Protection 2010 turned in equivalent times of 34 seconds compared to the baseline of 30 seconds for the same system with no endpoint security software installed. See Figure 1.

Where the top three solutions increase boot time by about 13%, Symantec Network Internet Security (NIS) 2011 Beta[1], Kaspersky Lab PURE and Symantec Norton 360 increase the boot time from 26% to over 63%.

Network File Copy

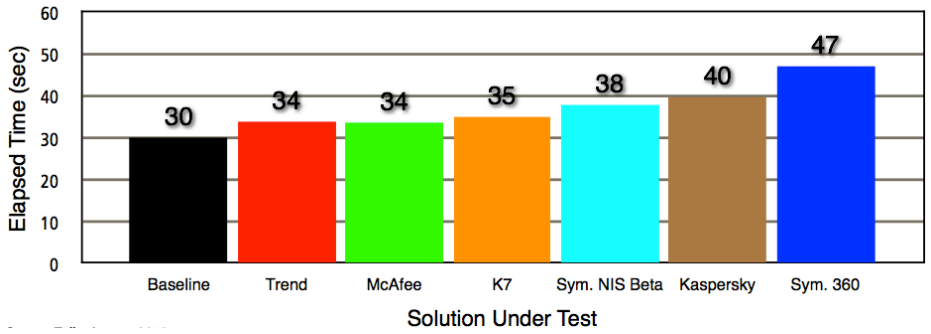
Even in home environments it is increasingly common for users to access files that reside on other machines connected to the network. Thus, it is important to understand the impact of the endpoint solution on the interaction between client and server.

In this test, a collection of data consisting of over 4,000 files of various types nested in over 1,000 folders (over 6GB of virus-free data in all) was copied from a Windows 7 network share to the endpoint's local C: drive.

When run on a PC with no endpoint security installed, the test took a minimum of two and a quarter minutes to complete. Of all the security solutions, Trend Micro Titanium completed the copy the fastest. (Note: by default, Trend Micro does not scan ZIP/ compressed files during on-access scans such as in this test.) See Figure 2.

The next fastest solutions added over 1.5 minutes to the copy time and the Symantec 360 and McAfee solutions nearly doubled the time required. K7's solution quadrupled the time required for the copy compared to the unprotected system baseline.

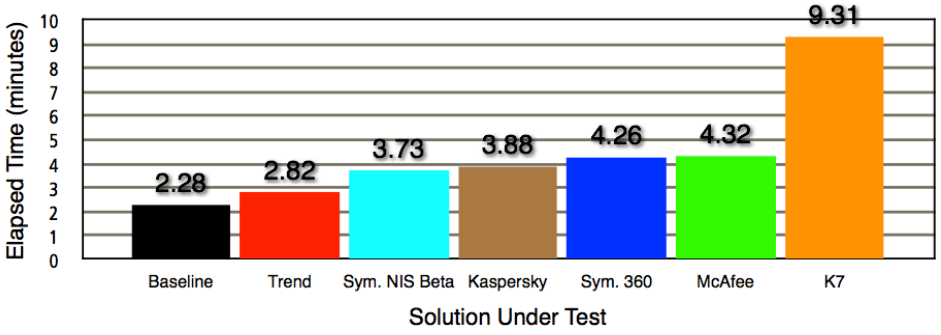
Endpoint Security Systems: Windows 7 Boot Time
From BIOS Screen to Windows Desktop



Source: Tolly, August 2010

Figure 1

Endpoint Security Systems: Windows 7 Network Copy
From Server to Endpoint Client



Note: Tested in default configuration. Trend does not scan ZIP files by default.

Source: Tolly, August 2010

Figure 2

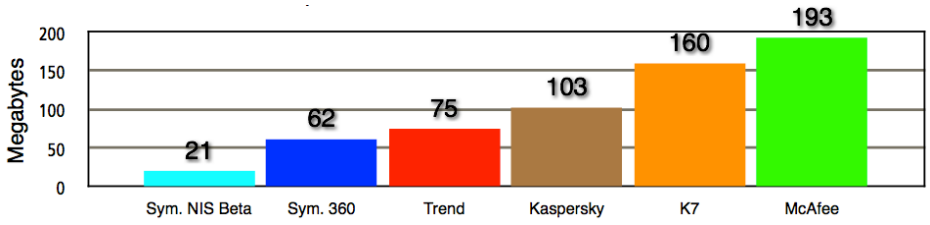
[1] Symantec notes that the performance and resource utilization of its beta software may not reflect accurately how the final version of the product will perform. Specifically, the beta software has extensive logging associated with the beta phase that Symantec notes will not be present in the production version.

Memory Footprint - Idle

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 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 10 with the two Symantec solutions using the least amount of RAM followed by Trend Micro at 75MB. Results are the delta between a baseline system without security and the solution under test. See Figure 3. Kaspersky, K7 and McAfee required increasingly larger amounts of memory with McAfee requiring the most at 193MB or almost 10% of the installed memory of the test system.

Endpoint Security Systems: Windows 7 System Memory Usage - Idle
Endpoint Client measured 10 min. after boot (5 min average)



Source: Tolly, August 2010

Figure 3

Full Scan Performance / Memory Footprint - Busy / CPU Usage

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 busy memory footprint and CPU 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, testers configured each solution to run a full scan of the C: boot drive.

The Symantec 360 product does not provide an option for scanning a single drive so the elapsed time test (Figure 5) was not run for that product. Testers gathered memory and CPU usage for Symantec 360 by running the product's full scan function for the 5 minute testing period.

The full scan test was the most complex of the series as results were measured in multiple ways that included: time to complete, memory and CPU usage, and number of objects scanned.

Figures 4, 5 and 6 illustrate summary results for separate but related tests.

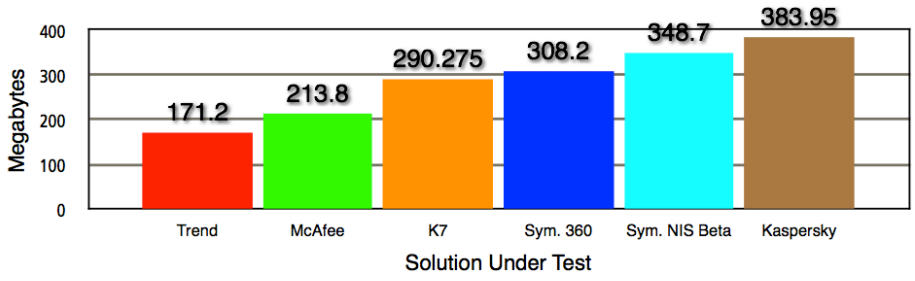
The data in Figure 4 represents the average memory usage of each product during the first 5 minutes of the full scan - the scope and duration of which, as noted earlier, varied across products.

The drive scan illustrated in Figure 5 was focused on determining both the amount of time required to scan the C: drive as well as to document the number of objects the security endpoint would report as scanned.

The data in Figure 6 represents the average CPU utilization during the same test.

Reviewed together, it can be seen that Trend Micro has the lowest memory utilization and the second-lowest run time for the full-drive scan. Where Symantec's NIS, on average, completes more rapidly, its memory usage is twice that of Trend Micro. Where all of the other products displayed

Endpoint Security Systems: Windows 7 System Memory Usage - Busy
Endpoint Client during Full System Scan (5 min average)



Source: Tolly, August 2010

Figure 4

consistent results across all three runs of the test, Symantec NIS results varied dramatically across the three runs. The first run required 10 min. 33 sec. and reported over 100K objects scanned where the two subsequent runs each reported 68,121 objects scanned and completed in 1 min. 17 sec. and 1 min. 14 sec. respectively. Thus, the average time for Symantec NIS is not representative of any of the three runs.

In addition to scanning the approximately 50, 000 files residing on the C: drive, it can be seen that Kaspersky, McAfee and Symantec NIS automatically include other objects in the custom scan. McAfee identifies these other objects as registry entries.

Irrespective of scope, it can be seen that all of the other offerings consume from 45 to over 200MB more memory when running a full scan than Trend Micro.

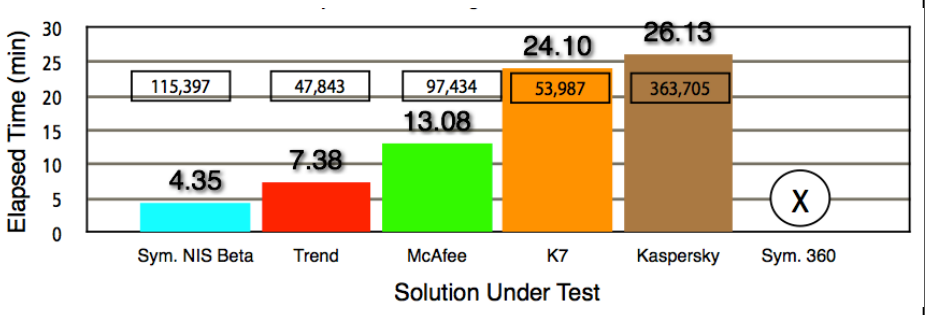
Trend Micro had the lowest CPU usage at 35.04% with K7 at 35.096 and the Symantec products at ~38%. McAfee averaged 45.79% CPU and Kaspersky averaged 78.277% CPU with engineers noting that the Kaspersky solution frequently drove the CPU to 100% utilization.

Quick Scan Performance

Perhaps more frequently used than the full scan, each solution offers a "quick" scan that apparently checks for the most commonly found viruses and/or vulnerabilities. As can be seen from the vastly differing number of objects scanned, each solution has a different scope for what each lists as a "quick scan".

Trend Micro turned in the quickest run time for this test and reported 133 objects scanned. All products except the McAfee solution completed in 16 seconds or less with McAfee averaging 69 seconds across its three runs. The number of objects reported as scanned by each product varied significantly from Trend Micro's 133 to roughly 5,000 objects for the two Symantec

Endpoint Security Systems: Windows 7 Full Scan of C:
Elapsed Time (Average of Three Runs)

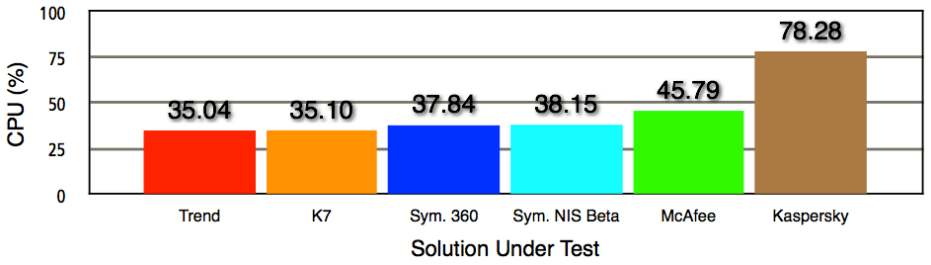


Note: Number in box represents the number of objects reported scanned on the first run and includes files and registry entries. Symantec/Norton 360 does not offer an option to scan a single drive.

Source: Tolly, August 2010

Figure 5

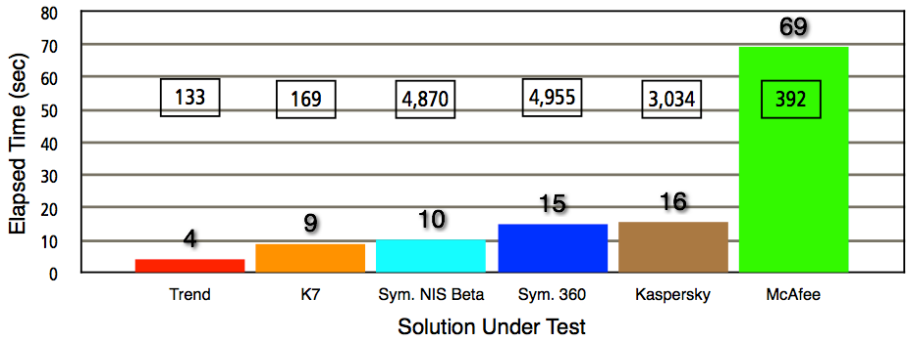
Endpoint Security Systems: Windows 7 System CPU Usage - Busy
Endpoint Client during Full System Scan (5 min average)



Source: Tolly, August 2010

Figure 6

Endpoint Security Systems: Windows 7 System Quick Scan
Elapsed Time (Average of Three Runs)



Note: Number in box represents the average number of objects reported scanned on all runs and includes files and registry entries.

Source: Tolly, August 2010

Figure 7

products. See Figure 7.

Third-Party Application Installation

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

Against a baseline measurement of 5 seconds for the install process and 3 seconds for the uninstall, Trend Micro delivered the best result because it added no measurable overhead to the process. Most of the other vendors results were in the range of 5 to 6 seconds for the install and 3 to 8 seconds for the uninstall. Noticeably longer were McAfee which required 10.47 seconds for the installation and 9.77 seconds for the uninstall and K7 which required 8.06 and 6.93 seconds for the install/uninstall. While the elapsed times were relatively short, testers note that install/uninstall overhead could become a bigger issue when installing a complex product that would have a much longer baseline install time.

Endpoint Security System Installation and Disk Usage

Tolly engineers noted the installer size and disk requirements for the solutions under test. Trend Micro packages Titanium as a single installer of 56MB, which has the smallest install package among the solutions. Other solutions, such as McAfee and Symantec deliver a small downloader program that, when run, initiates a download of installers that are 126MB for McAfee and 116 MB for Symantec 360.

Once installed, the solutions require from approximately 183MB to 700MB with Trend Micro in the mid-range requiring 292MB, K7 the lowest and Kaspersky the highest. See the appendix to this document for the detailed results.

Test Protocols

All 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. No additional applications were installed. See Tables 1 and 2 for details of the endpoint security solutions under test and the hardware platforms used.

Because of the level of detail and volume of results for this test, Tolly has prepared an appendix that contains a more detailed test methodology as well as individual results for each run used to calculate the average values reported herein. The appendix document can be found on tolly.com as document number 210142A and should be considered as an essential appendix to this document. In all cases where a baseline is referenced, those results were gathered from the Windows 7 system without any endpoint security software installed.

Trend Micro, Inc.
Titanium Maximum Security 3.0
Endpoint Security Performance

Tolly. Certified

Tested August 2010

System Boot

Tolly engineers measured the elapsed time from the appearance of the first text on the PC display (display by the system BIOS) until the Windows 7 desktop appeared and the busy icon was no longer displayed. The test was run three times and the results were averaged.

Network File Copy

A Windows 7 system was configured to share a directory and act as the server. That directory contained 1,087 nested folders containing a total of 4,068 files. The data corpus was a total of 6.65 GB and was free of viruses and malware. No endpoint

Systems Under Test

Vendor	Product	Version
Trend Micro, Inc.	Titanium Maximum Security	3.0.1303 (Most components v 1.5.1381. Virus Scan engine 9.200.1007)
K7 Computing Private Ltd.	K7 TotalSecurity	10.0.00.31 Antivirus ver 9.47.1238
Kaspersky Lab	PURE	9.0.0.192
McAfee	Total Protection 2010	10.5.195
Symantec	Norton 360	4.1.0.32
Symantec	Norton Internet Security (NIS) 2011 (Beta)	18.1.0.30 as per Windows control panel display

Source: Tolly, August 2010 Table 1

protection software was installed on the server machine.

Client machines established a connection with the server and testers ran a script that invoked the Windows XCOPY function to copy the entire corpus from server to client. This process was run three times with different target directories on the client for each run. The results were averaged. Both client and server connected to dedicated ports of a Gigabit Ethernet LAN switch.

Memory Footprint - Idle

Tolly engineers used the Windows Perfmon utility to monitor the committed memory allocations for idle systems in a baseline configuration and, subsequently, with each of the solutions under test installed. All measurements were made for a 5 minute period that started approximately 10 to 15 minutes after a system reboot when engineers observed that CPU utilization had dropped to near-zero. At that point, memory usage was captured for five minutes and the average utilization for that period was recorded. This test was run four times for each solution and the average results were used. The baseline memory for an idle system without endpoint security installed was subtracted from the total to provide the result for each product.

Full Scan Performance / Memory Footprint - Busy / CPU Usage

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 C: boot drive with no other options selected. The drive contained the base system image plus a single copy of the file corpus referenced in the network copy test.

To determine "busy" memory usage, test engineers configured the Perfmon utility to gather statistics for committed memory and CPU and then initiated a full scan for each product and captured the memory and CPU utilization for the first five minutes of each run. Tests were run three times and the results were averaged. The baseline memory for an idle system without endpoint security installed was subtracted from the total to provide the result for each product.

Quick Scan Performance

Tolly engineers ran each solution's on-demand quick scan procedure and noted both the elapsed time required for the scan to complete as well as the number of objects that the solution reported scanning. The test was run three times and the results were averaged.

Third-party Application Installation

Tolly engineers selected a publicly available installable component of Microsoft's .Net Framework (see appendix document for details) and measured the amount of time required to install and then uninstall the component. Tests were run three times and the results were averaged.

Endpoint Security System 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 any solutions were installed. After each solution was installed, 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, engineers manually deleted the files from the calculations. For example, Symantec 360 left 130.5 MB of files on the C: drive.

Performance Endpoint OS, Platform and Network Summary

Operating System	Microsoft Windows 7 Home Premium 32-bit (System maintenance current as of 10 August 2010. 40 recommended updates and 3 optional updates installed over system base. After install, system update was turned off.)
Hardware	Intel Core2 Duo CPU E7400 @ 2.80 GHz (Windows Experience Index 3.0), 2GB RAM. C: Western Digital Caviar Blue, SATA, 7200 RPM, 160GB, 8MB Cache, 148GB formatted as NTFS. Approximately 38 GB of disk used by OS and benchmarking applications. Target for scan and "copy from network" test.D: Western Digital Caviar Blue, SATA, 7200 RPM, 320GB, 8MB Cache, 298GB formatted as NTFS.Both drives verified to be virus-free and have 0% fragmentation prior to each vendor test.
LAN	1 GbE Atheros AR8121/AR8113/AR8114 PCI-E Controller (NDIS6.20)
LAN Switch	3Com SuperStack3 Baseline Switch 2808. All ports Gigabit Ethernet.
Network Server	Windows 7 Home Premium system. Intel Core2 Quad CPU Q8400 @ 2.66 GHz (Windows Experience Index 3.5). 4GB RAM, Realtek RTL8168D/8111D Family PCI-E Gigabit Ethernet NIC (NDIS 6.20)

Source: Tolly, August 2010 Table 2

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 test methodology and their results prior to publication. Only K7 and Symantec accepted this invitation. Comments from vendors are included in the main document as appropriate.

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.

210142-uv-2-kt-08Sep10-VerJ