TEST REPORT
Tolly.

#210154
November 2010
Commissioned by
AVG Technologies

AVG Business Edition 9.0

Ease of Management and Usability Evaluation Against Competing Security Suites and Anti-Virus Products for SMB Users

Executive Summary

Endpoint security is just as important for small and medium business (SMB) environments as it is for large enterprises. SMBs, though, are likely to have limited or no dedicated IT resources to manage installation and ongoing policy updates. Thus, understanding the effort required to install and conduct ongoing maintenance tasks is important when choosing an endpoint security solution for SMB deployment.

Testing showed that with AVG, users can save valuable time in managing their security solution -- time that can be better used to focus on their business. With AVG, they can rest assured that they have a solution that is one of the easiest-to-use for most common tasks, such as running scans, installing across a small business network etc.

Users should care because it is important that they choose a solution that provides robust protection in an easy-to-install and easy-to-use package. Impact on customers: save time, fewer frustrations. Impact on network: faster deployment, faster scanning and faster healing means lower risk of viruses spreading across the business network.

The Bottom Line

1. AVG Internet Security Business Edition is one of the fastest products on the market for installation across a small business network, saving business owners and IT professionals valuable time
2. AVG easily locates and deploys protection to a new endpoint (laptop, PC)
3. Required fewer steps and was faster than other products in scheduling a full scan that includes all threats
4. Required fewer steps and was faster than other products tested to trigger a scan on a single PC from the remote management console
5. Delivered fastest performance to remotely clean an infected machine on the network, an important task to prevent viruses spreading across the network

Best-in-Class Usability* For Various Management Tasks

AVG Internet Security Business Edition 9.0	AVG Anti-Virus Business Edition 9.0
Locate and deploy protection to a new endpoint	Create a new policy: Identify a potentially unwanted program by signature and allow for a single endpoint
Create a new policy: Identify a potentially unwanted program by signature and allow for a single endpoint	Trigger a scan on a single system from management console
Schedule a daily full scan that includes all threats	Execute remote cleaning of infected machine
Trigger a scan on a single system from management console	Configure updates to include application, engine and patches
Execute remote cleaning of infected machine	
Configure updates to include application, engine and patches	

* Among the products tested in this report

Source: Tolly, July 2010

Table 1

Background

Tolly engineers evaluated the AVG Internet Security Business Edition 9.0 against competing security suites and anti-virus products from leading vendors like Avast!, Avira, ESET, Kaspersky Lab, McAfee and Symantec. See Table 2 below for the version information of the products tested.

The evaluation focused on the usability of the management interfaces of the various products under test in terms of the number of steps and time taken while performing common tasks associated with the everyday administration of various security functions.

Management Usability

Engineers evaluated the products under test that fell into two categories: integrated security suites, and standalone anti-virus products.

Security Suites

This test evaluated integrated security suites from AVG, ESET, Kaspersky Lab, McAfee, and Symantec. As shown in Table 3, the test findings reveal that the AVG Internet Security Business Edition is one of the easiest and one of the fastest security suites tested. Particularly, the AVG suite took the

AVG Technologies

Internet Security Business Edition 9.0 and Anti-Virus Business Edition 9.0

Ease of Use and Performance Evaluation

Tested July 2010

Products Under Test

	Vendor	Product	Version	Platform
Endpoint Security Management Systems Under Test	AVG Technologies	Remote Administration Console	9.0 Build 827	Windows XP SP3
	Avast	Distributed Network Manager	Sep2009 (4.8.995)	Windows XP SP3
	Avira	Security Management Center Front End		Windows XP SP3
	ESET	Remote Administration Console	4.0.136.0	Windows XP SP3
	Kaspersky Lab	Kaspersky Administration Kit	8.0.2090	Windows XP SP3
	McAfee	ePolicy Orchestrator	4.5.0 b753	Windows Server 2003 SP2
	Symantec	Protection Center	12.0.1001.95	Windows XP SP3
Endpoint Security Suites	AVG Technologies	Internet Security Suite for Business 9.0	9.0 Build 839	Windows XP SP3
	ESET	Smart Security 4 Business Edition	4.2.64	Windows XP SP3
	Kaspersky Lab	Enterprise Space Security	6.0.4.1424a	Windows XP SP3
	McAfee	Total Protection for Endpoint	Virus Scan Enterprise 8.7.0.570	Windows XP SP3
	Symantec	Protection Suite Small Business Edition	12.0.1001.95	Windows XP SP3
Endpoint Anti-Virus Systems Under Test	AVG Technologies	Anti-Virus for Business 9.0	9.0 Build ___	Windows XP SP3
	Avast	Small Business Server Suite	4.8.1061	Windows XP SP3
	Avira	Small Business Suite	10.0.0.911	Windows XP SP3
	ESET	NOD32 Antivirus 4	4.2.64.12	Windows XP SP3
	Kaspersky Lab	Business Space Security	6.0.4.1424a	Windows XP SP3
	McAfee	Active VirusScan	Virus Scan Enterprise 8.7.0.570	Windows XP SP3
	Symantec	Endpoint Protection Small Business Edition	12.0.1001.95	Windows XP SP3

Source: Tolly, July 2010 Table 2

fewest steps and time to locate and deploy protection to a new endpoint introduced into the network. Likewise, the AVG suite was the easiest and took the least time to create a new policy to identify a potentially unwanted program using signatures. Similarly, the AVG suite required the fewest steps and the least time to schedule and trigger a daily full scan including all threats, or target a single endpoint for scanning from the management console. It was also the quickest and took the fewest steps to remotely clean an infected machine. These findings show that the AVG suite merits strong consideration among the products under test.

Standalone Anti-Virus Solutions

This test evaluated standalone anti-virus security products from AVG, Avira, Avast, ESET, Kaspersky Lab, McAfee, and Symantec. Once again, as shown in Table 4, the test findings reveal that the AVG Anti-Virus for Business 9.0 is one of the easiest and one of the fastest security suites tested. Particularly, the AVG Anti-Virus took the fewest steps and time to create a new policy to identify a potentially unwanted program using signatures. Similarly, AVG Anti-Virus required the fewest steps and the least time to target

Security Suite: Management Usability Summary
Time and "clicks" required to complete task

Task	AVG	ESET	Kaspersky	McAfee	Symantec
Install product on management station and deploy to 5 endpoints	49 Steps 15 Min	58 Steps 15 Min	51 Steps 15 Min	86 Steps 42 Min	31 Steps 12 Min
Identify out-of-date endpoint protection	1 Step	1 Step	On Home Screen	On Home Screen	On Home Screen
Identify an unprotected computer	8 Steps < 2 Min	1 Step	2 Steps < 1 Min	3 Steps 1 Min	9 Steps 2 Min
Locate and deploy protection to a new endpoint	16 Steps 4 Min	16 Steps 4 Min	23 Steps 5 Min	24 Steps 6 Min	16 Steps 5 Min
Create a new policy: Identify a potentially unwanted program by signature and allow for a single endpoint	9 Steps 1 Min	19 Steps 2 Min	31 Steps 4 Min	29 Steps 6 Min	26 Steps 3 Min
Create a new policy for all endpoints: Setup a policy to protect setup parameters to prevent end users from modifying AV agent's configuration	14 Steps <2 Min	20 Steps 2 Min	11 Steps 1 Min	10 Steps 1 Min	Variable*
Generate report showing all malware detected in past 24 hrs	8 Steps < 1 Min	7 Steps <1 Min	3 Steps < 1 Min	3 Steps 2 Min	1 Step
Generate report showing status/version for all endpoints	3 Steps < 1 Min	7 Steps <1 Min	2 Steps < 1 Min	4 Steps 1 Min	6 Steps < 2 Min
Schedule a daily full scan that includes all threats	8 Steps < 3 Min	34 Steps 6 Min	14 Steps 4 Min	18 Steps 4 Min	8 Steps < 3 Min
Trigger a scan on a single system from management console	3 Steps < 1 Min	6 Steps <1 Min	12 Steps 3 Min	19 Steps 4 Min	8 Steps < 1 Min
Execute remote cleaning of infected machine	3 Steps < 1 Min	6 Steps <1 Min	12 Steps 3 Min	19 Steps 4 Min	8 Steps < 1 Min
Configure updating frequency	8 Steps < 2 Min	7 Steps <1 Min	10 Steps 2 Min	8 Steps < 2 Min	11 Steps < 3 Min
Configure updates to include application, engine and patches	Enabled by default	14 Steps 2 Min	Enabled by default	Enabled by default	Enabled by default

* The number of "clicks" and the time required for Symantec is variable, as the number of options that can be locked is quite granular compared to other products tested. This offers increased flexibility in defining a policy restricting certain options, but at the same time could take a variable amount of time and clicks.

Legend

Cell in GREEN — Indicates best among products tested

Source: Tolly, July 2010

Table 3

Anti-Virus: Management Usability Summary Time and "clicks" required to complete task							
Task	AVG	Avast	Avira	ESET	Kaspersky	McAfee	Symantec
Install product on management station and deploy to 5 endpoints	49 Steps 15 Min	71 Steps 33 Min	36 Steps 10 Min	58 Steps 15 Min	51 Steps 15 Min	77 Steps 38 Min	31 Steps 12 Min
Identify out-of-date endpoint protection	1 Step	2 Steps <1 Min	3 Steps <1 Min	1 Step	On Home Screen	On Home Screen	On Home Screen
Identify an unprotected computer	8 Steps < 2 Min	2 Steps <1 Min	4 Steps 2 Min	1 Step	2 Steps < 1 Min	3 Steps 1 Min	9 Steps 2 Min
Locate and deploy protection to a new endpoint	16 Steps 4 Min	7 Steps 2 Min	15 Steps 5 Min	16 Steps 4 Min	23 Steps 5 Min	15 Steps 6 Min	16 Steps 5 Min
Create a new policy: Identify a potentially unwanted program by signature and allow for a single endpoint	9 Steps 1 Min	Not Supported	10 Steps 1 Min	19 Steps 2 Min	31 Steps 4 Min	29 Steps 6 Min	26 Steps 3 Min
Create a new policy for all endpoints: Setup a policy to protect setup parameters to prevent end users from modifying AV agent's configuration	14 Steps <2 Min	Enabled by default	20 Steps 2 Min	20 Steps 2 Min	11 Steps 1 Min	10 Steps 1 Min	Variable*
Generate report showing all malware detected in past 24 hrs	8 Steps < 1 Min	4 Steps 1 Min	11 Steps 1 Min	7 Steps <1 Min	3 Steps < 1 Min	3 Steps 2 Min	1 Step
Generate report showing status/version for all endpoints	3 Steps < 1 Min	4 Steps 1 Min	10 Steps 1 Min	7 Steps <1 Min	2 Steps < 1 Min	4 Steps 1 Min	6 Steps < 2 Min
Schedule a daily full scan that includes all threats	8 Steps < 3 Min	16 Steps 2 Min	12 Steps 1 Min	34 Steps 6 Min	14 Steps 4 Min	18 Steps 4 Min	8 Steps < 3 Min
Trigger a scan on a single system from management console	3 Steps < 1 Min	3 Steps <1 Min	8 Steps < 2 Min	6 Steps <1 Min	12 Steps 3 Min	19 Steps 4 Min	8 Steps < 1 Min
Execute remote cleaning of infected machine	3 Steps < 1 Min	10 Steps 1 Min	11 Steps 1 Min	6 Steps <1 Min	12 Steps 3 Min	19 Steps 4 Min	8 Steps < 1 Min
Configure updating frequency	8 Steps < 2 Min	7 Steps < 1 Min	6 Steps < 2 Min	7 Steps <1 Min	10 Steps 2 Min	8 Steps < 2 Min	11 Steps < 3 Min
Configure updates to include application, engine and patches	Enabled by default	5 Steps <1 Min	8 Steps < 2 Min	14 Steps 2 Min	Enabled by default	Enabled by default	Enabled by default

* The number of "clicks" and the time required for Symantec is variable, as the number of options that can be locked is quite granular compared to other products tested. This offers increased flexibility in defining a policy restricting certain options, but at the same time could take a variable amount of time and clicks.

Legend

Cell in GREEN — Indicates best among products tested

Source: Tolly, July 2010

Table 4

a single endpoint for scanning from the management console or to remotely clean an infected machine. Also with the AVG Anti-Virus, the feature to configure the updates to include the application, engine and patches is enabled by default. Once again, these findings show that the AVG Anti-Virus is a strong contender in terms of the ease of management among the products tested.

Test Bed

The test bed consisted of a management PC and an endpoint client PC. As testing did not involve performance, the hardware performance characteristics were not particularly relevant. Thus the management console and endpoint systems were implemented in a virtualized environment. Please see the Table 5 for a description of the physical server as well as the virtual clients.

Test Methodology

Engineers installed the products under test in their default configuration on the management and endpoint client PCs. The base OS on the management and client endpoint PCs; and the products under test were updated to their latest available software levels prior to the start of the testing. Then, the software configurations of the products under test were frozen for the duration of the testing. Then, engineers ran through the set of tasks listed in Tables 3 and 4, and documented the number of significant steps and the total time taken to execute each task. Tests were repeated three times on each product under test to ensure repeatability of the test results, and the results averaged from all the runs to arrive at the published numbers.

A Word From AVG ...

Since the completion of this test, AVG has made further enhancements to the Remote Admin Console, including:

- ENHANCED Active Directory Integration
- "NEW" Station Overview Window
- ENHANCED HTML and graphic reports
- ENHANCED Integrated remote installation
- "NEW" Disable protection button (Console and UI)
- "NEW" Customizable expiry dialogs
- "NEW" Customizable AVG update timings

Since the completion of this test, AVG has introduced a Desktop Widget to its business edition, providing managers with an overview of connection status, server workload & stations requiring attention with link to HTML reports.

Disclaimer:
Tolly has not tested these updated features.

Test Infrastructure Details

Virtualization Platform Summary	
Operating System	Ubuntu 9.04 Desktop
System Type	64-bit OS
Installed Memory (RAM)	32 GB
Processor	2x Xeon E5530 @ 2.40GHz
Hard Disk Drive	C: Western Digital Caviar Blue, SATA, 7200 RPM, 160GB, 8MB Cache
LAN Interface	Gigabit NIC
Network Switch	3Com SuperStack3 Baseline Switch 2808. All ports Gigabit Ethernet uplinked to DLink DGS-2208 Router (Gigabit Ethernet)

Virtual Endpoint System Summary	
Operating System	Microsoft Windows XP (SP3) (SP3 is the final service pack for Windows XP.)
System Type	32-bit OS
Installed Memory (RAM)	1.00 GB
Processor	1 vCore Xeon E5530 @ 2.40GHz
Hard Disk Drive	10GB
LAN Interface	Gigabit vNIC

Source: Tolly, July 2010 Table 5

About Tolly…

The Tolly Group companies have been delivering world-class IT services for 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 e-mail 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 Tolly's Fair Testing Charter, Tolly personnel invited representatives from the competing companies to review the testing. Representatives from Avast, Symantec and ESET actively participated in the review, but did not offer any comments on the test results. Representatives from Kaspersky Lab and McAfee did not respond to Tolly's invitation to participate.

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.

210154-bwbmpo1-kk-19Nov10-VerD