

ESET Smart Security 4 Product White Paper

Antivirus — Antispyware — Personal Firewall — Antispam

Contents

Introduction	3
ESET Smart Security® 4	3
Main Components	4
GUI	4
Anti-Threat	4
Personal Firewall	4
Antispam	5
ESET SysInspector™	5
New Features	5
Managing ESET Smart Security in a Network	6
Advantages	6
Speed and Performance Comparisons	7
Unsurpassed Protection	9
Excellent Customer Care	9
Free Online Support Offerings	9
Corporate Education and Training	10
System Requirements/Compatibility	10
Conclusion and Checklist	10
Reliable Architecture	10
Ease of Management	11
Performance	11

Introduction

The Internet is perhaps the greatest communication tool ever created. However, now that so many computers have an “always-on” connection to the Internet, there is an unprecedented amount of malware designed to take advantage of this global and ever-expanding, public network. To counter these threats, ESET is continually introducing effective countermeasures: not just signature updates for the detection of known malware, but also the industry’s most advanced heuristics for countering new threats. This is backed up by ThreatSense.Net®, a global system for monitoring evolving threats. ESET’s latest release is its most comprehensive product to date: ESET Smart Security 4.

ESET Smart Security® 4

ESET Smart Security 4 is a thoroughly integrated anti-malware solution providing endpoint security for home use and businesses of all sizes. ESET Smart Security 4 features the speed and precision of ESET NOD32® Antivirus with its powerful ThreatSense® engine, and combines it with custom-engineered firewall and antispam modules. The result is a security solution which is constantly vigilant in keeping computers safe from malware and other Internet threats. With this “smart” approach, ESET has improved on an already world-class product.

For business users, ESET Smart Security 4 Business Edition also features ESET Remote Administrator. ESET Remote Administrator provides easy configuration and administration of ESET client solutions in networked environments, saving bandwidth by centralizing the download and distribution of updates to ESET clients. It also allows you to provide updates to ESET clients which are not directly connected to the Internet.

In keeping with the previous generation of ESET security solutions, ESET Smart Security has been designed to provide maximum functionality with the smallest possible system footprint. With minimal impact on system resources, the scanning engine provides multi-threaded scanning support and has the ability to examine all parts of the host system including, but not limited to:

- ADS (NTFS Alternate Data Streams)
- All local files (including files hidden by rootkits)
- Remote files
- Files locked in memory
- Archived files
- Embedded files

Main Components

GUI

Standard mode – Standard mode offers a clean, easy-to-use program feature set for basic administration, compared to the more detailed Advanced mode.

Advanced mode – Advanced mode is more suitable for experienced users. It provides access to additional options and tools (Quarantine, Scheduler, Log files, etc.), but requires more user interaction. This mode is most useful to the administrator seeking to customize ESET Smart Security for their own environment.

Anti-Threat

Antivirus/Antispyware – ESET Smart Security's Antivirus and antispyware module provides robust protection against malicious programs attacking the system. It includes control of files, email and Internet communication. When it detects malicious code, it blocks it by disinfection, deletion, or transfer to quarantine.

Personal Firewall

Automatic mode – Uses ESET's predefined rules to automatically analyze communication. Known applications are allowed to establish outgoing connections. Applications that have been allowed to create outgoing connections are also allowed to receive incoming connections.

Automatic mode with exceptions (user-defined rules) – Uses all rules available in Automatic mode and also allows you to add custom rules.

Interactive mode – Communications are handled according to predefined rules. If there is no rule available for a specific connection, the user is prompted to allow or deny the connection. After Interactive mode is active for few days, a group of rules will have been created which fit your needs. Interactive mode can also help to warn you of unusual/suspicious attempts to create outgoing connections.

Policy-based mode – Communications are handled according to rules predefined by the network administrator. These rules can be distributed to many client workstations simultaneously using ESET Remote Administrator. If there is no rule match for a given communication request, the connection is automatically blocked.

Learning mode – Automatically creates and saves rules. No user interaction is required because ESET Smart Security saves rules according to predefined parameters. Learning mode is suitable for initial configuration of the Personal firewall and should only be used until all rules for required communications have been created.

Antispam

Antispam – ESET Smart Security's Antispam module provides protection for Microsoft Outlook, Outlook Express, Windows Live Mail, Windows Mail and Mozilla Thunderbird. All incoming email messages are scanned in parallel (non-sequentially) and assigned a rating from 0 (not spam) to 100 (spam). Any email message categorized as spam is transferred to the Junk Mail folder or to a user-defined folder. Scanning and rating is performed using Bayesian analysis, rule-based (heuristic) scanning and a check against a global fingerprint database. This analysis is done intelligently while downloading mail and has little to no impact on system performance.

ESET SysInspector™

ESET SysInspector is an easy-to-use trouble-shooting application which can be used as a complementary diagnostic tool. It's free and available for download on ESET's website and is also integrated with ESET Smart Security 4. ESET SysInspector examines your computer and displays information about installed drivers and applications, network connections and important registry entries. This data can be used to help investigate suspicious system behavior and determine the cause.

New Features

Several new features have been added to ESET Smart Security 4, including:

- Self-defense – Prevents unauthorized changes to ESET Smart Security's install directory, registry keys, and program services and drivers.
- Real-time Activity Pane to monitor system events
- Improved compatibility with screen readers to assist visually-impaired users
- Improved compatibility with UAC (User Account Control) for Vista (and later OS's)
- Advanced archive scanning for .zip, .rar, .cab and other formats, with user configurable scan depth, scan timeout, and max file size
- Scanning of SSL-encrypted email messages
- Scanning or disabling of removable media (diskettes, USB flash drives, CD/DVD, etc.)
- Password-protected uninstall
- Two additional Personal firewall modes: Automatic with user exceptions, and Learning mode.
- Integrated ESET SysInspector
- ESET SysRescue – Creates a bootable CD or USB flash drive with ESET Smart Security pre-loaded, to clean infected systems without re-imaging.

Managing ESET Smart Security in a Network

The ability to manage security software centrally, easily and reliably is a chief consideration when choosing a business solution. An otherwise valuable security tool quickly loses its value if it cannot be managed easily on more than a small number of systems. ESET has long provided system administrators with powerful, scalable tools to manage client solutions across the network/organization. ESET Smart Security Business Edition is fully integrated into ESET Remote Administrator, allowing detailed features to be managed remotely. In addition, ESET Remote Administrator manages the 2.x, 3.x and 4.x versions of ESET NOD32 Antivirus, as well as ESET Smart Security 3.x and 4.x, all on the same network.

Advantages

Fully Integrated Protection - ESET Smart Security offers comprehensive protection using Antivirus, Antispyware, Personal firewall and Antispam components. These components were designed to function as a tightly integrated unit; the thorough integration of these elements ensures unparalleled protection, minimal system footprint and award-winning performance (see Figure 1-3).

Smart Detection – ESET, a pioneer in heuristic malware detection, has created an intuitive and extremely efficient security solution in ESET Smart Security 4. ESET Smart Security uses ESET's ThreatSense technology: Advanced heuristics that protect against unknown threats, along with generic signatures to detect unfamiliar mutations of known malware. Computers are most vulnerable to new malware threats during the window of opportunity between the outbreak (release) and the signature update required by traditional anti-malware solutions. ThreatSense technology minimizes exposure to new malware by closing that window using advanced heuristic capabilities.

Extremely Light System Footprint – The unique structure of ESET Smart Security has been optimized for maximum compatibility with most system environments. ESET has engineered a "smart" solution with the smallest system footprint on the market, ensuring the fastest startup times and smoothest performance. Transparent to users, ESET Smart Security provides consistent, comprehensive protection.

Centralized Remote Administration – For businesses, ESET Remote Administrator and Mirror components ensure that the installation and subsequent administration of ESET Smart Security are hassle-free. Minimal effort is needed to manage ESET client solutions across the network, which minimizes the administrative time/resources required and allows employees to focus on other aspects of the business.

Speed and Performance Comparisons

ESET's security products have always surpassed other solutions in terms of low impact on system resources and superior performance. That performance has been maintained in ESET Smart Security 4, and in some respects, enhanced.

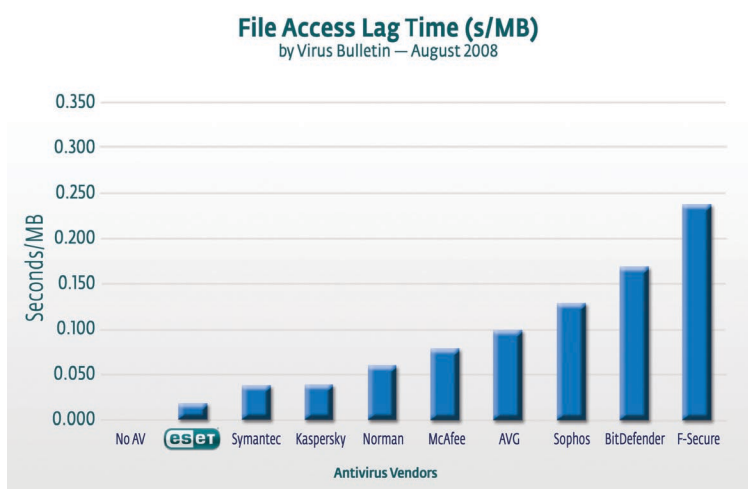


Figure 1-1: Excel scanning performance test

Figure 1-1 compares the performance of ESET NOD32 Antivirus (scanning engine used by ESET Smart Security) to a baseline system with no antivirus installed, as well as with competing products installed. The graph represents the performance delta (difference) between a computer with no antivirus software installed vs. those with various antivirus applications installed. This graph clearly illustrates the significantly higher performance of ESET's products.

The test set consisted of 100 unique Excel spreadsheets. Ten separate folders were created, each folder containing a copy of

the 100 spreadsheet test set. The benchmark tests were run with the following parameters:

- A program was executed to open and close each spreadsheet one at a time
- The time required to process the entire folder was recorded
- At the end of the test, 10 separate readings were taken, one for each folder
- The average of these 10 readings corresponded to the time required to open and close 100 spreadsheets

Figure 1-2 illustrates the average system resources available after running a series of tests on a Windows XP system with no antivirus application installed, and on the same system with various antivirus applications installed.

These tests were performed to obtain an average (weighted) rating, and inspected the following system attributes:

- CPU operations (i.e., floating point/ integer mathematical operations) program was executed to open and close each spreadsheet one at a time
- CD-ROM read access
- Hard drive read/write access
- Graphics impact (2D and 3D)
- Memory access and utilization

The test was performed using the commercial benchmarking product Performance Test from Passmark Software (<http://www.passmark.com>). When compared to an out-of-the-box system with no antivirus software installed, ESET Smart Security causes virtually no degradation of performance.

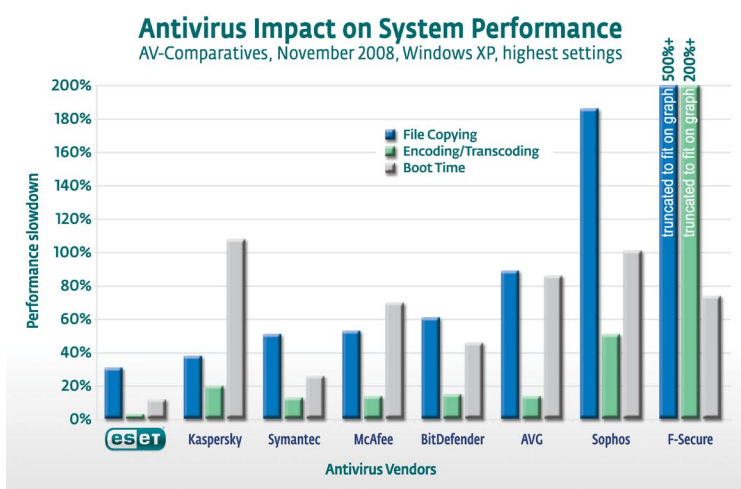


Figure 1-2: System efficiency based on a battery of tests

Both tests (Percentage Overhead and System Efficiency) were performed on three identical machines with the following configuration:

- Windows XP Professional Service Pack 3, with all patches to August 2008 applied
- Microsoft Office Service pack 3 and all updates
- 2 GB of RAM
- AMD Athlon64 X2 Dual Core 5200+ processor
- Dual 80 GB and 400 GB Hard Drives formatted with the NTFS file system
- Intel 82915G/GV/910GL chipset Graphics card
- Combo DVD/CD-RW Drives (52x Read)
- Gigabit LAN

Unsurpassed Protection

An important consideration in evaluating any anti-threat application is a consistently high level of achievement in detection tests. To date, third-party testing by AV Comparatives.org has acknowledged the consistent detection capabilities of ESET's products with more awards than any other antivirus vendor.

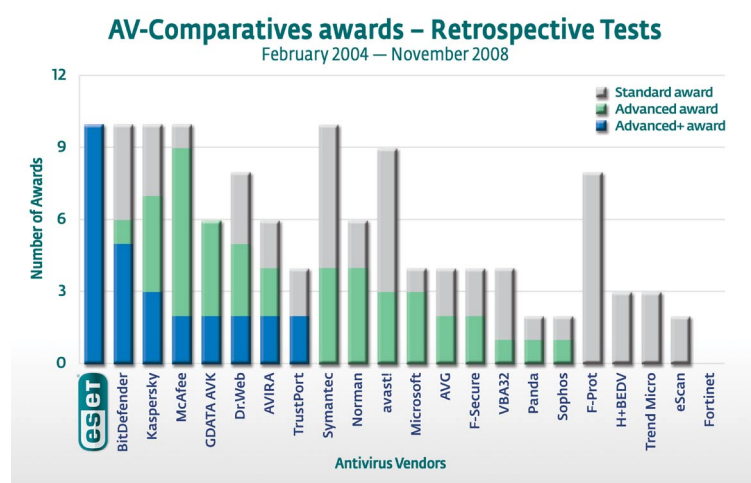


Figure 1-3: AV Comparatives Awards

One of the methods we use to continually improve detection rates is our unique ThreatSense technology. ThreatSense automatically collects data from our worldwide user base and immediately sends feedback to our Threat Laboratory on new threats detected by our heuristics. This information is immediately incorporated into new updates as necessary. The result is higher detection rates and a lower incidence of false positives.

The large volume of data retrieved by ThreatSense also allows us to fine tune detection. A recent example was the Conficker worm: we developed a generic

heuristic update for the worm and used ThreatSense technology to see how many variants of the worm were detected before a new heuristic update would be required.

Excellent Customer Care

The cornerstone of a great application is the support offered by the organization behind the product. If you have questions, ESET's world-class Customer Care department is ready to help. We also offer a variety of alternative support methods, including in-product trouble-shooting tips, online forums, and a world-class Knowledgebase.

Free Online Support Offerings

For answers to the most frequently asked questions, various problem solutions, directions and hints, see our Knowledgebase at <http://kb.eset.com>. Or, visit our online forums: <http://www.wilderssecurity.com/forumdisplay.php?f=15>. These resources are available twenty-four hours a day, seven days a week.

When supporting enterprise customers, ESET offers 24x7 Priority Service contracts. In addition to our standard support offerings, you will receive a dedicated support phone number with priority response and service level agreements allowing you to reach a support representative within a half-hour of your call. For more information, contact your ESET representative.

Corporate Education and Training

Effective security consists of three things: well-trained people, following best practices, and using effective tools. ESET consultants and partners can assist you in developing and acquiring all three. To schedule a training consultation, contact your ESET representative.

System Requirements/Compatibility

For seamless operation of ESET Smart Security 4 and ESET Smart Security 4 Business Edition, your system should meet the following hardware and software requirements:

Windows 2000 & Windows XP

- 400 MHz or higher processor (Intel or AMD x86-x64)
- 1280 MB available RAM

Windows Vista

- 1 GHz or higher processor (Intel or AMD x86-x64)
- 512 MB available RAM

Conclusion and Checklist

Anti-threat systems, by their nature, can be complex to evaluate and to deploy, whether for home, small business or enterprise users. ESET Smart Security 4 provides both simplicity and unmatched performance (detection rates, scanning speed and low resource requirements). This allows for less hands-on time and more productivity, which leads to a greater ROI (Return on Investment) and more peace of mind – protection made simple.

ESET Smart Security 4 is designed with the needs of all users in mind, from the home user with one or two computers, to large enterprises deploying thousands of systems. When selecting an anti-threat solution, the checklist below will help you make the most informed decision possible:

Reliable Architecture

- Does the solution provide a heuristic scanning engine (proactive protection which significantly increases detection rates)?
- Are multiple operating systems supported (Windows 2000/XP/Vista for home use, and Windows Server 2000/Server 2003/Server 2008, Linux, BSD, Solaris, and Novell Netware for business use) ?
- Is a remote installation option available?
- Can different products by the same vendor be supported by their enterprise server solution?
- Is the product truly integrated rather than consisting of multiple applications patched together?
- Are the Microsoft Outlook, Outlook Express, Windows Live Mail, Windows Mail and Mozilla Thunderbird email clients supported?

Ease of Management

- Is the user interface intuitive, reducing training time?
- Is customer support available 24×7?

Performance

- What is the actual scanning speed of the solution?
- How much memory does it truly require (total commit charge, not just memory footprint for the main process)?
- Does the default configuration provide sufficient protection and make sense?
- Overall, what proportion of the host system's resources (including CPU cycles) is required to run the solution?
- What are the detection rates reported by reliable third-party testers?
- Historically, how has the solution fared against its competitors?
- Is the company innovating new and effective solutions to address evolving malware?



Americas & Global Distribution

ESET, LLC.
610 West Ash Street, Suite 1900
San Diego, CA 92101, U.S.A.

Toll Free: +1 (866) 343-3738

Tel. +1 (619) 876-5400

Fax. +1 (619) 876-5845

© 2009 ESET, LLC. All rights reserved. ESET, the ESET Logo, ESET SMART SECURITY, ESET.COM, ESET.EU, NOD32, VIRUS RADAR, THREATSENSE, THREAT RADAR, and THREATSENSE.NET are trademarks, service marks and/or registered trademarks of ESET, LLC and/or ESET, spol. s. r. o., in the United States and certain other jurisdictions. All other trademarks and service marks that appear in these pages are the property of their respective owners and are used solely to refer to those companies' goods and services.

www.eset.com