

we protect your digital worlds



# ESET Smart Security

Product White Paper



# Table of Contents

	Page
Introduction	2
ESET Smart Security	3
The Sum of Its Parts	4
The GUI	4
Anti-Threat	4
The Personal Firewall	5
Antispam	5
Managing the Product in a Network	5
Advantages	6
Speed and Performance Comparisons	6
Unsurpassed Protection	9
Excellent Technical Support	11
Free Support Offerings	11
Corporate Education and Training	11
System Requirements/Compatibility	12
Conclusion and Checklist	13
Reliable Architecture	13
Ease of Management	13
Performance	13

## Introduction

The Internet is perhaps the greatest communications enabler ever created, but 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, for countering new threats, the industry’s most advanced heuristics. This is backed up by ThreatSense.Net®, a global system for monitoring evolving threats. ESET’s latest release is its most innovative and comprehensive product ever, ESET Smart Security.

## ESET Smart Security

ESET Smart Security is a new, completely integrated anti-threat solution providing endpoint security for homes as well as for businesses of all sizes. ESET Smart Security integrates the speed and precision of ThreatSense®, ESET NOD32 Antivirus' powerful heuristics engine, with a custom-engineered firewall and antispam solution. The result is an expert system that continuously defends computers from malware, spam, phishing and other Internet threats and intrusions. With this "smart" approach ESET is taking truly proactive protection to the next level.

For the enterprise, the ESET Smart Security Business Edition also features the ESET Remote Administrator tool. This ensures centralized administration and non-intrusive updating in networked environments. ESET Smart Security Business Edition optimizes PC and networking performance by saving bandwidth and management costs.

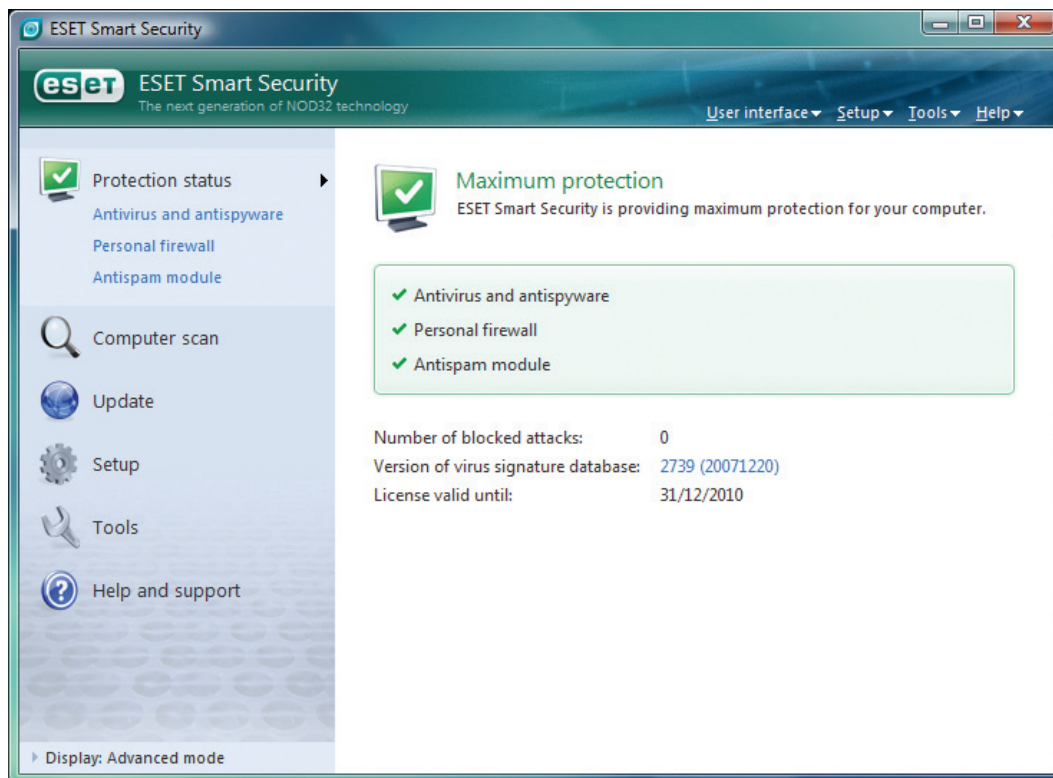
ESET Smart Security has been built from the ground up to provide maximum functionality with the smallest possible system footprint. Its scanning engine provides multithreaded scanning support and has the ability to examine all parts of the host system including (but not limited to):

- ADS (NTFS Alternate Data Streams)
- Archives and compressed files
- Executable files embedded in documents
- Files locked in memory
- Local files (including files hidden by rootkits)
- Packed (runtime compressed) executables
- Remote files
- Shared content and archives

## The Sum of Its Parts

### The GUI

**Standard Mode** – Standard Display Mode offers a clean, simple, easy-to-use program feature set for basic administration, in contrast to Advanced Mode, which is more granular and intended for advanced users.



**Advanced Mode** – This mode is more suitable for advanced users. It provides access to more options and tools (quarantine, log viewer, and so on), but requires more input from the administrator. It unlocks all the many options and tools available in ESET Smart Security, and is most useful to administrators seeking to customize ESET Smart security to deploy it to its best advantage in their own environments.

### Anti-Threat

**Antivirus/Antispyware** – ESET Smart Security's antivirus and antispyware protection provides robust protection against malicious programs attacking the system. It monitors files, e-mail and Internet communication. When it detects malicious code, it can disinfect or delete it, or move it into a quarantine folder.

## The Personal Firewall

**Automatic Mode** – This mode uses ESET’s predefined rules to analyze communications automatically. Applications known to be safe are allowed to establish outgoing connections. Applications that have been allowed to create outgoing connections are also permitted to establish incoming connections.

**Interactive Mode** – This mode does not just allow communications to be handled according to predefined rules, but also learns from the user’s feedback. If there is no rule available for a specific connection, the user is prompted to allow or refuse the connection. After Interactive Mode has been active for a while, a set of customized rules will have been created fitting the user’s needs. Interactive Mode is designed for advanced users wishing to setup the program to their own requirements: it can also warn users of suspicious attempts to create outgoing connections.

**Policy Mode** – In this mode communications are handled according to rules predefined by the network administrator in a policy distributed from the Remote Administrator module. If there is no rule match for a communication request, the connection is automatically blocked.

## Antispam

**Antispam** - ESET Smart Security’s antispam feature provides protection for Microsoft Outlook, Microsoft Outlook Express and Microsoft Mail. All incoming e-mail is scanned in parallel (non-sequentially) and assigned a rating ranging from 0 (not spam) to 100 (spam). Any e-mail that is categorized as spam is transferred to the Junk Mail folder, or to any other user-defined folder. The scanning and rating is performed using Bayesian analysis, rule-based (heuristic) scanning and a quick check against a global fingerprint database. This analysis is done intelligently while downloading mail and has little to no impact on system performance.

## Managing the Product in a Network

The ability to manage security software centrally, easily and reliably is a huge factor in choosing any security solution. The best security in the world is of limited value if it becomes more difficult to manage as the number of installations increases. ESET has long provided system administrators with powerful, scalable tools to manage every feature of the product over networks. ESET Smart Security Business Edition is now integrated into the Remote Administrator Console, so that its features can be managed centrally. It is also a simple task to manage the classic NOD32 version 2.x application, the new ESET NOD32 Antivirus version 3.0 upgrade, and ESET Smart Security, all on the same network.

## Advantages

ESET Smart Security offers several key advantages over other security products:

**Fully Integrated Protection** - ESET Smart Security offers comprehensive protection using antivirus, antispyware, antispam and a personal firewall. These components have been engineered as a single package so as to provide outstanding functionality and synergy. The thorough integration of these elements ensures unparalleled protection, stellar performance and impressive speed.

**Smart Detection** - ESET, a pioneer in heuristic malware detection, has created a system that is supremely efficient at detecting malicious behavior. ESET Smart Security incorporates ESET's ThreatSense® technology, which focuses on "smart" detection of malware and advanced heuristics to help protect from unknown threats, supplemented with generic signatures and genetic algorithms to detect variations of existing malware. Computers are most vulnerable to new malware threats during the window of opportunity between the outbreak (initial release) and the signature update required by traditional systems. ThreatSense® technology minimizes exposure to new malware by closing that window proactively with its advanced heuristic capabilities.

**Extremely Light System Footprint** - ESET Smart Security was designed from the from the outset to interface seamlessly with the system environment. ESET has engineered a "smart" solution with one of the smallest system footprints of any security solution on the market, ensuring the fastest startup and smoothest performance. Users barely know it's there, yet comprehensive protection is consistently maintained.

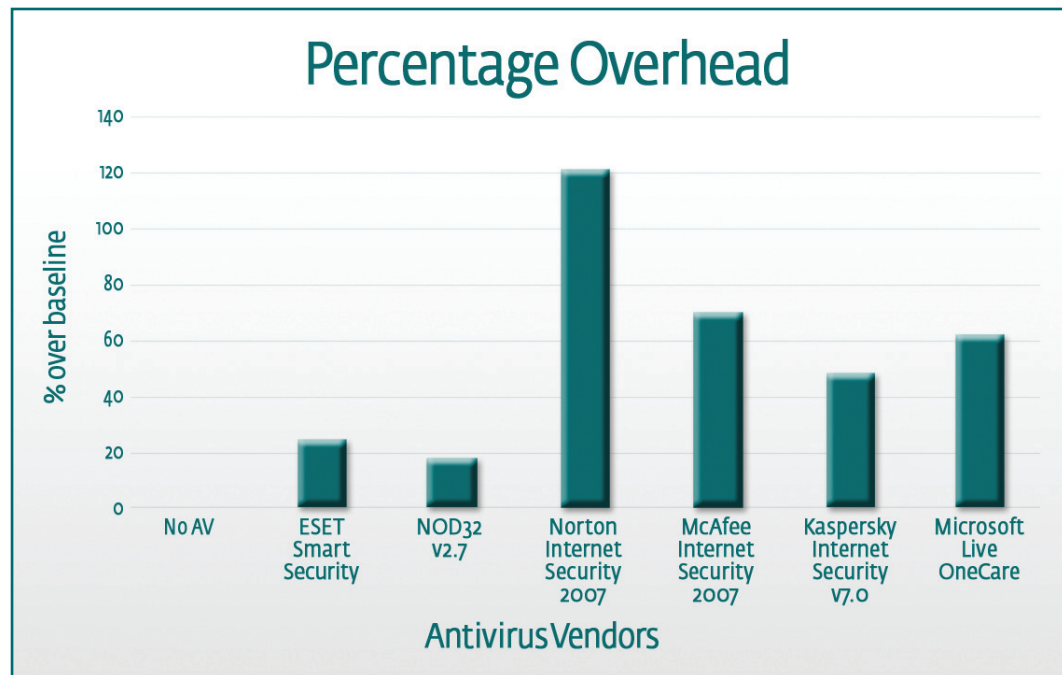
**Central Remote Administration** - For businesses, the ESET Remote Administrator and Mirror components ensure that the installation and subsequent administration of ESET Smart Security will be absolutely hassle-free. Minimal effort is needed to manage the products across your complete network environment, minimizing your cost in time and resources and enabling employees to focus on their jobs.

## Speed and Performance Comparisons

One aspect of NOD32 which has made it superior to other solutions is the product's minimal impact on systems, and the high performance it offers. Not only is that performance maintained by ESET Smart Security, but in some respects it is enhanced.

Previous versions of NOD32 sometimes required several instances of the scanning engine to run simultaneously: for instance when scanning runtime packed files. In ESET Smart Security's new integration framework, the engine is only loaded once, reducing the impact on performance to the barest minimum.

Figure 1 shows the performance of ESET Smart Security and NOD32, compared to the same system with competing products installed. In this graph, the greater the deviation from the baseline, the worse is the performance, clearly illustrating the ESET products' superiority.



**Figure 1: Excel Scanning Performance Test (1000 Excel Spreadsheets Scanned Sequentially)**

The test set consisted of 100 unique Excel spreadsheets, copied into each of ten separate folders. The benchmark tests were run with the following parameters:

- a program was executed so as to open and close each spreadsheet one at a time
- the time it took to process each folder was recorded
- at the end of the test the ten separate readings were combined, (one for each folder)
- the average time was taken for each of the ten readings corresponding to the time it takes to open and close the 100 spreadsheets

This simulates system load when opening and closing documents.

While ESET Smart Security does increase the impact on the system slightly more than the classic NOD32 product (a necessary overhead considering all the significant extra features it includes), its performance leads to a far smoother and more enjoyable user experience.

Figure 2 illustrates the average system resources available when 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.

The specific tests that were performed to obtain an average (weighted) rating looked at:

- CPU operations (for instance floating point/ integer mathematical operations)
- 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 a bare-bones system with no antivirus software installed, ESET Smart Security causes virtually no degradation of performance.

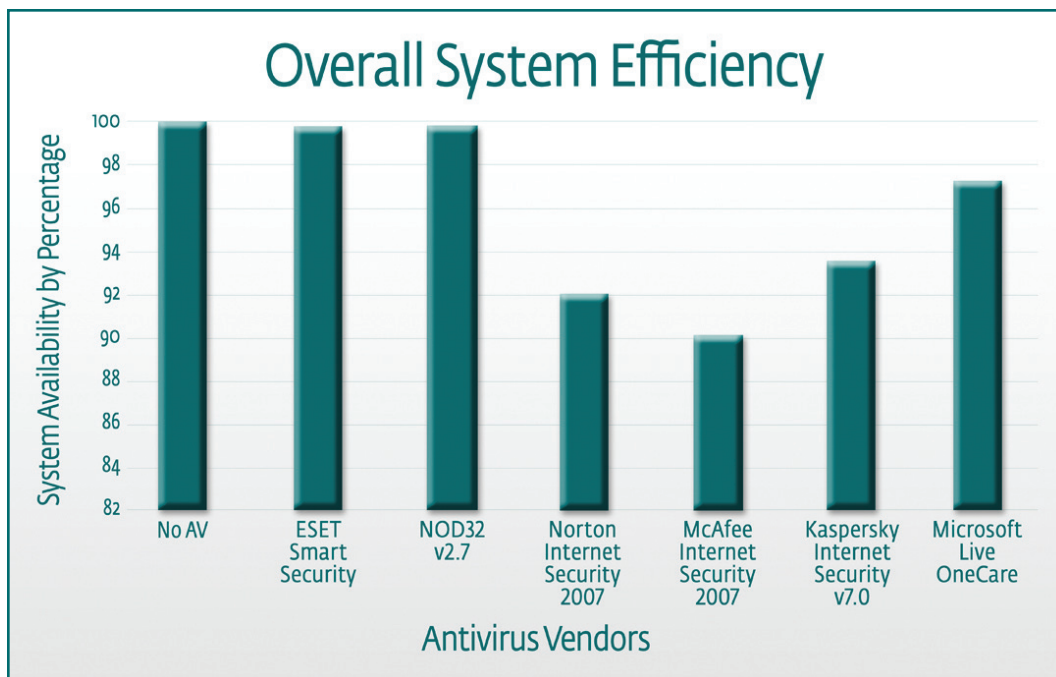


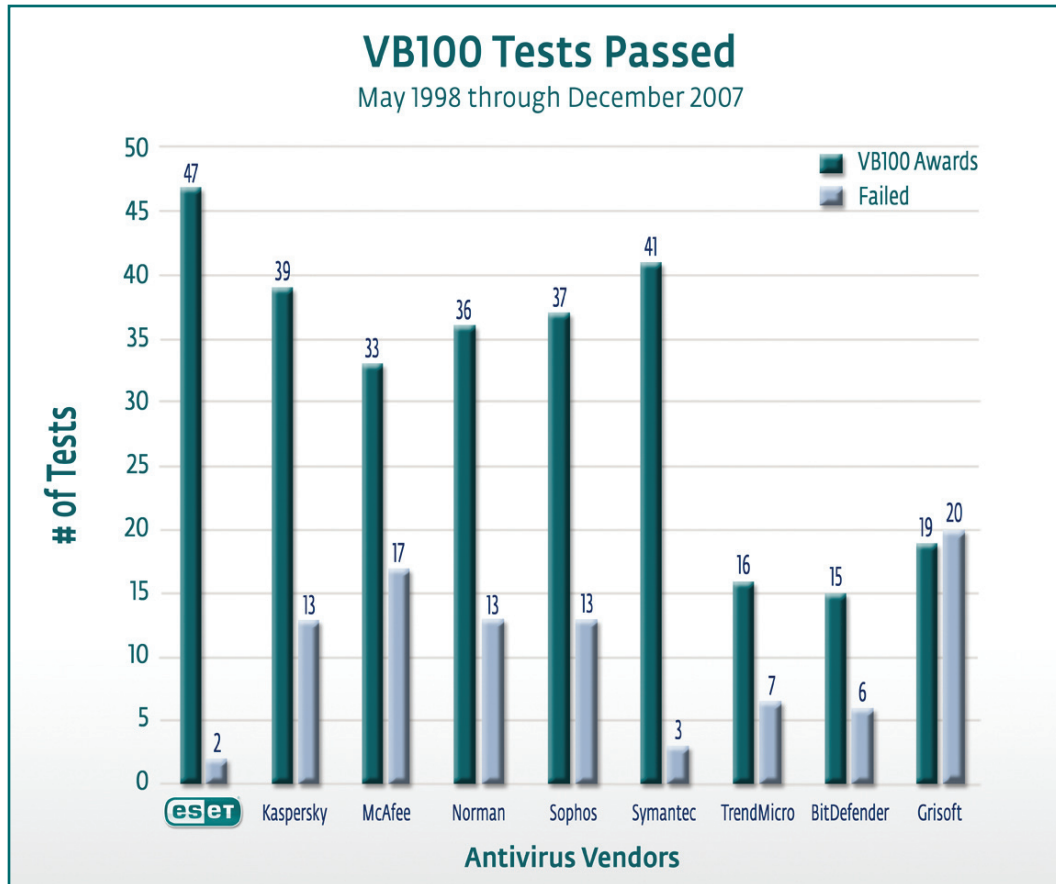
Figure 2: System Efficiency Based on a Battery Of Tests

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

- Windows XP Service Pack 2, with all patches to October 5, 2007 applied
- Microsoft Office Service Pack 2 with all updates except Service Pack 3
- 512 MB of RAM
- Intel Pentium 4 3.20GHz CPU with 2MB Cache
- 250GB Hard Drive formatted with the NTFS file system
- Intel 82915G/GV/910GL chipset with integrated graphics card
- Combo DVD/CD-RW Drives (52x Read)
- Gigabit LAN

## Unsurpassed Protection

An important consideration in evaluating any anti-threat software is the consistency of its detection. To date, third-party testing by Virus Bulletin has acknowledged the consistent detection capabilities of ESET's products with more VB100 awards than any other antivirus vendor's product has received (although one must bear in mind that ESET has also been around much longer than many other products, therefore ESET's products have also been tested more times).



**Figure 3: Virus Bulletin Pass/Fail Score (VB100 Tests: May 1998 – December 2007)**

One of the methods ESET uses to maintain its superior detection rates is our unique ThreatSense® technology. ThreatSense.Net® extends this technology by automatically collecting data from our worldwide user base and immediately sends feedback on new threats trapped by our heuristics to our Threat Laboratory. This information is then incorporated into new updates. This makes ESET NOD32 Antivirus and ESET Smart Security more efficient at detection while reducing false positives to a minimum.

The enormous amount of data retrieved by ThreatSense® also allows us to fine tune detection. A recent example is the Storm Worm (Win32/Nuwar). After developing a generic heuristic update for this malware, we use ThreatSense® to monitor the worm's evolution until new heuristic updates are required.

## Excellent Technical Support

The cornerstone of a great application is the support offered by the organization behind the product. ESET Smart Security is so advanced and so easy to use that you may never need to contact technical support, but if you do have a question, ESET's world-class support department is ready to assist each and every customer.

## Free Support Offerings

Common questions are answered in our list of Frequently Asked Questions (FAQ).

You can also contact technical support through our web site or visit the ESET NOD32 Anti-Virus Forum hosted by Wilders Security (<http://www.wilderssecurity.com/>). These online 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, as described above, you will receive a dedicated support phone number with priority response and service level agreements enabling 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 has three foundations: well-trained people, best practice processes, and effective technology. ESET consultants and partners can assist you in acquiring and developing all three. To schedule a training consultation, contact your ESET representative.

## System Requirements/Compatibility

As with any software application, there will be requirements and prerequisites that will determine compatibility with new or existing systems. Below are the minimum requirements for ESET Smart Security:

<b>Processor Architecture:</b>	i386 (Intel® 80386), amd64 (x86-64) or compatible
<b>Operating Systems:</b>	Microsoft Windows 2000 Professional/Server Microsoft Windows XP (32/64-bit) Microsoft Windows Server 2003 Microsoft Windows Vista (32/64-bit)
<b>Memory:</b>	40MB or less
<b>Disk-Space (Download):</b>	18-22MB (depending on version)
<b>Disk-Space (Installation):</b>	40-80MB (depending on version)

Note: Older versions of Microsoft Windows and systems which do not meet the minimum system requirements for ESET Smart Security or ESET NOD32 Antivirus v3 are supported by NOD32 v2.x.

## Conclusion and Checklist

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

ESET Smart Security 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)?
- Is support available for multiple platforms such as BSD, Exchange, Domino, Linux, NetWare and Windows?
- Is a “zero-desktop” central management option available?
- Can different products by the same vendor be supported by their enterprise server solution?
- Is the enterprise solution truly scalable so as to support even the largest enterprises?
- Is the product fully integrated, or does it consist of multiple applications “glued” together?
- Are Microsoft Outlook, Microsoft Outlook Express and Microsoft Mail supported?

### Ease of Management

- Is the GUI intuitive, reducing training time?
- Is customer support available 24x7?

### Performance

- What is the actual scanning speed of the solution?
- How much memory does it require?
- Overall, what proportion of the host system’s resources (including CPU cycles) is required to run the solution?
- What are the detection rates, as reported by reliable third-party testers?
- Historically, how has the solution fared against its competitors?
- Is the company innovating new and effective solutions so as to address evolving malware?



[www.eset.com](http://www.eset.com)

610 West Ash Street • Suite 1900 • San Diego • California 92101 • U.S.A.  
866-343-ESET

© 2007 ESET, LLC. All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET, LLC.  
All other names and brands are registered trademarks of their respective companies.