

October 2005

AntiVirus and Trojan Technology Report

For Server, Gateway and Appliance Solutions

ESET NOD 32 Anti Virus



Contents

Test Specifications	3
The Product	4
Company:	ESET
Product:	NOD32
Platform:	Windows 2003 server
Version:	2.50.25 + database 1.1197
Update method:	Online
Test Report	5
West Coast Labs Conclusion	7
Features and Functionality Buyers Guide	8
Additional Security Features	10
Appendix	11
Checkmark AntiVirus Level 1 Test Specifications	
Checkmark AntiVirus Level 2 Test Specifications	
Checkmark Trojan Test Specifications	

Test Specifications

The overall objective of this AntiVirus and Trojan Technology Report for Server, Appliance and Gateway Solutions is to evaluate each product in a controlled environment. Throughout the test period, each product was configured as recommended to update online. The testing environment represented that of a small to medium sized business or branch office.

Products were tested in accordance with the functionality criteria of the Checkmark certification system for AntiVirus Level 1 and, where Checkmark Certification registration permitted, for AntiVirus level 2 and Trojan .

Each Test Report is supplemented by a Features and Functionality Buyers Guide and information from the product developer concerning the type of business or organization the product is developed for, plus the direct technical and business benefits of the product.

Each White Paper looks at a product's **Management, Administration and Functionality**.

1. Management/Administration.

The testing will report on the following functions:-

- Installation
- Product update process
- Logging and reporting function

2. Functionality

Products will be tested in accordance with Checkmark AV level 1 and Trojan test (where registered) to determine the ability to detect viruses and Trojans.

For those products registered for Checkmark AV Level 2, the testing will report on the following virus disinfection capabilities:-

- Products will be tested to determine their ability to disinfect files infected with viruses.

What is a virus? A Virus is a program or piece of code attached to a file or diskette's boot sector and is loaded onto a computer without the user's knowledge. Viruses are manmade (though they can be corrupted in use to form new variants of the virus) and replicate themselves by attaching themselves to files or diskettes, often soaking up memory or hard disk space and bringing networks to a halt. Most recent viruses are internet-borne and capable of transmitting themselves across and bypassing security systems. Minor variants of the same virus are classed as families of viruses.

What is a Trojan? Trojan Horses or Trojans are destructive programs that pretend to be benign applications. Unlike Viruses or Worms, Trojan Horses do not replicate themselves but they can be damaging to networks by delivering other types of Malware.

The Product

ESET has been a member of the Checkmark AV certification scheme since 2003.

NOD32, both a standalone and a corporate product, has been certified on Windows 2003 server since 2000, currently holding the Checkmark AntiVirus Level One and Level Two, Trojan and Spyware certifications. (It is also certified on Linux, Exchange and Windows XP Professional).

As part of the scheme, NOD32 is tested on Windows 2003 server on four occasions to both AV Level 1 and Level 2 to assess its virus detection and disinfection capabilities, and on eight occasions against the West Coast Labs Trojan collection, during a 12 month registration period. The complete test history for this product, including results that may postdate this report, can be found at <http://www.westcoastlabs.org/checkmarkcertification.asp>.

ESET says...about the product.

ESET protects consumers and businesses from current and evolving threats. Its award-winning NOD32 Anti-Threat system offers the smallest, fastest and most advanced real-time protection against viruses, spyware and phishing attacks.

url : www.eset.com

ESET ...about the product's business benefits.

Users of ESET's NOD32 Anti-Threat System will benefit from fewer malware infections, lower performance impact, easier manageability and lower cost.

Proactive detection of current and future threats protects the integrity and confidentiality of business critical data also helping companies avoid bad press through breaches and disclosure requirements. It increases the productivity of employees and provides a cost savings from acquisition, staff maintenance and cleanup.

url : www.eset.com

ESET says ...about the product's technical benefits.

ESET's Anti-Threat System offers the best detection and performance with powerful centralized management. NOD32 has not missed a single, in-the-wild virus in seven years, and has the lowest false positive rate. Its unified anti-threat engine proactively stops current and future threats including variants of MyDoom, Netsky, Bagle, Mytob and Zotob.

NOD32 uses approximately 20MB of memory and has a 19MB/second throughput scanning rate. It has a minimal performance impact of 6% for on-access scanning. NOD32 is easy to use and allows for sophisticated control, logging and reporting. It usually installs in under a minute (under five minutes on typical networks).

url : www.eset.com

Test Report

Management and Administration.

NOD 32 installed without any difficulty, although one rather strange setting was noted: installing the typical configuration with no alterations means that the resident protection is not automatically started. To be fair, a screen asks the user to remove any other resident protection and then strongly recommends that the appropriate box is checked, but anyone clicking through the screens without paying full attention could find that the end result is a system with no resident protection running. The product updated without problems.

The product when installed is in two almost disconnected parts. From the menu both NOD32 and NOD32 Control Center can be started. An icon also leads to the Control Center where settings for the various monitors can be controlled. NOD32 is a separate set of screens from which manual scans can be run. Both sets of screens are functional and unfussy.

The Control Center lists the four monitors (files, documents, email and Internet protection), each of which can be configured separately. These settings are also independent of those set in NOD32, so that for instance each monitor and the manual scan can all use separate lists of extensions.

Each of the four monitors can be enabled or disabled, the icons turning red if the relevant monitor is disabled, so that the user is aware of the monitor's inactivity. Special settings are used for scanning newly created or modified files. (A link to the other part of the product enables manual scans to be targeted and run but from here the settings cannot be altered – that must be done in the manual scanner screens.)

In NOD32 all the usual settings for manual scans can be found and configured. By default scans are run against a list of extensions which the user can amend, but scans can be changed to scan all files, including those with no extension. Different actions can be set for malware found in files, boot sectors and memory. Settings can be saved in profiles that can then be allocated to various types of scanning, e.g. scanning of folders or of removable media.

Archives, self-extracting archives and email files can be scanned but are not done so by default in manual scanning, although the Control Center monitors do scan them by default when created or modified. NOD32's default settings include the use of virus signatures, heuristics and Adware/Spyware but not advanced heuristics and potentially dangerous applications, which are also available.

Logging can be enabled or disabled, with the entries written to a file of your choice. Entries for this file can either be appended or overwritten, and the maximum size of the log file can also be set.

Test Report (continued)

Functionality Testing.

Given the level of ESET's membership of the Checkmark Certification program, the functionality testing was conducted on the basis of the AV Level 1, AV Level 2 and Trojan certification tests.

The tests carried out were as follows:

Test 1

The scanner was used to scan viruses in the June 2005 Wildlist (the Wildlist being released on 11th August), both on-demand and on-access.

Using the definitions of 19 August, NOD32 detected all the viruses in the June Wildlist without problems.

Test 2

The scanner was used to disinfect infected files and diskettes infected with a selected list of the viruses in the above Wildlists.

NOD32 disinfects the appropriate files without problems.

Test 3

The West Coast Labs collection of Trojan Horses as it stood at 1st August 2005 was scanned.

NOD32 detected all the Trojans in the West Coast Labs collection without problems.

Additional Features

The product's ability to detect spyware was not examined as part of this report. Equally, its abilities to deploy to and control other machines were not investigated.

West Coast Labs Conclusion

It may take a little time to become familiar with the arrangement of NOD 32's settings but the accustomed user will be able to achieve even better results with this reliable and efficient product. Overlook it at your own risk.



West Coast Labs, William Knox House, Britannic Way, Llandarcy,
Swansea, SA10 6EL, UK. Tel : +44 1792 324000, Fax : +44 1792 324001.
www.westcoastlabs.org



Anti Virus & Trojan Technology Report Features and Functionality Buyers Guide

NOD32 Anti Virus

NOD32 Anti-Virus

Product

Is the product standalone or corporate? **S or C** → **c**

If corporate, is it self-contained or are other products needed to deploy/configure/monitor it? **Y or N** → **y**

Certification

Is the product certified to Checkmark AV Level 1 **Y or N** → **y**

Is the product certified to Checkmark AV Level 2 **Y or N** → **y**

Is the product certified to Checkmark Trojan **Y or N** → **y**

Updates

Can updates be scheduled? **Y or N** → **y**

Are new updates produced daily? **Y or N** → **y**

Can automatic updates be scheduled? **Y or N** → **y**

Are emergency updates produced during outbreaks? **Y or N** → **y**

If so, are these made available to all customers? **Y or N** → **y**

Can updates be pushed down? **Y or N** → **y**

Can updates be downloaded and installed manually? **Y or N** → **n**

(If corporate) can updates be distributed? **Y or N** → **y**

Are out-of-date virus definitions reported to the user? **Y or N** → **y**

Logs

Are logs produced? **Y or N** → **y**

Can entire logs be printed off? **Y or N** → **y**

Can selected entries be printed off **Y or N** → **y**

Can logs be saved in a file? **Y or N** → **y**

Can selected/filtered entries be saved in a file? **Y or N** → **n**

Can the format of the file be selected? **Y or N** → **n**

Can the logs be sorted? **Y or N** → **n**

Can the user select what information will appear in the log? **Y or N** → **y**

Can user notifications be disabled? **Y or N** → **y**



Anti Virus & Trojan Technology Report Features and Functionality Buyers Guide

NOD32 Anti Virus

NOD32 Anti-Virus

Scanning

Can folders/files be selected for scanning?	Y or N	▶	y
Are all file extensions scannable?	Y or N	▶	y
Can files without extensions be scanned?	Y or N	▶	y
Are all file extensions scanned by default?	Y or N	▶	y
Can ZIP and TAR files be scanned?	Y or N	▶	y
Can scans be scheduled?	Y or N	▶	y
Are unscannable files reported?	Y or N	▶	y
Is there a real-time scanner?	Y or N	▶	y
Can infected files be quarantined?	Y or N	▶	y
Can infected files be disinfected?	Y or N	▶	y
Can infected files be deleted?	Y or N	▶	y
Can users select the appropriate option when the infected file is found?	Y or N	▶	y
Are product plugins supported?	Y or N	▶	n
Does the product have system restore abilities?	Y or N	▶	n

Accessories

Is there a virus encyclopaedia on the hard disk?	Y or N	▶	n
Is there a virus encyclopaedia online?	Y or N	▶	y
Can virus samples be sent to the vendor via email?	Y or N	▶	y
Is the product dependent upon certain service packs being applied?	Y or N	▶	n

Additional Security Features

As stated by ESET

- ThreatSense™ technology - a single optimized anti-threat engine for analyzing code to identify malicious behavior; such as viruses, spyware, adware, phishing and more
- Unprecedented heuristic analysis capable of discovering new malware threats as they emerge, including advanced code analysis
- Powerful virtual PC emulation technology enables unpacking and decryption of all types of archives and run-time packing
- Advanced Predictive Profiling and Traditional malware signatures
- Able to clean active malware running in memory
- Protects at multiple infiltration points - including HTTP, POP3, SMTP, and all local and removable media
- Removes infections from files that are locked for writing (e.g. loaded DLL file)
- Prevents infected files from being opened, executed and warns on creation of infected files
- Automatic execution on system startup
- Supports multiple Terminal Server environments
- Supports scanning of mapped network disks

url : www.eset.com

Appendix

Anti Virus Level 1 Certification



For a product to be certified to Anti-Virus Checkmark Level 1, the product must be able to detect all viruses currently ‘In the Wild’ as at the time of testing. Test specifications can be downloaded from <http://westcoastlabs.org/cm-briefingdocs.asp>

Anti-Virus
Level 1

Anti Virus Level 2 Certification



For a product to be certified to Anti-Virus Checkmark Level 2, the product must be able to disinfect all viruses currently ‘In the Wild’ as at the time of testing, capable of being disinfected. Test specifications can be downloaded from <http://westcoastlabs.org/cm-briefingdocs.asp>

Anti-Virus
Level 2

Trojan Certification



For a product to be certified to the Trojan Checkmark, the product must be able to detect all Trojans currently in the Checkmark Trojan test suite as at the time of testing. Test specifications can be downloaded from <http://westcoastlabs.org/cm-briefingdocs.asp>

Trojan