Anti-Virus Comparative

Single Product Test

Sophos Anti-Virus 7.0.5

Date: December 2007

Last revision: 20th December 2007

Author: Andreas Clementi

Website: http://www.av-comparatives.org

1. Tested product

We tested Sophos Anti-Virus 7.0.5 with last signature update and version of the 12th December 2007 (Engine version 2.52.1, 4.24E and 319942+157 signatures) and with highest settings under Windows XP SP2. The used test-set is from the 5th August 2007 (about 4 months old).

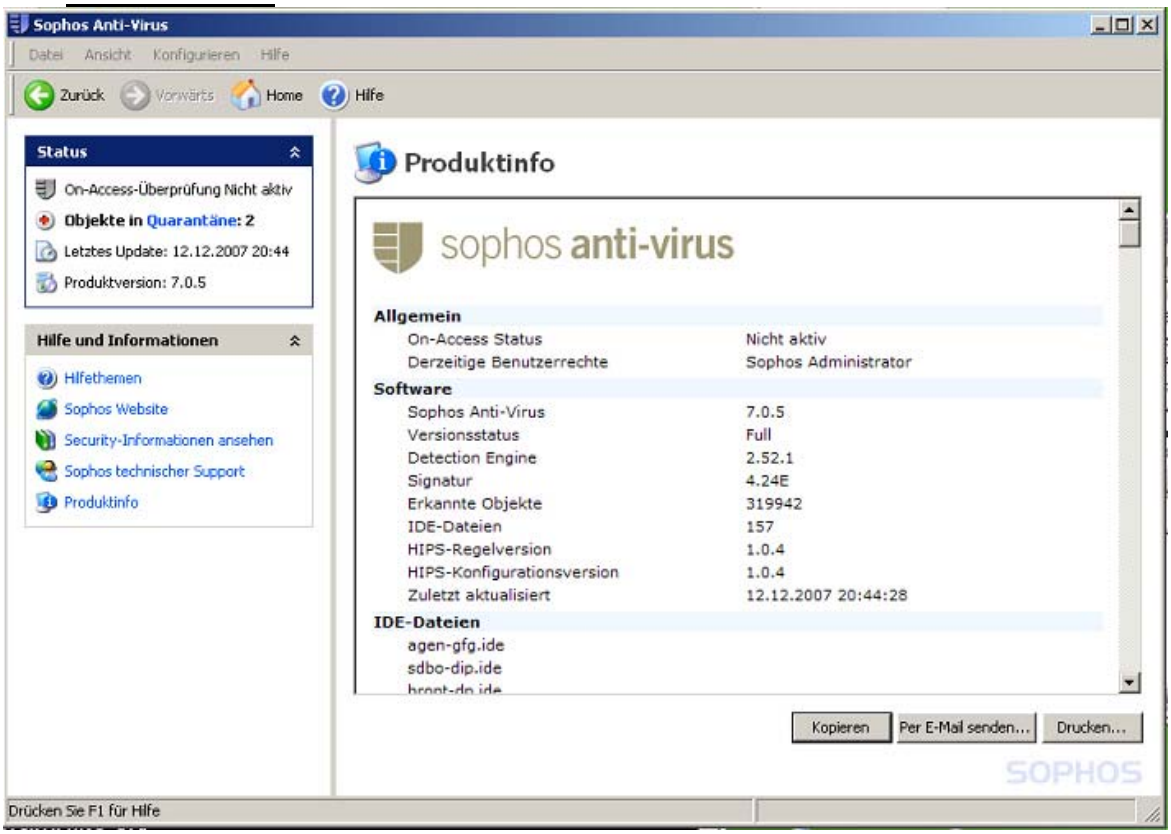
2. Test results

Below the on-demand detection rates of Sophos Anti-Virus 7.0.5:

Windows viruses	97%
Macro viruses	~100%
Script viruses/malware	68%
Worms	96%
Backdoors	98%
Trojans	95%
Other malware	69%
OtherOS viruses/malware	62%
TOTAL detection rate:	**95%**

Over our four month old test-set, Sophos had a total detection rate of 95%.

3. Screenshot



4. Comments

Sophos produces Antivirus solutions for business enviroments and large enterprises. Sophos (www.sophos.com) Anti-Virus is certified by ICSALabs (www.icsalabs.com) and by Check-Mark Level 1 and Level 2 (www.westcoastlabs.org), which means that the product was at least able to provide basic protection against malware listed on the Wildlist (www.wildlist.org).

The installation routine is simply designed and the program was very easy to install. During install, the user is asked to enter the username and password in order to get access to the download servers. The whole installation process took on the test system (Intel Pentium 4, 3GHz, 4GB RAM, 250GB SATA II) only about 60 seconds. The product automatically gets the latests signature updates during the install. Sophos Anti-Virus can be set to update itself automatically every hour by downloading very small incremental signature updates.
We scanned the test-sets with the highest settings (including extensive scanning and suspicious files and potentially unwanted applications detection). Setting the scan task caused no difficulty. The on-demand scan burdened the CPU with Hyperthreading about 90% of one core, allowing use of the second core for other activities. An on-demand scan during normal work is therefore possible and should not slow down the machine noticeably. Sophos Anti-Virus will re-scan only those files that are changed, reducing the time needed for the scans.
Sophos has pre-execution detection (Behavioral Genotype Protection) which is able to detect new malware variants and suspicious files before they are executed as well as runtime detection, which monitors the activities of executed files and reports/blocks them if they are doing something suspicious. This HIPS functionality also protects against buffer overflow attacks. The runtime protection will report or block (depending on how the administrator configured it) e.g. supsicious modifications to the registry, suspicious process activities or file modifications. In our test we saw the HIPS alerting some non-malicous files as suspicious (mainly because they were packed with exotic packers). Sophos also alerts when launching or installing e.g. ICQ, MSN Messenger, Skype, etc. But this it not a bug, it is a feature called application control: Sophos is targeted for the use in enterprises, where administrators want to control what software is going to be installed, esp. VoIP, IM, P2P software and games, which may pose security, legal, support and productivity risks.
All in all Sophos is an easy to manage anti-virus, ideal for large companies.

5. Copyright and Disclaimer