



Anti-Virus Comparative

Single Product Test

Safe'N'Sec Enterprise Pro

Date: January 2008

Last revision: 26th January 2008

Author: Andreas Clementi

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

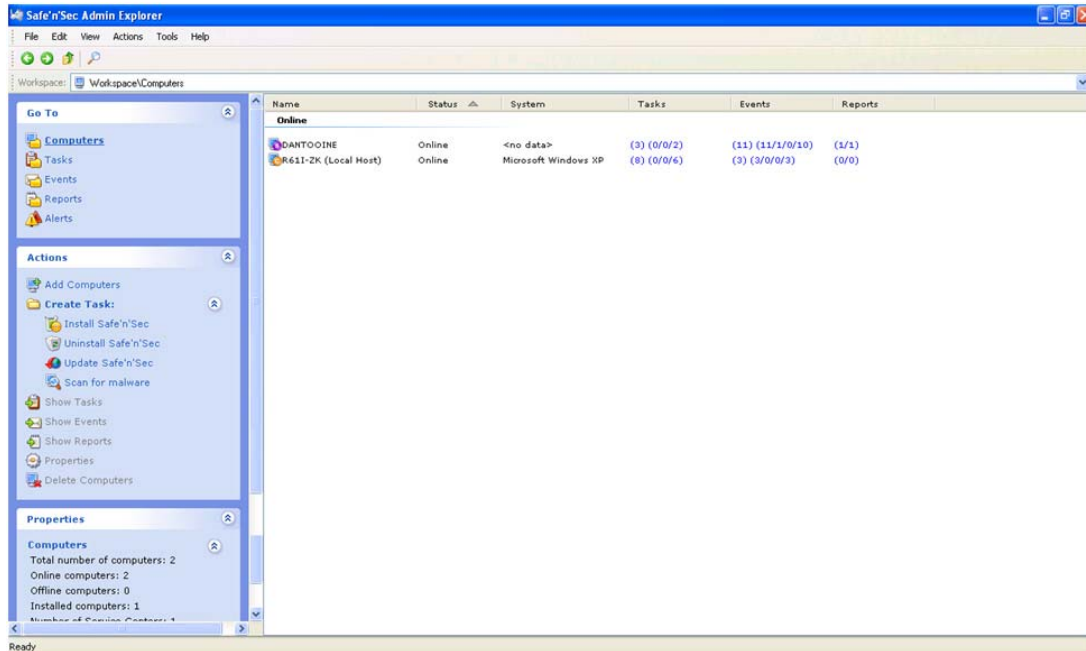
1. Tested product

We tested the latest Safe'N'Sec Enterprise Pro product of S.N.Safe&Software available at the beginning of January 2008. Safe'N'Sec Enterprise Pro is a product designed to protect computers in corporate networks (not for home users). The description of this product (available on http://www.safensoft.com/sns/snsentpro_eng.exe) sounds very promising and we were a bit sceptical from the start if this software can really keep what it promises. Therefore, we tested it regarding prevention of unknown worm spreading in the network, hacker attacks and unauthorized access from outside, prevention of damage caused by various malware, active rootkits, malicious/imprudent actions from inside network users, etc. We decided to include many pictures in this report, for better illustration and explaining what Safe'N'Sec does, how it works and what it offers. A presentation of how to install/uninstall and work with this program is available on the vendor's website.

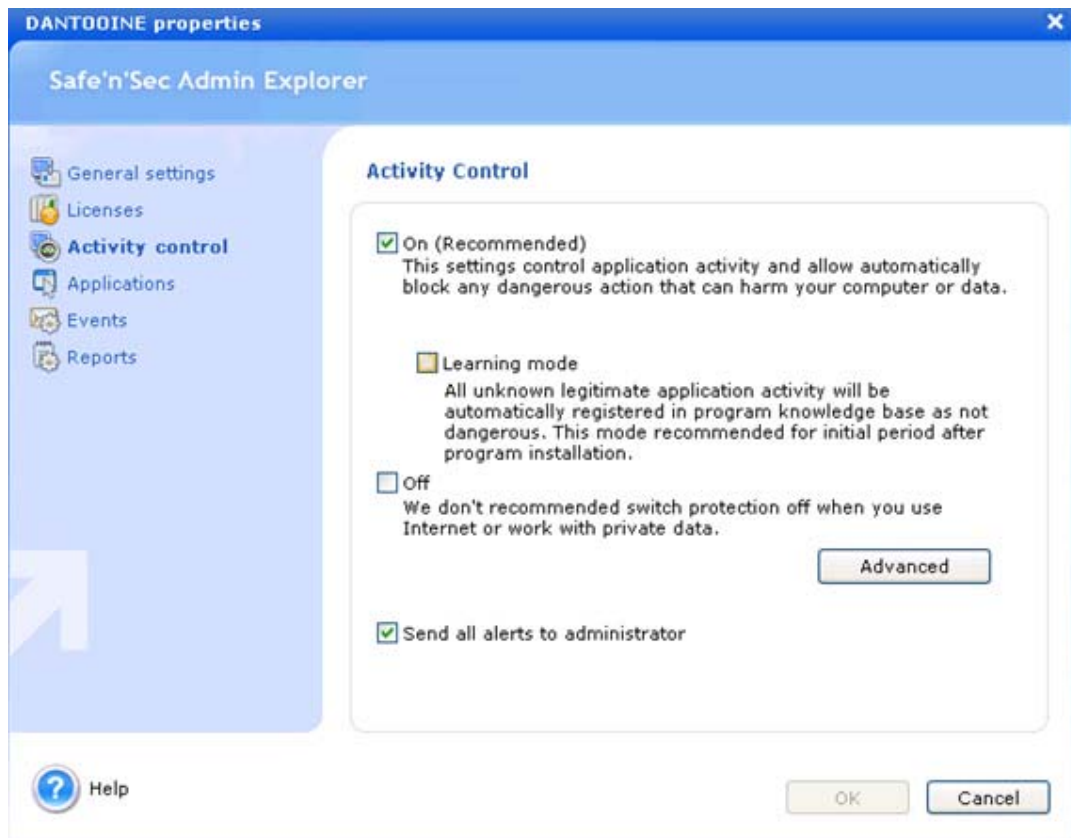
2. Review and Screenshots

We had some issues installing this software over the network, but after consulting the help file, we finally got it working without major problems. We were unable to find a detailed error message about why the installation over the network failed, but the technical support of Safe'N'Sec (which can be reached even on MSN or Skype) replied promptly to support requests.

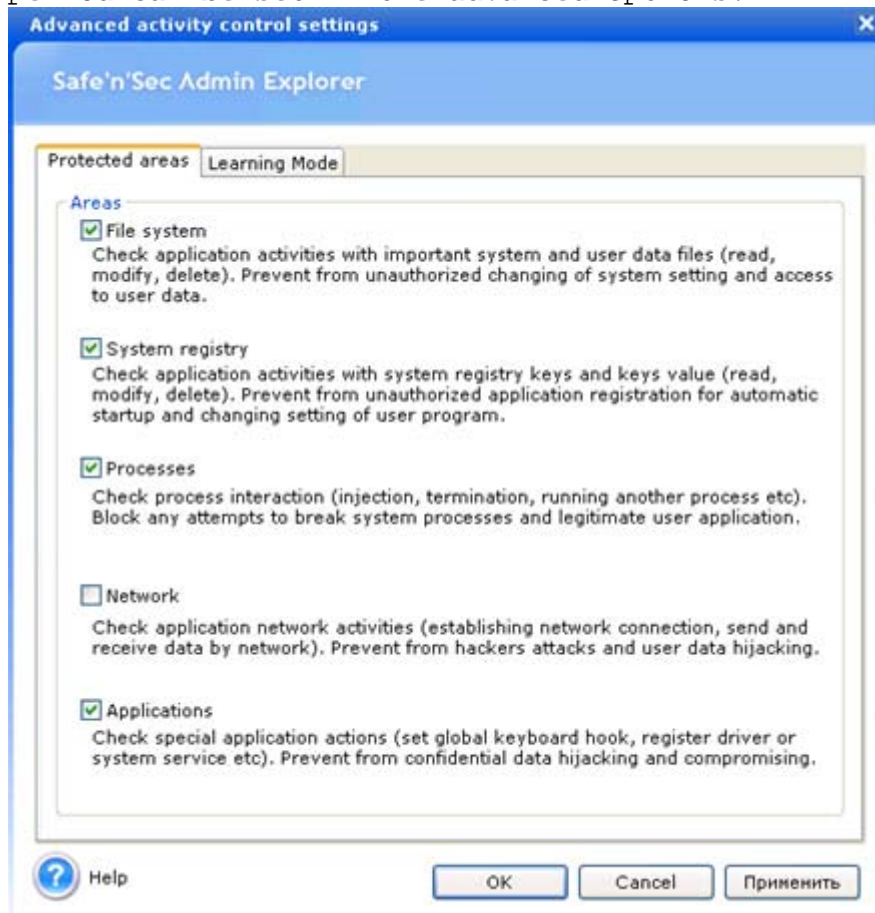
The interface of Safe'N'Sec Admin Explorer is very clear structured and nice-looking, allowing the admin to access and configure everything in no time. Creating automated/scheduled tasks or updating the clients is very easy and fast to perform.



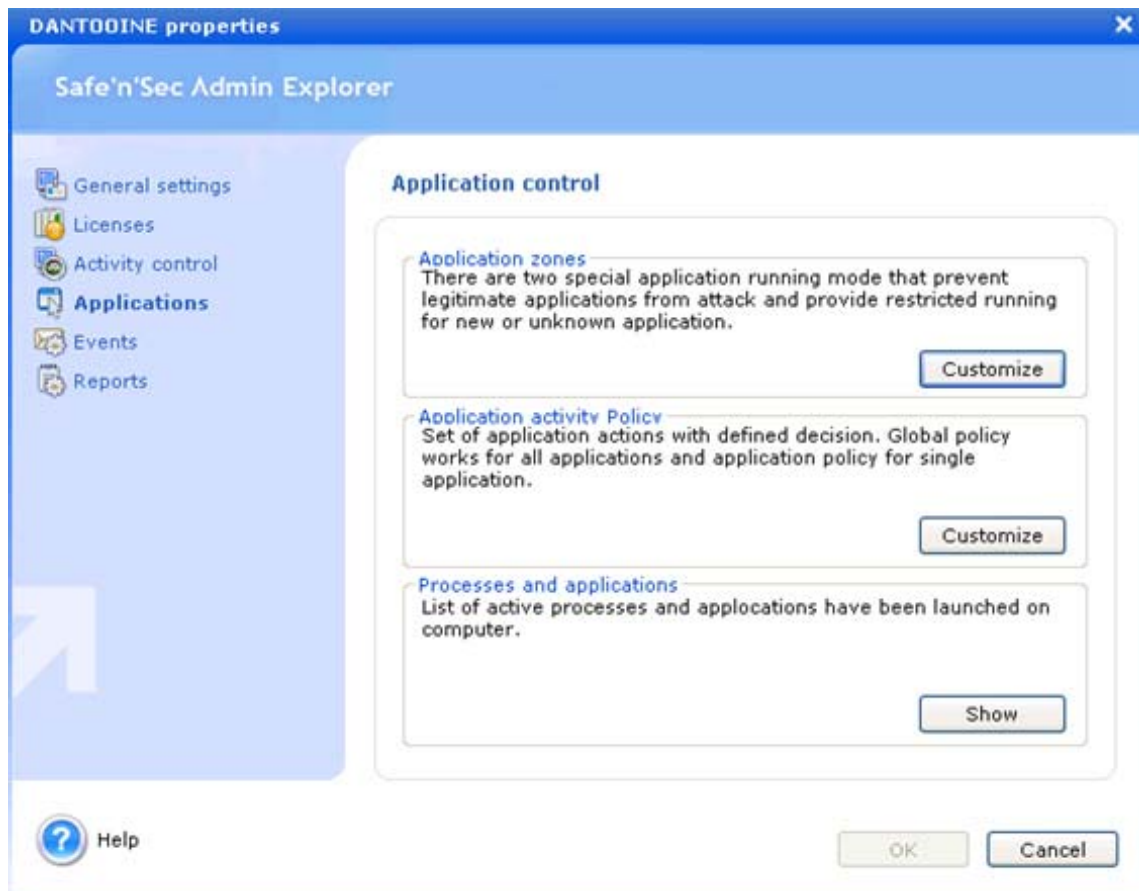
The activity control of Safe'N'Sec Enterprise Pro monitors all activities and if configured properly it blocks any kind of malicious action. As it can be seen in the Advanced settings of Activity Control, the program had - at the time of testing - still some minor bugs (mostly in program setting), like displaying some buttons in Russian language or some English mistypos, as well as not sorting events correctly in chronological order on user request. The mentioned bugs have been already fixed in the meantime.



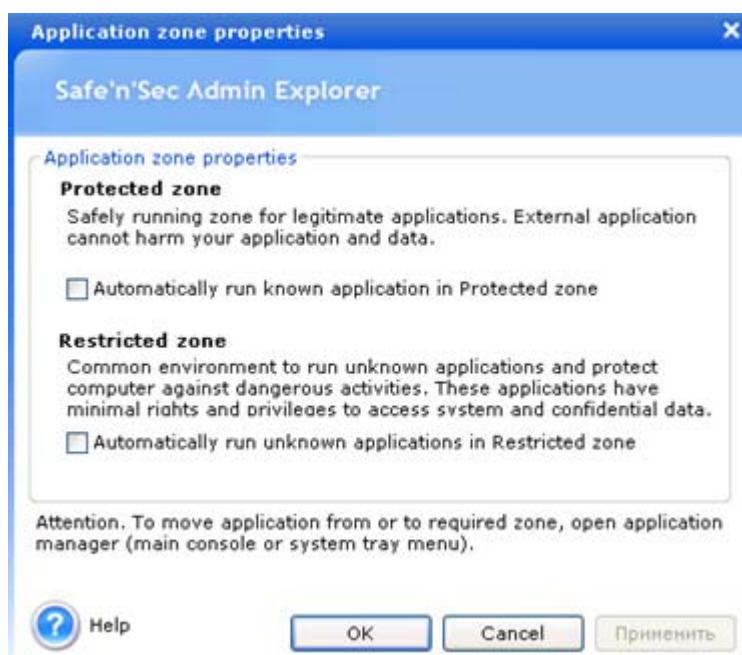
The Activity Control should be setup in a learning mode for some days, in order to avoid false alarms. The duration of the learning period can be set in the advanced options.



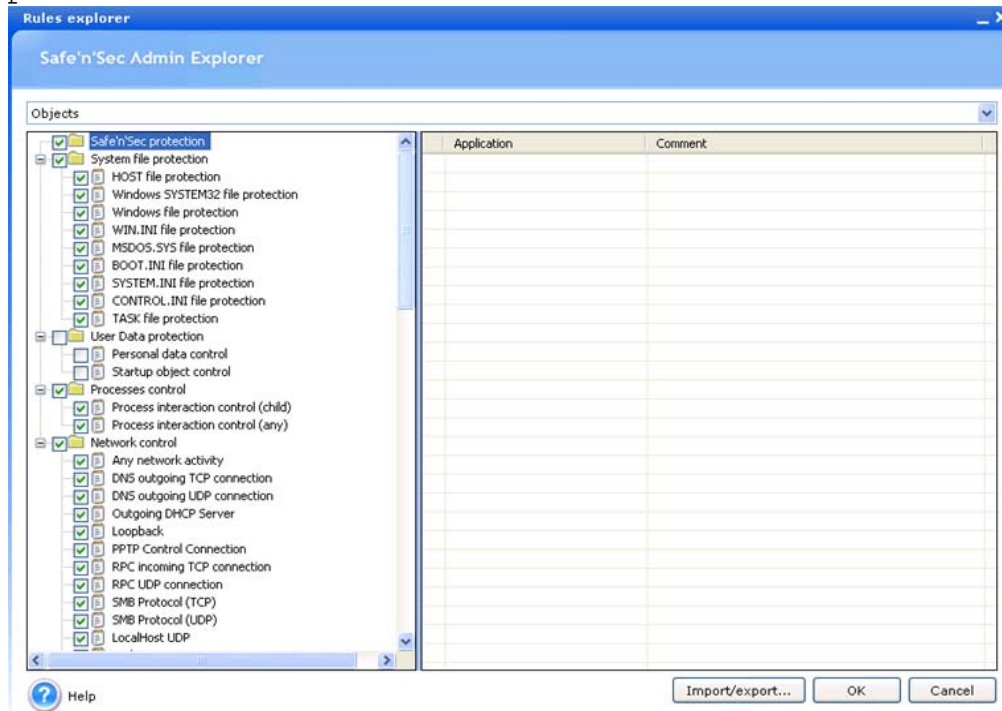
The application control allows running unknown or new applications in a secure zone, in order the system not to be harmed.



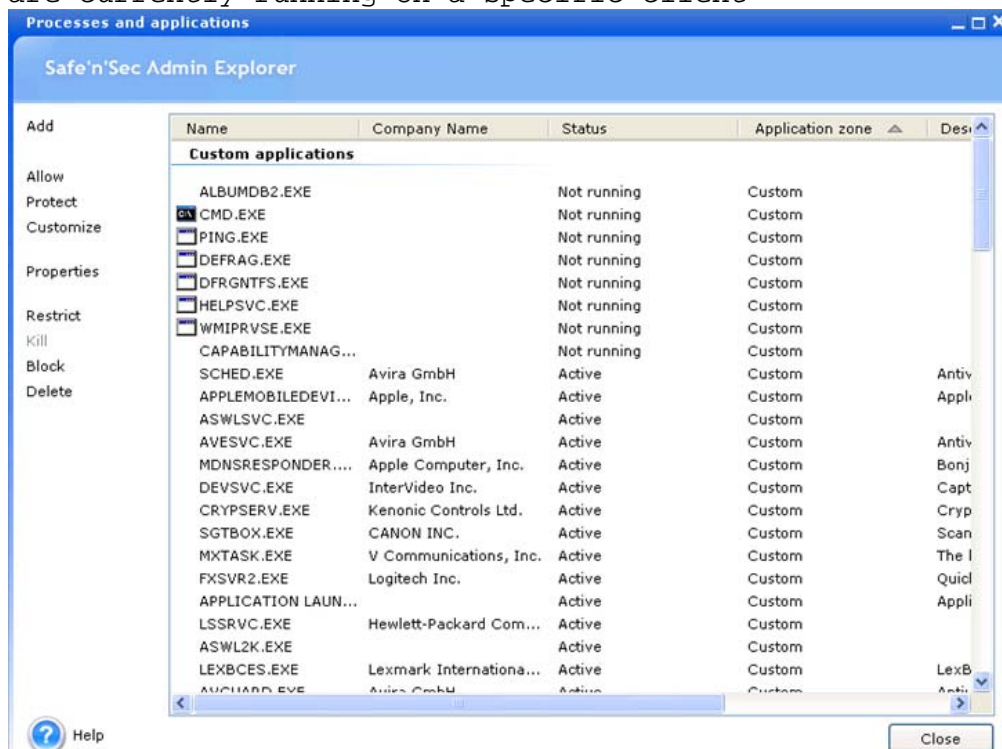
There are two zones for applications: a protected zone (for known applications) and a restricted zone, where unknown applications can be tested:



As it can be seen in the picture below, Safe'N'Sec allows to create rules for practically everything which needs to be under control / protection.

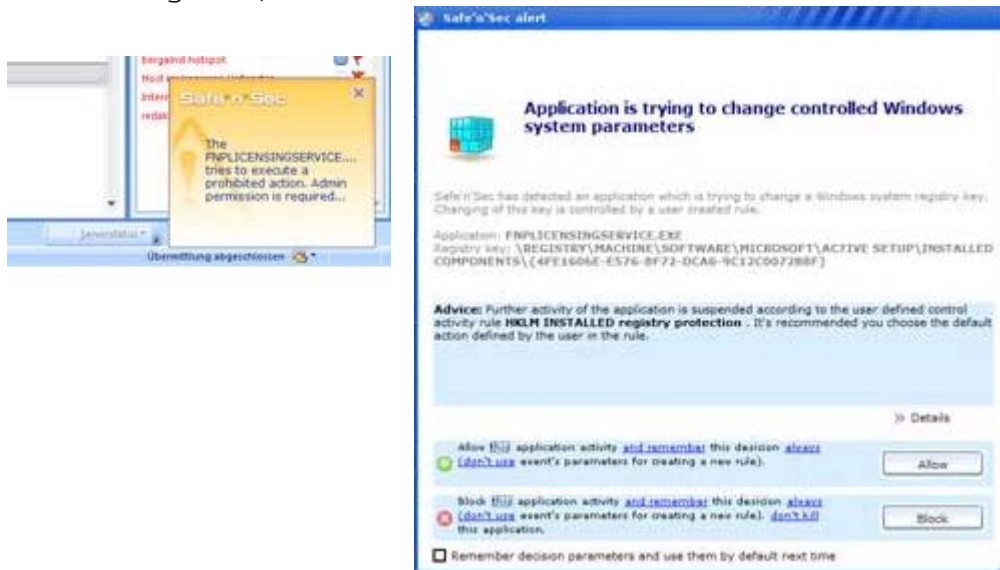


The admin can also see and control which processes and applications are currently running on a specific client:



Safe'N'Sec runs silently in the background and takes very less system resources. Safe'N'Sec has also firewall functions integrated and a version including an Anti-Virus module is also available. If needed, Safe'N'Sec can also work with any other antivirus or firewall, providing additional protection against zero-day malware and network intrusions.

When e.g. malware tries to harm the system or a new unauthorized software is getting installed, Safe'N'Sec will show a warning window notifying that it has blocked the potentially malicious action or that the permission of the Admin is required (depending on how it was configured)



Some key features of Safe'N'Sec Enterprise Pro:

1) One of the most useful features of Safe'n'Sec Enterprise in comparison with other HIPS class products is a self-education mode. This mode is downloaded automatically immediately after Safe'n'Sec Enterprise setting and controls applications activity and save the data about applications' actions for further analysis. After Safe'n'Sec Enterprise installation the program uses the integrated database of well-known applications and activity control policies of these applications. This database is periodically updated with Safe'n'Sec updates. However, corporate workstations can have some programs installed which are unknown to Safe'n'Sec Enterprise but are used regularly and Safe'n'Sec can detect some actions of such programs as potentially dangerous. The self-education mode is aimed to conduct an automatic research and creation of activity control policies for such unknown applications. During the education period Safe'n'Sec automatically creates activity control policies for such applications without system administrator involved.

The education mode is applied to the applications which have been installed on workstations prior to Safe'n'Sec Enterprise Client program installation. New or unknown applications which appear during the Internet navigation of workstations' users or which are being copied from different electronic devices can be potentially malicious. Thus, they are executed in an isolated zone by default. The self-education mode can have time limitations which system administrator can set manually and after that Safe'n'Sec Enterprise will automatically be switched to the Protection mode.

2) One of the most useful features for system administrators is the mobile management console. This console in Safe'n'Sec Enterprise is not tied to any specific workstation in the network so that system administrator can easily administrate the whole network and control service tasks execution from any workstation. All databases containing common settings and other necessary tools are stored on SQL server for administrator's convenience.

3) Also the most frequent and efficient settings of intrusion prevention systems for different types of servers are foreseen, such as web servers, server databases etc.

4) The most interesting module in Safe'n'Sec Enterprise is Safe'n'Sec Rootkit Detector (RD) which is able to detect hidden modules on kernel level (drivers), detect system functions interceptors and search for hidden processes. During start-up the module registers and downloads the service with dynamically generated name, which is deleted immediately after the work is done without leaving its drivers and records in the register. The applied methods of detection of hidden kernel level modules allow detecting drivers hidden with help of rootkit mechanisms including Direct Kernel Object Manipulation technologies. Besides system structure and system memory analysis, Rootkit Detector uses the "trap" technology. The detection of system functions interceptors includes the analysis of system tables modifications (tables of system services, kernel export, system breaks) and analysis of modifications of the machine code kernel. At that Safe'n'Sec RD checks the integrity of executable files in its database of control sums (for most spread OS builds). The module detects the majority of redirected calls such as JMP, CALL, PUSH-RET, Debug Trap; code modification by not detected adapter (the detector will inform about the interception - *unknown type*); detection of the module processing the intercepted functions. Safe'n'Sec RD will inform about any modifications of machine code kernel and define the name of the nearest exported or SSDT function of the kernel, delta-shift from its point of entry.

Safe'N'Sec Enterprise Pro blocked all attempts to penetrate into the network from outside, as well as blocking 100% of the randomly selected malware and detecting/killing active rootkits. After a training phase (to avoid false alarms) and proper strict configuration, Safe'N'Sec Enterprise Pro is ideal for enterprises, as it allows to control everything what happens in the network. Installing unauthorized/unwanted software will not be possible without the permission of the admin. The version we tested had some minor bugs, which are in the meantime already fixed by Safe'N'Sec team. Nevertheless, from the protection side, Safe'N'Sec Enterprise Pro kept its word - it really works and the licensing scheme is relatively cheap. S.N.Safe&Software provides the most complete protection available - Safe'n'Sec Enterprise with additional Anti-Virus, Anti-Spyware and Rootkit detector modules. A new version of Safe'N'Sec Enterprise Pro with easier installation procedure and other improvements will be released soon.

To know more about this product, go to <http://www.safensoft.com>

3. Copyright and Disclaimer

This publication is Copyright (c) 2008 by AV-Comparatives. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of Andreas Clementi, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

Andreas Clementi, AV-Comparatives (January 2008)