

Sophos Endpoint Security and Control 9.0

In this review, we describe, test, analyze and evaluate Sophos Endpoint Security and Control 9.0, a software security suite that integrates antivirus, client firewall, host-based intrusion prevention (HIPS) against malware (viruses, spyware, adware, Potentially Unwanted Applications (PUAs), worms, suspicious behaviour, etc.), data control, device control for DLP and application control. It operates in TCP/IP environments with Ethernet interface on a range of different operating systems such as Windows, Mac OS X, Linux, Netware and Unix (Solaris, HP-UX). The central management console provides a convenient interface to control, monitor, manage and deploy centralized role-based policies. It includes a highly flexible customized report generating system.

TOOL IDENTIFICATION. KEY FEATURES.

Sophos Endpoint Security and Control 9.0 software security suite is a protection system that includes the following key components: antivirus (AV), client firewall, and data, application and device control. It is all managed from a centralized console that configures and manages all the deployed components and defined policies.



The main features are: (i) Scalable management of a range of operating system platforms. (ii) Policies and role-based administration that reduces the administrator's workload by sharing tasks with other users. (iii) Allows the generation of a wide range of user-based graphic reports that can be customized, scheduled to run at specific times and automatically emailed to a list of addresses. It generates reports on virus alerts, infections and status of protection. (iv) Enables a rapid alert and policy compliance monitoring of all the corporate network computers. (v) Automatic discovery of the computers in the network. (vi) Synchronization with Microsoft Active Directory to enable the automatic protection of new computers that join the corporate network. (vii) The host-based intrusion prevention system monitors and controls suspicious files and behaviour. (viii) Controls sensitive and confidential data movements in order to prevent data loss. (ix) Controls removable storage devices and the installation and use of authorized software applications. (x) Enables the rapid

creation and deployment of security policies through multiple groups. (xi) Centralized malware and PUAs cleanup. (xii) Enables helpdesk privilege assignment and the use of read-only consoles.

The console enables the download of updates from the update managers; this role-based administration enables the delegation by specifying the console authorized users. From the console, you can perform tasks like: data control in order to reduce the accidental leakage of sensitive information from managed computers; device control, aimed to prevent the use of unauthorized external storage devices and wireless connection technologies by blocking these devices; antivirus, that detects, blocks and removes viruses, Trojan horses, worms, spyware, adware and PUAs; the Host Intrusion Prevention System (HIPS) technology, that protects the computers from suspicious files and rootkits, unidentified viruses and suspicious behaviour; application control, that blocks unauthorized applications such as VoIP (Voice over IP), instant messaging (Messenger), file sharing and gaming software; and the client firewall, that prevents from worms, Trojan horses, spyware, data leakage and sensitive information distribution: it also prevents from intrusion of internal and external attacks.

ENTERPRISE CONSOLE. EVENT VIEWERS

The following four components are included in the Enterprise Console architecture:

- (i) **Management console.** Enabling the protection and management of the corporate network computers.
 - (ii) **Management server.** Manages updates and communications.
 - (iii) **Database.** Stores network computers data. In large networks it is useful to install the database on several servers in order to balance the process load.
 - (iv) **Update Manager.** More than one update manager can be installed. It downloads software and updates automatically from the Sophos web servers.
- The Console is unique and automati-



The Sophos Endpoint Security and Control 9.0 software security suite is a protection solution that includes the following key components: antivirus (AV), HIPS, client firewall, and data, application, and device control. Machines of a range of operating systems (such as Windows, Mac, Linux and Unix) can be protected from the console, where the software is centrally managed. Its ease of use, the satisfactory performance, the outstanding extras such as 24/7 support, easy installation and configuration, and simplified, quick, highly robust and guided policy management are remarkable.

cally allows the central deployment, management and configuration of Sophos security software on computers running different operating systems like Windows, Mac, Linux and Unix. Amongst the main features we find:

(i) Network protection against viruses, Trojan horses, worms, spyware and unknown threats, adware, and other potentially unwanted applications. (ii) Control over the applications that can be executed in the network. (iii) Client firewall protection management in endpoint computers. (iv) Evaluation of computer compliance with the conditions established previously to allow opening a new network session and applying compliance. (v) Reduction of accidental data loss and unintentional transfer of sensitive data from endpoint computers. (vi) Preventing the use of unauthorized external storage devices and wireless connection technologies.

The console graphic interface includes the following elements:

(1) Dashboard. Provides a quick and comprehensive overview of the network security status. For example, the dashboard enables the visualization of the computers with events over a specified threshold within the last N days.

(2) Computers List. Includes two views: (i) Endpoints. Allows you to view the endpoint computers in a selected group. This view has several tabs: the status tab displays whether the computers are protected by the on-access scanner, if they comply with group policies, which policies have been applied, if the software is updated and if there are any alerts for the endpoint. The other tabs provide further information about the previous items. Icons are used in this view to indicate alerts, protection status, the status of each component, and whether the software has been (or is being) installed.

(ii) Update managers. The Update managers view shows which ones have been installed. In this view, security software automatic updates from the Sophos web site can be set up, and the status and details of the update managers can be viewed.

(3) Groups Panel. Displayed when the 'endpoints' view is selected. It allows you to create groups, place selected computers within them, and import containers from Active Directory (with or without computers), and use them as the console computer groups.

(4) Policies Panel. Displayed when the 'endpoints' view is selected. It allows you to create or change the policies that are applied to computers groups. The solution includes a range of default policies.

(5) Software subscriptions Panel. Displayed when the 'Update managers' view is selected. It allows you to create or edit the Sophos software subscrip-



Fig. 1.- View of the Endpoint Security and Control 9.0 Console.

tions that are required for each platform you wish to protect.

(6) Toolbars. Icons on the toolbar include the 'Find new computers' button, which enables the discovery of new computers in the network and adding them to the console, as well as 'Create Group', that allows you to create new groups of computers, and 'View/Edit policy' that make possible to perform actions on the policy selected in the corresponding panel. The 'Protect computers' button deploys the antivirus software and the firewall on the selected computers. There is also a 'Reports' button that enables the generation of reports on alerts and events in the network, an 'Endpoints/Update managers' button, that toggles the two views, as well as a 'Dashboard' button to open the Dashboard.

When an Application Control, Data

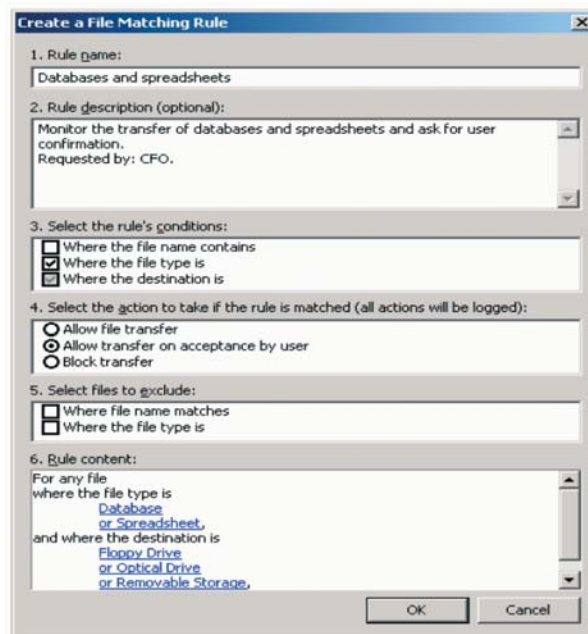


Fig. 2.- Interface for the creation of rules.

EQUIPMENT USED IN THE EVALUATION

♦ Equipment for the central management console, workstations and servers with Windows 2008/2003/2000 and VMWare ESX/W, PCs with 3 GHz Intel Core 2 Quad processors with 2GB RAM, 160GB hard disk, DVD/CD-ROM, WXGA graphic card, NIC card 10/100/1000 base T compatible with NE2000/NDIS. Browsers: Internet Explorer, Firefox, Safari, Opera, Netscape, Flock, SQL Server 2005, LDAP Servers, Windows Active Directory and DNS. Microsoft .NET Framework v2.0 SP1. Windows Installer MSI v3.1. Operating Systems: Linux, Unix (Solaris, HP-UX), Mac OS X, Network, Windows XP/2000.

♦ Nine local networks. Ethernet 10/100/1000 BaseT with IEEE 802.2-LLC, as physical support for the communications with Medium Access Control Protocol or MAC CSMA/CD. Internet Access.

♦ Hubs / 16 port switches Ethernet 10/100/1000. Analog modems for RTB/RTC V.90/ITU-TSS (56 Kbps) and digital cards RDSI-BE 2B+D/Basic Access-BRA as external switched access, and ADSL/Cable Modem connections. GSM/GPRS/UMTS access. Eight routers. Four WI-FI access points, IEEE 802.11g/b/a. Six printers.

♦ Protocol analyzer for monitoring the communication exchanges on all the levels of the architecture.

♦ Modules for evaluating the cryptographic coding mechanisms, authentication. Cryptanalysis valuation module.

♦ Test module for security measures and performance with a range of traffic loads and number of users. Traffic generators. EICAR tests.

♦ Batteries of attacks: malware, spyware, adware, zombies, spam, confidential information theft, policy non-compliance, etc., under manageable control of traffic loads.

Control, Device Control or Firewall event occurs on an endpoint computer, the event is sent to the Console and can be viewed in one of the event viewers.

The events viewer allows you to investigate the events occurred in the network. You can also generate events based on configured filters. For example, a list of all the Data Control events generated by a certain user during the last N days.

GROUPS AND POLICIES

A group is a folder that stores a number of computers; each group is configured with aspects such as updating, AV, and HIPS and firewall protection. A policy is a set of rules that are applied to all the computers within a group. When the Console is installed, the default policies provide a standard level of security; the policies can be edited or more specific new ones can be created, tailored to the type of organization. Before computers are assigned to groups, they are stored in the unassigned group. It is not possible to apply policies, to create sub-groups, or to move or delete the unassigned group.

The tool evaluated here restricts the access to certain parts of the endpoint software to members of certain groups. When the tool is installed, each user is initially assigned to one of three Sophos groups, based on their Windows group. The correlation between Windows and Sophos groups is as follows: Windows administrators with Sophos administrators, Windows power-users with Sophos power-users, and Windows users with Sophos users. The users not assigned to a Sophos groups are guest users that can only carry out on-access scanning and right-click scanning. The Sophos users can carry out these tasks and also open the Endpoint Security and Control user interface, configure and execute on-demand scans, configure right-click scans, manage the quarantined items that they have access to, and create and configure the firewall rules. The Sophos power-users have the same rights as the Sophos users, and the following additional ones: greater privileges in managing quarantined items, and access to the authorization manager. The Sophos administrators can use and configure any part of the tool evaluated here.

TYPES OF ANTIVIRUS SCANS. QUARANTINE MANAGEMENT

The AV functionality allows two types of scans: (i) **On-Access**. When

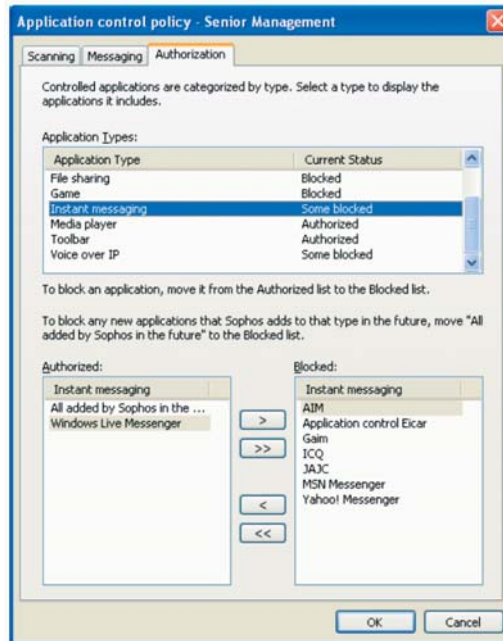


Fig. 3.- Application control Interface in Sophos Endpoint Security and Control 9.0.

you can scan a single file or the whole computer at once. The Quarantine Manager allows you to deal with items identified in the scan that were not eliminated automatically during the process. Each item is quarantined for a particular reason, such as: (i) Non-cleanup options were chosen (delete or move) for the scan type. (ii) A cleanup option was chosen for the scan type, but it failed. (iii) The item had multiple infections and still contains additional threats. (iv) The threat was only detected partially and a complete scan is required to make a complete detection. (v) The item is behaving suspiciously. (vi) The item is a controlled application. Adware, PUAs and multi-component infections detected during on-access scans are always reported by

a file is accessed (when it is copied, saved, moved or opened), the antivirus scanner scans the file and allows access to it only if there is no threat to the computer or if it has been pre-authorized for use. The tool displays an alert when a threat is found. There are two scenarios where the on-access doesn't automatically block malware: (a) When it has been temporarily deactivated. The on-access scanner may have to be temporarily deactivated by a Sophos administrator in order to carry out maintenance operations and troubleshooting, after which it should be reactivated. When the on-access scanner is disabled, the on-demand scanner can still be switched on. (b) When specific file extensions have been excluded from scans. You can specify which extensions you would like the on-access scanner to scan. (ii) **On demand**. There are several ways that the user may scan on-demand; for example,

the Quarantine Manager. The automatic cleanup functions for adware, PUAs and multi-component infections are available after an on-access scan. The cleanup process can fail if the user has insufficient privileges; an administrator can deal with the remaining items.

DEVICE CONTROL AND DATA CONTROL FUNCTIONALITIES

The device control feature blocks or enables two types of devices: (i) Storage. Removable storage devices such as USB flash/pen drives, PC Card readers and external hard disk units, and optical disc units such as CD-ROM/DVD/Blue-ray drives. (ii) Network. Modems, wireless units such as Wi-Fi/IEEE 802.11 interfaces, Bluetooth interfaces, IrDA infrared interfaces. The feature prevents the connection of devices to a computer for maintenance or the resolution of problems. This functionality can be activated or deactivated from the management



Fig. 4.- Screen displaying computers with problems.



Fig. 5.- The Dashboard in Sophos Endpoint Security and Control 9.0.

console: for example, a Sophos administrator can deactivate device control in order to install software from a CD.

If the data control functionality is activated in a computer, a blocking policy is applied to certain files, as the example below illustrates: Data control will block any attempt to move files to a monitored storage device using any of the following methods: (i) Saving data from within a program. (ii) Using the DOS copy command. (iii) Creating a new file in the device using Windows Explorer. In order to move the files to the storage device, you must save the file to the hard disk or a network driver and then use Windows Explorer to copy them to the storage device. When this approach is applied, the data control policy can intercept all the files for analysis before writing them on the storage device.

PROTECTION DEPLOYMENT WORKFLOW

In order to protect a corporate network with this tool, you need to perform the following steps: (i) **Creating groups.** You can either create groups one-by-one or you can import containers (with or without computers) from Active Directory and use them in the Console. It is useful to import containers from Active Directory without computers, assign group policies to them, and then add computers to these groups, by synchronizing the groups with Active Directory. (ii) **Establishing policies.** The Console includes a group of default policies for protecting a network; you can customize and personalize them as needed. (iii) **Finding the computers on the network and add them to the console.** You only need to do this if you haven't imported containers and computers from Active Directory. (iv) **Protecting the computers.** There are two approaches: (a) Using the computer protection wizard. (b) Automatic protection by synchronizing with Active Directory. (v) **Checking if the computers are protected.** In the Console, you can see if each computer is protected, including whether or not on-access scanning is enabled. (vi) **Cleaning up found threats using the Quarantine Manager if appropriate.**

DATA CONTROL POLICIES

Data control policies allow you to manage the risks associated with the accidental transfer of sensitive

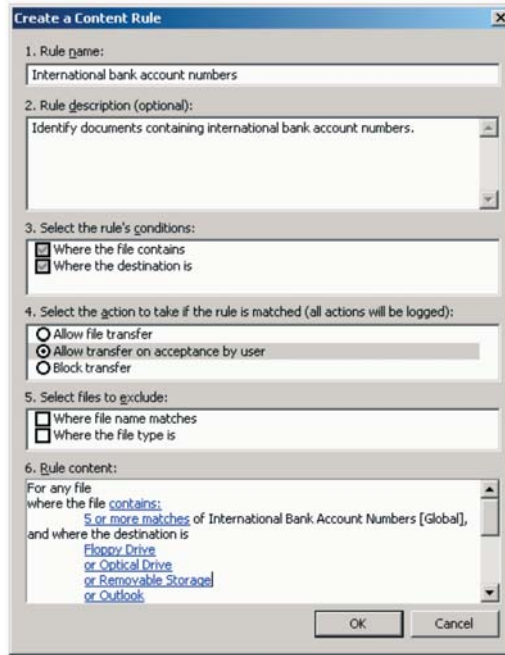


Fig. 6.- Content Rule creation interface.

data from your endpoint computers. Every organization has its own definition of sensitive data, some examples are: client records that contain identifiable personal information; financial data such as credit card numbers, or confidential documents. When a data control policy is activated, the software monitors user actions in common data exit points such as:

File transfer in storage devices (removable storage, optical support media and disc-based media), file upload to applications (Web browsers, email clients, instant Messaging clients such as Messenger, etc.).

A rule for data control is composed of three elements:

(i) **Items to be compared:** Options include file contents, file types and file names.

(ii) **Points to be monitored.** Such as types of storage device and applications.

(iii) **Actions to be taken.** Such as enabling file transfers (monitoring mode), enabling the transfer if the user accepts the notification (training mode) and blocking transfers. For example, the Data Control rules can be defined to log the transfer of spreadsheets using Internet Explorer or to enable the transfer of client addresses to DVD, once the transfer has been confirmed by the user. The definition of sensitive data can be a very complex task. A ready-built library of Content Control Lists is provided, including definitions of sensitive data. This library covers a wide range of formats of financial and personal data and is kept up-to-date by Sophos Labs. It is also possible to introduce customized or personalized definitions.

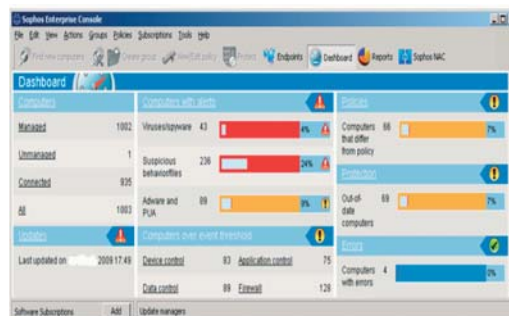


Fig. 7.- Update managers view in Sophos Endpoint Security and Control 9.0.

FIREWALL POLICIES. ROLES AND SUB-ESTATES MANAGEMENT

Firewall policies specify how the firewall protects the organization's computers. The firewall events viewer enables the monitoring of blocked traffic, the applications and the processes used, and enables the creation of rules to activate or block them. It is possible to configure the firewall for a double location; in this case, the primary location would be the corporate network based on DNS, where open access can be allowed, and the secondary location may require a more restricted access. There is a range of working methods for the firewall: (a) **Inter-active.** The users can be educated about what to block or permit. (b) **Default blocking.** The administrator is responsible for blocking or permitting traffic from the Console.

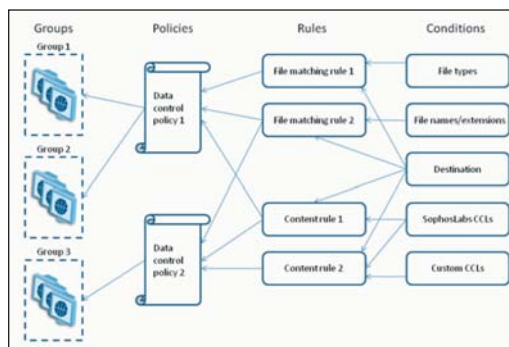


Fig. 8.- Diagram of data control building blocks in Sophos Endpoint Security and Control 9.0.

(c) **Blocking just this time.** Used when the user is not sure whether to block or not.

There are also four pre-configured administrative roles in the Console: (i) System Administrator. Default role with maximum administration rights. This role cannot be edited or deleted. (ii) Administrator. Default role with the right to manage all aspects of the software but not to manage roles in the Console. This role can be renamed, edited or deleted. (iii) Helpdesk. Default role with rights to undertake corrective tasks such as cleaning up or updating computers. This role can be renamed, edited or deleted. (iv) Guest. Pre-configured role with read-only access to the Console. This role can be renamed, edited or deleted.

FINAL CONSIDERATIONS

This solution was subjected to a constant and exhaustive range of tests over a period of twenty days. The evaluation of the Sophos software shows protection results over 88.7% in a 'worst case scenario'. In terms of speed of administration, wealth of functionality and user-friendliness, the console rated 96.8%. The results of constant performance tests

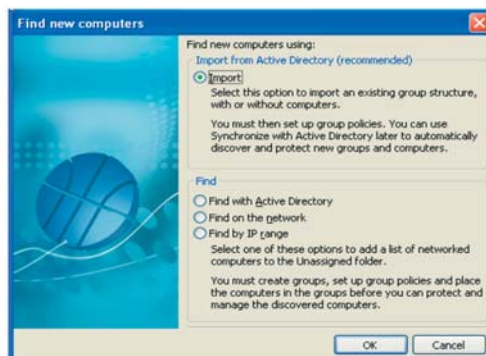


Fig. 9.- New computers finding interface.

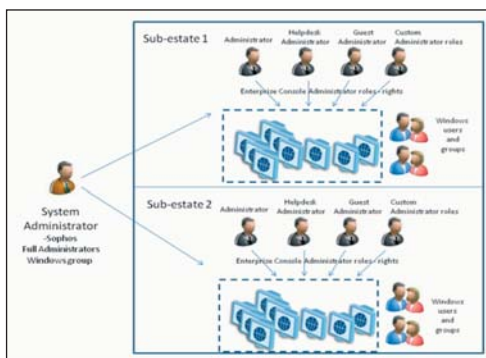


Fig. 10.- Approach to role-based administration in Sophos Endpoint Security and Control 9.0.

were around 92%, and the results of the AV effectiveness and prevention of information theft were 93%. It is worth pointing out that no significant instabilities were found (fewer than 1.8%) in stress and fatigue tests with load gradients, injection of threats and prolonged attacks. The tests related to policy effectiveness gave very satisfactory results, with values of 95.4%, and the tests concerning the update operations achieved values of around 92.3%. The rates for overall false positives were satisfactory, with especially good results for HIPS and AV. The conclusions of the centralized management tests were around 93%.

The generation of customized personalized reports scored 94% and the creation, deployment and personalization of policies scored 92%. As for the results of the control of data/applications, they were very satisfactory, scoring 94.2%. The control of removable devices achieved 94% and for wireless communication technologies, 93%. The results of the

firewall tests were 90.1%. Lastly, the combined AV, HIPS and firewall operating procedure came out with a satisfactory result of 93%. ■

CONCLUSIONS

- ♦ **OBJECTIVE:** A security software system that integrates antivirus, HIPS, client firewall, data control, application control and device control. It is managed centrally from an administration and control Console from which machines running Windows, Mac, Linux and Unix can be protected. The Console is able to disinfect computers remotely, create and deploy policies and delegate administration tasks with on role-based administration; it is also possible to generate reports very flexibly and quickly. It automates and speeds up protection with Active Directory synchronization.
- ♦ **NOTES / LIMITATIONS:** A user cannot edit a policy applied outside their active sub-estate. They can only view the sub-estates one at a time. It is not advisable to arbitrarily modify the ICMP default configurations, the global rules and the rules for applications in the firewall policies. Content scanning can be a very intensive process, which must be taken into account when content rules are created for a large group of computers. If error events are generated by an application when configuration files are opened, this can be resolved by adding customized location exclusions. The tool maintains the configuration of the on-access scan, even after restarting the computer. If there are multiple alerts or errors for a computer, the greatest priority icon is displayed in the alerts and errors column. The descending order of seriousness is virus/spyware, suspicious behaviour, suspicious files, adware/PUAs, and errors in the software, such as installation errors. When the console is installed, the default policies are set up automatically and can be applied to any group you create. The optimum number for updating in the same UNC location is from 550 to 650 computers.
- ♦ **IMPACT OF ITS USE:** Integration and synchronization with Active Directory. Own roles can be created or the predefined roles can be used. A user can only view the sub-status they were assigned. The Console enables commuting to what sub-status should be paid attention. Ease of use. It enables the generation of very granular and customized reports.
- ♦ **BENEFITS / KEY ADVANTAGES:** Friendly use. Satisfactory performance. Outstanding features. Appropriate 24/7 support. Simple installation and configuration. Simplified, quick and guided management of highly robust policies. The update process can be modified in several ways to reduce the network impact and to achieve a better integration into the existing infrastructure. The efficiency of the AV functionality is especially satisfactory. Monitoring and configuration of multiple operating systems from a single Console. It finds and disinfects computers remotely in one operation. Enables direct policy creation and their application to multiple groups simultaneously. The Console makes possible to manage all the features from a single point. It provides the possibility of excluding specific Microsoft Exchange directories from on-access scans when performance could be affected.
- ♦ **DOCUMENTATION:** suitable. It uses .pdf files.
- ♦ **TOOL'S STRUCTURE:** (1) Centralized administration and role-based management Console. (2) Antivirus, HIPS, data control, application control, client firewall, device control features, etc.
- ♦ **OVERALL RATING:** Scalable security software solution that includes antivirus, HIPS, data control, application control, client firewall and device control. It is administered, controlled and monitored from a centralized role-based console that allows the delegation of management functions and includes a wealth of features that make it easy to use. It allows the protection of multiple operating systems. It includes pre-defined policies to help quickly deploy protection across the network. It includes a well-designed and extremely flexible reports manager. The policy deployment is quick, customizable and well integrated into the protection environment. The effectiveness of the combination of AV, HIPS and firewall is satisfactory. The update mechanism is fail-tolerant.

EVALUATION TEAM

DIRECTOR:
Prof. Dr. Javier Areitio Bertolin
 Professor of the Faculty of Engineering. ESIDE.
 Director of the Networks and Systems Research Group.
UNIVERSITY OF DEUSTO

