

- Protects against 100% of known and unknown threats
- Safeguards against zero-day threats and targeted attacks
- Controls proliferation of unwanted applications from burdening network bandwidth
- Maximises benefits of new technologies and minimises risk of network disruption
- Enables adherence with software license agreements

Protect Against Malware, Spyware and Zero-Day Threats

The security landscape is shifting from large, widespread malware outbreaks to targeted, focused threats. Traditional solutions cannot possibly defend against these types of attacks as evidenced by the fact that of the 99 per cent of enterprises which have anti-virus solutions, 62 per cent suffered an infection in 2005 ¹.

End-points are the likeliest entry point for malware. And the threat is proliferating – a leading anti-virus vendor expects to double its recorded threats to 400,000 by 2008.

With more end users installing non-business related programs and an increased number of threats, 85 per cent of corporate machines need to be rebuilt every year ¹. The average enterprise downtime for each virus attack is 23 person days, with 31 person days required to achieve full recovery ².

Complete Prevention of Malware and Unwanted Applications



Comprehensive Policy Enforcement of Application Use

Sanctuary[®] Application Control, a component of Sanctuary, provides policy-based enforcement of application use to secure end-points from malware, spyware, zero-day threats and unwanted or unlicensed software. By employing a whitelist approach, Sanctuary Application Control enables only authorised applications to execute on a network, server, terminal services server, thin client, laptop or desktop. Unauthorised applications are prohibited from executing.

Malware is virtually eliminated and control is given to administrators over unwanted and unauthorised applications, including bandwidth-stealing P2P applications.

Simple, Fast, Flexible Administration and Management

Sanctuary Application Control enables administrators to rapidly identify applications and to assign permissions for applications to users, user groups or a particular computer.

Application policies are linked to user and user-group information stored in Active Directory[™] or eDirectory[™], dramatically simplifying the management of end-point application resources.

Automated Discovery

Sanctuary is automatically set up in non-blocking mode to simplify the discovery phase so that administrators can uncover all of the applications that are executing on the end-points.

Detailed Audit Capabilities

All application execution attempts can be logged, as well as any administrator actions, including changes of any application policy authorisations.

Flexible Authorisation Rules

Administrators can allow trusted users to authorise their own applications, providing ultimate flexibility. Administrators stay informed and in control with the ability to override local authorisation.

Feature	Function	Benefit
Whitelist	Assign permissions for authorised applications to users or user groups, and by default those not authorised are not allowed	Eliminates unknown or unwanted applications in your network, reducing the risk of malware and spyware and ultimately improving network stability
SecureWave File Definitions	Classified, pre-loaded whitelist of all supported OS files	Speeds and simplifies whitelist definition
Automated Application Discovery	Process of identifying, categorising and authorising applications which produces a record of all executables on client computers, file servers and/or local directories	Provides flexible and fast options to create or update whitelists
Automatic Authorisation of Software Updates	Automatic authorisation of Microsoft software updates through integration with Windows Updates: SUS and WSUS	Eliminates risk of accidentally restricting user access to frequently updated Microsoft applications
Script / Macro Protection	Controls execution of VBScript, Microsoft Office VBA and JavaScript with central authorisation or a prompt to local users	Extends application policy enforcement to include scripts/macros for greater protection
Path Protection	Optional file authorisation based on location or path rules; Create a trusted owner, such as administrator, to reinforce security	Provides flexibility to support executable files for which hash definitions are not useful or applicable (i.e. auto-changing .exe files)
Non-Blocking Mode	Execute and log activity for administrator review	Enables Sanctuary to identify current state before defining and enforcing policy
Flexible File Authorisation	Versatile File Processor (FileTool.exe) enables directory and subdirectory scans to discover new applications and packages while online or offline	Provides flexible and fast option to identify new and updated applications for review and ultimately to generate whitelists
Nested Executable File Groups	Hierarchical structure of organising file groups	Provides fast administration of file groups and assignment of user permissions
Relaxed Logon	Executes logon scripts without authorisation and automatically switches system into blocking mode after either a set of time or at the end of the script	Eliminates need to administer logon scripts in Sanctuary without compromising the security of the system
Local Authorisation	Trusted users can authorise applications locally, while maintaining a log for administrator review	Delivers flexibility to the user, without giving up administrative control
Spread Check	Disables suspicious executables that are locally authorised on too many computers	Contains risk of malicious code spreading through network due to local authorisation
Highly Scalable Architecture	Three tier architecture with Database, one or more Application servers, and Client	Provides flexible and scalable deployment options in large and complex networks
Powerful Log Analysis and Reporting	Detailed log analysis with flexible filter, sort and display options and stored query templates as well as central reporting	Demonstrates policy compliance and drills down on suspicious behavior for legal or management follow up
Offline Computer Protection	Local copy of updated hashes and permissions is kept on each machine	Ensures that remote/ disconnected users are constantly protected
Active Directory and eDirectory Support	Leverages user and user group definitions in existing Active Directory and eDirectory	Reduces setup and maintenance of users and user groups
Multi-Language Support	Supports 12 languages on Sanctuary client machines	Improves user experience in international organisations

Also available, Sanctuary Device Control with integrated Sanctuary management console. Sanctuary Device Control provides policy-based enforcement of removable device use to control the flow of inbound and outbound data from your endpoints, reducing the risk of data leakage.

Application Control: Server Edition

Provides server security software that enforces application use policies to secure mission critical servers from unauthorised, illegal or unwanted applications by default and preventing any interruption to the flow of your business.

Application Control: Terminal Services Edition

Enforces application use policies to secure Windows or Citrix terminal services environments from unauthorised, illegal or unwanted applications by default.

System Requirements

Client (Windows 32-bit only)

Windows 2000 (SP 3+) Professional, Windows XP Professional, Windows XPe, Windows Embedded Point of Service, Windows XP Tablet PC Edition

For Sanctuary Server/Terminal Services Edition: Windows 2000 Server or Windows Server 2003

Database

Windows 2000 (SP 3+) Server or Professional, Windows XP Professional, Windows Server 2003

Microsoft SQL Server (2000/2005), SQL Server 2005 Express Edition or MSDE 2000

Server

Windows 2000 (SP 4+) Server or Windows Server 2003

Management Console

Windows 2000 (SP 3+) Server or Professional, Windows XP Professional, Windows Server 2003

Sources

- 1 - 2005 Yankee Group Security Leaders and Laggards Survey
- 2 - 2005 National Survey on Data Security Breach Notification, Ponemon Institute



www.securewave.com
info@securewave.com

North America

13755 Sunrise Valley Drive
Suite 203
Herndon, VA 20171
United States of America
+1 (703) 713 - 3960 Phone
+1 (703) 793 - 7007 Fax

United Kingdom

Midsummer Court
314 Midsummer Boulevard
Milton Keynes MK9 2UB
United Kingdom
+44 (0) 1908 357 897 Phone
+44 (0) 1908 357 600 Fax

Continental Europe and Rest of World

Atrium Business Park
23, rue du Puits Romain
L-8070 Bertrange
Luxembourg
+352 265 364-11 Phone
+352 265 364-12 Fax



© 2007 SecureWave and Sanctuary are registered trademarks of SecureWave SA.
All third party trademarks are the property of their respective owners.