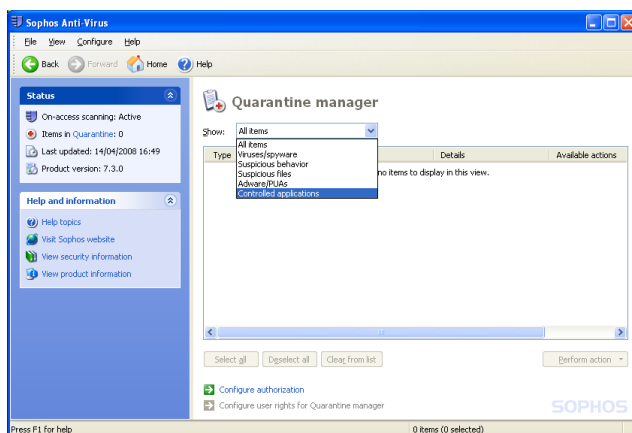


Sophos Anti-Virus for Windows

Sophos Anti-Virus for Windows, part of Endpoint Security and Data Protection, works alongside Sophos Client Firewall and Sophos NAC to provide award-winning protection across thousands of Windows desktops, laptops and servers. A single anti-virus client detects viruses, spyware and adware, suspicious files, suspicious behavior, potentially unwanted applications (PUAs), removable storage devices and unauthorized VoIP, IM, P2P and gaming software in just one scan – eliminating the need for separate standalone products.

Award-winning multi-threat protection in one product

- The Sophos virus detection engine protects Windows servers, desktops, laptops and mobile devices against viruses, spyware and adware, suspicious files, suspicious behavior, potentially unwanted applications (PUAs), removable storage devices and unauthorized VoIP, IM, P2P and gaming software.
- Our single anti-virus client has a built-in host intrusion prevention system (HIPS) to stop zero-day threats. It uses a combination of unique pre-execution detection and runtime technologies to identify unknown malware, suspicious files and behavior.
- Legitimate software applications like VoIP, P2P, IM, media players and games can be blocked or authorized for different groups of computers. This can be centrally controlled using ActivePolicies™ in Sophos Enterprise Console.
- Device Control blocks or allows removable storage including USB sticks, music players, external hard disks, CD/DVD drives and wireless connection technologies: Wi-Fi, Bluetooth and Infrared (IrDA).
- An easy-to-use, integrated quarantine manager, enables malware, potentially unwanted applications, suspicious files and controlled applications to be authorized, deleted, or disinfected.



Key benefits

- » Removes the need for point products. A single scan detects viruses, spyware, adware, suspicious files and behavior, removable storage devices and controlled applications
- » Automatically stops unknown malware, with Behavioral Genotype® Protection uniquely analyzing behavior before code executes
- » Identifies unknown malware, and suspicious files and behavior through built-in pre-execution and runtime intrusion prevention technologies
- » Controls use of legitimate software applications like VoIP and IM
- » Manages use of removable storage, optical media drives and wireless networking protocols
- » Can be centrally installed, set-up and monitored across the network
- » Provides role-based administration privileges assigned with Helpdesk and Read-Only Consoles
- » Enables anti-virus and HIPS policy to be quickly created and applied across multiple groups
- » Allows fully centralized system cleanup of files, registry entries, and running processes
- » Includes an integrated quarantine manager for deleting, disinfecting or authorizing files
- » Updates automatically with the latest protection from SophosLabs™ – a global network of threat analysis centers
- » Scans on access, on demand and on schedule with Decision Caching™ technology ensuring that only changed files are rescanned
- » Includes 24x7x365 support during the license and one-to-one assistance

Automated, simplified, central management from a single console

- Sophos Anti-Virus is managed by Sophos Enterprise Console alongside Sophos Client Firewall. The Security Dashboard shows real-time security status, and automatic email alerts are sent when chosen security thresholds are threatened.
- Synchronization with Microsoft Active Directory® ensures deployment is fast and new computers are automatically protected as they join your network.
- Integrated application and device control means there is no additional deployment or management overhead. Policies can be configured for groups of computers to reflect the security requirements for specific locations or departments.
- You can delegate limited access without handing over full administration rights. Helpdesk Console lets users take specific remediation actions, Read-Only Console gives a view of a threat situation but without the permission to take any action.
- A single ActivePolicy incorporating both anti-virus and HIPS allows the rapid creation and application of security settings across multiple computers and groups simultaneously.
- Updated protection is automatically downloaded every ten minutes and distributed across the network as frequently as every five minutes, at pre-set times or on demand.
- Endpoint computers can be completely disinfected in a single operation. Registry entries, running processes, and files on disk are removed if needed.
- Security and management information is delivered through customizable, integrated graphical reports. Virus alerts can be emailed instantly or to schedule and are displayed on Enterprise Console's Security Dashboard.

Faster, better, proactive protection using innovative technologies

- Genotype® virus detection technology proactively blocks families of viruses even before specific virus signatures are available.
- Sophos's HIPS technology uses the anti-virus engine to identify programs that will behave suspiciously before they execute.
- Behavioral Genotype® Protection scans for multiple specific behaviors and characteristics to proactively protect against zero-day malware, crucially it detects new threats before code even begins to execute.
- Built-in pre-execution suspicious file detection combines with runtime behavior analysis and buffer overflow protection to detect malware, suspicious files and behavior.
- Sophos behavioral rulesets are constantly validated against an extensive library of legitimate applications, to ensure accurate detection.
- Decision Caching technology improves on-access scanning performance by intercepting and scanning only files that have changed since last accessed.
- Rapid threat analysis from SophosLabs and the fastest updates in the industry are downloaded as frequently as every ten minutes.

Industry-leading expertise 24/7

- Our 24/7 customer support operation and SophosLabs™, our global network of threat analysis centres, provide a rapid response to emerging and evolving threats.

Languages available

- English, French, German, Japanese, Italian, Spanish, Simplified and Traditional Chinese.

System requirements

Platforms supported

- » Windows Vista*
- » Windows Server 2003**
- » Windows XP*
- » Windows 2000 Server
- » Windows 95/98 and NT4***
- » VMWare ESX 3.0
- » VMWare Workstation 5.0
- » VMWare Server 1.0
- » Windows Server 2008*

Disk space

- » Windows XP/2003/Vista: 120 MB
- » Windows 2000: 120 MB
- » Windows 95/98: 90 MB
- » Windows NT4: 90 MB

Recommended memory

- » Windows XP/2003/Vista: 256 MB
- » Windows 2000: 256 MB
- » Windows 95/98: 128 MB
- » Windows NT4: 256 MB

* Including AMD64

** Including Itanium

*** Adware and PUA detection, application control, and HIPS are not available on these platforms



Sophos Anti-Virus is also available for a wide range of non-Windows platforms, from gateway to endpoint, including Windows, Macintosh, Linux, UNIX, NetWare and OpenVMS. These solutions are described on separate datasheets.

To evaluate Sophos Endpoint Security and Data Protection, visit www.sophos.com/products