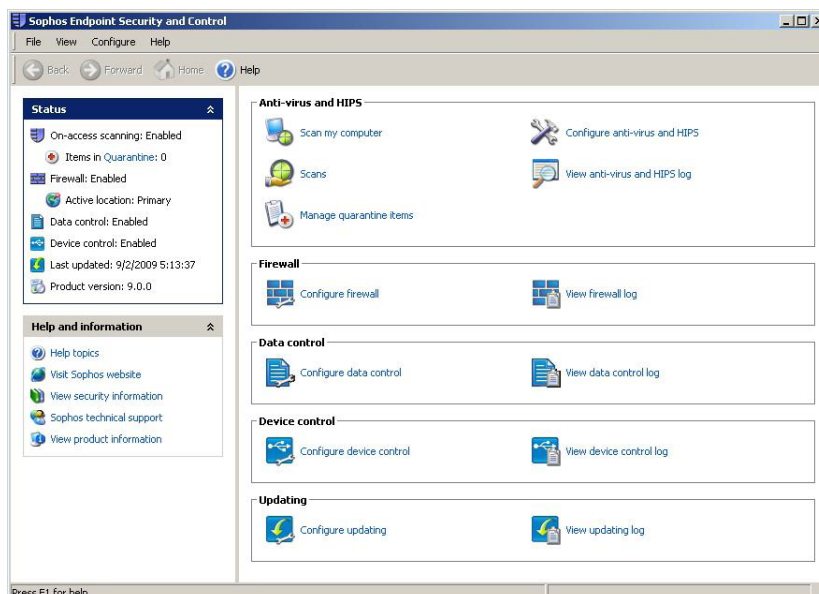


Sophos Endpoint Security and Control for Windows

Sophos Endpoint Security and Control for Windows, part of Endpoint Security and Data Protection, delivers award-winning protection across thousands of Windows desktops, laptops and servers. A single endpoint client detects viruses, spyware and adware, suspicious files, suspicious behavior and potentially unwanted applications (PUAs); monitors the transfer of sensitive and confidential data; and controls the use of removable storage devices and unauthorized VoIP, IM, P2P and gaming software—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, 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 suspicious 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™.
- Flexible control of removable storage devices enables the authorization of specific devices, enforcement of encrypted devices or even just read-only access. It also controls the use of wireless connections such as modems, including 3G versions.
- The fully integrated content monitoring feature for storage devices and applications—supported by a wide range of data definitions supplied and updated by SophosLabs™—monitors the transfer of sensitive data and minimizes the risk of accidental data loss.



Key benefits

- » Removes the need for point products with a single endpoint client
- » Automatically stops unknown malware, with Behavioral Genotype® Protection uniquely analyzing suspicious behavior before code executes
- » Prevents the accidental loss of confidential data through integrated content scanning
- » Identifies unknown malware, suspicious files; and behavior through built-in pre-execution and runtime intrusion prevention technologies
- » Controls the use of legitimate software applications like VoIP and IM
- » Manages the use of removable storage, optical media drives and wireless networking protocols
- » Can be centrally installed, set up and monitored across the network
- » Configurable role-based administration provides granular control of administrator privileges
- » 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-on-one assistance

Automated, simplified, central management from a single console

- The Security Dashboard shows real-time security status and critical events, and automatic email alerts are sent if 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 data, 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.
- Configurable role-based administration enables specific management tasks to be delegated to trusted users without handing over full administration capabilities.
- A single ActivePolicy incorporating both anti-virus and HIPS allows the rapid creation and application of security settings across multiple computers and groups simultaneously.
- Small, frequent protection updates are automatically downloaded and distributed across the network.
- 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 that can be scheduled to run at specific times and emailed directly to selected recipients.

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. 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's 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 the system was last accessed.
- Rapid threat analysis from SophosLabs and the fastest updates in the industry are downloaded as frequently as every 10 minutes.

Industry-leading expertise 24x7

- Our 24x7 customer support operation and SophosLabs our global network of threat analysis centers, provide a rapid response to emerging and evolving threats.

Languages available

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

Sophos Endpoint Security and Control for Windows delivers all the features covered. However, some of the functionality may be disabled depending on the Sophos license you purchase. For further information, please see www.sophos.com.

System requirements

Platforms supported

- » Windows 7
- » Windows Vista*
- » Windows Server 2003**
- » Windows Server 2008*
- » Windows XP*
- » Windows 2000 Server
- » Windows 95/98 and NT4***
- » VMware ESX 3.0
- » VMware Workstation 5.0
- » VMware Server 1.0

Disk space

- » Windows XP/2003/Vista/7: 120 MB
- » Windows 2000: 120 MB
- » Windows 95/98: 90 MB
- » Windows NT4: 90 MB

Recommended memory

- » Windows XP/2003/Vista/7: 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.