

Sophos Endpoint Security and Data Protection offers a single solution for anti-virus and anti-spyware protection, client firewall, management of removable storage devices, unauthorized software, NAC and encryption, giving you the best preventive endpoint and data protection. A single license means you can protect all users and computers across Windows, Mac, Linux, UNIX and other non-Windows platforms.

Comprehensive protection

Proactive blocking of new virus updates, simple automated management and small, frequent updates make it easy to protect against malware and data loss without slowing your users down. One scan stops viruses and detects adware, suspicious files and behaviour, unauthorized software and removable storage devices.

Full disk encryption protects your data ensuring lost or stolen computers do not result in a compliance or PR disaster. Data is further protected by controlling user access to USB drives, removable storage and wireless connections, as well as restricting access to P2P, IM and other applications.

Simplified management

Centralized deployment from a single management console reduces the amount of time and resource needed to implement new policies and functionality. Active Directory synchronization allows agents to be deployed and the right policies applied automatically, without affecting user productivity.

The at-a-glance dashboard and emailed outbreak alerts keep you up to date with the security status of all machines across your network and the central deployment of endpoint compliance ensures that all computers meet your security policies.

Our integrated third-party removal tool automatically removes your existing endpoint protection solution when you deploy the Sophos agent.







Trusted expertise

In business for over 20 years, trusted by tens of millions of users worldwide and recognised as a leader by industry analysts, Sophos provides the best protection against growing threats and exceptional data encryption that meets real-world enterprise requirements.

The license includes comprehensive support to ensure that you get the most out of your solution. SophosLabs™, our global network of threat analyses centres, supplies expertise and pre-packaged intelligence on all the latest threats, Sophos Technical Support is provided by our own in-house experts, and all major and minor product updates are delivered automatically. In addition, our Sophos Professional Services team is on hand to help you maximise the return on your investment.

Key benefits

- » Eliminates known and unknown threats with a single, centralized solution. Detects and removes viruses, spyware, rootkits, Trojans, adware and PUAs
- » Lets you instantly identify vulnerable computers to check compliance, update policies and clean up threats
- » Ensures compliance and prevents the loss of data by encrypting devices and information
- » Controls applications that can adversely impact network and user productivity, such as VoIP and IM
- » Allows assessment of the security status of managed and unmanaged computers. Alerts of issues such as a disabled patch agent or firewall, and can provide automatic resolution
- » Enforces protection against unknown users gaining access to your network
- » Lets you rapidly create and update security policies, and deploy them across multiple groups simultaneously
- » Receives and centrally deploys small, fast automatic updates every five minutes
- » Allows automatic deployment to new computers through Active Directory synchronization
- » Provides role-based administration privileges assigned with Helpdesk and read-only consoles
- » Enables a wide range of customized, graphical reports to be created on virus alerts, infections and status of protection
- » Includes 24x7x365 support for the duration of the license and one-to-one assistance

 <p>Central management</p>	 <p>Pre-execution control</p> <ul style="list-style-type: none"> » Anti-virus » Anti-spyware » Behaviour blocking » Application control 	 <p>Runtime control</p> <ul style="list-style-type: none"> » HIPS » Buffer overflow 	 <p>Communication control</p> <ul style="list-style-type: none"> » Client Firewall 	 <p>Network access control</p> <ul style="list-style-type: none"> » Compliance reporting » Patch and vulnerability assessment » Enforcement 	 <p>Data protection</p> <ul style="list-style-type: none"> » Full disk encryption » Encryption of data on removable storage devices
--	---	---	---	--	--

Faster, low-impact protection

One scan with our single anti-virus client blocks and cleans viruses, spyware and adware, suspicious behavior and files, removable storage devices and unauthorized applications.

- Sophos updates are small in size and are released as frequently as every five minutes – an advantage for companies wanting fast protection with low impact on network resources.
- Decision Caching™ technology improves on-access scanning performance by intercepting and scanning only the files that have changed since last accessed.
- SophosLabs signatures control applications that can adversely impact network and user productivity, such as VoIP and IM.

Effective zero-day protection

Sophos HIPS, technology pioneered by SophosLabs, provides detection that automatically guards against new and targeted threats and can detect over 85 percent of unknown threats.

The built-in intrusion-prevention technology detects malware, malicious and suspicious behavior and files, and delivers proactive protection without complex installation and configuration. Scanning is performed using Sophos's anti-virus engine, without the need to deploy any additional components.

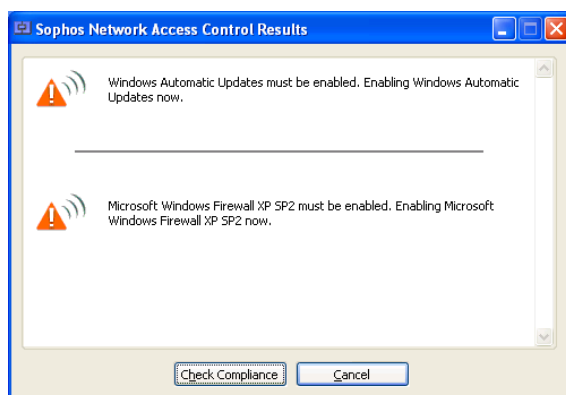
This innovative technology uniquely analyzes the behavior of code at two stages:

- Pre-execution – behavior of code is analyzed before it runs and is prevented from running if it is considered to be suspicious or malicious.
- Runtime – intercepts threats that cannot be detected before execution.

Preventive protection reduces risk of infection

By identifying managed and unmanaged computers with potential security flaws, like out-of-date anti-virus protection or a disabled firewall, you can reduce the risk of infection. You can choose to either block non-compliant computers or ensure that security is improved to meet a required standard before allowing access.

- Default policies check if anti-virus and client firewall protection is active and up to date on managed and unmanaged computers.
- Sophos NAC agent checks if Microsoft operating system service packs are installed, and that Microsoft/Windows Update is enabled.
- Enforcement options ensure that any unauthorized computers are not granted access to your network.



Software components

Enterprise Console

A single, automated console for Windows, Mac, UNIX and Linux that centrally deploys and manages anti-virus and client firewall protection, intrusion prevention, device and application control and endpoint assessment and control.

Sophos Anti-Virus

A single anti-virus client that detects viruses, spyware and adware, rootkits, suspicious files, suspicious behavior, removable storage devices and unauthorized VoIP, IM, P2P and gaming software across multiple platforms in just one scan.

Sophos NAC

A network access control solution that assesses managed, unmanaged and unauthorized computers to detect configuration issues, such as out-of-date anti-virus protection or a disabled firewall and optionally fixes them before allowing access.

Sophos Client Firewall

A centrally managed client firewall, designed for the enterprise environment, that blocks worms, stops hackers, and prevents intrusion from hackers.

Sophos Mobile Security

Anti-virus and anti-spyware protection for Windows Mobile smartphones and PDAs.

Sophos SafeGuard Disk Encryption

Full disk encryption with secure pre-boot authentication and a full set of password and machine recovery tools.

SafeGuard PrivateCrypto

Encryption of data on removable storage devices and secure information exchange with third parties.

Full data encryption provides comprehensive information security

Sophos SafeGuard Disk Encryption is an easy to implement solution providing full disk encryption that helps you to meet your compliance needs.

- Simple to use configuration wizard enables easy implementation and enforcement of your data security policy.
- Installation can be carried out on a standalone machine or unattended across your estate via your existing deployment tool.
- Requires no user intervention, eliminating any impact on their day-to-day productivity.

Simplifying deployment and administration

Sophos Enterprise Console simplifies management of Windows, Mac, Linux and UNIX protection, centralizing deployment, updating, reporting and security policy enforcement. It manages anti-virus and client firewall protection, and endpoint assessment and control, providing unrivalled visibility of the security status of your entire network.

- The console synchronizes with Active Directory to ensure your chosen security policy is automatically enforced as new computers join your network.
- Outbreak risk levels across the entire network are displayed on the security dashboard and automatic email alerts are sent when your chosen security thresholds are threatened.
- Protection is automatically updated as frequently as every five minutes – and because you control the download rate, you can preserve bandwidth.
- Endpoint computers can be completely disinfected in a single, simple operation from the console.
- ActivePolicies in the console allows you to create a policy once and then apply it across multiple groups, on Windows, Mac, Linux and UNIX computers.
- Policies cover updating schedules, anti-virus and HIPS, client firewall, application control and NAC.
- Integrated graphical reporting delivers instant and scheduled email reports of threat alerts and infections while the security dashboard gives you an at-a-glance report of outbreak risk.

The screenshot shows the Sophos Enterprise Console interface. The top navigation bar includes 'Home', 'View', 'Actions', 'Groups', 'Tools', and 'Help'. Below this is a 'Dashboard' section with several summary cards: 'Computers with alerts' (54), 'Policies' (66), 'Virus/spyware' (94%), 'Suspicious behaviours' (236), 'Enforcement' (94%), 'Blocked by firewall' (89), 'Out-of-date computers' (69), 'Adware/PUA' (30), and 'Controlled applications' (115). The main area displays a table of computer status for 'All computers'.

Computer	Alerts and events	On-access	Firewall enabled	NAC	Up-to-date	Antivirus and HIPS policy	Firewall policy	Updating policy	Applicat
Computer_100	Suspicious behavior detect	Active	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_115	Suspicious file detected	Active	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_140	Virus/spyware detected	Active	Yes	Installed	Not since 11/10/2...	Same as policy	Same as policy	Same as policy	Same as policy
Computer_151	Virus/spyware detected	Active	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_152	Virus/spyware detected	Active	Yes	Installed	Not since 11/10/2...	Same as policy	Same as policy	Same as policy	Same as policy
Computer_161	Active	Yes	Installed	Yes	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_163	Active	Yes	Installed	Yes	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_173	Active	Yes	Installed	Yes	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_178	Suspicious behavior detect	Active	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_213	Virus/PUA detected	Active	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_220	Adware/PUA detected	Active	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_222	Active	Yes	Installed	Yes	Not since 11/10/2...	Same as policy	Same as policy	Same as policy	Same as policy
Computer_224	Virus/spyware detected	Inactive	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_227	Active	Yes	Installed	Yes	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_228	Controlled application detect	Active	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_240	Active	Yes	Installed	Yes	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_280	Suspicious behavior detect	Active	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_283	Active	Yes	Installed	Yes	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_294	Adware/PUA detected	Inactive	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_299	Active	Yes	Installed	Yes	Not since 11/10/2...	Same as policy	Same as policy	Same as policy	Same as policy
Computer_311	Suspicious behavior detect	Active	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_312	Firewall alert	Active	Yes	Installed	Not since 11/10/2...	Same as policy	Same as policy	Same as policy	Same as policy
Computer_316	Suspicious behavior detect	Active	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_340	Active	Yes	Installed	Yes	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_342	Suspicious behavior detect	Active	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_344	Suspicious behavior detect	Active	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy
Computer_350	Controlled application detect	Active	Yes	Installed	Yes	Same as policy	Same as policy	Same as policy	Same as policy

Technology bytes

ActivePolicies™

Lets you create a new security policy once and then deploy it across multiple groups simultaneously

Application Control

Allows you to selectively authorize or block legitimate applications that impact network bandwidth, system availability, and user productivity

Behavioral Genotype Protection

Delivers the benefits of a Host Intrusion Prevention System (HIPS), guarding against unknown threats by analyzing behavior before code executes

Centralized cleanup

Lets you deal with malware and PUAs remotely from a central location, saving time and cost

Decision Caching™

Provides performance-enhanced on-access scans by ensuring that only those files that have changed are scanned

Device Control

Helps you control the use of removable storage, optical media drives and wireless networking protocols

Genotype® technology

Provides proactive protection from new variants of virus and spam families, even before specific, signature-based protection becomes available

Smart Views

Lets you instantly focus on vulnerable computers – including remote computers – to check compliance, update policies and clean up threats

Sophos AutoUpdate™

Offers failsafe updating and can throttle bandwidth when updating over low-speed network connections

Rootkit detection and clean-up

Integrated rootkit detection that finds and removes any rootkit hidden on desktop computers

Stealth mode

Lets Sophos Client Firewall prevent computers responding and falling victim to hacker attacks

Trusted support from the experts

All Sophos products are supported by experienced Sophos teams who are on hand to ensure you benefit from the best protection, and maximum return on investment.

- Highly-skilled analysts in SophosLabs, our global network of threat analysis centers, provide proactive rapid protection against known and unknown threats.
- Through technology, global visibility of emerging threats, and integrated threat expertise, SophosLabs provides the 24x7 research and fast global response your organization needs to protect it from increasingly complex threats.
- Our round-the-clock technical customer support operation is included as standard in every license and includes access to our in-house customer support team.
- Our support engineers provide one-to-one support by email or telephone, or you can take advantage of our web-based support knowledgebase.
- Sophos Professional Services team can demonstrate how to get the most out of Sophos products through optimizing your implementation.

Simple pricing and licensing

- A subscription-based license entitles you to protection, management and product updates, as well as technical support.
- Web Security and Control, Email Security and Data Protection, and NAC Advanced services can all be included in one license.

Languages supported

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

Note: Not all functionality/language support is available on all platforms.

Evaluate now for free

See Sophos Endpoint Security and Data Protection in action by registering for a free 30-day evaluation at www.sophos.com/eval

How to buy

Find your local Sophos office or Sophos Partner at www.sophos.com/contact. We also offer competitive pricing for charities, government agencies and the education sector.

Platforms supported

SOPHOS ANTI-VIRUS

- » **Windows**
95/98/NT/2000/XP Home and Pro/
Server 2003/Vista/Server 2008/Mobile
- » **VMWare**
ESX/Workstation/Server
- » **Non-Windows platforms**
Mac OS X/Linux/UNIX/NetApp Storage
Systems/EMC/OpenVMS/NetWare

SOPHOS NAC

- » **Windows**
2000/XP/Vista

SOPHOS CLIENT FIREWALL

- » **Windows**
2000 Pro/XP Home and Pro/Vista

ENTERPRISE CONSOLE

Management server

- » **Windows**
2000 Server/Server 2003 and R2/
Server 2008
- » **VMWare**
ESX/Workstation/Server

Remote console

- » **Windows**
2000 Pro and Server/Server 2003 and
R2/XP Pro
- » **VMWare**
ESX/Workstation/Server

Platforms managed

- » **Windows**
- » **Mac OS X**
- » **Linux**
- » **UNIX**

SAFEGUARD DISK ENCRYPTION

- » **Windows**
2000/XP

For full details, visit www.sophos.com