

## Sophos Endpoint Security and Data Protection

Sophos Endpoint Security and Data Protection offers a single integrated solution for both anti-malware and data protection. A single agent delivers anti-virus and anti-spyware protection, client firewall, data loss prevention (DLP) content monitoring, management of removable storage devices and detects and blocks unauthorized software. Combined with integrated network access control (NAC) and encryption to ensure policy compliance and secure your data, it gives you the best preventive endpoint and data protection, saving you time, money and resources. A single license means you can protect all users and computers across Windows, Mac, Linux, UNIX and other non-Windows platforms.

### Fast and preventive protection








A unified single client blocks malware, adware, suspicious files and behavior, removable storage devices and unauthorized software such as IM, VoIP, P2P and games, and provides content-aware DLP monitoring for the transfer of sensitive information. Its fast scanning engine, built-in intrusion prevention and live in-the-cloud protection technologies combine to detect new and zero-day threats without the need for a malware signature update. Integrated network access control functionality ensures all computers connecting to the network meet your security standards.

### Comprehensive data protection

The combination of a number of different technologies ensures that your data is protected against accidental loss. Content scanning integrated into the single agent ensures that all sensitive data being transferred by users to removable storage devices and internet-enabled applications such as email or instant messaging is detected and can be audited. Granular control of removable storage devices enables you to allow the use of specific devices, enforce the use of encrypted devices or simply allow read-only access. And full disk encryption secures your data on computers, preventing information from getting into the wrong hands if devices are lost.

### Simplified and automated management

Our management console reduces administrative burden by automating the deployment of protection, and simplifying policy management and reporting. The dashboard provides instant visibility of the protection status and events across Windows, Mac, Linux and UNIX platforms, and enables the centralized cleanup of malware; and fixes non-compliant computers. Role-based administration enables you to share specific tasks such as clean up with the help desk team and scheduled reporting means that specific reports can be emailed automatically to the people who need them.

 <p><b>Management</b></p> <ul style="list-style-type: none"> <li>» One console for multiple platforms</li> <li>» Unrivaled visibility</li> <li>» Role-based administration</li> </ul>	 <p><b>Anti-virus</b></p> <ul style="list-style-type: none"> <li>» Small, frequent updates</li> <li>» Proactive intrusion prevention</li> <li>» Live in-the-cloud checks</li> <li>» Buffer overflow</li> </ul>	 <p><b>Device Control</b></p> <ul style="list-style-type: none"> <li>» Detect and block unauthorized devices</li> <li>» Easy authorization of allowed devices</li> <li>» Prevent network bridging</li> </ul>	 <p><b>Application Control</b></p> <ul style="list-style-type: none"> <li>» Identify and stop use of unauthorized software</li> <li>» Easy to manage</li> <li>» Lists maintained by SophosLabs</li> </ul>	 <p><b>Network Access Control</b></p> <ul style="list-style-type: none"> <li>» Compliance reporting</li> <li>» Patch and vulnerability assessment</li> <li>» Enforcement</li> </ul>	 <p><b>Data Loss Prevention</b></p> <ul style="list-style-type: none"> <li>» Integrated into endpoint agent</li> <li>» Control transfer of sensitive data</li> <li>» Pre-packaged data definitions</li> </ul>	 <p><b>Encryption</b></p> <ul style="list-style-type: none"> <li>» Full disk encryption</li> <li>» Encryption of data on removable storage devices</li> </ul>
--	---	---	--	--	--	---

## Key benefits

- » Eliminates known and unknown threats with a single, centralized solution
- » Detects and removes viruses, spyware, rootkits, Trojans, adware and potentially unwanted applications (PUAs)
- » Live checks against SophosLabs reputation database protect against new and unseen threats
- » Scans for sensitive information being transferred off the network without requiring a separate agent
- » Lets you instantly identify vulnerable computers to check compliance, update policies and clean up threats
- » 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
- » 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
- » Centrally deploys small and frequent updates that don't impact network bandwidth or system performance
- » Allows automatic deployment to new computers through Active Directory synchronization
- » Reduces administrator workload with its ability to share specific tasks with other teams through configurable role-based administration
- » Enables a wide range of customized, graphical reports to be created, scheduled to run and automatically emailed
- » Includes 24x7x365 support for the duration of the license and one-on-one assistance

## Faster, low-impact protection

One scan with our single anti-virus client detects viruses, spyware and adware, suspicious behavior and files, removable storage devices and unauthorized applications. The client will also detect when users try to transfer sensitive data to removable storage devices and internet-enabled applications such as email and instant messaging.

- Sophos updates are small in size and are released frequently—an advantage for companies wanting fast protection with low impact on network resources—and protection is enhanced Sophos Live Protection that reduces the gap between updates even further.
- Decision Caching™ technology improves on-access scanning performance by intercepting and scanning only the files that have changed since the system was accessed last.
- SophosLabs™ signatures control applications that can adversely impact network and user productivity, such as VoIP and IM.

## Effective zero-day protection

Sophos combines proactive protection technologies to automatically guard against new and targeted threats eliminating the reliance on updates and without complex installation and configuration as SophosLabs do the fine tuning.

- The endpoint agent combines both pre-execution and runtime detection to create profiles of file characteristics, ensuring the accurate identification of malware and minimizing the chance of false positives. As soon as a file matches any existing malware profile the process is stopped and the threat cleaned up.
- Sophos Live Anti-Virus provides fast and effective detection of zero-day threats by instantly checking suspicious files against an extensive in-the-cloud database of known good and bad data.
- Sophos Live URL Filtering protects your roaming users from infection from websites with automatic in-the-cloud URL checks against the SophosLabs database of millions of compromised websites and blocking access to sites that are known to be hosting malware.

## Protecting against accidental loss of data

Sophos Endpoint Security and Data Protection delivers a number of components that combine to protect your data against loss and help you to meet your compliance needs:

- Content-aware DLP scanning—integrated into the engine—monitors the transfer of sensitive data to removable storage devices and internet-enabled applications. It uses an extensive library of data definitions supplied by SophosLabs, reducing the burden of manually creating and maintaining lists yourself.
- Flexible, granular control of removable storage devices allows the authorization of specific devices, enforcement of encrypted devices or even just read-only access, as well as control over network interfaces like 3G modems.
- Prevents the installation and use of unwanted applications such as P2P and IM clients that can act as means for sensitive data transfer. A comprehensive list of applications supplied and maintained by SophosLabs™ removes the need for administrators to add new applications or manually update detection of new versions.
- Full disk encryption secures data on computers by encrypting the entire hard drive without impacting your users. Installation can be carried out on a standalone machine or unattended across your organization via your existing deployment tool. Forgotten passwords can be easily recovered either through local self-help or by using a secure challenge response process. Users can also easily and secure share data with third parties using encryption features integrated into Windows Explorer and email clients.

## 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; data, 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 and suspicious behavior; scans for the transfer of sensitive data; controls the use of removable storage devices and unauthorized VoIP, IM, P2P and gaming software

### 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 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

## Preventive protection reduces risk of infection

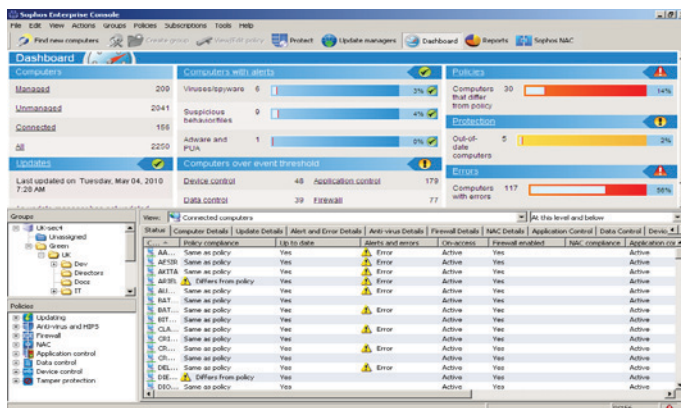
By identifying managed and unmanaged computers with potential security flaws, such as out-of-date anti-virus protection or a disabled firewall, you can reduce the risk of infection. You can choose to either block non-compliant computers or ensure that security is improved to meet a required standard 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 unauthorized computers are not granted access to your network.

## Simplifying deployment and administration

Sophos Enterprise Console™ simplifies management of Windows, Mac, Linux and UNIX protection, by centralizing deployment, updating, reporting and security policy enforcement. It manages endpoint and client firewall protection as well as 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 and data 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 frequently—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, data control, device control, application control and NAC.
- Specific roles can be configured to enable responsibility for specific actions like cleanup or management areas of the network, such as remote offices, to be delegated through role-based administration.
- Out-of-the-box compliance reports are provided and a reporting wizard enables administrators to create and customize reports that can be scheduled and emailed to selected recipients with threat alerts and infections.



## 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 PUA's remotely from a central location, saving time and money

### Data Loss Prevention

Allows you to monitor the transfer of sensitive data such as PII to storage devices and applications using an extensive library of global sensitive data definitions supplied and updated by SophosLabs

### 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

### Live Protection

In-the-cloud technology providing protection against the very latest threats without the need for an update and blocking access to malicious websites

### 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 cleanup

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

### Stealth mode

Lets Sophos Client Firewall prevent computers from 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 that you benefit from the best protection and the 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 around-the-clock technical customer support operation is included as standard in every license and provides 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.
- The Sophos Professional Services team can demonstrate how to get the most out of Sophos products by optimizing your implementation.

## Simple pricing and licensing

- A single license covers all users and computers across Windows, Mac, Linux, UNIX and other non-Windows platforms.
- Subscription-based licensing entitles you to protection, management and product updates as well as technical support.
- Sophos Web Security and Control, Sophos Email Security and Data Protection, and Sophos NAC Advanced services can all be included in one license.

## Languages supported

English, French, German, Italian, Japanese, Spanish, Simplified Chinese 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](http://www.sophos.com/eval).

## How to buy

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

<sup>1</sup> Including AMD64 and Itanium 64-bit versions .

<sup>2</sup>Available August 2010

## Platforms Supported

### SOPHOS ANTI-VIRUS

- » **Windows**  
Windows 7/Vista/XP Home and Pro/2000 and 2000 Pro/95/98/NT/Windows XPe/Windows Netbooks/Windows Embedded Standard/WePOS/Mobile/Server 2003/2003 R2/Server 2008 incl. Core /2008 R2 including Core
- » **VMware**  
vSphere 4/ESX 3.0, 3.5/Workstation 6.5/Server 1.0
- » **Hyper-V**  
Microsoft Hyper-V 2008
- » **Citrix**  
XenServer
- » **Non-Windows platforms**  
Mac OS X/Linux/UNIX/NetApp Storage Systems/EMC/OpenVMS/NetWare

### SOPHOS NAC

- » **Windows**  
Windows 7/Vista/XP/2000/Server 2003/2003 R2/Server 2008/Server 2008 R2

### SOPHOS CLIENT FIREWALL

- » **Windows**  
Windows 7/Vista/XP Pro or Home/2000 Pro

### ENTERPRISE CONSOLE

#### Management server

- » **Windows**  
Windows 7 (incl. XP mode)  
Server 2008/2008 R2/Server 2003/2003 R2
- » **VMware**  
vSphere 4/ESX 3.0, 3.5/Workstation 6.5/Server 1.0
- » **Hyper-V**  
Microsoft Hyper-V 2008
- » **Citrix**  
XenServer

#### Remote console

- » **Windows**  
Windows 7 (incl. XP mode)  
Server 2008/2008 R2/Server 2003/2003 R2/Vista/XP Pro
- » **VMware**  
vSphere 4/ESX 3.0, 3.5/Workstation 6.5/Server 1.0
- » **Hyper-V**  
Microsoft Hyper-V 2008
- » **Citrix**  
XenServer

#### Platforms managed

- » **Windows**  
Windows 7/Vista/XP/2000/98/95/NT4/Server 2008\* incl. Core/ Server 2003
- » **Mac OS X**  
Versions 10.4/10.5 /10.6
- » **Linux**<sup>1</sup>
- » **UNIX**<sup>1</sup>

### SAFEGUARD DISK ENCRYPTION

- » **Windows**  
Windows 7/Vista/XP
- » **Mac**<sup>2</sup>  
OS X 10.5.x, 10.6.x (EFI 64-bit only)

### SAFEGUARD PRIVATECRYPTO

- » **Windows**  
Windows 7/Vista/XP/2000/Windows 7/Vista/XP/2000