

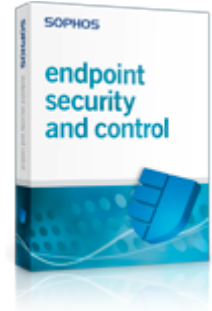
## The features of Sophos Endpoint Security and Control

### Endpoint Security and Control Assess, control and protect all endpoints with one product

Cross-platform security and control for your desktops, laptops, file servers and mobile devices. Sophos delivers complete protection against viruses, spyware and adware, controls VoIP, IM, P2P, games and removable storage devices, and enables you to assess and control all endpoints.

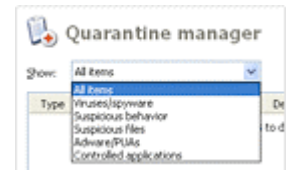
#### Scan once, not five times

One scan with our single anti-virus client detects viruses, spyware and adware, suspicious behavior and files, unauthorized VoIP, IM, P2P and gaming software and removable storage devices. We protect Windows, Mac, Linux, UNIX, NetApp Storage Systems and Windows mobile devices.



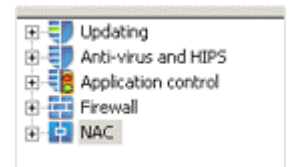
#### Automate management with one console

Our central management console manages anti-virus, client firewall, and endpoint assessment and control. Automatic email alerts and the security dashboard warn about outbreak risk for your network. Our console simplifies management of Windows, Mac, Linux and UNIX protection, centralizing deployment, updating, reporting and security policy enforcement.



#### Protect computers automatically

Synchronized with Active Directory, your security policies are automatically enforced as new computers join your network. It takes just minutes to set up our ActivePolicies™ in Enterprise Console. Create a policy once and apply it across multiple groups, platforms, and all versions of Sophos Anti-Virus.



#### Detect zero-day threats before they execute

Sophos HIPS, technology pioneered by SophosLabs™ automatically guards against new and targeted threats by analyzing behavior before code executes. Built-in intrusion-prevention technologies combine to detect malware, malicious behavior, and suspicious behavior and files, and deliver proactive protection without complex installation and configuration.

#### Assess and control all managed and unmanaged computers

Our software identifies managed, unmanaged and guest computers with problems, such as out-of-date anti-virus protection or a disabled firewall. Problems can be easily fixed before allowing computers to join the network, or you can choose to block non-compliant computers.

