

NETWORK ACCESS CONTROL

Business challenge

Business productivity and revenue are critically dependent on IT allowing employees, partners, consultants, and customers easy access to the corporate network while at the same time preventing access by unmanaged computers that can introduce viruses, spyware, Trojans, and worms, or that attempt to use unauthorised applications. The challenge is to find an easy-to-implement network access control solution that avoids the significant investment and upheaval involved in installing new network infrastructure.

The Sophos solution

Complete protection

Sophos NAC provides comprehensive and easy-to-deploy enterprise-ready network access control. Its broad enforcement framework protects enterprise networks from the threats posed by non-compliant, compromised, or misconfigured computers. Sophos NAC controls access based on policies set and controlled by the administrator – providing peace of mind that the network is secure, whether connections are made via the LAN or remotely, wired or wireless, or from managed or guest computers.

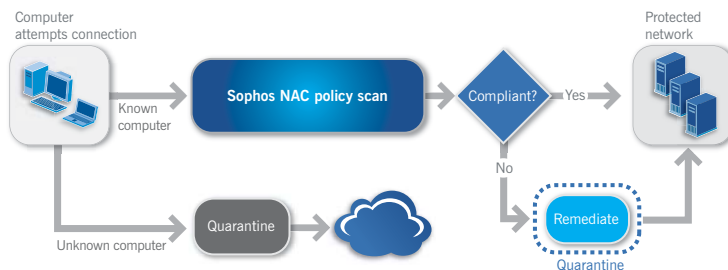
Central endpoint policy control

An intuitive web interface supports all major security applications, custom application definition, and point-and-click contextual operating system (OS) patch definition. Administrators can define and manage unique policies for detecting OS patches, security applications and signature updates – and ensure that no unwanted applications are run.

These policies are the basis for assessing whether computers are permitted or denied access to the network. Unauthorised or non-compliant computers can be isolated, quarantined for remediation, automatically remediated, or sent alerts.

Easy deployment

As a software overlay, Sophos NAC is vendor-neutral and fits within the existing network infrastructure (switches, VPN concentrators, DHCP servers, enterprise user stores). Sophos NAC works straight out of the box and does not require significant changes to existing hardware or to user groups already configured. It uses a range of predefined rules to detect all major security applications, which do not need to be replaced. A simple, central policy mode control enables enforcement steps to be phased in – from Report Only, through Remediate, to Enforce – avoiding an all-or-nothing approach, and providing optimum control and ease of policy deployment during each stage of implementation.



Sophos NAC Policy Scan: protecting the entire network

Key benefits

- » Enables easy identification and isolation of non-compliant endpoint computers.
- » Assesses computer compliance proactively prior to network access and periodically during the network session.
- » Defines security policies centrally.
- » Enhances ROI of existing security applications and network infrastructure.
- » Provides assessment options for managed and unmanaged computers with an installed agent or a web agent.
- » Provides flexible deployment for phased enforcement (Report Only; Remediate; Enforce).
- » Simplifies the process for exempting devices (servers, routers, printers, etc) from network-based enforcement.
- » Reports the state of a computer's compliance over time.
- » Responds rapidly to new, unforeseen threats using custom application creation and enforcement.
- » Provides systematic enforcement of security compliance policies.
- » Includes 24x7x365 support for the duration of the licence and Sophos can be contacted for one-to-one assistance at any time.

NETWORK ACCESS CONTROL

Technical details

Enforcement

- Agent enforcement protects the network by providing self-quarantine.
- DHCP enforcement protects the network from unauthorised computers connecting to the LAN by using an enterprise's existing DHCP infrastructure.
- IEEE 802.1X enforcement stops unauthorised computers connecting to the LAN.
- RADIUS enforcement protects the network from non-compliant laptops by providing enforcement prior to opening IPSec, SSL-VPN, or wireless connections.
- Cisco NAC-based enforcement uses Cisco NAC-enabled infrastructure.

Centralised policy definition and management

- Easy-to-use web interface offers extensive policy-building capabilities, flexible enforcement control, and extensive reporting and alerting.
- Customisable landing page provides immediate, easy-to-view NAC compliance statistics.

Extensive security application definitions

- Comprehensive range of predefined applications, including over 350 security applications and over 600 OS patches, covers all major security applications.
- Point-and-click inclusion in policy saves administrators hours of configuration time.
- Detection includes installation, last engine scan date/time, signature file date/time, running detection for processes, real-time protection status, and version/value.

Comprehensive alerting, reporting, and auditing

- Powerful audit and reporting capabilities enable administrators to monitor and manage endpoint compliance, and any changes made to policy.
- Access to real-time and historical endpoint data enable sophisticated analysis, reporting, and trending information.

Full range of assessment options

- Installed agent provides comprehensive compliance assessment and enforcement of managed endpoints, both prior to and during a network session.
- Web agent provides comprehensive compliance assessment prior to network access for remote or LAN-based unmanaged endpoints, or on managed endpoints when an agent is not practical.

To find out more about Sophos NAC, visit www.sophos.com

ds/070308

System requirements

Server

- » Operating system:
Windows Server 2003
- » Database:
Microsoft® SQL 2000

Agent

- » Windows 98 SE
- » Windows 2000
- » Windows XP
- » Windows Server 2003
- » Windows Vista

Compatible network equipment

- » Alcatel™
- » Aruba Networks™
- » Aventail®
- » Cisco®
- » Checkpoint®
- » Enterasys Networks
- » Extreme Networks™
- » Foundry® Networks
- » Hewlett-Packard
- » Infoblox®
- » Juniper Networks™
- » Lucent Technologies®
- » MetaInfo®
- » Nortel®
- » Novell
- » RSA Security®
- » Sun Microsystems
- » 3Com Corporation™

Sophos is a world leader in IT security and control. We offer complete protection and control to business, education and government organisations – defending against known and unknown malware, spyware, intrusions, unwanted applications, spam, and policy abuse, and providing comprehensive network access control (NAC). Our reliably engineered, easy-to-operate products protect over 100 million users in more than 150 countries. With over 20 years' experience and a global network of threat analysis centres, the company responds rapidly to emerging threats and achieves the highest levels of customer satisfaction in the industry. Sophos is a global company with headquarters in Boston, MA., and Oxford, UK.