

Network access control (NAC)

FORTUNE 500 COMPANIES

Large organizations need to provide an increasingly mobile and diverse workforce with easy access to the corporate network without compromising security. Sophos NAC provides comprehensive network access control that integrates with existing security and network infrastructure, enabling major firms – including Fortune 500 companies – to enforce security policies, maximize their return on investment (ROI), and demonstrate that they can meet regulatory compliance.



Key facts

Manufacturing company
Unregulated

No of users
5,000 mobile employees

Existing security
Anti-virus, personal firewall, patch management (Microsoft SMS)

Solution
Sophos NAC with RADIUS enforcement for mobile users

Financial services company
Regulated

No of users
40,000 employees, agents, contractors and consultants (VPN- and LAN-based)

Existing security
Anti-virus, patch management

Solution
Sophos NAC with RADIUS and 802.1X enforcement for remote and LAN-based users

Business challenge

IT and security managers in large companies face the problem of providing an increasingly dynamic workforce with easy access to critical applications, while limiting their network's exposure to spyware, viruses, Trojans, worms and other forms of malware. Contractors, teleworkers, and office-based employees are known users but, in common with guest users, their computers will not necessarily be compliant with corporate security policy. To prevent the introduction of potential security threats to the network, IT administrators must be able to assess, achieve, and report on the security compliance of all computers on the network, without reducing user productivity or increasing support costs.

Companies with mobile, diverse workforces can enforce their security policies by basing network access authorization on an assessment of the user's role, the access method used, the security status of the user's computer, and known responses to vulnerabilities and threats. To minimize disruption and maximize ROI, this must be accomplished with the existing infrastructure, organization, applications, and operational procedures.

Sophos NAC has helped many Fortune 500 companies in different sectors to implement network access control progressively, enforcing security policy and demonstrating compliance with regulatory requirements.

Energy company
Highly regulated

No of users
15,000 employees, contractors, consultants and advisors

Existing security
Multiple desktop security applications

Solution
Sophos NAC with DHCP enforcement for LAN users

Global manufacturing company

This international company relies heavily on its people, equipment, and network to stay competitive, and needs to provide more than 5,000 mobile users with secure remote access to corporate resources. It needed to demonstrate and report security compliance for a broad range of information disclosure and risk management reasons, but its existing single-vendor security application suite could not provide this at the end-user level. A more aggressive approach was required to deal with operating system vulnerabilities and unpredictable, non-compliant user behavior such as using unwanted peer-to-peer applications. The company needed an automated tool that assesses computers for compliance, both when they connect and at configurable periods, and that could report on operating system patch level, and security application status.

The firm chose Sophos NAC with RADIUS (a common authentication protocol) enforcement for its mobile users, completing initial installation in less than a week. During a phased deployment all remote PCs were assessed for compliance, both before connection and at defined intervals in their network sessions. By immediately collecting endpoint security compliance data, it was possible to analyze trends and produce summaries, enabling the company to track, improve, and report on compliance – limiting its exposure to vulnerabilities through the definition and enforcement of comprehensive security policies.

Leading financial services company

As a diversified insurance and financial services company, this firm is particularly committed to risk prevention, confidentiality, and security. It proactively invests in risk management education, process improvement, and technical resources to protect the computers used by more than 40,000 employees, field agents, contractors, and consultants in both VPN and LAN environments. The firm operates in a regulated industry and must demonstrate that it has made reasonable efforts to safeguard customer information and company assets. However, this task is complicated by a user base that provides its own PCs with a variety of operating systems, configurations, and security applications, resulting in high support costs. The company had no visibility of their state of compliance with policies governing anti-virus updates or operating system patches, and relied on its largely non-technical users to comply voluntarily with security requests – a totally unacceptable situation. A solution was needed that could provide comprehensive assessment and enforcement of security policy in a very large infrastructure containing multiple hardware platforms and desktop security software elements.

By implementing a Sophos NAC solution, the company was rapidly able to assess and report on compliance with a wide range of leading security applications for both its remote and LAN user populations, using its existing RADIUS and 802.1X infrastructure for enforcement. Policy compliance is measured and enforced at the time of user authentication and periodically during the network session, providing both the data necessary to mitigate risk exposure and the control and reporting required to comply with regulatory requirements.

“The extended enterprise network is vulnerable to malicious code that rides on the coat-tails of trusted employees, contractors, and business partners. This threat demands that enterprises move quickly to invest in endpoint security policy enforcement solutions.”

Jim Slaby, Senior Analyst, Yankee Group

US energy company

With more than 15,000 employees and hundreds of contractors, consultants, and advisors serving millions of customers, this highly regulated company takes network security very seriously. If the enterprise network or any of the computers that connect to it were compromised, the possible loss of service, downtime, and outages would be unacceptable. The potential exposure was highlighted by non-compliant user behavior, such as disabling security applications, and the introduction of viruses, worms, and other malware to the network by contractors and consultants. The problem was compounded by the sheer size of the network and the need to integrate a security enforcement strategy with the existing DHCP infrastructure and a planned upgrade to 802.1X-enabled switches. A solution was required that would assess and enforce security on the company's own varied desktop platforms, which employed a range of different security applications, and quarantine unauthorized computers prior to network access.

The IT department installed Sophos NAC with DHCP-based compliance and enforcement capabilities, which assesses the security status of computers when they connect to the network and at predefined intervals thereafter. Non-compliant users are notified and quarantined, protecting the network and providing a complete record of actions taken, enabling the firm to comply with local, regional, and governmental regulations.

To find out how Sophos products can help protect your organization, visit www.sophos.com/products