

## **NAC:** Bridging the network security gap

Enterprises must take a robust policy-driven approach to enforcing security compliance in order to protect against network vulnerabilities and meet regulatory requirements. This paper examines technology and initiatives designed to capitalize on existing investments and prevent any gaps in security.

# NAC: Bridging the network security gap

## Overview

IT managers are well aware of the threats to their networks, and have spent heavily on solutions to protect the corporate environment. Despite high expenditure on security software and hardware products, in today's diversified environment many organizations are not truly in control of their users. In the drive for more flexible working, networks are opened to third parties, such as contractors, whose security applications are not subject to control by the organization. As far as direct employees are concerned, administration rights usually granted to enable them to use their computers productively often compromises security by allowing critical security services to be disabled.

*“By 2008, the annual amount spent on security software support services in the United States alone is expected to top \$800 million*

*Anne Clifford, Secure Enterprise<sup>1</sup>*

However, the majority of organizations have no enforcement mechanism in place either to drive compliance or to report on results. This gap in corporate policy exposes the enterprise to a range of threats – not just from malware, hackers, and malicious users, but also to loss of intellectual property, and non-compliance with regulatory requirements.

The complexity of managing modern security applications, combined with the lack of control of endpoint computers attaching to the network, has persuaded many security vendors to incorporate compliance and enforcement capabilities as extensions to existing products. Indeed, some vendors have even shifted from promoting single endpoint security products to creating and endorsing entire endpoint security programs.

For IT managers to maximize their return on investment, they need vendor-neutral solutions that work with their existing infrastructures, enabling them to take control of threats from malware and unknown or non-compliant users. The critical factor for successful implementation is an ability to define firstly, unique policies that can be applied to groups of users, and secondly, the membership of those groups of users appropriate to the organization's operations.

## Technology and initiatives

Security experts agree that there is absolutely no way to eliminate every threat. What an organization can realistically do, however, is to assess and eliminate vulnerabilities, and have systems in place that consistently manage network security by looking for potential threats and adequately protecting enterprise resources.

The key, which is easier said than done, is to manage vulnerabilities. The complexity of network infrastructures, coupled with the vast choice of security solutions, provide little direction on what course of action an organization should take. The hardware and software security products available, for the most part, do a great job providing security for a network's up-to-date, managed computers – however, those products can only prevent the problems they find. Too often, unexpected threats are introduced to the network by some unmanaged means, such as a system that hasn't been patched, a computer not managed by the enterprise, or even worse, a managed computer that simply doesn't have the product correctly installed or running.

*“By year-end 2007, 80 percent of enterprises will have implemented network access control policies and procedures”*

*John Pescatore, Gartner Inc<sup>2</sup>*

Therefore, access to the protected, managed, and already compliant network must be controlled by determining a connecting computer's level of security before allowing it to connect – and preventing access by non-compliant computers – and continuing to assess compliance once connected.

#### Network access control

Network access control (NAC) technology is a viable answer to solving the issues of compliance of all computers attempting to connect to the network, whether LAN-based or remote, managed or unmanaged. True NAC reports on the security status of a computer to be assessed against a predefined policy before it connects and periodically during a network session, as well as enforcing policies that manage access at various levels, and provides for the remediation of non-compliant computers.

#### Programs and alliances

The growth and scope of security threats has stimulated the formation of fully-fledged programs and security alliances in the industry. Major players are using these initiatives to rally support from emerging vendors with varying approaches to policy-based compliance, enforcement assessment, and reporting capabilities. The three most widely recognized initiatives (see panels) are Microsoft's Network Access Protection (NAP), Cisco's Network Admission Control (NAC), and the Trusted Computing Group's interoperable standards and solutions, such as Trusted Network Connect.

#### Microsoft NAP

Microsoft's Network Access Protection (NAP) is a policy-enforcement platform that is integrated into both Windows Vista and the planned release of the Longhorn Server operating system. The NAP architecture consists of both client- and server-side components that perform specific functions such as policy configuration and remediation, and the NAP security policy incorporates enforcement and quarantine settings. The platform enforces system requirements defined in policies that must be met by computers connecting to a network. Non-compliant computers are limited to specific areas of the corporate network until they can be updated, and where they must meet policy compliance before gaining full network access.

Microsoft encourages partnership with third-party vendors to incorporate NAP into their solutions. For environments using just Microsoft operating systems or products that can incorporate NAP, this may be a good basic solution, which can be extended and enhanced by NAP business partners.

Network access control solutions should do the following:

- Assess the security state of a computer attempting to connect, and provide feedback on its level of compliance
- Compare a computer's security state to the relevant policy that defines the requirements for network access
- Enable a minimum level of network access for automated remediation or self-remediation of a computer to bring it to a state of compliance
- Monitor the security state of computers that are already connected to the network
- Enforce network access according to the requirements of the environment
- Provide effective reporting.

Scanning determines the state of a computer's configuration, such as its application levels and security status. The information is sent to a policy manager that determines what level of network access is allowed, which is then implemented by the network. After the initial scan, and potential blocking, the network access control process directs non-compliant computers to remediation resources, monitors changes in the security state and network activity of connected computers, and quarantines any infected computers to minimize the threat to the network. Overall, NAC is capable of maintaining the network's original security state through proper configuration management.

NAC solutions can be standalone or they can be incorporated into the internal network infrastructure. The solution appropriate for an organization is primarily dependent on its current network environment, such as how homogeneous the network currently is, what the main network access methods are, and the budget available.

### Cisco NAC

Cisco's Network Admission Control (NAC) Framework is a network-based approach to compliance enforcement that incorporates security policy into an organization's network infrastructure. Security policies are stored on policy servers, and enforced at routers and switches. A client mounted on computers connecting to the network communicate its security state to the policy server. Non-compliant computers are identified, and either quarantined or permitted restricted access on the network.

NAC is also a strategic program in which Cisco shares technology features that program participants can incorporate into their products. The strategic program is opened to all independent PC and server software vendors.<sup>3</sup> For large businesses whose networks consist exclusively of Cisco hardware and software, this may be the right basic solution to the problem of network admission.

Enterprises should focus expenditure on the solutions and services that solve their biggest problems, choosing the solutions that protect against vulnerabilities and provide a full security process instead of providing merely products. A solution that works with the existing network infrastructure and user management systems – one that is truly vendor-neutral – will be the least disruptive to implement and produce the best return on investment.

## Flexibility and control

User groups and the associated policies are closely interwoven and greatly enhance the degree of flexibility and control available to administrators. By determining which users are assessed for compliance against which policies, administrators can manage their policy deployment in the optimum and most convenient way.

*“Regulatory requirements such as Sarbanes-Oxley and HIPAA (Health Insurance Portability and Accountability Act) require controls as part of financial and patient health data protection.”*

Groups can be defined according to department, function, individual hire dates, or any combination of these. Ideally, a NAC solution should allow multiple policies to be created for various user groups, and to be shared between groups as necessary. The ability to change policy-to-group relationships at any time, and add new users to existing groups provides ultimate flexibility when rolling out security requirements for a constantly evolving workforce. In particular, if administrators want to mandate specific security applications for new users, they should be able to deploy new policies for those users independently of the rest of the user population. This degree of control is essential in the case of mergers and acquisitions, where organizations face the daunting task of imposing their corporate security policies on large numbers of new users. Here, it is vital that policies and groups can be modified rapidly in order to complete migration successfully.

## Phasing implementation

Administrators can implement a solution in a way that supports the progressive enforcement of security policy, as shown below.

- Create a policy that reports on the state of applications installed on endpoint computers

## Trusted Computing Group (TCG)

TCG exists to create open industry specifications for network security and to promote standards that are platform-, device-, and vendor-neutral.<sup>4</sup> TCG's Trusted Network Connect (TNC) specification establishes a security framework that prevents unmanaged devices from connecting to a network and infecting it. TNC is a formal extension of the TCG's Infrastructure Working Group. The TNC framework provides fundamental aspects of trusted computing, such as interoperable solutions from multiple vendors, the use of existing industry standards, including EAP, 802.1X, and RADIUS, and suitability for heterogeneous networks.

TCG comprises a core group of companies that are involved in the process of creating specifications, with additional companies as members of the association. Its goal is to ensure that no single platform or vendor dominates the development of an open solution, and that multiple countries participate to ensure the integrity of a global solution.<sup>5</sup>

- Update the policy to issue warnings for required applications that are not installed or running correctly, and provide links for users to update them
- Update the policy again to provide enforcement and require remediation for non-compliant computers before they gain access to the network.

This flexible, phased approach is a much more workable alternative to an all-or-nothing deployment of security compliance, minimizing frustration for both users and hard-pressed IT departments.

## Reporting

Effective reporting is essential not only in aiding the troubleshooting and analysis phases of implementing and managing security applications, but also in meeting regulatory compliance. Administrators need ready access to data in order to:

- determine applications in use by end users
- assess applications against security policies
- track trends in compliance enforcement
- update policies, or add new user groups
- distribute policy to the entire user population
- track changes to configuration and enable rollback.

Armed with this information, administrators are better able to change their enforcement strategies in relation to actual activity, depending on the threat level or simply if tougher enforcement rules are needed. In highly regulated businesses, the role of reporting is critical. Assessing and enforcing policies shows auditors that enterprise controls are in place and reasonable protection can be proven.

## Conclusion

Organizations should not wait to begin addressing the issues of security compliance. Having a policy-driven security program in place to prevent unwanted network access and to protect the integrity of the network is essential, and can be achieved progressively, with minimum upset to users, without compromising existing network infrastructure. ◆

---

## The Sophos solution

**Sophos network access control** blocks unauthorized users, controls guest access, and ensures that legitimate users comply with the organization's security policy – so administrators know who and what is connecting to the network.

Sophos's vendor-neutral solutions, and membership of the Microsoft NAP, Cisco NAC, and Trusted Computing Group programs ensures that customers' investments in its products are future-proof.

**To find out more about Sophos products and how to evaluate them, please visit [www.sophos.com](http://www.sophos.com)**

## Sources

- 1 Anne Clifford, Stats: Facts and Figures from the World of Secure Enterprise. Secure Enterprise, 9 December 2004
- 2 J Pescatore et al, Protect your Resources With a Network Access Control Process. Gartner Inc., 2004
- 3 Network Admission Control. Cisco Systems, Inc.
- 4 What Is the Trusted Computing Group? Trusted Computing Group  
<https://www.trustedcomputinggroup.org/home>
- 5 Trusted Computing Group Frequently Asked Questions. Trusted Computing Group  
<https://www.trustedcomputinggroup.org/faq/>

## See also:

NAC: Managing unauthorized computers. Sophos white paper, April 2007  
[www.sophos.com/security/whitepapers/sophos-nac-unauthorized-computers-wpus.pdf](http://www.sophos.com/security/whitepapers/sophos-nac-unauthorized-computers-wpus.pdf)

## About Sophos

Sophos is a world leader in IT security and control. We offer complete protection and control to business, education and government organizations – 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 centers, 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.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France  
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2007. Sophos Plc.

*All registered trademarks and copyrights are understood and recognized by Sophos.  
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.*

**SOPHOS**  
WWW.SOPHOS.COM