CMP
United Business Media

Network Computing

JULY 6, 2006 I WWW.NWC.COM

For IT By IT

NAC VENDORS SQUARE OFF

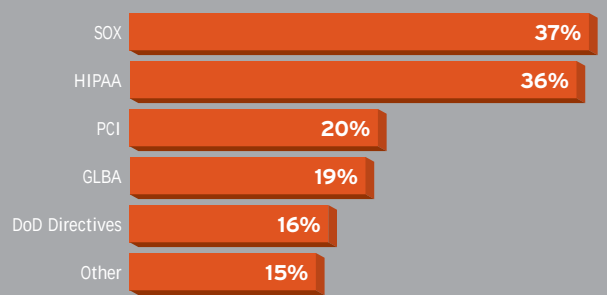
BY JOEL CONOVER

Cisco, Microsoft and the Trusted Computing Group vie for dominance in the network access-control market. Our reader survey analysis reveals whether brand recognition will beat out an open standard

"NAC" describes network access systems that deliver a broad range of features focused on coupling user identity, host posture assessment, threat remediation and policy-based access controls for enterprise networks. There's no single definition of the acronym, and customer expectations for what NAC systems should accomplish are evolving as well. In November 2005, NETWORK COMPUTING delivered a thorough analysis of emerging NAC offerings and the competitive architectures behind them. Six months later, the market is more hyperactive than ever, with dozens of vendors competing for your attention and IT dollars. NETWORK COMPUTING and industry analysts from Current Analysis put their collective heads together to provide a single, clear

READER POLL

To which of the following government or industry regulations is your organization specifically accountable?



Source: NETWORK COMPUTING Reader Poll and Current Analysis, 303 respondents

definition of NAC and identify the requirements customers expect, based on an extensive poll.

35 Questions, 5 Great Expectations

We started our research project by polling NWC readers. Three hundred three respondents reported that they were directly involved in evaluating or deploying a NAC solution. We asked them 35 detailed questions about NAC and its associated technologies.

We took a look at customer expectations for NAC, cross-referencing with marketing collateral from a broad selection of NAC competitors. We clearly defined five technology functions that are accepted and expected as part of a NAC product:

1) Preconnect host posture assessment
2) Host quarantine and remediation
3) Network access control based on user identity
4) Network resource control based on identity and policy
5) Ongoing threat analysis and containment

Most individuals responding to our survey were focused on one of two main issues: identifying and policing user access to the network, and eliminating threats brought onto the network by infected hosts. No single vendor has an offering that succinctly addresses all five NAC areas, but likewise most customers are attempting to solve only a portion of the access control problem. Broadly speaking, vendors have focused product development energies into either preconnect host posture assessment or identity- and access-control enforcement mechanisms.

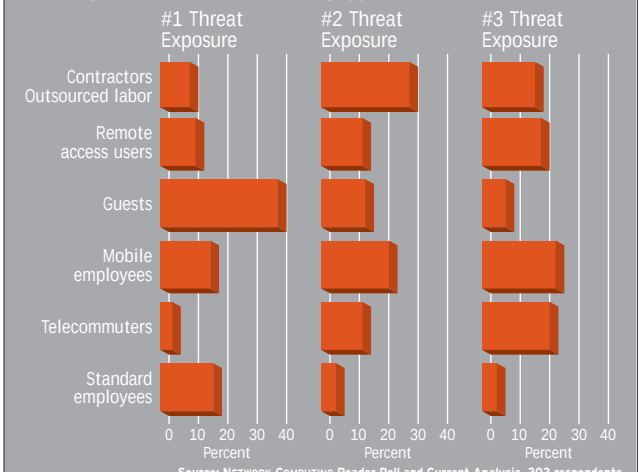
Why NAC, Why Now?

Our survey is a snapshot of early NAC adopters. The results indicate that customers evaluating NAC products are only at the tip of the purchasing and deployment iceberg. Thirty-six percent of organizations surveyed are impacted by HIPAA regulations as part of the health-care supply chain, which includes medical facilities, insurance providers and medical research organizations. Health-care organizations have an acute need to couple identity to information access. We spoke with vendors who confirmed health care has been a strong market for early NAC solutions, followed closely by education.

Regulatory control is a strong driver in the security market, and the impact of regulatory guidelines is acutely visible in the NAC market. According to our research, many CEOs and CTOs are mandating the deployment of NAC, and IT is left with the tasks of product evaluation and implementation. On the survey, 96 percent of our respondents indicated they are governed by at least one government or industry regulation. NAC is a prime candidate for compliance dollar spending, and NAC solutions that couple

READER POLL

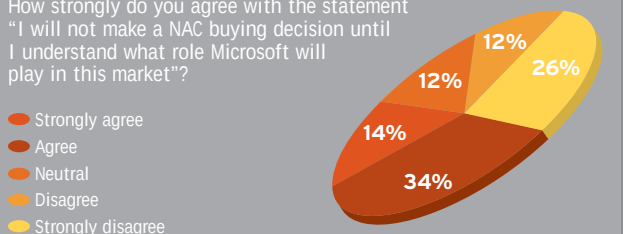
How large a threat are the following types of users?



Source: Network Computing Reader Poll and Current Analysis, 303 respondents

READER POLL

How strongly do you agree with the statement "I will not make a NAC buying decision until I understand what role Microsoft will play in this market"?



Source: Network Computing Reader Poll and Current Analysis, 303 respondents

Executive Summary

NAC

Call it network admission control, network access control or even network node validation. No matter the name you give this thorny rose, NAC can transform the way you secure and administer access to your networking resources. NAC vendors are struggling to innovate and differentiate themselves in a tempestuous marketplace.

Enterprise IT buyers are boxed in by three frameworks, each competing to solve the same problem: Cisco NAC, Microsoft NAP and Trusted Network Connect (TNC) from the Trusted Computing Group present unique solutions to the access-control challenge.

We surveyed 303 NWC readers directly involved in deploying or evaluating network access control. We asked 35 questions to gauge perceptions and expectations about NAC and its complementary technologies. The overwhelming response: IT pros expect identity and policy to play key roles in their next-generation network architectures, and they're willing to pay a premium to achieve that vision. In this article, we analyze the results of our survey and present our most current research and analysis on the changing face of the NAC market.

with identity management can greatly improve accountability.

Many current government and industry regulations have little specific language with respect to network-layer security and access control. The regulations also lack specific penalties for noncompliance. But that is changing, and NAC vendors are using the threat as a wedge when positioning NAC solutions, particularly in verticals where compliance is top of mind. Compliance aside, knowing exactly who is accessing the data on your network is just good business sense, and NAC solutions provide that visibility.

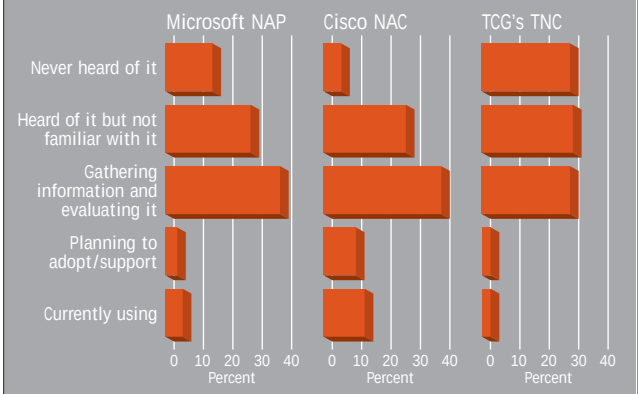
A changing work environment is also mandating the deployment of NAC. Survey respondents were asked to rank how great a threat users posed to LAN security. Forty percent considered guest users as the strongest threat, while 30 percent ranked contract labor as the second-highest threat. Mobile employees came in third. The fact that many organizations allow guests today is a radical departure from the LAN security policies of the past.

Cisco's NAC, Microsoft's NAP

There are three competing architectures for NAC: Sixty-five percent of respondents were familiar with, or already using, Cisco NAC (CNAC). Clearly leading

READER POLL

How familiar are you with the following NAC frameworks?



Source: NETWORK COMPUTING Reader Poll and Current Analysis, 303 respondents

the race for brand recognition, Cisco Systems also ranks highest in terms of customer expectations for interoperability and framework preference, with one important exception: When asked about the importance of adhering to a NAC framework or standard, customers responded strongly for Cisco NAC, but responded even more strongly for adherence to any industry standard (see the chart on page 4).

Cisco's dominant position in the IT infrastructure

A CLEAN BILL OF HEALTH

Details on the current state of Microsoft Network Access Protection (NAP) have been scarce. Microsoft has not launched a public awareness campaign, and vendors are under NDA prohibiting them from publicly discussing the details of the architecture. Perhaps Microsoft felt stung by the backlash against its early architecture? Despite the lack of outbound communication, progress has been made. Vendors have shared tidbits of information about the current state of Microsoft NAP, and the future of NAP looks much brighter than it did in version 1.0.

At the core of Microsoft NAP is the concept of a Health Certificate. Consider it a bill of health for the device trying to access the network. Microsoft has an agent that constructs the Health Certificate based on the state of the machine. Other agents such as antivirus, anti-spyware, personal firewall and so on must report in to the Microsoft Agent. Software vendors are responsible for writing integration components for the Microsoft agent.

Here's what's new. Under NAP, the client now attempts to connect to an 802.1X switch, and once an 802.1X authentication has taken place, the health agent sends its Health Certificate to a device designated as a System Health Server.

The System Health Server makes a decision about the state of the machine and passes that information back to the Microsoft Network Policy Server (NPS). The NPS ties back to the 802.1X-enabled switch, providing an appropriate VLAN for access, or for quarantine and remediation.

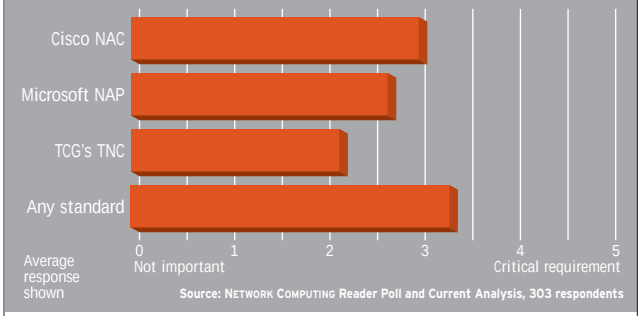
If you are keeping score here, Cisco Systems has a similar master-agent called the Cisco Trust Agent. It also has a "Network Policy Server" called ACS (Access Control System). Neither Cisco nor Microsoft offer any mechanisms for providing per-user access policy, though Cisco's forthcoming NAC appliance will offer ACL (Access Control List) capabilities. Both depend on VLANs defined by the IT department to provide granular access control to specific network resources.

The TNC architecture is, by necessity, somewhat more complex because each element can theoretically be delivered by a different vendor. It includes definitions of devices that provide enforcement, access request, access authority (identity), posture assessment and posture verification. There is also a formidable amount of glue that connects all these elements. This glue comes in the form of standards-based protocols including RADIUS, EAPoL (Extensible Authentication Protocol over LAN), and RADIUS RFC 2865 Filter-ID extensions.

It is up to the TNC members to use these standard protocols, but with the TNC architecture, any vendor can theoretically create one or more components of an interoperable NAC infrastructure.

READER POLL

How important is it that your NAC solution adhere to the following NAC frameworks?



Source: NETWORK COMPUTING Reader Poll and Current Analysis, 303 respondents

market virtually ensures customers will have a strong preference for its program. But, while Cisco enjoys a strong early preference for its CNAC program, Microsoft and its Network Access Protection (NAP) architecture are clouding the picture and creating concern with enterprise customers. This despite the fact that Microsoft and Cisco have both stated they are working together to create an interoperable solution.

Microsoft NAP complements portions of CNAC and overlaps with others. NAP was first announced as a set of extensions for Windows Server 2003 and Microsoft Windows XP in a white paper, "Network Access Protection Platform Architecture for Microsoft

Microsoft has fumbled by failing to assert its vision for NAP, engendering uncertainty in the market.

Windows Server 2003," in June 2004. This paper introduced a complex, multilayer software system that provides advanced system health assessment, quarantine and remediation using PEAP (Protected Extensible Authentication Protocol) and PPP (Point to Point Protocol) for remote access sessions, and DHCP-based controls for LAN sessions.

Microsoft's first stab at NAP was riddled with holes. Only LAN implementations using DHCP were secure. Microsoft's own literature warned that a malicious user assigning a local IP address could circumvent the entire NAP architecture. Microsoft's architecture called for multiple Windows servers to provide policy control, quarantine and remediation, and Microsoft quarantine agent software on the host desktop. Microsoft IAS server was also required if a remote access environment existed. NAP offered no provisions to leverage the assets, resources and security capabilities of the LAN infrastructure. Furthermore, Microsoft's implementation was Windows-specific. No support for other OSs or non-PC platforms was considered.

Microsoft also announced it would work closely with Cisco to deliver an integrated NAC/NAP solution, and some implementation details were outlined, but specifics about how NAP and NAC will integrate are still nebulous. Cisco is also no longer the only game in town. Many vendors have announced participation in Microsoft's NAP program, though several confided that the network integration portion of NAP leverages 802.1X and looks and smells exactly like Cisco NAC. Microsoft NAP remains a Windows-specific solution.

Microsoft plays a critical role in the NAC pipeline, providing a universal interface for auditing and assessing system posture. However, Microsoft has fumbled by failing to authoritatively assert its vision for NAP. By remaining practically silent for two years, it has engendered fear and uncertainty in the market. Forty-eight percent of our survey respondents indicated they would not buy a NAC solution until they understood Microsoft's role in this market, though only 36 percent of respondents indicated they planned on implementing NAP once it was mature.

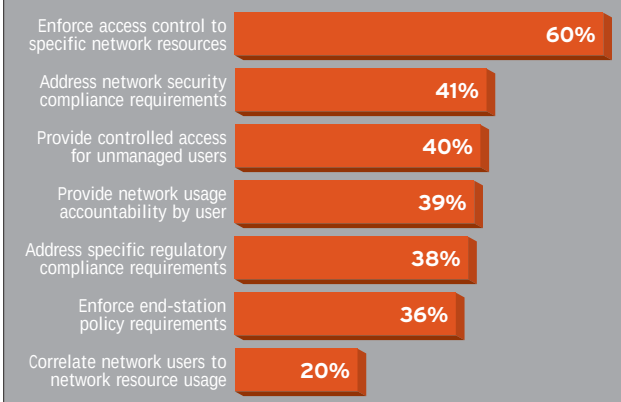
The Contenders

In the left corner of the NAC boxing ring is Cisco, the reigning network infrastructure champion. And in the right corner, a mob of angry competitors frustrated that Cisco can arbitrarily define a proprietary architecture for network access control, and then selectively choose which vendors are allowed to participate. The group on the right has banded together to form Trusted Network Connect (TNC), a subgroup within the Trusted Computing Group (TCG) tasked with defining an open industry standard for NAC. In the center of the ring is Microsoft, which has agreed to work with both Cisco and the TNC and has its own partner program with 66 members signed up. Microsoft is also a member of both Cisco's program and the Trusted Computing Group.

Is Cisco NAC a standard? With about 65 vendors

READER POLL

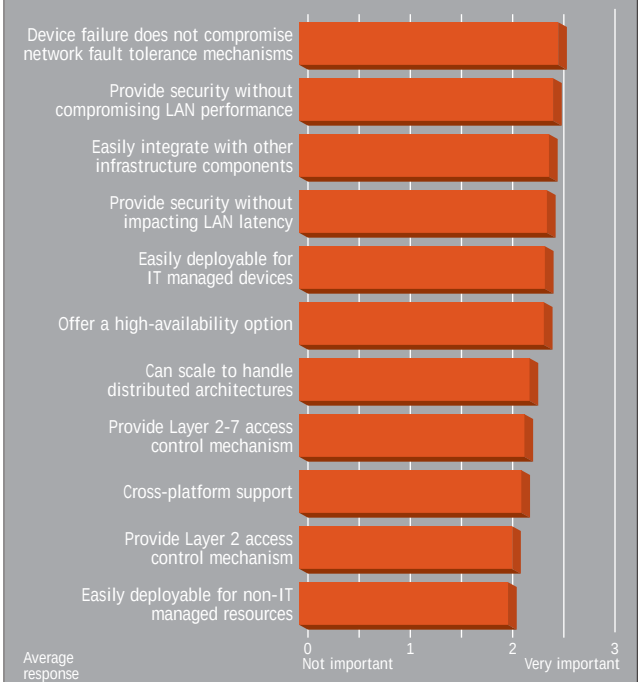
What are the top three issues driving your organization's interest or adoption of NAC solutions?



Source: NETWORK COMPUTING Reader Poll and Current Analysis, 303 respondents

READER POLL

How important is each of the following technical issues in your evaluation or selection of a NAC solution?



Source: NETWORK COMPUTING Reader Poll and Current Analysis, 303 respondents

participating, it might sound like the industry has joined hands with Cisco in one big happy circle. But the only standard in Cisco NAC is the double standard. Take ConSentry Networks' Secure LAN Controller, which we reviewed in "Catching Rogue Nodes." At that time, ConSentry was a member of Cisco's NAC program. But in May 2006, ConSentry announced its Secure LAN Switch, encroaching on Cisco's turf. A few days later ConSentry was no longer listed as a Cisco NAC partner. Open standards separate protocols from politics and protect the IT buyer from the games vendors play. Cisco's approach gives customers assurance, but locks them into a program where Cisco has ultimate control over their network architecture.

The TNC is struggling to gain visibility and acceptance in both the enterprise and vendor communities. Enterprises responding to our survey were least familiar with the TNC. Only 30 percent of respondents were familiar with the TNC, versus nearly 40 percent for both Cisco and Microsoft. Those surveyed showed less preference for products that adhere to the TNC standard. They also indicated they have lower expectations for interoperability of TNC solutions versus Cisco NAC and Microsoft NAP. But the same respondents indicated they strongly prefer "a standard, any standard" for their NAC implementation, more than they want Cisco NAC, Microsoft NAP or a TNC-based framework.

The Trusted Network Connect Sub Group has defined and released an open architecture and set of standards for endpoint integrity assessment. The TCG has more than 100 members (members join TCG, and can choose to participate in the TNC-SG), and a dozen TCG members have announced products that comply with the TNC architecture.

We spoke with vendors who also expressed frustration with the TNC, and that it hasn't created

NAC: Vendor Analysis

A wide range of vendors across multiple markets are addressing different aspects of NAC. All want a piece of your access control budget. Here's our snapshot of strengths and weaknesses across five key functional areas.

	Access Control	Identity-Based Resource Control	Posture Assessment	Quarantine/ Remediation	Threat Assessment
Cisco Systems	●	◑	●*	●	◑
ConSentry Networks	●	●	◑	◑	◑
Elemental	◑	◑	●	◑	◑
Enterasys Networks	●	◑	●*	◑	◑
Extreme Networks	○	○	●*	◑	◑
ForeScout	●	◑	◑	◑	◑
Hewlett-Packard	●	◑	◑	◑	◑
InfoExpress	●	◑	◑	◑	◑
Juniper Networks	●	◑	●*	◑	◑
Lockdown Networks	●	◑	●	◑	◑
McAfee	◑	○	●	◑	◑
Microsoft	◑	◑	●*	●*	○
Mirage Networks	●	○	◑	◑	◑
Nevis Networks	●	●	○	○	◑
StillSecure	◑	◑	●	●	○
Symantec	◑	○	●	◑	◑
Vernier Networks	◑	◑	◑	◑	◑

●High, ◑Medium, ○Low *Depends on integration with third-party solutions

enough market awareness of its architecture. Vendors also expressed concern that even if the TNC completes a standard, there won't be an organization to ensure interoperability. There is also growing frustration with the slow pace of development for the protocols and methods within the standard. At Interop 2006, TNC took some major steps forward, rolling out many of the critical mechanisms to move from proof-of-concept to a potentially interoperable multivendor solution. Several vendors, including Fujitsu, Hewlett-Packard, IBM, Juniper Networks, Meetinghouse Data Communications, Nortel Networks, Symantec and Wave Systems, demonstrated interoperability at the show.

In short, while TNC is lagging, the market is still very young and the TNC shouldn't be counted out just yet. The TNC has defined the ingredients of a NAC solution, and has even specified a recipe that outlines how to combine those ingredients together. But until this cake has been in the oven longer, it is going to be difficult to determine whether the TNC recipe is a hit or a disaster.

Defining a Strategy for NAC

Respondents to our survey indicated they would be willing to adopt a broad range of technologies to solve specific problems. The top three issues driving the adoption of NAC are the enforcement of access control policies; the ability to address security compliance requirements; and the ability to provide controlled access of unmanaged users, including partners and contractors.

Posture assessment coupled with identity management form the foundation of an effective enterprise NAC implementation. But our survey base was also acutely aware of the impact NAC might have on network performance and fault tolerance, rating these two as their top NAC concerns. Ease of use and ease of deployment were also high priorities. An effective NAC solution cannot introduce additional points of failure or choke points in the network infrastructure.

Identity was also a key requirement for the majority of our respondents. The ability to deny network access based on user identity was one of the top requirements for a NAC solution. Likewise, user identity was the No. 1 condition that network administrators wished to consider when writing a user policy.

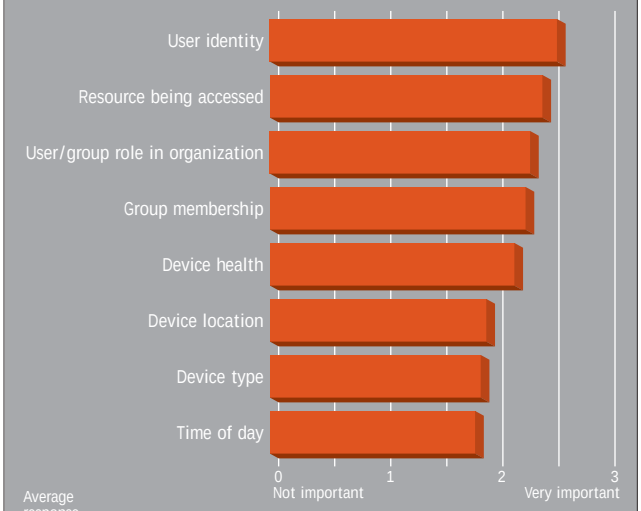
There are a broad range of solutions in the market that address the NAC problem. We spoke to a variety of vendors peddling NAC solutions, and found that they excel in one of two key areas. Those focused on assessing the state of the PC typically rely upon the underlying network architecture to police the decisions made by the policy enforcement system. At the other end of the spectrum are granular, hardware-based enforcement mechanisms which provide access and resource control based on both identity and policy.

Many companies sit in the middle; leveraging partnerships to fill in the weak spots in their product portfolio. Acquisitions are inevitable as this market matures.

Sixty-two percent of our respondents indicated they trusted network infrastructure and security vendors to deliver the most effective NAC implementations. We tend to agree. Policy evaluation is best handled at the host level, but enforcement and ongoing network behavior assessment is a job best left to the LAN infrastructure. Choosing a NAC vendor is largely dependent on the primary issue you want address, since vendors now tend to be either good at posture assessment, quarantine, remediation and ongoing threat assessment, or identity-based policy enforcement—but not both. If you're like most respondents, you want it all—in which case you may want to wait until best of breed solutions emerge. NWC

READER POLL

How important is each of the following in writing network-admission policies for a NAC solution?



Source: NETWORK COMPUTING Reader Poll and Current Analysis, 303 respondents

READER POLL

Which type of vendor do you trust to deliver a NAC implementation most effectively?

Source: NETWORK COMPUTING Reader Poll and Current Analysis, 303 respondents

JOEL CONOVER a former senior technology editor of NETWORK COMPUTING, is principal analyst for enterprise infrastructure at competitive intelligence firm Current Analysis. Write to him at *jec@currentanalysis.com*.