

## NAC: Slow Growth, For Now

Our third annual survey on network access control shows no dominant standard

**N**OT SURPRISINGLY, THE glow that surrounded network access control in its formative years has mostly dissipated. Early adopters—usually those who had to implement NAC to meet internal or external requirements for control and reporting—have deployed the technology and taken their knocks. Many of them shared their stories via our third annual *InformationWeek* NAC survey.

In a nutshell, we found that adoption took these cutting-edge companies longer than expected, and what they're getting out of NAC is slightly different from what they had planned. Moreover, with upward of 20 companies still calling themselves NAC providers, the market is ripe for consolidation. This year already we've seen three vendors exit the space, but even as they go, a few startups are entering.

What they'll find is a skeptical consumer base: Two years ago, 50% of companies said they were deploying NAC. Now just 22% make that claim. Those hardy souls still evaluating NAC face a spotty track record; a long implementation cycle; and, depending on their requirements for control at the network edge, an eye-popping price tag. Add to that the continued evolution of just what this technology does, and you've got a

recipe for disillusionment.

Ultimately, the shift to a critical mass of NAC adoption may happen slowly, as enterprises gain access to next-gen edge-switch features like 802.1X authentication. These niceties will come as we upgrade our networks; however, even though upgrades will facilitate deploying NAC, NAC won't drive many network upgrades.

For organizations that can sit tight, delay may not be a bad thing. Relying on edge switches to serve

as enforcers leaves NAC vendors to concentrate on policy engines, management interfaces, and reporting systems that meet regulatory compliance needs. And while you've lingered, the love/hate struggle that exists among Cisco, Microsoft, and the Trusted Computing Group—home to more infrastructure vendors—will have worked itself out a bit.

Maybe.

### STANDARDS SHAKEUP

There are four standards in the NAC market:

» Cisco's Network Admission Control, which includes its NAC framework and NAC appliance;

» Microsoft's Network Access Protection (NAP), which relies on Windows Server 2008, Windows Vista, and Windows XP Service Pack 3;

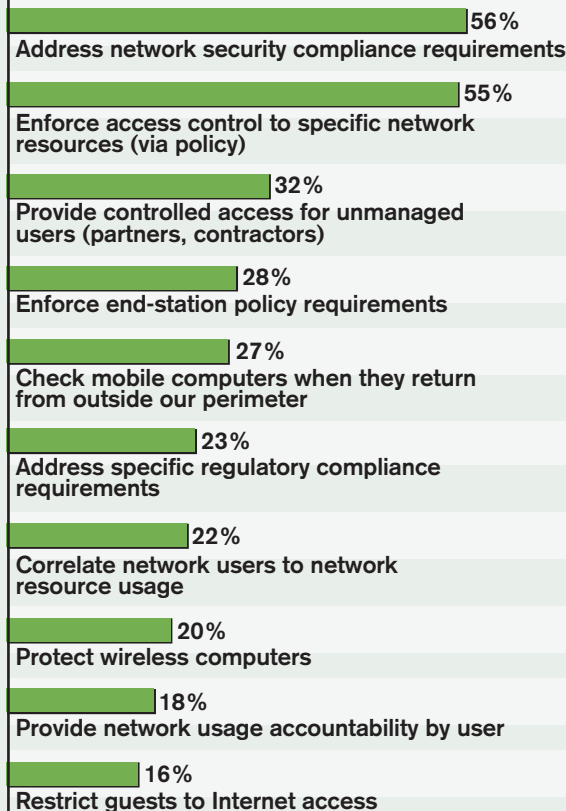
» The Trusted Computing Group's Trusted Network Connect (TCG/TNC), which is promoted through the TCG and defines a set of APIs and protocols for NAC; and

» The IETF Network Endpoint Assessment (NEA) working group, which is really just a way to bring Cisco to the NAC standards discussion, since Cisco doesn't recognize TCG as a standards body and won't participate in TCG's proceedings. Got that?

For the third year, companies are still mostly in a research phase, with the majority of respondents evaluating the various frameworks. While 15% are either using or plan to use Cisco's

### Why NAC Matters

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



Data: *InformationWeek* Analytics Network Access Control Study of 471 business technology professionals; 361 of those currently deploying, planning to deploy, or evaluating NAC

NAC framework, 8% are using or plan to use NAP. Shares held by both Cisco and Microsoft are down slightly from 2007, while the TNC/TCG is holding steady with 5% planning or using that framework. The NEA retains its position as "protocolus obscurus"—48% of respondents aren't even aware it exists.

Both Cisco and Microsoft have active and well-supported partner programs, with third-party add-ons like antivirus, patch management, and host-based firewalls that integrate with the giants' frameworks, not to mention the

### DIG DEEPER

**WANT TO KNOW MORE?** Our full *InformationWeek Analytics 2008 NAC Survey* results, including vendor analysis, are available for free for a limited time at:

[nac.informationweek.com](http://nac.informationweek.com)

See all our Analytics at [informationweekanalytics.com](http://informationweekanalytics.com)

preference for Cisco and 23% for Microsoft.

Only 8% of respondents think standardization is unimportant.

Of course, Windows Server 2008 just shipped in January, so NAP hasn't been available long enough to be widely deployed. The importance of NAP may increase over time, particularly among Microsoft shops.

Another twist: Vendor claims

critical requirement, while only 26% say third-party testing is the way to go.

### PURSES CLOSED

This year's results show a shift from 2007, when respondents who were willing to upgrade their network infrastructures slightly outnumbered those willing to add in-band appliances. This may be an indicator that recent infrastructure upgrades have been made, and most see no reason to do it again.

Still, even though respondents don't want to upgrade their infrastructures, they do recognize that they may not have a choice: Nearly half, 48%, indicate that between 10% and 50% of their infrastructures will need to be updated.

Notably, fully 79% of respondents agree or strongly agree that their NAC systems should support 802.1X. While the spec has been ratified for a few years and new switches commonly have no problem with it, there's still a lot of older gear out there that doesn't support 802.1X or other new functionality, like Radius extensions for setting switch-port configurations. The reality is that upgrades, at least firmware and possibly hardware, will be required in many cases.

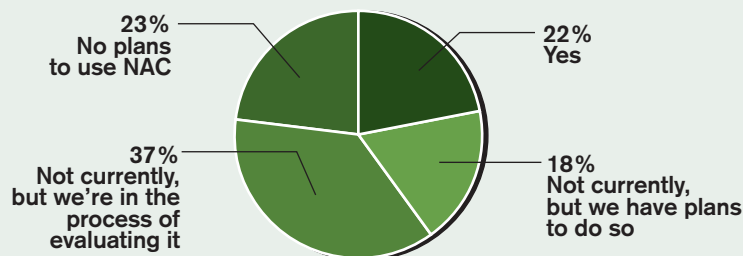
Respondents also are overwhelmingly concerned with the impact of NAC on network performance and reliability. Providing security without compromising the LAN ranked as the most important element of NAC (72%), with high availability in the NAC product (71%), not impacting latency (66%), not compromising network fault tolerance (65%), and easy integration with the infrastructure (65%) following behind.

Bottom line: Any technology, security related or not, that negatively affects network performance is a nonstarter.

—MIKE FRATTO

(mfratto@techweb.com)

## Is Your Organization Deploying NAC?



Data: *InformationWeek Analytics Network Access Control Study* of 471 business technology professionals

marketing muscle to get the word out about their products. We're surprised that neither framework is dominant with respondents.

While Cisco has the largest market share (well over 50%) in the access switch market, and Microsoft is king of the desktop, we've been expecting demand for integration and interoperation, and thus conformance with their respective frameworks to rise. Yet respondents don't seem to care which framework wins, though they clearly want one to take over: 38% say it's either very important or critical for an industry standard to come to the fore, while 29% state a

that a product "integrates" with a framework can mean vastly different things. Without clear testing procedures that demonstrate a level of integration among products, a partnership program is just empty marketing. All too often, integration is so limited, fragile, or complex that it is of little value. A common example is interaction with a help-desk application, where integration is nothing more than automatically generated e-mail acknowledgements or an SNMP trap. Forty-four percent of respondents indicate that conformance testing by the vendor or a standards body is an important or