

SPECIAL STUDY

Enterprise NAC Survey 2007: The Dynamic and Evolving Scope of NAC in the Enterprise

Gerry Pintal
Jon Crotty

Charles J. Kolodgy

IDC OPINION

Network access control (NAC) is seen by many IT professionals today as the most promising network security innovation enabling IT to enhance overall network security and health.

IT professionals who have the resources to pilot, beta, and roll out NAC solutions for their enterprises, are gaining valuable early experience and insight to assist them in addressing many of their network security needs.

Early NAC evaluation trials and experiences are providing enterprise IT with practical insight into critical business factors, including their return on investment and total cost of ownership, while assessing the overall effectiveness of NAC's ability to provide enhanced network health and security.

For many companies, however, NAC remains out of reach for practical, financial, business, and technical reasons. At the present time, main adoption barriers for NAC continue to exist, including the following:

- Lack of a clear and consistent definition for NAC
- Need for potential large capital and staff investments
- Lack of a NAC standard among the vendors
- Limited vendor interoperability in available solutions
- Mixed reviews of early NAC deployment results

Although NAC vendors are slowly addressing several of these adoption issues, such obstacles continue to be the root cause of a slow adoption rate across the enterprise spectrum. As these adoption barriers are addressed and as more businesses across the industry spectrum establish clear and demonstrable successes, IDC anticipates the adoption of NAC to broaden across the spectrum of enterprise sizes.

We are already beginning to see reports of major successes in NAC rollout projects.

With adoption barriers addressed and/or minimized and with NAC providing a broader scope of integrated security features, IDC forecasts that the NAC market will continue to grow from its current size of \$802 million to \$3.8 billion by 2011.

Summary Results

When the results of this survey are examined, we see that nearly 75% of IT professionals representing very large enterprises have already deployed NAC, are in the evaluation process, or are planning to deploy NAC within the next 24 months.

Nearly 60% of large companies reported the same NAC rollout plans as very large organizations.

At the same time, however, this survey report quantitatively shows that as many as 53% of IT professionals in small and midsize businesses participating in this survey have no immediate plans to deploy NAC.

TABLE OF CONTENTS

	P
In This Study	1
Methodology.....	1
Situation Overview	4
Introduction.....	4
Survey Findings.....	6
Future Outlook	24
Essential Guidance	25

LIST OF TABLES

	P
1 Completed Interviews by Company Size.....	2
2 Completed Interviews by Job Title	3
3 Top IT Network Security Concerns	8
4 Top 8 Enterprise IT NAC Outcome Priorities for the Next 12 Months	9
5 Features Most Preferred for Integration with NAC Solutions.....	16
6 NAC Vendors Currently in Use.....	22
7 NAC Vendors Likely to Be Considered in the Next 12 Months.....	23
8 Leading NAC Vendors	24

LIST OF FIGURES

	P
1 Survey Respondents by Company Size	7
2 IT NAC Solution Priorities.....	10
3 NAC Budget Allocations	11
4 NAC Budget Allocations by Company Size.....	12
5 NAC Deployment Plans	13
6 NAC Deployment Plans by Company Size	14
7 Devices to Be Managed by NAC.....	15
8 Important NAC Purchase Features	17
9 Importance of User Versus Machine Identity.....	18
10 Importance of User Identity by Company Size	19
11 Importance of Machine Identity (MAC Address) by Company Size.....	20
12 NAC Purchased Separately or as a Feature of Existing Products.....	21
13 NAC Delivered by a Single Vendor or Multiple Vendor Components	22

IN THIS STUDY

Methodology

This survey was conducted by IDC with the goal of determining the nature of and extent to which enterprises are adopting NAC as a networking security solution. Further, through this survey we sought to determine, in the eyes of the participants, who the current leading NAC vendors are.

The IDC Security research team designed the survey to gain a clearer understanding of how IT professionals are currently approaching NAC from the following perspectives:

- Budgeting
- Deployment planning
- NAC solution priorities
- LAN devices to manage
- Important integrated NAC features
- Identity and device management and control
- Single- versus multi- vendor purchasing options

The results of this survey provide an intriguing view of each of these NAC security dimensions. The results also reveal areas of both consistency and striking differences among small, medium-sized, large, and very large companies regarding the extent of planning, budgeting, and deployment of NAC.

Qualification and Sample Size

The survey targeted enterprises that have adopted or are planning to adopt NAC as a networking security technology. Within the sample base, the survey focused on gathering information about current NAC activities as well developing a quantifiable sense of where in the spectrum of company sizes the NAC action is currently taking place.

The survey was conducted with respondents who are directly responsible for network infrastructures within their organizations. The survey also included:

- Computer or network consultants
- Systems or network integrators
- VAR and VAD professionals.

Demographics

Respondents to this survey understood the available NAC technologies they required or desired to protect their company's IT network infrastructure. Respondents represented more than 20 industries with job functions that included:

- IT/technology management (43%)
- IT/technology professionals (21%)
- Corporate/business management (36%).

Respondents from within participating organizations included IT executives, managers, and/or professional staff who identified themselves as having "significant responsibility for information technology network security" in their organizations. With 657 individual responses to the Web-based survey, IDC has gained a unique perspective in understanding the current dynamics within this early enterprise NAC adoption curve.

Tables 1 and 2 present the number of completed surveys by the respondents' company size and job title, respectively.

Note: All numbers in this document may not be exact due to rounding.

TABLE 1

Completed Interviews by Company Size

Q. How many people are employed in your entire company, including all branches, divisions, and subsidiaries?

Company Size	Number of Responses
Small (1–99 employees)	269
Medium sized (100–999 employees)	145
Large (1,000–9,999 employees)	125
Very large (10,000+ employees)	105
Total	644

n = 657

Source: IDC's NAC Survey, 2007

TABLE 2

Completed Interviews by Job Title

Q. *What is your job title?*

Job Title	Number of Responses
IT/technology management	283
IT/technology professional	138
Corporate/business management	236
Total	657

n = 657

Source: IDC's *NAC Survey*, 2007

SITUATION OVERVIEW

Introduction

Network security continues to be a major focus for enterprise IT management and professionals. A significant challenge for IT is securely keeping pace with the proliferation and use of existing and newly introduced endpoint devices, including PDAs, iPods, printers, and copiers.

Many of these newly introduced IP devices that seek access to the network are unmanaged or unmanageable by IT and clearly represent added security exposure to the network's overall security posture.

Enterprise networks have been giving corporate local users near-instantaneous access to internal and external digital information while providing secure remote network access for SSL/VPN and wireless access points (WAPs). As corporate networks have experienced increased bandwidth, stability, and availability, they have also become the conduit for supporting digital voice (VoIP) and video datastreams.

As the proliferation of IP endpoint types continues, enterprise IT staffs recognize the significant increase in security vulnerabilities and threat vectors created by their introduction. At the same time, top-of-mind issues for enterprise IT and security professionals continue to include:

- Network availability
- Network performance,
- Network health
- Internal and external breach threats
- Malware
- Policy enforcement
- Private and confidential information leakage

Adding to this complex mix of technical challenges, federal, local, and international regulations now mandate that enterprises establish comprehensive policy enforcement mechanisms, significantly raising the risk stakes for enterprise management and IT.

To begin addressing these network security headaches, Network Admission Control, as a network-based security architecture, was first announced by Cisco Systems Inc. late in 2003.

In early specifications and implementations of NAC, its primary purpose was to ensure a secure and healthy network by forcing all devices seeking to attach to the network to conform to established policies. Devices failing to conform to these

policies were either placed into quarantine and given the opportunity to remediate or denied access to the network altogether. This definition remains a foundational tenant of what NAC does and/or should do. However, on the basis of the results of this IDC survey and further in-depth research, IDC anticipates that NAC will begin to play a broader and more significant role in securing and keeping enterprise networks sanitized.

This projection is clearly supported by survey results: Over 60% of the respondents indicated they want to see vendors broaden NAC's scope to include the following:

- Identity management
- Application-level authorization
- Patch management

Survey respondents would like to see these features more tightly integrated into NAC vendor product offerings.

Recent innovations in network security, now commonly referred to as network access control (NAC), have significantly increased the prospects for improved network health by reducing overall network security risks resulting from the proliferation of network attack vectors and the simultaneous introduction of existing and newly introduced IP network devices.

In IDC's *Worldwide Network Access Control 2007–2011 Forecast: Organizations Get the Knack for NAC* (IDC #206966, June 2007), we discussed that IT executives representing six industries unanimously expressed optimism for NAC as an effective approach to improving overall network security. In contrast, the participants to this recent survey expressed significant reservations and concern over the lack of a common standard and interoperability between NAC vendor offerings.

Early NAC implementations required large capital investments by IT to replace or "forklift" many of their existing infrastructure components to implement NAC within their existing network infrastructures. With IT budgets under constant pressure, the need to replace or upgrade significant portions of the network infrastructure components to accommodate NAC significantly constrains the rate of NAC adoption by enterprises independent of their size.

NAC architectures and vendor implementations continue to evolve at a rapid pace, with NAC vendors seeking to differentiate their NAC solutions with more unique architectural approaches and enhanced features.

In an effort to speed up the NAC adoption rate, some progress has been made by NAC vendors that address some earlier IT concerns. For example:

- The Trusted Computing Group (TCG) first introduced its Trusted Network Connect (TNC) open architecture specification in May 2004. The TNC standard was created by TCG to address PC client, mobile device, server, PDA, and other endpoint network integrity issues.

- ☒ In September 2006, Cisco Systems and Microsoft announced they would provide their customers and partners with clear guidance on how Cisco's NAC and Microsoft's Network Access Protection (NAP) architectures could interoperate.
- ☒ On May 1, 2007, TCG and Microsoft announced that they would provide customers and partners with interoperability of TCG's TNC architecture and Microsoft's NAP in both TNC-protected networks and NAP-protected networks.
- ☒ On May 1, 2007, Juniper Networks and Microsoft announced that the companies were collaborating to provide open standards-based interoperability between Juniper's Unified Access Control (UAC) v2.0 solution and Microsoft's NAP platform.

IDC believes that as a result of these announcements, two of the original NAC adoption concerns expressed by enterprises (i.e., standards and interoperability) have been, to a degree, lessened.

The Microsoft, Cisco Systems, and Juniper Networks announcements are considered to be significant steps forward for NAC adoption. IDC believes that some resistance to NAC adoption will continue until Microsoft releases its complete NAP support in Server 2008.

In an effort to address the concern over altering an existing network infrastructure to implement NAC, some vendors such as ConSentry Networks and Vernier Networks have architected their NAC solutions to ease the integration of NAC into existing IT network infrastructures. These NAC solutions provide IT staff with the flexibility of choice, where they are not forced into re-architecting their network infrastructures to implement NAC solutions.

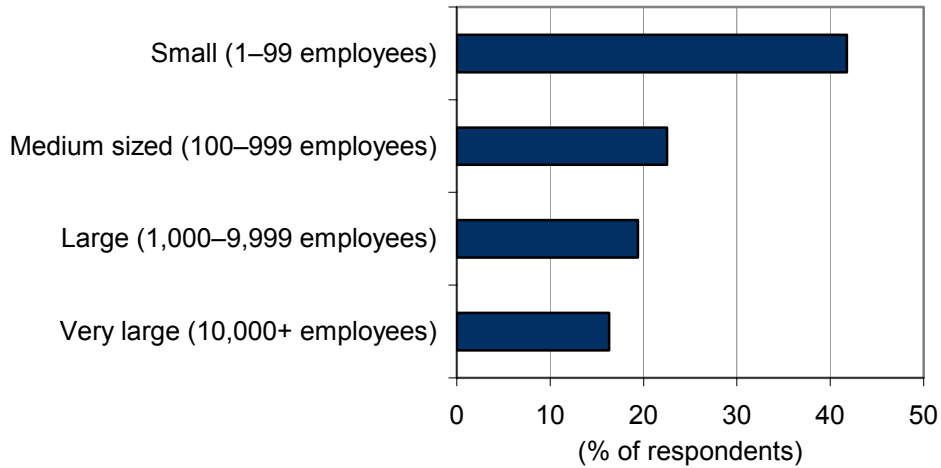
Survey Findings

We begin our analysis of survey findings with a description of the survey respondent demographics. Figure 1 provides a graphical view of the survey respondents by business size. As shown, business size is represented here by the number of employees.

FIGURE 1

Survey Respondents by Company Size

Q. *How many people are employed in your entire company, including all branches, divisions, and subsidiaries?*



n = 657

Source IDC's NAC Survey, 2007

As can be seen in the figure, over 40% of the respondents to this survey were with small companies (fewer than 100 employees), with a fairly level breakdown among the remaining respondents from medium-sized, large, and very large enterprises. Where appropriate, we provide more detailed drilled-down views of results by company size.

Table 3 provides insight into the current perceived security risk types faced by enterprises today. As indicated, the top security risk sources listed come as no surprise: Mobile employees and wireless access top the list of network security concerns, as indicated by 52% and 46% of respondents, respectively.

TABLE 3**Top IT Network Security Concerns**

Q. *In your enterprise what type of network users present the greatest security concern?*

Risk Source	% of Respondents
Mobile employees	52
Wireless access	46
Guests (internal access)	45
Local employees (internal access)	45
Contractors (internal access)	42
Managed remote offices	36
Partners (external access)	32
Customers (external access)	30

n = 657

Notes:

Values represent those respondents who chose 4 or 5 on a scale from 1 to 5, with 1 being no threat and 5 being a significant threat.

Multiple responses were allowed.

Source: IDC's *NAC Survey*, 2007

Of particular interest, however, we see that local employees (internal access) and guests rank third in terms of being a security threat, with 45% responding for each. This data point correlates well with data compiled during IDC's 2006 *Enterprise Security Survey*; at the time of that survey, local employees were also seen to be an increasing threat to enterprise security.

Table 4 provides insight into the primary NAC objectives enterprise IT professionals have set for themselves during the next 12 months. Unauthorized internal and external net access was the number 1 priority with 81% of the survey participants responding. This comes as no surprise as this is one of the primary NAC design goals.

TABLE 4**Top 8 Enterprise IT NAC Outcome Priorities for the Next 12 Months**

Q. *How important are each of the following outcomes to your company over the next 12 months?*

Priority Items	% of Respondents
Unauthorized internal and external net access	81
Data security and IP protection	74
Malware protection	68
Control unmanaged devices	58
Policy management and enforcement	57
Ensure endpoint compliance	53
Improved network health	52
Meet regulatory requirements	50

n = 645

Notes:

Values represent those respondents who chose 4 or 5 on a scale from 1 to 5, with 1 being not at all important and 5 being a extremely important.

Multiple responses were allowed.

Source: IDC's *NAC Survey*, 2007

The number 2 priority revealed by responses to this question, data security and IP protection, provides an interesting data point in the expanding scope of expectations regarding NAC.

Although managing internal and external access to the network will provide some level of mitigation for data security and IP protection, vendor products that fall into IDC's security taxonomy in the category of information protection and control (IPC), more broadly cover this area of security.

In terms of top-of-mind security issues, IDC research also identifies IPC as a rapidly increasing security concern for enterprises.

IPC includes solutions that discover, protect, and control sensitive information. It is a comprehensive approach that prevents sensitive customer data or company information from being distributed within or outside the enterprise — potentially in violation of regulatory or company policies. IPC includes the following technologies:

- Data-in-motion IPC:** Data-in-motion IPC includes solutions that monitor, encrypt, filter, and block outbound content contained in email, instant messaging, peer to peer, file transfers, Web postings, and other types of messaging traffic.

- ☒ **Data-at-rest IPC:** Data-at-rest IPC includes solutions that discover, protect, and control information on desktops, laptops, file/storage servers, USB drives, and other types of data repositories.
- ☒ **Data-in-use IPC:** Data-in-use IPC includes solutions that protect and control information in use. These solutions are used to maintain the integrity of sensitive information such as in contracts, term sheets, and other business-critical documents.

For more detailed information on IPC, refer to *Worldwide Information Protection and Control (IPC) 2007–2011 Forecast and Analysis: Securing the World's New Currency* (IDC #206750, May 2007).

The remaining NAC priority outcomes are consistent with the security issues that NAC vendor implementations currently address.

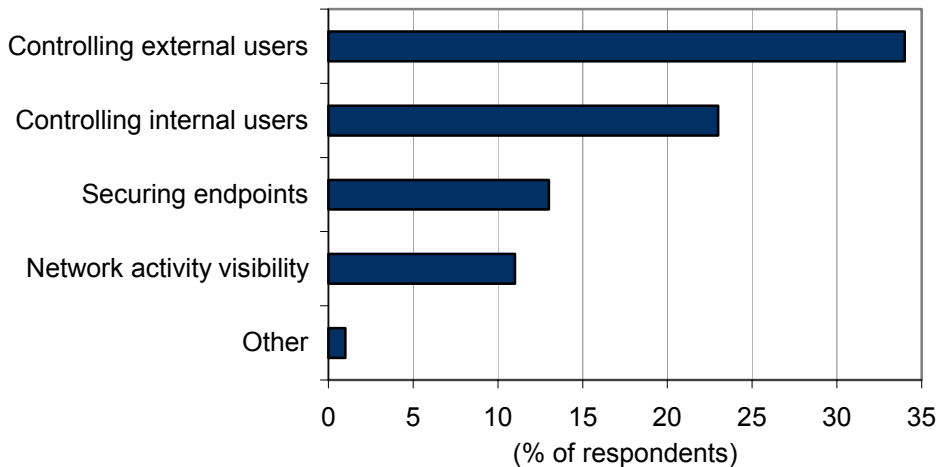
With the number 2 survey response indicating data security and IP protection is a top issue concerning IT, we begin to develop a sense of the broadening expectations by IT for NAC to become a more comprehensive network security solution.

In Figure 2 we see a strong confirmation of the expected primary functional roles that IT professionals expect NAC implementations will play in the enterprise. Controlling external and internal users, securing endpoints, and gaining additional visibility into the enterprise network activities are the predominant control factors expected of NAC.

FIGURE 2

IT NAC Solution Priorities

Q. Which one of the following is your company's highest priority for NAC deployment?



n = 657

Source IDC's NAC Survey, 2007

Controlling external users has always been a significant challenge for IT. Now with the ever-increasing number of mobile devices in use by enterprise personnel, the challenge and threat sources facing IT have increased significantly. In addition, the need for IT to manage unmanaged or unmanageable devices either seeking to connect to the network or already connected to the network is yet another source of threat to the integrity of the enterprise. Examples of currently unmanaged devices include the following:

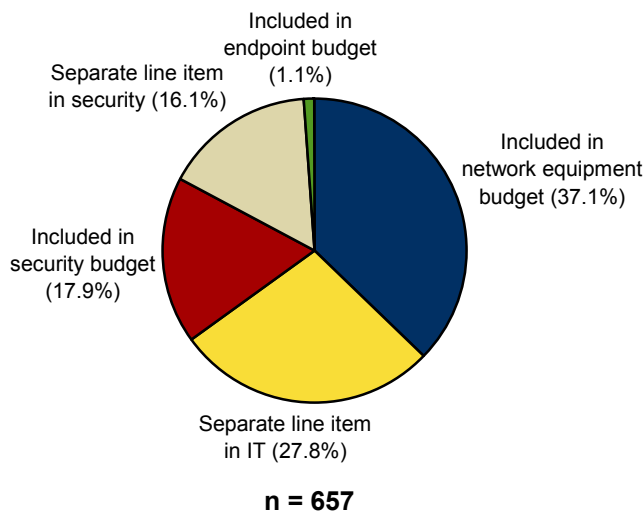
- ☒ Medical devices
- ☒ Process control devices
- ☒ Devices supported by legacy operating systems
- ☒ SCADA systems

Figure 3 provides a look at how enterprises are currently budgeting or are planning to budget for their NAC implementations. From this view we see that a majority of the respondents to the survey see NAC as either a network equipment budget line item or a separate line item in the IT budget. The interesting result, however, is that only 18% of the respondents see NAC as a security budget item; in contrast, 65% of the respondents consider NAC an IT network budget item.

FIGURE 3

NAC Budget Allocations

Q. *Is or will your company's budget for NAC purchases be:*



Source IDC's NAC Survey, 2007

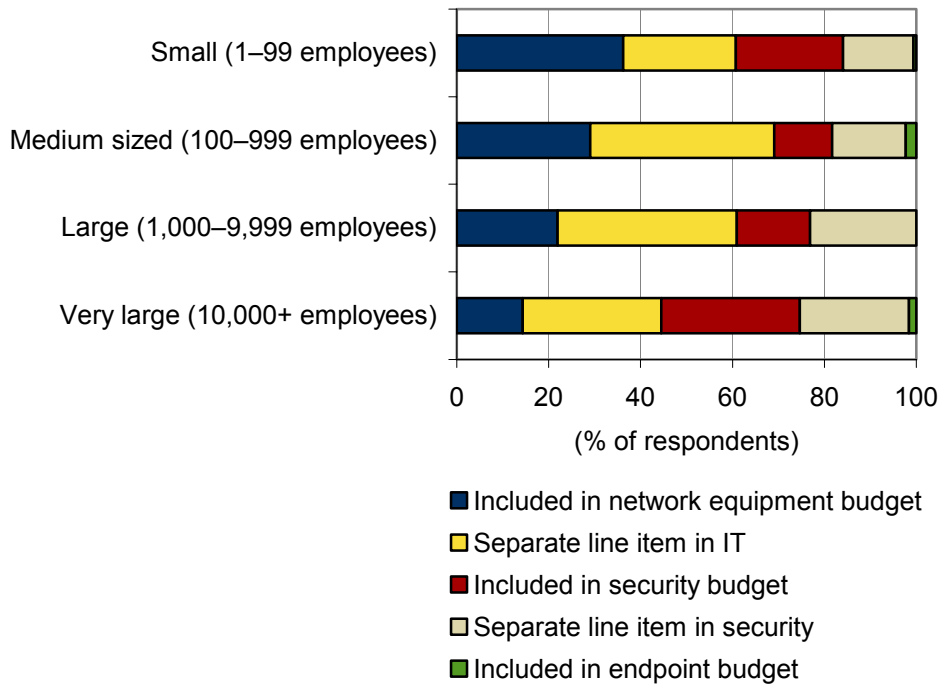
To gain a better perspective on the budgeting issue, Figure 4 provides a more detailed view of how NAC budgeting is being or will be addressed by company size. In Figure 4 we see that 60%–70% of small, medium-sized, and large companies appear to be inclined to incorporate NAC into their IT or equipment budgets, whereas very large enterprises are more evenly divided on budgeting for NAC in their IT/equipment budgets versus their security budgets.

The implication here is that NAC is currently being viewed as a feature of an IT network infrastructure rather than as a security component. IDC anticipates that this view of NAC may change over time as NAC functionality continues to grow beyond the current NAC vendor offerings.

Figure 5 provides an overall view into where the survey respondents are in their NAC deployments or deployment plans. With 44% of the respondents indicating they have no plans for NAC deployment and 19% in the evaluation phase, we see a continued reluctance to move forward with NAC deployments.

FIGURE 4

NAC Budget Allocations by Company Size

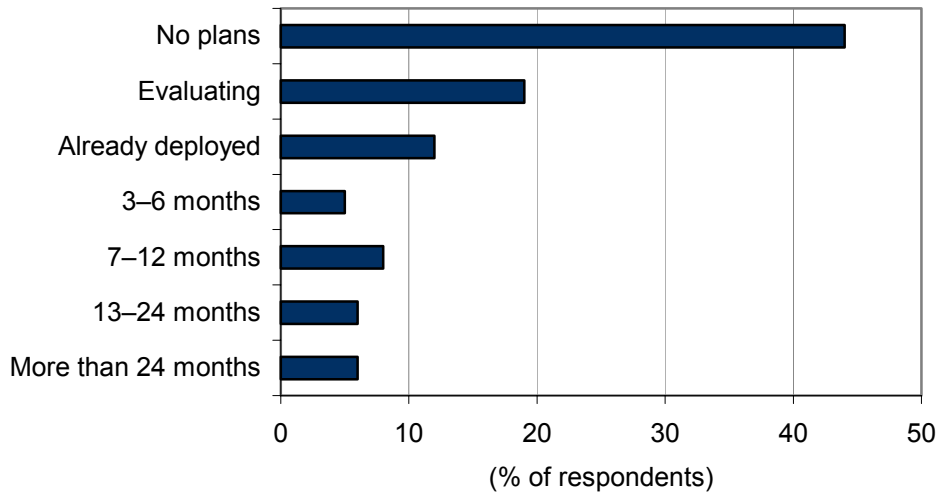


n = 657

Source IDC's NAC Survey, 2007

FIGURE 5

NAC Deployment Plans



n = 657

Source IDC's NAC Survey, 2007

IDC believes that previously discussed barriers to entry such as the lack of a common standard, cost of implementation, interoperability, and the need for more effective education continue to provide a drag on the overall adoption rate across the spectrum of company sizes.

For existing NAC vendors, these results clearly indicate significant remaining opportunities to continue strengthening their position in the market by addressing as many of the negating adoption issues as practical. For vendors that have been on the edge of deciding to enter the NAC market, IDC also sees opportunities to partner with existing NAC players by establishing themselves in unique feature/functionality niches within the overall NAC market.

When the survey data is examined in more detail, at the company size level, as shown in Figure 6, we see in Figure 5 that the aggregate data indicates 44% of the survey respondents have no plans for NAC. The results shown in Figure 5 are largely influenced by responses from small company representatives.

When we examine the responses from very large enterprise in more detail, we see that nearly 75% of respondents to the survey have either already deployed NAC or are in the evaluation process and are planning to deploy NAC within the next 24 months. Nearly 60% of large companies reported the same rollout plans as were indicated by the very large organizations.

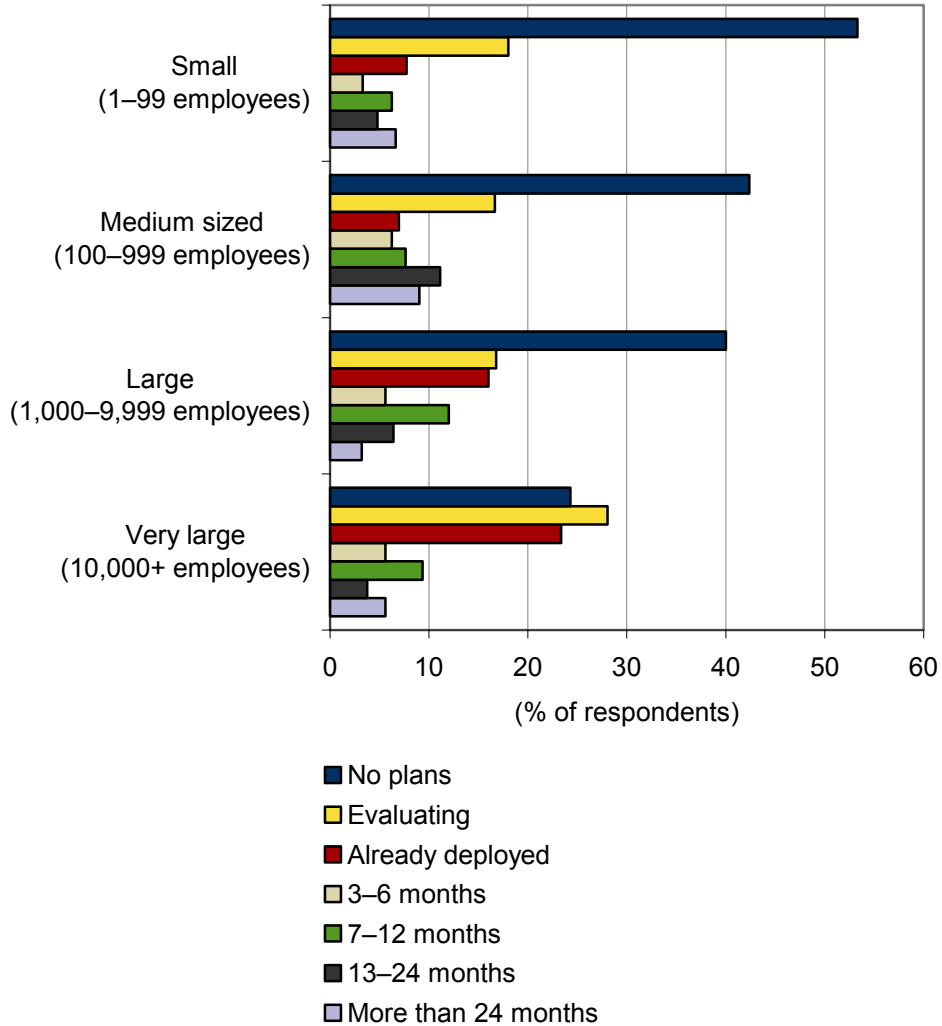
On the opposite end of the adoption scale, 53% of small companies reported no current plans to deploy NAC. These results correlate well with the fact that smaller companies are generally not eager early technology adopters. The lack of incentive to adopt new technologies in small to midsize companies is principally driven by the lack of dedicated qualified technical staff and sufficient financial resources to direct and

invest in leading-edge technologies. In practical terms, for small to midsize businesses there is no immediately obvious cost/benefit or return on their investment.

Figure 7 describes the devices that survey respondents want to have NAC manage.

FIGURE 6

NAC Deployment Plans by Company Size

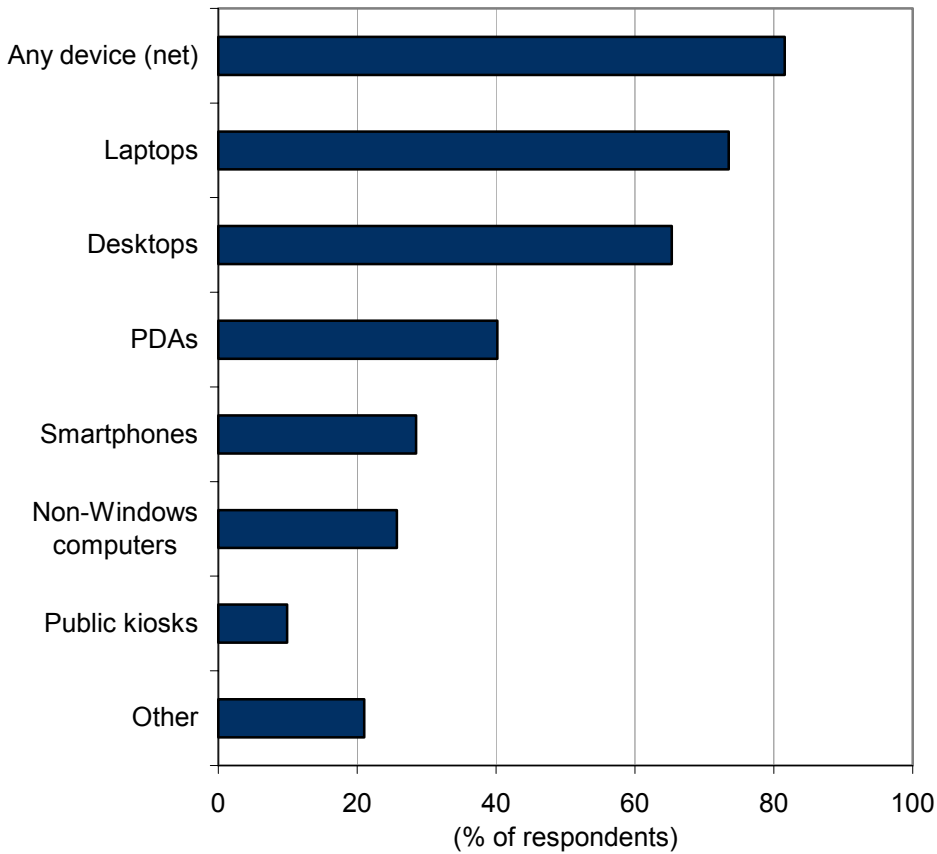


n = 657

Source IDC's NAC Survey, 2007

FIGURE 7

Devices to Be Managed by NAC



n = 657

Note: Multiple responses were allowed.

Source IDC's NAC Survey, 2007

When the survey participants were asked what devices they want managed by NAC, over 80% indicated that they expect NAC to manage all/any devices connecting to their networks. Laptops, PDAs, and smartphones ranked among the top 5 devices that IT professionals want managed by NAC.

Table 5 contains a detailed listing of the results to the question regarding what features they would like to see integrated into NAC solutions.

TABLE 5**Features Most Preferred for Integration with NAC Solutions**

Q. How important is it that the following features be integrated with NAC solutions?

Feature	% of Respondents
Identity management	75
Antivirus	74
Endpoint quarantine	70
Policy management	69
Application-level authorization	63
Automated remediation	61
Patch management	61
Compliance reporting	60

n = 646

Notes:

Values represent those respondents who chose 4 or 5 on a scale from 1 to 5, with 1 being not at all important and 5 being a extremely important.

Multiple responses were allowed.

Source: IDC's *NAC Survey*, 2007

When respondents were asked about what additional features they would like to see integrated into NAC vendor solutions, their responses in most cases were consistent with expected results — and included antivirus, endpoint quarantine, and automated remediation.

However, with 75% of the respondents selecting identity management as an important integrated feature, we again see a clear shift in the expanding role that IT would like NAC to play in network security solutions. Overall, 63% of the respondents selected application-level authorization as an important feature they want to see integrated into NAC.

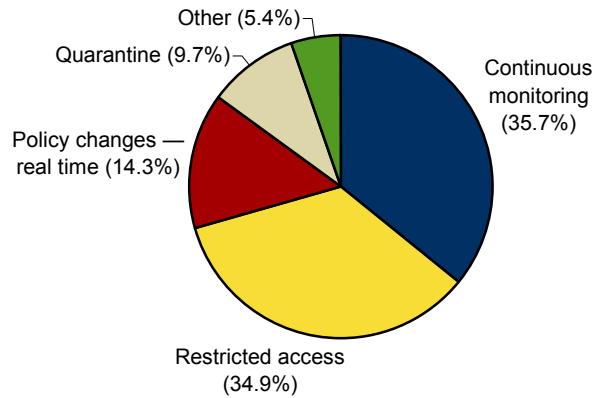
Figure 8 provides a view into what features the survey respondents consider to be an important part of the NAC purchase decision. When respondents were asked about the NAC features that are important to their decision to purchase, continuous monitoring and restricted access accounted for over 70% of the responses received.

With 35.7% of the survey respondents indicating continuous monitoring is an important feature to consider when purchasing a NAC solution, we again see a broadening scope for NAC's role in the enterprise. IT respondents clearly see a benefit and need for endpoint monitoring to extend beyond the initial scans initiated and performed by NAC.

FIGURE 8

Important NAC Purchase Features

Q. *What features are important to your company when making NAC purchase decisions?*



n = 657

Source IDC's NAC Survey, 2007

IT professionals clearly want more visibility into what these endpoint devices are doing while connected to their networks. Only 14% of the respondents indicated a desire to see policy changes implemented in real time. The interesting laggard in this area is quarantining, capturing slightly less than 10% of the responses to this question.

Figure 9 provides a view into the responses to a survey question regarding the relative importance of having NAC track user identity versus machine identity. As indicated in Figure 9, over 60% of the respondents to the survey clearly see machine identity as extremely important; 36% see user identity as extremely important.

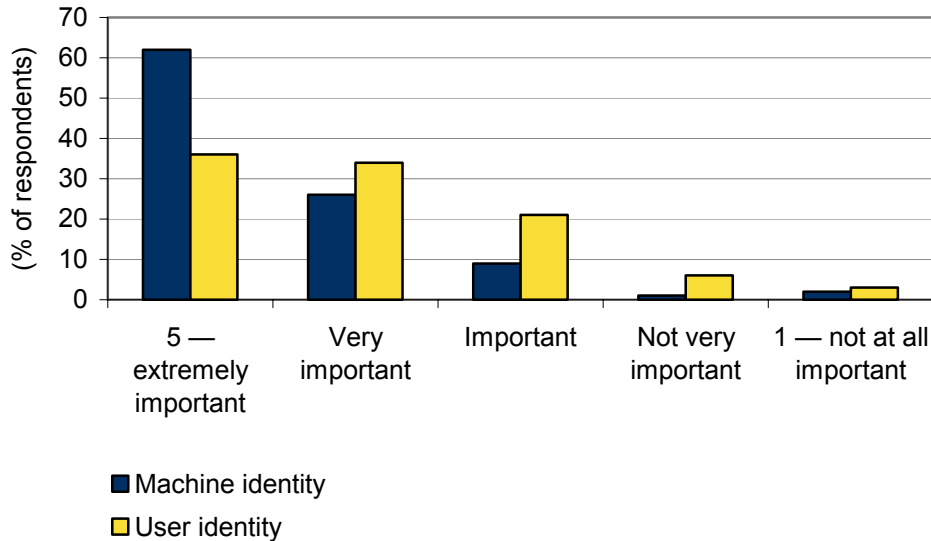
Original versions of NAC sought to manage and control endpoints via IP address and/or machine or Media Access Control (MAC) address. While managing devices by machine ID is a primary NAC capability, tracking machine ID (MAC) can also be used in managing and tracking capital equipment for inventories.

As enterprise IT professionals recognize NAC's ability to provide a broader level of control on what and who seek access to the network, ascertaining user identity is becoming an increasingly more important feature for their NAC implementations.

FIGURE 9

Importance of User Versus Machine Identity

Q. On a 5-point scale where 5 is extremely important and 1 is not at all important, how important is user identity vs. machine identity?



n = 657

Source IDC's NAC Survey, 2007

To gain a clearer understanding of the responses to the user identity-versus-machine identity question, Figures 10 and 11 provide some additional insight into the survey responses by company size.

Although the clear choice, as shown in Figure 9, is managing the access of endpoints by machine identity, we see in Figure 10 a clear shared interest (53% to 66%) among small to very large enterprises in capturing and tracking the user identity of devices attaching to their networks.

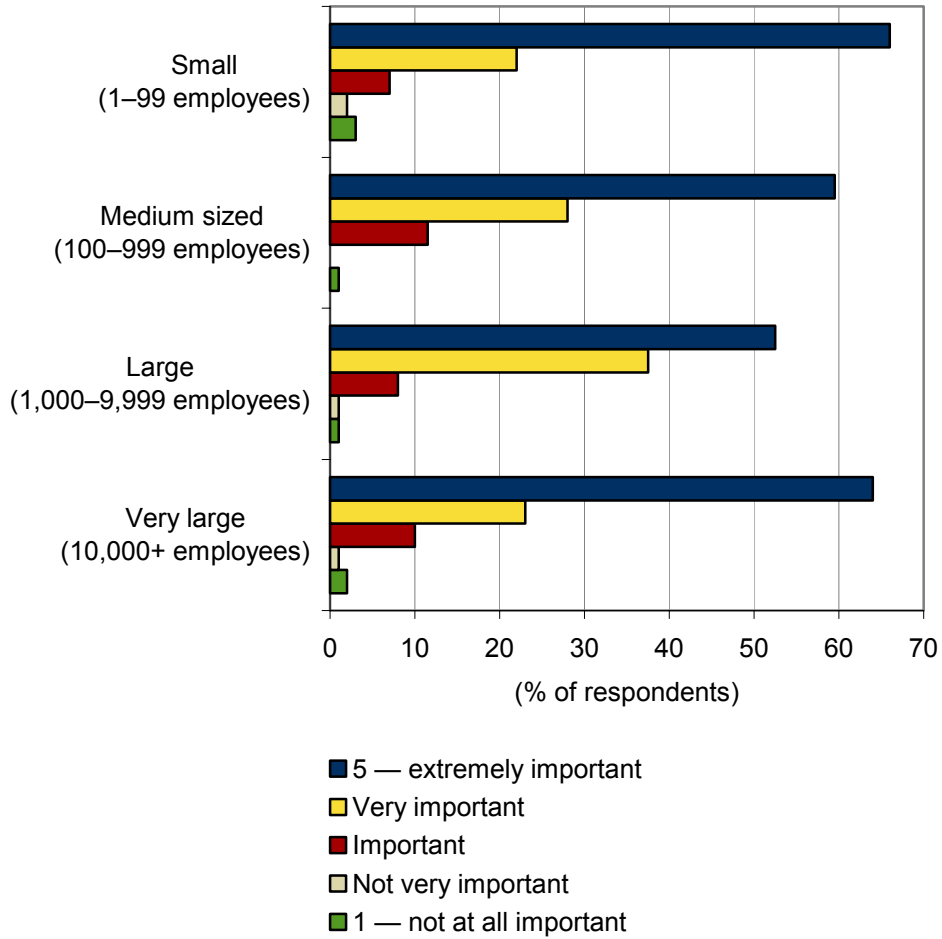
The responses to the question regarding the importance of knowing and tracking user identity correlate well with the responses to the question regarding desired integrated NAC product features listed in Table 5. There, 75% of the survey respondents indicated they want to see identity management as an integrated feature of their NAC solutions.

Figure 11 illustrates the respondents' belief in the relative importance of tracking endpoint devices by their MAC address. Although this data indicates minor variances in the perceived importance of tracking machine identity across the enterprise size spectrum, it is quite clear from these results that tracking machine identity is viewed as very to extremely important to IT professionals.

FIGURE 10

Importance of User Identity by Company Size

Q. On a 5-point scale where 5 is extremely important and 1 is not at all important, how important is user identity vs. machine identity?



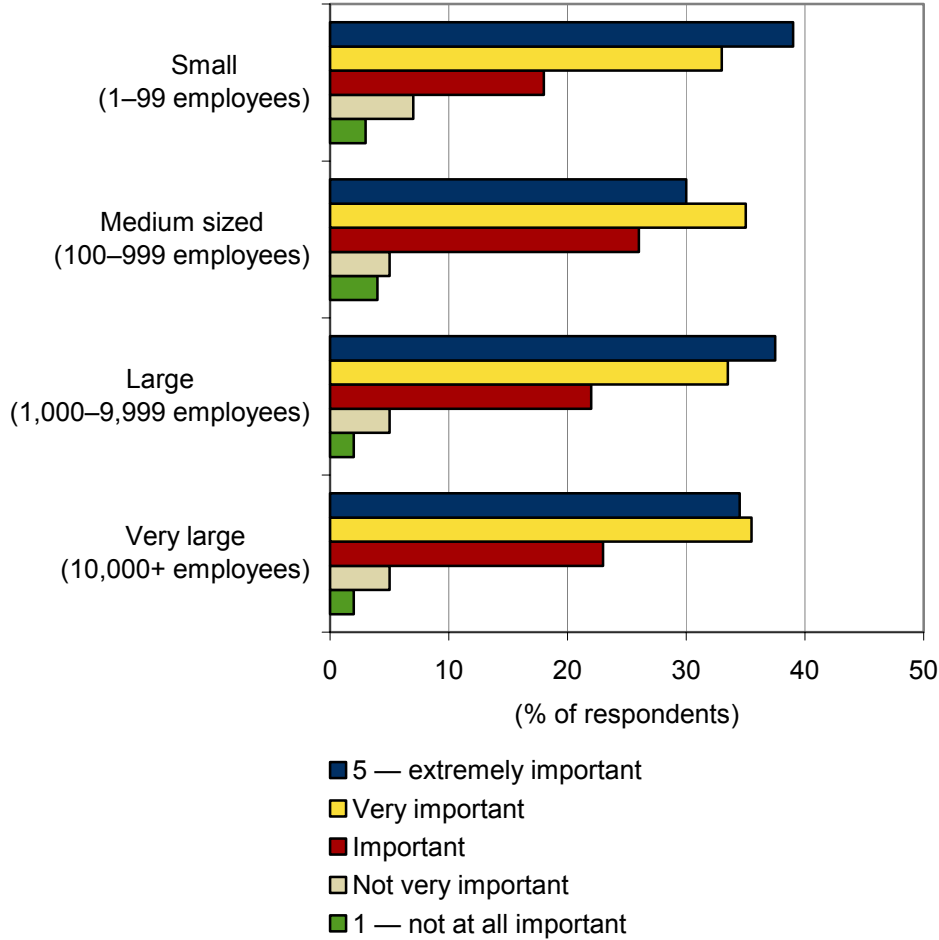
n = 657

Source IDC's NAC Survey, 2007

FIGURE 11

Importance of Machine Identity (MAC Address) by Company Size

Q. On a 5-point scale where 5 is extremely important and 1 is not at all important, how important is user identity vs. machine identity?



n = 657

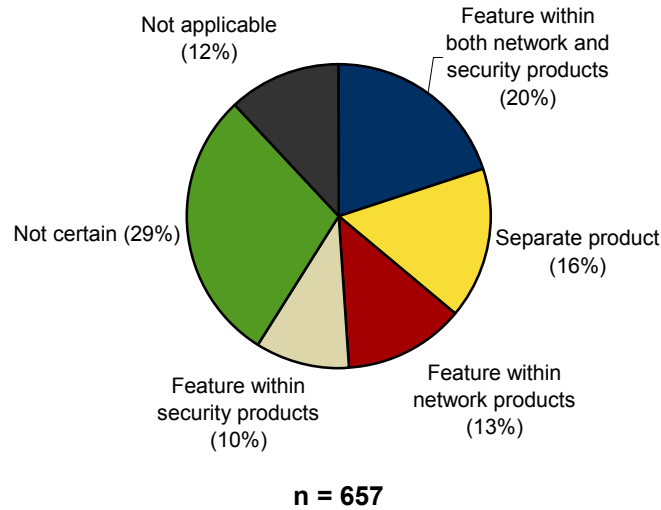
Source IDC's NAC Survey, 2007

Figure 12 provides some insight into whether IT views a NAC purchase to be a separate acquisition or a feature of existing vendor offerings. Nearly 30% of the respondents indicated they are not certain how NAC should be offered by vendors. Only 16% believe that NAC should exist as a separate product, and 20% believe that NAC should be a feature within both network and security products. From these responses, it is quite clear that there remains a great deal of uncertainty about what the most effective NAC implementations are, or should be.

FIGURE 12

NAC Purchased Separately or as a Feature of Existing Products

Q. *Do you envision NAC being a product category you will purchase separately or a feature of existing products?*



Source IDC's NAC Survey, 2007

Figure 13 provides a view into whether the survey participants view NAC as being effectively delivered by single or multiple vendors. In terms of NAC implementations being provided by a single vendor or multiple vendors, we again observe disparity in IT points of view. Nearly 34% of the respondents see NAC requiring a multivendor solution. However, if we take the sum of single-vendor responses, we see 30% of the respondents expect their NAC implementations to be with a single vendor. IDC sees this result as an indication of current tightly bound partners being the preferred method for NAC implementations.

Tables 6–8 provide insight regarding the vendors currently considered to be the prominent NAC players.

Table 6 provides a listing of the responses to the question regarding which of the NAC vendors currently have a presence in their companies.

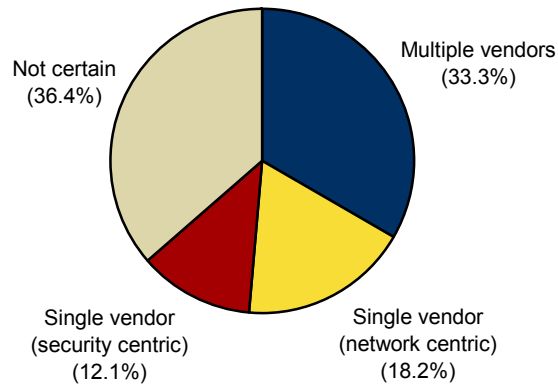
Table 7 provides a listing of the responses to the question regarding which of the NAC vendors are likely to be considered for use in the next year.

Table 8 provides a listing of the survey responses to the question regarding who the respondents consider the leading NAC vendors to be.

FIGURE 13

NAC Delivered by a Single Vendor or Multiple Vendor Components

Q. *Do you believe NAC can be effectively delivered by a single vendor or that it requires multiple vendor components?*



n = 657

Source IDC's NAC Survey, 2007

TABLE 6

NAC Vendors Currently in Use

Q. *Which, if any, of the following NAC vendors are currently in use at your company?*

Vendor	% of Respondents
Cisco	40
Microsoft	31
Symantec	28
McAfee	22
Trend Micro	10
Check Point	9
HP ProCurve	8
Juniper Networks	7
Nortel Networks	5
IBM (ISS)	4

n = 657

Note: Multiple responses were allowed.

Source: IDC's NAC Survey, 2007

TABLE 7**NAC Vendors Likely to Be Considered in the Next 12 Months**

Q. Which, if any, of the following NAC vendors is your company likely to consider for use during the next 12 months?

Vendor	% of Respondents
Cisco	38
Microsoft	22
Symantec	21
McAfee	16
Juniper Networks	11
Check Point	9
HP ProCurve	8
Nortel Networks	4
IBM (ISS)	3
Tipping Point	2

n = 657

Note: Multiple responses were allowed.

Source: IDC's *NAC Survey*, 2007

TABLE 8**Leading NAC Vendors**

Q. Which one of these vendors do you consider to be the leading NAC vendor?

Vendor	% of Respondents
Cisco	49
Symantec	10
Microsoft	8
Check Point	5
McAfee	5
Juniper Networks	4
Trend Micro	2
F5	2
Nortel Networks	2
HP ProCurve	2

n = 497

Source: IDC's NAC Survey, 2007

FUTURE OUTLOOK

IDC believes that ongoing developments by NAC vendors that are aimed at minimizing the overall complexity, difficulty, and costs of integrating NAC into existing network infrastructures will continue at a rapid and accelerated pace. As these issues become secondary concerns, IDC forecasts a broadening of NAC's appeal across a wider range of enterprise sizes.

In addition to easing the integration of NAC into IT network infrastructures, NAC vendors are also aggressively leading the charge to broaden the overall scope of NAC and the role it plays in addressing other top-of-mind network security issues experienced by most enterprise IT professionals.

Current top-of-mind issues IT professionals are looking for NAC to help them address include the following:

- Unauthorized network access by internal and external users
- The proliferation of manageable and unmanageable endpoint devices, including mobile, wireless, and other consumer-oriented devices

- ☒ Central control, management, and monitoring of endpoints
- ☒ Enhanced malware protection for the network
- ☒ Data leakage and/or information protection and control
- ☒ Policy management and enforcement
- ☒ Overall improvement in network health and performance
- ☒ Meeting regulatory mandates and auditing requirements

As these IT needs begin to be comprehensively addressed by NAC vendor offerings, IT professionals will be able to build strong cases for funding their NAC projects on the basis of more attractive return on investments and cost of ownership.

ESSENTIAL GUIDANCE

Over the past several years NAC has become a major focus of interest for IT and security professionals within a wide spectrum of industries and businesses. NAC is no magic silver bullet that resolves all of an enterprise's IT security issues and concerns. However, NAC does currently offer the best promise for significantly improving overall network security in the enterprise.

The continued high level of interest in NAC by IT and security professionals is being driven by the fact that NAC will allow IT professionals to centrally manage and control overall network security.

NAC as a component of the network infrastructure is still in the early stages of evolution. However, NAC is rapidly developing into a technology that will have broad appeal to enterprises committed to the highest levels of security.

There is no single "one size fits all" NAC solution. NAC products, in some cases, can be tightly integrated into the network fabric, or they can be made to integrate into an existing network infrastructure with minimal impact and changes. Some enterprises may look to NAC for management and control of all devices seeking to attach to their networks, while others will want their NAC solutions to centrally manage and control as much of their network security defenses as possible.

From this research effort involving more than 650 IT and security professionals, we see that there has been a learning curve in terms of understanding NAC's potential for improving security in the enterprise. IT professionals continue to have raised expectations on what additional security features they want to see NAC vendors address in their NAC solutions.

As NAC vendors respond to these IT expectations and continue to assimilate additional security features into their NAC solutions, IDC sees the potential for a widening appeal and acceptance of NAC across a broader spectrum of company sizes. We are already seeing vendors responding to IT expectations by integrating additional features into their offerings.

These features include the following:

- ☒ Identity management
- ☒ Identity controlled application access
- ☒ Central management of access policies
- ☒ Pre- and postadmission scanning

NAC solutions that offer these optional integrated features will provide IT with a much stronger ROI case in their pursuits to fund their NAC solutions.

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2007 IDC. Reproduction is forbidden unless authorized. All rights reserved.