

World Network Access Control Technologies

Markets

N350-74

Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation.

Frost & Sullivan reports are limited publications containing valuable market information provided to a select group of customers in response to orders. Our customers acknowledge when ordering that Frost & Sullivan reports are for our customers' internal use and not for general publication or disclosure to third parties.

No part of this report may be given, lent, resold, or disclosed to non-customers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the permission of the publisher.

For information regarding permission, write:

Frost & Sullivan
2400 Geng Road, Suite 201
Palo Alto, CA 94303-3331
United States

Table of Contents

CHAPTER I

Executive Summary

Executive Summary	I-1
<i>Market Overview & Definitions</i>	I-1
Introduction	I-1
Product Defined	I-2
Revenues Defined	I-4
Vertical Market Segments Defined	I-4
Geography Defined	I-5
<i>Market Dynamics</i>	I-5
Market Drivers	I-5
Market Restraints	I-6
<i>World Network Access Control Technologies Market Forecast</i>	I-6
<i>Summary of Major Findings</i>	I-7

CHAPTER 2

World Network Access Control Technologies Markets

Market Overview	2-1
<i>Market Overview & Introduction</i>	2-1
<i>Market Definitions</i>	2-2
Product Defined	2-2
NAC Architecture Defined	2-3
CISCO NAC	2-3
MICROSOFT NAP	2-3
TCG TNC	2-4
OTHER END-TO-END SOLUTIONS	2-4
NAC Appliance Defined	2-4

Revenues Defined	2-5
<i>Market Engineering Analysis</i>	2-5
Market Stage	2-7
Number of Competitors	2-7
Degree of Technical Change	2-7
Customer Satisfaction	2-7
Market Concentration	2-8
Market Dynamics	2-8
<i>Industry Challenges</i>	2-8
Conveying the Value of NAC to Potential Customers	2-8
Developing and Adhering to a Single Standard for NAC Solutions	2-9
Creating a Transparent End-user Experience	2-9
Adding Value to NAC Products through Increased Functionality	2-10
Providing Consulting Services for Customers Lacking Security Policies or Experience	2-10
<i>Market Drivers</i>	2-10
Publicity of Financial Losses Caused by Network-based Attacks Increases	
Demand for Network Security Products	2-11
Dissolution of the Security Perimeter Due to Increasing Numbers of Remote Workers and Mobile Devices	2-12
Extra Functionality Increases the Value of NAC Products and Creates a Stronger Business Case	2-12
Policy Enforcement Without Technology Proves to be Ineffective	2-12
Government and Industry Regulations Mandating Strict Security Practices	2-13
NAC Technology has Matured to Provide Acceptable Levels of Scalability and Performance	2-13
Progression of NAC Solutions Improve and Broaden Organization's Security Abilities	2-13
Customers Recognize NAC Services as Long-term Investments	2-14
<i>Market Restraints</i>	2-14
Costly Solutions that Require Replacements or Upgrades of Major Network	
Components Reflects Poorly in Customer Cost-benefit Analysis	2-15
Lack of Agreement on a Single Set of Standards Hinders Uptake in Larger Organizations	2-15
Many Approaches to NAC Creates a Wide Range of Options for Potential Customers; Causing Confusion and Complicating the Sales Process	2-15
Slow Adoption Rates of Windows Server 2008	2-16
Low Adoption Rates of NAC Related Technology Such as 802.1X	2-16
NAC Deployments Stalled by Inadequate Sets of Organizational Security Policies	2-16
Competition with Other Security Products	2-17
Low Entry and Exit Barriers May Allow Knock-off NAC Products into the Market	2-17
<i>Partnerships</i>	2-17

Revenue & Unit Shipment Forecasts	2-18
<i>World Network Access Control Appliance Market Forecasts</i>	2-18
Vertical Market Analysis	2-20
<i>Overview</i>	2-20
<i>Education</i>	2-21
<i>Government</i>	2-22
<i>Healthcare</i>	2-22
<i>Financial Institutions</i>	2-22
<i>Telecommunications & Technology</i>	2-23
<i>Utilities</i>	2-23
<i>Others</i>	2-23
Geographic Market Analysis	2-24
<i>Overview</i>	2-24
<i>North America</i>	2-24
<i>Europe</i>	2-25
<i>Asia-Pacific</i>	2-25
<i>Rest-of-World</i>	2-25
Competitive Analysis	2-25
<i>Overview</i>	2-25
<i>Product Analysis</i>	2-27
<i>Market Share Analysis</i>	2-29
<i>Competitive Landscape</i>	2-29
<i>Market Leader</i>	2-31
Cisco Systems, Inc.	2-31
<i>Market Contenders</i>	2-31
ForeScout	2-31
Mirage Networks	2-32
Symantec	2-32

Juniper Networks	2-32
<i>Market Specialists</i>	2-33
Bradford Networks	2-33
Lockdown Networks	2-33
StillSecure	2-33
McAfee	2-33
<i>Niche Players</i>	2-34
Nevis Networks	2-34
TippingPoint	2-34
Insightix	2-34
Nortel Networks	2-35
<i>Emerging Players</i>	2-35
Sophos	2-35
Novell	2-35
Napera Networks	2-36
HP ProCurve	2-36
Strategic Recommendations	2-36
<i>Strategic Recommendations for NAC Architecture Vendors</i>	2-36
Comprehensive Protection	2-37
Flexible Deployment	2-37
Scalability	2-38
Natural Extension of Infrastructure	2-38
<i>Strategic Recommendations for NAC Appliance Vendors</i>	2-38
Low Total Cost of Ownership	2-39
Ease of Deployment/Maintenance	2-40
Compatibility	2-40
Customer Focused	2-40

List of Figures

CHAPTER 1

Executive Summary

1-1	Network Access Control Appliance Market: Revenue Forecasts (World), 2004-2014	1-7
-----	--	-----

CHAPTER 2

World Network Access Control Technologies Markets

2-1	Network Access Control Technologies Market: Impact of Top Industry Challenges (World), 2008-2014	2-8
2-2	Network Access Control Technologies Market: Market Drivers Ranked in Order of Impact (World), 2008-2014	2-11
2-3	Network Access Control Technologies Market: Market Restraints Ranked in Order of Impact (World), 2008-2014	2-14
2-4	Network Access Control Appliance Market: Unit Shipment and Revenue Forecasts (World), 2004-2014	2-19
2-5	Network Access Control Appliance Market: Percent of Revenues by Vertical Segment and Trend (World), 2006-2007	2-21

2-6	Network Access Control Technologies Market: Competitive Structure (World), 2007	2-26
2-7	Network Access Control Technologies Market: Database of Key Industry Participants by Product Type (World), 2007	2-27
2-8	Network Access Control Appliance Market: Company Market Share by Revenues (World), 2007	2-29

List of Charts

CHAPTER 1

Executive Summary

- | | | |
|-----|--|-----|
| 1.1 | Network Access Control Technologies Market:
Full Network Access Control Cycle (World), 2007 | 1-3 |
| 1.2 | Network Access Control Technologies Market:
Intersection of Various Security Technologies (World), 2007 | 1-4 |

CHAPTER 2

World Network Access Control Technologies Markets

- | | | |
|-----|---|------|
| 2.1 | Network Access Control Technologies Market:
Market Engineering Measurements (World), 2007 | 2-6 |
| 2.2 | Network Access Control Appliance Market:
Unit Shipment and Revenue Forecasts (World), 2004-2014 | 2-19 |
| 2.3 | Network Access Control Appliance Market:
Revenue Forecasts (World), 2004-2014 | 2-20 |
| 2.4 | Network Access Control Appliance Market:
Percent of Revenues by Region (World), 2007 | 2-24 |
| 2.5 | Network Access Control Appliance Market:
Competitive Market Positioning by Product Strengths (World), 2007 | 2-28 |
| 2.6 | Network Access Control Architecture Market:
Competitive Landscape (World), 2007 | 2-30 |

2.7	Network Access Control Appliance Market: Competitive Landscape (World), 2007	2-30
2.8	Network Access Control Architecture Market: Matching Product Strengths to Target Market (World), 2007	2-37
2.9	Network Access Control Appliance Market: Matching Product Strengths to Target Market (World), 2007	2-39

I

Executive Summary

EXECUTIVE SUMMARY

Market Overview & Definitions

INTRODUCTION

In recent years, the security community has identified a shift away from attacks done as a show of hacking prowess to much more criminal activities. What used to be a show of skill is now a lucrative black market. A bot-net is a large group of compromised computers called zombie computers. This is used for spam e-mail campaigns, distributed denial-of-service attacks, click-fraud, and other such attacks. This is a problem for everyone rather than just an individual corporate network.

Malware is the traditional threat to corporate networks. The history of the NAC market can be traced to a severe outbreak of worms in the summer of 2003. These included Blaster, Welchia, Dumaru, and variations of SoBig starting with SoBig.A in January to SoBig.F (the most rampant) in August. Shortly thereafter, Cisco announced the Cisco Network Admission Control project and the expected participation of Symantec, Trend Micro, and Network Associates.

The more traditional malware, viruses and worms can cause expensive work stoppages and extensive fixes. Malware has become even more insidious with tailor-made malware, root-kits that are able to evade detection by AV software and Trojans designed to open a back-door into the system for attackers. Furthermore, many legitimate programs are not welcome on a corporate network. NAC solutions provide customers with a way to scan for and remove problematic applications. Peer-to-peer networks, instant messaging, and junk-ware form an indicative list.

Often times, it is not enough to enforce policy without technology. It is human nature to shrug off a rule and more so for users that don't understand the threat associated with that. In addition, the security perimeter is becoming much more porous with the increasing numbers of remote workers and mobile/wireless devices (smart phones, hand-devices and laptops). Most security problems come from innocent or careless users. Network access control means not just keeping malware out but controlling who gets into which resources. This has been an important consideration for organizations that are concerned about the insider threat.

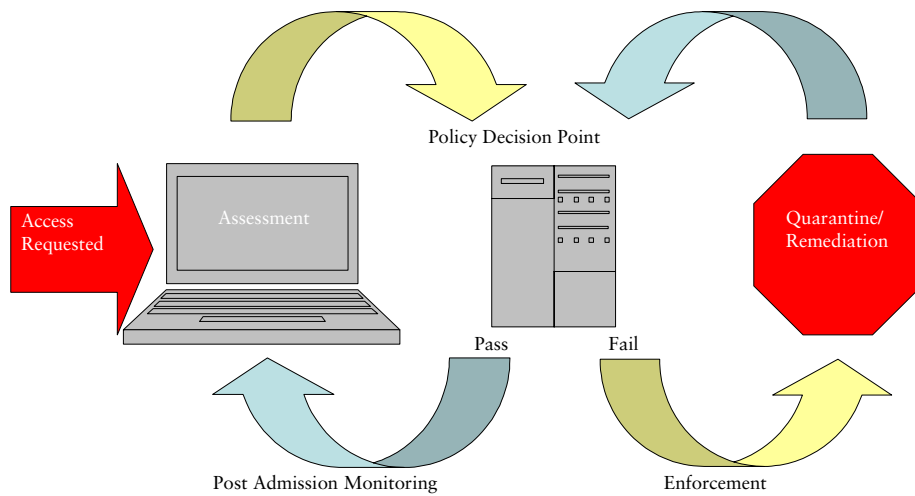
Network access control is not the cure-all for network security issues but does aim to tie together multiple endpoint security products. The umbrella term for this solution is network access control (NAC) but many vendors employ a proprietary version of NAC. Cisco has Network Admission Control, Microsoft has Network Access Protection (NAP) and many other vendors have solutions that define the acronym differently. Frost & Sullivan has chosen to adopt the definition of Network Access Control (NAC) for this research. Unless specifically noted as Cisco NAC, any reference to NAC in this study is generic and non-vendor specific.

PRODUCT DEFINED

Chart 1.1 represents key NAC elements and emphasizes the cyclical nature of a NAC solution in the World Network Access Control Technologies Market in 2007. These include pre-admission inspection and post-admission monitoring, a policy decision and enforcement point, and a method of quarantine/remediation for noncompliant machines. When a user requests access, the machine is checked and if found to be compliant then it is allowed to access the network. Post admission monitoring will ensure that the user stays compliant—entering the assessment/decision/enforcement process again periodically. If the user is found noncompliant, NAC solutions must offer a means of quarantine and remediation to bring the user into compliance. The user should then be allowed to access the network, once again under post-admission monitoring.

CHART 1.1

Network Access Control Technologies Market: Full Network Access Control Cycle (World), 2007



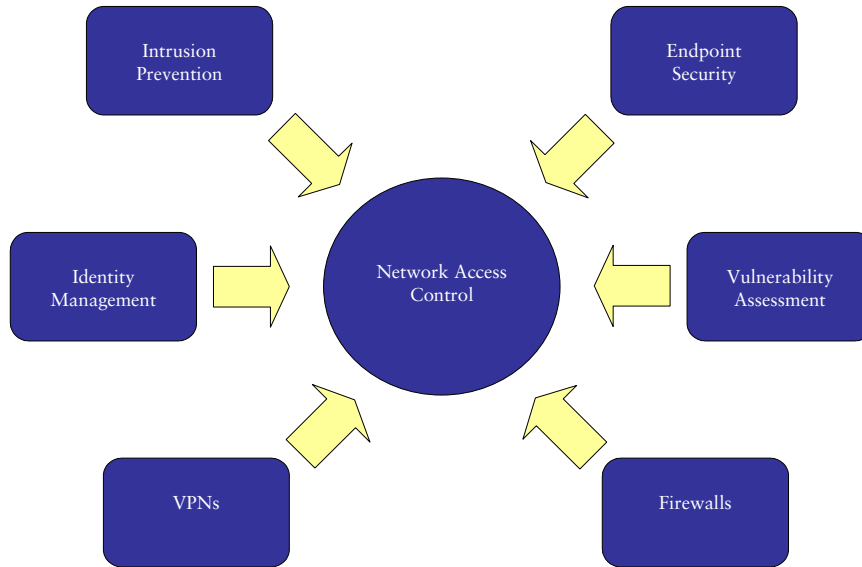
Source: Frost & Sullivan

Vendors can offer a NAC solution in either an appliance form or in an architecture approach. A NAC architecture approach involves using a number of different components—either software or network infrastructure components. This approach includes technologies such as firewalls, virtual private networks (VPN), NAC-enabled switches and routers, policy servers, directory servers and agents. Because software and hardware are often considered components of the IT infrastructure, Frost & Sullivan will refer to these as architecture-based NAC solutions in this study.

As of 2007, architecture-based NAC solutions in the World Network Access Control Technologies Market require a number of different technologies as shown in Chart 1.2. By comparison NAC appliances are single-point devices that provide full NAC functionality. These are deployed either inline or out-of-band with a clear set of advantages and disadvantages for either deployment option.

CHART 1.2

Network Access Control Technologies Market: Intersection of Various Security Technologies (World), 2007



Source: Frost & Sullivan

REVENUES DEFINED

Total revenues reflected in this chapter are derived from market participants who provided a NAC solution, as defined above, and sold their NAC solutions direct to end users or through a distribution channel. Thus, companies lacking any component of the NAC product definition were not included in the calculation of the total market units and revenues. Forecasts are for the world market, which has been subdivided into North America, Europe, Asia, and the rest of the world (ROW). Revenues represent dollars earned strictly from the sale of a NAC solution and do not include sales of related security products, as to avoid double counting.

VERTICAL MARKET SEGMENTS DEFINED

- Education
- Healthcare
- Government
- Financial Institutions
- Telecommunications/Technology
- Others: Others include construction, manufacturing, utilities, entertainment, retail, professional services and transportation

G E O G R A P H Y D E F I N E D

Geographic regions included in this research include:

- North America
- Europe: Western, Central and Eastern Europe
- Asia Pacific: Countries on the western border of the Pacific Ocean, including those of the Indo-Chinese peninsula, Pacific islands and Central Asia
- Rest-of-World: Regions not mentioned above including Central America, South America, the Middle East and Africa

Market Dynamics

M A R K E T D R I V E R S

The key drivers for the NAC market are as follows:

- Publicity of financial losses caused by network-based attacks increases demand for network security products
- Dissolution of the security perimeter due to increasing numbers of remote workers and mobile devices
- Extra functionality increases value of NAC products and creates a stronger business case
- Policy enforcement without technology proves to be ineffective
- Government and industry regulations mandating strict security practices
- NAC technology has matured to provide acceptable levels of scalability and performance
- Progression of NAC solutions improve and broaden organization's security abilities
- Customers recognize NAC services as long-term investments

MARKET RESTRAINTS

The key restraints for the NAC market are as follows:

- Costly solutions that require replacements or upgrades of major network components reflects poorly in customer cost-benefit analysis
- Lack of agreement on a single set of standards hinders uptake in larger organizations
- Many approaches to NAC creates a wide range of options for potential customers; causing confusion and complicating the sales process
- Slow adoption rates of Windows Server 2008
- Low adoption rates of NAC related technology such as 802.1X
- NAC deployments stalled by inadequate sets of organizational security policies
- Competition with other security products
- Low entry and exit barriers may allow knock-off NAC products into the market

World Network Access Control Technologies Market Forecast

Figure 1-1 represents the revenues and growth rate for the World Network Access Control Appliance Market in 2007.

FIGURE I - I

Network Access Control Appliance Market: Revenue Forecasts (World), 2004-2014

Year	Revenues (\$ Million)	Revenue Growth Rate (%)
2004	19.0	---
2005	44.7	135.3
2006	91.7	105.0
2007	114.0	24.4
2008	147.9	29.7
2009	189.7	28.3
2010	245.6	29.5
2011	310.7	26.5
2012	405.9	30.6
2013	530.2	30.6
2014	692.6	30.6

Compound Annual Growth Rate (2007-2014): 29.4%

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Summary of Major Findings

The World Network Access Control Technologies Market is poised for a CAGR of 29.4 percent from 2007 to 2014. This strong growth coincides with the release of anticipated software, maturing technology and a better understanding of network access control among potential customers. In 2007, multiple vendors left the NAC market, despite showing significant growth. On the other hand, new entrants to the market promise strong long-term growth.

Frost & Sullivan has identified the following challenges that are critical to growth in this market:

- Conveying the dollar-value of NAC solutions to potential customers
- Developing and adhering to a single standard for NAC solutions
- Creating a transparent end-user experience
- Adding value to NAC products through increased functionality

2

World Network Access Control Technologies Markets

MARKET OVERVIEW

Market Overview & Introduction

This research study will provide a quantitative and qualitative overview of the NAC market. This market includes any vendor offering a solution with complete NAC functionality. At its core, a NAC solution includes endpoint assessment, policy enforcement, and remediation capabilities. As technology improves and additional network security vendors enter the market, extra functionality has been added to the basic NAC product. This chapter will cover the multiple approaches to each facet of a NAC solution in greater detail.

The vendors covered in this study offer a NAC solution that addresses the three key components listed above, usually with multiple options for the above steps. Vendors offer either an appliance or an architecture based solution, each with its distinct advantages and disadvantages. Customers have been waiting to see what effect, if any, the release of Microsoft NAP would have on the market. This has provided valuable time for NAC appliance vendors to gain a foothold in the market.

This market has seen success in vertical markets that are not traditionally security focused. Although this has resulted in some new deployment/marketing challenges, the more important effect is that NAC solutions are compared against other security products in a more objective manner. In addition, key players have exited this market; even players that seemingly were doing well. This has prompted sensational speculation that NAC is a dying market among a few industry pundits. However the entrance of larger players into this market, such as Sophos and Novell, indicates otherwise. NAC has proven to be a key enterprise security product capable of mitigating zero-day threats, and effectively enforcing security policies. Overall, the NAC market has enjoyed healthy growth and is poised for stronger growth in 2008.

Market Definitions

PRODUCT DEFINED

To define the NAC market, Frost & Sullivan researched the popular industry opinion in order to ensure the relevance of the market study as an aid to decision-making. Reaching a consensus on the definition of a NAC product has been a key challenge in this industry primarily due to the evolving nature of technology. In 2003, Cisco announced its plans for network admission control in response to the serious malware outbreak that summer. Initially, the goal was to assess the state of the endpoint before granting or denying it access onto the network.

Over the years, the definition of NAC has gradually changed to include more features and functionality. For example, as more vendors began entering the market, post-admission monitoring became available to customers. In past years, customers had to choose between pre-admission or post-admission NAC. Now it is accepted that NAC solutions must use a combination of these solution types. The evolution of this definition has been spurred on by vendors with expertise in similar technologies that found the transition into the NAC market fairly easy. Some intrusion detection/prevention system (IDPS) vendors, for example, have added their IDPS functionality to their NAC solution to give their product a slight advantage. Similarly, behavior-based IPS, identity management, discovery, and anti-malware vendors each offer a distinct NAC product. Overall, Frost & Sullivan has identified three basic functions that all NAC solutions perform:

- An assessment/authorization method
- A policy decision and enforcement point
- A quarantine/remediation method

All the vendors covered in this study offer a NAC solution that addresses the three key components listed, usually with multiple implementation options for the above functions. Vendors can offer a NAC solution in either appliance form or as part of a framework solution, which will also be explained further in-depth.

NAC ARCHITECTURE DEFINED

Vendors can offer a NAC solution in either an appliance form or in an architecture approach. A NAC architecture approach involves using a number of different components—either software or network infrastructure components. This approach includes technologies such as firewalls, virtual private networks (VPN), NAC-enabled switches and routers, policy servers, directory servers and agents. Because software and hardware are often considered components of the IT infrastructure, Frost & Sullivan will refer to these as architecture-based NAC solutions in this study. For organizations interested in NAC there are three prominent framework solutions—Cisco Network Admission Control (NAC), Microsoft Network Access Protection (NAP) and Trusted Computing Group's Trusted Network Connect (TCG TNC).

Cisco NAC

The Cisco NAC framework approach uses the network infrastructure to ensure that devices are compliant with security policy before allowing them access to the network. Cisco NAC started as an initiative sparked by a series of worms that plagued networks in summer 2003. In addition, Cisco is the dominant vendor for the network infrastructure which has translated into a leadership position in the NAC market. These factors have given the Network Admission Control architecture a decided advantage over the others.

Cisco, not known for software development, has been partnering with software vendors to provide a means of client assessment. The interoperability with Microsoft NAP is the most prominent example of this, although there are many others. This partnership with software vendors allows Cisco to focus on their core competency.

Cisco NAC works exclusively with Cisco technology, making it the obvious NAC choice for vendors with a Cisco infrastructure. On the other hand, the Cisco NAC solution is a tough sell for organizations that would have to upgrade and replace key infrastructure components. While this is a point of criticism for Cisco, there is no doubt that narrowing the range of infrastructure components allows Cisco to ensure compatibility and performance.

Microsoft NAP

Software giant Microsoft has been advertising their policy enforcement technology for years and it is finally about to be available as part of Microsoft's newest enterprise operating system, Windows Server 2008. Success of Microsoft Server 2008 would make NAP an integral part of the software architecture.

Many potential customers, enticed by the idea of a NAP solution being included with the next generation of enterprise operating system, have been waiting for NAP to be released. Although some customers have decided to move on without NAP, many vendors have still been planning and advertising their interoperability with NAP. The release of Windows

Server 2008/NAP, regardless of its success or failure, will further spur the growth of the NAC market.

TCG TNC

Trusted Computed Group has been developing an open architecture and standards for endpoint security called Trusted Network Connect. Ensuring interoperability between NAC products and vendors will generate tremendous growth for participants and the overall NAC market. Although network hardware vendors such as Juniper have supported TNC, Cisco has been public about their non-participation. This results in a strange two-camp effect—Cisco and everyone else. Because of Cisco's extensive presence in the infrastructure, many vendors chose to partner with Cisco NAP. However, vendors that are dissatisfied with Cisco's commitment to NAC are participating in the TCG TNC. In addition, TNC has support from many software vendors as well such as Symantec and Microsoft.

Other End-to-End Solutions

The three NAC architectures mentioned above are the best known architecture based approaches to NAC. There are many other vendors that have pledged interoperability with Cisco NAC, NAP or TCG TNC, but also offer an end-to-end NAC solution of their own. Juniper, Symantec, and McAfee are among the companies interesting in the improvement of NAC technology rather than strictly their own product line. In fact, because a NAC framework solution requires a combination of hardware and software technologies, partnerships and distribution channels have been key to the development of the NAC architecture market.

NAC APPLIANCE DEFINED

The appliance-based approach to NAC offers potential customers additional options but also gives them more factors to consider. NAC functions are performed by an appliance that can sit inline or out-of-band of the network. NAC functions can also be performed on intelligent switches. Sitting inline allows an appliance to perform deeper packet inspection. While this has been considered a performance bottleneck in years past, technology has improved enough to dispel this concern. Detractors of inline appliances will point out that they are single points of failure and requiring redundant appliances effectively doubles the cost of inline appliance deployments.

Out of band appliances lack the negative connotations associated with any inline device, however it is considered a retroactive, passive approach to NAC. For customers this used to be an either-or option, however many vendors have recognized the benefits of both options. Vendors such as TippingPoint and StillSecure have recognized the demand for both solutions and offer combination deployment solutions.

The NAC appliance vendors have traditionally held a pricing advantage over the architecture approach to NAC, which has a high total cost of ownership for customers requiring infrastructure replacement or upgrades. This means that NAC appliances have a pricing advantage over NAC frameworks in smaller organizations. NAC appliances have limited scalability so larger organizations will require multiple appliances. The delay of Microsoft NAP and reluctance to make drastic infrastructure changes has made NAC appliances much more appealing to the NAC target market. In addition, even with the NAP release, NAC vendors are expected to have a strong business case with a certain customer base.

REVENUES DEFINED

Total revenues reflected in this chapter are derived from market participants who provided a NAC solution, as defined above, and sold their NAC solutions direct to end users or through a distribution channel. Thus, companies lacking any component of the NAC product definition were not included in the calculation of the total market units and revenues. Forecasts are for the world market, which has been subdivided into North America, Europe, Asia, and the rest of the world (ROW). Revenues represent dollars earned strictly from the sale of a NAC solution and do not include sales of related security products, as to avoid double counting.

Market Engineering Analysis

Chart 2.1 details the market engineering measurements for the World Network Access Control Technologies Market in 2007.

CHART 2.1

Network Access Control Technologies Market: Market Engineering Measurements (World), 2007

Market Engineering Drives Market Strategy and Planning



Measurement Name	Measurement	Trend
Market Stage	High Growth	---
Revenues (2007)	\$114.0 million	Increasing
Potential revenues (2014)	\$692.6 million	---
Base year revenue growth rate (2007)	24.4%	Decreasing
Forecast period revenue growth rate (CAGR)	29.4%	---
Units (2007)	3,629	Increasing
Potential units (2014)	18,917	---
Base year unit growth rate (2007)	18.8%	Decreasing
Forecast period unit growth rate (CAGR)	26.6%	---
Average price (appliance based solutions)	\$31,420	Increasing
Price range	\$20,000 to \$1,000,000	---
Price sensitivity	Medium	Increasing
Competitors (active market competitors in base year)	25+	Stable
Companies entering the market (2007)	3	Increasing
Companies exiting the market (2007)	3	Increasing
Degree of competition	High	Stable
Degree of technical change	High	Stable
Customer satisfaction	Medium	Increasing
Customer loyalty	Medium	Increasing
Market concentration (percent of base year market controlled by top three competitors)	59.0%	Decreasing

Note: All figures are rounded. Source: Frost & Sullivan

MARKET STAGE

The NAC market is in the high growth stage, carrying over from 2007. Many factors that have restrained the growth of the NAC market in the past have steadily been alleviated and will continue to decrease through 2008. Vendors are reporting that most customers are familiar with NAC products and the many options available to them. The release of Microsoft NAP will help undecided customers to decide on a NAC solution to deploy. Furthermore, NAC products continue expanding their capabilities, increase performance and effectiveness. These factors have resulted in strong growth in 2007 and stronger growth in 2008.

NUMBER OF COMPETITORS

In 2007 there were 25 competitors in the NAC market. Players such as Vernier and Caymas left the market or repositioned their product in spite of reporting steady growth. On the other hand, 2007 saw the entrance of Novell and Sophos into this market through acquisitions of Senforce and Endforce, respectively. This market is divided between large, diversified companies such as Cisco, Symantec, Juniper, McAfee, Sophos, and smaller, innovative, security-focused companies.

DEGREE OF TECHNICAL CHANGE

The NAC definition has expanded over the years to include functionality that vendors introduced through innovation or through background expertise in other security markets. Certain capabilities have become standard while other features vary depending on the vendor. Frost & Sullivan has seen a trend of health assessment-based NAC products that moved to intrusion prevention-based NAC. The most recent trend is vendors offering identity management-based NAC products. Vendors report that many customers like the information that this provides them.

This high degree of technical change has been a source of customer confusion but is going to be a more significant market driver now that many more customers understand the options available to them. Increased functionality adds value to the product and is more attractive to top decision makers in dollar terms.

CUSTOMER SATISFACTION

In the early stages of the NAC market customer satisfaction included failed solutions, performance problems, and difficult implementations. As the market matures there have been many third-party product evaluations as well as customer reviews. Customers now have a plethora of information at their finger tips to help them make a well-informed decision. Consequently, customers will buy the superior NAC product and revenues will better reflect the better NAC solution.

MARKET CONCENTRATION

In 2007, the top three NAC vendors accounted for 60 percent of total market revenues as compared to 75 percent in 2006. This is accounted for by the entrance of new players into this market.

MARKET DYNAMICS

Industry Challenges

Figure 2-1 presents the market challenges ranked in order of impact in the World Network Access Control Technologies Market for the period 2008-2014.

FIGURE 2-1

Network Access Control Technologies Market: Impact of Top Industry Challenges (World), 2008-2014

Challenge	1-3 Years	4-6 Years
Conveying the value of NAC to potential customers	High	High
Developing and adhering to a single standard for NAC solutions	High	High
Creating a transparent end-user experience	High	Medium
Adding value to NAC products through increased functionality	Medium	High
Providing consulting services for customers lacking security policies or experience	Medium	Medium

Source: Frost & Sullivan

CONVEYING THE VALUE OF NAC TO POTENTIAL CUSTOMERS

Potential customers are showing genuine interest in NAC, going so far as conducting cost/benefit analysis and feasibility testing. However, even customers that are prime candidates for a NAC solution are slow to move to implementation. Customers that spend a great deal of time considering a NAC solution cause a drain on sales and marketing resources. This hesitation is primarily due to a prevailing misperception of NAC technology as an exorbitant product rather than a necessary investment with clear-cut financial benefits.

NAC vendors are challenged to convey the tangible return on investment that NAC solutions provide. This is considered the triggering event for customers that are likely to invest in a NAC solution but require more motivation. There are other triggering events such as industry and government regulations or even a security breach; although this is the one trigger that NAC vendors can directly influence. Vendors that can quickly move a company from considering a NAC implementation to an actual implementation will reduce their chances of losing the sale, cut overhead costs, and speed up their revenue growth.

DEVELOPING AND ADHERING TO A SINGLE STANDARD FOR NAC SOLUTIONS

There have been three potential sets of standards for the framework approach to network access control. Cisco's Network Admission Control (CNAC), Microsoft's Network Access Protection (NAP), and Trusted Computing Group's Trusted Network Connect (TCG TNC) are the key standards that are most widely known. Issues that have been hindering the adoption of one set of standards are just about set to play themselves out in 2008. Microsoft is releasing Windows Server 2008 and its adoption rate will translate directly to the success of its NAP initiative. Even though Cisco is still the de facto standard for NAC architecture products, Cisco is also pledging more support towards their NAC appliance. Regardless of which standard(s) wins, choosing and adhering to a single standard is integral to growth in the NAC market.

CREATING A TRANSPARENT END-USER EXPERIENCE

A transparent user experience is very high on potential customers' checklists. This is a make or break factor as customers are not willing to trade productivity for security, especially in the NAC target market. Many vendors are meeting this demand by offering agentless client assessments or both dissolvable agents and pervasive agents where applicable. Overall, the assessment should not require an excessive amount of time. The best situation is when a user is unaware that any sort of assessment was conducted at all. The remediation process should also be as painless as possible. This includes clear dialogue and intuitive steps that can be completed in a timely, easy manner. This is an area in which all NAC vendors can improve on and create a distinct advantage for themselves.

ADDING VALUE TO NAC PRODUCTS THROUGH INCREASED FUNCTIONALITY

Vendors are encouraged to offer NAC products that come with bonus functionality. This increases the financial value of the product offering – which is what grabs the attention of actual decision makers. Some vendors have reported byproduct functions that were discovered by customers. Others have relied upon their expertise in other network security products to offer a unique product. NAC vendors that move beyond basic NAC functionality will not only improve their own growth rate but the overall NAC market's growth as well.

PROVIDING CONSULTING SERVICES FOR CUSTOMERS LACKING SECURITY POLICIES OR EXPERIENCE

NAC deployments are stalled by organizations that lack security policies. NAC vendors report spending some time with customers devoted to developing acceptable security policies to implement. This is a drain on resources for NAC vendors that are not planning to spend time holding their customer's hand through security basics.

Rather than count these occurrences as a loss or as an annoyance, vendors can incorporate this into their marketing strategy. Customers that are prime candidates for a NAC solution but lacking in any security expertise will embrace any vendor that caters to their needs and is willing to work with them. The ability to deliver this marketing message and services will give NAC vendors an advantage and a wider customer base.

Market Drivers

Figure 2-2 presents the market drivers ranked in order of impact in the World Network Access Control Technologies Market for the period 2008-2014.

FIGURE 2 - 2

Network Access Control Technologies Market: Market Drivers Ranked in Order of Impact (World), 2008-2014

Rank	Driver	1-2 Years	3-4 Years	5-7 Years
1	Publicity of financial losses caused by network-based attacks increases demand for network security products	High	Very High	Very High
2	Dissolution of the security perimeter due to increasing numbers of remote workers and mobile devices	High	High	High
3	Extra functionality increases the value of NAC products and creates a stronger business case	Medium-High	High	Very High
4	Policy enforcement without technology proves to be ineffective	Medium-High	Medium-High	Medium-High
5	Government and industry regulations mandating strict security practices	Medium-High	Medium-High	Medium
6	NAC technology has matured to provide acceptable levels of scalability and performance	Medium	Medium-High	High
7	Progression of NAC solutions improve and broaden organization's security abilities	Medium	Medium	Medium-High
8	Customers recognize NAC services as long-term investments	Low-Medium	Medium	Medium-High

Source: Frost & Sullivan

PUBLICITY OF FINANCIAL LOSSES CAUSED BY NETWORK-BASED ATTACKS INCREASES DEMAND FOR NETWORK SECURITY PRODUCTS

There have been a number of well-publicized security breaches over the years which have increased the overall demand for network security products. Major malware outbreaks have highlighted the importance of protecting the network from vulnerable or infected machines. In addition, the Computer Security Institute (CSI)/FBI Survey has drawn due attention to the insider threat and has computed a tangible number of dollars in financial losses caused by network-based attacks. This is the statistic that gets the attention of decision makers. The media's sensational coverage of network security breaches highlights key problems for which NAC solutions are well suited.

DISSOLUTION OF THE SECURITY PERIMETER DUE TO INCREASING NUMBERS OF REMOTE WORKERS AND MOBILE DEVICES

An increasing number of companies are embracing the idea of remote employees and contractors. As a result, laptops and smart mobile devices are becoming more prevalent throughout the enterprise. These devices are essentially weak links in the network's security perimeter. Laptops can be off the network for extended periods of time and come back out of compliance. Smart phones and other mobile devices form another point of entry into the network. Whether intentionally, or not, insiders pose the most serious threat to an organization's sensitive data and crucial systems. As long as companies have remote employees, contractors, or guests on their networks, they will need a way to control who accesses what on their network.

EXTRA FUNCTIONALITY INCREASES THE VALUE OF NAC PRODUCTS AND CREATES A STRONGER BUSINESS CASE

Combining extra security functions into a NAC solution provides a stronger business case for organizations that are considering a NAC solution. A number of vendors in this market are already selling NAC solutions with value-adding security features. An interesting example is Bradford Networks, whose customers report being able to use the assessment agent for emergency broadcast purposes. With campus violence already a rampant problem, this is a feature which could easily be sold as a stand-alone product.

POLICY ENFORCEMENT WITHOUT TECHNOLOGY PROVES TO BE INEFFECTIVE

For the most part, the "insider threat" consists of unintentional transgressions. Because of simple human nature, rarely is it enough to simply establish a policy and expect everyone to follow it. In fact, malware has only become more insidious in recent years from rootkits—capable of avoiding detection by anti-virus products—to web sites requiring minimal user interaction to download malicious files, known as drive-by malware. In addition, it only takes one rogue machine to compromise a network.

Worse still, recent studies such as those published by the CSI/FBI Survey shows that network-based attacks, including insider attacks, are increasingly criminal based. As organizations strive to find a balance between adequate security and adequate availability, NAC vendors with fine-grained authorization capabilities have struck a chord with a wide range of customers.

GOVERNMENT AND INDUSTRY REGULATIONS MANDATING STRICT SECURITY PRACTICES

Government legislation and industry regulations, i.e. the Payment Card Industry (PCI) Data Security Standard and the Health Insurance Portability and Accountability Act (HIPAA), are prompting an increased interest in the overall network security market. This has an interesting effect – organizations that haven't typically been a strong target market for network security vendors are now interested in NAC. This puts NAC on the same level as other network security solutions. With the traditional network security customers, NAC has often taken a back seat to other security products such as intrusion detection/prevention systems, content filtering solutions or vulnerability scanners. This is driving growth in the overall network security market and is trickling down to the NAC market as well.

NAC TECHNOLOGY HAS MATURED TO PROVIDE ACCEPTABLE LEVELS OF SCALABILITY AND PERFORMANCE

In previous years, a valid criticism of NAC technology was that it was not up to par in terms of scalability and performance. NAC solutions were difficult to implement across large networks, requiring several boxes at strategic points in the network. Inline devices have always been branded as a bottleneck or a single point of failure. While some vendors build their own hardware with custom designed silicon, others have partnered with OEMs to provide enhanced performance for NAC customers. In addition, multiple vendors have started offering a choice of inline or out-of-band solutions in order to meet customer needs. There are even a few hybrid products with the benefits of both implementations rolled into one box. As NAC technology improves in scalability, potential customers will find NAC to be a more attractive solution.

PROGRESSION OF NAC SOLUTIONS IMPROVE AND BROADEN ORGANIZATION'S SECURITY ABILITIES

The definition of NAC is evolving to include a wide array of security services, which makes this technology much more valuable. For example, NAC was originally meant to check endpoints for proper levels of security and up-to-date security before admitting it onto the network. Post-admission monitoring was the logical next step and NAC vendors were either pre or post admission based. Today, both pre-admission inspections and post-admission monitoring are fairly standard capabilities of NAC solutions as well as patch management and user profiling. Depending on the vendor, NAC can also include fine-grained identity management, intrusion detection/prevention, and even network discovery capabilities. As these capabilities become standard, customers will show increased interest in NAC.

CUSTOMERS RECOGNIZE NAC SERVICES AS LONG-TERM INVESTMENTS

Vendors that offer NAC services as part of a framework approach have the clear advantage of selling a product that is complimentary to the existing IT infrastructure. Selling NAC as a forklift upgrade or infrastructure overhaul has been a difficult proposition for potential customers. Instead, marketing campaigns should focus on positioning their NAC solution as the next step in the natural evolution of network infrastructure. As a long-term investment, customers will be better able to recognize the value of implementing a NAC solution.

Market Restraints

Figure 2-3 presents the market restraints ranked in order of impact in the World Network Access Control Technologies Market for the period 2008-2014.

FIGURE 2-3

Network Access Control Technologies Market: Market Restraints Ranked in Order of Impact (World), 2008-2014

Rank	Restraint	1-2 Years	3-4 Years	5-7 Years
1	Costly solutions that require replacements or upgrades of major network components reflects poorly in customer cost-benefit analysis	High	Medium-High	Medium-High
2	Lack of agreement on a single set of standards hinders uptake in larger organizations	Medium-High	Medium-High	Low
3	Many approaches to NAC creates a wide range of options for potential customers; causing confusion and complicating the sales process	Medium-High	Medium	Medium
4	Slow adoption rates of Windows Server 2008	Medium-High	Low-Medium	Very Low
5	Low adoption rates of NAC related technology such as 802.1X	Medium-High	Medium	Low-Medium
6	NAC deployments stalled by inadequate sets of organizational security policies	Medium	Medium-High	Medium
7	Competition with other security products	Medium	Low-Medium	Low
8	Low entry and exit barriers may allow knock-off NAC products into the market	Very Low	Medium	Very Low

Source: Frost & Sullivan

COSTLY SOLUTIONS THAT REQUIRE REPLACEMENTS OR
UPGRADES OF MAJOR NETWORK COMPONENTS REFLECTS
POORLY IN CUSTOMER COST-BENEFIT ANALYSIS

The media and marketing campaigns do a good job of stressing the need for controlling network access control as well as conveying the consequences of inadequate network protection. The impact of malware outbreaks and DDOS attacks are readily interpreted by tech-savvy users, however the top decision makers require a numeric value attached to these attacks before they can decide. On the low end of the scale, an organization will have to purchase at least a couple of inline or out-of-band appliances. Vendors that offer architecture based NAC solutions will have a more difficult time showing that the benefits their product provides outweigh the costs. Propositions that include fork-lift upgrades without demonstrating clear return on investment have left potential NAC customers believing that all NAC solutions are unaffordable.

LACK OF AGREEMENT ON A SINGLE SET OF STANDARDS
HINDERS UPTAKE IN LARGER ORGANIZATIONS

The lack of a single set of standards has been, and is likely to stay the primary restraint on the NAC market's growth. Customers are hesitant to implement a solution if it will potentially become discontinued. Cisco NAC has the most traction so far owing to Cisco's prevalence in the information technology infrastructure. Microsoft's dominance in the software market has many customers waiting to see the impact that NAP will have on the NAC market. TCG TNC is the other major set of standards that is vying to be the set of NAC standards. Most vendors offering a NAC solution that requires multiple components or software implementations are planning to interoperate with one or more of these standards. A single set of standards would help move customers from considering a NAC implementation to deploying a NAC solution.

MANY APPROACHES TO NAC CREATES A WIDE RANGE OF
OPTIONS FOR POTENTIAL CUSTOMERS; CAUSING CONFUSION
AND COMPLICATING THE SALES PROCESS

Many of the old arguments such as out-of-band/inline appliances or agent/agentless assessments are over, with many vendors choosing one approach or the other or even combinations. While patch management and post-admission monitoring are now considered fairly standard NAC capabilities there are many vendors offering a wide range of additional features that seem to vary from vendor. This makes the search for a NAC product very difficult for customers. Theoretically this could allow the customer to find the solution that meets their exact needs. Practically though, it is very difficult to review the 25+ players in this market before making a decision. Customers that view these options from a half-empty perspective will consider this a lack of features rather than as a NAC solution with bonus functionality.

SLOW ADOPTION RATES OF WINDOWS SERVER 2008

Microsoft NAP is being released as a feature of Windows Server 2008. Microsoft's Longhorn project was announced in 2004 and was due to be released as far back as 2006. By 2007 the only thing released was the name, Windows Server 2008. This operating system shares the same code base as Windows Vista, which has not been warmly embraced among desktop operating systems. It will be interesting to follow how well Windows Server 2008 is received by enterprise level organizations because of the direct relationship it will share with Microsoft NAP.

Many organizations have been reluctant to commit to a set of standards before there was a clear winner. Although the release of Windows Server 2008 seems like the deciding factor in this contest, only the two least likely results will help to alleviate this market restraint: the widespread success of Windows Server 2008/NAP or the catastrophic failure of Windows Server 2008/NAP.

LOW ADOPTION RATES OF NAC RELATED TECHNOLOGY SUCH AS 802.1X

Customers have long been known to shy away from network technologies that are excessively difficult to implement. 802.1X, a protocol that is necessary for port-based NAC, is very effective but has been reported by many sources to be complicated to implement. In addition, there is lack of consensus on a standard 802.1X supplicant. This is a critical component for vendors that have an out of band appliance or an architecture approach to NAC. Another similar factor is the cost of switches and other network components that must be replaced as part of a NAC implementation. Until NAC vendors can successfully address price, compatibility, and ease of deployment issues, this will continue to be a checkmark in the "Cons" box for potential customers.

NAC DEPLOYMENTS STALLED BY INADEQUATE SETS OF ORGANIZATIONAL SECURITY POLICIES

The NAC market is seeing traction in vertical markets which are not considered the norm for a network security product. Nontraditional customers are not security focused and often lack organization-wide security policies. NAC vendors have reported the need to hold customer's hands through even the basic procedures of developing a set of security policies. This is critical to the deployment of NAC and customers lacking these basics will drag out the deployment process. This is a drain on the vendor's resources that is rarely seen in other security market.

COMPETITION WITH OTHER SECURITY PRODUCTS

Potential customers that are interested in network security products usually have a very specific and limited spending budget. NAC must compete with a wide range of security technologies such as anti-malware, firewalls, IDPS, vulnerability scanners and many others. In previous years NAC products have been edged out; especially by the more established security products. While this was a serious restraint in years past, it will have an increasingly diminished effect on the NAC market. The high rate of growth in this market compared to other security products indicates that this is already becoming a non-factor.

LOW ENTRY AND EXIT BARRIERS MAY ALLOW KNOCK-OFF NAC PRODUCTS INTO THE MARKET

There are many network security products that translate easily into NAC products. On occasion, these products sometimes do not perform as well as NAC focused products. NAC vendors are encouraged to use their expertise in other security areas to add value to their NAC solution or even develop a unique product. Companies that tack on NAC functionality to an existing product will—at the very least—introduce a lower quality product into the market. Any company that releases low quality NAC products onto the market can just as easily exit the market and leave behind a bad taste in customers' mouths.

Partnerships

Due to the broad, expanding NAC definition, partnerships have been an essential strategic element for vendors. Most vendors have partnered with big market players Microsoft or Cisco. Interoperating with Cisco is considered of very high importance because of the Cisco-only infrastructure needed to implement Cisco NAC. Microsoft NAP has also garnered much support as it is included free with the next generation of Microsoft's enterprise level operating system. Vendors that are not content with Cisco's support of its NAC framework have decided to interoperate with TCG TNC. While Microsoft NAP will interoperate with both Cisco NAC and TCG TNC, Cisco has made clear its intentions to not operate with TCG TNC. The TNC has fared well in spite of lacking support from the largest infrastructure vendor in the market. NAC vendors support at least one of these three NAC architectures. Most vendors support either Cisco NAC and Microsoft NAP, or TCG TNC and Microsoft NAP—with a few supporting all three.

NAC vendors, i.e. Mirage Networks, have reported mutually beneficial relationships with managed security service providers (MSSP) such as IBM Internet Security Systems. Other partnerships have been crucial for vendors that realize that their NAC solution is lacking a component that they lack specialty in. Symantec—known for its software solutions—partners with OEMs to provide capabilities that are not its primary focus. The Symantec solution gives customers the option of choosing whether they want to use a plug-in or an appliance for policy enforcement. Strategic partnerships and distribution channels will improve a NAC vendor's growth.

REVENUE & UNIT SHIPMENT FORECASTS

World Network Access Control Appliance Market Forecasts

In 2007, the World Network Access Control Appliance Market generated \$114 million from sales of 3,629 NAC deployments. Despite the exit of larger NAC appliance vendors, the NAC market still experienced a strong 24.4 percent growth rate in 2007. Large market entrants and stronger acceptance among customers is expected to drive growth in the NAC market. This market is expected to generate \$692.6 million by 2014 and enjoy a CAGR of 29.4 percent over the forecast period.

Figure 2-4 and Chart 2.2 represent unit shipment and revenue forecasts for the World Network Access Control Appliance Market for the period 2004-2014.

FIGURE 2 - 4

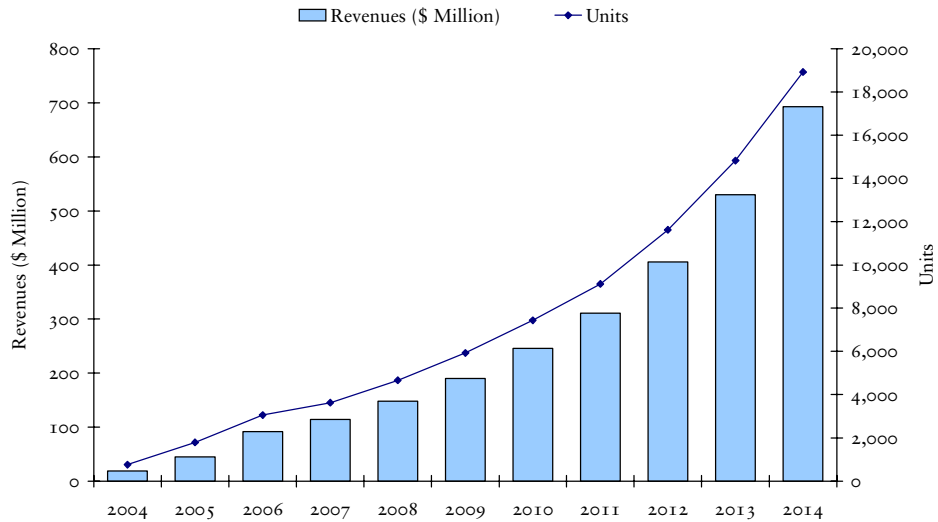
Network Access Control Appliance Market: Unit Shipment and Revenue Forecasts (World), 2004-2014

Year	Unit		Revenue	
	Units	Growth Rate (%)	Revenues (\$ Million)	Growth Rate (%)
2004	760	---	19.0	---
2005	1,788	135.3	44.7	135.3
2006	3,055	70.9	91.7	105.0
2007	3,629	18.8	114.0	24.4
2008	4,663	28.5	147.9	29.7
2009	5,928	27.1	189.7	28.3
2010	7,435	25.4	245.6	29.5
2011	9,113	22.6	310.7	26.5
2012	11,625	27.6	405.9	30.6
2013	14,829	27.6	530.2	30.6
2014	18,917	27.6	692.6	30.6
Compound Annual Growth Rate (2007-2014):		26.6%		29.4%

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

CHART 2 . 2

Network Access Control Appliance Market: Unit Shipment and Revenue Forecasts (World), 2004-2014

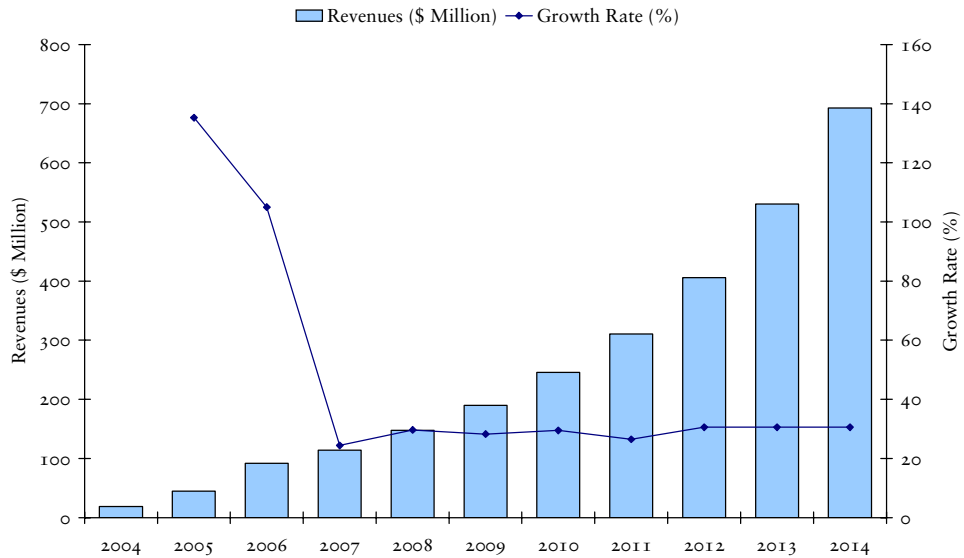


Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Chart 2.3 shows revenue forecasts for the World Network Access Control Appliance Market for the period 2004-2014.

CHART 2.3

Network Access Control Appliance Market: Revenue Forecasts (World), 2004-2014



Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

VERTICAL MARKET ANALYSIS

Overview

Initial adopters of NAC solutions have been organizations with pressing needs that NAC solutions perfectly address. Organizations with remote users and many unmanaged resources are prime examples of the NAC target market. This has resulted in the NAC market gaining traction in untraditional security market verticals such as education and healthcare. Many vendors are reporting more significant adoption rates in other vertical markets such as financial services, government, and even utilities. This is a sign that NAC is now being viewed as an integral security component rather than a secondary security feature. These market verticals represent untapped potential sales and penetrating them is important for the overall growth of the NAC market.

It should be noted that organizational size is an important adoption rate factor as well. NAC appliances have a definite price advantage over the NAC architecture in smaller organizations. This price advantage is nullified by scalability issues that require larger organizations to purchase multiple appliances.

Figure 2-5 illustrates the revenues and revenue trends for the World Network Access Control Appliance Market by vertical market segment for 2006 and 2007.

FIGURE 2 - 5

Network Access Control Appliance Market: Percent of Revenues by Vertical Segment and Trend (World), 2006-2007

Vertical Market	2006 (%)	2007 (%)	07/06 Trend
Education	45	41	Decreasing
Government	11	14	Increasing
Healthcare	9	11	Increasing
Financials	5	13	Increasing
Telecommunication/Technology	9	7	Decreasing
Others	21	14	Decreasing
TOTAL	100	100	

Note: Others include construction, manufacturing, utilities, entertainment, retail, professional services and transportation.

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Education

The NAC market has consistently seen the most support in the education vertical market. This interest has been fueled by the high number of unmanaged resources that require access to the network. Higher education institutions generally have the problems that NAC was designed to remedy. University networks represent a revolving door with the user base in a constant state of flux. Users and laptops may be on and off the network quite frequently or for months at a time. NAC's appeal also comes in the form of not only being able to control who gets on the network but also what they have access to.

Market leader Cisco has been a big player in the education vertical, which is part of the reason why education is such a strong vertical for the NAC market. Bradford is a NAC focused company that has rooted itself into the education market. Although educational institutions typically have stricter IT budgets, NAC is expected to experience a great deal of traction in this vertical.

Government

NAC vendors are reporting increased penetration in state and local governments. This customer base has many of the needs that NAC products were designed to address. The high number of remote users, varied levels of access required, and frequent guest users are all factors that are driving growth in this market.

Growth in this market is driven by laws passed by related branches of the government. While governments are usually considered bureaucratic and lethargic, securing critical network infrastructure and sensitive data has been a very high priority. Combined with healthy spending budgets, the government vertical will be important for the network security industry. This growth is expected to trickle down to the NAC market.

Healthcare

Healthcare is another strong vertical in which the NAC market has strong traction. Like education, healthcare is not a typically strong vertical for network security products. As technology plays a more crucial role in hospitals and other healthcare establishments, many organizations are still becoming familiar with network security practices. This effectively levels the playing field between NAC and better established security products. On the other hand, a customer base that is not familiar with security policies presents a number of deployment challenges. Some deployments are stalled by organizations that lack a set of security policies and require additional guidance through the implementation process. This challenge is expected to taper off as organizations become more comfortable with security practices.

Financial Institutions

The NAC market has seen more significant traction in the financial vertical in 2006. Customers in the financial market are more familiar with security products and are consequently quite sure about what features and implementations options they want. For example, vendors have reported difficulty when trying to sell an agent based NAC solution. Vendors that offer agentless NAC or at least a combination are reporting better adoption rates than in previous years.

In addition, these customers can be biased towards solutions that they are more familiar with. Competing with IDS/IPS, vulnerability assessment, and better established security products in the past has limited adoption in this vertical market. NAC vendors are expected to further penetrate this market as NAC technology receives recognition as a core security product.

Telecommunications & Technology

NAC vendors have reported some success with some high tech customers. Telecommunications vendors have also shown general interest in NAC technology. This market vertical is unrestrained by most of the factors that affect other companies because of the tech-savvy customer base. This customer base is well informed and understands the various options available to them. These customers are also willing to adopt new technologies and very adept at implementing them. Moreover, technology and telecommunications companies have a large amount of remote workers and invaluable intellectual property. This vertical market will be one of the most important for the NAC market.

Utilities

Utility organizations are usually a late adopter of new technologies, but have taken more interest in security due to the increased threats of terrorism. While utilities have generally done a good job of protecting physical assets, successful hacking demonstrations have been widely publicized and generated more interest in network security. This has trickled down through the network security market to the NAC market as reported by multiple NAC vendors. In addition, NAC solutions are a nice fit for the problems faced by the utility networks.

Others

The others category consists of manufacturing, transportation and other less technology-oriented organizations. Because technology is not as important to these organizations they have not accounted for a very significant share of the revenues in the total NAC market. While these organizations will eventually show interest in network security practices, they will not constitute a viable target market for years. Only legislation mandating stricter security practices or a successful attack on these systems will cause any growth in this market.

Two NAC vendors have reported big deals with entertainment organizations. There is significant potential for growth in this vertical market as leaked or pirated intellectual property results in serious losses for entertainment companies. A NAC solution would have a strong business case among this audience.

GEOGRAPHIC MARKET ANALYSIS

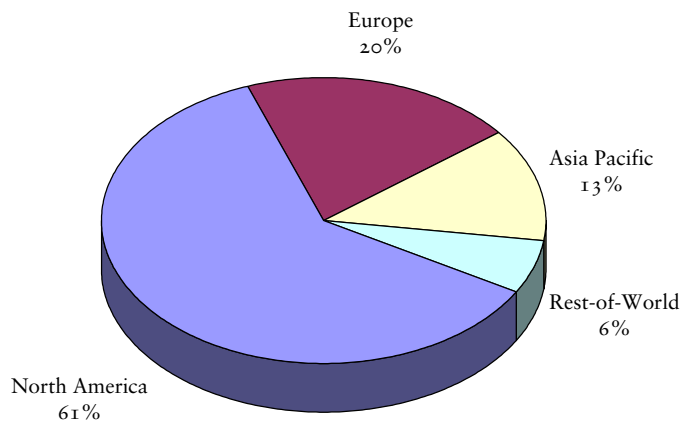
Overview

The NAC market is starting to see greater adoption rates worldwide. This is due to a number of reasons but a common factor is the entrance of newer market players that are based outside of the U.S. or have some international presence. Frost & Sullivan has identified four regions that have demonstrated in which NAC vendors have been reporting success.

Chart 2.4 illustrates the revenues for the World Network Access Control Appliance Market by geographic region in 2007.

CHART 2.4

Network Access Control Appliance Market: Percent of Revenues by Region (World), 2007



Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

North America

The United States has long been the focal point for the NAC market as many American companies have shown interest. This geographic region is the strongest contributor to the overall NAC market and consequently this region is the most competitive. North America is expected to stay the main stage for the NAC market over the long term.

Europe

Many European organizations are showing interest in NAC for some of the same reasons that their American counterparts are. Most significantly, the threat of terrorist attacks is much more significant in this region. This is driving NAC adoption rates, particularly in utilities, transportation, government organizations and other critical systems.

Asia-Pacific

Expansion into East Asian and Southeast Asian countries has been slow due to the lack of presence in these countries. Larger, more diversified vendors, such as Cisco and Checkpoint, are reporting traction in these regions simply because they are more familiar to customers in this region. In addition, resellers are primarily responsible for the expansion into this region meaning that vendors with strong distribution channels are more heavily favored. Mirage Networks, for example, has reported success in Japan as far back as 2004.

Rest-of-World

The rest of the world is a very broad category but is basically comprised of countries that are either less economically developed, technologically advanced, or security focused. Globalization and the natural economic development have produced some noticeable exceptions though. Vendors that report growth into Africa and South America are instant market leaders for those areas and should focus on securing their foothold. It should be noted that none of the companies interviewed mentioned any sales in Russia. This is alarming considering the statistics that show the percentage of mal-ware and zombie machines originating in Russia.

COMPETITIVE ANALYSIS

Overview

Figure 2-6 shows the key metrics of the competitive structure of the World Network Access Control Technologies Market in 2007.

FIGURE 2 - 6

Network Access Control Technologies Market: Competitive Structure (World), 2007

Number of Companies in the Market	Over 25
Types of Competitors	Large multinational hardware & software vendors Network security vendors Pure play NAC vendors
Distribution Structure	Direct OEM and reseller relationships as aids to increasing vertical market penetration and international presence
Tiers of Competition	Tier I: Cisco is the market leader in both the appliance and architecture iterations of its NAC solution. Juniper Networks and Symantec have leveraged their experience and presence in other markets to penetrate the NAC market Tier II: ForeScout, Mirage Networks and Still Secure have shown significant growth. Nortel and McAfee have also used their expertise in other markets to gain traction in the NAC market Tier III: Others holding 26 percent of the market
Notable Acquisitions, Mergers	Novell acquired Senforce Sophos acquired ENDFORCE
Key End-User Groups	Large scale network operations Large education, enterprise, government, financial and healthcare organizations Medium enterprises
Competitive Factors	Assessment/authorization methodologies Enforcement/remediation methodologies Standards compatibility Price Ease of deployment/deployment options Performance Ease of use/maintenance

Source: Frost & Sullivan

Since its birth in late 2003, the NAC market has shown a tremendous growth rate through 2006. The market currently consists of pure-play NAC vendors, network security companies, and larger technology companies with broad product lines. The NAC market experienced a small shake-out in 2007 with surprising market exits by unexpected vendors. However, new market entrances hold significant promise for growth and innovation in this market.

Product Analysis

NAC vendors offer either an appliance based NAC solution or an architecture based solution with very distinct advantages to each type of solution. Figure 2-7 represents the type of product offered by each vendor in the World Network Access Control Technologies Market in 2007.

FIGURE 2 - 7

Network Access Control Technologies Market: Database of Key Industry Participants by Product Type (World), 2007

Company	Architecture	Appliance
Apere		■
Bradford Networks		■
Check Point Software Technologies, Ltd.	■	
Cisco Systems, Inc.	■	■
ConSentry		■
Elemental Cyber Security	■	
ForeScout		■
Identity Engines		■
InfoExpress		■
Insightix	■	
Juniper Networks	■	
Lockdown Networks		■
McAfee	■	
Mirage Networks		■
NeoAccel		■
Nevis Networks		■
Nortel Networks	■	
Novell	■	
StillSecure		■
Sophos	■	

FIGURE 2 - 7

Network Access Control Technologies Market: Database of Key Industry Participants by Product Type (World), 2007

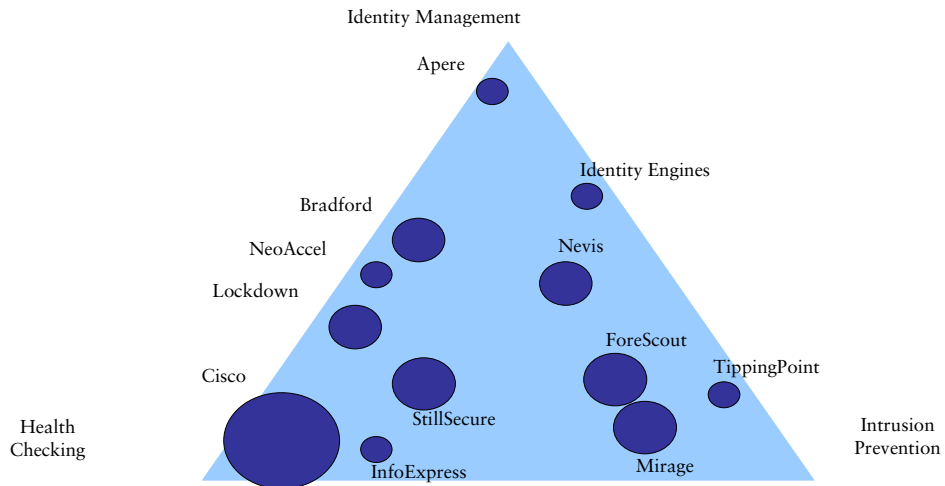
Company	Architecture	Appliance
Symantec	■	
TippingPoint		■
Trend Micro	■	
Trusted Network Technologies		■

Source: Frost & Sullivan

Vendors each bring a distinctive approach to their NAC solution. Primarily, there are three approaches that NAC appliances fall into with vendors showing strengths in each segment. These categories are: health/endpoint checking, intrusion prevention, and identity management. Most vendors in the NAC appliance market have some expertise in two or more of these categories. Chart 2.5 represents Competitive Market Positioning by Product Strengths.

CHART 2 . 5

Network Access Control Appliance Market: Competitive Market Positioning by Product Strengths (World), 2007



Source: Frost & Sullivan

Market Share Analysis

Figure 2-8 lists the market share of the leading vendors in the World Network Access Control Appliance Market. Lockdown and Vernier, who are both recently exited the NAC market, combined for a total of 9 percent market share in 2007. The departure of these companies and Caymas in 2007 will cause the size of the overall NAC market to dip slightly in 2008 before demonstrating the growth anticipated.

FIGURE 2 - 8

Network Access Control Appliance Market: Company Market Share by Revenues (World), 2007

Company	2007 (%)
Cisco	39
ForeScout	11
Mirage Networks	9
ConSentry	9
StillSecure	6
Others	26
TOTAL	100

Note: Others include Apere, Bradford Networks, Elemental Cyber Security, Identity Engines, InfoExpress, Lockdown Networks, NeoAccel, Nevis Networks, TippingPoint, Vernier.

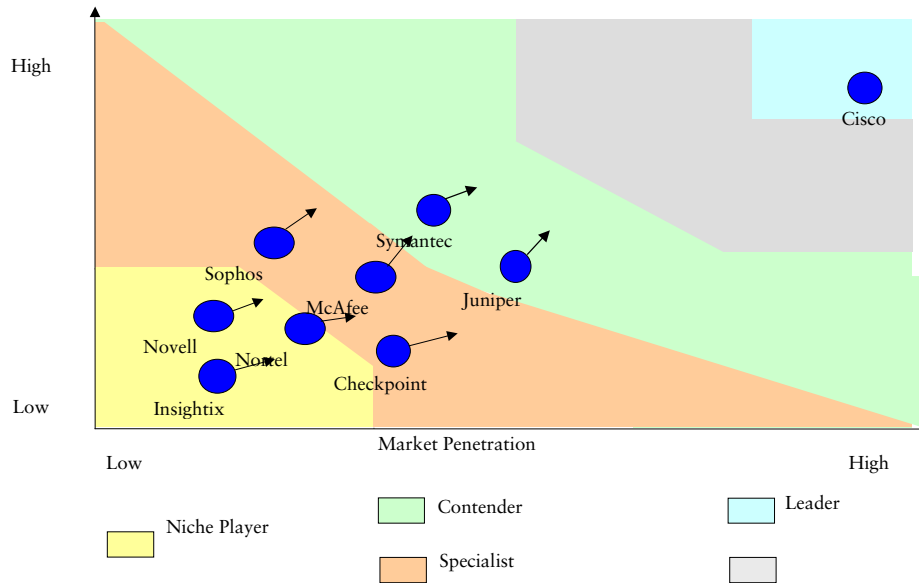
Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Competitive Landscape

Chart 2.6 represents the competitive landscape for the World Network Access Control Architecture Market in 2007.

CHART 2.6

Network Access Control Architecture Market: Competitive Landscape (World), 2007

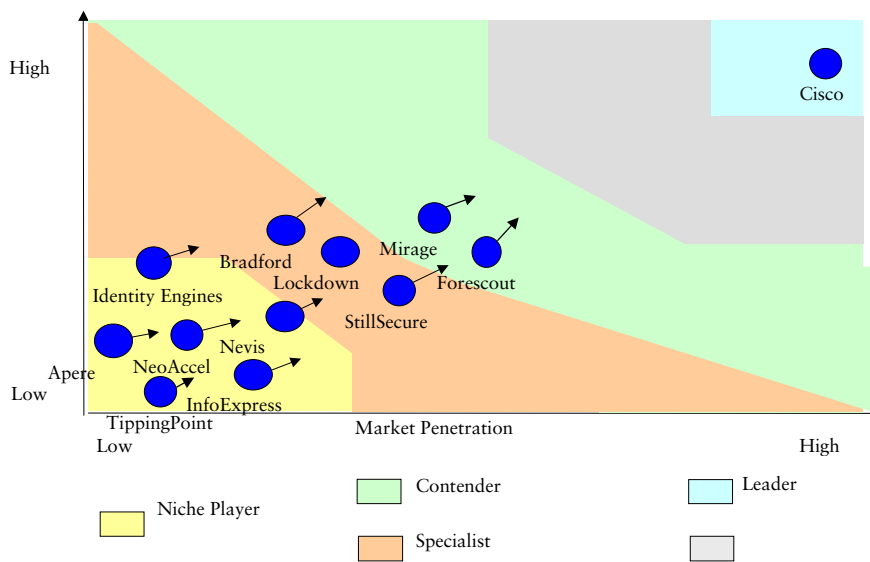


Source: Frost & Sullivan

Chart 2.7 represents the competitive landscape for the World Network Access Control Appliance Market in 2007.

CHART 2.7

Network Access Control Appliance Market: Competitive Landscape (World), 2007



Source: Frost & Sullivan

Market Leader

CISCO SYSTEMS, INC.

Cisco offers a Network Admission Control framework that is a combination of Cisco routers and switches. As the leading network infrastructure vendor, Cisco is the inherent leader in the NAC infrastructure market as well. Competition in the NAC architecture market is a slightly more significant threat as it is comprised of large network equipment vendors or large software vendors. Regardless, Cisco has been able to hold its dominant spot with its NAC solution and many NAC vendors are pledging interoperability with this architecture.

Cisco also dominates the NAC appliance market with its Cisco NAC Appliance 4.1, formerly known as Clean Access, which it gained through acquiring Perfigo in 2004. This appliance interoperates with Cisco infrastructure and NAC architecture to provide immediate NAC functionality. This has proven to be a key decision as selling NAC architecture as a forklift network overall solution has been difficult and many organizations have been slowly upgrading their infrastructure to Cisco's NAC solution. Thus, Cisco NAC Appliance 4.1 can be a strong stand-alone product or an immediate NAC solution for organizations working on their NAC architecture. Although Cisco's market leadership position is not threatened, the smaller appliance vendors are looking to cut into Cisco's market share.

Market Contenders

FORESCOUT

ForeScout's CounterACT appliance is a clientless NAC solution that sits out of band. This combines to create a transparent end-user experience while alleviating the IT staff of worries about network performance issues. In addition, this solution is completely software and infrastructure vendor agnostic and reportedly easy to deploy, with some deployments taking only an hour or less. ForeScout offers multiple enforcement options and even offers a scripting engine for customers that wish to customize their remediation techniques. Furthermore, ForeScout offers 5 different iterations of their CounterACT appliance in order to best fit customer's needs and budgets. In 2007, ForeScout experienced incredible growth and will be focusing more intently on their NAC solution going forward.

MIRAGE NETWORKS

Mirage Networks offers a distinctive NAC solution and considers behavior-based threat prevention an important part of a full-cycle NAC solution. The Mirage NAC appliance sits out-of-band, thus avoiding the problems associated with an inline appliance. This NAC solution is truly agentless and offers automated policy enforcement—ensuring that end-users have a transparent experience. Furthermore, Mirage employs a distinctive approach that modifies the host's ARP cache to appropriately control traffic.

Mirage has built several strategic relationships that have been crucial to its strong growth in 2007. Partnerships with MSSPs such as IBM ISS and AT&T, along with other distribution channels have propelled Mirage Networks' growth in North America and abroad.

SYMANTEC

Symantec acquired Sygate in 2005 and has used its knowledge of a wide range of security products to develop Symantec Network Access Control (SNAC) 11.0. SNAC is a comprehensive and complete NAC solution designed to integrate with Symantec Endpoint Protection 11.0. Symantec offers flexible deployments with options for 802.1X enforcement, gateway enforcement, or DHCP enforcement using a plug-in or an appliance. Assessments and authorizations are done with a dissolvable agent and SNAC is centrally managed through an intuitive web-based application. The many options available for each key NAC function make Symantec's NAC a solid solution.

JUNIPER NETWORKS

Juniper Networks Unified Access Control (UAC) is an architecture-based approach to NAC that includes routers, any 802.1X enabled wireless access point and switch (such as Juniper EX-series switches), Juniper firewalls, wireless controllers, and other network infrastructure. At the heart of this solution is Juniper's policy server, the Infranet Controller. This hardened infrastructure solution offers customers a comprehensive security overlay for their entire network. In addition, as part of the network infrastructure, this standards-based, vendor-agnostic solution works in heterogeneous network environments, and scales in direct relationship to the growth of the overall network. Juniper's UAC has fared well in spite of direct competition with several other leading NAC vendors.

Market Specialists

BRADFORD NETWORKS

Bradford uses role-based access control to give its customers the tightest control possible. The Bradford NAC solution is a non-obtrusive out of band appliance. This effectively cuts the need for redundant devices and eliminates worries of a negative impact on network performance. Furthermore, the Bradford solution interoperates with a wide range of software and infrastructure products.

NAC is known for its success in the education market but flexibility is important as NAC gains traction in other markets. Bradford, which is best known for its success in the education vertical market, has demonstrated this flexibility with some early successes in penetrating other vertical markets.

LOCKDOWN NETWORKS

Despite having reported steady growth and boasting a strong product with a comprehensive breadth of options, Lockdown Networks will be exiting the market on March 18, 2008. This departure is taken into account in Frost & Sullivan forecasts.

STILL SECURE

The StillSecure NAC solution is the SafeAccess appliance that does pre-connect inspections and post-connect monitoring. Safe Access uses role-based access control and allows administrators to define their own set of roles. The Safe Access appliance provides inline enforcement or out-of-band enforcement using 802.1X enabled switches or a DHCP server. StillSecure has leveraged OEM relationships with large network equipment vendors resulting in steady growth and a strong position in the NAC market. Combining IDS/IPS technology, vulnerability management and NAC has a strong value proposition with customers, and the combination of technologies and products that StillSecure sells should continue to help their market position.

McAFEE

The McAfee NAC solution is designed to integrate with other McAfee solutions and snaps into McAfee ePolicy Orchestrator (ePO) for ease of deployment and management. McAfee NAC uses an agent for both assessment and a degree of enforcement. McAfee NAC also interoperates with VPN vendors for customers that wish to use switches and VLANs for enforcement. Because ePO controls McAfee's line of anti-malware and host intrusion prevention applications, the McAfee NAC solution is an obvious choice for organizations that use McAfee products and represents a strong business case to potential McAfee customers.

Niche Players

NEVIS NETWORKS

Nevis Networks is a company focused entirely on LAN security. The Nevis family of LAN security products includes the LANenforcer Secure Access Switch, LANenforcer Security Appliance and LANSight Security Management Appliance. Nevis LANenforcer includes critical options that customers are demanding these days: pre-connect and post-connect assessment and the ability to control both managed and unmanaged endpoints. LANenforcer offers wire-speed IPS, and identity-based firewall capabilities in addition to the NAC functionality. These additional capabilities are most appealing to budget-conscious or less-technical organizations that are wary of shopping around for a wide range of network security technologies and vendors.

TIPPING POINT

TippingPoint has been a leading vendor of intrusion prevention systems since 2002 and boasts one of the leading vulnerability research teams, DV Labs. TippingPoint started offering its NAC appliance in 2006 and has improved this product based on customer needs. Despite being the largest proponent of inline IPS, their NAC solution includes options for both inline and out-of-band policy enforcement. Frost & Sullivan believes that their expertise in the IPS market will aid TippingPoint's growth into the NAC market. Furthermore, TippingPoint's plans for its product line and the integration of all these products means that this company's potential is only limited by its ability to deliver.

INSIGHTIX

The Insightix NAC solution is an innovative blend of its Visibility product and more traditional endpoint control. Insightix Stateful Network Detection and Quarantine Silo technologies allow customers to monitor and control, in real-time, who accesses the network and what they are allowed to access. The Insightix NAC software is agentless, requires no changes to the network, and is not dependent on network infrastructure to perform quarantine and enforcement. This solution has a strong appeal to organizations requiring a NAC solution that is comprehensive, easy to deploy, and cost-effective. In addition, the non-intrusive nature of this solution is warmly embraced by customers that are hesitant to install "yet-another security agent" on their endpoints.

N O R T E L N E T W O R K S

Nortel is a large multinational telecommunications vendor with reliable and secure network solutions that has earned the business and trust of government and Fortune 500 companies. Nortel's Secure Network Access (SNA) solution is based around its Secure Network Access Switch (SNAS). Nortel SNAS delivers Nortel NAC framework services for routers, switches, wireless controllers, VPN devices including third-party Ethernet switches and other third-party devices. Nortel SNA meets the most important customer demands by supporting managed clients with single sign-on, unmanaged clients through an agentless captive portal, standards based operation, and performance. Nortel SNA interoperates with Microsoft NAP benefiting both solutions and providing investment protection, scalability and flexibility in deployment for customers.

Emerging Players

S O P H O S

Sophos entered the NAC market in 2007 by acquiring nac-vendor ENDFORCE. Sophos plans to integrate NAC and endpoint security into a product called Sophos Endpoint Security and Control 8.0 for release in early 2008. This solution will include a personal firewall, anti-virus software, and of course, network access control. The Sophos solution is designed to be both flexible and intuitive. It is centrally managed through a web browser, offers automatic remediation, and persistent or dissolvable agent assessments, as the customer desires. The Sophos solution is a strong stand-alone product but represents a powerful NAC solution when implemented as an overlay with other security products.

N O V E L L

Novell acquired Senforce in 2007, making it a player in the NAC market. Reportedly, Novell was most interested in using Senforce's endpoint security products in order to improve its ZENworks Endpoint Security Management product. It will be interesting to watch whether Novell shows interest in expanding into this market or decides to move out of this space.

N A P E R A N E T W O R K S

Napera Networks offers solutions that enable small and medium enterprises to build safe, secure and healthy networks—a productive, efficient, up-to-date network that is cost-effective as well. Utilizing Microsoft's Network Access Protection (NAP) technology, Napera's products deliver large enterprise security with the ease of use and price point demanded by smaller companies. The Napera solution will allow IT administrators to easily keep their networks healthy while providing employees and guests with secure access to company resources, printers, and the Internet. Napera Networks will unveil its network health solution at this year's RSA Conference in San Francisco on April 8, 2008.

H P P R O C U R V E

HP ProCurve sells flexible and secure network infrastructure and started offering NAC in mid 2007. The ProCurve Network Access Controller 800 appliance can be deployed inline or out of band using 802.1X or DHCP protocols. It also offers an installed agent, temporary agent or agentless testing. Network Access Controller 800 is controlled by the ProCurve Manager management platform. Because of this, Network Access Controller 800 integrates with the ProCurve Network Immunity Manager 1.0 and Network Driven Identity Manager, which are also both managed by ProCurve Manager. Network Immunity Manager 1.0 detects and responds to threats using Network Behavior Anomaly Detection and Network Identity Driven Manager 2.2 allows for dynamic role-based authentication. These capabilities meet the needs of any customer requiring a secure and high availability network infrastructure.

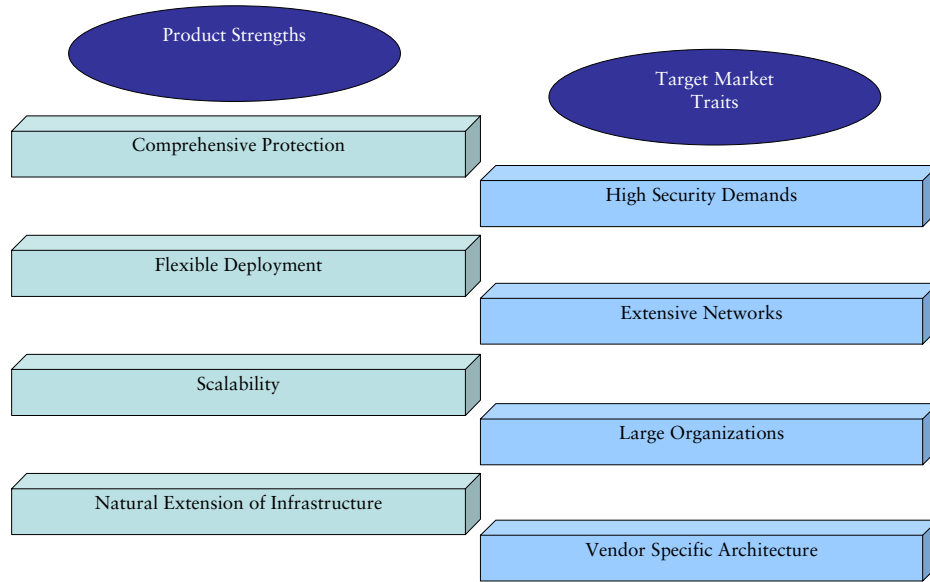
S T R A T E G I C R E C O M M E N D A T I O N S

Strategic Recommendations for NAC Architecture Vendors

Vendors that offer an architecture approach to network access control have a unique value proposition and should target a certain audience set accordingly. Just as customers evaluate the various NAC solutions available to them, so too should NAC vendors evaluate their target market. More focused marketing activities will resonate strongly with potential customers while reducing dollars wasted chasing unsubstantial sales leads. Chart 2.8 illustrates the NAC Architecture value proposition and the relationship that it has with the primary target market.

CHART 2.8

Network Access Control Architecture Market: Matching Product Strengths to Target Market (World), 2007



Source: Frost & Sullivan

COMPREHENSIVE PROTECTION

Securing the network against remote, traveling, short-term, or careless employees has been an escalating concern in recent years. Architecture based NAC solutions provide comprehensive protection across the network hardware and software infrastructure. With a NAC framework, the layers of NAC-enabled switches, routers, VLANs, VPNs, policy servers, scanning agents and other technologies form a hardened, secure network. Organizations with high security requirements or identifiable security concerns would greatly benefit from investing in an architecture based NAC solution.

FLEXIBLE DEPLOYMENT

Larger organizations typically have extensive networks with multiple segments and a wide range of infrastructure components. While the task of implementing either a set of NAC appliances or a NAC framework is a daunting one, customers appreciate the many options available to them in a framework NAC approach. Framework NAC deployments allow the customer to prioritize and roll out the deployments based on budget, value or time factors. In addition, the flexibility of these deployments lowers the sense of risk that a customer feels, as compared to a forklift, overnight upgrade. Unfortunately, this advantage is not recognized until after the sale is complete. NAC framework vendors that successfully convey this message as part of the marketing strategy will have an advantage over other vendors.

SCALABILITY

As part of the network infrastructure, the NAC architecture is not restrained by scalability issues. This is the strongest advantage over an appliance based NAC solution which can support up to 4,000 users. While many NAC appliance vendors boast the maximum number of users that their box supports, NAC architecture vendors usually omit their clearly advantageous point. Although the IT staff may consider this an obvious attribute, the top decision makers and check-signers may not be so technically savvy. NAC architectures inherently appeal to large multinational customers with tens of thousands of users, though this should not be taken for granted in marketing efforts.

NATURAL EXTENSION OF INFRASTRUCTURE

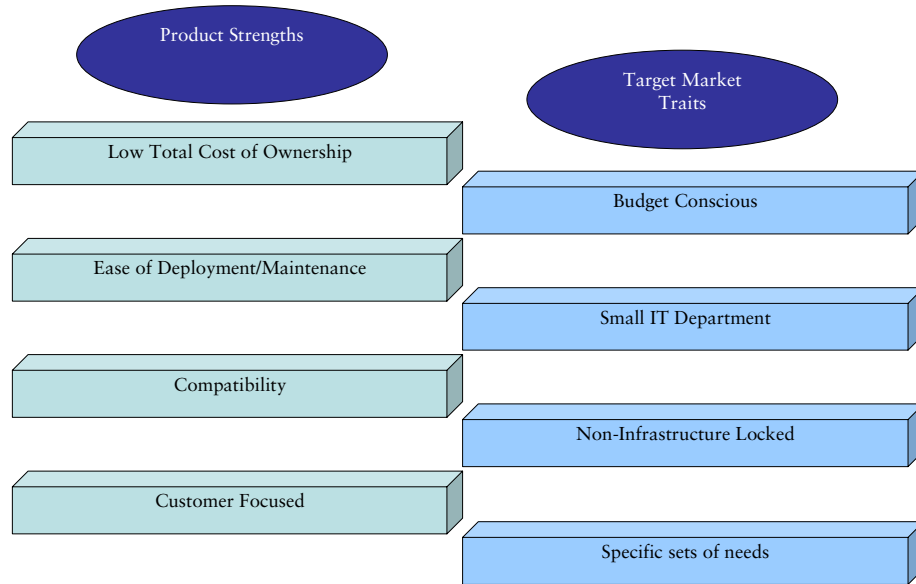
NAC architecture vendors should emphasize the fact that a NAC framework is really an upgrade of the existing infrastructure. It's crucial to change customers' conceptions of NAC as "yet-another-security product" to "a natural extension of the network infrastructure." Companies that can do this successfully will find their marketing and sales efforts much more fruitful. Microsoft has done just that by advertising that their NAC solution would be a part of the next generation of enterprise operating system. On the other hand, Cisco's architecture has been successful due in-part to their dominance in the network infrastructure market.

Strategic Recommendations for NAC Appliance Vendors

Vendors that offer an appliance approach to network access control have a unique value proposition and should target a certain audience set accordingly. Just as customers evaluate the various NAC solutions available to them, so too should NAC vendors evaluate their target market. More focused marketing activities will resonate strongly with potential customers while reducing dollars wasted chasing unsubstantial sales leads. Chart 2.9 illustrates this NAC Appliance value proposition and the relationship that it has with the primary target market.

CHART 2.9

Network Access Control Appliance Market: Matching Product Strengths to Target Market (World), 2007



Source: Frost & Sullivan

LOW TOTAL COST OF OWNERSHIP

To some degree, every organization is price sensitive or budget conscious. As an appliance, this solution is far less costly than the NAC framework which requires upgrading or replacing the entire network infrastructure. Because of scalability issues, this price advantage is most prominent with smaller and medium-sized organizations. For small customers, NAC appliance vendors hold the price advantage even if redundant or multiple appliances are required. NAC appliances will gain more acceptance in larger organizations as technology improves and the capability of these appliances increases. For the most part, NAC appliance vendors have made this a key selling point and have been targeting the correct target audience.

E A S E O F D E P L O Y M E N T / M A I N T E N A N C E

Forklift upgrades and lengthy deployment rollouts are factors that scare off many potential NAC architecture vendors. Customers with particularly small IT departments are wary of products that are difficult to implement or maintain. NAC appliances are easily deployed in the network—often taking only a matter of hours—and are also easy to replace. Once again, this is a widely accepted, clear-cut advantage for NAC appliance vendors. This should continue to be a key marketing message and this target market should remain the primary focal point through the forecast period.

C O M P A T I B I L I T Y

Any organization that is not locked into any specific infrastructure vendor is instantly a good candidate for a NAC appliance solution. Cisco's NAC architecture solution is not compatible with network technology from any other vendor. This is a double-edged sword that causes customers with Cisco gear to favor Cisco NAC and drives away customers with non-Cisco hardware. This single point device also lacks the compatibility issues encountered when having to deploy authentication servers, switches, routers, firewalls and other network infrastructure components as part of a NAC framework. As a major evaluation criterion, NAC appliance vendors must remember to advertise this advantage.

C U S T O M E R F O C U S E D

The many vendors that are selling a NAC appliance have each brought a solution to the market that is distinctive in one way or another. Customers can shop around and find the solution that meets or exceeds their needs. There is much debate over which approach to a NAC appliance is correct. Health checking, identity management, and intrusion prevention based NAC each meets a customer's needs, thus there is no one approach to NAC. However, it is up to NAC vendors to demonstrate how their solution will fit their customer's needs.