

September 5, 2008

The Forrester Wave™: Network Access Control, Q3 2008

by Robert Whiteley and Usman Sindhu
for Security & Risk Professionals

September 5, 2008

The Forrester Wave™: Network Access Control, Q3 2008

Microsoft, Cisco, Bradford, And Juniper Lead The Pack

by **Robert Whiteley and Usman Sindhu**

with Rachel A. Dines

EXECUTIVE SUMMARY

In Forrester's 73-criteria evaluation of network access control (NAC) vendors, we found that Microsoft, Cisco Systems, Bradford Networks, and Juniper Networks lead the pack because of their strong enforcement and policy. Microsoft's NAP technology is a relative newcomer, but has become the de facto standard and pushes NAC into its near-ubiquitous Windows Server customer base. Cisco's and Juniper's NAC solutions are anchored by mature, standalone appliances with top marks for manageability and ease of use. Bradford has pushed into the enterprise space with one of the most scalable overlay solutions. Symantec, McAfee, and StillSecure are all close behind with software-based solutions, which we predict will ultimately win as the best NAC architecture. Mirage Networks' unique out-of-band system provides superior deployment flexibility and just edges out Nevis Networks, which operates as a secure inline switch with built-in threat prevention. HP ProCurve Networking rounds out the bunch with an approach that marries appliance with Ethernet switches.

TABLE OF CONTENTS

2 NAC Provides Control And Visibility

- Three NAC Architectures Emerge
- To Pull Off NAC, Security Managers Need Tight Collaboration With Infrastructure Teams

4 NAC Evaluation Overview

- Evaluation Criteria Focus On NAC Architecture And The Ability To Handle Diverse Scenarios
- Evaluated Vendors Excel At Large-Enterprise Deployments

6 Top NAC Vendors Offer Well-Integrated Hardware And Software Components

- Focus On Scenarios, Not Features And Functions

9 Vendor Profiles

- Leaders: Microsoft, Cisco, Bradford, And Juniper
- Strong Performers: Symantec, Mirage Networks, McAfee, StillSecure, And Nevis
- Contenders: ProCurve

13 Supplemental Material

NOTES & RESOURCES

Forrester conducted product evaluations in May 2008 and interviewed 30 vendor and user companies, including: Bradford Networks, Cisco Systems, Juniper Networks, McAfee, Microsoft, Mirage Networks, Nevis Networks, ProCurve Networking by HP, StillSecure, and Symantec.

Related Research Documents

- ["Inquiry Insights: Client Security, Q3 2008"](#)
July 14, 2008
- ["Overcoming The Common Pitfalls Of NAC"](#)
April 23, 2008
- ["Client Management 2.0"](#)
March 29, 2007

NAC PROVIDES CONTROL AND VISIBILITY

Security and risk management professionals have been pursuing NAC for a few years now. NAC provides the ability to authenticate all users as they enter your network and to ensure they meet minimum health and compliance requirements. Although the technology has gone through many iterations, it's now finally mature enough that security teams should look to NAC as a key component in a good network security architecture. So why deploy yet another security widget? Because NAC is not just a widget; it's a framework for addressing:

- **A consistent set of access controls for a mix of users accessing your network.** Enterprises need to provide access to data and applications to a mix of users across the globe. These users include customers, contractors, consultants, suppliers, partners, auditors, and internal employees. They are connecting to companies' intranet, Internet, and databases either through VPN or Web-based interfaces.
- **An enforcement architecture for a growing mobile workforce.** Organizations need to provide access to employees and nonemployees who are connecting to the network via public Wi-Fi and 3G cellular networks. Even inside your four walls you'll find a pervasive population of users connecting through in-house Wireless LAN (WLAN). We've found that approximately one-third of organizations are using public wireless while more than half provide WLANs.¹
- **User visibility for compliance and regulatory mandates.** Reporting and auditing for compliance with such standards as PCI, SOX, and HIPAA, pressure organizations to employ automated ways to stay compliant without operational overhead. A NAC framework doesn't end compliance woes, but it does allow organizations to track who's on the network, where they went, and what resources they accessed.

Three NAC Architectures Emerge

The NAC market is finally stabilizing, but security teams must wade through many underlying architectures. However, all NAC solutions provide endpoint security that ties health, device, and identity information to your network. It's an important add-on to your enterprise's network since it provides granular policy control and enforcement. But more enterprises will find they already have a mixture of tools in place, including IDS/IPS, DLP, and client security agents. Done right, NAC will complement these investments by providing policy enforcement and remediation features above and beyond standard security tools. To get it right, you must consider the three main NAC architectures:

- **Infrastructure-based NAC.** This category includes gear already in your environment, such as NAC-enabled switches, routers, and servers. They employ various enforcement modes like 802.1x, DHCP, and IPSec. They also integrate with endpoint agents to perform ongoing compliance checks, security updates, and remediation. These inline solutions tend to have a relatively longer learning curve and are more complex to deploy but provide some of the more scalable options.

- **Appliance-based NAC.** Most appliance solutions are out-of-band, meaning users are passed to the devices for inspection without requiring hardware in every single data path. Out-of-band appliances leverage the same deployment modes but often add additional capabilities to control inline devices — such as sending SNMP commands to a switch. These appliances excel at post-admission checks based with safeguards for malicious activity and ongoing compliance checks.² They can be less scalable in a larger environment but tend to be less complex to deploy.
- **Software-based NAC.** Software-based solutions require that agents be installed directly on the endpoint — usually as part of a client security suite. They are the most scalable and easy-to-deploy but often provide just basic host-based enforcement; for a richer set of enforcement options they need integration with a number of third-party infrastructure and appliance components. However, a persistent presence on the endpoint often means superior compliance checks and automatic remediation.

To Pull Off NAC, Security Managers Need Tight Collaboration With Infrastructure Teams

We see that nearly a quarter of all enterprises have already adopted NAC, and an additional 15% will be doing so by 2009.³ However, for all of its momentum, it will still take some time before enterprises fully absorb NAC due to its complexity and lengthy deployment time. Today's security teams must plan, build, and implement access policies with the litany of underlying servers, switches, routers, firewalls, intrusion prevention systems (IPS), and VPN gateways that are part of NAC. As a result, security specialists must rely on a close partnership with the IT infrastructure and operations (I&O) teams that manage the day-to-day infrastructure. Doing so will prevent:

- **Underestimating the complexity of a NAC deployment.** NAC requires an immense undertaking depending on your network size and environment. Most security teams will find they need I&O's cooperation to reconfigure the network and avoid overtaxing DHCP, DNS, and RADIUS services.
- **Prolonging deployments in production environments.** Implementing NAC all at once means users will be too disrupted by the change from a wide-open network to one that's tightly controlled. Coordinating NAC with the help desk means a phased approach smoothes out wrinkles in the employee experience.
- **Implementing a NAC architecture that doesn't scale to your environment.** I&O teams are often plagued with technology that doesn't scale. NAC is no different. Security managers must perform a needs assessment to identify the relevant scenarios NAC needed within a five-year horizon; otherwise, your I&O team will be stuck ripping out prematurely obsolesced gear.⁴

NAC EVALUATION OVERVIEW

To assess the state of the NAC market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top NAC vendors.

Evaluation Criteria Focus On NAC Architecture And The Ability To Handle Diverse Scenarios

After examining past research, user needs assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 73 criteria, which we grouped into three high-level buckets:

- **Current offering.** We evaluated each vendor's NAC solution across overall product architecture, access control architecture, enforcement architecture, policy architecture, scalability, manageability, managed and unmanaged systems, compliance, and the strength of the solution, against 12 scenarios based on client conversations.
- **Strategy.** We evaluated each vendor's NAC strategy across product strategy/vision, product support, corporate strategy, and the financial resources to support the strategy.
- **Market presence.** We evaluated each vendor's presence in the NAC market through its installed base, revenue, revenue growth, services, number of employees, and number and quality of channel partners.

Evaluated Vendors Excel At Large-Enterprise Deployments

Forrester included 10 vendors in the assessment: Bradford Networks, Cisco Systems, Juniper Networks, McAfee, Microsoft, Mirage Networks, Nevis Networks, ProCurve Networking by HP, StillSecure, and Symantec. Each of these vendors has (see Figure 1):

- **NAC products shipping in Q2 2008.** Each vendor had NAC solutions shipping at the time of the evaluation. Any products in planning to be released after this period are not part of this evaluation, although future enhancements were captured as part of the vendor's strategy.
- **Multiple mentions in the client inquiries.** The NAC vendors must have been considered by our enterprise clients and mentioned repeatedly in Forrester's inquiries. We selected the participating 10 vendors from among more than 40 based on client inquiries from the last three years.
- **A large-enterprise product and strategy.** Evaluated NAC solutions must be designed for and able to support a large-enterprise environment. We selected the vendors based on their ability to scale, support heterogeneous infrastructure, and provide management interfaces designed for large IT organizations.

Figure 1 Evaluated Vendors: Product Information And Selection Criteria

Vendors	Product evaluated	Software-based solution	Infrastructure-based solution	Appliance-based solution
Bradford Networks	NAC Director, Campus Manager, NAC Director GCS		-	
Cisco Systems	Cisco NAC appliance, NAC server, NAC Manager, NAC Profiler, Guest Server			
Juniper Networks	UAC Infranet Controller 4000/4500, Infranet Controller 6000/6500, Odyssey Access Client, NAC Profiler			
McAfee	MNAC 3.0 (ePolicy Orchestrator)		-	
Microsoft	Microsoft NAP for Windows Vista, XP SP3, Server 2008			-
Mirage Networks	NAC Management Server, Advanced Compliance Server, Sensors	-	-	
Nevis Networks	LANenforcer (Nevis LAN Switch, Nevis LAN Security Appliance)			
ProCurve Networking by HP	ProCurve Network Access Controller 800, ProCurve NAC 800 Endpoint Integrity Agent, ProCurve Identity Driven Manager			
StillSecure	Safe Access		-	
Symantec	SNAC 11.0			

Full NAC solution
 Partial NAC solution or not licensed product
 NAC capability, but not primary focus
 NAC functionality, but no dedicated product
 - No solution or functionality

Vendor selection criteria

Shipping Q2 2008: The NAC product was shipping in Q2 2008.

Client inquiries: The vendor is mentioned in numerous Forrester client inquiries.

Large-enterprise driven: The NAC solution is designed for large enterprises.

Source: Forrester Research, Inc.

TOP NAC VENDORS OFFER WELL-INTEGRATED HARDWARE AND SOFTWARE COMPONENTS

The evaluation uncovered a market in which (see Figure 2):

- **Microsoft, Cisco Systems, Bradford Networks, and Juniper Networks lead the pack.** Microsoft, Cisco Systems, Bradford Networks, and Juniper Networks have the best all-around NAC solutions. In particular, these vendors have the highest combined scores for access and enforcement architectures, the two linchpin criteria for NAC. Furthermore, the larger vendors — Microsoft, Cisco Systems, and Juniper — leverage a large pool of partners and customer bases to push NAC into larger, heterogeneous enterprise environments. These leaders also excel at providing extensive policy architectures, which security managers need to create granular access controls. Although it doesn't have the best all-around policy architecture, Bradford compensates by providing one of the strongest solutions for the 12 scenarios we evaluated.
- **Symantec, Mirage Networks, and McAfee offer competitive options.** Symantec, Mirage Networks, and McAfee are not far from the lead and are among the easiest solutions to deploy. All three vendors require minimal impact to your existing network architecture. Symantec and McAfee provide strong threat protection solutions that marry NAC with endpoint agents that include firewalling, antimalware, and host intrusion protection. As a result, they excel at providing solutions that can proactively combat risk to managed endpoints. Mirage provides the strongest out-of-band appliance with its patented technique that manipulates ARP packets on the network.
- **StillSecure, Nevis Networks, and HP ProCurve round out the group.** StillSecure and Nevis Networks are practically tied due to their respective strengths in pre- and post-admission capabilities. StillSecure — which many vendors license to provide NAC — provides excellent authentication and authorization, highlighted by excellent compliance features that address mandates like PCI and SOX. Nevis' post-admission control uses deep packet inspection for excellent identity-based security. It uniquely employs its Nevis Labs to provide ongoing support and security updates. ProCurve has a relatively new NAC product, which combines an appliance product and a NAC-enabled switching line; however, it provides a seamless management of both with its Identity Manager (IDM).

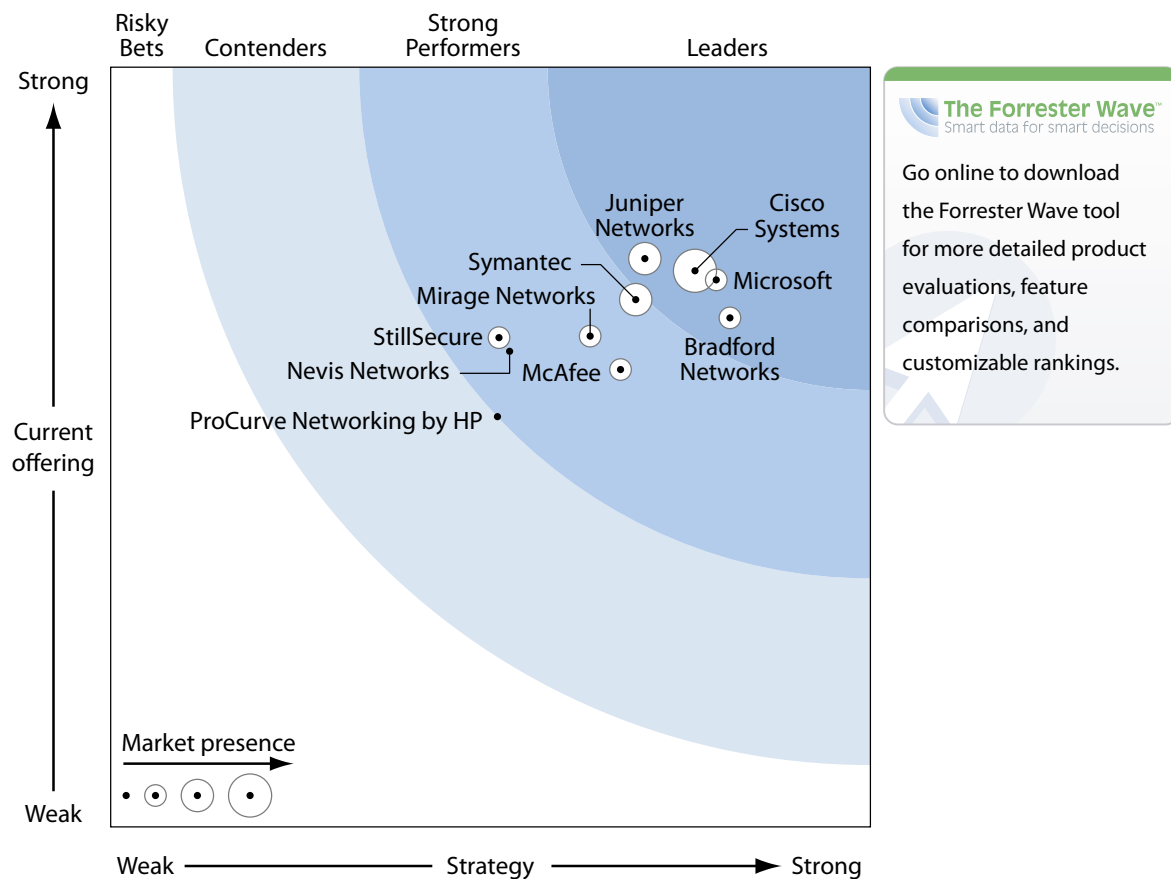
This evaluation of the NAC market is intended to be a starting point only. We encourage readers to view detailed product evaluations and adapt the criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool.

Focus On Scenarios, Not Features And Functions

For this evaluation, Forrester has placed a great deal of emphasis on scenarios. Why? Because NAC solutions vary widely in their underlying architecture. However, by focusing on key use cases, organizations can begin NAC for one particular scenario — most often controlling guest

access or external employees, such as contractors — and then scale to additional scenarios as business requirements evolve. Forrester has evaluated each vendor across 12 scenarios, which is the most heavily weighted part of the Current Offering portion of the evaluation. In the past three years, we have seen that organizations are most successful when they select NAC based not on features or functions, but rather on the ability to support the four or five scenarios that are most relevant to their business. We encourage security managers to focus on the scenarios that mirror the requirements for people like guests, customers, employees, and outsourcers; processes like disaster recovery procedures; operational tasks like remediation and provisioning guest access; and technology like integrating with other pieces of infrastructure and handling virtualized environments (see Figure 3).

Figure 2 Forrester Wave™: Network Access Control, Q3 '08



The Forrester Wave™
 Smart data for smart decisions

Go online to download the Forrester Wave tool for more detailed product evaluations, feature comparisons, and customizable rankings.

Source: Forrester Research, Inc.

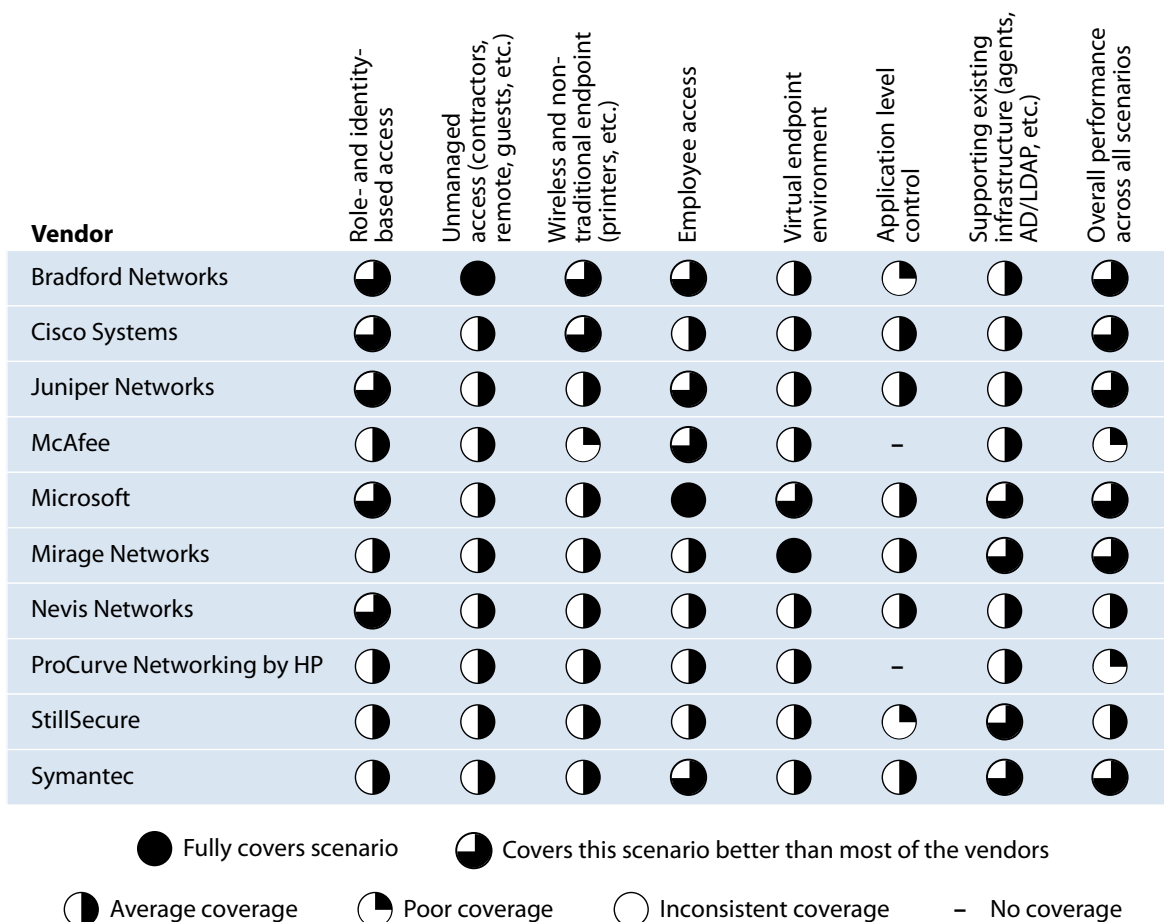
Figure 2 Forrester Wave™: Network Access Control, Q3 '08 (Cont.)

	Forrester's Weighting	Bradford Networks	Cisco Systems	Juniper Networks	McAfee	Microsoft	Mirage Networks	Nevis Networks	ProCurve Networking by HP	StillSecure	Symantec
CURRENT OFFERING	50%	3.35	3.66	3.74	3.01	3.60	3.23	3.13	2.70	3.22	3.47
Overall architecture	15%	3.35	4.25	3.95	3.35	3.80	3.40	3.25	2.95	3.45	4.05
Access control architecture	10%	3.65	3.52	3.89	3.32	3.38	3.00	2.75	2.63	2.76	3.62
Enforcement architecture	5%	4.00	3.00	4.00	2.00	4.00	3.00	3.00	2.00	2.00	2.00
Policy architecture	10%	2.85	4.70	4.60	3.05	4.85	2.85	2.85	2.70	2.85	3.00
Scalability	10%	3.00	3.00	4.00	3.00	4.00	2.00	3.00	2.00	4.00	4.00
Manageability	5%	3.00	3.50	3.50	3.15	2.65	2.75	2.75	2.75	3.00	3.00
Managed and unmanaged systems	10%	4.00	5.00	4.00	3.00	3.00	5.00	4.00	3.00	3.00	4.00
Compliance	5%	3.00	2.00	3.00	3.00	3.00	3.00	3.00	3.00	5.00	3.00
Scenarios	30%	3.34	3.26	3.24	2.86	3.40	3.32	3.16	2.78	3.14	3.32
STRATEGY	50%	4.07	3.84	3.51	3.35	3.98	3.15	2.62	2.54	2.55	3.45
Product strategy and vision	60%	4.28	3.73	3.23	3.58	3.88	3.00	2.15	2.23	2.25	3.45
Product support	15%	4.00	5.00	5.00	3.00	5.00	3.00	3.00	3.00	3.00	3.00
Corporate strategy	10%	4.50	2.50	2.25	3.00	1.50	4.50	4.25	1.50	3.00	3.25
Financial resources to support strategy	15%	3.00	4.00	4.00	3.00	5.00	3.00	3.00	4.00	3.00	4.00
Cost	0%	3.40	1.70	1.70	3.55	3.60	3.15	1.75	2.35	2.60	3.25
MARKET PRESENCE	0%	2.52	4.04	3.76	2.57	2.50	2.11	1.89	1.86	2.63	3.43
Installed base	30%	2.40	4.70	4.00	2.40	1.90	2.20	1.90	1.00	2.30	3.00
Revenue	30%	2.00	5.00	4.00	3.00	1.00	2.00	2.00	1.00	3.00	4.00
Revenue growth	15%	5.00	3.00	3.00	2.00	4.00	2.00	1.00	4.00	3.00	3.00
Services	10%	3.00	3.00	3.00	5.00	4.00	3.00	3.00	3.00	3.00	3.00
Employees	5%	1.00	4.00	4.60	3.00	4.20	1.80	1.80	1.20	1.30	3.20
Channel partners	10%	1.00	1.80	3.80	0.00	4.20	1.60	1.80	3.00	2.20	4.20

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc.

Figure 3 Top NAC Vendors Excel At Handling A Broad Array Of Enterprise Scenarios



36450

Source: Forrester Research, Inc.

VENDOR PROFILES

Leaders: Microsoft, Cisco, Bradford, And Juniper

- **Microsoft.** Microsoft has the strongest NAC product for managed endpoints. Its solution is composed of built-in Network Access Protection (NAP) functionality in its Windows desktop and server OSes combined with the back-end Network Policy Server (NPS). This architecture affords Microsoft one of the most scalable solutions, supporting hundreds of thousands of endpoints with as few as four NPSes. Moreover, Microsoft can leverage its existing Forefront and Active Directory assets for superior policy management, but also leverages System Center Configuration Manager and System Center Operations Manager for easy remediation and

daily operations. However, Microsoft NAP is also a vendor framework that guarantees NAC interoperability with more than 100 different vendors. Thus, even though its official product has only been shipping since the inception of Windows Server 2008, Microsoft has already established itself as a critical thought leader and contributor to the standardization of NAC. As a result, Microsoft has the overall highest score among the 12 scenarios we evaluated.

- **Cisco Systems.** Cisco's Network Admission Control (CNAC) is perhaps the longest-running NAC solution. And similar to Microsoft, CNAC is both a product and part of a broader access control framework. The primary product is the Cisco NAC Appliance, which has two required components: the Cisco NAC Server and Cisco NAC Manager. Cisco NAC can also work with Cisco Security Agent (a separate software) to provide additional protection and policy controls. Each of these rounds out specific access, enforcement, and policy capabilities. The Cisco NAC Profiler performs endpoint profiling and asset management, which is a critical requirement for extending NAC to non-computing IP endpoints like HVACs, security badge readers, and printers. The CNAC also provides an infrastructure-based approach that extends NAC into other Cisco infrastructure, including its Catalyst switching line. Through this infrastructure-based approach, Cisco is able to focus on evolving virtualization, identity control, and application layer (Layer 4 through Layer 7) functionality. Cisco provides additional role-based access controls via the TrustSec features on its switches, which complements its NAC offerings.
- **Bradford Networks.** Bradford is a relatively new NAC entrant in the enterprise market. Originally designed for university campuses, Bradford has since retooled its NAC solution and now offers NAC Director — an out-of-band solution that includes an appliance with both persistent and dissolvable agents. NAC Director leverages existing network devices such as routers and switches to perform enforcement, which highlights Bradford's greatest strength, its ease of deployment. As a result, Bradford provides one of the most scalable solutions as well as the flexibility to support a wide range of enforcement options. Although many vendors support a similar architecture, Bradford has the best all-around support for third-party infrastructure. Bradford also offers its NAC Director Guest/Contractor Services (GCS) product, which is a slimmed-down version of NAC Director, designed specifically for guests or contractors. Finally, Bradford has one of the strongest road maps, which focuses on emerging NAC scenarios for virtualization and identity management.
- **Juniper Networks.** Juniper's Unified Access Control (UAC) is the most complete NAC solution and scored highest in Current Offering. It has an impressive array of enforcement options and deployment modes. Juniper's UAC is anchored by the Infranet Controller (IC) — a centralized policy manager — that enforces NAC on a variety of Juniper infrastructure (switches, firewalls, IDS/IPS, etc.), but also supports third-party gear via 802.1x. Juniper supports multiple agent technologies to provide endpoint security and remediation, as well as the strongest 802.1x solutions thanks to its Juniper Odyssey Access Client supplicant. Juniper's IC is built on its well-established SSL VPN product, which provides strong integration with back-end policy servers,

a mature management interface for very granular authorization capabilities, and a broad set of role- and identity-based features. Juniper can also be deployed as both an inline and out-of-band solution, depending on whether you use the underlying infrastructure or IC as the main point of enforcement. Juniper also tightly integrates with Microsoft's NAP and can seamlessly interchange both client- and server-side NAC components.

Strong Performers: Symantec, Mirage Networks, StillSecure, And Nevis

- **Symantec.** Symantec NAC (SNAC) is a software-based NAC solution composed of a host-based functionality built into its flagship Symantec Endpoint Protection (SEP) 11.0 client, Symantec Endpoint Protection Manager (SEPM) for configuration and management, and its Enforcer appliance for network-based deployment options. The cornerstone of SNAC, however, is its Sygate firewall, which has comprehensive capability of granular policy checks and enforcement. Symantec combines SNAC with threat protection capabilities on the endpoint, but also provides one of the most comprehensive reporting and auditing frameworks, which is critical for heavily regulated organizations. Symantec's vision is pretty strong and includes one of the more aggressive plans on working with VMware to include SNAC into virtual endpoints. Moreover, it plans to further integrate SNAC with Altiris to introduce asset management and automatic remediation capabilities. Further integration will also simplify deployment and pricing options.
- **Mirage Networks.** Mirage has a well-defined solution geared toward post-admission NAC and preventing zero-day threats. Its components consist of three appliance flavors: Management Server, Advanced Compliance Server, and Sensors. Mirage scales from one (which can perform all three functions) to 100 appliances in a cluster. Mirage NAC uses ARP caching to perform deep packet inspection for a truly agentless deployment. As a result, Mirage's strength is its ability to assess unmanaged endpoints where not even a dissolvable agent can be implemented. Mirage's strategy includes complementing Microsoft NAP's pre-admission architecture with its stronger, threat-based post-admission capabilities. Mirage also has one of the most mature strategies around virtualization. It's developing Mirage appliances as virtual sensors to be used in both virtual desktop and server environments. Mirage is also working with partners like Oracle to provide application level control.
- **McAfee.** McAfee NAC (MNAC) consists of a specific NAC agent with two back-end software requirements: ePolicy Orchestrator (ePO) 4.0 and Rogue System Detection 2.0. McAfee also rolls NAC into its Total Protection for Endpoint, which is a comprehensive client security suite. McAfee currently relies heavily on Microsoft NAP integration to round out its enforcement capabilities but will continue to integrate with its IntruShield IPS appliance. This more comprehensive inline NAC capability will ship in Q3 2008 and will provide more native enforcement controls from within the McAfee product portfolio. But for now, McAfee has one of the better integration strategies with Microsoft NAP and uses features like Microsoft NPS to force policies and remediation. As with other vendors, McAfee plans to better support

virtualization, but its primary vision is around scalability and ease-of-use. McAfee intends to build on the strength of ePO to create a solution that supports 400,000 endpoints under a single policy server as well as streamline both security and IT operations administration.

- **StillSecure.** StillSecure has a two-pronged approach to the NAC market. It works with major infrastructure vendors to license its technology as well as its own purpose-built software NAC, Safe Access. Safe Access includes both pre- and post-admission NAC, identity-based management, and remediation — but admittedly, StillSecure is strongest in its pre-admission compliance checks, authentication, and authorization capabilities. It has demonstrated very granular policy capabilities that appeal to a wide range of scenarios without sacrificing scalability. StillSecure accomplishes this through agentless, agent-based, and dissolvable agents, and Safe Access can be deployed to enforce NAC using 802.1X, DHCP, inline using a firewall, and host-based using the agents. StillSecure provides excellent reporting and auditing capability to address mandates like PCI, SOX, and HIPAA — a capability for which most vendors require integration with a separate compliance solution.
- **Nevis Networks.** Nevis's NAC is part of a larger identity-oriented network security solution built on the LANsecure ASIC. Specifically, Nevis has two components: 1) its LANenforcer appliances, which are inline security switches with built-in IPS and firewalling; and 2) its LANsight management appliance. As a result, Nevis is technically an appliance-based solution, although some organizations are looking to Nevis to replace existing switch infrastructure. Nevis provides good pre-admission compliance checking, but its true strength lies in per-port threat protection and monitoring, which provides post-admission access control at 10 Gbps speeds. The larger Nevis appliances can only scale to 3,000 users, but its throughput and switch-based architecture can cluster to support larger NAC environments. Nevis' unique strength is its lab service, which further builds on the threat-oriented capabilities Nevis brings to a NAC deployment.

Contenders: ProCurve

- **ProCurve Networking by HP.** HP ProCurve has a well-balanced NAC solution that's anchored by its Network Access Controller 800 — an appliance-based solution (both inline and out-of-band) and the associated Endpoint Integrity Agent. However, ProCurve really shines with its back-end management systems. It offers two plug-ins for its management console: the Identity Driven Manager (IDM), for centrally managing NAC policies, and Network Immunity Manager (NIM), for ongoing monitoring and threat mitigation for post-admission NAC. With this back-end management suite it can also tie NAC policies across the 800 appliances and the entire line-up of switches, which use the ProVision ASIC to provide wire-speed NAC as an additional inline deployment option. ProCurve is a relatively new entrant to the overall NAC market, even though it's provided the built-in access control on its switching line for several years. We

anticipate the continued build-out of its IDM will strengthen its back-end policy capabilities and establish ProCurve as one of the strongest switch-based vendors. This complements its vision to continue integration with Microsoft's NAP to provide deeper NAC on network appliances and infrastructure.

SUPPLEMENTAL MATERIAL

Online Resource

The online version of Figure 2 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Data Sources Used In This Forrester Wave

Forrester used a combination of data sources to assess the strengths and weaknesses of each solution:

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with two of each vendor's current customers.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we then narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and we encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve.

ENDNOTES

- ¹ The need for solutions that facilitate the movement between mobile networks is pressing as users' devices are exposed to more and more wireless networks. These networks are ever-changing and increasing in their ability to replicate the user's wired experience. See the August 1, 2008, "[The State Of Mobile Infrastructure: 2008](#)" report.
- ² Pre-admission refers to the authentication and authorization process that effectively stops the bad guys from getting on the network in the first place; post-admission refers to the ongoing compliance checks, monitoring, and anomalous behavior detection that kick legitimate users off if they don't comply with company policy.
- ³ To better understand where NAC stands today, Forrester surveyed 496 security decision-makers at North American and European companies about their interest in adopting NAC. Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2007.
- ⁴ The key to successfully assessing NAC is to determine your access scenarios before you begin implementation. Let business requirements (e.g., maximizing productivity or reducing costs by using contractors) prioritize scenarios that warrant access control, which, in turn, will dictate the underlying NAC architecture. For more information on the top enterprise scenarios, see the April 23, 2008, "[Overcoming The Common Pitfalls Of NAC](#)" report.

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

*For a complete list of worldwide locations,
visit www.forrester.com/about.*

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866.367.7378, +1 617.617.5730, or resourcecenter@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. For more than 24 years, Forrester has been making leaders successful every day through its proprietary research, consulting, events, and peer-to-peer executive programs. For more information, visit www.forrester.com.