

## Magic Quadrant for Network Access Control

Lawrence Orans, John Pescatore, Mark Nicolett

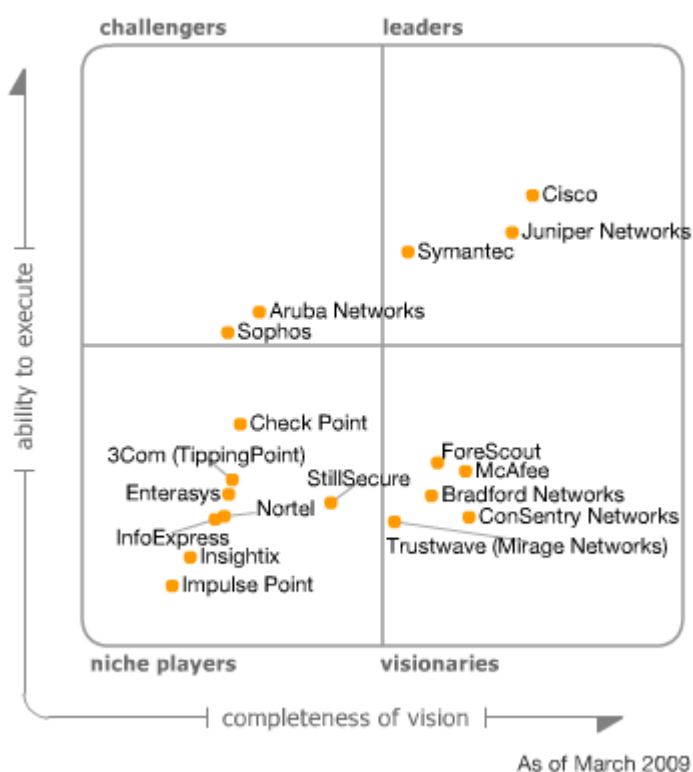
Network infrastructure, endpoint protection and network security vendors are increasingly adding NAC features to their solutions, helping the overall NAC market to mature. Several point solutions persist, with some continuing to provide differentiated value.

## WHAT YOU NEED TO KNOW

Because network access control (NAC) is an embedded feature of so many network and security components, enterprises should look first within their existing vendor base to evaluate NAC solutions. Enterprises should be sure to broaden their search to include point solutions or other embedded NAC solutions that may be a better fit for their future NAC plans. Long-term planning is critical, because most organizations plan to phase in NAC as they progress through multiple usage cases (for example, guest networking, endpoint baselining and identity-aware networking).

## MAGIC QUADRANT

Figure 1. Magic Quadrant for Network Access Control



Source: Gartner (March 2009)

## Market Overview

The NAC market showed signs of maturing in 2008, prompting Gartner to shift the 2009 analysis to a Magic Quadrant instead of the MarketScope format used in previous years. The market remained relatively stable: Only one vendor (Nevis Networks) from the 2008 MarketScope exited the market, and one vendor was acquired (Trustwave acquired Mirage Networks). The following highlights point to the maturation of the NAC market:

- Gartner estimates that the size of the NAC market in 2008 was approximately \$221 million (see Note 1), and that the market in 2008 grew at a rate of 51% over the market

in 2007. We had anticipated growth of 100% in 2008, but the weak economy, the stable nature of most networks (due in part to the absence of a massive-scale worm attack) and the slow uptake of Microsoft Network Access Protection (MNAP) contributed to lower growth.

- Several vendors reported raising additional rounds of venture capital financing in 2008 and 2009 (Bradford Networks raised \$8 million; ConSentry Networks raised \$9.4 million; and ForeScout raised \$8 million). StillSecure announced that it secured a \$5 million line of venture debt financing.
- The vast majority of organizations that have implemented NAC report high levels of satisfaction. Many are expanding the scale (increasing the number of endpoints) and the scope (adding additional functionality) of their NAC projects.
- Interest in NAC (as reflected in Gartner inquiries) is widespread and cross-vertical-market, although the most dominant vertical market for NAC remains higher education.

NAC is being implemented in 2009 differently from the way it was originally envisioned back in 2003 and 2004. That period was the height of the worm era, and the common wisdom at the time was that NAC would be used to block PCs from accessing the network if they were noncompliant (for example, if they were missing patches or their antivirus signatures were out of date). In 2009, that approach is rarely used, because most organizations are reluctant to block employees from the network (and from doing their jobs) just because their PCs are noncompliant. Some organizations have implemented blocking or quarantining, but most choose to remediate the noncompliant PCs once they are on the network. As highlighted in "Network Access Control in 2009 and Beyond," the four most common uses for NAC are:

- **Guest network services** — Isolating guests and visitors from the corporate network, and providing them with limited connectivity — typically, Internet access only. Guest networking was the primary driver in approximately 80% of NAC deployments. Most organizations are starting with wireless guest access and are planning to extend guest networking capabilities to the wired network.
- **Endpoint baselining** — Determining if endpoints on the corporate network are compliant with device configuration policies, and providing support for remediation efforts. Endpoint baselining was the primary driver in approximately 15% of NAC deployments.
- **Identity-aware networking** — Providing greater visibility and control over user behavior on the network. Organizations add identity awareness to the network to monitor user traffic and enforce access to critical resources. Identity-aware networking was the primary driver in approximately 5% of NAC deployments.
- **Monitoring/containment** — Monitoring endpoints or network traffic to detect and quickly contain endpoints that begin to exhibit dangerous behavior. Monitoring/containment is a secondary driver for one of the other three usage cases.

Because these use cases all represent subsets of NAC, Gartner believes many enterprises will expand their use of NAC beyond the initial focus. Trends such as the consumerization of IT are increasing the demand to allow unmanaged PCs onto corporate networks — initial NAC deployments to support guest networking can easily be expanded to deal with employee access from "guest" PCs.

## Market Definition/Description

The NAC market consists of several categories, as outlined below:

- **Infrastructure** — Most enterprise-class LAN switch manufacturers offer NAC solutions. Of the nine vendors analyzed in "Magic Quadrant for Campus LAN (Global), 2008," seven sell NAC products. The LAN switch vendors primarily target their NAC solutions to their installed base. That is a good strategy because network managers, who are the buyers of LAN switches, are usually the buyers of NAC solutions. Infrastructure vendors have had limited success in selling their NAC solutions outside of their installed bases and into their competitors' accounts.
- **Endpoint protection (EPP)** — Some vendors that sell EPP suites also offer NAC solutions (for example, McAfee, Sophos and Symantec). All of these vendors benefit from their existing desktop "footprint," which gives them an advantage in the endpoint baselining usage case.
- **Network security vendors** — A mix of intrusion prevention system (IPS), firewall and virtual private network (VPN) vendors offer NAC solutions. Because they already serve as enforcement points in the network, these products can be easily repurposed to become NAC policy enforcement points.
- **"Pure plays"**— Several vendors are pure-play NAC vendors or vendors with multifunctional offerings whose primary focus is NAC (for example, Bradford Networks, ForeScout and InfoExpress).

The infrastructure, EPP and network security vendors are all represented in the Leaders quadrant this year. The pure-play vendors face the biggest challenges as vendors in the other three categories continue to enhance their NAC offerings.

The NAC market has been benefiting from high revenue growth rates during the past two years (approximately 90% in 2007 and 50% in 2008). However, as we said in "Dataquest Insight: Network Access Control Market, Worldwide, 2007 to 2012," the market for dedicated NAC components will be squeezed by NAC capabilities that are integrated into network equipment, desktop operating systems and EPP platforms. Gartner expects revenue growth to continue to decline in 2009 (with an anticipated growth of 25%) and in the near future. Interest in NAC remains strong, and the number of deployments continues to increase, but revenue will decline as the "embedded NAC" trend gains momentum. Through 2011, Gartner expects to see additional consolidation in the NAC marketplace, with the surviving NAC vendors being those with aggressive pricing and demonstrated innovation beyond integrated capabilities.

## Inclusion and Exclusion Criteria

The goal of these inclusion and exclusion criteria is to identify vendors that own core NAC technology. Vendors whose solutions are based heavily on technology that is licensed from original equipment manufacturers have been excluded from this Magic Quadrant.

To be included in this Magic Quadrant, the vendors' solutions must include the policy, baseline and access control elements of NAC, as defined by the following criteria:

- **Policy** — The NAC solution must include a dedicated policy management server with a management interface for defining and administering security configuration requirements and for specifying the access control actions (for example, allow or quarantine) for compliant and noncompliant endpoints. Because policy administration

and reporting functions are key areas of NAC innovation and differentiation, vendors must own the core policy function to be included in this Magic Quadrant.

- **Baseline** — A baseline determines the security state of an endpoint that is attempting to access the network, so that a decision can be made about the level of access that will be allowed. Baselining must include the ability to assess policy compliance (for example, up-to-date patches and antivirus signatures) and may include the ability to detect installed malware. Various technologies may be used for the baseline function, including agentless solutions, dissolvable agents and permanent agents. NAC solutions must include a baseline function, but "reinventing the wheel" is not necessary. Baseline functionality may be obtained via an OEM licensing partnership.
- **Access control** — The NAC solution must include the ability to block, quarantine or grant full access to an endpoint. The solution must be flexible enough to enforce access control in a heterogeneous network environment (such as a multivendor network infrastructure). Enforcement must be accomplished either via the network infrastructure (for example, 802.1X, virtual LANs and access control lists [ACLs]) or via the vendor's NAC solution (for example, Address Resolution Protocol [ARP] spoofing). Dynamic Host Configuration Protocol (DHCP) enforcement qualifies for inclusion, provided that policy enforcement can be delivered via partnerships with two or more DHCP solutions. Vendors that rely solely on agent-based endpoint self-enforcement do not qualify as NAC solutions.

Additional criteria include:

- Solutions must link to remediation systems (for example, patch and configuration management), but they do not need to own core mitigation technology.
- The products with the required features and functions must have been shipped by 1 December 2008.
- The vendor must have had at least \$2 million in NAC sales during the 12 months leading up to 1 December 2008.
- The vendor must have supplied three customer references (paying customers) to Gartner for its NAC solution. The references must have deployed the solution in a production environment.

## Vendors Considered but Not Included in the 2009 Magic Quadrant

### LAN Switch Manufacturers

Three vendors were excluded from the Magic Quadrant, because at least one critical component of their NAC solutions is based on technology licensed from an original equipment manufacturer (all three vendors base their policy servers on OEM technology):

- Alcatel-Lucent — The OmniAccess SafeGuard product line consists of rebranded products supplied by ConSentry Networks.
- Extreme Networks — The Sentriant AG200 is based on StillSecure's Safe Access solution.
- HP ProCurve — The ProCurve Network Access Controller 800 is based on StillSecure's Safe Access solution. ProCurve also offers its internally developed Identity Driven Manager, an identity-aware networking solution that integrates with multiple Remote Authentication Dial-In User Service (RADIUS) servers and interoperates with RADIUS-

compatible (RFC 3580) network devices. Identity Driven Manager is optimized for a ProCurve environment, where it utilizes RADIUS features built into ProCurve Intelligent Edge devices.

Customers of Alcatel-Lucent, Extreme Networks and HP ProCurve should consider the respective NAC offerings and should refer to our analysis of the underlying OEM solution for further insight. All three represent valid NAC offerings, but because they are based on technology from small vendors, they present an additional viability risk. All three solutions can enforce NAC in a heterogeneous (multivendor) network infrastructure.

### **Small or Midsize Business (SMB) Vendors**

Two vendors provide cost-effective NAC solutions that target SMBs, but they lack enterprise-class features and functions:

- Napera Networks simplifies the deployment of Microsoft's Network Access Protection — Microsoft's version of network access control. The company sells an Ethernet switch that includes embedded support for MNAP. Organizations that build LANs with Napera switches will not need to purchase add-on appliances or additional software to implement MNAP, provided that their endpoints are MNAP-ready (Microsoft Windows Vista and XP Service Pack 3 include support for MNAP; other operating systems will need an MNAP-compatible agent). Napera switches can be added to existing LANs to protect pain points (conference rooms and so on), or they can be used to upgrade or build new LANs.
- NetClarity's family of NACwall appliances use an agentless (no additional software on the PCs) approach to baseline the health of the endpoints. NACwalls are deployed out of band in LANs, so they install easily and are not in the line of traffic (no additional latency to the network). NACwall appliances interface with existing switches and firewalls to enforce access control. ARP manipulation can also be used to enforce access.

### **Microsoft**

Microsoft embeds NAC functionality (branded as Microsoft Network Access Protection) within its operating systems (Vista and XP Service Pack 3) and within Windows Server 2008. We did not include Microsoft in this year's Magic Quadrant because of the requirement that organizations need to upgrade to the required Microsoft products. None of the other solutions in this Magic Quadrant require an operating system update. However, we will re-evaluate Microsoft and the market penetration of MNAP-ready endpoints in 2010.

### **Added**

- Enterasys' NAC solution is internally developed, and it is able to function in a multivendor environment.
- Nortel's NAC solution is internally developed, and it is able to function in a multivendor environment.
- Trustwave has entered the Magic Quadrant through its February 2009 acquisition of Mirage Networks.

### **Dropped**

Nevis Networks is re-evaluating its strategy for the NAC market.

## Evaluation Criteria

### Ability to Execute

Ability to Execute criteria are:

- *Product/Service*: An evaluation of the features and functions of the vendor's NAC solution. Higher ratings were assigned to solutions with strong guest networking features and to solutions with a comprehensive feature set for baselining endpoints and for enforcing access control.
- *Overall Viability*: Viability includes an assessment of the vendor's overall financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue to invest in an NAC solution.
- *Sales Execution/Pricing*: The vendors' capabilities in all presales activities and the structure that supports them. This includes pricing and negotiation, presales support, and the overall effectiveness of the sales channel.
- *Market Responsiveness and Track Record*: Ability to respond, change direction and be flexible as market dynamics vary. This criterion also considers the vendor's history of responsiveness.
- *Marketing Execution*: This criterion assesses the effectiveness of the vendor's marketing programs and its ability to create awareness and "mind share" in the NAC market.
- *Customer Experience*: Quality of the customer experience, based on reference calls and Gartner client teleconferences.
- *Operations*: The ability of the organization to meet its goals and commitments in an efficient manner. Past performance is weighted heavily.

**Table 1. Ability to Execute Evaluation Criteria**

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	High
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	Standard
Marketing Execution	High
Customer Experience	Standard
Operations	No Rating

Source: Gartner (March 2009)

### Completeness of Vision

Completeness of Vision criteria are:

- *Market Understanding*: Ability of the vendor to understand buyers' needs and translate these needs into NAC products. The ability to anticipate market trends (for example, guest networking) and to quickly adapt via partnerships and/or acquisitions.

- *Marketing Strategy*: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the Web site, advertising, customer programs and positioning statements.
- *Sales Strategy*: The vendor's strategy for selling to its target audience, including an analysis of the appropriate mix of direct and indirect sales channels.
- *Offering (Product) Strategy*: An evaluation of the vendor's strategic product direction, including an analysis of its road map.
- *Business Model*: The soundness and logic of the vendor's underlying value proposition.
- *Vertical/Industry Strategy*: The vendor's strategy for meeting the specific needs of individual vertical markets and market segments (for example, higher education).
- *Innovation*: This criterion includes product leadership and the ability to deliver NAC features and functions that distinguish the vendor from its competitors.
- *Geographic Strategy*: The vendor's strategy for penetrating geographies outside its home or native market.

**Table 2. Completeness of Vision Evaluation Criteria**

<b>Evaluation Criteria</b>	<b>Weighting</b>
Market Understanding	High
Marketing Strategy	Standard
Sales Strategy	Standard
Offering (Product) Strategy	High
Business Model	Standard
Vertical/Industry Strategy	Low
Innovation	Standard
Geographic Strategy	Low

Source: Gartner (March 2009)

## Leaders

Leaders are successful in selling large NAC implementations (5,000 nodes and above) to multiple large enterprises as a primary offering. Leaders are networking and/or security companies that recognized early on that NAC would be an important component of their overall product portfolios and have been first to market with enhanced capabilities as the market matures. Leaders have the resources to maintain their commitment to NAC, have strong channel strength and financial resources, and have demonstrated a strong understanding of the future market direction. Leaders should not equate to a default choice for every buyer, and clients should not assume that they must buy only from vendors in the Leaders quadrant.

## Challengers

Challengers are networking and/or security companies that have been successful in selling NAC to their installed bases. NAC is a strategic component of their overall product portfolios, although they did not show the vision to enter the NAC market as strongly as did the leaders. Challengers generally rapidly match product capabilities that leaders come out with, rather than being first to

market with a needed capability. Challengers are large enough and diversified enough to continue investing in their NAC strategy and can withstand challenges and setbacks more easily than niche vendors.

## Visionaries

Visionaries have led the market in product innovation and/or displayed an early understanding of market forces and trends. They are either smaller pure-play NAC vendors or larger networking and/or security companies. A common theme in visionary vendors is that they don't have significant channel strength and have not succeeded in building installed bases as large as the leaders. Pure-play vendors in the Visionaries quadrant face challenges in moving into the Leaders quadrant, due to the trend of network and security companies embedding NAC functionality in their existing solutions.

## Niche Players

Niche vendors represent a mix of small and large companies. The large companies are network and/or security vendors that have had some success in selling NAC to their traditional installed base, but also face stiff competition from other NAC vendors. Large niche vendors have generally struggled to sell NAC to the broader market. Small niche vendors don't appear often on Gartner clients' shortlists, but some of them are successful in addressing subsets of the overall market. Niche vendors are valid suppliers in the market and often provide solutions targeted to the needs of a particular vertical industry.

## Vendor Strengths and Cautions

### 3Com (TippingPoint)

The TippingPoint NAC solution includes dissolvable and permanent agent-based endpoint baselining, and 802.1X and DHCP enforcement. It also includes the NAC Policy Enforcer, which can provide in-line blocking and can interoperate with any deployed TippingPoint IPS devices. Based on technology from its acquisition of Roving Planet, the TippingPoint NAC Policy Server provides provisioning and administration capabilities for guest access. Appropriate use cases for TippingPoint NAC are existing users of TippingPoint IPS and other enterprises that will take advantage of in-line filtering capabilities.

#### Strengths

- TippingPoint NAC has flexible enforcement options.
- As a leading IPS vendor, TippingPoint has strong internal threat and vulnerability research capabilities.
- TippingPoint customers generally chose TippingPoint NAC because of positive experiences with the performance of TippingPoint Intrusion Prevention System.

#### Cautions

- Although 3Com has settled on a strategy to retain TippingPoint as a business unit, 3Com's overall strategy for security remains unclear. This impacts TippingPoint's ability to compete with larger competitors. 3Com will also need to demonstrate the capability to sell NAC into its installed base of LAN infrastructure products.
- TippingPoint has very few large-scale NAC customers.

## Aruba Networks

Aruba's capabilities in distributed wireless LANs (WLANs) bring it into many NAC deals, because WLANs are widely used for guest access. Aruba's approach to NAC integrates the Endpoint Compliance System (ECS) appliance (which is an OEM solution from Bradford Networks) with its Mobility Controller switches. When Mobility Controllers have been deployed for WLAN use, they can provide in-line stateful policy enforcement to devices that are connected over wireless via an integrated firewall. The Mobility Controllers can also be integrated with Cisco's Network Admission Control, Juniper's Unified Access Control (UAC) and MNAP approaches for wired NAC enforcement. Alternatively, Aruba ECS can be deployed to implement a stand-alone Aruba NAC approach.

### Strengths

- Aruba offers flexible enforcement options, including DHCP, 802.1X, Media Access Control (MAC)-based and in-line enforcement.
- Aruba Mobility Controllers provide network usage and identity-based enforcement profiles.
- Aruba's strength in wireless LANs means it is often used for WLAN-based guest networking. Aruba NAC customers generally report ease of extension from WLAN access to NAC as the primary reason for selecting Aruba.

### Cautions

- Aruba's NAC solution has limited remediation support.
- Because Aruba licenses the ECS technology from OEM Bradford Networks, an acquisition of Bradford by an Aruba competitor could impact Aruba's ability to deliver NAC.
- Where Aruba is not being used for WLANs, the Mobility Controller approach does not compete well with other in-line approaches.

## Bradford Networks

Bradford has primarily targeted the higher education market, where it claims more than 500 NAC customers for its Campus Manager solution. It is well-suited to the demands of university environments because of its ability to deal with heterogeneous, unmanaged endpoints (via a dissolvable agent or via a Nessus scan integrated with its policy server appliance). Bradford also offers a permanent agent. Bradford targets the broader enterprise market via its NAC Director offering. Bradford's solutions are positioned out of band and provide enforcement via ACLs, virtual LANs (VLANs) and DHCP.

### Strengths

- Bradford has strong name brand recognition in the higher education vertical market. Nearly all of Gartner's clients that are colleges or universities include Bradford on their shortlists of NAC vendors.
- Bradford's OEM relationship with Aruba contributed strongly to revenue growth in 2008. Bradford, a privately held company, announced that its sales of its NAC solutions for 2008 were up 87% over 2007.

- Bradford earned visionary points for anticipating the needs of the NAC market. In 2008, it delivered a reasonably priced guest networking package that it can use as a beachhead to sell broader NAC functionality.
- The ability to profile devices (for example, identify an endpoint as a printer or IP phone) represents another innovation for Bradford. Other vendors in this Magic Quadrant offer this function, but all do so by licensing technology from an OEM.

### **Cautions**

- As a small pure-play NAC vendor, Bradford faces a challenging road ahead. Because an endpoint agent is an important component of Bradford's solution, it will continue to face pressure from McAfee, Sophos and Symantec.
- Microsoft's embedded NAP functions also present a challenge to Bradford.
- Bradford's native VPN support is limited to Cisco's concentrators. However, Bradford resells and integrates with an Aruba in-line controller, which enables it to support all VPN concentrators.

### **Check Point**

Check Point's NAC strategy is centered on its Check Point Endpoint Security client, along with a dissolvable agent for use on unmanaged endpoints. The Endpoint Security client provides a strong level of local enforcement and makes NAC easy to deploy for Check Point VPN users. Check Point's large installed base drives many vendors to integrate with Check Point's OPSEC program, so there are several choices of WLANs and switches for NAC control points. Check Point appears to be reinvigorating its IPS-1 intrusion prevention system product line, which should lead to an in-line NAC enforcement capability as well.

### **Strengths**

- Check Point has a very strong channel and a broad range of network security products that can be used as part of an NAC strategy.
- Check Point's large installed base of VPN client software simplifies remote-access NAC deployment.
- Check Point NAC users generally based their selection on the ease of integration of NAC capabilities into overall management of Check Point Endpoint Security client software already in use.

### **Cautions**

- Many of Check Point's NAC OPSEC partners have competing NAC strategies, which will limit their support for Check Point's approach.
- Check Point's strength in NAC depends on its ability to compete in the EPP market against entrenched antivirus players (see "Magic Quadrant for Endpoint Protection Platforms, 2007"). Check Point is not a leader in that market, so its NAC solution is at a disadvantage for the majority of enterprise desktop applications.
- Although Check Point does support secure remote guest access, it does not provide the capabilities for easy administration and sponsorship of guest access.

## Cisco

Cisco offers a family of NAC appliances. Its NAC Server has the flexibility to be deployed in band or out of band. The out-of-band positioning improves the scalability of the NAC appliance, but it is currently limited to implementations with Cisco Catalyst switches only. Endpoint baselining is accomplished via an optional endpoint agent (permanent or dissolvable) or via a scanning function (using Nessus signatures). Other members of the product family include the NAC Guest Server and the NAC Profiler (both products are from OEM deals with small vendors). The Guest Server provides the provisioning, management and reporting capabilities for wired and wireless guest networks. The Cisco NAC Profiler makes it easier to discover and monitor nonauthenticating devices (for example, IP phones and printers) in an NAC environment.

### Strengths

- Cisco is well-positioned to sell complementary NAC solutions to its installed base of wired and wireless LAN and VPN customers. It already has more NAC customers than any other vendor in this Magic Quadrant.
- Cisco's NAC Guest Server appliance and NAC Profiler appliance, both available since 2007, are a reflection that the company adapts quickly to trends in the NAC market.
- Cisco offers an NAC module for its Integrated Services Router (ISR), making it easier and less expensive to implement NAC in remote offices.

### Cautions

- Cisco has a history of stalling the market with NAC. It abandoned its original framework concept (based on partnerships with other security companies), and its partnership with Microsoft has yielded a negligible installed base of NAC/NAP customers.
- Cisco's TrustSec initiative (which was announced in 2007), an identity-aware networking solution, is still a question mark. Cisco has yet to ship TrustSec-enabled Catalyst switches or other elements of the TrustSec solution.
- Cisco needs to provide a more detailed road map for its authentication and NAC-related solutions. Questions persist around its agent strategy (separate agents for 802.1X and for NAC) and TrustSec's role in relation to NAC.
- Vendor lock-in remains a concern among Gartner clients that have evaluated Cisco NAC.
- Gartner clients consistently report that Cisco's NAC proposals are more expensive than proposals from its competitors.

## ConSentry Networks

ConSentry offers an in-line approach to NAC via two options — Ethernet switches and LAN appliances that are positioned between an edge switch and a core switch. Both products are based on ConSentry's programmable application-specific integrated circuit (ASIC) technology. ConSentry also offers permanent and dissolvable agents for endpoint baselining. From the start, ConSentry focused on building in "identity aware" capabilities, supporting advanced features that can apply granular access controls based on who is using a particular endpoint. In early 2009, ConSentry obtained \$9.4 million in venture funding, at a time when such funding was hard to obtain. ConSentry users based their selection on the flexibility and visibility provided by the ConSentry in-line approach.

## Strengths

- ConSentry offers advanced identity-aware features, including the ability to control user access to applications and specific files.
- ConSentry NAC deploys in-line and flexible enforcement options, including the ability to allow, deny and rate-limit traffic. It also offers logging capabilities.
- ConSentry's InSight Command Center network management tool goes beyond the typical endpoint compliance reporting to provide detailed user and application visibility (for example, questionable traffic and applications such as games and peer-to-peer sharing).

## Cautions

- ConSentry's viability is largely dependent on its success in attacking the LAN switch market. The current economic climate will make this more difficult.
- ConSentry has very limited channel strength.
- ConSentry's NAC solution has limited native guest networking sponsorship and administration features.

## Enterasys

Enterasys offers out-of-band (NAC Gateway) and in-line (NAC Controller) components. The NAC Controller enables NAC for older third-party switches that do not support 802.1X or RADIUS-based authentication. The Enterasys solution performs endpoint baselining via agents (permanent and dissolvable) and agentless technology. The primary usage case for Enterasys NAC is Enterasys switch and wireless LAN customers, although the solution is capable of supporting non-Enterasys environments.

## Strengths

- Enterasys' viability has improved now that it is part of Siemens Enterprise Communications (formed October 2008), a Gores Group company. The Gores Group and Siemens have pledged to invest up to €350 million in the joint venture.
- Enterasys has integrated its Dragon IPS solution with its NAC offering, so that it can quarantine endpoints that Dragon identifies as suspicious.
- When implemented with Enterasys N-Series switches, NAC policies can be applied for each unique flow (by tracking the source/destination address pairing). For example, granular policies can be established to implement bandwidth rate limits or trigger deep packet inspection. The N-Series switches provide the flow-based intelligence, so any NAC solution can set these policies, although it is easier to do so with the Enterasys Policy Manager software.

## Cautions

- Enterasys has had limited success in selling NAC to the broader market (beyond Enterasys' installed base of LAN switch customers).
- Enterasys NAC provides identity-aware networking capabilities, but needs to improve per-user audit trail reports.

## ForeScout

ForeScout's CounterACT NAC product is an out-of-band NAC appliance that primarily takes an agentless approach to baselining endpoints (via credential access). ForeScout can also baseline endpoints with persistent or dissolvable agents. CounterACT includes the ability to detect malicious traffic (this capability is included within the product — it does not require integration with a separate IPS appliance). Malicious traffic can be contained using several methods, including VLAN steering, ACLs and TCP resets.

### Strengths

- ForeScout has some of the largest NAC deployments (that is, number of endpoints) in the market.
- ForeScout's customers consistently report that its out-of-band, appliance-based solution is easy to deploy and manage.
- The CounterACT appliance provides a good mix of preconnect endpoint baselining with postconnect monitoring and containment features.

### Cautions

- The market trend toward embedded NAC features is a threat to ForeScout, which is largely a pure-play NAC vendor.
- ForeScout lacks an OEM deal with a large partner in North America or Europe. Several other small NAC vendors benefit from this type of partnership in their sales and distribution channels.

## Impulse Point

Impulse Point has primarily targeted the higher education market with its Safe Connect solution. Safe Connect is designed to enforce network access at Layer 3, via ACLs on routers or Layer 3 switches. This approach is suitable for some university environments, although it does not meet the enforcement requirements of most corporate environments, where enforcement is required at Layer 2 (in the LAN). Safe Connect also supports 802.1X enforcement. Endpoint baselining is provided via an agent (permanent or dissolvable), which can also provide self-enforcement. Unlike most endpoint software NAC solutions, which require scheduled agent scans, the agent runs continuously on the endpoints and can immediately detect endpoint configuration changes. Impulse Point delivers its solution as a managed service, whereby it manages updates (patches and antivirus status) to its policy server and houses daily policy configuration backups. Safe Connect is available as an appliance or via software (it is certified to run in a virtualized VMware environment).

### Strengths

- Impulse Point provides a scalable and relatively inexpensive approach to NAC. At 10,000 nodes and above, Impulse Point's pricing model is highly favorable.
- The Safe Connect solution includes several features that are targeted at the higher education vertical market.

### Cautions

- Safe Connect's Layer 3-based enforcement mechanism (ACLs on routers) makes it a poor choice for enterprises seeking to implement guest networks in corporate

environments. This approach does not prevent an endpoint from gaining LAN access. Safe Connect does support guest networking via 802.1X.

- Outside of the higher education market, Impulse Point suffers from low market visibility (due to its small size and its limited resources).
- Impulse Point Customers have expressed that its native graphical reporting capabilities are lacking (although log information can be exported to external database stores and customized).

## InfoExpress

InfoExpress provides the CyberGatekeeper line of NAC solutions, CyberArmor personal firewall technology and a VPN product. The NAC solution is composed of an endpoint agent in combination with network-based enforcement. Persistent or dissolvable agents can be used to baseline endpoints. CyberGatekeeper appliances provide in-line and out-of-band enforcement for LAN, wireless LAN and VPN connections, and 802.1X-based control is also supported. CyberGatekeeper's in-line enforcement mechanism works with all major Internet Protocol security (IPsec) VPN gateways (by dropping/filtering packets). InfoExpress also supports Juniper's Secure Sockets Layer (SSL) VPN gateways. InfoExpress also sells a software-based NAC solution known as Dynamic NAC, which uses permanent agents to implement ARP-based enforcement of noncompliant endpoints.

## Strengths

- InfoExpress' CyberGatekeeper NAC solution is a good complement to its personal firewall and VPN offerings.
- Dynamic NAC can be a cost-effective solution for organizations that have many sparsely populated branch offices, because it doesn't require additional hardware.
- InfoExpress renewed focus on its indirect sales and distribution channel and recently added Alcatel-Lucent as a channel partner.

## Cautions

- The primary challenge for InfoExpress is its size, relative to other endpoint security vendors that provide NAC. Although it can sell its NAC solution to its VPN and personal firewall customers, this potential customer base is small compared with major endpoint security vendors that also offer NAC solutions.
- Although customer satisfaction with InfoExpress remains high, the company's technology differentiation has eroded as large competitors such as McAfee and Symantec have expanded their endpoint security solutions to include better personal firewalls and NAC support.

## Insightix

Insightix is known mostly for its Visibility network discovery and monitoring technology that provides dynamic endpoint profiling. By using Visibility to build a baseline of every device connected to the network, Insightix NAC can quickly determine if a new connection represents a known or unknown device and then use ARP manipulation to enforce quarantining on suspect devices. Insightix provides a dissolvable agent for dealing with unmanaged endpoints. The appropriate use case for Insightix NAC is customers of Insightix's Visibility network discovery solution that want to add inexpensive NAC functionality.

## Strengths

- Insightix has very strong capabilities for detecting and profiling devices on the network.
- Similar to Mirage Networks, Insightix's ARP manipulation approach provides a flexible enforcement mechanism.

## Cautions

- Insightix had multiple management changes in 2008 and has been more focused on the network discovery market than on the NAC market.
- Insightix has very limited channel support in North America, although it has strong partners in Europe. The company has no meaningful technology partners.
- Remediation support is limited.

## Juniper Networks

Juniper's Unified Access Control NAC product builds on Juniper's strength in the SSL VPN and in-line network IPS markets and on its acquisition of Funk Software's RADIUS and 802.1X products. Juniper UAC provides a wide array of enforcement options, lacking only DHCP enforcement. When deployed in conjunction with UAC, Juniper's firewalls and EX LAN switches become identity-aware and are able to enforce policies based on the user's role.

## Strengths

- Unified Access Control is a strong solution for implementing device policies and/or user policies, which enables Juniper to compete effectively for opportunities in all four NAC usage cases outlined in the Market Overview section.
- Juniper has some of the largest NAC deployments (that is, number of endpoints) in the market.
- Juniper has been a driver for open NAC standards and was an early partner with Microsoft and its MNAP efforts. Juniper is well-positioned to grow its NAC business as more PCs become MNAP-ready.

## Cautions

- Like other network infrastructure vendors, Juniper faces challenges in convincing its customers to install permanent NAC clients on their endpoints. (Juniper's solution does not require a permanent client, but it is the preferred solution for managed endpoints.)
- Some Juniper users reported integration challenges between Juniper components (the Steel-Belted RADIUS Server did not integrate seamlessly with Juniper's Infranet Controller).
- Juniper was a new entrant in the LAN switching market in 2008 and, therefore, does not have any meaningful installed base to which it can sell complementary NAC solutions.

## McAfee

In 2008, McAfee overhauled what had been a failed NAC strategy. Through a combination of acquisitions and internal development, it now owns a broad set of NAC technologies. Its NAC technology portfolio includes in-band (via its IPS and NAC-only appliances) and out-of-band (from purchasing the assets of Lockdown Networks) monitoring and enforcement capabilities. McAfee

also owns the components to implement device-based and user-based policies. Thus, if McAfee is able to execute, it will be able to address all four NAC usage cases outlined in the Market Overview section.

### **Strengths**

- The out-of-band NAC technology that McAfee gained by acquiring the assets of failed NAC vendor Lockdown Networks is appropriate for many small and midsize businesses and will be a good fit for McAfee's distribution channel. McAfee has plans to ship this product in 2H09.
- Technology from Securify (which McAfee gained by way of its Secure Computing acquisition) should enable McAfee to strengthen its identity-aware networking capabilities.
- McAfee's acquisition of Secure Computing should strengthen its ability to sell its IPS-based NAC solution (a McAfee-developed product). If it executes, McAfee will have an advantage over Sophos and Symantec in reaching network security managers, who are commonly the buyers of NAC.
- McAfee's large installed base of EPP customers represents a good target for its NAC solution.

### **Cautions**

- McAfee is essentially a late entrant in the NAC market. It has been shipping its flagship IPS-based NAC offering only since September 2008 and NAC Appliance since December 2008, and it needs to demonstrate that it can succeed with these products.
- Organizations should carefully check references for the IPS-based NAC and NAC Appliance offerings, because they are new to the market.
- McAfee has a lot to accomplish with its acquisitions of Secure Computing (including Securify) and the assets of Lockdown Networks. It needs to articulate a clearer road map and demonstrate that it is capable of delivering on its plans.

### **Trustwave (Mirage Networks)**

Mirage Networks' Endpoint Control NAC appliance monitors endpoints for anomalous traffic patterns and uses ARP manipulation to isolate suspect endpoints. This technique allows the Endpoint Control appliance to be installed out of band but effectively to insert itself in line and provide selective enforcement. This agentless approach is often a very good fit for heterogeneous networks. Mirage has a number of patents on aspects of this technique. Mirage offers a range of appliances with up to 1 Gbps throughput and is generally the least expensive NAC offering in head-to-head competitions. During the writing of this Magic Quadrant, Mirage Networks was acquired by Trustwave, a Payment Card Industry (PCI) Qualified Security Assessor and managed security service provider. Trustwave is primarily a managed service company, not a product vendor. The future appropriate use case for Mirage Networks' NAC will be enterprises that are looking for an externally managed NAC solution to meet PCI compliance needs.

### **Strengths**

- Mirage is generally the lowest-priced NAC approach.
- Mirage's ARP manipulation approach, similar to Insightix, offers flexible enforcement options.

## Cautions

- Mirage was recently acquired by Trustwave, a PCI Qualified Security Assessor and managed service firm. Trustwave offers managed services and typically does not sell or support products. The Trustwave acquisition may also cause conflict with existing Mirage service partners, such as AT&T and IBM.
- Mirage's dependence on ARP-based enforcement limits its ability to enforce NAC policies in an SSL VPN environment.
- Mirage does not offer a permanent agent (although it does offer an optional dissolvable agent and an agentless option for endpoint baselining).

## Nortel

Nortel has evolved its Secure Network Access (SNA) solution to operate in multivendor LAN switch environments (Nortel's early NAC solutions were targeted at Nortel-centric LANs). The SNA Switch (SNAS) acts as an out-of-band policy server and communicates to policy enforcement points (for example, switches, routers and wireless controllers). The primary usage case for Nortel NAC is Nortel switch and wireless LAN customers, although the solution is capable of supporting non-Nortel environments (more enforcement options are available with Nortel switches).

## Strengths

- SNA is tightly integrated with MNAP. Nortel's policy server can take the place of Microsoft's Network Policy Server, thereby simplifying migration to an MNAP/Nortel environment (Microsoft for endpoint baselining and Nortel for policy decisions and enforcement).
- Nortel has acquired certain intellectual property of Identity Engines. The acquisition gives Nortel strong 802.1X technology and a strong guest networking solution that is complete with user provisioning, reporting and management capabilities. Nortel is also working with the OpenSEA Alliance and its open-source 802.1X supplicant.

## Cautions

- In January 2009, Nortel filed for creditor protection in Canada, Chapter 11 bankruptcy protection in the U.S. and administration in the U.K. Until Nortel's poor financial situation improves, it faces challenges in selling NAC to its installed base.
- Nortel's NAC solution has little visibility in the broader market (beyond Nortel's installed base).

## Sophos

Sophos offers two NAC solutions (both are based on technology from its 2007 acquisition of Endforce). Sophos' EPP suite, Endpoint Security and Control, provides basic NAC policy, reporting and enforcement capabilities. Sophos' NAC Advanced solution, which requires a separate agent and management console, provides more-advanced features, such as custom policy creation, stronger reporting capabilities and more enforcement options (including support for 802.1X). Sophos' solutions are optimized for preconnect NAC. Appropriate usage cases for Sophos are existing Sophos endpoint security customers that seek to add NAC via a unified agent (when NAC Advanced is integrated with Sophos Endpoint Security and Control). Non-Sophos customers can also implement Sophos' NAC Advanced solution.

## Strengths

- Basic NAC functions are embedded (at no extra charge) in Sophos' Endpoint Security and Control suite.
- Sophos' installed base of EPP customers represents a good target for its NAC solution.

## Cautions

- Sophos is behind its major EPP suite competitors (McAfee and Symantec) in delivering an integrated NAC and EPP agent architecture. Sophos will require a separate NAC agent in its EPP suite until late in 2009 when it introduces a unified agent with the suite.
- The Sophos endpoint security base is much smaller than its primary endpoint security competitors (Symantec and McAfee).
- As an EPP vendor, Sophos' challenge is to get the attention of the network team that typically makes the NAC decision.
- Some Sophos customers said that its reporting is cumbersome (the database schema is complex), which makes customized reporting difficult.

## StillSecure

StillSecure provides NAC, IPS and vulnerability management solutions. The Safe Access solution has broad preconnect NAC capabilities and multiple enforcement options, including in-line support for VPNs. Baselineing can be achieved via a persistent agent, a dynamic agent or an agentless scan. Access control can be implemented with 802.1X, DHCP or agent-based self-enforcement. StillSecure targets large accounts directly via its small sales force and is also pursuing an OEM strategy. It licenses its technology to several partners, including Extreme Networks, HP ProCurve and Novell.

## Strengths

- StillSecure provides a flexible solution (multiple baselineing, as well as in-band and out-of-band enforcement options) for preconnect NAC device policies.
- The company has integrated its IPS solution with Safe Access, so that it can quarantine endpoints that its IPS identifies as suspicious.
- StillSecure has a strong presence and some large-scale implementations in the U.S. military.

## Cautions

- StillSecure is a small company that struggles with low visibility and market awareness (outside of the military), which hampers its direct sales efforts.
- StillSecure's acquisition of security managed service vendor ProtectPoint (in January 2009) is an indication that, after several years of focusing on NAC, it is now redirecting resources back to develop its IPS and vulnerability management offerings.
- StillSecure is late to the market with guest networking functionality — specifically, provisioning and reporting capabilities.
- OEM relationships have been ineffective and have done little to help StillSecure expand its customer base.

## Symantec

Symantec provides two solutions for NAC. Symantec Network Access Control is an NAC point solution. Symantec Endpoint Protection 11.0 provides NAC through a common agent that also delivers malicious code protection and intrusion prevention. Symantec Endpoint Protection Manager provides policy management for both NAC solutions. Endpoint baselining is provided via permanent or dissolvable agents or via an agentless scanning option. Access control is provided via appliances, with separate models for 802.1X, DHCP and in-line (packet filtering) enforcement. A DHCP plug-in is available for Microsoft's DHCP server, and Symantec's persistent NAC agent also provides self-enforcement. Symantec has completed its initial integration with Altiris PC life cycle management technology to provide additional automated mitigation options.

### Strengths

- Symantec is well-positioned in the NAC market, because it can target its installed base of EPP customers to upgrade to NAC.
- Symantec's strength is in preconnect NAC, where it offers multiple endpoint baselining and multiple enforcement options.

### Cautions

- Symantec's ability to leverage its installed base for NAC has been limited to some degree by issues with Symantec Endpoint Protection 11.0 (Symantec customers report that these issues have been reduced with the most recent maintenance release).
- Symantec's NAC solution has limited guest networking sponsorship and administration features.
- Like its competitors in the endpoint security market, Symantec's challenge is to get the attention of the network team that typically makes the NAC decision.

## RECOMMENDED READING

---

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"Network Access Control in 2009 and Beyond"

"Simplify the NAC Vendor Selection Process"

"Introducing the Identity-Aware Network"

### Note 1

#### Change in Gartner's Market-Sizing Methodology

In 2009, we modified our calculations for recognizing revenue when NAC is delivered as an embedded feature. Applying this methodology change to our 2007 analysis results in an estimated market size of \$146 million and reflects 2008 NAC market growth of 51%.

### Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope

one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

## Evaluation Criteria Definitions

### Ability to Execute

**Product/Service:** An evaluation of the features and functions of the vendor's NAC solution. Higher ratings were assigned to solutions with strong guest networking features and to solutions with a comprehensive feature set for baselining endpoints and for enforcing access control.

**Overall Viability:** Viability includes an assessment of the vendor's overall financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue to invest in an NAC solution.

**Sales Execution/Pricing:** The vendors' capabilities in all presales activities and the structure that supports them. This includes pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

**Market Responsiveness and Track Record:** Ability to respond, change direction and be flexible as market dynamics vary. This criterion also considers the vendor's history of responsiveness.

**Marketing Execution:** This criterion assesses the effectiveness of the vendor's marketing programs and its ability to create awareness and "mind share" in the NAC market.

**Customer Experience:** Quality of the customer experience, based on reference calls and Gartner client teleconferences.

**Operations:** The ability of the organization to meet its goals and commitments in an efficient manner. Past performance is weighted heavily.

### Completeness of Vision

**Market Understanding:** Ability of the vendor to understand buyers' needs and translate these needs into NAC products. The ability to anticipate market trends (for example, guest networking) and to quickly adapt via partnerships and/or acquisitions.

**Marketing Strategy:** A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the Web site, advertising, customer programs and positioning statements.

**Sales Strategy:** The vendor's strategy for selling to its target audience, including an analysis of the appropriate mix of direct and indirect sales channels.

**Offering (Product) Strategy:** An evaluation of the vendor's strategic product direction, including an analysis of its road map.

**Business Model:** The soundness and logic of the vendor's underlying value proposition.

**Vertical/Industry Strategy:** The vendor's strategy for meeting the specific needs of individual vertical markets and market segments (for example, higher education).

**Innovation:** This criterion includes product leadership and the ability to deliver NAC features and functions that distinguish the vendor from its competitors.

**Geographic Strategy:** The vendor's strategy for penetrating geographies outside its home or native market.

## **REGIONAL HEADQUARTERS**

---

### **Corporate Headquarters**

56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

### **European Headquarters**

Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

### **Asia/Pacific Headquarters**

Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

### **Japan Headquarters**

Gartner Japan Ltd.  
Aobadai Hills, 6F  
7-7, Aobadai, 4-chome  
Meguro-ku, Tokyo 153-0042  
JAPAN  
+81 3 3481 3670

### **Latin America Headquarters**

Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509