Magic Quadrant for Network Access Control

12 December 2013 ID:G00249599

Analyst(s): Lawrence Orans

VIEW SUMMARY

NAC vendors are beginning to differentiate their solutions through their breadth of integrations with other products. Mobile device management integrations are a requirement to address the BYOD trend, and integrations with firewalls and other security components enable sharing of contextual data.

Market Definition/Description

The "bring your own device" (BYOD) trend has transformed the network access control (NAC) market. While the original driver for NAC was the need to enforce access policies for Windows PCs, the primary driver now is controlling the access of personally owned devices. Today, enterprises are using NAC to adapt to the environments of heterogeneous endpoints, and to decide which devices, and which users, will gain network access. NAC policies dictate which devices are granted full network access, which are blocked from the network, and which ones are granted limited network access. Partnerships with mobile device management (MDM) vendors have become an important factor in the NAC market, as NAC solutions rely on input from MDM solutions for information about the status and configuration of mobile devices.

Enterprises are increasingly integrating their NAC implementations with other security components. Integrations with security information and event management (SIEM) are the most common, followed by integrations with next-generation firewalls (NGFWs). Several vendors provide bidirectional integrations, so that NAC solutions can share data and also act on alerts from these systems (for example, removing a device from the network). Some vendors have also begun to integrate their NAC solutions with advanced threat defense offerings to remove compromised endpoints from the network. Integrating with other network and security solutions is not a primary driver for adopting NAC, but enterprises are progressively implementing these integrations after the initial rollout of NAC.

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Network Access Control

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

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

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

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

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Source: Gartner (December 2013)

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

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

Return to Top

Vendor Strengths and Cautions

Aruba Networks

Aruba's ClearPass NAC offering is a Remote Authentication Dial-In User Service (RADIUS)-based solution that is available in a family of hardware and virtual appliances. It also offers an MDM solution known as WorkSpace. Aruba, based in Sunnyvale, California, moves into the Leaders quadrant this year due to the overall strong growth of ClearPass and a demonstrated ability to win large opportunities. Aruba's customers and any enterprise that needs an NAC solution capable of supporting heterogeneous endpoints and heterogeneous networks should consider ClearPass.

Strengths

Aruba's 802.1X innovations include a built-in certificate authority to ClearPass, which eases BYOD implementations by not requiring an external certificate authority. The ClearPass Onboard module provides the ability to revoke and delete certificates (for example, when devices are lost or stolen).

ClearPass offers a strong guest network application. Guest portals can be customized with a wide range of options, including localized language support. Granular policies allow guests to share printers and projectors that use Apple's Bonjour protocol.

Aruba provides detailed diagnostic information to assist network administrators in troubleshooting failed 802.1X authentications.

Cautions

Aruba lags behind several competitors in its breadth of prepackaged integrations with SIEM vendors and advanced threat defense vendors.

Aruba faces a difficult balancing act with its WorkSpace MDM offering, because it is now competing with the same MDM vendors that it partners with to enhance ClearPass.

Aruba is still ramping up its value-added reseller (VAR) channel's ability to sell and support ClearPass. Before purchasing ClearPass from an Aruba partner, verify that the partner is ClearPass-certified.

Return to Top

Auconet

Auconet was founded in 1998 as a system integrator, and began shipping NAC solutions in 2005. It is a privately held company based in Germany, with offices in Austria, Switzerland and the U.S. Auconet is deployed most commonly as an agentless solution, because its RADIUS-based policy server supports native 802.1X supplicants embedded in multiple operating systems. The policy server is available as a hardware appliance or a virtual appliance. Auconet also offers a permanent agent on Windows and

some Unix/Linux platforms (excluding Mac OS X). Organizations within the company's geographic reach that have a heterogeneous network infrastructure should consider Auconet.

Strengths

Auconet has several large customers, including some implementations with more than 100,000 endpoints.

Customer references consistently comment favorably on the solution's agentless approach and its ease of implementation.

Auconet complements its NAC solution with good network management features. For example, it can run dynamic scripts on any command-line interface (CLI)-supported device in the network. This capability enables Auconet to automatically respond to alerts generated from other devices. Customers can use this feature to issue a rate-limiting command to switch ports in response to a suspicious traffic alert.

Cautions

Auconet's BYOD strategy is limited. At the time of this report, it has only integrated with Citrix's XenMobile solution.

The solution lacks a supplicant configuration tool, which is an important ease-of-use feature for 802.1X-based solutions.

Auconet has a limited geographic reach and only a small but growing presence in the U.S. Customers and prospects outside of Europe may face challenges in obtaining presales and postsales support from the company.

Return to Top

Bradford Networks

Bradford Networks is a privately held company based in Cambridge, Massachusetts, that has been delivering NAC solutions since 2001. Its Network Sentry NAC product is available in hardware appliances, in a virtual appliance and as a cloud service. Bradford Networks' NAC products should be considered by enterprises with heterogeneous networks and wide mixes of endpoint devices.

Strengths

Bradford has a broad set of technology partnerships. It has published a set of APIs as a component of its Network Sentry SmartEdge Platform that enables other network and security vendors to integrate bidirectionally with its NAC solution and share contextual data. Several vendors in each of the following categories have integrated with Network Sentry: MDM, SIEM, intrusion prevention systems (IPSs), NGFWs and advanced threat defense. Network Sentry can enforce policies after receiving alerts from these systems.

Bradford offers a unique cloud-based analytics service that helps its customers analyze trends about devices and users that connect to their networks. Customers use this information to develop network access policies and to plan for wireless LAN capacity.

Customers of HP's and Xirrus' wireless LAN solutions can benefit from integrations with Bradford. HP has integrated Bradford's authentication component, and Xirrus licenses Bradford's technology, which it packages as its NAC solution.

Cautions

The vast majority of Bradford's customers are in North America. Prospective customers outside of North America should validate that Bradford's partners can provide an appropriate level of support in their respective regions.

Some reference customers requested improvements in the Network Sentry graphical user interface (GUI).

Return to Top

Cisco

Cisco is headquartered in San Jose, California. Its Identity Services Engine (ISE) policy server is RADIUS-based, which enables Cisco to support authentication in heterogeneous network infrastructure environments (although advanced NAC features will require Cisco components). ISE is available in hardware appliances and also as a virtual server. ISE software is available in three versions: The Base package supports 802.1X and guest provisioning, and the Advanced package supports endpoint baselining (posture assessment), granular identity policies and other more sophisticated features. A Wireless package supports advanced functionality for wireless devices only. Cisco wired and wireless customers should consider ISE, especially when the Cisco AnyConnect endpoint client will be in use.

Strengths

ISE has several API-level integrations with MDM vendors (including AirWatch and MobileIron) and SIEM vendors (such as ArcSight and Splunk), in addition to its integration with Lancope. Separately, Cisco's Platform Exchange Grid (pxGrid) initiative will broaden its scope of partnerships for ISE. pxGrid will enable network and security solutions to coordinate the sharing of contextual information (such as identity and location) through ISE. A limited set of pxGrid integrations will be available in 1H14, although Cisco needs to attract many more technology partners in more markets to deliver on its vision for pxGrid.

Device profiling capability is embedded in Cisco switches and wireless controllers (this may require firmware upgrades), eliminating the need to deploy stand-alone profiling sensors in the network. The ISE server can identify and classify endpoints using templates that are provided by Cisco or defined by an administrator. ISE uses a combination of active and passive profiling techniques.

Cisco's support of identity tags (which it calls TrustSec SGA) in the Ethernet frame (via a proprietary enhancement to the 802.1AE standard) enables its more advanced customers to enforce granular identity-based policies on some Cisco LAN, WLAN and firewall products. Most organizations will require infrastructure upgrades to benefit from this feature.

Cautions

To benefit from the features in the Advanced License of ISE (for example, endpoint profiling), the firmware on Cisco switches and wireless access points needs to be at recent levels. In large enterprises, network administrators may need to update hundreds or thousands of Cisco devices.

Cisco has two NAC agents — one to support VPN access (Cisco VPN AnyConnect Client) and one to support the capabilities of the ISE Advanced License (Cisco Network Admission Control Agent). Customers that need NAC for VPN and advanced NAC functionality will need both agents. Cisco plans to integrate its Network Admission Control Agent with the VPN AnyConnect Client in 1H14, although the integration was initially planned for 2013.

Several Cisco references objected to the subscription-based licensing model and the overall cost of the ISE solution.

Return to Top

Extreme Networks (Enterasys)

In November 2013, Extreme Networks announced that it had completed its acquisition of Enterasys Networks. Extreme, which is based in San Jose, California, will sell the Enterasys NAC solution and the broader Enterasys security product portfolio, including IPS and SIEM products. Enterasys' NAC offering includes out-of-band (NAC Gateway) and in-line (NAC Controller) appliances (also available as virtual appliances). The primary use case for Enterasys NAC is Enterasys switch and WLAN customers, although the solution is capable of supporting non-Enterasys environments.

Strengths

Enterasys' tight integration of its NAC solution with its LAN switch product family enables granular policy enforcement. Policies may permit, deny, rate-limit and apply other controls to traffic based on user identity, time, location, end system and user groups.

Enterasys has a good BYOD strategy. Its Mobile IAM component enables it to integrate with several MDM solutions, including AirWatch, JAMF Software, McAfee and MobileIron.

Enterasys customers consistently highlight the company's service and support as strengths.

Cautions

Enterasys may face challenges executing its NAC road map in 2014, as it may experience distractions as a result of its acquisition by Extreme.

Enterasys suffers from limited brand awareness in the NAC market. Gartner clients rarely include Enterasys on their shortlists when evaluating NAC vendors. The acquisition by Extreme will only marginally improve the awareness issue, given Extreme's small installed base of LAN infrastructure equipment.

Return to Top

ForeScout Technologies

ForeScout Technologies is a privately held company based in Campbell, California, that sells the CounterACT family of hardware and virtual appliances. Although ForeScout offers optional agents, its clientless approach eases the support of Windows, Mac OS X and Linux endpoints. ForeScout should be considered for midsize and large NAC deployments.

Strengths

ForeScout has a strong partnership strategy for integrating with other network and security vendors. It has published a set of APIs, known as ControlFabric, to enable these vendors to integrate their solutions and share contextual data with CounterACT. Vendors in these markets have used ControlFabric to integrate bidirectionally with CounterACT: SIEM, NGFWs, MDM, vulnerability assessment and advanced threat defense. CounterACT can enforce policies after receiving alerts from these systems.

ForeScout has a strong BYOD strategy. In addition to supporting integrations with several MDM vendors, it also sells a ForeScout-branded MDM solution (an OEM of Fiberlink MaaS360; in November 2013, IBM announced its intention to acquire Fiberlink), and it offers the ForeScout Mobile product. The latter is an "MDM-lite" solution that enforces device policies and reports health and configuration status back to the CounterACT appliance.

Users continue to cite ease of deployment, flexible enforcement methods and network visibility as primary selection criteria.

ForeScout has some of the largest active deployments of all vendors.

Cautions

Obtaining postadmission threat protection in distributed environments requires CounterACT appliances at each remote location, which drives up the cost of deployment. ForeScout customers have the option of implementing CounterACT appliances in a centralized approach, which is less expensive, but also reduces ForeScout's threat protection functionality.

In its most commonly implemented approach, CounterACT is positioned on Switched Port Analyzer (SPAN) or "mirror" ports on core network switches. Network administrators need to ensure the availability of these ports in their networks.

ForeScout charges an additional licensing fee for its ControlFabric modules. (Many vendors include support for third-party integrations in their base pricing.)

Return to Top

Impulse Point

Based in Lakeland, Florida, and founded in 2007, Impulse Point continues its focus on the higher education and K-12 markets. Impulse Point delivers its flagship SafeConnect solution as a managed service, which includes system monitoring, problem determination and resolution, updates to device type, antivirus and OS profiling recognition, and remote backup of policy configuration data. All Impulse Point products can be implemented as a hardware or virtual appliance. Education institutions should consider Impulse Point.

Strengths

Feedback from Impulse Point customers continues to indicate that SafeConnect can be quickly implemented. Its Layer 3 approach to enforcement eliminates the need to test compatibility at Layer 2 (at the LAN switch level).

The Identity Publisher feature correlates device and user identity information and exports it to multiple third-party sources (such as AirWatch, Exinda, Procera Networks, iboss Network Security, Palo Alto Networks and Fortinet), which enables identity-based policies. For example, for a specific user, the integrated solution can provision how much bandwidth all of that user's devices are consuming, and can apply the appropriate policy.

Impulse Point customers consistently point to the company's service and support as strengths.

Cautions

SafeConnect lacks a historical reporting feature (for example, reporting on the number of devices quarantined in the past month).

Impulse Point has had limited success in penetrating the corporate environment. When implemented with Layer 3 enforcement, its most commonly deployed approach, Impulse Point does not meet the needs of enterprises that require switch-based (Layer 2) enforcement. Impulse Point has addressed this limitation by enhancing its support for 802.1X and adding Layer 2 enforcement capabilities for wired and wireless LANs. Since these new capabilities have only been available since October 2013, prospective customers should perform thorough testing before implementing in production environments.

SafeConnect provides limited troubleshooting data for failed 802.1X authentications. For example, network administrators must search through error logs because failed authentication errors are not readily highlighted in the user interface.

Return to Top

InfoExpress

Founded in 1993, InfoExpress is a privately held company based in Mountain View, California, that is largely focused on the NAC market. Its CGX solution is available as a hardware appliance and a virtual appliance. Enterprises with a heterogeneous infrastructure should consider InfoExpress.

Strengths

CGX correlates data from multiple sources (for example, InfoExpress endpoint agents, Syslogs, Nmap data and MobileIron) to enable more-granular NAC policies. By analyzing when devices change state, CGX can enforce the appropriate policy. For example, when a mobile device reported as stolen reappears on the network, CGX can quarantine the device.

InfoExpress offers endpoint agents for a wide variety of operating systems, including Windows, Mac OS X, Apple iOS, Android and Linux.

Dynamic NAC (an agent-based Address Resolution Protocol [ARP] enforcement solution) and multiple other enforcement options help facilitate implementation of CGX across complex networks.

Cautions

InfoExpress lacks a broad set of technology integration with security solutions. For example, it does not have a bidirectional integration with any NGFWs or IPSs, and it only integrates with one MDM vendor (MobileIron).

InfoExpress' lack of marketing focus hampers its ability to differentiate its product and contributes to the company's low visibility among Gartner clients.

The loss of Alcatel-Lucent as a value-added reseller partner for CGX has weakened InfoExpress' sales channel, particularly in Europe. Alcatel-Lucent had been reselling CGX to its network infrastructure customers. It still resells InfoExpress' original CyberGatekeeper NAC solution.

Return to Top

Juniper Networks

In 2013, Juniper, based in Sunnyvale, California, renamed its NAC solution Junos Pulse Policy Secure and enhanced its management console with an internally developed solution (previously, the management console was based on technology licensed from IBM). Junos Pulse Policy Secure is available in a family of hardware and virtual appliances. The solution is available in two packages — as a basic RADIUS server (for authentication only) or a full NAC offering. The latter option can be RADIUS-based or non-RADIUS-based (in which case, policy enforcement is implemented via Juniper firewalls). Junos Pulse Policy Secure should be considered where Juniper IPS, SSL VPN gateway, firewall and LAN switch products are in use, and where enterprises seek an 802.1X standards-based solution.

Strengths

Junos Pulse Policy Secure is tightly integrated with Juniper's core security products (firewall, IPS and SSL VPN), network infrastructure offerings (LAN switches) and SIEM solution. In addition to common NAC device-based policies, Juniper's network and security components can also enforce identity-based policies (role-based policies).

In addition to integrations with AirWatch and MobileIron, Juniper offers its own Pulse agent for Apple iOS and Android, and supports basic posture checks for these platforms. Juniper Pulse Policy Secure is also tightly integrated with Juniper's Junos Pulse Mobile Security Suite, which supports some MDM functions.

Juniper has established full FIPS compliance and EAL3 certification for Junos Pulse Policy Secure in virtual and physical solutions. These certifications provide an advantage in government procurements, because most other NAC vendors have yet to meet these qualifications.

Cautions

Juniper provides limited prepackaged integration with third-party network and security monitoring tools. Juniper's NAC integrates with its SIEM, and the Juniper solution uses IF-MAP, an open protocol published by the Trusted Computing Group. However, since very few security vendors have embraced IF-MAP, Juniper has a limited number of network security partners for its NAC offering.

Juniper relies heavily on OEM technology for its NAC offering. Its profiling technology is an OEM of Great Bay Software's solution, and its 802.1X-based supplicant configuration tool is an OEM of Cloudpath Networks. Both Great Bay and Cloudpath are small companies, and any change to their independent status could negatively impact Juniper.

Juniper faces a difficult balancing act with its Pulse MDM offering, because it is now competing with the same MDM vendors that it partners with for NAC.

Return to Top

Portnox

In 2013, the company formerly known as Access Layers renamed itself Portnox, after its flagship product. Portnox, based in Israel and founded in 2007, is a pure-play NAC vendor. The Portnox solution is agentless and based on endpoint discovery. When a device connects to the network, Portnox checks the OS type and applies the appropriate policy to the network access point (LAN switch, WLAN controller or VPN gateway). Organizations that can tolerate the risk of a startup and that are within the geographic range of Portnox's service and support coverage should consider this vendor.

Strengths

Portnox has integrated its solution with the following MDM vendors: MobileIron, AirWatch, Soti, NativeFlow, Good Technology and Citrix (XenMobile).

The company's customers consistently report that the Portnox solution is easy to deploy and manage. It attaches to any LAN switch port and does not require a "mirror" or SPAN port.

Portnox can enforce NAC policies in a VMware environment. For example, it monitors and graphically represents the number of virtual machines (VMs) in use and enforces policies for these VMs by blocking or allowing access to virtual switches.

Cautions

To achieve the maximum benefits of Portnox at remote locations, the vendor suggests deployment of its Knoxer software (free of charge) at each location. Knoxer provides a consistent approach to isolating unknown and noncompliant endpoints. Without Knoxer, the process of isolating endpoints may vary according to the infrastructure at the remote location.

Customization of Portnox may be required to enable special-purpose endpoints, such as security cameras or videoconferencing systems, to gain network access. Because endpoint discovery is at the core of the Portnox solution, all endpoints must be accurately profiled. Some customer references commented that Portnox's library of profiled devices could be larger to avoid the customization effort required to identify nonstandard endpoints. Portnox provides templates to ease the customization.

Portnox has a limited geographic reach. While it has a growing presence in the U.S., its primary operations are in Israel and the U.K. Customers and prospects outside of these regions may face challenges obtaining presales and postsales support from the company.

Return to Top

StillSecure

Founded in 2000, StillSecure is a privately held company focused exclusively on the NAC market. In June 2013, the company sold off its managed security services provider (MSSP) business to SilverSky. In September 2013, private equity firm Versata acquired the remainder of the StillSecure business, moved its headquarters to Austin, Texas, and appointed a new CEO. StillSecure is strongly focused on the defense vertical. Gartner estimates that more than 50% of its revenue comes from U.S. Department of Defense (DoD) customers. StillSecure's Safe Access NAC solution is available as a hardware appliance and as a virtual appliance. Consider Safe Access where heterogeneous networks are in use and where the flexibility of agentless baselining options is required.

Strengths

Safe Access' flexible deployment options enable it to address a wide range of network environments. It supports multiple endpoint baselining methods and several different approaches for policy enforcement. Support for DHCP-based enforcement enables Safe Access to enforce policies independent of the network infrastructure.

Safe Access provides detailed information about the configuration status for Windows endpoints.

StillSecure's FIPS 140-2 and Common Criteria certifications provide an advantage in government procurements because most other NAC vendors have yet to achieve these certifications.

Cautions

As a small company, StillSecure is challenged to support its large DoD customers and its small and midsize business (SMB) customers. Gartner believes the company lacks the resources to effectively pursue both market segments. StillSecure's late support for MDM (it didn't have any MDM partners until 2013) is a reflection of the challenges it faces in serving two markets.

StillSecure lacks a broad set of technology integration with security solutions. It only integrates with one SIEM vendor (LogRhythm).

The Safe Access dashboard has not been designed to address the BYOD use case. For example, it does not readily show the number of Apple iOS devices (although this information can be obtained by applying search filters).

Return to Top

Vendors Added and 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's appearance 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. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Return to Top

Added

None

Return to Top

Dropped

Avaya and Trustwave were excluded from the 2013 Magic Quadrant because their NAC solutions do not provide basic MDM capabilities (natively or through partners) for Apple iOS and Android.

Return to Top

Inclusion and Exclusion Criteria

To be included in this Magic Quadrant, a vendor's solution must be able to enforce NAC policies in a heterogeneous infrastructure environment. In addition, 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 a network connection, so that a decision can be made about the level of access that will be allowed. Baselining must work in heterogeneous endpoint environments (for example, Windows, Mac OS X, Apple iOS and Android). It must include the ability to assess policy compliance (for example, up-to-date patches and antivirus signatures for Windows PCs, or the presence of an MDM agent for mobile devices). Various technologies may be used for the baseline function, including agentless solutions (such as vulnerability assessment scans), dissolvable agents and persistent agents. NAC solutions must include a baseline function, but "reinventing the wheel" is not necessary. Baseline functionality may be obtained via an OEM or licensing partnership.

Access control — The NAC solution must include the ability to block, quarantine or grant partial (limited access) or full access to an endpoint. The solution must be flexible enough to enforce access control in a multivendor network infrastructure, and it must be able to enforce access in wired LAN, wireless LAN and remote access environments. Enforcement must be accomplished either via the network infrastructure (for example, 802.1X, virtual LANs, access control lists [ACLs]) or via the vendor's NAC solution (for example, dropping/filtering packets or ARP spoofing). Vendors that rely solely on agent-based endpoint self-enforcement do not qualify as NAC solutions.

Additional criteria include:

Vendors must provide basic MDM capabilities (natively or through partners) for Apple iOS and Android.

Network infrastructure vendors must have demonstrated their ability in 2012 and 2013 to sell NAC solutions beyond their installed base of infrastructure customers.

NAC vendors must consistently target and show wins at enterprises with 5,000 endpoints and above to be included. This Magic Quadrant does not analyze solutions that only target the SMB market.

Vendors must have an installed base of at least 100 customers or an aggregate endpoint coverage of 500,000 endpoints.

The vendor must have at least $5 million in NAC sales during the 12 months leading up to 1 November 2013. Solutions that do not directly generate revenue for the vendor, such as those that embed basic NAC functionality in other products at no extra charge, have been excluded from this analysis.

The NAC solutions had to be generally available as of 1 November 2013.

Return to Top

Evaluation Criteria

Ability to Execute

Product or Service: An evaluation of the features and functions of the vendor's NAC solution, including the ability to integrate with solutions that provide network visibility and event monitoring. Due to the influence of the BYOD trend on NAC, this criterion heavily weights the ability to establish and enforce policies in heterogeneous endpoint environments (Windows, Mac OS X, Apple iOS and Android). Other BYOD-related NAC functions, such as profiling of endpoints and guest networking services, have been be heavily weighted.

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. The ability of vendors to succeed in their target markets is important. Vendors should demonstrate success in winning NAC deals of 5,000 endpoints or more.

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. Those vendors that frequently appear on client shortlists are succeeding in marketing execution.

Customer Experience: Quality of the customer experience based on input from Gartner clients and vendor references. Input is gathered via reference calls and an online survey.

Table 1. Ability to Execute Evaluation Criteria

Criteria	Weight
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Not Rated
Marketing Execution	Medium
Customer Experience	Medium
Operations	Not Rated

Source: Gartner (December 2013)

Return to Top

Completeness of Vision

Market Understanding: The ability to anticipate market trends, such as the impact of BYOD, and to quickly adapt via partnerships, acquisitions, or internal development.

Marketing Strategy: This criterion analyzes whether the vendor's marketing strategy succeeds in differentiating its NAC solution from its competitors.

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 and its road map for NAC. The product strategy should address trends that are reflected in Gartner's client inquiries.

Vertical/Industry Strategy: The vendor's strategy for meeting the specific needs of individual vertical markets and market segments. For example, does the vendor have an effective strategy for pursuing vertical markets that have been aggressive adopters of NAC, such as higher education, healthcare and financial services?

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

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Not Rated
Vertical/Industry Strategy	Low
Innovation	Medium
Geographic Strategy	Low

Source: Gartner (December 2013)

Return to Top

Quadrant Descriptions

Leaders

Leaders are successful in selling large NAC implementations (10,000 nodes and greater) to multiple large enterprises. Leaders are pure-play NAC vendors or networking and/or security companies that 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 have financial resources. They have also demonstrated a strong understanding of the future direction of NAC, including the impact of BYOD. 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.

Return to Top

Challengers

Challengers are networking and/or security companies that have been successful in selling NAC to their installed bases, although they are generally unsuccessful in selling NAC to the broader market. Challengers are generally not NAC innovators, but are large enough and diversified enough to continue investing in their NAC strategies. They are able to withstand challenges and setbacks more easily than Niche Players.

Return to Top

Visionaries

Visionaries have led the market in product innovation and/or displayed an early understanding of market forces and trends. They are smaller pure-play NAC vendors or larger networking and/or security companies. A common theme among Visionary vendors is that they don't have significant channel strength in the NAC market and have not succeeded in building installed bases as large as those of vendors in the Leaders quadrant.

Return to Top

Niche Players

Niche Players are typically strong in strategic NAC verticals (for example, education and healthcare) and certain geographies. They don't often appear on Gartner clients' shortlists, but they are valid options for organizations within those key geographies and vertical industries.

Return to Top

Context

If your organization faces BYOD challenges, consider solutions that can easily profile personally owned mobile devices, and apply controls that are consistent with your organization's mobile device policies. Because there are multiple approaches for enforcing NAC policies (for example, virtual LANs, firewalls and access control lists), look for solutions that best fit your network infrastructure.

Return to Top

Market Overview

NAC vendors had an exceptionally strong year in 2013. Gartner estimates that the size of the 2013 NAC market will be approximately $350 million, an increase of about 55% over 2012. Much of the growth can be attributed to larger NAC vendors investing heavily in sales and marketing to position NAC as a solution for the BYOD trend. In 2014, we expect growth to slow to approximately 45%, as the vendors will be challenged to match the growth rates of 2013, particularly since advanced threat defense solutions are also competing for budget dollars. Given our projections, we expect that the NAC market will reach $510 million by year-end 2014.

Starting in approximately 2006 (after the worm era of Sasser and Blaster) and continuing up to Apple's announcement of the iPad in 2010, the NAC market experienced slower growth. In 2009, the market actually declined by about 10%. During this period, enterprises were primarily considering NAC to protect their wired networks from untrusted devices (some also implemented NAC for VPNs). Most enterprises implemented wireless guest networks as an alternative to purchasing a commercial NAC

solution, since the guest network approach served to keep "honest" visitors off the corporate wired network. However, after the introduction of the iPad and the subsequent momentum behind BYOD, enterprises began to reassess NAC — this time to control access to wireless networks. Security-conscious organizations are also implementing NAC to control access to the wired network, mainly via basic authentication policies.

NAC technology providers fall into two major categories:

Pure play — Vendors whose primary focus is on NAC.

Wired and wireless network infrastructure — Several LAN switch and wireless LAN vendors offer NAC solutions. Some of the network infrastructure vendors own NAC technology, while others license it from OEM providers.

The BYOD trend ensures that enterprises will continue to require NAC, particularly to control access to wireless networks. Wireless LAN vendors will need to offer some NAC features, if not a full-blown NAC solution, to satisfy access control requirements. Rather than develop their own NAC capabilities, many will turn to partnerships with NAC pure plays, as HP and Xirrus have done with Bradford Networks. Gartner expects to see more partnerships between wireless LAN vendors and NAC pure plays in the 2014-2015 period. As more infrastructure vendors embed NAC functionality, NAC pure plays will experience downward pricing pressure when selling directly to enterprises.

Return to Top