Market Guide for Network Access Control

Published: 09 May 2017 **ID:** G00303075

Analyst(s):

Claudio Neiva, Lawrence Orans

Summary

NAC solutions support network visibility and access management through policy enforcement on devices and users of corporate networks. Security and risk management leaders should develop requirements that determine which vendor solutions best address their cost and manageability requirements.

Overview

Key Findings

- Network visibility and control continue to be drivers for the adoption of network access control.
- New vendors delivering NAC solutions aimed primarily at the midmarket have recently appeared.
- Client feedback indicates that two-phase implementations are the most manageable for addressing discovery and policy.

Recommendations

Security and risk management leaders responsible for network and gateway security should:

- Implement NAC to deliver visibility and control over the endpoints on their corporate networks.
- Integrate NAC solutions with threat detection products, so that NAC can automatically enforce the appropriate policies for compromised endpoints (for example, to quarantine endpoints from the network).
- Evaluate NAC solutions from infrastructure providers to consolidate management and leverage advanced networking capabilities.
- Analyze pure-play NAC solutions for leveraging interoperability in the case of multibrand network infrastructures.

Market Definition

Security and risk management leaders are responsible for responding to inquiries from audits regarding the ability to discover what devices are connected to the corporate infrastructure. Therefore, Gartner defines network access control (NAC) as technologies that enable organizations to implement policies for controlling access to corporate networks by devices such as the Internet of Things (IoT) and by users. Policies may be based on authentication, endpoint configuration (posture) or users' role/identity. NAC also includes postconnect policies, in which the NAC solutions integrate with other security products. For example, if an advanced threat detection (ATD) product detects a compromised endpoint via integration, the NAC solution could enforce the appropriate policy (e.g., remove the device from the network). Network visibility and control continue to be drivers for the adoption of NAC.

Other NAC use cases include:

- Management of access from consultants, contractors and other guests taking control over the devices' connectivity to limit their access.

- Visibility and control over the connectivity of bring your own device (BYOD) programs, primarily wireless, to enable employees to access networks with personally owned devices.
- Management or identification of IoT devices on the network.

NAC solutions should include the minimum capabilities described in the sections that follow.

Policy Life Cycle Management

The NAC solution must include a dedicated policy management server with an interface for defining and administering security configuration requirements, and for specifying the access control actions for compliant and noncompliant endpoints. Examples of these actions include allowing access or quarantining a device or user. Policies can cover several functions, including device authentication, user authorization, location, time/date, duration and application/resource access.

Security Posture Check

The NAC solution should enable protection resources to decide the proper level of access, based on security state of an endpoint that is attempting a network connection. A baseline feature must work in heterogeneous endpoint environments, such as Windows, macOS X, Apple iOS and Android. The feature must include the capabilities to assess policy compliance or posture of the device — for example, up-to-date patches and antivirus signatures for Windows PCs, or an enterprise mobile management (EMM) agent for mobile devices. Technologies used for the baseline functions may include vulnerability assessment scans (e.g., agentless scanning), dissolvable agents and persistent agents.

Access Control

The NAC solution must include the ability to block, quarantine, or grant limited or full access to an endpoint. The solution should be flexible enough to enforce access control in a multivendor network infrastructure. Enforcement must be accomplished through the network infrastructure — for example, 802.1X, virtual LANs (VLANs) and access control lists (ACLs) — or by the vendor's NAC solution (e.g., dropping/filtering packets or Address Resolution Protocol [ARP] spoofing).

Guest Networking Service

The NAC solution should include the ability to manage guests through a customizable, self-service captive portal. Guest networking should include guest registration, guest authentication, guest sponsoring and a guest management portal.

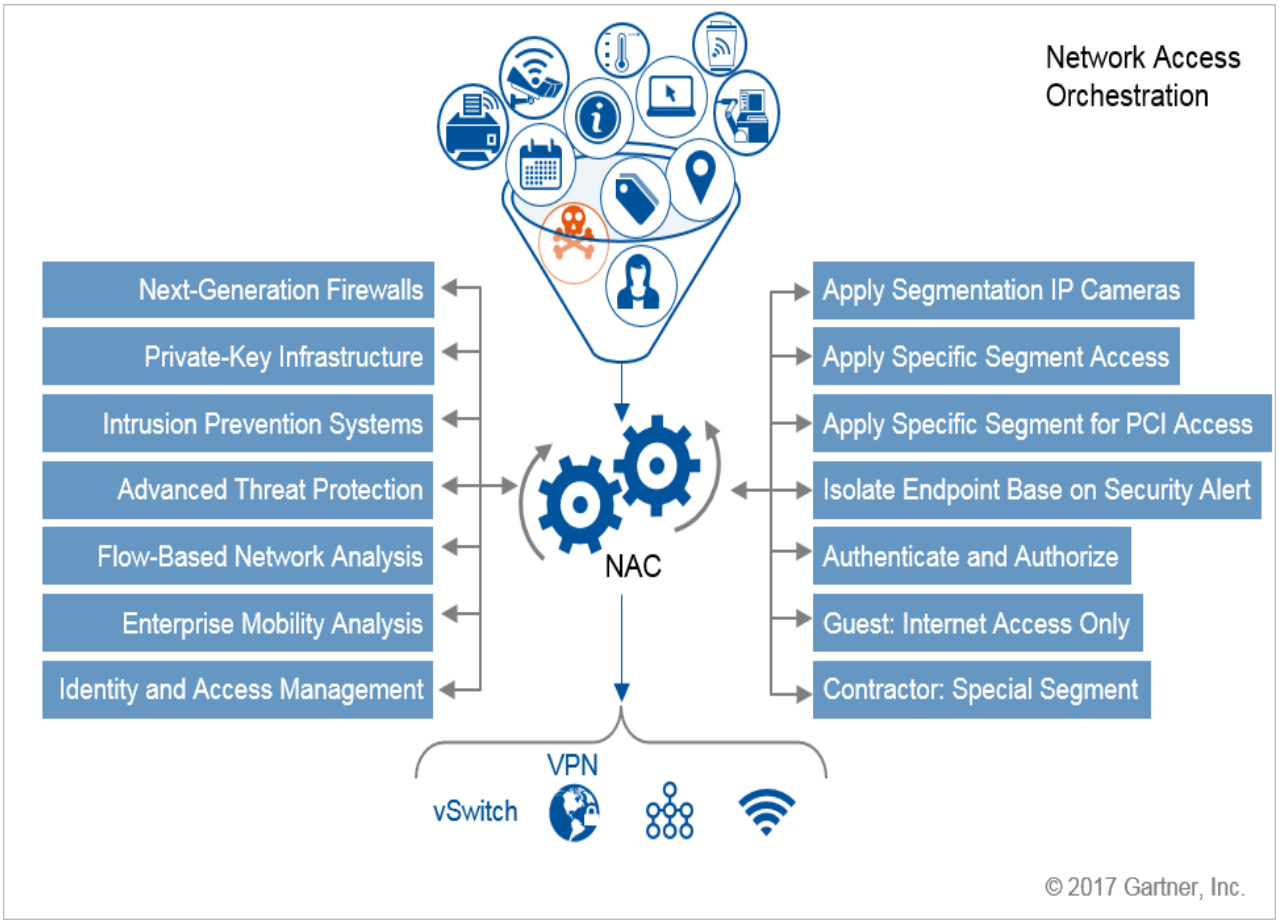
Profiling and Visibility

The NAC solution should include a profiling engine that delivers dynamic discovery, identification and the monitoring of all network-attached endpoints. It can be passive or active to aggregate data from various sources to provide a device identification.

Bidirectional Integration

Integration with other security components must be accomplished through the syslog (sharing information via log messaging protocol) or through the open/RESTful API (see Figure 1).

Figure 1. Network Access Orchestration



Source: Gartner (May 2017)

Market Direction

Client inquiries demonstrate an interest in pursuing NAC for the reasons described in the sections that follow.

Respond to Audit Findings

Many organizations (primarily regulated verticals) pass through third-party security assessments for audit purposes. The most common finding is the ability to connect to internal infrastructure with no identification of the device/user, which increases the risk of internal attacks by unauthorized devices. Clients are looking for NAC as an option to simplify network visibility and control of network access, primarily in wired and wireless networks, and, sometimes, virtual

private networks (VPNs). Future editions will perform similar functions for IoT devices, which will dramatically increase possible connections of unauthorized devices.

Improve Network Visibility

NAC can increase network visibility to reduce the risks associated with noncompliant devices and open access to enterprise network facilities. It can also provide the ability to plan for network provisioning, because security and networking leaders can assess the actual number of devices and categories to plan for when determining access policies and network requirements. Future editions will provide visibility across nonstandard wireless networks (e.g., cellular or microwave), because IoT devices will be linked to the enterprise network.

Manage Guest/Contractor Access

In the rush to provide connectivity to guests and contractors, many Gartner clients are overwhelmed by the number of devices accessing their networks. Organizations must prepare for multiple levels of access — depending on whether the user is a contractor, employee or guest — and for times and locations that access should be available. New mobile and nonmobile device types will also require support.

Incident Response

When an alert occurs, an automated mechanism will remove the endpoint, or a mechanism will quickly identify the endpoint. This happens through integration with other security components, such as next-generation firewalls, ATDs, and security information and event management (SIEM) solutions, all of which enhance continuous monitoring. NAC vendors have positioned their solutions as "warehouses of context" to share contextual information (for example, user ID or device type) with third-party security components. NAC can also respond

to ATD alerts by automatically enforcing security policies that isolate compromised endpoints.

To gain more visibility into the configuration of corporate-owned devices, many organizations can integrate with EMM solutions (see "Magic Quadrant for Enterprise Mobility Management Suites") with their NAC solutions. Gartner is seeing vendors form technology partnerships as a common solution to expand NAC capabilities.

IoT and NAC

Even though the IoT security market is nascent, IoT devices were already used in a large-scale incident in late 2016 to initiate a series of distributed denial of service (DDoS) botnet attacks, using devices such as closed-circuit TVs (CCTVs), webcams and DVRs. The resulting attack set new records for data used in a DDoS attack. [1] This event created awareness among security and risk managers and security decision makers about the need for better approaches to securing IoT devices connected to their infrastructures.

The risk to organizations of unsecure IoT devices varies from industry to industry. For example, industries classified as "critical infrastructure" to countries (such as power, oil, gas, manufacturing, transportation and healthcare) have infrastructure that not only requires the data in it to be protected, but also the lives of people and the quality of the environment in which they operate. Network infrastructure that serves such industries faces a significantly higher risk from IoT device compromises than those that have only data protection to consider as their primary goal.

In healthcare, common threats to medical devices from IoT devices include:

- Network infiltration through an exploitation of vulnerabilities in hardware and software
- Self-propagating ransomware encrypting critical data and forcing the hospital to pay to restore systems and administrative capabilities

- Physical device compromise

IoT devices, such as VCRs, CCTV and web cameras, smart lighting systems, building automation, and facilities management systems, all may be partially or entirely connected corporate data networks in the organization without IT awareness. One simple step for providing security from IoT-supported compromises would be proper network segmentation to maintain connectivity only within segments that support IoT-rich systems. New IoT devices may also be invisible to typical IT security asset discovery and tracking systems, so new IoT-specific solutions for discovery and management may be required.

One way to prepare for IoT security is to view IoT devices as defined by class, depending on their functional capabilities (see "Assessing Integration Architecture for Internet of Things Solutions"). Different device classes represent distinct levels of visibility to NAC solutions:

- **Class 1 —** Simple devices, such as sensors, that sense and transmit data, or simple actuators that receive data to initiate commands.
- **Class 2 —** Devices that perform more-sophisticated data storage or analysis functions, in addition to Class 1 capabilities, such as a simple hub, concentrator or gateway for devices. This category also includes cameras, door locks and smart TVs.
- **Class 3 —** Devices such as general-purpose IT servers that can serve as IoT gateways or platforms.

Historically, NAC solutions are optimized to identify devices for Class 2 and Class 3. NAC solutions have a feature called "Profiling," with which Class 1 devices present their data in different formats over different wireless networks. Most NAC solutions are unable to identify by device type accurately. However, more NAC products and NAC-enabled service providers are developing IoT capabilities across the NAC functional spectrum for IoT-rich environments.

Market Growth

The information security market was expected to grow at an annual average of 8% in revenue in constant currency (see "Forecast: Information Security, Worldwide, 2014-2020, 4Q16 Update"), while the NAC market is estimated to have grown by 26% from 2015 to 2016, with an estimated market size of $685 million, which includes three more vendors this year. Gartner market size estimates indicate that Cisco, ForeScout Technologies and Hewlett Packard Enterprise (ClearPass) remain the top three vendors in market share (as measured by revenue). NAC helps eliminate unnecessary security risk, due to lack of visibility through corporate infrastructure. Although there is a significant movement of endpoints to access corporate assets on cloud environments outside the corporate infrastructure, many companies have thousands of endpoints within the enterprise perimeter, and new use cases are emerging that demand visibility.

Market Analysis

The NAC technology providers fall into two categories, which are described in the sections that follow.

Wired and Wireless Infrastructure Vendors

Wired and wireless infrastructure vendors rely mostly on a Remote Authentication Dial-In User Service (RADIUS)-based approach to manage device and user access to the network infrastructure. Although infrastructure providers rely on 802.1X to authenticate and authorize, they are investing in alternatives for clients that lack the resources to deploy 802.1X. If your infrastructure provider offers an NAC product, you should include it in your evaluation product shortlist. The advantages of this category of vendors include:

- Infrastructure management consolidation and in-depth integration with other security products. Some vendors integrate with VPN, access layer

switches and access point features, firewalls, intrusion prevention systems (IPSs), ATDs, and network traffic analysis (flow-based).

- The use of full capabilities embedded in the network infrastructure components to provide unique benefits, such as integrated device profiling and granular policy enforcement.
- Strong authentication processes, with 802.1X using digital certificates (EAP-TLS) with built-in certificate authority (CA) — not all infrastructure vendors have these capabilities — using multiple domains. Those that do not have built-in CA would need to integrate with third-party public-key infrastructure (PKI) systems.

Challenges with wired and wireless infrastructure vendors include:

- **Lock-in capabilities —** Gartner clients have shown concern about the adoption of advanced capabilities in the infrastructure vendors, limiting the ability to change providers through a network life cycle refresh.
- **The complexity of management of different consoles —** Some infrastructure vendors have a different set of consoles to perform network configuration changes and NAC management.

Pure-Play NAC Vendors

The capability to support heterogeneous infrastructure and devices is the main advantage of pure-play NAC. Due to their multivendor support and integration nature, most providers in this category integrate with a wider range of other security products through syslog and off-the-shelf APIs (ready to integrate). Still, some pure-play vendors also offer a RADIUS-based approach. There is also the concept of using NAC through unique partnership to leverage in-depth capabilities of contextual information from other security partners to leverage NAC as part of the incident response. For example, collecting indicators of compromise (IoC) from ATD to discover other endpoints at the same risk to enforce policy to protect the rest of the network environment.

Customers with multibrand network infrastructure should consider using pure-play NAC solutions to leverage interoperability and use capabilities, such as:

- **Ease of deployment —** For example, the ability to detect/discover devices using alternative methods, as opposed to 802.1X. For many Gartner clients, achieving visibility and being able to control it without using 802.1X would satisfy the first phase of deployment. Clients, of course, realize that, in some scenarios (wireless), 802.1X would be the best approach to ensure minimal security, due to the lack of physical access constraints.
- **Flexible enforcement methods —** Flexible policy enforcement includes the use of Simple Network Management Protocol (SNMP), ARP spoofing, denial of service (DoS) to noncompliant endpoints and dropping/filtering traffic through NAC appliances.
- **Agentless security posture check —** Several vendors offer an agentless solution for Windows and macOS systems.
- **Cloud-based management —** Some NAC vendors offer the management console through a cloud service; this could be beneficial to small or midsize businesses (SMBs).

Challenges with pure-play vendors include:

- **One product only —** Some NAC vendors can be considered as one product only. This situation may require closer attention from a business perspective. Through client inquiry, this concern comes as if the vendor will keep competing on this market or may be bought by another vendor, creating difficulties through customer support.
- **Lack of transparency on financial health —** The reliability of an NAC solution also depends on the financial viability of the vendor. Many smaller vendors are privately held, which makes it difficult to assess their overall viability.

Challenges that apply to both categories include:

- Non-802.1X-compatible endpoints, such as printers and IP phones, represent 50% or more of all network-attached endpoints. Supporting these devices adds operational complexity (accuracy), especially with new emerging technologies around IoT devices.
- Some companies still have old networking devices with limited or no management capability at all. Customers need to perform an inventory of their network devices to define which control method can be applied, and whether there's a need for network topology changes.

Alternatives to NAC Providers

Alternative providers relate to solutions that can fulfill part of NAC minimal capacities, with a set of capabilities of device detection, rogue detection and maintain an effective IoT "asset database," complete with attributes and entitlements for access by those devices (see "Market Guide for IoT Security").

The vendors shown in this section do not comprise an exhaustive list that could be considered alternatives to NAC, depending on business requirements:

- Great Bay Software
- Pwnie Express

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Auconet

Auconet is a privately held company that moved its headquarters from Germany to San Francisco in 2014. It has been delivering NAC solutions since 2005. The

vendor has integrated NAC security and network troubleshooting capabilities into one solution for operations and security use cases for heterogeneous networks. Auconet works directly with global enterprises and with managed security service providers (MSSPs) offering large-scale, multitenant, managed NAC services.

The Auconet Business Infrastructure Control Solution (BICS) is deployed most commonly as an agentless solution, using Layer 2 Media Access Control (MAC)-based authentication, in addition to its RADIUS- based policy server, which supports native 802.1X supplicants embedded in multiple OSs. BICS is available as a hardware appliance, a virtual appliance or SaaS. Auconet also offers an optional permanent agent on Windows, Unix/Linux platforms and macOS. BICS includes the ability to discover devices and apply NAC policies in industrial and supervisory control and data acquisition (SCADA) environments and to use its workflow automation capabilities to automate tasks. BICS enables NAC for industrial environments by implementing specific industrial protocols. In 2016, Auconet added real-time, dynamically updated dashboards based on user role (e.g., CIO, data center director, IT/OT network operator) and integration with SIEM providers, such as Splunk, and HPE ArcSight ESM.

Bradford Networks

Bradford Networks is a privately held company based in Boston. It has been delivering NAC solutions since 2001. Its flagship Network Sentry product is a RADIUS-based solution available in hardware, virtual appliances and as a cloud service. The newly packaged Network Sentry comes in three flavors — Secure Enterprise Advanced (SEA), Secure Enterprise Response (SER) and Secure Enterprise Premier (SEP) — each of which includes the ability to share contextual information about endpoints and provide tools for security analysts to respond to alerts from next-generation firewalls, ATD solutions and other security products. Network Sentry SEP provides an automated workflow that can be used to contain compromised user devices. Bradford Networks' mobile

applications can perform limited mobile device management (MDM) capabilities (such as jailbreak detection) and can determine a device's type and OS.

In 2016, Bradford added integration with Tenable to share vulnerability data with Network Sentry's correlation engine to increasing number of trust factors, assign priority, enforce policy-based threat containment actions and it can guide remediation through a web portal. In addition, an integration with Cyphort enables automated malware analysis, and threat triage and response. Network Sentry's new security parser supports any third-party security solution — including standardized interfaces for vulnerability scanner integrations — through "build your own" security device integrations. Bradford Networks is securing network and facilities infrastructure devices by leveraging microsegments on top of Cisco and Arista Networks' network switches.

Cisco

Cisco Identity Services Engine (ISE) policy server is RADIUS- and Terminal Access Controller Access Control System Plus (TACACS+)-based, which enables Cisco to support authentication and device administration in heterogeneous network infrastructure. ISE is available in hardware appliances and as a virtual server. The device-profiling capability (updated via its profile feed service) provides endpoint classification and reports on devices connected to switches and wireless access points.

Through its pxGrid framework, Cisco integrates with Cisco's security products and third-party technologies in partner ecosystems that share alerts and contextual information. Cisco packages its NAC posture agent (baseline capabilities) within its AnyConnect endpoint bundle (endpoint agents within AnyConnect can be enabled via software keys), which unifies other capabilities, such as VPN, NetFlow, MACsec, Supplicant, Cisco Umbrella and Advanced Malware Protection (AMP). There is also support for certificate authority, Active Directory multidomain. Among its new capabilities in 2016, Cisco continues to get feature parity from the Cisco Secure Access Control System (ACS) into ISE,

because ACS's end of life was recently announced. Also, ISE has added multiple matrices for segmentation, which are referred to as ISE DEFCON. For example, you may have a general policy that allows certain users to connect on the network. If the risk of compromise increases, ISE can quickly and easily apply more-rigorous policies that restrict access, especially to those critical areas of the network.

Extreme Networks

Extreme Networks, based in San Jose, California, acquired Enterasys Networks in 2013 and began selling its NAC solution and the broader Enterasys security product portfolio. In 2015, Extreme positioned its NAC solution under the Extreme Access Control brand name. In addition to NAC, Extreme offers other security products in the IPS, next-generation firewall and SIEM areas — especially IBM Security Network Intrusion Prevention System and SIEM products, because the two companies share an OEM partnership. The NAC offering includes out-of-band (NAC Gateway) and in-line (NAC Controller) appliances (also available as virtual appliances). The primary use case for NAC is for the Extreme's Switches and WLAN customers, although the solution can support nonextreme environments.

Extreme Networks' NAC is an RADIUS-based solution that is available in a family of hardware and virtual appliances. Extreme's tight integration of its NAC solution with its unified wired/wireless product family enables granular policy enforcement. Policies may permit, deny, apply quality of service (QoS), rate limit and implement other controls to traffic based on user identity, time, location, end system and user groups. NAC also integrates with several security solutions, including OpenStack and Microsoft Lync. The Lync integration enables Extreme to apply dynamic policies per call — for example, settings can prioritize voice traffic over the data network. In addition, Extreme offers virtual machine (VM) management by applying policy on vSwitch and physical switches to manage VM access through VMware and OpenStack integration. In 2016, Extreme

implemented new user interfaces to optimize workflow, performance tracking and onboarding options, with Google and Microsoft support.

ForeScout Technologies

a privately held company based in San Jose, California, ForeScout Technologies sells the ForeScout CounterACT product for visibility and control of all network-connected devices. CounterACT is primarily an out-of-band solution for heterogeneous network infrastructure; however, it also includes a RADIUS server to support 802.1X environments. CounterACT hardware and virtual appliances are available in a variety of sizes that should be considered for midsize to large deployments.

Although ForeScout offers optional agents, its agentless approach performs security posture assessment for Windows, macOS X and Linux endpoints. Through the ForeScout ControlFabric architecture, ForeScout promotes a series of modules that share alerts and contextual information with third-party security products. Via these modules, CounterACT can be configured to automatically enforce policy (for example, remove an endpoint from the network) in response to alerts from ATD, VA, EDR and other third-party products. In 2016, integrations with FireEye, Palo Alto Networks, Check Point, McAfee and Bromium offer IoC hunting and threat response capability. Also, deeper integration with Splunk enables CounterACT to orchestrate network and host response actions and share response status back with Splunk Enterprise Security. In addition, new capabilities provide enhanced visibility and control of Cloud workloads (Amazon Elastic Compute Cloud [EC2] and VMware), and improved segmentation through Palo Alto Networks and Check Point, using tagging to apply appropriate policy.

Hewlett Packard Enterprise (Aruba)

In 2015, Hewlett Packard Enterprise (HPE) entered the NAC market with the acquisition of Aruba and its NAC offering named ClearPass , which includes the

ClearPass Policy Manager. ClearPass Policy Manager offers RADIUS and non-RADIUS enforcement options for user devices, as well as TACACS for device management authentication. It is available as hardware and virtual appliances, and it includes guest access management (ClearPass Guest), device onboarding (ClearPass Onboard) and endpoint posture assessments (ClearPass OnGuard). ClearPass has broad support for OSs, such as Windows, macOS and Linux, as well as mobile OSs, such as iOS and Android.

Third-party products have been integrated and validated using ClearPass Exchange, including firewalls, MDM/EMM, and SIEMs — via REST-based APIs, syslog messaging and RADIUS proxy functions. In 2016, Aruba introduced two capabilities to the ClearPass Policy Manager, Extensions and OnConnect. ClearPass Extensions is a framework that enables the creation of microservices to fast track new and upcoming integrations with third parties. For wired customers, OnConnect enables non-RADIUS enforcement workflows. By adding capabilities to the existing profiling engine to support Nmap, NetFlow and WMI, plus enhancing SNMP enforcement, ClearPass can provide solutions for customers unable to deploy features such as 802.1X or MAC-Auth on their wired infrastructure. In 2017, HPE acquired Niara, a user and entity behavior analytics (UEBA) solution that uses machine learning and custom algorithms to detect attacks that have evaded traditional security. HPE plans to integrate with ClearPass Policy Manager to take remedial action, where appropriate.

Impulse Point

Based in Tampa, Florida, and founded in 2004, Impulse traditionally catered to the higher education and K12 markets but now also focuses on corporate enterprises. Impulse delivers its SafeConnect solution as a cloud managed service, which includes system monitoring, problem determination and resolution, daily updates to device type, antivirus and OS profiling recognition, and remote backup of policy configuration data. All Impulse products can be implemented as hardware or as virtual appliances.

SafeConnect offers 802.1X and non-802.1X RADIUS-based policy enforcement options at Layer 2 or a Layer 3 enforcement approach that eliminates the need to integrate with Layer 2 LAN switches. SafeConnect's Network Security Orchestration (NSO) feature correlates device type, user identity, location, and ownership information and shares contextual data to multiple third-party security platforms such as VMware AirWatch, RSA, Palo Alto Networks, SonicWall, Fortinet, IBM Security QRadar and Splunk to enable identity/role-based policies and security assessment analytics. NSO also supports the ability to automate device enforcement and remediation based on threat and vulnerability alerts from next-generation firewalls, intrusion detection systems, SIEM, MDM and advanced threat protection providers. Impulse has established strategic partnerships with Juniper, [2] Dell [3] and Aerohive Networks. [4] In 2016, Impulse Point announced a cloud-based deployment option for SafeConnect (Azure and Amazon Web Services [AWS]), and Security Assertion Markup Language (SAML) integration support for single sign-on (SSO) and multifactor authentication.

InfoExpress

Founded in 1993, InfoExpress is a privately held company, based in Mountain View, California, that is focused on providing NAC solutions. Its CGX solution is available as hardware or a virtual appliance. The NAC offering includes out-of-band and in-line appliances (typically used for VPN implementation).

CGX offers optional endpoint agents for a wide variety of OSs, including Windows, macOS X, Apple iOS, Android and Linux. CGX correlates data from multiple sources, such as syslog, Nmap, MobileIron and NAC agents to support granular NAC policies. By analyzing when devices change state, CGX can enforce the appropriate policy. For example, if a mobile device is reported as stolen and reappears on the network, CGX can quarantine the device and notify administrators. Dynamic NAC (DNAC) comes as an agent-based or hardware

enforcement solution. CGX also works as a proxy RADIUS, when using 802.1X to facilitate implementation of CGX across complex networks.

IntelliGO Networks

Founded in 2005, IntelliGO Networks is a privately held company based in Toronto, Ontario, Canada. IntelliGO focuses on providing the SMB suite with action-oriented security intelligence capabilities on its NAC solution. Its RADIUS-based IntelliGO Security Platform NAC solution is available in a family of hardware and virtual models with support from 100 to 100,000 users/devices. The IntelliGO Security Platform supports onboarding and enforcement in an agentless approach through Secure Shell (SSH).

IntelliGO Security Platform primarily focuses on SMB use cases, with an aggregated set of control features for an MDM, NAC, PKI, virtual appliance scanner or IoC hunting, and profiling for Windows and macOS. In addition, IntelliGO Security Platform also promotes NAC as a managed service, which can include assistance tuning security tools, such as firewalls and SIEM. IntelliGO Security Platform has its vulnerability scanning engine and collects IoC from sandboxes solution to include indicators of compromise definitions. In addition to sandbox integration, it is able to search for endpoints (Windows-, Linux-, and Macintosh-based) with patterns that indicate compromise to isolate the endpoint automatically. Enforcement can be applied using different methods of discovery/visibility (802.1X, MAC authentication) and control (VLAN, ACL and QoS settings per user/device). IntelliGO Security Platform also promotes a built-in MDM for device onboarding with certificate-based access.

For K-12 and universities, it promotes device management through wizards for configuration and integration with firewalls and secure web gateways to apply policy per user. In addition, onboarding includes transparent authentication for Chromebook devices. In 2016, IntelliGO Security Platform added a collection of data through syslog, app logs (agents Linux, Windows, macOS, etc.) and network traffic. With the data collected, IntelliGO Security Platform can provide

log data visualization for search queries and with Network Map to map traffic or changes to devices.

Inverse (PacketFence)

Founded in 2008, Inverse is a privately held company based in Montreal (Quebec), Canada. Inverse develops the PacketFence NAC solution, which is completely free and open source. PacketFence is a RADIUS-based solution, and Inverse delivers consulting services and product support for the software.

PacketFence includes a captive-portal for registration and remediation. It uses Fingerbank to leverage profiling capability. The Fingerbank solution is a set of device fingerprints that identifies connected endpoints to the network infrastructure. In 2016, Inverse added a new reporting engine to PacketFence, enabling customers to customize or add new reports from PacketFence web administration interface. Inverse also added advanced auditing capabilities to PacketFence and launched a cloud version of PacketFence for MSSP use case. Also, the captive-portal engine in PacketFence received a new look and feel for an improved experience on mobile devices.

OpenCloud Factory

Founded in 2011 and based in Spain, OpenCloud Factory (OCF) is a privately held company that provides NAC solutions, such as openNAC Enterprise or openNAC Community, an open and free version. OCF customers are based mainly in Europe and Latin America. openNAC is offered as a virtual appliance that can be deployed on-premises or cloud. The Radius-based openNAC Core policy engine contributed to the foundation of OCF, openNAC Sensor (probe) supports endpoint discovery without 802.1X, and openNAC Analytics implements the graphical user interface for openNAC and integrates with SIEMs solutions. In addition, openNAC offers an optional agent for Windows, Mac and Linux.

The openNAC solution provides multivendor support for network infrastructure, based on standard methods of authentication and enforcement through VLAN. For the authentication process, it can integrate with multiple LDAPs and Active Directories. It may also include a second factor of authentication integrating Google Authenticator or Mobile Connect. The discovery process can be done at authentication time or via SNMP traps. Additionally, it leverages captive portal for guest management and specific use cases that can be customized by OCF. Finally, openNAC integrates with other third-party security solutions, such as firewalls (e.g., Palo Alto and Fortinet), endpoint protection solutions (e.g., Panda Security and Kaspersky Lab) or SIEMs to receive or send complementary security information.

Portnox

Founded in 2007, Portnox is a pure-play NAC vendor that operates mainly in the Americas and EMEA. Portnox solution is agentless and is based primarily on endpoint discovery. After a device connects to the network, Portnox checks the OS type, then applies the appropriate policy to the network access point — for example, a port on a LAN switch, a WLAN controller or a VPN gateway.

Portnox Clear is a cloud-based offering enabling cloud deployment of 802.1X, including RADIUS server and certificate authority functionality. The optional Clear app runs on iOS, Android, Windows and macOS and includes onboard configuration for 802.1X supplicants. It also calculates the risk associated with device attributes, including applications, encryption, open ports and updates. Operating as a standard/simple app and not an MDM profile, Clear allows administrators to identify the device, its owner and its monitor compliance status, and to see all visited Wi-Fi networks. The Portnox Core on-premises solution can also enforce NAC policies in wired, wireless, VPN and VMware environments. For example, it monitors and graphically represents the number of VMs in use, and it enforces policies for these VMs by blocking or allowing

access to virtual switches. Portnox Clear and Core support visibility, control and management of all devices and users in the network.

Pulse Secure

Pulse Secure was created in 2014 when private equity firm Siris Capital Group acquired the Junos Pulse product line from Juniper. In addition to its NAC solution, Pulse Secure offers a VPN solution and a mobile security solution. Pulse Policy Secure NAC solution is based on a RADIUS platform and is available as a family of hardware and virtual appliances.

Since Pulse Secure became an independent company, it has focused on features (evolving from its support from RADIUS Change of Authorization) that enable it to work in a heterogeneous network infrastructure. Historically, Pulse Secure is still tightly integrated with Juniper's core security products (firewall and IPS) and network infrastructure offerings (LAN switches). Also, Pulse Secure continues to broaden its ecosystem with other security vendors, such as Palo Alto Networks, Check Point and IBM Security QRadar (SIEM). Pulse Secure offers a central management (via its Pulse One product), which is available on-premises or as a cloud service, and one agent for its portfolio (VPN, NAC and mobile management). Along with its onbox feature (for onboarding and profiling), Pulse Secure offers network device profiling with Great Bay Software. In 2016, SNMP was added as an alternative to 802.1X for policy enforcement and enhancement with Pulse User Interface.

SnoopWall

SnoopWall is a pure-play NAC vendor targeting SMBs. SnoopWall's NAC solution is based on technology developed when the company was known as NetClarity. In 2014, Hexis Cyber Solutions acquired NetClarity; however, in 2015, the founder of NetClarity reacquired its assets and relaunched the NAC appliances under the SnoopWall brand. Its NetSHIELD product uses agentless endpoint discovery. Rogue assets may be dynamically or manually blocked by

applying a DOS attack stream against the asset that needs to be blocked or quarantined. NetSHIELD also supports dynamic VLAN (802.1Q) at unauthorized endpoints.

NetSHIELD appliances are equipped with a malware detection feature designed to identify outbound "command and control" traffic destined for known malware sites. Its NAC solution is available as a hardware appliance that ranges from 100 to 1,000 protected assets. As part of a BYOD strategy, SnoopWall also offers the MobileSHIELD endpoint agent that runs on iOS, Android and Windows. MobileSHIELD is controlled from Command Center (an NAC management console), which enables the administrator to control device settings, applications, application privileges, and port and mobile data connectivity defined by policy, while connected to corporate infrastructure. In 2016, SnoopWall can deliver integrated control through its WinSHIELD with MDM-like capabilities: device control settings, application, lightweight DLP and privacy controls (e.g., microphone eavesdrop blocking, keyboard and storage encryption, and camera blocking).

Market Recommendations

Organizations should focus on price, implementation cost and integration with existing infrastructure vendors to differentiate solutions. Given the range of solutions in the marketplace, we recommend that you:

- Focus on vendors that target organizations of your size and complexity. Because NAC is a mature market, many vendors are clearly aligned regarding SMB and large-enterprise opportunities.
- Perform a network inventory as part of your NAC project. This will influence your decision, based on the capabilities of your network devices.

- Determine which enterprise mobility management (EMM) solutions are already installed on the network to identify providers that have direct integration with existing EMM solutions.
- Implement NAC to deliver visibility (for example, which devices are connected to your network) and control (allow or deny access) over your corporate network.
- Use the postconnect functionality of your NAC solution. Most NAC products integrate with multiple security products. Configure NAC to automatically enforce policy when your threat detection solution (for example, network sandbox) alerts that an endpoint has been compromised. NAC can automatically remove the endpoint from the network, or it can enforce another policy that limits the endpoint's ability to communicate externally.

Evidence

[1] D. Goodin. "Record-Breaking DDoS Reportedly Delivered By >145K Hacked Cameras." Ars Technica: Risk Assessment. 29 September 2016.

[2] "Juniper and Impulse Deliver Cloud-Managed Mobile and IoT Security," Juniper.

[3] Dell Network Management/Utility — Selling Impulse Point NAC product .

[4] "Aerohive and Impulse: Solution Brief," Aerohive Networks.

K. J. Higgins. "Hospital Medical Devices Used as Weapons in Cyberattacks." Dark Reading. 8 June 2015.

C. Osborne for Zero Day. "Experts Weigh In on the State of Medical Device Security Today and Beyond." ZDNet. 21 February 2017.

"Heightened DDoS Threat Posed by Mirai and Other Botnets." US-CERT: Alert (TA16-288A).

C. Osborne for Zero Day. "Hackers Release New Malware Into the Wild for Mirai Botnet Successor: The Malware Focuses on Turning Vulnerable IoT Devices Into Botnet Slaves." ZDNet. 1 November 2016.

S. Gallagher. "Maryland Hospital Group Hit by Ransomware Launched From Within (Updated)." Ars Technica: Zombie Server Ransomware Apocalypse. 1 April 2016.

R. Winton. "Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating." Los Angeles Times: Business/Technology. 18 February 2016.