FROST & SULLIVAN

Market Engineering

Network Access Control (NAC) Global Market Analysis
Selected Excerpts: Point of Competitive Differentiation

Most Scalable and Best NAC Wired and Wireless

HPE Aruba Networks ClearPass

Christopher Kissel

Analyst, Knowledge-Based Security
Information & Network Security

K001-74
May 2016

Points of Competitive Differentiation

Most Scalable

CRITERIA

- The first criterion in scalability starts with a simple premise. In many NAC deployments (as well as with many other network security platforms), a network security vendor is going to win a small scale deployment. There are many reasons why a company will start with a smaller commitment:
  - Many companies have a multi-vendor networking hardware environment. A customer will want to see how well a platform performs in environment that has different switch and routing vendors and different server OS.
  - The usability of a NAC may or may not scale. It is one thing for a central IT person to use a NAC in a trial environment, and quite another thing for different security and operations personnel to use the NAC in the live implementation.
  - Unless there is a greenfield installation, NAC is installed in largely mature networks. How the NAC operates with existing IDS/IPS, SIEM, MDM, or other IT and security platforms cannot be known until the NAC is field-ready.
- Scalability also means expansion. A given company can expand from a single office to a regional presence or from a regional presence into a national or international business presence.
- Ultimately, the NAC is going to have to be adaptable in multiple networking environments. The NAC will have to provide visibility and access controls in cloud environments, over BYOD devices, with cellular band and Wi-Fi wireless, in API with IoT (eventually), as well as providing full functionality in traditional managed on-premises networks.
- One advantage to contemporary NAC platforms is central visibility and management over many endpoints. NAC platforms can manage in excess of 250,000 endpoints from a single vantage point.
- The proof of concept stage is important. It stands to reason, if a company has trouble “standing up” a platform in the POC stage, then expansion is likely to be problematic.

Source: Frost & Sullivan

Points of Competitive Differentiation (continued)

The Citation for Most Scalable

Aruba ClearPass

- Addressing the first criterion of scalability, Aruba ClearPass has a low overhead model in terms of equipment deployment. The all-in-one ClearPass appliance is sold as either a hardware appliance or as a virtual machine. As a form factor, a hardware appliance comes in an all-in-one box. The Policy Manager, Onboard, Guest, and, OnGuard are all on the same appliance.
- The number of endpoints determines the number of appliances a business will want to purchase, although, Aruba advises the necessary number of appliances, plus-one appliance, to serve as a back-up and provide redundancy.
- The ClearPass platform is highly scalable. In terms of appliances, three appliance sizes are available: 500, 5,000, and 25,000 MAC authentication address appliances are sold. Licenses for OnGuard, Guest, and on-boarding can be purchased in 1-, 3- or 5-year increments for 100, 500, 1,000, 2,500, 5,000, 10,000, 25,000, 50,000, and 100,000 endpoints.
- The vendors in this report support NAC integrations with third-party IT and security technology platforms; but each vendor has a different approach. Many vendors will upsell an “integration module.”
- The majority of ClearPass product integrations are available pre-existing on the appliance. For instance, for an integration with an MDM, a drop down menu gives you the option to integrate with MobileIron or AirWatch. The MDM module is not sold as a separate module. Worth noting: unlike other NAC vendors Aruba does not charge anything extra for its third-party integration exchange.

Source: Frost & Sullivan

Points of Competitive Differentiation (continued)

The Citation for Most Scalable (continued)

Aruba ClearPass

- ClearPass has several important software and hardware integration partners. As one would expect, Aruba acquisition by HP has helped with product/platform integrations. (Please note that as we list software and hardware integrations, greater detail is provided in Vendor Profile: Aruba (continued), Architectural Advantages.
- ClearPass has a significant integration with the Juniper SRX security service gateway platform.
- Leveraging 802.1X, ClearPass offers ubiquitous support all of the RADIUS dictionaries from industry compliant 802.1X switch providers (Juniper, Brocade, Arista, Cisco, etc.). ClearPass is compatible with Arista Networks' software defined 10/40 Gbps switching and routing devices.
- Perhaps, the most flexible hardware support comes with Aruba' own wired/wireless equipment. Aruba supports role-based access rules within their own Wi-Fi equipment. Additionally, ClearPass shares information with the Aruba Airwave Network manager.
- With an eye toward IoT, ClearPass includes the ability for IT to create categories and policies for devices that are new and not previously profiled and connected to the network – newly developed engineering devices, HVAC systems, hand held devices. Etc. ClearPass also allows for users to help IT by entering information about devices via an online portal. Enhanced profiling capabilities provides accurate device attributes that also helps toward understand what type of new devices are connecting.

Source: Frost & Sullivan

Points of Competitive Differentiation (continued)

Best NAC Wired and Wireless

CRITERIA

- The wired and wireless category includes management and visibility over wired, wireless, BYOD, VPN, and cloud environments.
- In NAC environments, often the end user traverses different networks while mobile (moving from Wi-Fi to secure cellular bands, or from wireless to Ethernet). The NAC should maintain visibility and allow the end user to stay authenticated throughout transitions.
- Device profiling will become important to reduce the involvement of IT and to associate roles and establish rules when a device enters the network.
- The IoT is in its nascent stages. NAC access controls invariably will include management of devices that have not been connected by Ethernet such as smart meters, medical equipment, and home automation.

Source: Frost & Sullivan

Points of Competitive Differentiation (continued)

The Citation for Best NAC Wired and Wireless

Aruba ClearPass

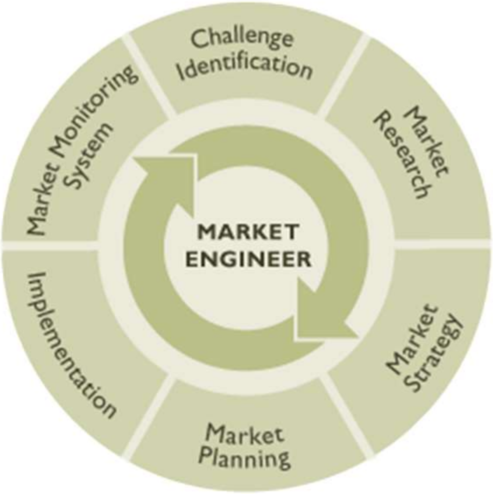
- Previously cited for scalability, many of the attributes that make ClearPass a scalable platform contribute to wired and wireless.
- The first criterion in unified communications is the ability to have access control, visibility, and the ability to continuously monitor wired/wireless/BYOD/IoT devices over a central console.
- The support of social media is now a requisite in NAC—ClearPass Guest natively supports social media log-ins.
- Using the 802.1X, Aruba Auto Sign On will automatically log an end user into apps using a valid network auth.
- ClearPass uses DHCP and NAD discovery data as a way to build information to profile devices. This is interesting; if a device has characteristics of a printer, ClearPass will create an asset group called PRINTERS and assign the device to the asset group. However, ClearPass has settings that allow network administrators to pre-classify devices (this feature is used often for medical devices).
  - Note: Aruba provides fingerprint updates automatically on the 15th and 30th of each month.
- ClearPass Exchange uses API's, Syslog and Extensions to offer integration with PMS, help desk, MFA and other 3rd party services and security solutions.
- The ClearPass Policy Manager offers a portal that lets people define what Digital Living Network Alliance (DLNA), and Apple Bonjour network configuration resources can be used.

Source: Frost & Sullivan

Market Engineering Methodology

One of Frost & Sullivan's core deliverables is its Market Engineering studies. They are based on our proprietary Market Engineering Methodology. This approach, developed across the 50 years of experience assessing global markets, applies engineering rigor to the often nebulous art of market forecasting and interpretation.

A detailed description of the methodology can be found here.



Source: Frost & Sullivan

About the Author

Chris Kissel
Senior Industry Analyst

Frost & Sullivan
North America
Phoenix, AZ

Functional Expertise

- Ten years of research and sales experience in the network security, cellular infrastructure, wireless, telecomm, PCs, semiconductor, and high-definition consumer device sectors.
  - Presented a Vulnerability Management Analyst Brief, Moderated an IBM Navigator on Cloud Webinar, and served as a panellist on a Wireless Week webinar about cellular backhaul
  - Developing expertise in knowledge-based network security technologies.: vulnerability management, SIEM, network forensics, network access control (NAC), and Internet of Things.
  - Well-regarded analyst in LTE and cellular infrastructure.

Primary Research Domains

- Industry Analyst on IT and Information and Network Security market strategies, business opportunities, and technologies

What I bring to the Team

- A synergistic viewpoint about network security technologies that involves threat mitigation, forecast techniques, vendor profiling, and in-depth report methodologies.
- Ten years of experience in TMT (Technology, Media, Telecomm)
- Experience with several research templates including primary research, in-depth research reports, Pivot Table, and PowerPoint deliverables.

Career Highlights

- Moderator and guest blogger for IBM Navigator on Cloud project.
- Published a report that forecast LTE cellular infrastructure shares by vendor, by region, and by operator.
- Product endorsements for BeyondTrust, Qualys, and Fortinet.
- Changed In-Stat LTE & Cellular Infrastructure service to be far more granular in backhaul and small cell coverage.
- Worked with Fierce Wireless as a contributor to their annual Cellular Backhaul eBook..

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan

About Frost & Sullivan
Information and Network Security Research Programs

Frost & Sullivan's Network Security Research and Consulting practice provides global industry analysis, custom consulting, growth consulting and market research & forecasts that help your firm grow.

Market Analysis: Information & Network Security

- Advanced Persistent Threats (APT) Detection and Mitigation
- Distributed DoS (DDoS) Attack Mitigation
- Endpoint Protection and Security
- Network Forensics
- Identity & Access Management (IAM)
- Intrusion Detection and Prevention Systems
- Managed and Professional Security Services
- Network Access Control (NAC)
- Public Vulnerabilities
- SIEM and Log Management
- SSL Certificates
- Strong Authentication
- Unified Threat Management and Next-Gen FW
- Vulnerability Management
- Web and Email Content Filtering
- Web Application Firewall (WAF)

Strategic Analysis: Stratecast Secure Networking

- Examination of market dynamics
- Creation and presentation of market dimensions
- Examination of market participants' strategic movements
- Creation and presentation of market growth recommendations
- Advanced Threat Detection and Mitigation
- Cloud Security
- Desktop Virtualization
- File Sharing and Synchronization
- Hardware-embedded Security
- Identity and Access Management (IAM)
- Identity Assurance and Strong Authentication
- Network Security Usability
- Secure Containerization and MDM
- Secure Software Development
- Software Defined Networking (SDN)
- Tokenization

Legal Disclaimer

Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Our customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for customers' internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, write to:

Frost & Sullivan

331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041

Source: Frost & Sullivan