Market Outlook: Network Access Control (NAC), 2018-2023, Worldwide

January 2018

Abridged Report for Pulse Secure

Copyright 2018 © Quadrant Knowledge Solutions Private Limited. No part of this report may be reproduced or published, orally or in written form, or distributed in any form to anyone outside client’s organization without prior written permission of Quadrant Knowledge Solutions.

Copyright 2018 © Quadrant Knowledge Solutions Private Limited

All information contained in this report are proprietary to and copyrighted by Quadrant Knowledge Solutions and are to be used by client’s internal organization only. No part of this report may be reproduced or published, orally or in written form, or distributed in any form to anyone outside client's organization without prior written permission of Quadrant Knowledge Solutions.

Disclaimer: While significant effort has been made in ensuring the accuracy of this research findings as presented in this report, Quadrant Knowledge Solutions accepts no liability what so ever for consequences of any actions taken upon the findings of the report.
Table of Contents

Executive Overview

• NAC Adoption
• Industry Vertical Trends
• Competition Dynamics & Trends

Key Market Drivers

Market Background and Technology Trends

Capabilities of a Modern NAC Solution

Market Forecast Analysis

• Market Forecast Analysis by Total Market
• Market Forecast Analysis by Industry Verticals
• Market Forecast Analysis by Customer Segments

Competition Landscape and Analysis

• Competitive Landscape Quadrant
• Vendor Profile: Pulse Secure

Research Methodologies
Executive Overview

Quadrant Knowledge Solutions Network Access Control (NAC) Market Outlook research provides strategic information to the market participants, and to technology users to evaluate different vendors capabilities, competitive differentiation, and its market position.

NAC technologies have evolved significantly from early focus on authentication and authorization of managed endpoints to focus on securing BYOD and guest-access, such as business partners, contractors, visitors, and others. NAC solution continue to evolve driven by significant adoption of smart IoT-enabled devices.

NAC Adoption
Global NAC Market to reach $5.37 billion by 2023

Global NAC market is expected to grow significantly in the next five to six years from a market size of $997.3 million in 2017 to $5.37 billion by 2023. The market which has grown by 28.4% in 2017 is expected to grow at a compound annual growth rate (CAGR) of 32.4% from 2017-2022.

The long-term trend for NAC market indicates that the developed regions of North America and Europe market continue to be predominant buyers. However, driven by increasing awareness of NAC benefits, increasing regulation requirements, and adoption of digital technologies by large organizations, Asia Pacific region NAC adoption will continue to gain traction.

Industry Vertical Trends
Banking & financial services (BFS) and healthcare industry to grow at an above average growth rate
Globally, banking & financial services, education, government, and healthcare sectors are the primary users of NAC solutions. Together they contributed to a market share of nearly 80% with an individual share of 29.9%, 18.5%, 16.1%, and 14.9% respectively in the year 2017. However, industry trends reflect that the adoption of NAC technologies will mark presence in each industry vertical, because businesses are embracing smart digital technologies.

### Competition Dynamics & Trends

Cisco, ForeScout Technologies, Pulse Secure, and HP Enterprise are positioned as the top 4 overall technology leaders and are the top four top selling enterprise NAC solutions. These companies provide comprehensive NAC solution targeting large enterprise organization in improving their network visibility and granular policy implementation.

### Key Market Drivers

*Widespread adoption of smart IoT-devices is making significant impact on technology development as well as market growth*

Followings are the key factors that are driving the market growth:

**Global Regulations are Increasingly Becoming Complex**

Stringent compliance requirements, driven by regulations, such as FISMA, PIC-DSS, NERC, ISO/IEC 27001, and the GDPR, is significantly impacting the overall network and cyber security market. While compliance to the global regulations helps in improving organization’s security, non-compliance means higher risk of
information theft or misuse, huge penalty, negative publicity, and such others. Global regulations are increasingly becoming complex, requiring the organizations to focus on building robust security infrastructure and implementing best practices. The upcoming EU general data protection regulation (GDPR) taking effect from May 2018 is expected to have a significant impact on the overall network and cyber security market. Organizations are required to account for all sensitive data and the access granted to it. GDPR regulation includes a provision of fine up to 4% of annual turnover or 20 million Euros, whichever is higher. NAC solution helps organizations in securing a wide range of devices and users and helps organizations in improving compliance to global regulations and avoid costly security breaches.

**NAC Solutions to Secure Mobility and BYOD**

Increasingly popularity of mobility and bring-your-own-device (BYOD) implementation have significantly increased the organizations risk factors. Also, management and access control of wide variety of mobile devices with multiple versions of software have further stimulated the risk. It is very important for security and risk management professionals to secure corporate network with BYOD security policy formulation and implementation across organization networks. Access of corporate resources, services, and applications from a mobile device extends all of the risk factors. In addition, BYOD has its own specific challenges as organizations have limited administration controls of these BYOD devices. NAC technologies helps in securing BYOD and mobile access by providing comprehensive visibility and enabling granular access policy implementation. It provides a centralized platform to manage access of all the systems that govern BYOD-related policy.

**IoT and NAC**

IoT devices are increasingly becoming an integral part of business as well as industrial operations. It is widely being adopted from a simple functionality of tracking product use and re-order alerts to a complex application of interconnected products with built-in intelligence to communicate and take actions. Widespread adoption of smart IoT devices in various business and industrial applications have significantly increased attack surface as well as number of potential threats. Emergence of IoT devices is making significant impact in the technology development as well as market growth.

**Improved NAC Technology Capabilities**

NAC technologies have significantly evolved in recent years to improve comprehensive capabilities for providing advanced level of network visibility, posture assessment, granular access control and policy enforcement, and effectively addressing challenges due to BYOD, WYOD, guest-access, cloud applications & services, and IoT technologies. Modern NAC solutions support integration with other security technologies that significantly enhances NAC
performance and organization’s overall network defenses. Introduction of security automation and orchestration capabilities are further disrupting the market and are increasingly finding traction amongst large enterprise organization. These enhanced capabilities coupled with growing awareness of NAC solution benefits is expected to contribute significantly to the market growth of NAC vendors.

**Market Background and Technology Trends**

*NAC Technologies are Evolving Towards Security Automation and Orchestration (SAO) for Comprehensive Network Security*

Network Access Control (NAC) is an approach in network security to manage and control access of endpoint devices and users to corporate networks based on the organizations security policies. Organizations access policies can be based on endpoint configuration, authentication, or user’s identity. NAC technologies have evolved significantly from early focus on authentication and authorization of managed endpoints to focus on securing BYOD and guest-access, such as business partners, contractors, visitors, and others. NAC solution continue to evolve driven by significant adoption of smart IoT-enabled devices.

The first generation of NAC systems (NAC 1.0) was introduced to prevent access to infected computers into corporate network to avoid spreading of malware. The second generation of NAC systems (NAC 2.0) included capabilities for endpoint visibility, access, and security features to help organizations in implementing robust security policies driven by mobility, cloud, virtualization, BYOD, and WYOD trends. NAC 2.0 system uses more coarse data to implement access policies, such as user’s data, location, business considerations, and risk management. NAC 2.0 systems provide organization capability to secure and manage the complex co-relations between users, corporate networks, devices, cloud applications, and services.

**NAC 3.0:**

*NAC Technologies are Evolving Towards Security Automation and Orchestration (SAO) for Comprehensive Network Security*

While organizations were still struggling to protect their enterprise network from BYOD and WYOD threats, widespread adoption of IoT-enabled smart devices are further disrupting the organization’s security strategy. IoT devices are increasingly becoming an integral part of business as well as industrial operations. From simple functionality of tracking product use and re-order alerts to a complex application of inter-connected products with built-in intelligence to communicate and take actions. IoT devices have significantly increased the risk-factor than BYOD. This has also resulted into increased complexities of handling thousands of security alerts on a regular basis. Organization’s internal security team often find it difficult to address these security alerts in a timely manner.
Organizations are increasingly looking at automation solutions to improve their threat response processes and implement a robust enterprise-grade defense system to secure all endpoints with an integrated network security solution. Automation provides promising and measurable benefits in terms of reduced total cost of ownership (TCO), improved capability of the security team, and reduction in breaches. While all major vendors have solutions to provide complete endpoint visibility, companies are looking at automating their threat response processes and improving response time. Vendors are expected to continue to improve their offerings with sophisticated SAO capabilities during 2018-2023. Driven by further technology innovation and maturity of artificial intelligence (AI) and machine learning (ML) technologies with expanding use cases in multiple industry solutions, it may lead to NAC 4.0 in the next five to seven years.

Capabilities of a Modern NAC Solution

A modern NAC solution includes capabilities including comprehensive network visibility and control, automated BYOD onboarding, bi-directional integration and interoperability, and automated threat detection and response. However, these technology capabilities are drawn from an overall market perspective and emerging market trends. User organizations should conduct a detailed technology evaluation with the analysis of specific features required as per their own organization-specific and industry-specific requirements. Quadrant Knowledge Solutions, with analyst briefing and user consulting services, can help users in evaluating different NAC technologies available in the market to suit organization’s specific requirements. Following are the key capabilities of a modern NAC solution:
**Comprehensive Network Visibility and Control:** NAC solution should provide comprehensive visibility of all endpoints (managed and unmanaged) and users (internal and guest) connected to the corporate network. It should provide contextual information in terms of user identity, device type & configuration, location, time, date, duration, and access to application and network resources. Organizations should be able to implement and enforce their granular security policy based on these attributes. For secure connectivity of BYOD, WYOD, and IoT-enabled smart devices, organizations require an ability to identity device/user and apply security policy before its connection to corporate networks. With comprehensive endpoint visibility and improved posture assessment, organizations can establish more granular policies, reduce the number of security alerts, and effectively anticipate potential weakness.

**Automated BYOD Onboarding:** This enables self-registration of users and their devices into the corporate network. NAC can perform risk assessment analysis based on the attributed, including who, what, when, and where for both user and device, and provide right level of access to the corporate network or guide towards self-remediation in case of unsafe devices. This automated provisioning helps organization in minimizing overall support and operations cost.

**Bidirectional Integration and Interoperability:** NAC solution should offer seamless integration with multiple network security, risk management, and analytics solution to improve the efficacy of NAC solution as well as organizations overall network defense system. Major NAC vendors provider uses syslog, openAPI or RESTful API to achieve integration with multiple security solutions.

**Automated Threat Detection and Response:** Due to presence of numerous smart IoT-enabled devices in the network, with no user to self-remediate, automated detection and remediation capability is important especially to large enterprise organizations. NAC should be able to automatically detect threats, identify the compromised devices, and quarantine to safeguard corporate network. With integration with best-of-breed security products, NAC solution can record contextual information and execute response based on the granular security policies.

Market Forecast Analysis by Total Market

Globally the network access control market is poised to grow significantly. With multiple successful deployments by large enterprise organizations, NAC is increasingly being seen as the key technology to improve organization’s overall security defenses. The technology is moving from early adoption to rapid growth stage of the overall product lifecycle. Large organizations from multiple industries, including banking and financial services, education, healthcare, government, IT & telecom, manufacturing, and others are looking at full-scale NAC deployments and are extending more number of devices and endpoints. Several large organizations are also considering migration from their early version of NAC with the latest NAC technologies with advanced visibility and control capabilities.

On deployment type, Global NAC market is largely dominated by on-premise deployments which constitutes 90.8% of the total market compared to SaaS-based deployment with a market share of 9.2% in the year 2017. However, SaaS-based deployment is expected to find significant adoption during the forecast year and is expected to cover approximately a third of the total market.

Vendor’s efforts in improving technology value proposition in terms of improved integration capabilities and addition of security automation & orchestration capabilities is leading the NAC investment by large enterprise organizations.

Market Forecast Analysis by Industry Verticals

Global NAC market has an important aspect along all industry vertical. Organizations are increasing embracing BYOD, smart IoT devices, and digital technologies to improve operations and thereby emerging network security challenges pose a significant risk for every organization irrespective of the industry vertical. In the global market, banking & financial services, education, government, and healthcare sectors are the primary users of NAC solutions. Together they contributed to a market share of 79.4% in the year 2017. The other major industries, include IT & telecom, manufacturing, and energy & utilities. Traditionally, adoption of security technologies is primarily driven by compliance to growing global regulations. However, organizations from several industry verticals are increasingly focusing on improving their security measure to improve overall security.

Market Forecast Analysis by Customer Segments

On customer type, large and enterprise organizations dominate the global market with a market share of 83.7%, while SMB sector constitute 16.3% of the total market in 2017. Large and enterprise organizations often prefer on-premise deployments as they can have dedicated resources to manage their extensive IT infrastructure. Small and medium businesses often go for cloud-based deployments due to lower cost, ease of installation, and maintenance.

Enterprise customer segment look for more comprehensive NAC platform. A NAC solution should provide contextual information and support automatic threat response mechanism in accordance with granular security policies. The solution should support bi-direction integration with multiple best-of-breed security, risk management, and analytics solution in the market. Overall, enterprise segment often looks for comprehensive features rather than being price sensitive.
Driven by growing competition, NAC vendors continue to focus on improving their technology platform in terms of comprehensive visibility for wide range of devices and users, integration with best-of-breed security technologies, support for hybrid deployment with availability of virtual and SaaS-based solution, addition of advanced security automation & orchestration capability, and such others.

**Competition Landscape and Analysis**

Quadrant Knowledge Solutions conducted in-depth analysis of major NAC vendors in evaluating their products, market presence, and value proposition. The evaluation is based on the primary research with expert interviews, analysis of use cases, and Quadrant’s internal analysis of the overall NAC market. This study includes analysis of key NAC vendors – Cisco, ForeScout Technologies, Pulse Secure and HP Enterprise are positioning as the top 4 overall technology leaders. These companies provide comprehensive NAC solution targeting large enterprise organization in improving their network visibility and granular policy implementation.

Driven by growing competition especially in large enterprise segment, NAC vendors continue to focus on improving their technology platform in terms of comprehensive visibility for wide range of devices and users, integration with best-of-breed security technologies, support for hybrid deployment with availability of virtual and SaaS-based solution, addition of advanced security automation & orchestration capability, and such others.

Quadrant Knowledge Solutions’ competitive landscape analysis provides a snapshot of the market positioning of the key market participants. Competitive landscape representation provides a visual representation of market participants and provides strategic insights on how each supplier ranks related to their competitors, with respect to various performance parameters based on the category of technology excellence and customer impact.

Each market participants are analyzed against several parameters of Technology Excellence and Customer Impact. In each of the parameters (see charts), index is assigned to each supplier from 1 (lowest) to 10 (highest). These ratings are designated to each market participant based on best practice research findings. Based on the individual participant ratings, X and Y coordinate values are calculated. These coordinates are finally used to make Competitive Landscape Quadrant.

### Competitive Factor Analysis – Technology Excellence

<table>
<thead>
<tr>
<th></th>
<th>Sophistication of Technology</th>
<th>Technology Application Diversity</th>
<th>Scalability</th>
<th>Competitive Differentiation &amp; Strategy</th>
<th>Industry Impact</th>
<th>Final Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weightages</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
<td>100%</td>
</tr>
<tr>
<td>Leader</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competitor 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competitor 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competitor 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Competitive Factor Analysis – Customer Impact

<table>
<thead>
<tr>
<th></th>
<th>Addressing Unmet Needs</th>
<th>Product Performance</th>
<th>Proven Record</th>
<th>Ease of Deployment</th>
<th>Customer Service Excellence</th>
<th>Final Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weightages</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
<td>100%</td>
</tr>
<tr>
<td>Leader</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competitor 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competitor 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competitor 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Quadrant Knowledge Solutions
Competitive Landscape Quadrant

Our Competitive Landscape Quadrant representation is based on the evaluation from overall NAC market perspective. Technology is an important consideration when evaluating and selecting a network access control solution and vendor. End user organizations are advised to conduct comprehensive evaluation of different NAC technologies and vendors before making purchasing decision. Users should employ a weighted analysis of the several factors important to their specific organization and industry-specific requirements.

Some of the key competitive factors user organizations should consider includes comprehensive endpoint visibility with support for wide-variety of devices, security posture assessment, access control, ease of deployment, ease of use, scalability, granular policy enforcement and management, integration of other security technologies and interoperability, price/performance ratio, global support services, and such others. NAC technology capabilities vary between different vendors’ offerings. Also, requirements of NAC features vary between SMB, large, and enterprise organizations.
Vendor Profile – Pulse Secure

https://www.pulsesecure.net/
https://www.pulsesecure.net/policy-secure/

Pulse Secure was formed in 2014 after private equity firm Siris Capital acquired the Junos Pulse business from Juniper Networks. The company acquired MobileSpaces in the same year to strengthen its mobile and BYOD security capabilities by offering mobile container features that complement its mobile VPN tunneling technology. In mid-2017, the company acquired Brocade’s virtual Application Delivery Controller product line. Presently, with a vision of providing secure access solutions for people, device, things and services, Pulse Secure offers an integrated secure access platform with visibility and enforcement capabilities for onsite, remote, mobile and cloud environments.

Pulse Secure is fiscally strong and serves more than 20,000 enterprises globally including 80% of the Fortune 500. The company has provided positive enterprise customers references including financial services, healthcare, hi-tech, manufacturing, and government. With regard to government standards, PPS system has achieved various certifications, including: Common Criteria certification, FIPS 140-2, U.S. DoD Unified Capabilities (UC) Approved Products List (APL) and JTC joint warfighting IT interoperability.

Pulse Secure sells its products through a global network of distributor and reseller partners. The company offers an array of professional services and mature technical support services from follow the sun support and training to dedicated account management. The company also has a growing list of partnerships and interoperability with popular network and security infrastructure vendors. Along its NAC offering, Pulse Secure provides a Secure Access portfolio comprised of virtual private network (VPN), mobile security (container), application delivery controller (ADC), and cloud security solutions.

Pulse Policy Secure (NAC) Key Findings

- Pulse Policy Secure (NAC) offers extensive technical acumen inclusive of deployment, manageability and scalability, advanced visibility and enforcement features, and automated response capabilities – earning Pulse Secure a technical leader ranking and distinction among the top four bestselling NAC solutions.
- Pulse Secure offers flexible, and cost-effective implementation with built-in, high performance RADIUS and rich device profiling, layer-2 and layer-3 802.1x enforcement leveraging popular switch, wireless, firewall, SIEM and mobile infrastructure interoperability, and a granular policy engine with pre-defined and custom controls.
- Solid guest and BYOD management, as well as device profiling applying agent or agentless technologies to enable rich pre-connect and continuous post-connect visibility, including classification and response to IoT devices.
- Unique VPN/NAC industry advantages for existing Pulse Secure VPN customers in terms of: rapid NAC deployment, consistent VPN to NAC endpoint
policy migration, use of unified VPN/NAC client, and 360-degree visibility (remote user/device activity, pre-connect and post-connect), and unified VPN/NAC appliance administration.

- Enterprise-class scale with one appliance (physical or virtual) supporting 50,000 concurrent users and Pulse One manager for unified system administration for millions of endpoints – suitable for global enterprises, government, and large MSSPs.

Overview

The Pulse Secure network access control solution offers enterprises an easy to deploy, use, and extend system that provides 360-degree visibility with security enforcement to control managed, unknown, and IoT devices connecting locally or remotely to the network. The vendor-agnostic solution, essentially Pulse Policy Secure (PPS), consists of three primary components: Pulse Secure Profiler, Pulse Policy Secure, and Pulse Client.

Pulse Secure Profiler dynamically identifies and enables automatic and custom classification of both managed and unmanaged devices, to provide operational visibility, reporting and policy-based controlled access to networks and resources based on the user, device, applications and other attributes. Pulse Secure’s profiling features offer continuous profiling of the host with agent-based and agentless operation using a variety of methods, including DHCP, SNMP, Nmap, WMI, SSH, EMM, and HTTP session details.

Pulse Policy Secure is a context-aware policy engine that applies granular policies for monitoring, reporting, and access enforcement based on user, role, device, location, time, network, and application. Unlike most other NAC solutions, Policy Secure provides an in-built, high-performance, proven RADIUS server – offering a lower total cost of deployment. Enterprises can purchase the Pulse Secure Profiler to gain network visibility, and subsequently purchase PPS for enforcement features.

Enforcement can be flexibly enabled at Layer 2 leveraging 802.1X/RADIUS, and at Layer 3 enabling NAC and perimeter traffic control through next-generation firewalls. The system works with popular 802.1X-enabled switches, 802.1X/RADIUS-enabled wireless access points, NGFWs, SIEMS and EMMs (essentially core network and security infrastructure that satisfies the vast majority of typical enterprise NAC deployments). A granular policy engine allows for pre-defined and custom visibility, monitoring and response controls including the means to identify and respond to Internet of Things (IoT) exposures.

A unified Pulse Client delivers endpoint assessment and monitoring across Windows, Mac OS mobile devices, and smart IoT devices. The Client includes granular Host Checker functionality, enabling the activation of predefined policies or the custom definition of policies to assess devices attempting to connect to network resources. If devices pass the host check policy and the user/device is authenticated, appropriate network access is granted. Post connection, Host Checker continually monitors device compliance. This is accomplished by using compliance information from the Pulse Client (agent or agentless) and optionally from third-party EMM solutions.

Implementation and Scale
Operationally, Pulse Policy Secure set up is relatively easy to implement and maintain. Pulse Policy Secure can be flexibly deployed and scaled using multi-purpose physical (PSA series) or virtual (VMware, Hyper-V & KVM) appliances. Pulse Policy Secure easily integrates with existing heterogeneous infrastructure, leveraging an open architecture that supports a native 802.1X supplicant. It comes with an embedded, standards-based RADIUS Server, IF-MAP Server, and EMM support. The system supports popular Firewall, SIEM and EMM interoperability described further. Pulse Secure has considerably less components, simpler deployment and greater infrastructure operability when compared to 802.1x NAC infrastructure vendors.

Pulse Policy Secure is managed centrally using Pulse One, an IT administrative interface that is powerful, yet simple to use. It saves operators time managing a distributed NAC (as well as combined VPN and NAC) infrastructure by centrally managing appliances and policies – individually or by group designation. Pulse One provides a dashboard of appliance status to monitor overall system health and unifies operational and compliance reporting by providing insight across devices and users. Unlike conventional NAC suppliers, Pulse Policy Secure displays a 360-degree view of pre- and post-connected network devices, as well as remote connected devices when combined with the Pulse VPN solution.

Pulse Secure offers a flexible and scalable architecture that simplifies the end user experience, while covering a broad array of access use cases. Leveraging embedded RADIUS physical and virtual appliances, a unified client, and cloud-based Pulse one management, Pulse Policy Secure offers assured means to scale-out. A single PSA7000 appliance (physical or virtual) can support 50,000 concurrent users – making it the highest performing NAC appliance in the industry (according to commercially available data). The Pulse Secure solution ships with an embedded Radius server that speeds NAC processing, simplifies network planning, and reduces total cost of ownership. A small enterprise can manage one or more PPS appliances directly. For larger, distributed environments, the Pulse One management system can centralize administration for up to 400 appliances. This capability enables a Fortune 500 customer to manage over 1M endpoints with Pulse Policy Secure, which can theoretically scale to 20M endpoints, suitable for global enterprises and large MSSPs.

**NAC/VPN Advantages**

Pulse Secure customers using Pulse for VPN have a convenient way to add NAC capabilities. Many enterprises either have former (end of life) Juniper VPN appliances, have upgraded to Pulse Connect Secure (VPN) appliances, or have purchased a Pulse Secure Access Suite. With a Pulse Secure VPN in place, enterprises can import existing endpoint security configuration requirements from the VPN right into their NAC for expedited deployment, consistent security policies, and simplified administration. The unified Pulse Client makes it simple for users to gain protected access to applications and data remotely via VPN or locally via the Wi-Fi network regardless of device.

For example, the VPN/NAC combo user experience is enhanced by seamless roaming between remote and local access as the VPN enables dynamic sharing of user session data with the SSL VPN, seamlessly transitioning remote access user sessions to LAN user sessions at login, or alternatively local LAN user sessions into remote access sessions — uninterrupted access to the LAN through the same or different Pulse Policy Secure...
instances, without re-authentication to enable “follow-me” policies no matter the user’s device or worldwide location.

**Enforcement and Interoperability**

Enforcement for PPS can be flexibly enabled at Layer 2 leveraging 802.1X/RADIUS; at Layer 3 using an overlay deployment or in a mixed mode using 802.1X for network admission control and a Layer 3 overlay deployment for resource access control via next-generation firewalls. It fully integrates with popular 802.1X-enabled switches such as those from Cisco, HP and Juniper, and also integrates with 802.1X/RADIUS-enabled wireless controllers such as Cisco, HP/Aruba Wireless, and Arris/Ruckus Wireless networks. For example, when PPS 802.1x is deployed with Juniper Networks EX Series Ethernet Switches additional enriched policy enforcement can be invoked.

Pulse Policy Secure performs pre-admission and post-admission compliance check with host checker and isolates the endpoint if it is not compliant with corporate policies. Host Checker detects the latest anti-malware software, personal firewalls, installed software and processes, vulnerability patches, hard disk encryption, ports, machine cert, and other criteria to validate whether endpoints are compliant with corporate policies and to prevent potential threats. The policy engine provides pre-defined and custom polices to address a wide variety of endpoint security issues.

The system includes a complement of standard NAC functions for guest management (both self-serve and sponsored) and EMM integration, such as with MobileIron, Microsoft and Airwatch. PPS can also identify, classify and respond to IoT and Industrial Internet of Things (IIoT) devices as a fundamental control utilizing its policy engine and available classifications (device attributes). PPS supports open interoperability standards such as API, Syslog, and IF-MAP protocols. PPS works with popular SIEMs such as Splunk, IBM, Micromuse (ArcSight) and others — where by PPS can send endpoint and user activity content, events and incidents. PPS also integrates with next-generation firewalls (Juniper, Palo Alto Networks, Fortinet, and Checkpoint) for identity-based context-sharing and alert-based admission control. This bidirectional integration provides granular access control utilizing:

- Identity-based admission control where Pulse Policy Secure sends endpoint contextual identity information to the firewall for granular enforcement at the perimeter; and
- Alert-based integration where the firewall sends threat alerts to Pulse Policy Secure which takes automated action to quarantine or block compromised devices.
Research Methodologies

Quadrant Knowledge Solutions uses comprehensive approach to conduct global market outlook research for various technologies. Quadrant’s research approach provides our analysts with the most effective framework to identify market trends, technology trends, and helps in formulating meaningful growth strategies for our clients. All the sections of our research report are prepared with considerable amount of time and thought process before moving on to the next step. Following is the brief description of the major sections of our research methodologies.

Secondary Research

Following are the major sources of information for conducting secondary research:

Quadrant’s Internal Database

Quadrant Knowledge Solutions maintains a proprietary database in several technology marketplaces. This database provides our analyst with an effective foundation to kick-start the research project. This database includes information from the following sources:

- Annual reports and other financial reports
- Industry participant lists
- Published secondary data on companies and their products
- Database of market sizes and forecast data for different market segments
- Major market and technology trends

Literature Research

Quadrant Knowledge Solutions leverages on several magazine subscription and other publications that covers wide range of subjects related to technology research. We also use extensive library of directories and Journals on various technology domains.
Our analysts use blog posts, whitepaper, case studies, and other literatures published by the major technology vendors, online experts, and industry news publications.

**Inputs from Industry Participants**
Quadrant analysts collect relevant documents such as whitepaper, brochures, case studies, price lists, datasheet, and other documents from all major industry participants.

**Primary Research**
Quadrant analysts use two-step process for conducting primary research that helps us in capturing meaningful and most accurate market information. Following is the two-step process of our primary research:

**Market Estimation**: Based on top-down and bottom-up approach, our analyst analyses all industry participants to estimate their business in the technology market for various market segments. We also seek information and verification of client business performance as part of our primary research interviews or through detailed market questionnaire. Quadrant research team conducts detailed analysis of the comments and inputs provided by the industry participants.

**Client Interview**: Quadrant analyst team conducts detailed telephonic interview of all major industry participants to get their perspectives of the current and future market dynamics. Our analyst also gets their first-hand experience with vendor’s product demo to understand their technology capabilities, user experience, product features, and other capabilities. Based on the requirements, Quadrant analysts conduct interview with more than one person from each of the market participants to verify the accuracy of the information provided. We typically engage with client personnel in one of the following functions:

- Strategic Marketing Management
- Product Management
- Product Planning
- Planning & Strategy

**Data Analysis: Market Forecast & Competition Analysis**
Quadrant’s analysts’ team gathers all the necessary information from secondary research and primary research to a computer database. These databases are then analyzed, verified, and cross-tabulated in numerous ways to get the right picture of the overall market and its segments. After analyzing all the market data, industry trends, market trends, technology trends, and key issues, we prepare preliminary market forecasts. This preliminary market forecast is tested against several market scenarios, economic scenario, industry trends, and economic dynamics. Finally, the analyst team arrives at the most accurate forecast scenario for overall market and its segments.

In addition to market forecasts, our team conducts detailed review of industry participants to prepare competitive landscape and market positioning analysis for overall market as well as for various market segments.
Final Report Preparation

After finalization of market analysis and forecasts, our analyst prepares necessary graphs, charts, and table to get further insights and preparation of final research report. Our final research report includes information including market forecast; competitive analysis; major market & technology trends; market drivers; vendor profiles, and such others.