



Network Access Control (NAC) Market, Global, Forecast to 2022

NAC Evolving As Enterprise Networks Expand Beyond Secure Walls

Abridged Market Research Report

www.frost.com

October 2018

List of Tables	3
List of Figures	3
Introduction: Emerging Trends Driving NAC to Evolve Beyond the “Traditional” AAA Functionality in 2018.....	4
NAC Market Overview	4
<i>The Issue of 802.1X</i>	6
<i>The Importance of NAC</i>	7
<i>NAC Features and Functions</i>	7
NAC Market Drivers	8
<i>Endpoint growth driven by IoT and BYOD</i>	8
<i>Shortage of skilled security professionals</i>	9
<i>Organizations move to the cloud</i>	9
<i>Convergence of IT and OT</i>	9
<i>Security Orchestration</i>	9
Macro Trends Impacting NAC.....	10
<i>Supporting IoT, BYOD and Mobility</i>	10
<i>Breaking down IT and OT silos</i>	10
<i>Migration to cloud and SaaS</i>	10
Market Share and Competitive Analysis—Total NAC Market.....	11
<i>Large Enterprise dominates NAC</i>	13
ForeScout—the NAC Market Growth Leader	13
<i>ForeScout’s Growth Strategy</i>	14
The Last Word.....	15
<i>Predictions on the NAC market</i>	15

List of Tables

Table 1: Total NAC Market Global, Market Shares, 2016 and 2017	11
Table 2: Total NAC Market Global, Market Share Gains, 2017	12

List of Figures

Figure 1: Total NAC Market Global Metrics, 2017	5
Figure 2: Total NAC Market Global, Market Shares, 2017	11
Figure 3: Total NAC Market Global, Market Share Gains, Top Vendors, 2017	12
Figure 4: Large Enterprise Segment NAC Market Global, Market Shares, 2017	13

NETWORK ACCESS CONTROL MARKET

INTRODUCTION: EMERGING TRENDS DRIVING NAC TO EVOLVE BEYOND THE “TRADITIONAL” AAA FUNCTIONALITY IN 2018

Network access control (NAC) is a foundational network security defense. The premise of NAC is the security principle that end-users/endpoints can be provided policy-based access to different parts of a network and blocked, quarantined, or redirected if there are Indications of Compromise (IOC) or vulnerabilities. NAC also provides endpoint visibility after data passes a cyber security perimeter, but before data is enriched and taken into storage by a security information and event management (SIEM) platform.

Rules to ensure legitimate end-user device and role-based access are critical to the overall health of the network. Devices and endpoints are ultimately the place where intrusions to networks matter, and the last chance to defend or detect a network breach. Endpoint devices include desktop PCs, notebook PCs, servers, tablets, smartphones, virtual desktops and various Internet of Things (IoT) devices.

The “traditional” focus of NAC has been Authentication, Authorization, and Accounting (AAA). At its core, NAC is all about enabling mobility and dynamic security. However, the enterprise network no longer sits within four secure walls. It extends to wherever employees and data travel. Mobility, digitization, and IoT are changing the way we live and work. The result is that networks are expanding, resulting in increasing complexity of managing resources and disparate security solutions.

The enterprise network no longer sits within four secure walls. Mobility, digitization, and IoT are changing the way we live and work.

NAC is evolving toward improved visibility and monitoring of network devices, more security features, and orchestration with other security products such as Next-Generation Firewalls (NGFW), SIEM, and Web Content Filters. Today’s NAC security solutions must also deliver profiling, policy enforcement, guest access, BYOD on-boarding and more, in order to offer IT-offload, enhanced threat protection, and an improved end-user experience.

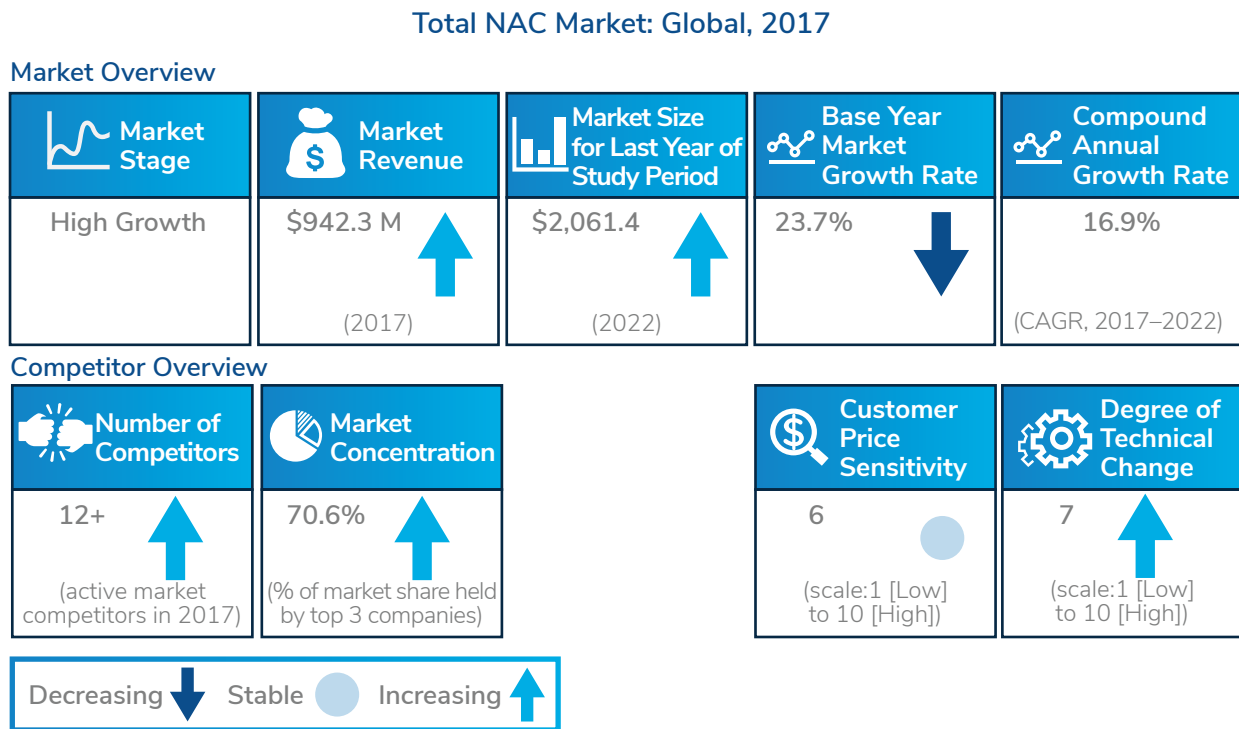
The increasing level of malware and cyber attacks is also driving additional NAC investments. Network visibility into endpoints and devices is critical. Every device on a network is a potential attack or reconnaissance point that must be discovered and secured. NAC vendors continue to innovate to meet new usage cases—most notably IoT, Operational Technology(OT), and cloud.

NAC MARKET OVERVIEW

- NAC is a rapidly growing market. Revenues are expected to grow from 2017 – 2022 at a 16.9% CAGR, reaching \$2.1 billion.
- The top three NAC vendors controlled over 70% of the market in 2017. There are several smaller, innovative players.

- Emerging trends driving NAC demand are the growth of IoT, mobility, BYOD, and cloud. Essentially, the network enterprise is expanding beyond the “traditional” secure walls.
- NAC is evolving beyond the “traditional” AAA functionality. Vendors are developing improved visibility, agentless technology, granular policy settings, classification, segmentation, and contextual awareness.
- Security orchestration is also forming. Security vendors with broad product portfolios are integrating their solutions with NAC. Standalone NAC vendors are integrating with third-party partners.

Figure 1: Total NAC Market Global Metrics, 2017



Note: All figures are rounded. The base year is 2017.
Source: Frost & Sullivan

The NAC market has seen strong, steady growth for several years, driven by the increasing number and diversity of endpoint devices. There are diverse operating systems (OSs). Each has its own management and vulnerability issues. Increasingly, endpoint devices are mobile and not on-premises. Consequently, new NAC technology is needed as network enterprises expand beyond the “traditional” secure walls.

Traditional AAA is not enough in today’s networks. Customers look to NAC to solve various problems such as visibility (who and what is accessing the network); control (policy enforcement); protection (appropriate level of access); automation; detection/blocking of unknown devices/users; data protection; incident analysis and response; threat protection; audit and compliance requirements; guest access; BYOD on-boarding; and IoT devices.

In 2017, the NAC market reached \$942.3 million—an increase of 23.7% over 2016. The increasing number of endpoints per deployment is increasing the average selling point (ASP). NAC vendors are adding more features and capabilities. While Enterprise and Large Enterprise customers dominate NAC, vendors seek to expand penetration into smaller segments, thus growing the market further.

Most NAC solutions are deployed as a physical appliance. However, higher growth is occurring for virtual appliances, software platforms, and NAC as SaaS. A growing trend is organizations moving workloads to the cloud, both public and private. Many NAC vendors are developing support for AWS, Azure, and other cloud computing platforms.

An important concept in network security is contextual awareness. Endpoint visibility may be a vague term; but to properly investigate security alerts pertaining to an endpoint, a security team needs to know how the endpoint is attached to the network, its posture assessment, the certificates on the endpoint, applications running on the endpoint, and other even greater granular detail.

Next generation NAC is able to facilitate bidirectional communication with other network IT and network security solutions.

One of the key aspects of next generation NAC is the ability to facilitate bidirectional communications with other network IT and network security platforms. Integration with other platforms/technologies ostensibly makes NAC an ally to other network security platforms. Ultimately, NAC is the last line of defense in network security. If perimeter network defense products represent the front door of cyber defense, NAC is the back door.

NAC empowers IT administrators to define, implement, and enforce granular access policies for connecting endpoints based on user identity and role; device type, and its security posture and location; connection type; and other relevant factors. To accomplish these objectives, NAC products must be able to detect connecting endpoints regardless of device type (e.g., smartphone, laptop, or wireless router) or connection type (e.g., wired, wireless, or remote). NAC products are designed to operate with or without on-device agents. The installation of an agent requires the full lifecycle management of agents and may not be possible on the growing number of IoT and OT devices.

The Issue of 802.1X

NAC technologies have been protecting networks for over 15 years. The majority of traditional NAC deployments used the 802.1X protocol, an IEEE 802.1X open-standard protocol for port-based network access control. 802.1X deployments require three components supporting 802.1X management: devices with a supplicant or software agent, an authenticator such as a switch, and an authentication server such as remote authentication dial-in user service (RADIUS) server.

While IEEE 802.1X is an authentication standard, it is difficult to implement. For on-premises 802.1X implementation, the level of expertise required from a network engineer is very high. Further adding to the challenges, there is a shortage of qualified security specialists.

In an 802.1X deployment, all respective endpoints, switches, servers, and RADIUS must be able to support and be configured for 802.1X. An agentless endpoint—one that does not have a supplicant, e.g., an IoT device—is authenticated based only on its media access control (MAC) address.

IEEE 802.1X is difficult to implement, requiring a high level of security expertise, and is time consuming. Next generation NAC provides agentless technology, as well as faster and easier deployment.

The growth of unmanaged devices poses further challenges for “traditional” NAC. Many of these devices are non-802.1X compliant. A next generation NAC can provide agentless capabilities, flexible enforcement, and centralized control. This simplifies deployment, and does not require a high level of expertise by IT.

Frost & Sullivan forecasts that there will be 45.4 billion connected devices by 2023. The high growth of IoT poses challenges to enterprise networks, since these devices are mostly non-802.1X compliant.

The Importance of NAC

The growth of BYOD, guest and contractor access, and IoT has made it evident that the network is no longer composed of securely managed devices. NAC is more than an authentication mechanism for endpoints and users. It enables an organization to gain visibility into what exists on the network, and where it connects—both wired and wireless.

As previously noted, there is a growing wave of unmanaged devices driven by IoT and mobility. Next generation NAC is making implementation easier with agentless technology, improved tools and automation.

With the growing diversity of devices, there are different operating systems (OS) and devices that do not have the resources for embedding an agent. Also, IoT and Operational Technology (OT) devices are new targets for threats. Next generation NAC is critical for visibility and assessment of these devices, to reduce risk and attack surface.

Enterprise scalability is an important feature for keeping pace with device growth. Organizations have invested in many different security technologies such as SIEM and NGFW. NAC is able to orchestrate with these technologies, as well as provide them with IoT and OT device context.

NAC Features and Functions

There are several issues customers seek to solve with a NAC investment. Not all NAC vendors have all of these functions and features, but the following are frequently offered.

- **Visibility of the endpoints and the context:** This informs the NAC what type of devices there are; who those devices belong to; when they connected; and where they are located. This provides critical data points for more granular policy and access control.
- **Control:** Customers need a high degree of scalability and flexibility to enforce policy.
- **Protection:** Providing only the appropriate level of access is a type of network perimeter.
- **Segmentation:** Related to protection, segmenting the network is critical to ensuring proper access, reducing the attack surface, stopping lateral threat movement, and containing threats. A properly segmented network limits the damage of a breach.
- **Centralized Control:** Customers can make centralized changes to policy, and have them immediately enforced network-wide. This is also known as single-pane of glass.

- **Automation for IT Administration and End-Users**
- **Endpoint Compliance and Posture:** Verifies endpoint posture assessment and remediation options.
- **Ease of Deployment:** This usually includes a tool that enables configuration of all necessary settings plus basic customization of Guest, BYOD, and Secure Access (802.1X) flows.
- **IoT / Secure Access:** Includes on-boarding, identification and policy enforcement for IoT devices. Some NAC vendors allow customers to create profiles that recognize devices that are unique to their operation.
- **Granular Policies:** Applied based on context such as location, device, user and compliance.
- **Classification of device identity:** Characteristics such as OS, device type, and business function assist in identifying devices. Classification is also important in updating device profiles for IoT and OT devices.
- **Automated Threat Response:** Contains compromised devices in real time.

NAC MARKET DRIVERS

The major growth drivers of the NAC market are:

- Endpoint growth driven by IoT and BYOD
- Shortage of skilled security professionals
- Organizations moving to the cloud
- Convergence of IT and OT
- Security Orchestration

Endpoint growth driven by IoT and BYOD

The number of connected devices is expanding greatly; as noted previously, Frost & Sullivan projects 45.4 billion connected devices by 2023. The majority of these will be IoT devices with IP addresses. These devices include security cameras, printers, infrastructure, factory automation, building automation, healthcare equipment, and more.

Endpoints have become more mobile. Organizations must deal with BYOD and on-boarding guests. IoT and BYOD are potential threat vectors that an organization needs to manage. The volume of devices, as well as diversity of OS's and devices must be factored in. As the volume of devices and OS's and their diversity increases, the ability of an organization to see and control devices declines.

Organizations need to stay up to date with NAC, or acquire NAC, in order to protect their networks from this wave of unmanaged devices. Agentless technology will be a key factor.

Shortage of skilled security professionals

An oft-cited issue for enterprises is the severe shortage of skilled security professionals. This is challenging organizations to keep abreast of cybersecurity threats. Organizations are in need of better security tools and automated systems to alleviate these limitations.

While large organizations have the resources to put together an expert team, they will likely be pressed to perform many other IT functions. Next generation NAC provides tools to offload many of the functions, and to automate their workload.

Organizations move to the cloud

Cloud adoption creates new challenges. Network administrators must deal with multiple device locations and access points. It is a heterogeneous environment with multiple vendors; and management is typically decentralized.

Organizations need to extend visibility into public cloud, such as AWS, Microsoft Azure and Google Cloud Platform. They also need to extend visibility and control into private cloud, with support for VMware vSphere and NSX, for example. NAC is providing this visibility.

Cloud customers must manage the security of their cloud instances; and NAC vendors provide solutions that support a hybrid IT implementation. NAC virtual appliances and NAC as SaaS are growing quickly as customers turn to the cloud for easy and rapid deployment, savings on energy, space, and hardware maintenance.

Convergence of IT and OT

OT networks began as simple methods to connect machines and data. This is morphing into the Industrial Internet of Things (IIoT). The OT network is a control network in which the endpoints control or measure things.

OT networks were isolated silos, but are now no longer physically separated from IT networks. Threats are moving between cyber and physical dimensions, with IT threats impacting OT networks. Many OT devices are legacy systems, and difficult to patch.

Interest in NAC for OT has been growing significantly. NAC enforces security policies across IT and OT, and expands visibility into OT. Most devices in OT cannot support agents; thus, NAC agentless technology is best suited in OT. NAC offers network segmentation to reduce OT attack surface. As IT and OT converge, the security technology used in IT, including NAC, is being applied to OT.

Security Orchestration

NAC is used to orchestrate other security tools. Network orchestration is bidirectional communication between NAC and other cyber security defenses which enhances the efficacy of each. It optimizes the relationships among the layers of a network to boost protection against hackers.

Enterprises typically have a dozen or more security products operating as independent security management silos. NAC orchestration breaks down this disjointed approach thereby coordinating enterprise-wide security response, and cutting down the time hackers have to exploit system vulnerabilities.

NAC vendors are able to extend network, security and management interoperability technologies to their third-party partners for security products such as Next-Generation Firewalls, IDS/IPS products, ATD, SIEM, User Behavioral Analysis, Network-based Anomaly Detection and MDM/EMM, Web Content Filters, CASB and more. Many NAC vendors offer a centralized console to manage orchestration.

MACRO TRENDS IMPACTING NAC

NAC vendors are expanding the scope of their work beyond the traditional IT perimeter. Innovations in other technologies drive change in NAC. These macro trends are:

- Supporting IoT, BYOD and Mobility
- Breaking down IT and OT silos
- Migration to cloud and SaaS

Supporting IoT, BYOD and Mobility

IoT, BYOD and mobility are increasing. Most IoT devices do not have the resources to accommodate an agent therefore, agentless technology is required. Device profiling databases for IoT and BYOD are being developed and used by NAC vendors.

Being able to integrate with third-party systems for device validation, in addition to device profiling, is increasingly important for modern NAC systems to accurately identify IoT devices so they can apply appropriate policies. NAC vendors also engage with third-party vendors such as Enterprise Mobility Management (EMM) and Mobile Device Management (MDM) for securing mobile devices.

Breaking down IT and OT silos

The focus of NAC on OT has emerged in the past two years. Customers are breaking down technical silos between OT and IT. While these two areas have developed independently, with different objectives, organizations still seek improved efficiency.

NAC vendors are working on delivering broader and deeper OT visibility and control. The profile classification developed for IoT is being extended to OT devices. Network segmentation based on dynamic classification has become a best practice. Segmenting the network is critical to ensuring proper access, reducing the attack surface, stopping lateral threat movement, and rapidly containing threats. A properly segmented network limits the damage of a breach.

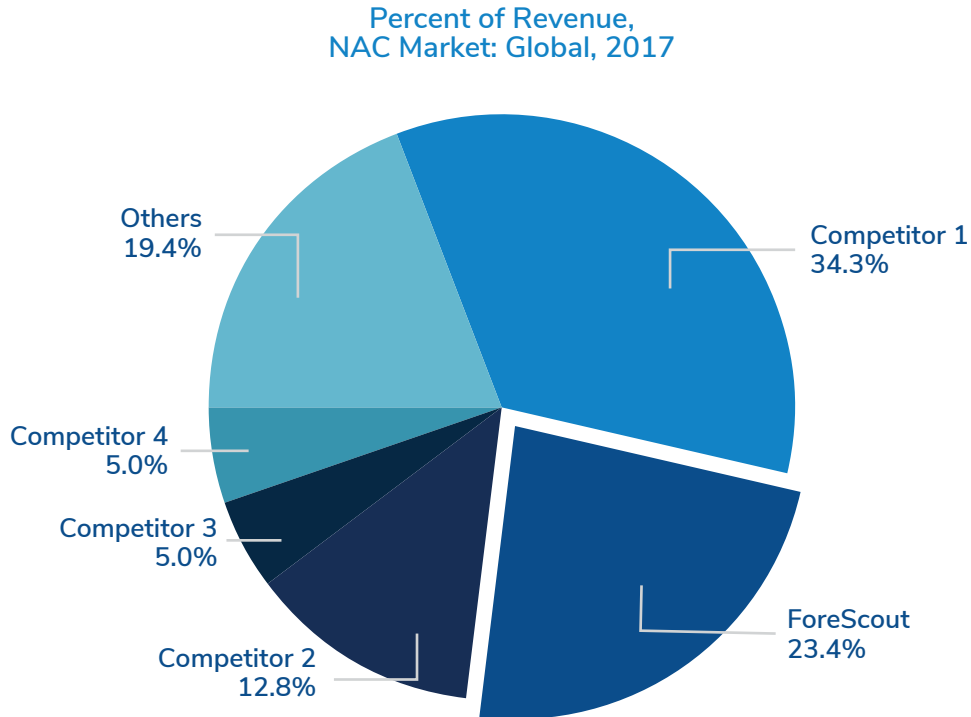
Migration to cloud and SaaS

Customers are accelerating their movement to the cloud. They are turning to the cloud for easier and more rapid deployment, energy and space savings, scalability, and reduced hardware maintenance costs. NAC vendors are extending visibility into public clouds with support for AWS, Microsoft Azure, and Google Cloud Platform. They are also extending visibility and control into private clouds, with support for VMware vSphere and NSX. The high growth areas for NAC are virtual appliances and NAC as SaaS. NAC vendors have cloud platforms for Managed Service Providers and Managed Security Service Providers (MSP/MSSPs).

MARKET SHARE AND COMPETITIVE ANALYSIS—TOTAL NAC MARKET

NAC is a competitive, high growth market. The top 3 vendors continue to hold their dominant positions.

Figure 2: Total NAC Market Global, Market Shares, 2017



Source: Frost & Sullivan

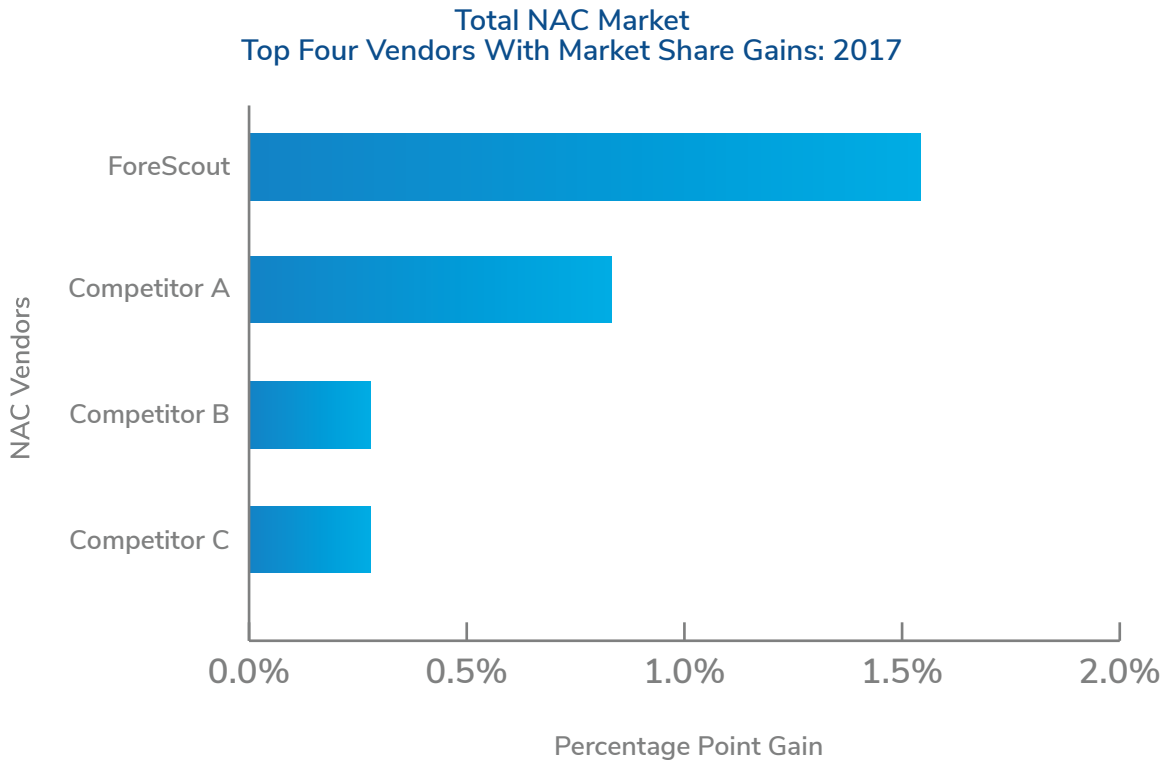
Table 1: Total NAC Market Global, Market Shares, 2016 and 2017

Company	Market 2016	Shares 2017
Competitor 1	37.2%	34.3%
ForeScout	21.9%	23.4%
Competitor 2	12.6%	12.8%
Competitor 3	4.9%	5.0%
Competitor 4	5.1%	5.0%
Others	18.4%	19.4%

Source: Frost & Sullivan

ForeScout is transitioning to high growth solutions of virtual appliances and software. It is also developing solutions for cloud and IoT. CounterACT 8 was released April 2018. The company had the highest gain in market share in 2017, at 1.5 percentage points in a market that increased nearly 24% over the previous year.

Figure 3: Total NAC Market Global, Market Share Gains, Top Vendors, 2017



Source: Frost & Sullivan

Table 2: Total NAC Market Global, Market Share Gains, 2017

Company	Market 2016	Shares 2017	Gain (Loss)
ForeScout	21.9%	23.4%	1.5%
Competitor A	2.9%	3.7%	0.8%
Competitor B	1.6%	1.9%	0.3%
Competitor C	12.6%	12.8%	0.3%
Others	61.1%	58.1%	-2.9%

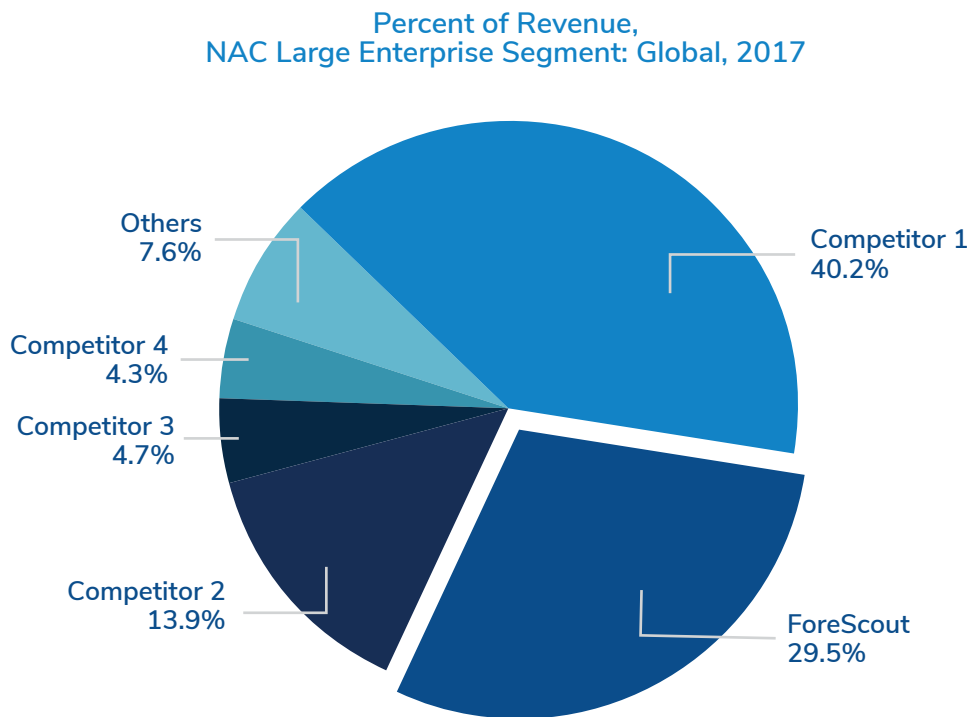
Source: Frost & Sullivan

Large Enterprise dominates NAC

The Large Enterprise market is comprised of businesses and organizations with 10,000 or more endpoints. This market segment accounts for 59% of the NAC market. Compared to smaller segments, the Large Enterprise segment has more endpoints, more complex networks, and the need for more advanced tools. Thus, there is a higher ASP in this segment. Growth is due to scaling to larger deployments, in response to increasing populations of IoT devices.

ForeScout is one of the top two vendors that dominate the Large Enterprise segment, with a combined 69.6% market share.

Figure 4: Large Enterprise Segment NAC Market Global, Market Shares, 2017



Source: Frost & Sullivan

FORESCOUT—THE NAC MARKET GROWTH LEADER

ForeScout Technologies is the fastest growing NAC vendor, garnering the highest market share gain in 2017. The company's product vision covers visibility across the campus, data center, cloud, and OT. The company was founded in 2000, and closed its IPO on October 31, 2017.

ForeScout provides visibility and control solutions to a broad range of organizations. Its agentless technology provides NAC for traditional, mobile, virtual, and IoT devices. ForeScout's "...technology orchestrates with disparate security tools to help organizations accelerate incident response, break down silos, automate workflows and optimize existing investments."

ForeScout's solution is comprised of CounterACT, CounterACT Enterprise Manager and Extended Modules. CounterACT's agentless technology discovers, classifies, assesses and controls IP-based devices. ForeScout bases its NAC capability on a visibility-first approach. When devices attempt to connect to the network, they are discovered and profiled immediately, as CounterACT interrogates the network via a combination of passive and active techniques. CounterACT 8 was released April 3, 2018.

ForeScout offers CounterACT and Enterprise Manager in both physical and virtual appliance form factors. Extended modules are sold as software add-ons to CounterACT. Deployments are split evenly between physical and virtual appliances, with an increasingly significant software license component.

While customers initially choose ForeScout for agentless device visibility and NAC, the ForeScout platform addresses additional use cases for device compliance, network segmentation, asset management, and incident response initiatives. Each leverages the foundational feature of visibility across the extended enterprise—campus, public cloud, private cloud, and operational technology (OT). ForeScout does not require vendor-specific network equipment, upgrades of existing infrastructure, or reconfiguration of each switch and switch port to support 802.1X.

ForeScout sees IT and OT converging, eventually. The company touts that its customers report seeing up to 60% more devices on their networks than previously known. This is due to the increasing number of IP-based devices without agents that ForeScout can discover. Additional customer benefits are continuous visibility, automated control based on policy, and orchestration of actions between systems. ForeScout continues to develop classifications for vertical markets and behavioral monitoring.

ForeScout's Growth Strategy

ForeScout has consistently shown strong growth in recent years. In 2017, ForeScout's revenues grew 32.4%, almost matching its 2016 growth of 32.5%. The company has outperformed the overall NAC market for several years. In 2017, ForeScout ranked second in the NAC market globally with 23.4% overall market share and 29.5% large enterprise segment market share. This represented an impressive gain of 1.5 percentage points over 2016 – the highest market share gain in the industry.

This growth is the result of ForeScout addressing the dynamic changes facing its NAC customers. Organizations are migrating quickly to the cloud, both public and private. The convergence of IT and OT is accelerating. The growth of IoT and BYOD poses challenges for organizations. ForeScout emphasizes its foundational visibility platform across the customer's extended enterprise—campus, data center, public cloud, private cloud and OT.

ForeScout's customer base includes large organizations which are dealing with the growth of device volumes and platform diversity. ForeScout counts 19% of the Global 2000 among its customer base.

ForeScout is focused on three growth areas: IoT Security, OT security, and Data Center and Cloud security. The company is addressing the dynamic changes emerging in these areas. It is expanding visibility into OT and IPv6 systems. ForeScout is delivering industry-leading classification for traditional, mobile, virtual, network infrastructure, IoT and OT devices.

ForeScout has close partnerships which enable this growth strategy. It has extended visibility into public cloud working with AWS. The company is also extending visibility and control into private cloud working with several other leading security technologies including VMWare. ForeScout engages with several key partners for its continued product development and increasing scope of visibility across the extended enterprise. The company has a broad global strategic alliance network.

ForeScout is defining best practices for IoT and OT. These include classification, assessment of posture of endpoints, segmentation, and behavioral monitoring. ForeScout has continued to develop its CounterACT NAC solution. The company has been migrating its business model from delivering physical appliances into the higher growth software solution and virtual appliance market. With its product developments and partnerships the company is targeting the high growth areas of IoT, OT and cloud.

THE LAST WORD

Predictions on the NAC market

1. Growth is being driven by cloud-centric solutions, virtual appliances, and NAC as SaaS, along with software solutions. NAC is adapting to a more mobile environment as enterprises expand beyond their traditional secure walls. Long-term success will be gained by those NAC vendors that focus on these areas.
2. IoT and the convergence of IT and OT extend NAC into new usage models. The number of endpoints will grow exponentially. NAC must be able to scale to handle this increase in endpoints.
3. Large cybersecurity vendors with broad product portfolios will want to add NAC, if they do not already have it. NAC integration enhances their product lines, which they can leverage. Security vendors will either develop NAC or will acquire a NAC vendor in order to get to market quickly.





Silicon Valley
3211 Scott Blvd
Santa Clara, CA 95054
Tel +1 650.475.4500
Fax +1 650.475.1571

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel +1 210.348.1000
Fax +1 210.348.1003

London
Floor 3 - Building 5,
Chiswick Business Park
566 Chiswick High Road,
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

877.GoFrost • myfrost@frost.com
<http://www.frost.com>

NEXT STEPS

-  [Schedule a meeting with our global team](#) to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.
-  Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.
-  Visit our [Digital Transformation](#) web page.
-  Attend one of our [Growth Innovation & Leadership \(GIL\)](#) events to unearth hidden growth opportunities.

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
3211 Scott Blvd
Santa Clara CA, 95054