FROST & SULLIVAN

Market Engineering

Global Network Access Control Market, Forecast to 2024

Innovation Continues to Be Driven by Cloud, BYOD, and the Internet of Things

Global Information & Communications Technologies Research Team at Frost & Sullivan

K45F-74

March 2020

Key Findings

Network access control (NAC) is a foundational network security defense. The premise is the security principle that end users/endpoints can be blocked, quarantined, or redirected to different parts of a network if there is an indication of compromise or vulnerabilities. NAC also provides endpoint visibility after data passes a cybersecurity perimeter, but before data is enriched and taken into storage by a security information and event management (SIEM) appliance.

Rules written to end-user devices and role-based access are critical to the overall health of the network. End-user 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.

Frost & Sullivan estimates that NAC vendors sold $1,348.8 million worth of NAC appliances, NAC-related services, and NAC software as a service (SaaS) in 2019 — a 16.1% increase over 2018.

The Covid-19 pandemic has interrupted the continued strong growth previously forecasted for NAC revenue in 2020. NAC revenue growth will drop drastically to 2.0% year over year. This is due primarily with disruptions in 2Q and 3Q of 2020. Growth is expected to resume in 4Q 2020 and continue through the forecast period. This is driven by growth of the IoT, the bring your own device (BYOD) concept, increasing mobility, more remote workers, and organizations migrating workloads to the cloud.

The growth of malware and cyber attacks also is driving NAC investments. Network visibility 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 use cases — most notably IoT, BYOD, and cloud. The result is sustained growth for the NAC market. Frost & Sullivan forecasts that NAC revenue will reach $2,214.8 million by 2024, reflecting a compound annual growth rate (CAGR) of 10.4% from 2019 to 2024.

Source: Frost & Sullivan

Market Engineering Measurements

NAC Market: Market Engineering Measurements, Global, 2019

Market Overview

Market Stage	Market Revenue	Market Size for Last Year of Study Period	Base Year Market Growth Rate	Compound Annual Growth Rate
High Growth	$1,348.8 ↑	$2,214.8 ↑	16.1% ↓	10.4%
	Million USD (2019)	Million USD (2024)		(CAGR, 2019–2024)

Competitor Overview

Number of Competitors	Market Concentration	Customer Price Sensitivity	Degree of Technical Change
13+ ↑	68.3% ↑	6 ●	8 ↑
(active market competitors in 2019)	(% of market share held by top 3 companies)	(scale:1 [Low] to 10 [High])	(scale:1 [Low] to 10 [High])

Decreasing ↓ Stable ● Increasing ↑

Note: All figures are rounded. The base year is 2019. Source: Frost & Sullivan

Recent Developments

NAC vendors continue to roll out new functions, features, and enhancements. Since the prior Frost & Sullivan report in July 2018, vendors have focused strongly on supporting IoT, IIoT, IT/OT convergence, cloud migration, SDP, and ZTN. They also continue to improve ease of deployment, such as with automated onboarding tools.

Security automation is being adopted; tasks being handled include threat detection and rapid threat response at the endpoint access level, and dynamic provisioning of NGFW with user-/device-specific policies.

IoT security is focused on detecting and continuously monitoring IoT devices for suspicious activity. This includes segmentation of different IoT/IIoT devices. More vendors are promoting taking network segmentation enterprise-wide rather than implementing in small measures. They are emphasizing more consistent implementation:

- Mobile monitoring and security for authorized end users and devices regardless of location.
- Support for multiple operating systems: iOS, OSX, Android, Windows, and Linux.
- Improved integration with third-party vendors and expanding their respective ecosystems.
- Accelerating the shift to cloud-delivered solutions.

SDP is an approach to computer security that micro-segments network access. It protect users as they access workloads and applications, and is complementary to NAC. Several NAC vendors offer SDP, and the long-term trend is for SDP to be integrated more tightly with NAC.

Source: Frost & Sullivan

Drivers

NAC Market: Key Market Drivers, Global, 2020–2024

	1–2 years	3–4 years	5th year
Endpoint growth driven by the IoT and BYOD	H	H	M
Shortage of skilled security professionals	H	H	M
Organizations move to the cloud	H	M	M
Convergence of IT and OT	H	M	M
Security orchestration and ZTN	M	H	L

Impact: **H** High **M** Medium **L** Low

Source: Frost & Sullivan

Forecast Assumptions

Factors having a POSITIVE impact on forecasted revenue:

- Continued growth of mobile devices, IoT and BYOD will drive volumes. More devices on the network will require further scaling and larger deployments.
- NAC vendors continue to develop effective solutions for cloud environments and NAC as SaaS.
- The threats against which NAC solutions need to protect will increase in sophistication and complexity. Vendors will continue to innovate, such as in delivering more operational security, automated systems, segmentation, classification, and behavioral monitoring.
- New opportunities emerge as organizations outside North America increase NAC deployments.
- Improved orchestration and integration with other security solutions such as NGFW, SIEM, and threat intelligence networks will increase NAC efficacy and justify its investment.
- NAC vendors will leverage these capabilities to make NAC the key element for ZTN.
- NAC vendors seek to expand into smaller business segments to generate new sources of revenue.

Factors having a NEGATIVE impact on forecasted revenue:

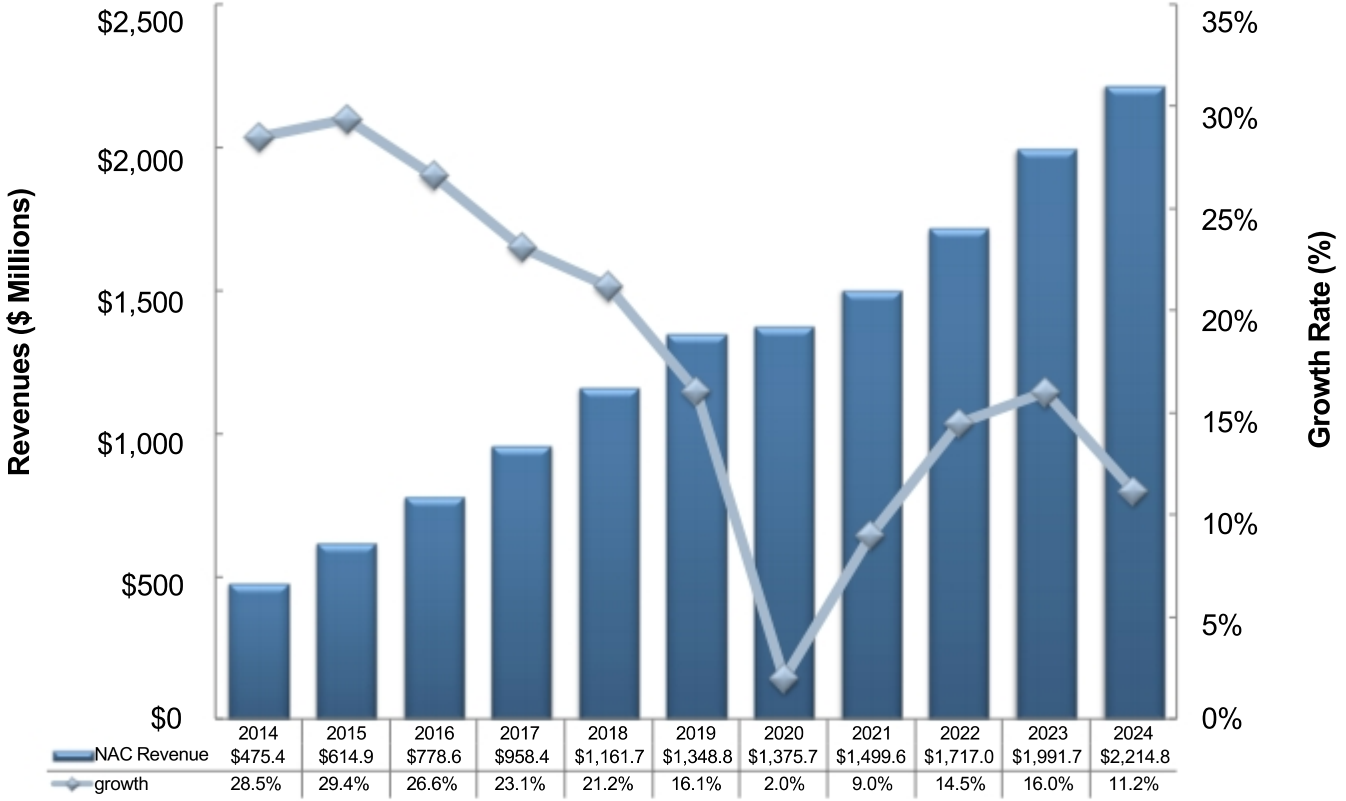
- NAC products compete with other endpoint visibility products: vulnerability management platforms, endpoint security platforms, network behavior anomaly detection companies, and even SIEM vendors are offering platforms providing visibility and knowledge about endpoints.
- Competing technologies could cut into the value of NAC contracts if customers believe they are receiving better endpoint visibility, endpoint posture assessment, network mapping, and contextual awareness from other types of technologies.

Source: Frost & Sullivan

Revenue Forecast

Key Takeaway: Following the disruption by the Covid-19 pandemic, NAC will return to mature substantial, sustained growth.

Total NAC Market: Revenue Forecast, Global 2014 - 2024



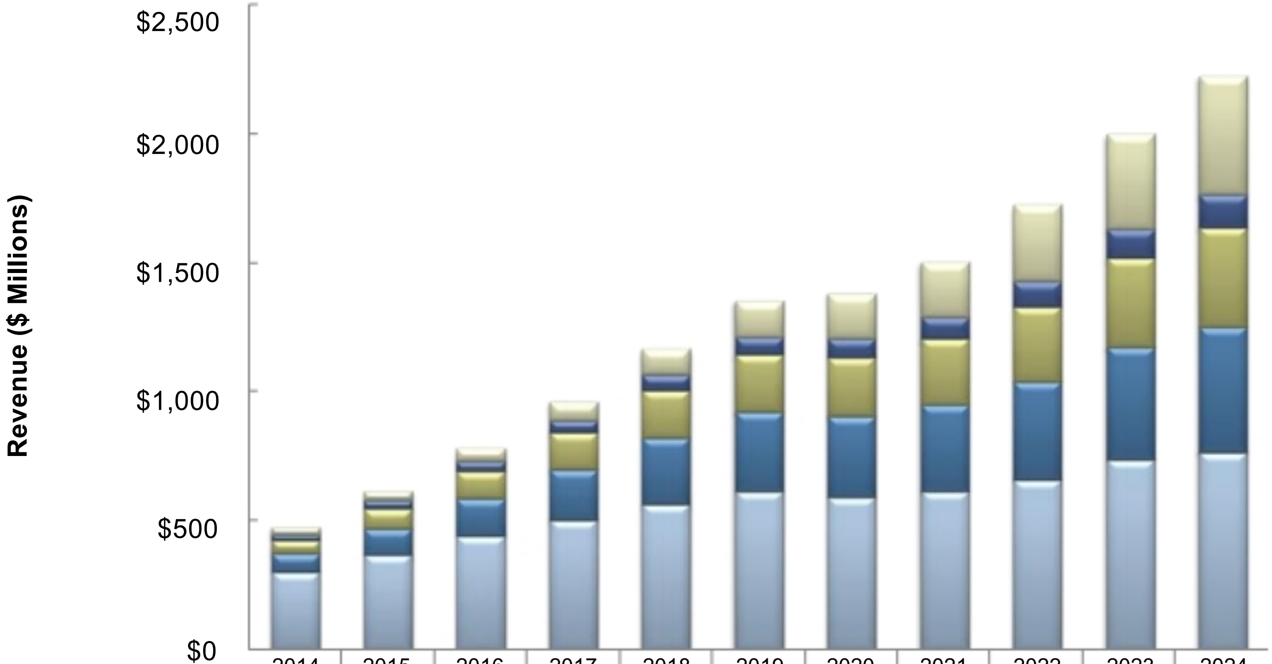
	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
NAC Revenue	$475.4	$614.9	$778.6	$958.4	$1,161.7	$1,348.8	$1,375.7	$1,499.6	$1,717.0	$1,991.7	$2,214.8
growth	28.5%	29.4%	26.6%	23.1%	21.2%	16.1%	2.0%	9.0%	14.5%	16.0%	11.2%

Note: All figures are rounded. The base year is 2019. Source: Frost & Sullivan

Revenue Forecast by Product Type

All NAC product types/service will experience significant growth. NAC as SaaS will grow at a 26.8% CAGR from 2019 to 2024.

NAC Market: Revenue Forecast by Product Type, Global, 2014 – 2024



	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
NAC as SaaS	$28.8	$35.5	$50.3	$71.1	$99.3	$139.8	$172.0	$214.4	$293.6	$366.5	$458.5
Managed/Professional	$23.1	$30.8	$39.3	$48.4	$60.0	$69.5	$75.7	$84.0	$96.2	$111.5	$124.0
Software	$50.9	$77.2	$106.0	$139.9	$185.1	$219.8	$225.6	$251.9	$291.9	$342.6	$385.4
Virtual Appliance	$71.4	$104.1	$144.4	$195.2	$254.8	$305.7	$310.9	$334.4	$377.7	$438.2	$482.8
Physical Appliance	$301.2	$367.3	$438.6	$503.9	$562.5	$613.9	$591.6	$614.8	$657.6	$733.0	$764.1

Note: All figures are rounded. The base year is 2019. Source: Frost & Sullivan

Strategic Imperatives for Success and Growth in NAC

Frost & Sullivan has identified these opportunities for vendors.

Integration and orchestration with other security solutions is a key selling point for NAC. This increases efficacy of NAC and overall security. Vendors should continue to develop this further, breaking down silos across solutions. This is an important feature in pursuing a Zero Trust Architecture.

Third-party ecosystems are essential to long-term growth of NAC. Third-party systems for device validation in addition to device profiling is increasingly important. NAC vendors should focus on growing third-party ecosystems and partnerships, including improving APIs and open standards-driven platforms.

Growth will be driven by IoT, BYOD, and mobility. The number of connected devices is surging. Employees are traveling and working away from a main office. Streamlining device onboarding, focusing on agentless technology, and improving the scalability of an NAC solution are essential for success.

IT and OT are converging. Silos are breaking down, but IT and OT have had different objectives. Vendors should extend NAC technology into OT and improve security tools for better coordination, and leverage IoT technology to better serve OT.

Vendors must get onto the cloud, because customers are moving there quickly—both public and private clouds. They should continue to innovate cloud security; work closely with AWS, Azure, and others; and focus on virtual appliances and NAC as SaaS.

Points of Competitive Differentiation in Solutions

NAC Market: Relative Significance in a Vendor ’s Product Offering

Company	Physical Appliance	Virtual Appliance	Software	Managed - Professional	NAC as SaaS
Cisco	▮▮▮▮	▮▯▯▯	▯▯▯▯	▮▯▯▯	
Forescout	▮▯▯▯	▮▮▮▯	▮▮▮▯	▮▯▯▯	▮▯▯▯
Aruba	▮▮▮▮	▮▯▯▯	▮▯▯▯		
Auconet	▮▮▯▯	▮▮▮▯	▮▮▯▯		▮▯▯▯
Fortinet		▮▮▯▯	▮▮▯▯	▯▯▯▯	▮▮▮▯
Portnox			▯▯▯▯	▯▯▯▯	▮▮▮▮
OPSWAT (Impulse)		▮▮▮▮			▯▯▯▯
PulseSecure	▮▮▮▮	▮▯▯▯		▯▯▯▯	▯▯▯▯
Extreme Networks	▮▮▮▮	▯▯▯▯	▯▯▯▯		▮▯▯▯
InfoExpress	▮▮▮▯	▮▯▯▯	▮▯▯▯	▮▯▯▯	▯▯▯▯
Netshield	▮▮▮▮				
macmon	▮▮▮▯	▮▮▮▯			
Genians	▮▮▮▮	▮▮▮▯	▮▮▮▯	▮▮▯▯	▮▮▯▯

Minimal	Mild	Moderate	Strong	VeryStrong
▯▯▯▯	▮▯▯▯	▮▮▯▯	▮▮▮▯	▮▮▮▮

Source: Frost & Sullivan

Genians

Description

Genians is a pure-play NAC vendor whose solution helps maintain full visibility and control of all network assets, ensuring they meet the highest levels of cybersecurity and compliance. Genians secures millions of endpoints in organizations of all sizes and industries, including global Fortune 500 companies, governments, military, energy, finance, healthcare, and education. Genians serves more than 1,600 customers. The company headquarters and R&D is in South Korea; its global service center is in Boston.

Product

Genians' network surveillance approach, powered by its Device Platform Intelligence (DPI) technology, is the key to identifying and classifying all IP-enabled devices. DPI can present the most accurate device platform name (e.g., not just —Android phone‖ but —Samsung Galaxy S6 mobile phone‖), correlated with contextual access information (who, what, where, when, how), business context (e.g., EOL, EOS, manufacturer Info), and common vulnerabilities and exposures. With this enhanced visibility, Genians can leverage multiple access control techniques (e.g., 802.1x, DHCP, ARP Enforcement, TCP reset, agent-based, agentless) to enforce IT security policies dynamically, quarantine any non-compliant devices, and remediate them to be compliant through automated processes. Genians offers 3 editions: Basic (network surveillance), Professional (NAC), and Enterprise (network automation), and 3 flexible deployment options: on-premises, cloud-managed, and NAC as service for MSSPs.

Target Market & Strategy

Most of Genians revenue comes from midsized and large enterprise customers. The company is looking to expand into SMBs through MSSPs. By leveraging cloud technology, Genians can deliver its enterprise-grade NAC solutions to businesses of all sizes, including any organizations that struggle with technical challenges and budget issues. Government, manufacturing, and finance are the dominant verticals.

Value Proposition

Securing the edge quickly and accurately via Genians next-gen NAC, Genians' Layer 2-based sensing technology ensures full network surveillance for all connected devices in real time and provides dynamic access control to maintain compliance with IT security policies without disturbing existing network infrastructure. Out of the box, it provides the most essential cybersecurity features, such as IP address management, desktop configuration management, WLAN security, switch port management, BYOD, guest management, and IT asset management. It can also integrate a wide range of IT security and business solutions to ensure unified policy enforcement.

What makes them special?

Genian NAC is an affordable and comprehensive NAC solution, featuring full network surveillance for wired and wireless networks in real time without disturbing existing operations. It provides the most essential cybersecurity features and actionable intelligence through an intuitive user interface. It offers affordable pricing via free trials and subscription options. Pragmatic implementation extends from network surveillance to NAC to network security automation. Genians' solution is ready for MSSPs to support SMBs.

Source: Frost & Sullivan