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

네트워크 접근 제어(NAC, Network Access Control, 이하 NAC)는 네트워크 보안을 위한 첫걸음 입니다. 취약점을 보유하거나 침해가 진행된 사용자 또는 단말을 차단하거나 격리하거나 다른 곳으로 이동 조치하는 것은 정보보안을 위한 기본사항 입니다. 또한 NAC는 경계선(cybersecurity perimeter)을 이미 통과하였거나 보안 정보 및 이벤트관리(SIEM) 솔루션이 충분한 정보를 제공하기 이전에 단말에 대한 가시성(Visibility)를 제공할 수 있습니다.

사용자의 단말과 역할(Role)에 따른 접근 제어는 전체 네트워크의 보호를 위한 핵심적인 사항입니다. 사용자 단말을 포함하는 엔드포인트는 네트워크 침입의 관문역할을 함과 동시에 반대로 침입을 탐지하거나 방어할 수 있는 마지막 기회이기 때문 입니다. 이러한 엔드포인트에는 데스크톱, 노트북, 서버, 태블릿, 스마트폰, 가상 데스크톱 및 다양한 사물인터넷(IoT, Internet of Things)기기 등이 포함될 수 있습니다.

Frost & Sullivan은 NAC 벤더들이 2019년 13억 달러(약 1조5천억 원) 규모의 NAC 솔루션과 서비스 그리고 서비스형(SaaS, Software as a Service)NAC 를 판매한 것으로 예상합니다. 그리고 이는 2018년 대비 16.1% 증가한 수치입니다.

2020년 코로나바이러스(COVID-19)는 NAC의 고속성장에 부정적인 영향을 줄 것으로 예상됩니다. 2020년 2사분기(2Q) 와 3사분기(3Q)의 영향으로 NAC의 매출 성장률은 2.0% 대로 급감할 것으로 예상됩니다. 다행이 4분기(4Q)에 감소폭이 회복되어 이후 지속적으로 성장할 것으로 예상하고 있습니다. 이러한 성장은 IoT의 폭발적 증가, BYOD(Bring Your Own Device)의 확대, 이동성 향상, 재택근무의 증가, 워크로드의 클라우드로의 이동 등 이 견인차 역할을 할 것 입니다.

악성코드(Malware) 및 사이버 공격의 증가로 인한 NAC의 투자(도입) 역시 증가하고 있습니다. 왜냐하면 네트워크 가시성(Network visibility)이 매우 중요하기 때문입니다. 네트워크의 모든 단말들은 잠재적으로 공격 또는 내부 정찰을 위한 포인트로 사용될 수 있으므로 모두 식별되고 보호되어야 합니다. NAC 벤더들은 IoT, BYOD 및 클라우드 환경을 위한 NAC의 적용 및 활용방안을 지속적으로 연구하고 있습니다. 이러한 노력의 결과로 NAC 시장은 지속적인 성장세를 보이고 있습니다. Frost & Sullivan은 NAC 시장이 2019년부터 2024년까지 향후 5년간 연평균 10.4% (CAGR, Compound Annual Growth Rate) 2024년 22억 달러(약 2조6천 억) 이상의 규모를 형성할 것으로 전망 하고 있습니다.

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 벤더들은 신규 기능과 개선된 기능을 지속적으로 출시하고 있습니다. 2018년 7월 Frost & Sullivan 보고서 이래로 벤더들은 IoT, 산업용 사물 인터넷(IIoT, Industrial Internet of Things), IT/OT 융합(convergence), 클라우드 마이그레이션(cloud migration), 소프트웨어 정의 경계(SDP, Software Defined Perimeter) 및 제로 트러스트 네트워크(ZTN, Zero Trust Networking) 지원에 중점을 두고 있습니다. 또한 NAC 구축을 용이하게 하기 위한 자동화된 온보딩(onboarding) 기술 등 을 지속적으로 개선하고 있습니다.

보안 자동화(Security Automation)의 적용에 따라 단말수준의 위협탐지와 빠른 대응이 가능해 졌으며 차세대방화벽(NGFW) 등 다양한 보안 솔루션과의 연동을 통한 동적 프로비져닝(Dynamic Provisioning) 역시 가능해 지고 있습니다.

IoT 보안은 IoT 단말의 의심스러운 활동의 탐지 및 지속적인 모니터링에 중점을 두고 있습니다. 뿐만 아니라 서로 다른 IoT 및 IIoT 단말을 위한 세그멘테이션(Segmentation)이 필요하며 아래와 같은 사항에 대한 일관적이고 전사적 수준의 적용을 권장하고 있습니다.

- 장소에 관계없이 인증된 사용자 및 단말에 대한 모바일 모니터링 및 보안 기능의 제공
- 다양한 운영체제 지원: iOS, OSX, Android, Windows 및 Linux 등
- 유관(3rd Party) 벤더와 연동을 개선하고 각 벤더의 에코시스템으로 확장
- 클라우드가 제공하는 솔루션으로의 전환을 가속화

SDP(Software Defined Perimeter, 소프트웨어 정의 경계)는 보다 정교한 세그멘테이션(micro-segment)을 위한 방법 입니다. SDP는 사용자가 워크로드 및 응용 프로그램에 접근할 때 사용자를 보호할 수 있으며 NAC와는 상호보완 관계 입니다. 여러 NAC 벤더에서 이미 SDP를 제공하고 있으며, 장기적으로 SDP의 기능이 NAC에 긴밀하게 통합될 것 입니다.

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			
Shortage of skilled security professionals			
Organizations move to the cloud			
Convergence of IT and OT			
Security orchestration and ZTN			

Impact:	H High	M Medium	L Low

Source: Frost & Sullivan

Forecast Assumptions

NAC 성장에 **긍정적 영향**을 미치는 요인 :

- IoT, BYOD 등으로 인한 모바일 단말의 증가가 예상되며, 물리적 단말의 증가는 더 많은 NAC를 요구하게 됨
- NAC 벤더들은 NAC as SaaS 등 클라우드 환경을 위한 솔루션을 지속적으로 개발함
- 위협(threat)이 정교하고 복잡해 짐에 따라 NAC 역시 지속적으로 고도화 됨(Segmentation, Behavioral Monitoring 등)
- 북미 이외 지역에서 신규 NAC 도입 기회가 발생함
- NGFW(차세대 방화벽), SIEM 등 유관 보안 솔루션과 협업 및 연동을 통한 NAC 효율성 제고 및 투자 정당성 확보
- NAC를 차세대 접근통제 기술인 ZTN(Zero Trust Network)의 핵심이 되도록 NAC 벤더가 노력
- NAC 벤더들의 신규 시장 발굴 및 진출 노력(SMB 등)

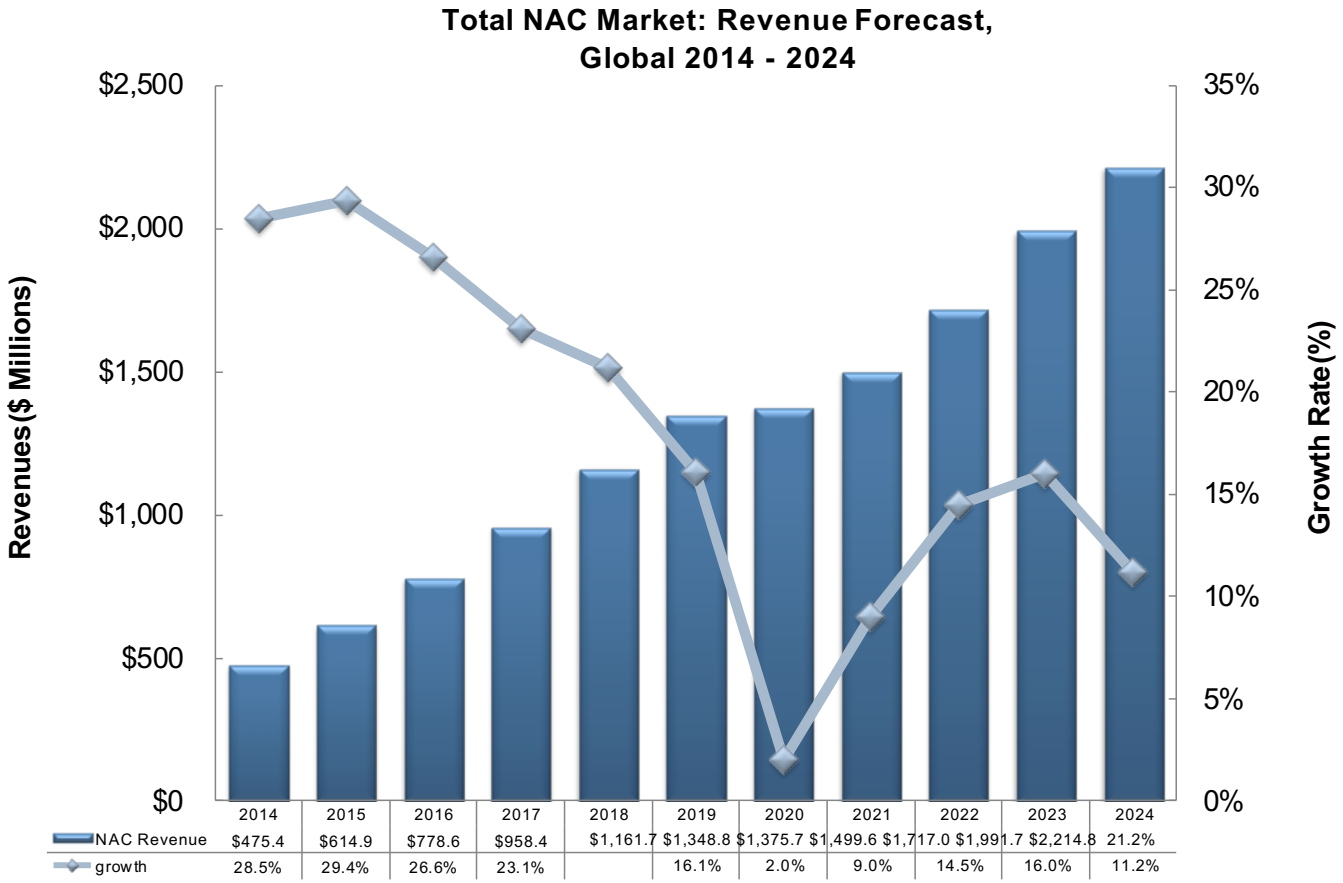
NAC 성장에 **부정적 영향**을 미치는 요인 :

- 기타 단말 가시성 솔루션과의 경쟁 (취약점 관리, SIEM, 단말보안 솔루션 등)
- 단말 가시성(Endpoint visibility), 보안 상태 평가(Posture assessment), 상황 인식(contextual awareness) 등 NAC 중요 기술에 대한 다른 기술의 대체

Source: Frost & Sullivan

Revenue Forecast

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

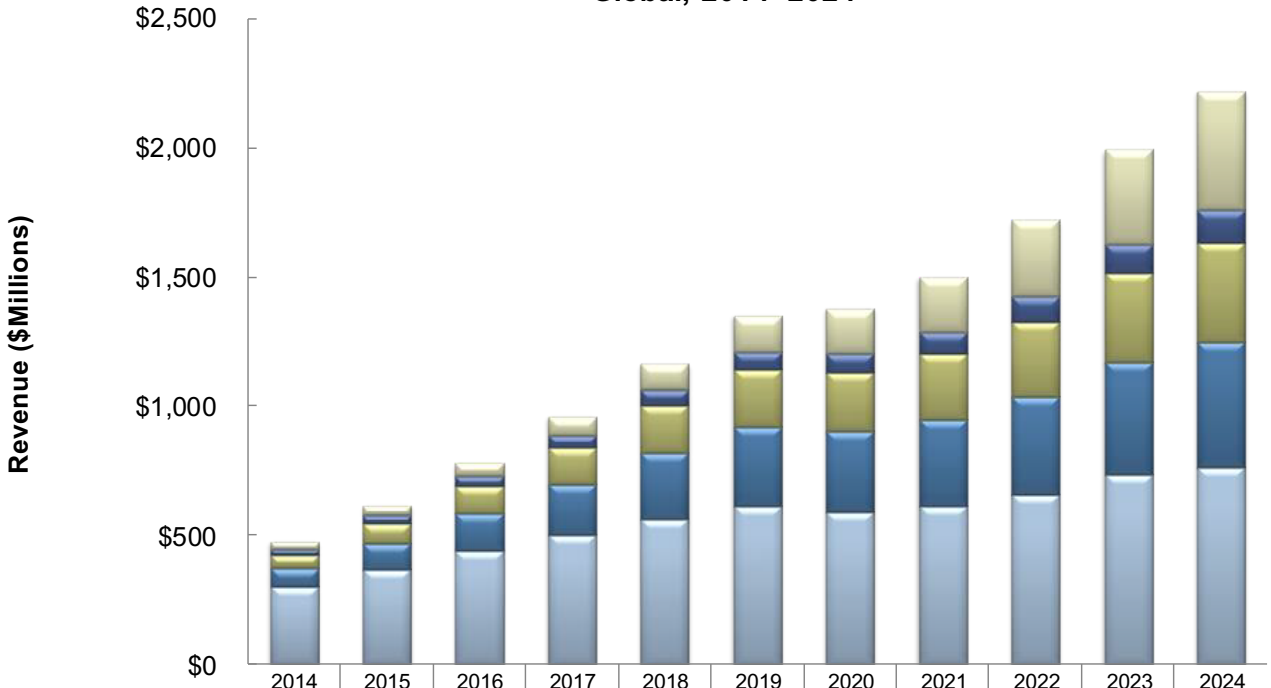


Note: All figures are rounded. The base year is 2019. Source: Frost & Sullivan

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.

타 보안 솔루션과의 통합 및 연동은 NAC의 주요한 판매 포인트(key selling point)입니다. 이를 통해 NAC의 효율성과 전체적인 보안 수준이 향상됩니다. 벤더들은 이를 지속적으로 발전시켜 솔루션들의 사일로(silos) 현상을 방지해야 합니다. 이것은 제로 트러스트 아키텍처를 추구하는데 있어 중요한 특징(특성)입니다.

서드파티(3rd party)와의 에코시스템(ecosystem)은 NAC의 장기적 성장에 필수 요소입니다. 단말 검증(validation)과 프로파일링(profiling)을 위한 서드파티와의 협업은 점점 더 중요해지고 있습니다. NAC 벤더들은 API(API, Application Program Interface) 및 개방형 표준 기반 플랫폼(open standards-driven platforms)을 개선하는 등 서드파티 에코시스템과 파트너십을 확대하는 데 주력해야 합니다.

IoT, BYOD 및 모빌리티(mobility)에 의해 성장이 주도될 것입니다. 연결된 단말의 수가 기하급수적으로 늘고 있습니다. 직원들은 기존 사무실을 떠나 이동하며 업무를 수행하고 있습니다. 중단 없는 온보딩(onboarding) 및 Agentless 환경 지원 등 기존 NAC 솔루션의 확장성을 개선하는 것은 성공을 위한 필수 요소 입니다.

IT와 OT가 융합되고 있습니다. 이로 인해 사일로(Silos)는 무너지고 있지만 IT와 OT의 목표는 서로 다릅니다. 벤더들은 IT 와 OT의 더 나은 협력을 위하여 NAC 기술을 OT로 확장하고, IT 기술이 OT 보안을 위한 지렛대 역할을 할 수 있도록 노력해야 합니다.

고객들이 퍼블릭과 프라이빗 클라우드로 빠르게 이동하고 있기 때문에 NAC 벤더들은 클라우드를 지원해야 합니다. 클라우드 보안을 지속적으로 혁신하고, AWS, Azure 등과 긴밀하게 협력하며, SaaS로써 가상 응용 프로그램과 NAC에 집중해야 합니다.

Source: Frost & Sullivan

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

지니언스는 모든 네트워크 자산을 완벽하게 파악하고, 제어하여 최고 수준의 사이버 보안 및 규제 준수를 보장하도록 지원하는 pure-play NAC 벤더입니다. 지니언스는 전세계 Fortune 500대 기업, 공공, 국방, 에너지, 금융, 의료, 교육 등 모든 규모의 조직에서 수백만 개 이상의 엔드포인트를 보호하고 있습니다. 지니언스는 1,600개 이상의 고객사를 대상으로 서비스를 제공하고 있습니다. 본사와 R&D 부문은 한국에 있으며, 글로벌 서비스 센터는 미국 보스턴에 위치하고 있습니다.

Product

지니언스의 특허받은 DPI(Device Platform Intelligence) 기술을 통해 모든 IP 지원 단말을 식별하고, 분류합니다. DPI는 가장 정확한 단말 플랫폼 이름(예: "Android phone" 뿐만 아니라 "Samsung Galaxy S6")을 나타낼 수 있으며, 상황별 접근 정보(who, what, where, when, how)와 비즈니스 컨텍스트(예: EOL, EOS, 제조업체 정보) 뿐 아니라 취약점(CVE) 정보 까지 포함하고 있습니다. 이러한 정보를 바탕으로 다양한 접근 제어 기술(예: 802.1x, DHCP, ARP Enforcement, TCP reset, agent-based, agentless)을 통하여 IT 보안 정책을 동적으로 적용하고, 미 준수 단말을 격리하며, 자동화된 프로세스를 통해 규정을 준수하도록 적용할 수 있습니다. 지니언스는 온프레미스, 클라우드 관리, MSSP 서비스로서의 NAC 등 3가지 유연한 배포 옵션을 제공합니다.

Target Market & Strategy

지니언스는 중견기업과 대기업 위주의 사업을 수행하고 있으며 MSSP 사업자와 협업하여 SMB 시장으로 확대하기 위해 노력하고 있습니다. 지니언스는 클라우드 기술을 활용하여 기술 및 예산 문제로 어려움을 겪고 있는 기업(조직)을 비롯하여 모든 규모의 기업에 엔터프라이즈급 NAC 솔루션을 제공할 수 있습니다. 공공, 기업, 금융권이 지니언스가 시장 지배력을 가지고 있는 주력 분야입니다.

Value Proposition

지니언스의 차세대 NAC는 독자적인 Layer 2 기반 감지기술을 통해 기존 네트워크의 변경 없이 빠르고 정확하게 에지(edge)를 보호함과 동시에 연결된 모든 단말에 대한 실시간 가시성을 확보하고 동적 접근 제어를 제공하며 IT 보안 정책을 준수하도록 유지합니다. 설치와 동시에 IP 주소 관리, 데스크톱 구성 관리, WLAN 보안, 스위치 포트 관리, BYOD, 게스트 관리 및 IT 자산 관리와 같은 가장 필수적인 사이버 보안 기능을 제공합니다. 또한 광범위한 IT 보안 및 비즈니스 솔루션을 통합하여 일관된 정책 시행을 보장할 수 있습니다.

What makes them special?

지니안 NAC는 기존 네트워크 운영에 지장을 주지 않으며 유/무선 네트워크를 포함하는 전체 네트워크 감시 기능을 제공하는 합리적이고 포괄적인 NAC 솔루션입니다. 직관적인 사용자 인터페이스를 통해 가장 중요한 사이버 보안 기능과 실행 가능한 인텔리전스를 제공합니다. 조직의 규모와 목적에 따라 단순 가시성의 확보에서 부터 자동화된 대응까지 다양한 옵션의 선택이 가능합니다. 서비스 사업자(MSSP)를 위한 다양한 지원이 가능합니다.

Source: Frost & Sullivan