한국IR협의회
기업리서치센터 기업분석 | 2026.01.27

KOSDAQ | 소프트웨어와서비스

지니언스 (263860)

사이버 보안 솔루션 NAC, EDR 1위 기업

KOSDAQ RISING STAR
KRX KOREA EXCHANGE
2025년 코스닥 라이징스타

체크포인트

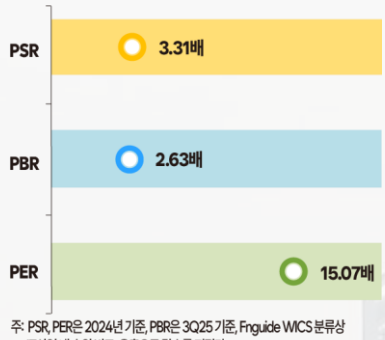
- 사이버 보안 전문기업으로 NAC(Network Access Control), EDR(Endpoint Detection & Response) 시장 1위 기업(2024년 조달청 기준). 2025년 3분기 누적 매출 기준으로 네트워크 보안 제품이 81%, 네트워크 보안 용역 매출이 19%를 차지
- 투자포인트: 정부 주도의 사이버 보안 시장 성장
- 기업에 대한 규제와 제재 수위 강화, 보안 투자 현황의 대외 공개 범위 확대, 물리적 망분리 체계의 유연화가 추진되며 사이버 보안 시장의 성장이 기대되는 2026년에는 매출액 601억 원(yoy 16%), 영업이익 115억 원(yoy 53%)이 전망됨

주가 및 주요이벤트

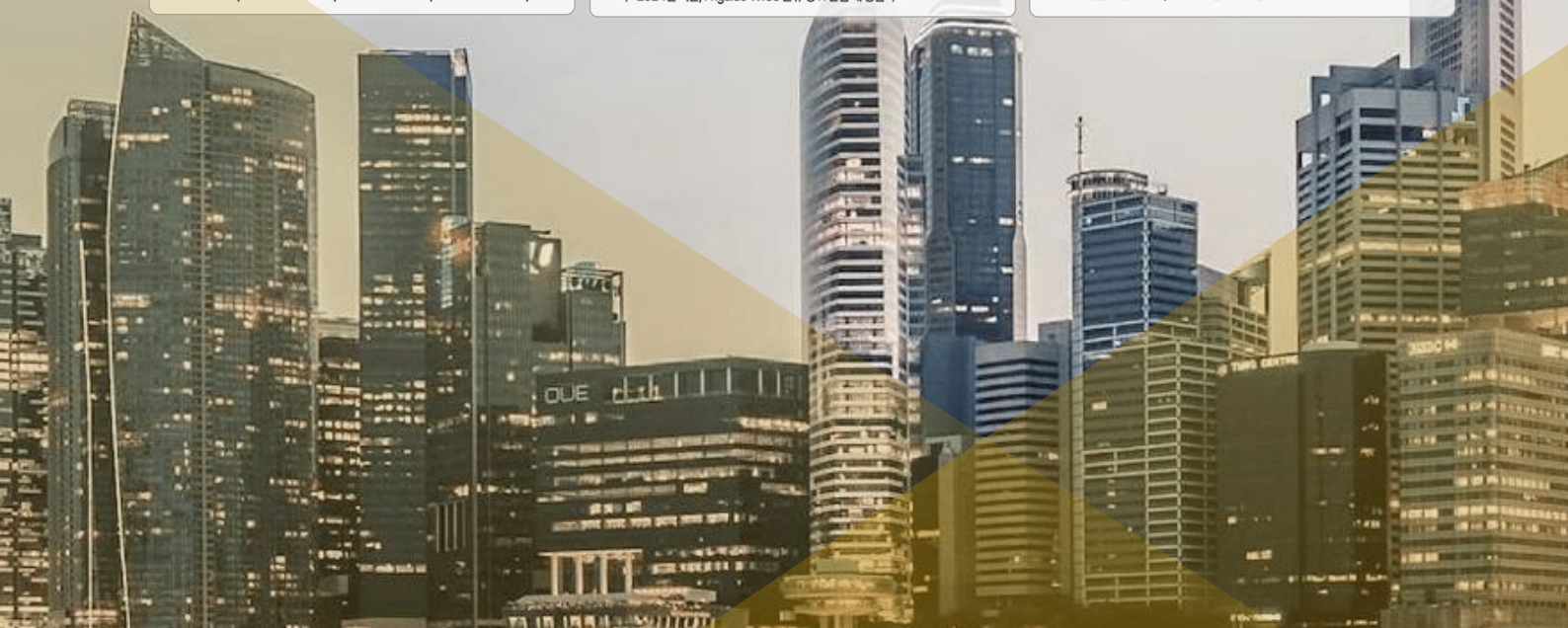
재무지표

주: 2024년 기준, Fnguide WICS 분류 상 IT산업 내 등급화

밸류에이션 지표



주: PSR, PER은 2024년 기준, PBR은 3Q25 기준, Fnguide WICS 분류상 IT산업 내 순위 비교, 우측으로 갈수록 저평가



지니언스 (263860)

KOSDAQ
소프트웨어와서비스

Analyst 김선호 shkim@kirs.or.kr
RA 이희경 hk.lee@kirs.or.kr

사이버 보안 NAC, EDR 1위 기업

2005년에 설립된 사이버 보안 전문기업으로 NAC(Network Access Control), EDR(Endpoint Detection & Response) 시장 1위 기업(2024년 조달청 기준). 2025년 3분기 누적 매출 기준으로 네트워크 보안 제품이 81%, 네트워크 보안 용역 매출이 19%를 차지

정부 주도의 사이버 보안 시장 성장

정부의 기업에 대한 규제와 제재 수위 강화, 상장기업 보안 투자 현황의 대외 공개 범위 확대, 물리적 망분리를 완화하고 다층보안체계(Multi-Level Security)로의 전환은 사이버 보안 시장의 성장을 촉진. 제로 트러스트에 대한 도입이 촉진되면서 지니언스의 NAC, EDR, ZTNA 솔루션에 수혜가 전망됨

기대가 현실이 되는 시기

연이은 정보 보안 사고로 사이버 보안 시장 성장이 기대되며 주가는 한차례 상승 후 조정 중. 2026년 기대가 현실이 된다면 EPS와 밸류에이션 상승이 동시에 가능할 것으로 예상

Forecast earnings & Valuation

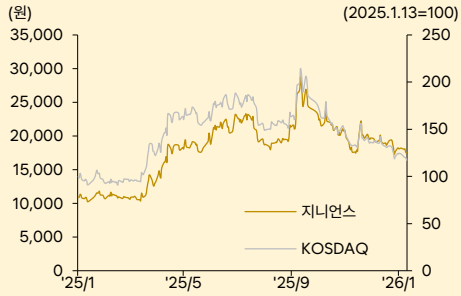
	2022	2023	2024	2025F	2026F
매출액(억원)	385	429	496	520	601
YoY(%)	20.5	11.5	15.7	4.8	15.6
영업이익(억원)	69	65	98	75	115
OP 마진(%)	18.0	15.1	19.8	14.4	19.1
지배주주순이익(억원)	71	62	109	86	122
EPS(원)	757	661	1,165	945	1,348
YoY(%)	15.8	-12.6	76.1	-18.8	42.6
PER(배)	10.9	19.1	8.0	19.7	13.8
PSR(배)	2.0	2.8	1.8	3.3	2.8
EV/EBITDA(배)	5.8	12.4	4.6	14.8	9.3
PBR(배)	1.6	2.4	1.5	2.7	2.3
ROE(%)	16.1	12.7	20.3	14.3	17.9
배당수익률(%)	1.8	1.6	2.7	1.3	1.3

자료: 한국IR협의회 기업리서치센터

Company Data

현재주가 (1/26)		18,920원
52주 최고가		28,800원
52주 최저가		10,250원
KOSDAQ (1/26)		1,064.41p
자본금		47억원
시가총액		1,718억원
액면가		500원
발행주식수		9백만주
일평균 거래량 (60일)		3만주
일평균 거래액 (60일)		5억원
외국인지분율		27.47%
주요주주	이동범 외 2 인	39.26%
	Miri Capital Management LLC	15.12%

Price & Relative Performance



Stock Data

주가수익률(%)	1개월	6개월	12개월
절대주가	0.1	-18.4	84.6
상대주가	-13.5	-38.2	26.4

▶ **참고** 1) 표지 재무지표에서 안정성 지표는 '이자보상배율', 성장성 지표는 'EPS증가율', 수익성 지표는 'ROIC', 활동성지표는 '순운전자본회전율,' 유동성 지표는 '당좌비율'임. 2) 표지 밸류에이션 지표 차트는 해당 산업군내 동사의 상대적 밸류에이션 수준을 표시. 우측으로 갈수록 밸류에이션 매력도 높음.

▶ **'코스닥 라이징스타'**는 우수한 기술력과 성장가능성을 갖춘 기업을 발굴·육성하기 위해 매년 한국거래소가 선정하고 있는 기업

기업 개요

1 국내 1위 NAC 및 EDR 보안 솔루션 업체

사이버 보안 솔루션 전문기업

지니언스는 2005년 설립된 정보보안 소프트웨어 기업으로 해킹 및 랜섬웨어와 같은 사이버 위협을 예방 및 대응하는 솔루션을 개발 및 판매한다. 동사는 2005년부터 2024년까지 연평균 매출액 성장률(CAGR) 23.9%를 달성했으며, 설립 이후 20년간 지속적으로 영업이익 흑자를 기록하고 있다. 2017년 코스닥 시장에 상장된 이후, 2023년부터 3년 연속 한국거래소가 주관하는 '코스닥 라이징스타' 기업에 선정되었다.

주요사업

사업부문은 네트워크 보안과 기타(임대) 사업으로 구분되며, 매출의 대부분이 네트워크 보안 사업에서 발생하고 있다. 2025년 3분기 누적 연결기준 매출액은 312억 원으로, 네트워크 보안 사업 내 제품(솔루션) 매출액 비중은 81%, 용역 매출 비중은 19%이다. 네트워크 보안 솔루션은 내부 네트워크에 접속하는 단말과 사용자의 상태를 식별·인증·통제함으로써 내부 침해 및 악성코드 확산을 방지하는 정보보호 솔루션을 의미하며, 용역 서비스 매출은 솔루션 도입 고객을 대상으로 한 유지보수 및 기술지원 서비스에서 발생하는 매출이다. 매출의 96.5%가 내수에서 발생하고 있어, 국내 공공 및 민간 보안 시장 중심으로 사업을 영위하고 있다.

지니언스의 주요 제품으로는 NAC(Network Access Control, 네트워크 접근제어 솔루션), Insights E(통합 단말 보안 플랫폼), ZTNA(Zero Trust Network Access), GPI(Genian Policy Inspector, PC 보안진단솔루션) 등이 있다. 동사의 제품 포트폴리오는 제로 트러스트 아키텍처를 구현하는 통합 보안 체계를 형성한다. NAC가 네트워크 접근 제어의 기반을 담당하고, ZTNA가 애플리케이션 수준의 접근을 검증하며, Insights E가 엔드포인트 위협을 탐지·대응하고, GPI가 단말 보안 수준을 진단·관리하는 구조다.

1. NAC

NAC는 네트워크 접근 제어 솔루션으로, 기업 내부 네트워크에 접속하는 장비를 식별·인증·통제하는 역할을 한다. NAC는 동사의 캐시카우 제품으로, 설립 초기부터 현재까지 NAC 제품을 중심으로 사업을 전개해왔으며 국내 NAC 시장에서 선도적인 지위를 확보하고 있다.
동사는 가트너가 선정한 2022년 '글로벌 톱5 NAC 업체'에 진입하였으며, 2023년에는 글로벌 NAC 시장 점유율 4위를 기록하였다. 2025년 3분기말 기준 NAC 누적 고객 수는 3,000개에 달해, 공공기관은 물론 민간 기업 전반에 걸쳐 독보적인 레퍼런스를 구축하고 있다. NAC 솔루션은 온프레미스 및 클라우드 환경을 모두 지원하며, 구독형(SaaS) 모델로의 제공도 가능하다.

2. Insights E

Insights E는 EDR(Endpoint Detection & Response)과 AV(Anti-Virus)를 통합한 엔드포인트 보안 플랫폼이다. EDR은 단말 기반 지능형 위협 탐지 및 대응 솔루션으로, 기존 백신으로 탐지하기 어려운 신종·변종 악성코드와 지능형 공격에 대응하는 역할을 한다. 단말에서 발생하는 다양한 행위 정보를 상시 수집·분석함으로써 이상 행위를 선제적으로 탐지

하고 대응할 수 있어, 재택근무 환경과 문서 유출 방지 등에서 활용도가 높다.

동사는 2017년 국내 최초로 EDR 솔루션을 개발한 이후 누적 고객 수 200곳 이상을 확보하며 국내 EDR 시장 점유율 1위를 차지하고 있다. 2022년에는 국내 최초로 국가정보원 보안기능확인서를 획득했으며, 안티 랜섬웨어 모듈을 EDR 제품에 최초로 탑재하였다. 2025년에는 자체 개발한 백신 솔루션을 EDR과 통합한 Insights E를 출시하여, 알려진 위협(백신)과 알려지지 않은 위협(EDR)을 단일 플랫폼으로 방어할 수 있는 통합 엔드포인트 보안 체계를 완성하였다.

3. ZTNA

ZTNA는 Zero Trust 보안 모델을 기반으로 한 차세대 네트워크 접근 보안 솔루션으로, 사용자와 단말을 지속적으로 검증하는 방식을 통해 기존 경계형 보안의 한계를 보완한다. NAC가 네트워크 수준의 접근을 통제한다면, ZTNA는 애플리케이션 수준의 접근을 검증하여 더욱 세밀한 보안 제어가 가능하다.

동사는 2022년 '지니안 ZTNA'를 국내 최초로 출시했으며, 2023년 제로 트러스트 실증과제 컨소시엄 참여, 2024년 제로 트러스트 도입 시범사업 주관사 선정을 통해 공공 부문 레퍼런스를 축적하고 있다. 레거시 환경의 변경 없이 신규 보안체계 적용이 가능하다는 점에서 확장성과 유연성이 강점이며, 원격 근무 및 클라우드 환경 확산에 따라 중장기적으로 ZTNA 솔루션의 수요 확대가 기대된다.

4. GPI

GPI는 PC 보안 수준 진단 솔루션으로, 단말의 보안 설정·취약점·정책 준수 여부를 자동으로 점검하고 관리하는 역할을 수행한다. 기업 및 공공기관 내 PC를 대상으로 보안 성취도 평가 시스템을 통해 보안 수준을 정량적으로 진단하며, 실시간 단말 상태 정보 수집·분석 기능을 제공한다.

대규모 환경에서도 시스템 부하를 최소화하는 분산 수집 방식을 지원하며, 수집된 취약점 분석 결과를 중앙에서 통합 관리할 수 있다. 최근에는 AWS 등 클라우드 환경 지원이 추가되며 NAC·ZTNA와 연계된 단말 보안 통합 관리 솔루션으로 역할이 확대되고 있다.

종속회사

종속회사로는 미국 소재의 GENIANS USA, INC.(지분율 100.0%)가 있으며, 2016년 설립된 네트워크 보안 솔루션 제공 업체이다. 2025년 3분기말 기준 매출액은 9억 원, 당기순이익은 -3억 원을 기록하였다.

주주현황

최대주주는 2025년 3분기말 기준 이동범 대표이사(지분율 31.54%)로, 최대주주 및 특수관계인 지분율은 총 39.32%이다. 이동범 대표이사는 2020년부터 2024년 2월까지 한국정보보호산업협회 회장을 역임하였으며, 현재 디지털플랫폼 정부위원회 보안분과 위원, 중소기업기술정보진흥원 비상임이사, 국가정보원 사이버정책 자문위원, 국가보훈부 정책자문위원 등을 겸직으로 하고 있다.

5%이상 주주로는 해외투자자인 THE MIRI STRATEGIC EMERGING MATKETS FUND LP(15.12%)와 MORGAN STANLEY AND CO INTERNATIONAL PLC(5.27%), 그리고 김계연 부사장 7.05%, 등이 있다.

지니언스 연혁

2005~2015 원천기술을 기반으로 국내 NAC 시장 선도

- 2005.01 지니네트웍스㈜설립
- 2006.03 네트워크 접근제어 솔루션 'Genian NAC v1.5' 출시
- 2008.08 지식경제부 우수보안기술 업체 선정
- 2008.10 기술혁신형 중소기업(INNO-BIZ) 선정
- 2012.06 안양 평촌 사옥 이전
- 2012.07 유무선 네트워크 접근제어 'Genian NAC Suite v4.0' 출시
- 2013.10 'Genian 내PC지키미 v3.0 GS' 인증 획득

2016~2020 글로벌 사업 확대 및 엔드포인트 시장 진출

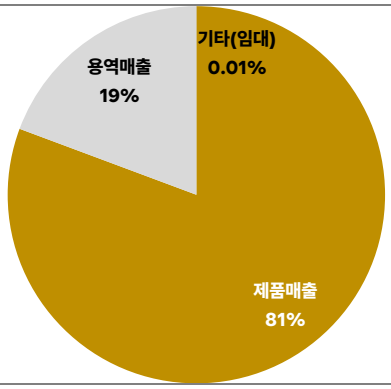
- 2016.01 미국법인 GENIANS, INC. 설립
- 2016.02 미국 RSA 2016 참가
- 2017.02. EDR 솔루션 'Genian Insights E' 출시
- 2017.03. 지니언스㈜사명 변경
- 2017.08 코스닥 상장
- 2018.01 머신러닝 엔진 탑재 EDR 'Genian Insights E' 출시
- 2018.02 IoT·클라우드 지원 네트워크 접근제어 솔루션 'Genian NAC v5.0' 출시
- 2019.09 전 세계 33개국 34개 현지 파트너 확보
- 2019.11 미주·유럽·중동에 클라우드 기반 차세대 NAC 공급
- 2019.12 EDR 사업 부문, 공공·금융·제조 대형 레퍼런스 확보
- 2020.12 지니언스 미국법인, 실리콘밸리로 이전
- 2020.01 EDR 솔루션 'Genian Insights E v2.0' 출시
- 2020.05 Genian NAC Frost & Sullivan 글로벌 마켓 리프트 등재
- 2020.09 가트너 '차세대 NAC' 대표기업 선정

2021~ 글로벌 보안 플랫폼으로 도약

- 2021.06 가트너 NAC 마켓가이드 대표 기업 선정
- 2021.10 중기·스타트업 대상 혁신중소기업부문 중소벤처기업부 장관상(대상)
- 2022.02 가트너 선정 '글로벌 톱5 NAC 업체' 진입
- 2022.06 RSAC에서 차세대 보안 솔루션 Genian ZTNA 공개
- 2022.08 제로 트러스트 관련 기술 특허 취득
- 2022.10 국내최초 Genian EDR 국정원 보안기능 확인서 획득
- 2023.01 클라우드 전문 기업 클라이온 투자 협정
- 2023.03 딜로이트와 전략적 파트너십 체결
- 2023.11 글로벌 상용SW명품대전' 공공부문발주자협의회 회장상 수상
- 2023.12 시큐리티어워드코리아 고객만족도상 수상
- 2024.01 글로벌 NAC 고객 100곳 돌파
- 2024.04 제로트러스트 사업 관련, 퓨쳐텍정보통신 지분 인수
- 2024.05 제로트러스트 시범 사업 수주
- 2024.08 사이버보안 국제협력기반기술개발 국책과제 수주
- 2024.08 KRX 주관 코스닥 라이징스타 2년 연속 선정
- 2024.10 UAE 신규 사무소 개설
- 2025.02 클라우드 기반의 관리형 탐지 대응(MDR) 서비스 사업 진출
- 2025.03 인도 글로벌 기술지원센터 개소
- 2025.03 AI 기반 혁신 전략 발표
- 2025.05 위협 분석 보고서 영문판 정식 발간
- 2025.06 정보보호 자율 공시 시행
- 2025.08 09 '2025 한국IR대상' 우수기업 선정
- 2025.08 지니안 인사이츠 E 3.0 출시
- 2025.08 KRX 주관 코스닥 라이징스타 3년 연속 선정

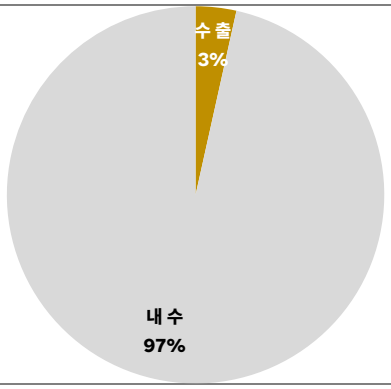
자료: 지니언스, 한국IR협의회 기업리서치센터

사업부별 매출비중(3Q25누적)



자료: 지니언스, 한국IR협의회 기업리서치센터

내수/수출 매출비중(3Q25누적)



자료: 지니언스, 한국IR협의회 기업리서치센터

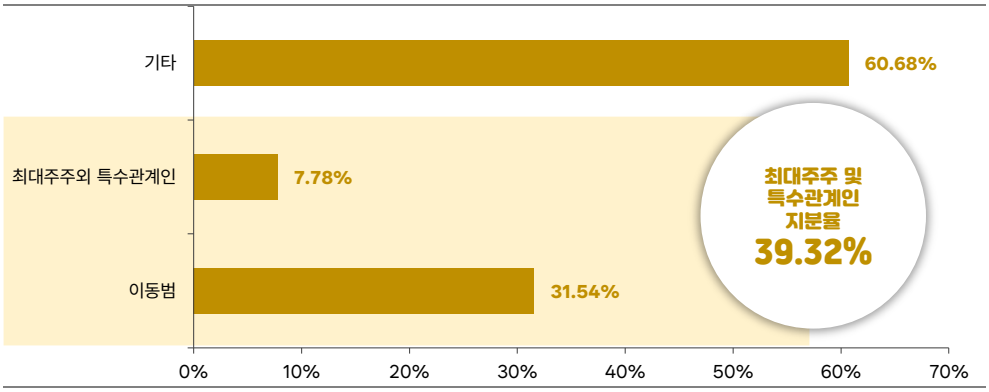
Genian NAC 레퍼런스

자료: 지니언스, 한국IR협의회 기업리서치센터

Genian EDR 레퍼런스

자료: 지니언스, 한국IR협의회 기업리서치센터

주주현황(2025년 3분기말 기준)



자료: 지니언스, 한국IR협의회 기업리서치센터

산업 현황

1 제로 트러스트(Zero Trust)

제로 트러스트: Never Trust, Always Verify

제로 트러스트(Zero Trust)의 부상 배경

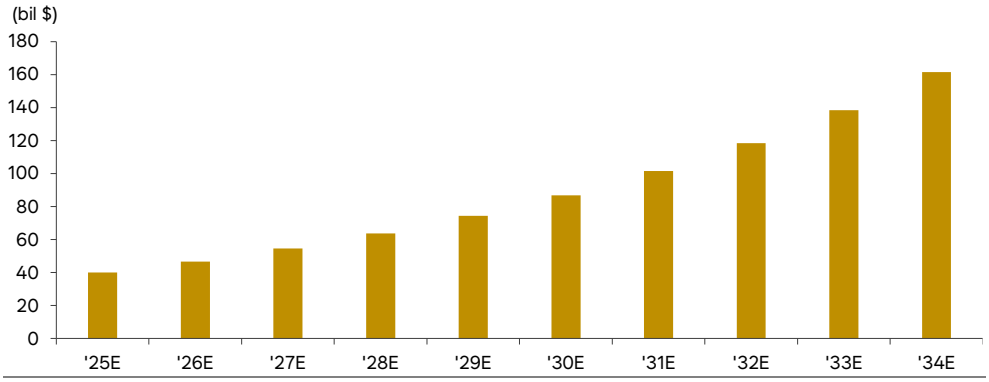
21세기 디지털 전환의 가속화는 기업의 IT 인프라 환경을 근본적으로 변화시켰다. 과거의 기업 보안은 명확한 물리적·논리적 경계를 중심으로 설계되었다. 기업 내부 네트워크는 안전한 신뢰(Trust) 영역으로 간주되었고, 외부 인터넷은 위험한 비신뢰(Untrust) 영역으로 정의되었다. 이에 따라 방화벽(Firewall), 침입 탐지 시스템(IPS, Intrusion Prevention System) 등 경계를 방어하는 솔루션이 보안 투자의 핵심이었다.

그러나 클라우드 컴퓨팅의 보편화, 원격 및 하이브리드 근무의 확산, 그리고 사물인터넷(IoT) 기기의 폭발적인 증가는 이러한 전통적인 경계 기반 보안 모델을 무력화시켰다. 기업의 데이터와 애플리케이션은 더 이상 사내 데이터 센터에만 머무르지 않고, AWS, Azure와 같은 퍼블릭 클라우드, 직원들의 개인 모바일 기기, 파트너사의 네트워크 등 다양한 위치에 분산되어 있다. 이는 공격자가 침투할 수 있는 공격 표면이 기하급수적으로 확장되었음을 의미한다.

특히, 내부는 안전하다는 암묵적인 가정은 내부자 위협이나 공급망 공격, 그리고 피싱을 통해 계정을 탈취한 공격자의 횡적 이동에 취약점을 드러냈다. 이러한 배경 속에서 "아무것도 신뢰하지 않고, 항상 검증한다(Never Trust, Always Verify)"는 제로 트러스트(Zero Trust) 보안 모델이 기업의 필수 생존 전략으로 부상하게 되었다.

글로벌 시장 조사 및 전략 컨설팅 전문 기업 Precedence Research는 2024년 343억 달러 규모의 전세계 제로 트러스트 시장이 2034년 1,616억 달러까지 성장하여 연평균 16.8%의 높은 성장세를 보일 것으로 전망하고 있다.

전세계 제로 트러스트 시장 규모 전망치



자료: Precedence Research, 한국IR협의회 기업리서치센터

제로 트러스트의 기술적 구현 요소

제로 트러스트를 구현하기 위해서는 다양한 보안 솔루션들이 필요하다. 제로 트러스트는 보안 아키텍처로서 단일 솔루션이 아니라 신원, 기기, 네트워크, 애플리케이션 등 다양한 영역의 보안 기술이 유기적으로 결합된 체계를 의미한다. 제로 트러스트를 구현하기 위한 솔루션은 크게 사용자 인증, 접근 제어, 엔드포인트 보안, 모니터링의 네 가지 영역으로 구분된다.

1. 신원 및 접근 관리

보안의 출발점은 사용자와 기기의 신원을 명확히 식별하고 적절한 권한을 부여하는 것에 있다. 이를 위해 비밀번호 외에도 생체 정보나 OTP 등을 추가로 요구하는 다중 요소 인증(MFA, Multi-Factor Authentication)을 도입하여 인증 단계를 강화한다. 또한 아이덴티티 관리(IAM, Identity and Access Management)를 통해 사용자의 직무나 역할 변화에 맞춰 접근 가능한 자원 범위를 실시간으로 조정함으로써 권한 남용을 방지한다.

2. 네트워크 접근 제어 및 경계 보안

네트워크 영역에서는 접근 권한을 세밀하게 검증하고 제어하는 기술이 필수적이다. 네트워크 접근 제어(NAC, Network Access Control))는 접속 기기의 보안 상태를 검증하는 첫 번째 관문 역할을 수행하며, 제로 트러스트 네트워크 액세스(ZTNA, Zero Trust Network Access)는 전체 네트워크가 아닌 특정 애플리케이션에만 한정된 접근을 허용하여 기존 VPN의 보안 취약점을 해결한다. 아울러 소프트웨어 정의 경계(SDP, Software Defined Perimeter) 기술로 인프라 자체를 외부에 노출하지 않고, 미세 분할(Micro-segmentation)을 통해 네트워크를 격리함으로써 공격자의 측면 이동(Lateral Movement)을 차단한다.

3. 엔드포인트 및 기기 보안

접근을 시도하는 기기 자체의 안전성을 실시간으로 확인하는 과정도 중요하다. 엔드포인트 탐지 및 대응(EDR, Endpoint Detection and Response)은 단말에서 발생하는 이상 행위를 상시 모니터링하여 침해 사고에 신속히 대응한다. 동시에 통합 엔드포인트 관리(UEM, Unified Endpoint Management)를 활용해 최신 패치 적용 여부나 백신 실행 상태를 점검하고, 이를 수치화된 신뢰 점수로 환산하여 접근 승인의 근거로 삼는다.

4. 보안 가시성 및 분석

마지막으로 모든 접근 기록을 통합적으로 분석하여 잠재적 위협을 식별해야 한다. 보안 정보 및 이벤트 관리(SIEM, Security Information and Event Management)는 전사적인 로그 데이터를 수집하여 위협 징후를 포착하는 역할을 한다. 여기서 한 걸음 더 나아가 보안 오케스트레이션 및 자동화 대응(SOAR, Security Orchestration, Automation and Response)을 통해 탐지된 위협에 대해 미리 설정된 시나리오대로 자동 대응함으로써 사고 처리 속도와 효율성을 극대화한다.

제로 트러스트 보안 모델을 실제 업무 환경에 적용한 사례를 예로 들면 다음과 같다.

외부 네트워크 환경인 카페에서 직원이 사내 회계 시스템에 접속을 시도하는 상황을 가정한다. 보안 체계는 가장 먼저 사용자의 신원을 엄격히 식별하기 위해 다중 요소 인증(MFA)을 실시한다. 이는 단순히 비밀번호를 입력하는 수준을 넘어 생체 인식이나 일회용 비밀번호(OTP) 등 추가적인 인증 수단을 요구함으로써 타인에 의한 계정 도용 가능성을 차단한다.

신원 확인이 완료된 후에는 접속에 사용되는 노트북의 보안 상태를 실시간으로 점검하는 단계가 진행된다. 제로 트러스트 솔루션은 해당 기기의 운영체제가 최신 보안 패치를 유지하고 있는지, 백신 소프트웨어가 정상적으로 작동하며 실시간 감시 기능을 수행하고 있는지 확인한다. 만약 기기의 보안 수준이 기업의 정책 기준에 미달할 경우 접속은 즉시 거부된다.

기기의 무결성이 입증되면 제로 트러스트 네트워크 액세스(ZTNA) 기술을 통해 논리적인 연결 통로가 형성된다. 이때 직원은 사내의 전체 네트워크에 접근 권한을 갖는 것이 아니라, 업무 수행에 반드시 필요한 '회계 시스템'이라는 특정 애플리케이션에만 한정하여 접근할 수 있다. 이러한 방식은 공격자가 내부망에 침투하더라도 다른 시스템으로 확산해 나가는 수평 이동(Lateral Movement)을 근본적으로 차단하는 효과를 거둔다.

마지막으로 접속이 유지되는 세션 전체 과정에 대해 지속적인 모니터링이 수행된다. 보안 정보 및 이벤트 관리(SIEM) 시스템은 직원의 활동을 실시간으로 분석하며, 평소의 업무 범위를 초과하는 대량의 데이터 반출 시도와 같은 이상 행위를 감지한다. 위협 징후가 포착되는 즉시 시스템은 해당 연결을 자동 차단하고 관리자에게 경고를 전송하여 데이터 유출 사고를 사전에 방지한다.

이러한 일련의 과정은 '결코 신뢰하지 않고 언제나 검증한다'는 제로 트러스트의 핵심 철학이 기술적으로 구현된 결과물이다.

2 네트워크 관문 NAC

NAC

내부 네트워크의 문지기

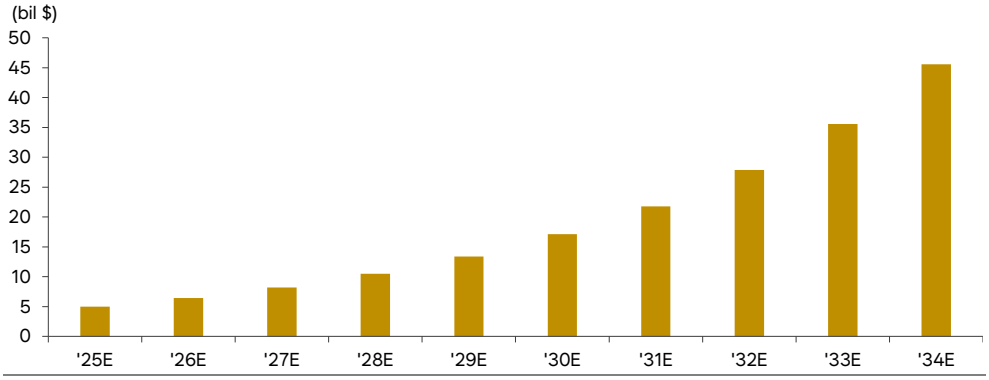
개요 및 핵심 기능

NAC(Network Access Control, 네트워크 접근 제어)는 네트워크에 접속하려는 모든 단말기(PC, 노트북, 스마트폰, IoT 기기 등)의 신원을 식별하고, 보안 정책 준수 여부를 검토하여 접속 권한을 차등 부여하는 보안 솔루션이다.

NAC는 내부 네트워크의 '문지기' 역할을 수행하며, 단순히 계정 정보를 확인하는 것에 그치지 않고 접속 기기의 무결성(백신 설치 및 최신 패치 여부 등)을 종합적으로 판단한다. 특히 제로 트러스트(Zero Trust) 관점에서는 모든 기기를 잠재적 위협으로 간주하여, 초기 접속 시점뿐만 아니라 접속이 유지되는 전 기간에 걸쳐 지속적으로 기기의 안전성을 검증하는 중추적인 기능을 담당한다.

글로벌 시장 조사 및 전략 컨설팅 전문 기업 FMI는 2024년 39억 달러 규모의 전세계 NAC 시장이 2034년 456억 달러까지 성장하여 연평균 27.8%의 높은 성장세를 보일 것으로 전망하고 있다.

전세계 NAC 시장 규모 전망치



자료: FMI, 한국IR협의회 기업리서치센터

NAC의 4단계 작동 과정

지니언스 NAC의 작동 과정은 그림에 표시된 세 가지 핵심 구성요소인 정책 서버(Policy Center), 차단 센서(Net-Sentry), 에이전트(NAC Agent)의 상호작용을 통해 이루어진다.

1. 식별 (Visibility) 네트워크에 기기가 접속하면 본사와 지점에 위치한 차단 센서가 이를 가장 먼저 감지한다. 차단 센서는 에이전트 설치가 불가능한 프린터나 IP 카메라 같은 IoT 기기까지 스스로 탐색하여 분류함으로써 네트워크 전체에 대한 가시성을 확보한다.

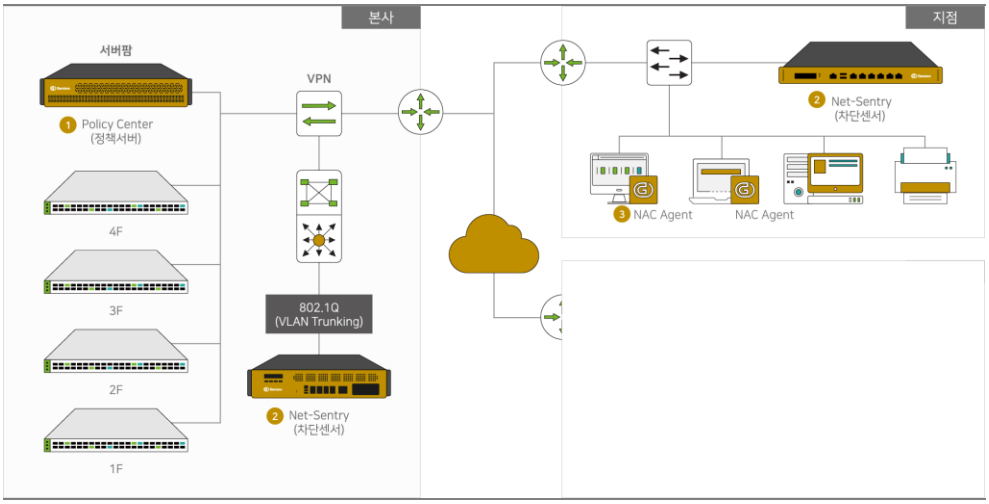
2. 검증 (Posture Check) 식별된 단말기가 사내 보안 정책을 잘 따르고 있는지 점검한다. PC나 노트북에 설치된 에이전트가 운영체제 패치 상태나 백신 활성화 여부를 확인하며, 이 정보는 정책 서버로 전달되어 보안 결함 유무를 최종 판단한다.

3. 통제 (Access Control & Quarantine) 보안 검증에서 통과하지 못한 기기는 네트워크에서 즉시 분리된다. 이때 차단 센서는 802.1Q 기술을 사용하여 해당 기기가 다니는 길에 '격리 대상'이라는 이름표를 붙인다.

이렇게 이름표가 붙은 데이터는 사내 내부망으로 연결된 통로가 아닌, 별도로 분리된 '격리 구역(VLAN)'으로만 흐르게 된다. 격리된 단말은 다른 PC나 중요 서버에는 접근할 수 없으며, 오직 백신을 업데이트하거나 보안 패치를 받을 수 있는 특정 서버에만 접속이 허용된다. 즉, 하나의 물리적 네트워크 안에서 소프트웨어적으로 완전히 벽을 세워 통제하는 방식이다.

4. 관리 (Monitoring) 접속이 허용된 이후에도 정책 서버는 세션이 유지되는 동안 기기의 상태를 지속적으로 모니터링한다. 사용 중 보안 설정이 변경되거나 이상 행위가 감지되면 즉시 접속 권한을 회수하거나 재인증 단계를 수행하여 보안성을 유지한다.

Genian NAC 설치 및 구성요소



자료: 지니언스, 한국IR협의회 기업리서치센터

제로 트러스트와 NAC의 유기적 협업

제로 트러스트 환경에서 NAC는 '관문(Gateway)'의 역할을 수행한다. 사용자나 기기가 네트워크에 접속을 시도하는 최초 시점에 신원을 확인하고, 보안 정책 준수 여부를 검증하여 접속 자체를 허용하거나 거부하는 것이 NAC의 핵심 기능이다.

제로 트러스트의 핵심 원칙 중 하나인 '최소 권한 부여(Least Privilege)'는 네트워크 계층에서 NAC를 통해 구현된다. 예를 들어, 동일한 사무실에 출근한 직원이라 하더라도 NAC는 해당 직원의 부서, 직급, 업무 범위에 따라 접근 가능한 네트워크 영역을 차등적으로 설정한다. 영업팀 직원의 노트북은 고객관계관리(CRM) 서버가 위치한 네트워크 세그먼트에만 접근이 허용되고, 개발팀 서버에는 접근이 원천 차단되는 방식이다.

NAC가 담당하는 또 다른 핵심 원칙은 '접속 전 실제 상태 확인'이다. NAC는 접속을 시도하는 기기가 최신 보안 패치를 적용했는지, 승인된 백신 소프트웨어가 실행 중인지, 비인가 소프트웨어가 설치되어 있지 않은지를 실시간으로 점검한다. 단순히 계정 정보만 확인하는 것이 아니라, 기기의 실제 보안 상태를 구체적으로 검증한다는 의미다. 이러한 보안 준수 검증을 통과하지 못한 기기는 네트워크 접속이 거부되거나, 보안 업데이트만 가능한 격리 영역(Quarantine Zone)으로 유도된다.

NAC는 다른 보안 솔루션들이 내린 결정을 실제로 실행하는 집행자 역할을 수행한다. 신원 및 접근 관리(IAM) 시스템이 사용자 인증을 완료하면 NAC가 해당 사용자의 기기에 네트워크 접속을 허용하고, 반대로 엔드포인트 탐지 및 대응(EDR) 솔루션이 특정 단말에서 악성 행위를 탐지하면 NAC는 즉시 해당 단말의 네트워크 포트를 차단하여 위협의 확산을 방지한다. 이처럼 NAC는 보안 정책의 결정은 다른 시스템들이 내리지만, 그 결정을 네트워크 수준에서 강제하는 것은 NAC의 몫이다.

이처럼 NAC는 네트워크라는 물리적 인프라 계층에서 접근 통제를 실행하는 '집행자' 역할에 특화되어 있다. 제로 트러스트 네트워크 액세스(ZTNA)가 주로 원격 사용자의 애플리케이션 접근을 관리한다면, NAC는 사무실 내부의 유·무선 LAN 환경에서 단말의 신뢰를 구축하고 유지하는 역할을 담당한다. 결론적으로, NAC는 '누가, 어떤 기기로, 어디에 접속할 수 있는가'라는 질문에 답하는 솔루션이다.

NAC 솔루션 경쟁구도

현재 글로벌 NAC 시장은 제로 트러스트 보안 아키텍처의 확산에 발맞추어, 기존의 단독 솔루션 형태에서 탈피하여 '통합 보안 플랫폼'과 '전문 독립 솔루션' 사이의 치열한 경쟁 체제를 구축하고 있다.

Cisco(미국), Fortinet(미국), Aruba(미국, HPE 소유), Juniper(미국) 등 주요 기업들은 네트워크 인프라 시장에서의 강력한 지배력을 토대로 NAC 기능을 자사의 네트워크 장비 및 보안 스택에 통합하여 제공한다. 이들은 관리의 편의성과 비용 효율성을 핵심 경쟁력으로 내세우며, 대규모 네트워크 자원을 보유한 엔터프라이즈 시장을 중심으로 영향력을 확대하고 있다.

반면 Forescout(미국)와 같은 전문 독립 솔루션 기업들은 특정 네트워크 장비 제조사에 종속되지 않는 범용성을 강점으로 내세운다. 특히 보안 관리 소프트웨어인 에이전트를 설치하기 어려운 다양한 IoT 기기들을 효과적으로 식별하는 능력을 강조한다. 이러한 특성 덕분에 에이전트 설치가 불가능한 기기의 비중이 높은 공공, 의료, 제조 현장 등에서 독보적인 강세를 보인다.

글로벌 시장이 클라우드 중심의 통합과 유연한 연결을 지향하는 것과 달리, 국내 시장은 강력한 물리적 망분리 규제와 중앙집중적 통제를 중시하는 특수한 환경을 형성하고 있다. 이러한 특수성으로 인해 외산 솔루션의 진입 장벽이 존재하며, 국산 솔루션들은 국내 보안 규제에 최적화된 준수 역량을 바탕으로 압도적인 시장 점유율을 확보하고 있다.

우선 망분리 대응력 측면에서 글로벌 시장이 ZTNA와 같은 논리적 가상 경계를 선호하는 반면, 국내는 업무망과 인터

넷망을 물리적으로 분리하는 것이 법적 의무라는 차이점이 있다. 이에 따라 국산 NAC는 두 망 사이의 접점을 정밀하게 관리하고 비인가 기기의 혼용을 엄격히 방지하는 차단 능력을 필수적인 경쟁력으로 삼는다.

또한 사용자 편의성보다 보안 통제를 우선시하는 국내 정서에 맞추어 국산 NAC는 매우 강력한 단말 통제 기능을 수행한다. 이는 백신 및 패치의 강제 업데이트나 비인가 소프트웨어의 삭제를 직접 실행할 뿐만 아니라, 국내에서 주로 쓰이는 다양한 보안 프로그램들과 긴밀하게 연동되어 빈틈없는 통제 환경을 제공한다.

마지막으로 자산 식별의 정확도 면에서도 국산 벤더들은 국내 기업이 요구하는 부서별·자산 번호별 상세 관리 수준을 충족한다. 특히 국내에서 유통되는 다양한 장비와 IoT 기기에 대한 방대한 지문 데이터베이스를 자체적으로 보유하고 있어, 국내 환경 내에서의 기기 식별 정확도가 상대적으로 높다는 강점을 지닌다.

국내 NAC 시장에서는 지니언스가 2024년 조달청 기준 점유율 75%를 기록하며 압도적인 1위를 차지하고 있으며, 안랩과 넷맨 등이 그 뒤를 이어 경쟁하고 있다.

최근 한국 정부가 기존의 이분법적 망분리에서 벗어나 중요도에 따라 보안 수준을 차등화하는 다중보안체계(MLS) 로의 전환을 발표함에 따라, 국내 NAC 시장도 전환기를 맞이하고 있다. 향후 국산 솔루션들은 기존의 강점인 '통제 기능'을 유지하면서도, 외산 솔루션의 특징인 클라우드 유연성과 ZTNA 호환성을 신속히 확보하는 것이 시장 주도권 유지를 위한 관건이 될 것으로 전망된다.

3 내부의 블랙박스 EDR

EDR

내부 감찰관

개요 및 핵심 기능

엔드포인트 탐지 및 대응(EDR, Endpoint Detection and Response)은 PC, 서버, 스마트폰 등 네트워크의 말단(Endpoint)에서 발생하는 모든 행위를 실시간으로 기록하고 분석하여, 알려지지 않은 위협을 탐지하고 대응하는 보안 솔루션이다.

EDR은 단말 내부의 블랙박스 역할을 수행한다. 전통적인 백신(EPP, Endpoint Protection Platform)이 방패라면, EDR은 침투한 적을 찾아내는 역할을 수행한다. 특히 제로 트러스트 관점에서는 네트워크 경계를 뚫고 들어온 공격자의 은밀한 이동 경로를 파악하고, 실질적인 데이터 유출이 발생하기 전에 차단하는 심층 방어의 핵심 기능을 담당한다.

글로벌 시장 조사 및 전략 컨설팅 전문 기업 FMI는 2024년 49억 달러 규모의 전세계 NAC 시장이 2035년 403억 달러까지 성장하여 연평균 23.4%의 높은 성장세를 보일 것으로 전망하고 있다.

EDR의 4단계 작동 과정

EDR의 운용 프로세스는 EDR의 운용 프로세스는 수집, 탐지, 대응, 분석의 4단계로 구분된다.

1. 로그 수집 (Data Collection) 가장 먼저 단말 내에서 발생하는 프로세스 실행, 파일 생성, 네트워크 연결 등 모든 행위 데이터를 실시간으로 수집한다. 이를 통해 침해 사고 발생 시 과거의 역추적할 수 있는 실시간 이미지의 왼쪽에서 유입되는 화살표들은 이러한 기초 데이터를 의미하며, 이는 침해 사고 발생 시 과거 시점까지 역추적할 수 있는 포렌식(Forensics) 데이터를 확보한다.

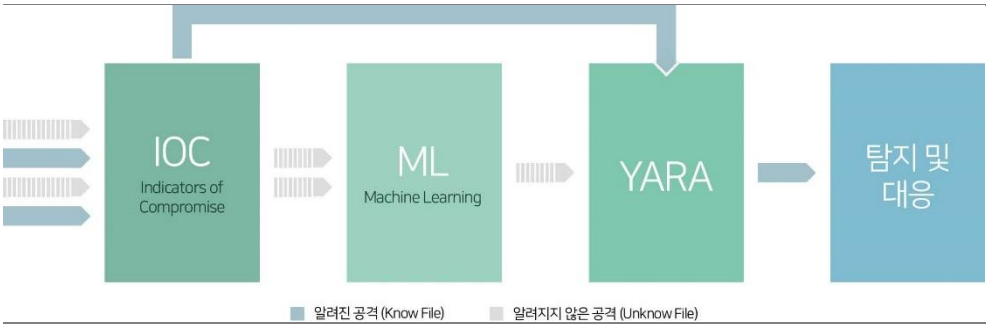
2. 위협 탐지 (Detection) 수집된 데이터는 세 가지 주요 필터를 거치며 정교하게 분석된다. 침해지표(IOC, Indicators of Compromise)는 이미 알려진 공격 정보를 바탕으로 위협을 1차적으로 식별한다. 알려진 악성코드뿐만

아니라, 악성 파일을 디스크에 남기지 않고 메모리에서만 실행되는 '파일리스(Fileless)' 공격이나 랜섬웨어의 행위 패턴을 머신러닝 기반으로 분석하여 잠재적 위협을 찾아낸다. .

3. 대응 및 격리 (Response & Containment) 위협이 확인되면 즉각적인 대응 조치를 수행한다. 악성 프로세스를 강제 종료하고, 관련된 파일을 삭제하며, 공격자가 다른 시스템으로 이동하지 못하도록 해당 단말을 네트워크로부터 논리적으로 격리한다.

4. 심층 분석 (Investigation) 공격의 유입 경로(Root Cause)와 피해 범위를 시각화하여 제공한다. 보안 담당자는 이를 통해 공격의 전체적인 맥락을 파악하고, 재발 방지를 위한 정책을 수립한다.

Genian EDR의 위협 탐지 단계



자료: 지니언스, 한국IR협의회 기업리서치센터

제로 트러스트와 EDR의 유기적 협업

NAC가 관문을 지키는 역할이라면, EDR은 관문을 통과한 이후 내부에서 벌어지는 모든 행위를 감시하는 '내부 감찰관'의 역할을 수행한다. 제로 트러스트의 핵심 전제 중 하나인 '침해 가정(Assume Breach)'은 아무리 견고한 관문을 세워도 공격자는 결국 내부에 침투할 수 있다는 현실을 인정하는 것이다. EDR은 이러한 전제하에 설계된 솔루션으로서, 이미 내부에 들어온 위협을 탐지하고 추적하는 데 초점을 맞춘다.

NAC가 접속 '시점'을 통제한다면, EDR은 접속 '이후' 전 기간에 걸쳐 단말 내부의 행위를 모니터링한다. 프로세스 실행, 파일 생성 및 변경, 레지스트리 수정, 네트워크 연결 시도 등 단말에서 발생하는 모든 이벤트가 EDR의 감시 대상이다. 예를 들어, 정상적인 인증 절차를 거쳐 네트워크에 접속한 직원의 PC에서 갑자기 다수의 파일이 암호화되기 시작하거나, 평소 접속하지 않던 서버로 대량의 데이터가 전송되는 행위가 감지되면 EDR은 이를 랜섬웨어 감염 또는 데이터 유출 시도로 판단하고 즉각적인 대응 조치를 수행한다.

EDR은 제로 트러스트 아키텍처에서 '위협 인텔리전스의 원천'이자 '대응 조치의 트리거' 역할을 수행한다. EDR이 수집한 단말 행위 로그는 보안 정보 및 이벤트 관리(SIEM) 시스템으로 전송되어 전사적 위협 분석의 기초 데이터로 활용된다. EDR이 이상 징후를 탐지하면 보안 오케스트레이션 및 자동화 대응(SOAR) 시스템에 신호를 보내 방화벽 정책 수정, 계정 잠금, NAC를 통한 네트워크 격리 등 연쇄적인 대응 조치를 자동으로 실행한다.

특히 현대의 네트워크 환경에서는 암호화 통신(HTTPS, TLS 등)의 비중이 급격히 증가하여 네트워크 단에서의 트래픽 분석만으로는 위협을 탐지하기 어려워졌다. 이러한 환경에서 EDR은 암호화되기 전 또는 복호화된 이후의 단말 내부 행위를 직접 관찰함으로써 네트워크 기반 탐지의 사각지대를 보완한다. 결론적으로, EDR은 '접속한 사용자가 내부에서 무엇을 하고 있는가'라는 질문에 답하는 솔루션이다.

EDR 솔루션 경쟁 구도 및 시장 동향

현재 글로벌 EDR 시장은 클라우드 기반의 분석 능력을 앞세운 전문 EDR 기업과 기존 백신 시장을 장악했던 대형 보안 기업 간의 치열한 경쟁 구도를 형성하고 있다.

우선 CrowdStrike(미국)나 SentinelOne(미국)과 같은 전문 EDR 기업들은 태생부터 클라우드 네이티브 아키텍처를 채택하여 전 세계에서 수집된 방대한 위협 데이터를 AI로 분석하는 능력에서 기술적 우위를 점하고 있다. 이들은 단말에 가해지는 부담을 최소화한 경량화된 에이전트와 위협 발생 시 즉각적으로 작동하는 자동화된 대응 능력을 핵심 경쟁력으로 삼아 시장의 변화를 주도하고 있다.

반면 Microsoft(미국), Trend Micro(일본), Trellix(미국, 구 McAfee 기업보안 사업부)와 같은 대형 보안 기업들은 기존에 이미 널리 보급된 백신 엔진이나 윈도우(Windows)와 같은 운영체제와의 강력한 통합성을 주요 무기로 내세운다. 특히 별도의 에이전트를 추가로 설치할 필요 없이 기존 환경에서 기능을 활성화하는 방식의 편의성을 제공함으로써 기존 고객층의 점유율을 견고하게 방어하고 있다.

국내 EDR 시장은 글로벌 트렌드를 따르면서도 망분리 환경과 국산 소프트웨어 호환성이라는 특수한 요인으로 인해 국산 솔루션들이 시장에서 강세를 보인다.

먼저 폐쇄망 지원 측면에서 국산 솔루션의 강점이 두드러진다. 위협 분석을 위해 클라우드 서버와의 통신을 필수적으로 요구하는 글로벌 솔루션과 달리, 국산 EDR은 인터넷이 차단된 국내 공공 및 금융권의 폐쇄망 환경을 고려하여 온프레미스 서버에서도 원활한 분석 기능을 제공함으로써 환경적 제약을 해결한다.

또한 국내 업무 환경에 필수적인 DRM(Digital Rights Management, 키보드 보안 등)이나 키보드 보안 프로그램 등 각종 보안 솔루션과의 충돌 문제를 해결하는 것이 EDR 도입의 핵심 난제로 꼽히는데, 국산 벤더들은 이러한 국내 특유의 소프트웨어 환경에 대한 높은 이해도를 바탕으로 신속한 최적화와 기술 지원을 제공한다.

마지막으로 행위 기반 탐지 영역에서도 국산 솔루션은 차별화된 경쟁력을 보유하고 있다. 단순한 시그니처 매칭 방식에서 벗어나 한국형 랜섬웨어나 북한발 사이버 공격과 같이 국내를 겨냥한 타깃형 위협에 특화된 행위 분석 시나리오를 정교하게 제공함으로써 보안의 실효성을 높인다.

국내 EDR 시장에서는 지니언스가 초기 시장을 선점하며 공공 및 금융권에서 높은 점유율을 바탕으로 국내 시장의 49%(2024년 조달청 기준)를 차지하고 있으며, 백신 시장의 강자인 안랩이 EPP와 EDR을 통합한 모델로 추격하고 있다. 이외에 소만사 등이 데이터 유출 방지(DLP, Data Loss Prevention)와 연계된 EDR을 선보이며 경쟁에 가세하고 있다.

향후 EDR 시장은 단말 보안을 넘어 네트워크(NDR, Network Detection and Response), 클라우드 등을 통합 관제하는 XDR(Extended Detection and Response)로 빠르게 진화할 것으로 전망된다. 그러나 XDR로 확장될수록 방대한 위협 로그를 실시간으로 분석하고 대응하는 데 필요한 전문 인력과 운영 역량의 부담이 커진다. 이에 따라 보안 전문가가 고객사를 대신하여 24시간 위협을 모니터링하고 대응하는 MDR(Managed Detection and Response, 관리형 탐지 및 대응) 서비스의 중요성이 부각되고 있다. 국내 기업들도 단순히 솔루션을 판매하는 것을 넘어, 고객사의 보안 운영을 전담하는 MDR 서비스 역량을 확보하는 것이 경쟁의 핵심이 될 것이다.

1 정부 주도의 사이버 보안 시장 성장

사이버 보안 정책의 흐름

1. 규제 강화

2. 투명성 강화

3. 유연성 확보

정부 사이버 보안 정책의 패러다임 전환

2024년부터 2025년에 걸쳐 한국 정부의 사이버 보안 정책은 세 가지 축을 중심으로 근본적인 변화를 겪고 있다. 첫 째는 기업에 대한 규제와 제재 수위의 강화이고, 둘째는 보안 투자 현황의 대외 공개 범위 확대이며, 셋째는 기존 물리적 망분리 체계의 유연화이다. 이 세 가지 정책 방향은 모두 '기업의 자율적 보안 역량 강화'라는 공통된 목표를 지향하며, 보안을 선택적 비용이 아닌 경영상의 필수 요건으로 격상시키고 있다.

1. 규제 강화: 범부처 정보보호 대책 및 개인정보보호법 개정

정부는 2025년 10월 잇따른 대규모 개인정보 유출 사고에 대응하여 과학기술정보통신부를 중심으로 국가안보실, 금융위원회, 개인정보보호위원회, 국가정보원 등 관계 부처 합동의 범부처 정보보호 종합대책을 발표하였다. 이번 대책은 기존의 자율 규제 기조에서 벗어나 정부의 직접적인 통제 권한을 강화하고, 소비자 중심의 피해 구제 체계로 전환하는 것을 핵심으로 한다.

구체적인 내용을 살펴보면, 우선 국민 생활과 밀접한 공공기관, 금융권, 통신사 등 1,600여 개 핵심 IT 시스템에 대해 즉시 보안 취약점 전수 점검이 실시된다. 특히 통신사 등 주요 인프라 사업자에 대해서는 실제 해킹 방식을 적용한 고강도 불시 점검이 정례화되며, 기존 서류 위주였던 정보보호 관리체계(ISMS, Information Security Management System) 인증 심사가 현장 심사 중심으로 전환된다. 중대 결함 발견 시 인증을 즉시 취소하는 원스트라이크 아웃 제도도 도입된다.

사고 발생 시 책임 소재 또한 명확해진다. 해킹 사고 시 소비자가 기업의 과실을 증명해야 했던 기존 관행이 개선되어, 기업이 무과실을 입증하지 못하면 배상 책임을 지도록 입증 책임이 전환된다. 또한 기업의 자진 신고가 없더라도 해킹 정황이 포착되면 정부가 즉시 직권으로 조사에 착수할 수 있도록 권한이 확대된다.

범부처 대책이 행정적 관리 감독을 강화하는 조치라면, 개인정보보호법 개정은 기업에 대한 재무적 제재 수위를 높여 실질적인 보안 투자를 강제하는 역할을 한다. 2023년 9월 개정된 현행법은 과징금 산정 기준을 기존 '위반 행위 관련 매출액'에서 '전체 매출액'의 3%로 변경하였다. 여기에 더해 2025년 12월 국회 상임위를 통과한 개정안은 고의 또는 중과실로 인한 사고나 대규모 피해 발생 등 중대 위반 행위에 대해 과징금 상한을 전체 매출액의 10%까지 상향하는 내용을 담고 있다. 이는 유럽의 일반개인정보보호법(GDPR, General Data Protection Regulation)을 상회하는 수준의 규제로서, 보안 사고가 단순한 비용 처리가 아닌 경영상의 중대한 위기로 직결될 수 있음을 시사한다.

2. 투명성 강화: 정보보호 공시 의무 대상 확대

정보보호 공시 제도는 기업이 정보보호 투자 현황이나 인력 보유 현황 등을 대외에 공개하도록 하는 제도로서, 2016년 자율 공시 형태로 처음 도입된 이후 단계적으로 강화되어 왔다.

제도의 분기점이 된 것은 2021년 12월이다. 비대면 서비스의 확산으로 기업의 정보보호 책임이 강조되면서 법률 개정을 통해 정보보호 공시가 의무 제도로 전환되었다. 다만 당시에는 산업계의 부담을 고려하여 의무 대상을 매출액 3,000억 원 이상이면서 일일 평균 이용자 수가 100만 명 이상인 대형 사업자와 기간통신사업자, 집적정보통신시설 사

업자, 상급종합병원, 클라우드 서비스 제공자 등으로 한정하였다. 이에 따라 현재까지는 해당 기준을 충족하는 약 600~700여 개의 대기업 및 특수 사업자만이 IT 예산 대비 정보보호 투자 비중과 전문 인력 현황 등을 의무적으로 공개하고 있다.

그러나 2026년 1월 과학기술정보통신부가 발표한 시행령 개정안과 범부처 정보보호 대책에 따라 공시 제도는 대폭 확대될 예정이다. 정부는 2027년부터 기존의 매출액 및 이용자 수 기준을 폐지하고, 유가증권시장 및 코스닥시장에 상장된 모든 법인과 정보보호 관리체계(ISMS) 인증을 받은 기업으로 의무 대상을 확대할 방침이다. 이는 정보보호 공시가 더 이상 대기업만의 의무가 아니라 상장 기업이라면 갖춰야 할 기본 요건이 됨을 의미하며, 향후 수천 개 기업이 새롭게 공시 의무를 지게 된다.

3. 유연성 확보: 망분리 완화 및 다층보안체계(MLS) 도입

망분리는 외부 인터넷망과 내부 업무망을 서로 접속하지 못하도록 차단하여 외부 해킹 위협을 원천 봉쇄하는 보안 체계로서, 그간 한국 보안의 표준으로 자리 잡아왔다. 그러나 인터넷망과 업무망의 단절로 인해 생성형 인공지능이나 서비스형 소프트웨어(SaaS) 등 외부 기반 기술을 업무에 활용하는 것이 불가능하며, 자료 이동 시 별도의 망 연계 솔루션을 거쳐야 하는 복잡한 절차가 기업 및 공공기관의 생산성을 저해하는 요인으로 지목되어 왔다.

이에 정부는 기존의 획일적인 물리적 망분리 원칙을 완화하고, 데이터의 중요도에 따라 보안 등급을 차등화하는 다층보안체계(MLS, Multi-Level Security)로의 전환을 추진한다. 공공 부문에서는 국가정보원이 주도하여 업무 중요도에 따라 시스템을 기밀(C, Classified), 민감(S, Sensitive), 공개(O, Open)의 3단계로 분류하는 로드맵을 수립하였다. 안보와 직결된 기밀 등급은 기존과 동일하게 물리적 망분리를 유지하지만, 일반 행정 정보인 민감 등급은 논리적 망분리를 허용한다. 특히 공개 등급의 경우 인터넷망 활용을 전면 허용함으로써 공공기관에서도 생성형 인공지능이나 민간 클라우드 서비스를 자유롭게 이용할 수 있는 환경이 조성된다.

금융 부문 역시 금융위원회를 중심으로 규제 개선이 단계적으로 추진된다. 초기에는 금융규제 샌드박스를 활용하여 내부망에서도 예외적으로 SaaS 기반의 협업 툴이나 생성형 인공지능 사용을 허용하며, 점진적으로 개인정보가 없는 연구개발 및 테스트 서버에 대해서는 물리적 망분리 규제를 적용하지 않는다.

정부 사이버 보안 정책 패러다임

자료: Gemini, 한국IR협의회 기업리서치센터

변화의 흐름

1. 컴플라이언스 수요 증가

2. 제로 트러스트 도입 촉진

3. 엔드포인트 보안 부각

정책 변화가 보안 시장에 미치는 영향

앞서 살펴본 세 가지 정책 방향은 보안 시장에 구조적인 변화를 야기한다. 규제 강화는 컴플라이언스 수요를 증가시키고, 망분리 완화는 제로 트러스트 아키텍처 도입을 가속화하며, 입증 책임 전환은 엔드포인트 보안의 중요성을 부각시킨다.

1. 컴플라이언스 수요 증가

범부처 대책이 주요 IT 시스템에 대한 전수 점검과 불시 점검을 예고함에 따라, 기업들은 내부 네트워크에 존재하는 모든 자산을 식별하고 통제해야 할 의무를 지게 된다. 또한 정보보호 공시 의무 대상이 전체 상장사로 확대되면, 기존에 보안 체계가 미비했던 중소·중견 상장사들도 공시 데이터 산출을 위한 기초 인프라를 갖추어야 한다.

2021년 정보보호 공시가 의무화되었을 당시, 보안 산업계에는 '보안 투자의 정량화'라는 구조적 변화가 발생하였다. 이전까지 기업의 보안 지출은 비용으로만 인식되어 최소화해야 할 대상이었으나, 공시 제도를 통해 정보보호 투자액과 전담 인력 수가 대외에 공개되면서 동종 업계 간의 비교 우위를 점하기 위한 지표 경쟁이 시작되었다. 특히 공시 데이터의 신뢰성을 확보하기 위해 필수적으로 요구되는 정보보호 관리체계(ISMS) 인증 수요가 급증하였으며, ISMS 인증 심사 항목 중 '자산 관리'와 '접근 통제'를 만족시키기 위해 네트워크접근제어(NAC) 솔루션 도입이 필수적인 요소로 부상하였다.

2027년 정보보호 공시 의무의 전체 상장사 확대 시행이 예고되면서, 관련 컴플라이언스 수요가 크게 늘어날 것으로 예상된다. 보안 인프라가 견고한 대기업에 비해 보안 체계가 미흡한 중소·중견 상장사들이 대거 공시 대상에 포함될 것으로 보여, 이들의 신규 보안 솔루션 도입이 가속화될 전망이다.

2. 제로 트러스트 아키텍처 도입 가속화

망분리 완화로 인해 내부와 외부의 경계가 모호해짐에 따라, 기존의 '신뢰 구역'이라는 개념은 더 이상 유효하지 않게 된다. 물리적 경계 차단이라는 방어막이 사라진 상태에서는 '아무것도 신뢰하지 않고 항상 검증한다(Never Trust, Always Verify)'는 제로 트러스트 원칙이 새로운 보안 표준으로 부상한다.

제로 트러스트 환경에서는 단순히 특정 네트워크에 접속해 있다는 사실만으로 권한을 부여하지 않는다. 접속하는 사용자의 신원, 기기의 보안 상태, 접근 위치와 시간 등을 종합적으로 분석하여 최소한의 권한만을 부여하는 자격 증명 중심의 접근 통제가 요구된다. 또한 최초 접속 시뿐만 아니라 세션이 유지되는 동안에도 지속적으로 단말의 상태를 감시하고, 이상 징후 발생 시 즉각적으로 접속을 차단하는 실시간 대응 능력이 필수적이다.

정부는 2026년부터 공공기관에 제로 트러스트 도입을 의무화할 방침이며, 이에 따라 제로 트러스트 네트워크 액세스(ZTNA) 솔루션에 대한 수요가 본격화될 것으로 전망된다. 제로 트러스트는 단일 솔루션이 아니라 신원 및 접근 관리(IAM), 네트워크접근제어(NAC), 엔드포인트 탐지 및 대응(EDR) 등 다양한 보안 기술이 유기적으로 결합된 아키텍처를 의미하므로, 관련 솔루션 시장 전반에 걸쳐 성장이 예상된다.

3. 엔드포인트 보안의 중요성 부각

입증 책임의 전환은 엔드포인트 보안 솔루션의 위상을 근본적으로 변화시킨다. 강화된 법령 하에서 기업이 전체 매출액의 10%에 달하는 징벌적 과징금을 회피하기 위해서는 해킹 사고 발생 시 회사의 무과실이나 충분한 보호 조치를 스스로 입증해야 한다. 이를 위해서는 침해 사고의 원인을 규명하고 기업이 적절한 대응 조치를 수행했음을 증명할 수

있는 포렌식 데이터의 확보가 필수적이다.

엔드포인트 탐지 및 대응(EDR) 솔루션은 단말 내에서 발생하는 프로세스 실행, 파일 생성, 레지스트리 변경, 네트워크 연결 등 모든 행위 데이터를 실시간으로 수집하고 기록한다. 이를 통해 침해 사고 발생 시 과거 시점까지 역추적할 수 있는 증거 자료를 확보할 수 있으며, 사고 원인을 규명하고 기업의 면책 사유를 증명하는 데 활용된다. 따라서 EDR은 단순한 보안 솔루션을 넘어, 징벌적 과징금 리스크에 대비하기 위한 경영진의 필수 리스크 관리 수단으로 위상이 격상된다.

또한 망분리 완화로 인해 외부 인터넷망과 직접 접촉하는 단말은 사이버 공격의 최전선이 된다. 공개 등급 데이터가 외부 클라우드 및 생성형 인공지능과 연결될 때, 전통적인 백신과 같이 알려진 패턴만을 차단하는 방식으로는 지능형 지속 위협(APT, Advanced Persistent Threat)에 대응할 수 없다. 단말 내부에서 일어나는 모든 행위를 기록하고, 비정상적인 프로세스나 파일 실행을 인공지능 기반으로 탐지하여 즉각 대응하는 EDR의 역할이 더욱 중요해지는 이유이다.

지니언스가 솔루션

지니언스에 대한 시사점

앞서 분석한 정책 변화와 시장 영향은 국내 네트워크접근제어(NAC) 시장 점유율 1위이자 엔드포인트 탐지 및 대응(EDR) 선도 기업인 지니언스의 구조적 실적 성장을 견인할 것으로 전망된다. 지니언스는 다층보안체계의 핵심인 NAC, EDR, ZTNA 전 영역에서 기술적 우위를 점하고 있어 정책 수혜의 가장 직접적인 영향권에 위치한다.

1. NAC: 자산 식별 및 접근 통제 수요 지속

지니언스의 주력 제품인 Genian NAC는 2024년 조달청 기준 국내 시장점유율 75%를 기록하며 압도적인 1위를 차지하고 있다. NAC는 네트워크에 접속하려는 모든 단말기의 신원을 식별하고 보안 정책 준수 여부를 검토하여 접속 권한을 차등 부여하는 솔루션으로서, 정보보호 관리체계(ISMS) 인증의 핵심 요건인 '자산 관리'와 '접근 통제'를 충족시키기 위한 기초 인프라 역할을 수행한다.

정보보호 공시 의무 대상이 전체 상장사로 확대되면, 새롭게 규제 시장에 진입하는 수천 개의 중소·중견 상장사들은 공시 데이터 산출을 위해 가장 먼저 '보호해야 할 IT 자산이 무엇인지'를 파악해야 한다. 이를 자동화하여 식별해주는 솔루션이 바로 NAC이며, 지니언스는 국내 유통 장비 및 IoT 기기에 대한 방대한 장비 지문 데이터베이스를 보유하고 있어 식별 정확도 측면에서 외산 솔루션 대비 경쟁 우위를 갖추고 있다.

물리적 망분리가 완화되면 경계 보안의 중요성이 낮아질 것이라는 우려와 달리, 다층보안체계 하에서는 내부망에 접속하는 다양한 단말을 식별하고 통제하는 기능이 더욱 중요해진다. 제로 트러스트 환경에서 NAC는 기기(Device) 영역의 검증을 담당하는 기반 기술로서 그 역할이 확대되며, 이는 지니언스의 NAC 사업이 성숙 시장에서도 안정적인 현금 창출 능력을 유지할 수 있는 근거가 된다.

2. EDR: 입증 책임 전환에 따른 필수재화

지니언스의 EDR은 국내 최초로 개발된 EDR 솔루션으로서, 2024년 조달청 기준 49%의 시장점유율로 1위를 기록하고 있다. 침해사고지표(IOC, Indicator of Compromise), 머신러닝, 행위기반탐지, YARA 룰[1]등 다단계 위협탐지 엔진을 탑재하고 있으며, 특히 안티랜섬웨어 모듈을 국내 최초로 EDR에 탑재하여 기술적 차별성을 확보하였다.

입증 책임 전환에 따라 EDR은 단순한 위협 탐지 도구를 넘어 법적 리스크를 관리하는 필수재로 전환된다. 기업이 해

[1] YARA 룰: 악성코드 분석 및 탐지를 위한 규칙 기반 스캐너인 YARA 도구에서 사용하는 패턴 규칙으로 악성코드의 존재 여부를 식별하고 분류

킹 사고 시 무과실을 입증하기 위해서는 악성 행위의 징후를 탐지하고 상세 기록을 저장하는 EDR의 포렌식 데이터가 핵심적인 증거 자료로 활용되기 때문이다. 이는 공공 및 금융권을 중심으로 EDR 도입을 가속화하는 요인으로 작용할 것이다.

또한 망분리 완화로 인해 공개 등급 데이터가 인터넷 및 클라우드 서비스와 연결되면, 단말 보안의 중요성이 비약적으로 증대된다. 지니언스는 공공 조달 EDR 시장에서 최다 레퍼런스를 보유하고 있으며, 구독형(SaaS) 모델을 통해 초기 투자 비용에 민감한 중소 상장사들의 진입 장벽을 낮추고 있어 시장 확대에 따른 수혜를 가장 크게 누릴 것으로 판단된다. 특히 기존 NAC 고객사가 보안 강화를 위해 EDR을 추가 도입하는 교차 판매 기회가 확대될 것으로 예상된다.

3. ZTNA: 공공 부문 의무화에 따른 신성장 동력

정부가 2026년부터 공공기관에 제로 트러스트 도입을 의무화함에 따라, 지니언스의 ZTNA 솔루션이 본격적인 실적 기여 단계에 진입한다. 지니언스는 2024년 과학기술정보통신부가 발주한 '제로 트러스트 도입 시범사업'을 수주하여 ZTNA 기반의 정책시행지점(PEP, Policy Enforcement Point) 개발을 담당하였으며, 이를 통해 기술적 역량을 검증받은 바 있다.

지니언스의 Genian ZTNA는 기존 NAC의 강력한 단말 식별 기술에 정교한 사용자 인증과 권한 제어를 결합한 차세대 보안 솔루션이다. 이는 전통적인 가상사설망(VPN)의 한계를 극복하여 사용자에게 네트워크 전체가 아닌 승인된 특정 애플리케이션에 대해서만 최소 권한을 부여하는 방식을 채택하고 있다.

성능 및 신뢰성 측면에서는 2024년 8월 Genian ZTNA 6.0이 공통평가기준(CC) 인증을 획득한 데 이어, 2025년 상반기 중 조달 등록을 완료함으로써 공공 시장 진입을 위한 모든 행정적·기술적 준비를 마쳤다. 현재는 다층보안체계(MLS) 및 제로 트러스트 전환을 추진하는 주요 공공기관과 기업을 대상으로 본격적인 공급이 이루어지며 시장 표준으로서의 입지를 공고히 하고 있다.

지니언스는 NAC, EDR, ZTNA를 통합한 'Zero Trust Access Platform'을 제공하고 있으며, 기기 플랫폼 인텔리전스(DPI, Device Platform Intelligence)를 기반으로 네트워크에 연결된 모든 기기의 정보를 수집하고 일관된 보안 정책을 적용할 수 있도록 설계되어 있다. 이러한 통합 플랫폼 전략은 제로 트러스트 아키텍처가 다양한 보안 기술의 유기적 결합을 요구한다는 점에서 경쟁 우위 요소로 작용한다. 2025년까지의 선제적 투자가 2026년 정부 실증 사업 및 본 사업 예산 집행과 맞물리며 수익성을 견인할 것으로 전망된다.

소결

국가 보안 정책이 자율 규제에서 강제 규제로, 물리적 망분리에서 다층보안체계로 전환되는 과정은 지니언스에게 단순한 규제 변화를 넘어선 구조적 성장의 기회를 제공한다. 과거 물리적 망분리가 제공하던 경계 보안의 시대가 저물고, 실시간 검증과 엔드포인트 가시성이 핵심인 데이터 중심 보안의 시대가 도래하였기 때문이다.

정부의 강력한 통제 정책과 징벌적 과징금 제도는 기업들의 보안 예산 집행을 강제하는 요인으로 작용하고 있다. 이는 NAC의 안정적인 현금 창출 능력 위에 EDR이라는 고성장 동력이 더해지고, ZTNA를 통한 신규 시장 개척이 가능해지는 복합적인 실적 성장의 근거가 된다. 지니언스가 보유한 NAC 기반의 식별 기술과 EDR의 탐지 역량은 새로운 보안 인프라의 필수 구성 요소로 자리 잡을 것이며, 이는 동사의 시장 지배력을 공공 부문을 넘어 민간 상장사 전반으로 확장시키는 요인이 될 것으로 판단된다.

실적 추이 및 전망

1 실적 전망

2025년 전망

매출액 520억 원(yoy 5%)

영업이익 75억 원(yoy -24%)

2025년 전망: '투자의 해', 퀀텀 점프를 위한 체력 비축

지니언스의 2025년 실적은 공공 및 민간 부문의 보안 수요 확대에도 불구하고 수익성이 일시적으로 둔화될 전망이다. 이는 정부 예산 집행 지연과 투자 우선순위 변화, 그리고 미래 성장을 위한 선제적 비용 투입에 기인한다. 연간 매출액은 520억 원(yoy +5%), 영업이익 75억 원(yoy -24%), 영업이익률 14.4%(전년대비 5.4%p 하락)로 예상된다.

참고로 2025년 3분기까지의 누적 실적은 매출액 312억 원(yoy +7%), 영업이익 22억 원(yoy -41%), 영업이익률 6.9%(전년동기대비 5.5%p 하락)를 기록했다. 4분기는 보안 업체들의 전통적 성수기로, 연간 매출의 40%에 해당하는 208억 원(yoy +2.2%)의 매출이 예상된다.

1. 네트워크 보안 제품

네트워크 보안 제품 매출(NAC, Insights E 등)은 434억 원(yoy +5%)이 예상된다. 제로 트러스트(ZTNA) 도입 의무화 등 우호적인 정책 환경은 조성되었으나, 연초 정부의 정보보호 예산 삭감과 고위 실무진의 인사 지연으로 인해 예산 집행이 하반기로 크게 밀려난 점이 외형 성장의 제약 요인으로 작용했다. 특히 행정망 마비 사태 이후 정부의 투자 우선순위가 백업 및 재해 복구(DR, Disaster Recovery) 솔루션으로 일시적으로 쏠리면서 보안 제품 수주가 예상보다 지연되었다. 또한 사이버 위협 증가로 인한 기업들의 높은 관심이 벤치마킹 테스트(BMT) 등 실무 검토 단계에 머물며 실제 매출로 전환되기까지 시차가 발생한 점도 실적에 영향을 미쳤다.

2. 네트워크 보안 용역

네트워크 보안 용역 매출은 86억 원(yoy +6%)으로 추정된다. 기존 고객사를 대상으로 한 유지보수 및 컨설팅 수요가 꾸준히 발생하며 안정적인 캐시카우 역할을 수행하고 있다. 특히 망 분리 규제 완화에 따른 보안 고도화 수요가 용역 매출의 질적 개선으로 이어지고 있는 점은 긍정적이다.

지니언스는 2026년 실행의 해를 앞두고 제로 트러스트 및 ZTNA 솔루션 고도화와 신규 백신 라인업 강화를 위한 R&D 인력 확충 등을 진행했다. 이로 인해 2025년 영업이익은 전년 대비 감소한 75억 원이 전망된다.

2026년 전망

매출액 601억 원(yoy 16%)

영업이익 115억 원(yoy 53%)

2026년 전망: 실적 퀀텀 점프와 수익성 정상화

지니언스의 2026년 실적은 2025년의 선제적 투자를 발판 삼아 본격적인 외형 성장과 수익성 개선이 맞물리는 실행과 결실의 해가 될 것으로 전망된다. 연간 매출액은 전년 대비 16% 증가한 601억 원, 영업이익은 전년 대비 53% 증가한 115억 원을 기록할 것으로 보이며, 영업이익률은 19.1%까지 회복될 것으로 전망된다. 이러한 반등은 공공기관의 제로 트러스트(ZTNA) 도입 의무화와 더불어, 민간 상장사 전체로 확대되는 보안 규제 강화에 따른 신규 수요 창출에 기인한다.

1. 네트워크 보안 제품: 규제 강제화에 따른 구조적 성장

2026년 네트워크 보안 솔루션(NAC, Insights E, ZTNA) 매출은 전년 대비 18% 증가한 511억 원을 기록할 것으로 예

상된다.

- NAC (자산 식별의 필수화): 2027년 정보보호 공시 의무가 전 상장사로 확대가 추진됨에 따라, 2026년부터 수천 개의 중소·중견 상장사들이 공시 데이터 산출을 위한 기초 인프라로 NAC를 도입할 것으로 보인다. 특히 지니언스의 NAC는 공시의 핵심인 '자산 식별' 및 '접근 통제' 영역에서 압도적 점유율을 보유하고 있어 규제 확대에 따른 직접적인 수혜가 예상된다.
- Insights E (법적 리스크 관리의 필수재): 개인정보보호법 개정으로 기업의 입증 책임이 강화되고 과징금 상한이 전체 매출의 10%로 상향됨에 따라, EDR은 경영진의 필수 방어 기제로 격상되었다. 사고 발생 시 무과실을 증명할 수 있는 포렌식 데이터를 제공하는 EDR의 특성상, 공공 및 금융권을 넘어 민간 대형 사업자의 도입이 가속화될 전망이다.
- ZTNA/MLS (망분리 완화의 대안): 기존의 획일적인 물리적 망분리 원칙이 다층보안체계(MLS)로 전환되면서, 경계 보안의 공백을 메울 ZTNA 솔루션 수요가 본격화될 것이다. 2025년까지 기술 검증과 조달 등록을 마친 지니언스의 ZTNA가 공공기관 제로 트러스트 도입 의무화와 맞물려 실질적인 실적 성장을 견인할 것으로 분석된다.

2. 네트워크 보안 용역: 서비스 매출 확대 및 영업 레버리지 본격화

유지보수 및 컨설팅 등 서비스 부문은 전년 대비 5% 성장한 90억 원의 매출이 기대된다.

- 구독형 매출(SaaS) 비중 확대: NAC와 EDR의 설치 기반(Installed Base)이 대폭 늘어남에 따라, 안정적인 유지보수 매출 비중이 확대되어 실적의 안정성이 높아질 전망이다.

전체적인 수익성 개선은 매출 확대에 따른 고정비 분산 효과에서 비롯된다. 2025년 단행된 R&D 인력 확충과 신규 솔루션 라인업 강화 투자가 마무리된 상태로 매출이 확대됨에 따라 영업 레버리지 효과가 본격적으로 나타날 전망이다.

지니언스 실적 추이 및 전망

(단위: 억 원)

구분	1Q24	2Q24	3Q24	4Q24	1Q25	2Q25	3Q25	4Q25E	2021	2022	2023	2024	2025E	2026E
매출액	70	119	104	203	94	114	104	208	319	385	429	496	520	601
네트워크 보안 제품매출	54	99	82	179	76	94	82	182	263	314	348	415	434	511
네트워크 보안 용역 매출	16	20	21	24	17	21	22	26	56	70	81	81	86	90
기타(임대)	0	0	0	0	0	0	0	0	0	0	0	0	0	0
매출 비중														
네트워크 보안 제품매출	77%	84%	79%	88%	82%	82%	79%	88%	82%	82%	81%	84%	83%	85%
네트워크 보안 용역 매출	23%	16%	21%	12%	18%	18%	21%	12%	18%	18%	19%	16%	17%	15%
영업이익	-5	19	22	62	0	11	11	53	59	69	65	98	75	115
영업이익률	-6.5%	15.7%	21.6%	30.4%	0.4%	9.3%	10.3%	25.7%	18.5%	18.0%	15.1%	19.8%	14.4%	19.1%
성장률														
매출액					34%	-4%	0%	2%		20%	12%	16%	5%	16%
네트워크 보안 제품매출					41%	-6%	-1%	2%		19%	11%	19%	5%	18%
네트워크 보안 용역 매출					9%	6%	4%	5%		26%	15%	1%	6%	5%
영업이익					-108%	-43%	-52%	-14%		17%	-7%	52%	-24%	53%

자료: 지니언스, 한국IR협의회 기업리서치센터

Valuation

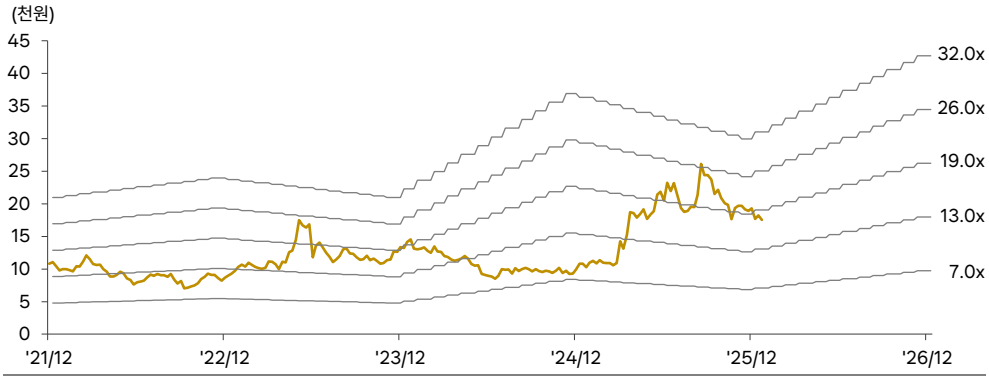
1 기대가 현실이 되기 전

지니언스의 현재 주가는 2026년 예상 실적 기준 P/E 14배 수준에서 거래되고 있다. 이는 2022년 이후 형성된 동사의 역사적 P/E 밴드(7배~26배)의 중하단 부근에 위치한 수치로, 과거 대비 밸류에이션 부담이 완화된 구간으로 판단한다.

지난 2025년 9월, 잇따른 해킹 사고와 국가정보자원관리원 화재 등으로 사이버 보안 강화에 대한 시장의 기대 심리가 극대화되며 동사의 주가는 역사적 밴드 상단(26배)에 도달한 바 있다. 그러나 공공 부문 예산 집행의 일시적 지연, 정부 정책 수립 후 실제 기업들의 수주 및 수행까지 발생하는 시차(Time Lag) 등의 영향으로 하반기 실적이 당초 기대치를 하회하며 밸류에이션 프리미엄이 지속되지 못했다. 특히 2025년은 이례적인 EPS 감소가 예상되며 주가 성장이 제한되는 인고의 시기를 보냈다.

2026년은 지난 1년간 지연되었던 보안 예산 집행이 본격화되고, 제로 트러스트(Zero Trust) 등 정부의 보안 로드맵이 실제 수주로 연결되는 실적 턴어라운드의 원년이 될 전망이다. 단순한 심리적 기대감을 넘어 EPS 성장이 가시화되는 구간에 진입함에 따라, P/E 배수가 상승할 수 있을 것으로 전망된다.

지니언스 역사적 PER 밴드



자료: Quantiwise, 한국IR협의회 기업리서치센터

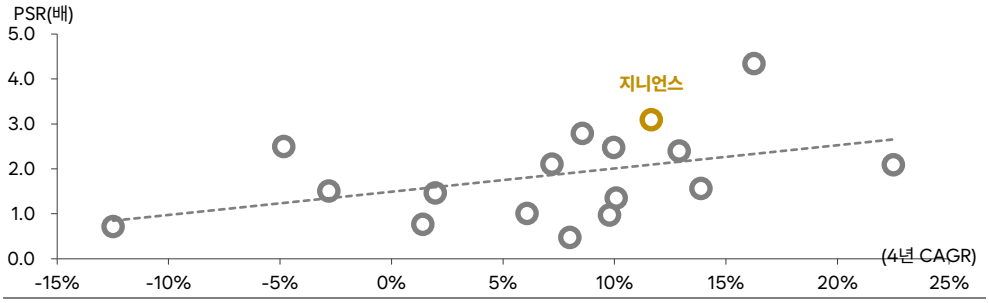
2 합당한 프리미엄

사이버 보안 솔루션 기업을 비교 평가할 때 PSR(주가매출비율)은 다른 가치평가 방법론에 비해 효과적인 기준을 제시한다. 이는 사이버 보안 산업의 고유한 특성, 즉 정책 변화에 따른 수요 변동성과 R&D 투자 부담에 기인한다. 사이버 보안 기업들은 제로 트러스트, 망분리 완화 등 정부 정책 변화에 선제적으로 대응하기 위해 지속적인 기술 투자가 필수적이다. 이로 인해 매출이 성장하더라도 연구개발비 증가로 이익률이 일시적으로 하락하는 경우가 빈번하다. 또한 사이버 보안 기업들은 공공 부문 수주 시기에 따라 분기별 실적 변동성이 크고, 구독형(SaaS) 모델 전환 과정에서 단기 수익성이 저하되는 경향을 보여 수익가치 중심으로 기업의 본질적인 가치를 제대로 평가하기 어렵다.

PSR은 매출액에 초점을 맞추고 있어, 기업이 시장에서 얼마나 빠르게 성장하고 있는지를 명확하게 보여준다. 또한 매출액이 회계적인 처리 방식에 따른 이익의 왜곡 가능성이 적어, 동종 산업 내 기업들을 비교하는 데 있어 보다 일관되고 안정적인 기준을 제공한다.

지니언스의 지난 4개 분기 실적(2024년 4분기~2025년 3분기) 기준 Trailing PSR은 3.1배로, 안랩, 윈스, 이글루, 라온시큐어, 파수, 모니터랩, 한싹 등 상장된 주요 사이버 보안 업체 16개사의 평균인 1.8배 대비 높은 프리미엄을 받고 있다. 일반적으로 PSR 배수를 결정하는 가장 중요한 변수는 매출의 기대성장률인데, 지니언스의 과거 4년(2020년~2024년) 평균 매출액 성장률은 11.7%를 기록하며 동종업체 평균인 6.8%를 4.9%p 상회하는 높은 성장성을 입증했다. 특히 2026년부터 범부처 정보보호대책 강화와 개인정보보호법 개정 등 규제 환경이 변화하고, 정보보호 공시 의무 대상 확대 및 다층 보안체계(MLS) 도입 등이 예정되어 있어 향후 보안 산업 전반의 성장이 기대되고 있다. 이에 따라 NAC 시장에서 독보적인 위치를 점하고 있는 지니언스가 EDR과 ZTNA 분야로 사업 기회를 성공적으로 확장하며 시장 평균을 상회하는 성장을 지속할 것으로 기대되는바, 현재 동종업체 대비 부여받고 있는 높은 수준의 프리미엄은 당분간 정당화될 것으로 보인다.

보안 업체 과거 4년 매출액 성장률과 Trailing PSR(2024년 4분기~2025년 3분기)



자료: Quantiwise, 한국IR협의회 기업리서치센터

동종업체 valuation

	주가(원)	시가총액 (억 원)	매출액(억 원) '20	'21	'22	'23	'24	CAGR	P/S '24	3Q25 TTM
지니언스	18,920	1,718	268	319	385	429	496	11.7%	1.8	3.3
안랩	65,000	7,232	1,782	2,073	2,280	2,392	2,606	10.0%	2.6	2.7
윈스테크넷	11,380	1,397	939	964	1,014	1,069	1,015	2.0%	1.6	1.5
이글루	5,340	587	817	920	1,030	1,051	1,112	8.0%	0.5	0.5
라온시큐어	9,730	1,090	372	434	468	518	625	13.9%	1.9	1.7
파수	4,160	487	364	422	441	427	461	6.1%	1.2	1.0
모니터랩	3,955	487	107	121	141	142	149	8.6%	2.8	3.0
한싹	4,690	511	155	184	219	241	205	7.2%	2.0	2.3
지란지교시큐리티	2,910	247	582	573	322	353	341	-12.5%	0.8	0.7
시큐브	3,840	307	147	132	137	144	121	-4.8%	3.1	2.6
아톤	7,810	1,912	290	433	447	550	654	22.5%	2.0	2.7
SGA 솔루션즈	604	536	406	219	373	461	429	1.4%	0.7	0.8
신시웨이	8,450	315	73	79	97	105	118	12.9%	1.9	2.5
케이사인	10,150	717	353	373	432	471	519	10.1%	1.1	1.5
소프트캠프	1,438	359	189	206	190	185	169	-2.8%	1.4	1.7
엑스게이트	7,620	2,175	236	309	383	428	432	16.3%	6.9	4.6
휴네시온	3,930	378	254	265	304	361	369	9.8%	0.8	1.0
동종업체 평균								**6.8%**	**2.0**	**1.9**

자료: Quantiwise, 한국IR협의회 기업리서치센터, 주: 2026년 1월 26일 종가 기준, TTM: Trailing 12 months

리스크 요인

1 글로벌 벤더와의 본격 경쟁

다층보안체계(MLS) 도입은 그동안 국내 기업을 보호하던 망분리 장벽을 낮춰 글로벌 벤더와의 진검승부를 예고한다. 과거 물리적 망분리 정책은 클라우드 기반 기술을 보유한 마이크로소프트, 팔로알토 네트웍스, 크라우드스트라이크의 국내 진입을 막는 장벽이었다. 그러나 MLS는 글로벌 표준인 제로 트러스트와 클라우드 보안을 공공 시장의 주류로 만들고 있다.

핵심 리스크는 글로벌 벤더들의 '플랫폼 통합 공격'이다. 이들은 NAC, EDR, ZTNA, 방화벽, 클라우드 보안을 하나로 묶은 AI 보안 플랫폼을 제공하며, 고객사는 지니언스의 개별 솔루션보다 검증된 통합 플랫폼을 선택할 유인이 크다. 또한 규모의 경제를 통한 번들링과 공격적 가격 정책은 지니언스에게 기술 개발 비용 증가와 영업이익률 둔화 압박을 가할 수 있다.

방어 요소: 국내 시장 특수성

MLS 도입으로 글로벌 벤더의 진입 장벽이 낮아지는 것은 사실이나, 국내 보안 업체들이 쌓아온 독보적 강점과 시장 특수성은 여전히 강력한 경제적 해자로 작용할 전망이다. 가장 큰 이점은 국내 특유의 보안 인증 제도다. 공공기관 보안 제품은 국가용 보안요구사항 준수와 국정원 보안적합성 검증, KCMVP(국가암호모듈검증) 등 까다로운 인증이 필수다. 글로벌 벤더들은 한국만을 위한 별도 암호 모듈 탑재나 소스코드 검증 요구에 소극적인 반면, 지니언스를 포함한 국내 업체들은 규제 변화에 즉각 대응하며 국내 전용 인증을 선제 취득해 왔다. 이는 MLS 하에서도 강력한 '라이선스 장벽'으로 작동한다.

또한 국내 업체들은 글로벌 벤더가 흉내 낼 수 없는 밀착형 유지보수와 커스터마이징 능력을 보유하고 있다. 한국 공공기관의 IT 환경은 부처별로 복잡한 레거시 시스템이 얽혀 있어, 글로벌 기업은 본사 표준 가이드라인의 제약으로 과도한 커스터마이징이나 온사이트 긴급 대응에 한계가 있다. 반면 지니언스는 고객사 요구사항에 맞춘 유연한 기능 수정과 장애 발생 시 즉각적 현장 대응이 가능하며, MLS 도입 초기 전환 과정의 시행착오에서 풍부한 구축 경험과 소통 능력으로 기관 담당자들의 압도적 신뢰를 확보하고 있다.

국가 중요 데이터에 대한 '보안 주권' 문제 역시 국내 업체에 유리하게 작용한다. 국가 안보 직결 데이터 보안을 외산 솔루션에 전적으로 맡기는 것에 대한 정부 내 심리적·전략적 거부감이 존재하며, 국내 업체들은 한국 법령과 국정원 가이드라인을 가장 깊이 이해하고 제품에 반영한다. 지니언스는 NAC 시장 점유율 75%로 한국 공공기관 네트워크 생태계를 누구보다 잘 파악하고 있으며, 이러한 시장 지배력은 MLS 도입 이후에도 한국형 제로 트러스트 모델을 설계하고 제안하는 과정에서 글로벌 기업보다 유리한 고지를 점하게 하는 근거가 된다. 결국 MLS는 기술적으로는 글로벌 벤더에게 문을 열지만, 실질적 운영과 인증, 보안 거버넌스 측면에서 국내 업체의 홈그라운드 이점은 여전히 강력하다.

포괄손익계산서

(억원)	2022	2023	2024	2025F	2026F
매출액	385	429	496	520	601
증가율(%)	20.5	11.5	15.7	4.8	15.6
매출원가	158	171	186	203	229
매출원가율(%)	41.0	39.9	37.5	39.0	38.1
매출총이익	227	258	310	317	372
매출이익률(%)	58.9	60.1	62.5	61.0	61.9
판매관리비	157	193	211	242	257
판관비율(%)	40.8	45.0	42.5	46.5	42.8
EBITDA	75	71	106	85	125
EBITDA 이익률(%)	19.6	16.6	21.4	16.4	20.8
증가율(%)	13.4	-5.9	49.3	-19.4	46.4
영업이익	69	65	98	75	115
영업이익률(%)	18.0	15.1	19.8	14.4	19.1
증가율(%)	17.2	-6.5	52.2	-23.8	53.3
영업외손익	12	4	18	17	16
금융수익	12	15	14	15	17
금융비용	0	2	1	0	2
기타영업외손익	1	-8	4	2	1
종속/관계기업관련손익	-4	-4	-1	-1	-1
세전계속사업이익	78	65	115	90	129
증가율(%)	7.8	-16.4	75.8	-21.2	42.9
법인세비용	7	3	6	5	7
계속사업이익	71	62	109	86	122
중단사업이익	0	0	0	0	0
당기순이익	71	62	109	86	122
당기순이익률(%)	18.6	14.6	22.0	16.5	20.4
증가율(%)	15.8	-12.6	74.6	-21.3	42.6
지배주주지분 순이익	71	62	109	86	122

재무상태표

(억원)	2022	2023	2024	2025F	2026F
유동자산	475	463	512	584	709
현금성자산	53	42	76	127	181
단기투자자산	291	273	289	302	350
매출채권	80	84	101	106	122
재고자산	40	47	35	37	42
기타유동자산	11	17	12	12	14
비유동자산	122	173	181	179	175
유형자산	53	54	54	53	45
무형자산	31	34	48	46	44
투자자산	34	78	67	68	74
기타비유동자산	4	7	12	12	12
자산총계	597	636	693	763	884
유동부채	108	125	96	101	116
단기차입금	0	0	0	0	0
매입채무	41	47	29	30	35
기타유동부채	67	78	67	71	81
비유동부채	10	6	29	30	35
사채	0	0	0	0	0
장기차입금	0	0	0	0	0
기타비유동부채	10	6	29	30	35
부채총계	118	131	125	131	151
지배주주지분	479	505	568	632	733
자본금	47	47	47	47	47
자본잉여금	133	133	133	133	133
자본조정 등	-63	-86	-54	-54	-54
기타포괄이익누계액	0	-3	-24	-24	-24
이익잉여금	362	414	466	530	631
자본총계	479	505	568	632	733

현금흐름표

(억원)	2022	2023	2024	2025F	2026F
영업활동으로인한현금흐름	94	67	98	91	126
당기순이익	71	62	109	86	122
유형자산 상각비	5	5	6	8	8
무형자산 상각비	2	1	2	2	2
외환손익	0	0	0	0	0
운전자본의감소(증가)	5	-23	-28	-1	-4
기타	11	22	9	-4	-2
투자활동으로인한현금흐름	-71	-38	-50	-20	-51
투자자산의 감소(증가)	-2	-49	-10	-0	-4
유형자산의 감소	0	0	0	0	0
유형자산의 증가(CAPEX)	-2	-2	-2	-7	0
기타	-67	13	-38	-13	-47
재무활동으로인한현금흐름	-12	-41	-14	-21	-21
차입금의 증가(감소)	0	0	-6	0	0
사채의증가(감소)	0	0	12	0	0
자본의 증가	0	0	0	0	0
배당금	-11	-13	-17	-22	-22
기타	-1	-28	-3	1	1
기타현금흐름	-0	-0	1	2	1
현금의증가(감소)	11	-12	35	51	54
기초현금	43	53	42	76	127
기말현금	53	42	76	127	181

주요투자지표

	2022	2023	2024	2025F	2026F
P/E(배)	10.9	19.1	8.0	19.7	13.8
P/B(배)	1.6	2.4	1.5	2.7	2.3
P/S(배)	2.0	2.8	1.8	3.3	2.8
EV/EBITDA(배)	5.8	12.4	4.6	14.8	9.3
배당수익률(%)	1.8	1.6	2.7	1.3	1.3
EPS(원)	757	661	1,165	945	1,348
BPS(원)	5,072	5,348	6,254	6,961	8,071
SPS(원)	4,071	4,541	5,296	5,727	6,619
DPS(원)	150	200	250	250	250
수익성(%)					
ROE	16.1	12.7	20.3	14.3	17.9
ROA	12.7	10.1	16.4	11.8	14.9
ROIC	61.1	53.2	65.0	45.3	69.6
안정성(%)					
유동비율	438.0	370.5	533.1	580.0	609.4
부채비율	24.6	26.0	22.0	20.7	20.6
순차입금비율	-71.4	-61.5	-63.4	-67.2	-71.7
이자보상배율	1,107.8	417.0	191.3	503.9	727.8
활동성(%)					
총자산회전율	0.7	0.7	0.7	0.7	0.7
매출채권회전율	4.2	5.2	5.4	5.0	5.3
재고자산회전율	12.0	9.9	12.0	14.5	15.2

최근 3개월간 한국거래소 시장경보제도 지정 여부

시장경보제도란?

한국거래소 시장감시위원회는 투기적이거나 불공정거래 개연성이 있는 종목 또는 주가가 비정상적으로 급등한 종목에 대해 투자자주의 환기 등을 통해 불공정거래를 사전에 예방하기 위한 제도를 시행하고 있습니다. 시장경보제도는 '투자주의종목 투자경고종목 투자위험종목'의 단계를 거쳐 이루어지게 됩니다.

※관련근거: 시장감시규정 제5조의2, 제5조의3 및 시장감시규정 시행세칙 제3조~제3조의 7

종목명	투자주의종목	투자경고종목	투자위험종목
지니언스	X	X	X

발간 History

발간일	제목
2026.01.27	지니언스-사이버 보안 솔루션 NAC, EDR 1위 기업
2025.01.02	지니언스-국내 보안시장 압도적 1등을 넘어 중동, 북미 성과 가시화
2023.09.08	지니언스-제로트러스트 시대 돋보일 NAC, EDR 독보적 1위 업체
2022.07.28	지니언스-보안 솔루션 시장의 강자

Compliance notice

본 보고서는 한국거래소, 한국예탁결제원과 한국증권금융이 공동으로 출연한 한국IR협의회 산하 독립 (리서치) 조직인 기업리서치센터가 작성한 기업분석 보고서입니다. 본 자료는 투자자들에게 국내 상장기업에 대한 양질의 투자정보 제공 및 건전한 투자문화 정착을 위해 무상으로 작성되었습니다.

- 당사 리서치센터는 본 자료를 제3자에게 사전 제공한 사실이 없습니다.
- 본 자료를 작성한 애널리스트는 자료작성일 현재 해당 종목과 재산적 이해관계가 없습니다.
- 본 자료를 작성한 애널리스트와 그 배우자 등 관계자는 자료 작성일 현재 조사분석 대상법인의 금융투자상품 및 권리를 보유하고 있지 않습니다.
- 본 자료는 중소형 기업 소개를 위해 작성되었으며, 매수 및 매도 추천 의견은 포함하고 있지 않습니다.
- 본 자료에 게재된 내용은 애널리스트의 의견을 정확하게 반영하고 있으며, 외부의 부당한 압력이나 간섭 없이 신의 성실하게 작성되었음을 확인합니다.
- 본 자료는 투자자들의 투자판단에 참고가 되는 정보제공을 목적으로 배포되는 자료입니다. 본 자료에 수록된 내용은 자료제공일 현재 시점의 당사 리서치센터의 추정치로서 오차가 발생할 수 있으며 정확성이나 완벽성은 보장하지 않습니다.
- 본 조사자료는 투자 참고 자료로만 활용하시기 바라며, 어떠한 경우에도 투자자의 투자 결과에 대한 법적 책임 소재의 증빙자료로 사용될 수 없습니다.
- 본 조사자료의 지적재산권은 당사에 있으므로, 당사의 허락 없이 무단 복제 및 배포할 수 없습니다.
- 본 자료는 텔레그램에서 "한국IR협의회(https://t.me/kirsofficial)" 채널을 추가하시어 보고서 발간 소식을 안내받으실 수 있습니다.
- 한국IR협의회가 운영하는 유튜브 채널 'IRTV'에서 1) 애널리스트가 직접 취재한 기업탐방으로 CEO인터뷰 등이 있는 '小中한탐방'과 2) 기업보고서 심층해설방송인 '小中한 리포트 가치보기'를 보실 수 있습니다.