기업 밸류업 공시법인
KRX KOREA EXCHANGE
CORPORATE VALUE-UP

KOSDAQ | 소프트웨어와서비스

파수AI (150900)

국내 매출 1위의 문서 보안 전문 기업

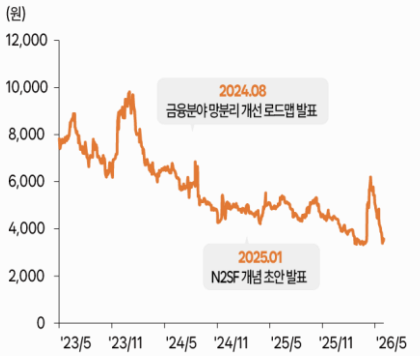
기업가치 제고 계획 및 이행상황

- 2025년 6월에 발표된 기업가치 제고에 따르면 2030년까지 연평균 매출성장률 20%, 영업이익률 25%, 주주환원율 30%
- 기업가치 제고 계획 이행 상황: 2025년 매출성장률 1.2%, 영업이익률 5.4%, 주주환원율 42.5%로 주주환원율을 제외하고는 목표치와 괴리가 큰 편
- 목표 달성의 핵심은 미국 시장의 성공적인 진입 및 국내 매출 다각화
  미국 법인 Fasoo는 미국 현지 AI 플랫폼, 컨설팅 업체 컨실릭스와 합병해 "심볼로직(Symbologic)"으로 신규 출범
  국내 보안 시장에서는 기업용 AI, DSPM 등 신규 솔루션에서의 실질적인 매출 기여가 필수적

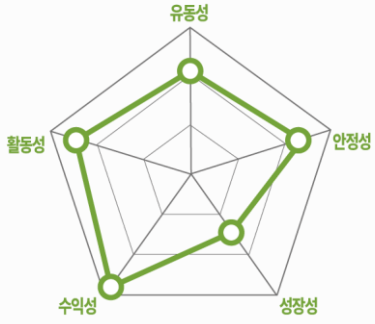
체크포인트

- 국내 문서 보안 솔루션(DRM) 기업 중 매출 1위
- 세계적으로 제로 트러스트 아키텍처 도입 흐름 속에 국내에는 N2SF, 금융권 망분리 완화 정책이 도입되며 데이터 보안에 대한 중요성 강화
- 데이터 보안의 첫 단추인 식별 및 분류를 해결하는 솔루션에 대한 수요가 확대되며 파수AI의 매출은 전년대비 5.4% 증가한 492억 원 기대

주가 및 주요이벤트

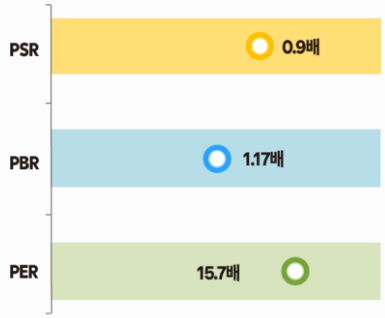


재무지표



주: 2025년 기준, Fnguide WICS 분류 상 IT산업 내 등급화

밸류에이션 지표



주: PSR, PER은 2025년 기준, PBR은 1Q26 기준, Fnguide WICS 분류상 IT산업 내 순위 비교, 우측으로 갈수록 저평가

파수AI (150900)

KOSDAQ
소프트웨어와서비스

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

국내 DRM 업체 중 매출 1위

2000년에 설립되어 국내 최초로 DRM(Digital Right Management) 기술을 상용화. 2025년 기준 매출 비중은 데이터 보안 44%, 애플리케이션 보안 18%, 정보보호컨설팅 3%, 유지관리 35%

다층보안체계가 재점화하는 데이터 보안 모멘텀

정부의 다층보안체계 도입에 발맞추어, 콘텐츠 보안 시장의 수요는 미분류 데이터의 식별·자동 라벨링 단계에서 외부 유출 후 원격 제어 및 맥락 기반 접근제어 솔루션으로 확장될 전망. 이에 따라 파수AI의 데이터 식별·분류 솔루션(FDR)과 사용자 행동 기반 리스크 관리 솔루션(FRV)의 확산이 예상됨

동트기 전의 주가

N2SF 도입 및 금융권 망분리 완화 등 새로운 보안 정책과 세부 가이드라인이 잇따라 발표됨에 따라, 현재 국내 정보보안 산업은 구조적 변화의 초입에 있음. 데이터 보안에 대한 중요도가 상승하며 파수AI의 사업기회가 확대되고 있음에도 주가는 PBR Band 하단에 머무름

Forecast earnings & Valuation

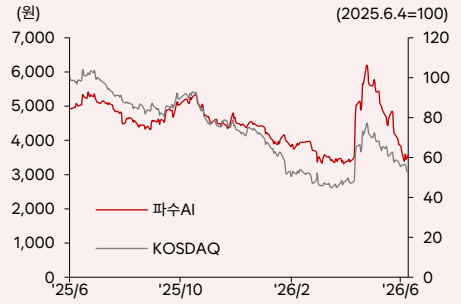
	2022	2023	2024	2025	2026F
매출액(억원)	441	427	461	467	492
YoY(%)	4.6	-3.3	8.1	1.2	5.4
영업이익(억원)	52	38	39	25	31
OP 마진(%)	11.8	8.9	8.5	5.4	6.3
지배주주순이익(억원)	52	44	45	27	31
EPS(원)	448	377	384	228	261
YoY(%)	18.1	-15.8	1.9	-40.8	14.6
PER(배)	20.3	25.2	12.7	19.4	13.7
PSR(배)	2.4	2.6	1.2	1.1	0.9
EV/EBITDA(배)	9.2	11.6	6.3	6.5	4.1
PBR(배)	3.3	3.2	1.6	1.4	1.1
ROE(%)	18.0	13.2	12.7	7.2	8.0
배당수익률(%)	1.1	1.1	2.0	2.3	2.8

자료: 한국IR협의회 기업리서치센터

Company Data

현재주가 (6/15)		3,655원
52주 최고가		6,200원
52주 최저가		3,315원
KOSDAQ (6/15)		1,034.03p
자본금		59억원
시가총액		428억원
액면가		500원
발행주식수		12백만주
일평균 거래량 (60일)		133만주
일평균 거래액 (60일)		76억원
외국인지분율		9.12%
주요주주	조규곤 외 5 인	19.50%

Price & Relative Performance



Stock Data

주가수익률(%)	1개월	6개월	12개월
절대주가	-25.1	-16.7	-27.0
상대주가	-18.2	-24.4	-45.8

▶**참고** 1) 표지 재무지표에서 안정성 지표는 '이자보상배율', 성장성 지표는 '매출액 증가율', 수익성 지표는 '매출총이익률', 활동성지표는 '순운전자본회전율,' 유동성지표는 '당좌비율'임. 2) 표지 밸류에이션 지표 차트는 해당 산업군 내 동사의 상대적 밸류에이션 수준을 표시. 우측으로 갈수록 밸류에이션 매력도 높음.

▶**기업 밸류업 공시 법인** 주주가치 존중 기업문화로의 변화를 위해 자발적으로 기업가치 제고 노력을 하는 기업. 기업가치 제고 계획을 자율적으로 수립하고, 이행하며 투자자와 소통하는 기업

기업 개요

1 연혁

DRM 기업

DRM 기술 상용화와 시장 기반 구축 (2000년~2006년)

파수AI의 출발은 2000년 6월 조규곤 대표가 세계 최초로 DRM(Digital Rights Management) 기술을 상용화하면서 시작되었다. DRM은 파일 자체에 암호화를 내장하여 문서·도면·이미지가 어디로 이동하든 설정된 접근 제어가 유지되는 방식이다.

2000년대 초반 국내 기업들 사이에서 DRM 솔루션 수요가 증가했다. 파수AI는 2004년 CAD 도면 보안 제품을 추가로 출시하여 제조업 시장으로 확대했다. 삼성·포스코·CJ·롯데 등 주요 대기업이 파수AI의 DRM을 채택했고, 중앙부처와 공공기관 납품 실적도 쌓였다. 기존 암호화 파일과의 호환 문제로 인해 후발 진입자들의 경쟁력이 제한되었고, 국내 DRM 시장은 파수AI·소프트캠프·마크애니 3사 구도로 형성되었다.

사업 포트폴리오 다양화와 상장 (2007년~2023년)

2013년 10월 코스닥 상장을 기점으로 파수AI는 사업 영역을 본격적으로 확대했다.

2007년 애플리케이션 보안 분야에 진출했다. 이후 2018년 5월 스패로우로 물적분할하여 별도 법인화했다. SAST(정적 분석)·DAST(동적 분석)·SCA(오픈소스 관리)를 포함한 DevSecOps 솔루션을 독립적으로 운영하기 위한 구조였다.

글로벌 사업으로는 2012년 설립한 미국 메릴랜드의 Fasoo, Inc.를 중심으로 GE·TRW 등 글로벌 제조기업에 CAD 도면 보안 솔루션을 공급했다. Mac OS와 CAD 파일 형식 지원으로 기존 외산 업체들과 차별화되었다.

2017년에는 데이터 관리 플랫폼 랩소디(Wrapsody)를 출시했다. Wrapsody는 기업의 문서, 파일, 데이터를 일관되게 관리하고 보호하는 솔루션으로, DRM과 함께 데이터 거버넌스 영역을 확대하는 상품이었다. 2023년에는 클라우드 환경에 최적화된 Wrapsody Drive를 추가로 출시했다.

AI 기반 솔루션 포트폴리오 확대 (2024년~현재)

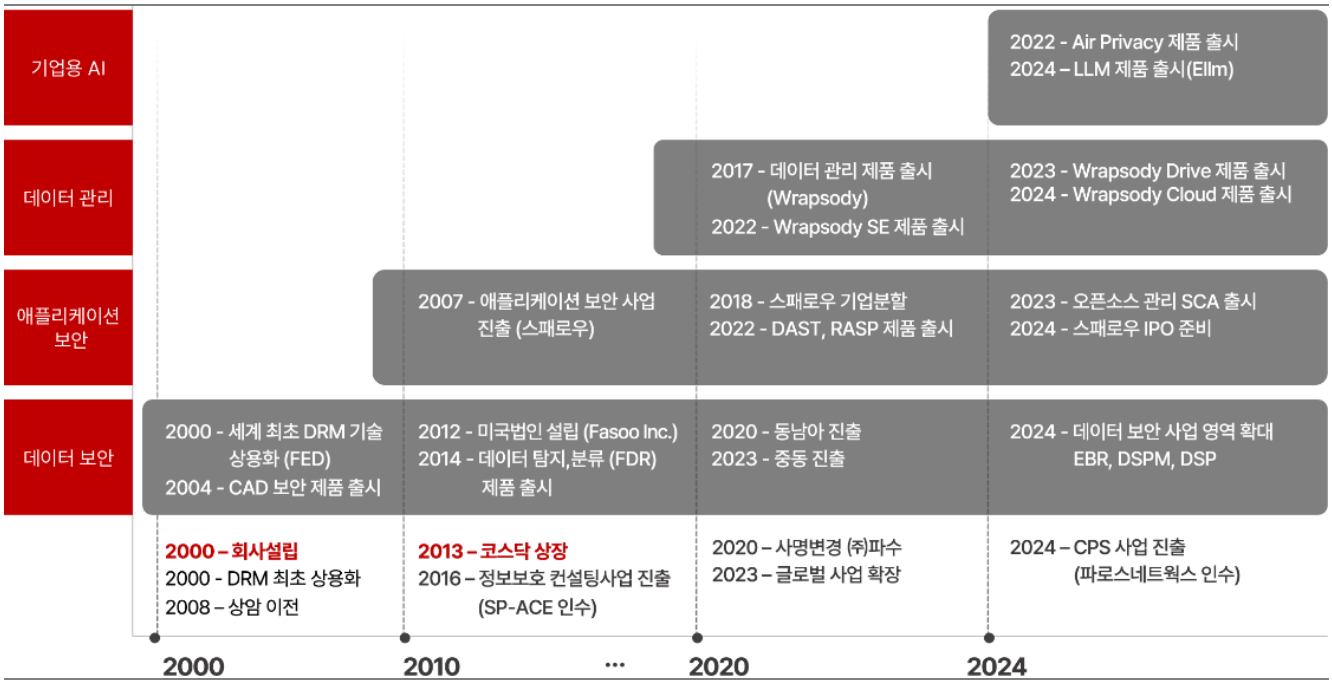
2024년 파수AI는 Wrapsody Cloud를 통해 클라우드 기반 데이터 관리 기능을 강화하는 한편, 3월에는 기업형 소규모 언어모델(sLLM) 솔루션 일름(Ellm)을 출시했다. Ellm은 온프레미스(자체 서버) 구축형으로 설계되어 외부 데이터 전송 없이 기업 내부 데이터만 사용하여 작동한다. 이는 기업들이 외부 AI 서비스의 정보 보안 위험을 우려할 때 내부 AI 인프라 수요에 대응하는 솔루션이다.

같은 해 파로스네트웍스(OT·ICS 보안 전문)의 CPS(Cyber-Physical System) 사업부문을 영업양수도 방식으로 인수했다. 이를 통해 데이터 보안 역량을 산업용 환경까지 확대했다.

2025년에는 DSPM(데이터 보안 상태 관리) 제품을 출시했다. DSPM은 클라우드 환경에서 데이터의 위치, 접근 권한, 보안 상태를 파악하는 시스템이다. 동시에 Fasoo DSP Cloud를 통해 클라우드 기반 데이터 보안 플랫폼 기능을 강화했다.

2026년 3월 정기주주총회에서 회사는 사명을 파수에서 파수AI로 변경했다.

파수AI 연혁



자료: 파수AI, 한국IR협의회 기업리서치센터

2 기업 개요

매출 비중(2025년)

데이터 보안 44%

애플리케이션 보안 18%

정보보호컨설팅 3%

유지관리 35%

파수AI의 매출은 데이터 보안, 애플리케이션 보안, 정보보호컨설팅, 유지관리로 구분된다. 2025년 연간 기준 각 비중은 44%, 18%, 3%, 35%다.

데이터 보안(2025년 매출 비중 44%)

파수AI의 데이터 보안 사업은 세 가지 핵심 솔루션으로 구성된다.

Fasoo Enterprise DRM(FED)은 비정형 데이터가 생성되는 순간 자동으로 암호화를 적용하고, 파일이 이동하거나 외부로 전송되어도 설정된 접근 제어가 유지되도록 한다. 조직 내부자라도 권한이 없으면 파일을 열람할 수 없다는 점에서 네트워크 차단 방식 보안과 근본적으로 다르다. PC, 서버, 모바일, 외부 협업 환경 등 다양한 사용 환경에 대응하며, 출력·화면 캡처·메일 전송 등 각 채널별 보안 정책을 적용할 수 있다. 클라우드 환경으로의 확대에 따라 온프레미스와 클라우드 경계에서의 보안 공백을 메우는 Fasoo DSP Cloud 등이 추가되었다. 글로벌 시장에서는 CAD 도면 보안과 Mac OS 지원이 차별화 포인트로, GE 등 글로벌 제조기업에 연간 리뉴얼 계약이 있다.

데이터 거버넌스 플랫폼 랩소디(Wrapsody)는 기업의 문서, 파일, 데이터를 일관되게 관리하고 보호하는 통합 플랫폼이다. 데이터의 탐지·분류·암호화·모니터링을 포괄하는 데이터 보안 전체 주기를 지원한다. 2023년 클라우드 환경 최적화 제품인 Wrapsody Drive, 2024년 Wrapsody Cloud를 추가하며 클라우드 기반 데이터 관리 기능을 강화했다.

데이터 보안에서 강점을 바탕으로 AI 산업으로 확장을 시도하고 있다. 기업형 소규모 언어모델(sLLM) 엘름(EIlm)은 외부 데이터 전송 없이 기업 내부 데이터만으로 작동한다. 2025년 11월 GS인증을 취득하여 공공기관 납품 자격을 확보했다. 기업이 인공지능 기술을 도입하고 운영할 때, 안정성, 윤리성, 법적 규제 준수, 그리고 투명성을 확보하기 위해 갖추어야 하는 AI 거버넌스 인프라 솔루션도 공급하고 있다.

애플리케이션 보안(2025년 매출 비중 18%)

자회사 스패로우는 '소프트웨어 보안(DevSecOps)' 사업을 담당하고 있다. 과거에는 보안이 개발 후반부에나 고려되었지만, 최근에는 개발 초기 단계부터 보안을 통합해 제품을 만드는 전 과정에서 취약점을 상시 관리하는 방식으로 패러다임이 바뀌고 있으며 스패로우가 바로 이 영역을 담당하고 있다.

소스 코드 점검(정적 분석)부터 실제 실행 중인 프로그램의 해킹 취약점 진단(동적 분석·자기방어), 외부 오픈소스 소프트웨어의 안전성 검사까지 보안의 전 과정을 하나의 통합 플랫폼(스패로우 엔터프라이즈)으로 제공한다.

그동안 정부·공공기관의 의무 보안 시스템 구축(시큐어코딩)과 금융권의 취약점 진단 수요를 바탕으로 안정적인 성장 기반을 다져왔다.

정보보호 컨설팅(2025년 매출 비중 3%)

법정 의무 수요에 기반한 안정적 매출원이다. ISO27001·ISMS 인증심사, 주요정보통신기반시설 취약점 분석평가, 모의해킹·개인정보보호 컨설팅 등으로 구성된다.

유지관리(2025년 매출 비중 35%)

납품했던 보안 솔루션에 대한 유지 보수 매출이다. 특히 EDRM은 타 소프트웨어 대비 OS 및 문서 어플리케이션 업그레이드, 쏟아지는 악성코드와 타 보안 솔루션들과의 충돌 및 호환 이슈, PC 교체 등의 문제로 도입 후 유지 관리가 필수인 소프트웨어이다. 따라서 유상유지관리 계약율이 90%를 상회하며, 평균 요율이 14% 수준이다. 기존에 구축된 고객사가 늘어날수록 유지관리 매출이 누적으로 증가하는 구조이다.

주요 사업내용

데이터 보안	데이터 관리	기업용 AI	애플리케이션 보안
사이버 해킹, 내부자에 의한 위협 등 중요 정보 유출에 대해 개인이 보유한 정보로부터 기업의 중요 정보 파일까지 모든 콘텐츠에 대한 가장 완벽하고 효율적인 데이터 보안 방안 제공 ▪ 데이터 탐지, 암호화, 정책 최적화, 리스크 관리 등 모든 위협에 대응하는 다중 레이어 방식 ▪ 세계 최초 DRM 상용화로 25년 이상 축적된 DRM기술력, 고객요구 기반 세밀한 권한 정책 설정 가능, 공공기관, 금융, 대기업 포함 1,500개 고객사 이상 보유 Fasoo Enterprise DRM Fasoo DSPM Fasoo Data Radar Fasoo RiskView	**기업내 문서관리, 보안 문제를 해결하여 업무 생산성을 극대화하고, 생성형 AI 활용을 위한 최적의 데이터 관리 환경을 제공합니다. 또한 외부와의 협업 시 업무 효율과 보안기능 제공** ▪ 문서 가상화 기술 기반의 콘텐츠 관리 플랫폼으로 사용 이력, 연관 관계, 유통 경로 파악 ▪ 생성형 AI LLM 구축을 위한 기업 내 ROT, 데이터 관리 Wrapsody Wrapsody eCo	**기업이 생성형 AI 도입을 통해 업무 효율을 높일 수 있도록 산업특성에 특화된 LLM 구축, AI 사용으로 인한 정보유출 방지, AI기반의 개인정보 보안까지 통합 솔루션 제공** ▪ RAG 기술을 적용으로 환각 현상 최소화, 복수의 LLM 연결로 최적의 답변 AI 기반 개인정보 검출 및 마스킹 처리 ▪ 생성형 AI 사용시 민감정보 차단 및 데이터 정보 유출 방지 AI Radar DLP AI Radar Privacy ellm	**소스코드 구문 분석만으로 프로그램 실행 시 발생하는 보안취약점과 결함을 정확히 검출하는 대한민국 1위 정적분석도구로 고품질의 애플리케이션 개발 환경 제공** ▪ 정적분석(SAST), 동적분석(DAST), 자가방어(RASP), 오픈소스 관리(SCA) 등 통합 플랫폼 제공, 애플리케이션 시큐어코딩과 품질 모두 만족 Sparrow SAST Sparrow DAST Sparrow RASP Sparrow SCA

자료: 파수AI, 한국IR협의회 기업리서치센터

3 주요 종속회사

2026년 1분기 기준 연결 대상 종속회사는 2개사다.

국내에는 스패로우가 있다. 2018년 5월 파수에이아이의 애플리케이션 보안 사업부를 단순·물적분할 방식으로 독립시킨 법인으로, 파수AI가 89%를 보유하고 있다.

해외에는 미국 법인 Fasoo가 있다. 2012년 메릴랜드주에 설립한 100% 자회사로, 북미·중동·동남아 글로벌 영업과 데이터 관리 플랫폼 현지 사업을 담당해 왔다. Fasoo는 지난 6월 1일, 미국 현지 AI 플랫폼, 컨설팅 업체 컨실릭스(Konsilix)와 합병해 '심볼로직(Symbologic)'으로 신규 출범했다. 신규 법인은 파수의 데이터 관리·보안 역량과 AI 포트폴리오에 컨실릭스의 AI 컨설팅·서비스를 더해 AX 실현에 필요한 서비스를 지원할 계획이다. 아직 구체적인 지분 구조 등은 공시되지 않은 상황이다.
글로벌 제조기업 레퍼런스를 기반으로 2025년에는 19억 원의 매출이 발생했다.

종속회사 현황(1Q26 기준) (단위: 억 원)

회사명	지분율	지역	자산	부채	자본	당분기매출	당분기순이익(손실)
FASOO, INC.	100%	미국	12	2	9	1	-7
스패로우	89%	한국	59	12	47	16	-6

자료: 파수AI, 한국IR협의회 기업리서치센터

종속회사 현황(2025년 기준) (단위: 억 원)

회사명	지분율	지역	자산	부채	자본	매출	당분기순이익(손실)
FASOO, INC.	100%	미국	16	7	8	19	-21
스패로우	89%	한국	71	18	53	105	5

자료: 파수AI, 한국IR협의회 기업리서치센터

산업 현황

1 국내 보안 산업 진단

정보 보안 산업을 이해하기 위한 두 가지 키워드: 규제, 심층 방어 구조

국내 정보 보안 산업을 이해하려면 두 가지 축을 함께 봐야 한다. 하나는 누가 무엇을 강제하는가, 즉 법적 규제 체계다. 다른 하나는 그 요구를 기술적으로 어떻게 구현하는가, 즉 심층 방어 구조다. 전자가 수요의 구조를 결정하고, 후자가 공급의 형태를 규정한다. 두 축이 맞물리는 지점에서 보안 담당자의 실제 의사결정이 이루어진다.

정보 보안은 사업 주체에 따라 다르게 적용

정보 보안의 법적 규제 체계

보안 솔루션 공급자가 국내 공공 및 금융 조달 시장에 진입하기 위해서는 법적 인증과 기술 평가라는 구체적인 허들을 넘어야 한다. 이는 기업들에게 초기 투자 비용이자 동시에 시장 진입 장벽으로 작용한다. 규제 주체에 따라 요구되는 인증의 종류와 수준이 엄격하게 차등 적용되기 때문이다. 국내 정보보안 규제 체계는 개인정보 보호법 중심의 일반법과 산업별 특별법 구조로 구성되며, 사업 주체가 속한 산업군에 따라 적용 법령과 소관 부처가 달라진다. 크게 네 가지 주체별 영역으로 구분된다.

1)공공기관 및 국가 지자체

국가기관, 지방자치단체, 공공기관 및 교육기관 등은 일반 기업보다 엄격한 기준과 상위 기관의 통제를 받는다. 이들은 주로 전자정부법, 사이버안보 업무규정, 개인정보 보호법의 적용을 받으며 소관 부처는 행정안전부, 국가정보원, 개인정보보호위원회다. 기본적으로 대국민 서비스를 제공하는 모든 시스템은 행정안전부의 가이드를 준수하여 구축·운영해야 한다. 여기에 공공 전산망과 국가 중요 정보시스템은 구조적으로 국가정보원의 지침과 강력한 보안성 검토 감독을 받게 되어 있다. 특히 공공기관이 도입하는 모든 하드웨어 및 소프트웨어 보안 제품은 국정원이 검증하는 국가용 보안요구사항(CC인증[1] 등)을 충족해야만 조달 및 도입이 가능하다. 최근 가속화되는 공공 클라우드 도입 가상 환경 역시 클라우드컴퓨팅법에 의거하여 일원화된 '국정원 클라우드 보안검증 체계'를 통과한 솔루션만을 채택하도록 강제된다.

2)일반 기업 및 온라인 서비스 사업자

영리 목적으로 웹사이트를 운영하거나 온·오프라인에서 고객 데이터를 다루는 모든 기업이 이 주체에 해당하며, 국내 보안 시장에서 가장 광범위한 영역을 포괄한다. 핵심 법령은 개인정보 보호법과 정보통신망 이용촉진 및 정보보호 등에 관한 법률(정보통신망법)이며, 개인정보보호위원회와 과학기술정보통신부가 주로 감독한다. 개인정보 보호법은 온·오프라인을 불문하고 모든 개인정보 처리자에게 기술적·관리적·물리적 보호조치 의무를 부여하는 최상위 일반법 역할을 한다. 반면 정보통신망법은 인터넷 쇼핑몰, 포털, IT 서비스 기업 등 '정보통신서비스 제공자'에게 교차 적용되는 특별법 성격을 띤다. 이 정보통신망법의 기준에 따라 일정 규모 이상의 민간 기업은 정보보호 최고책임자(CISO, Chief Information Security Officer)를 반드시 지정하여 정부에 신고해야 하며, 전사적 보안 체계의 무결성을 증명하는 정보보호 관리체계(ISMS/ISMS-P) 인증을 의무적으로 획득하여 유지해야 한다.

3)금융회사 및 핀테크 기업

[1] CC(Common Criteria)인증: 정보보호제품에 구현된 보안기능이 평가보증등급 수준에 부합하는지 검증하여 일정 수준의 보안성을 갖춘 정보보호제품에 인증을 부여하는 제도

자산과 신용 정보를 직접 다루는 금융 영역은 보안 사고 발생 시 사회·경제적 피해 규모가 막대하므로, 국내 법령 중 가장 구체적이고 타이트한 규제를 양산한다. 주된 법령은 전자금융거래법과 신용정보의 이용 및 보호에 관한 법률(신용정보법)이며, 금융위원회와 금융감독원의 철저한 밀착 통제를 받는다. 전자금융거래법은 전통적인 금융사뿐만 아니라 토스, 카카오페이 같은 전자금융업자(핀테크 스타트업)에게도 예외 없이 적용된다. 특히 하위 규정인 전자금융감독규정에 명시된 '물리적 망분리 의무'는 외부 인터넷망과 업무용 내부 전산망을 완벽히 단절하도록 강제하며, 이 외에도 전산실 출입통제와 백업센터 구축 등 고도의 기술적 수단을 요구한다. 또한 신용정보법은 금융 소비자의 '개인신용정보'를 다룰 때 발동되는데, 일반 개인정보보다 수집, 이용, 파기 기준이 훨씬 까다로워 금융권 내부 보안 아키텍처를 규정하는 가장 핵심적인 법적 근거가 된다.

4)국가 핵심기술 보유 기업 및 주요 정보통신기반시설

국가 안보나 국민 경제에 치명적인 타격을 입힐 수 있는 인프라(발전소, 교통 통제소, 대형 병원 등)를 운영하거나 세계 시장을 선도하는 첨단 기술을 보유한 주체들이다. 이들은 정보통신기반 보호법과 산업기술의 유출방지 및 보호에 관한 법률(산업기술보호법)의 지배를 받으며, 과학기술정보통신부와 산업통상자원부, 국정원 등 관계 중앙행정기관들이 다각도로 관할한다. 정부가 지정한 주요정보통신기반시설의 관리기관은 매년 전산 시스템 전반에 대한 취약점 분석·평가를 수행하고, 이를 바탕으로 상세한 보호계획을 수립하여 소관 부처에 의무 제출해야 한다. 이와 결을 같이하여 반도체, 디스플레이, 이차전지 등 국가 핵심기술을 보유한 제조 및 연구 기업들 역시 산업기술보호법에 따라 사내 연구망 분리, 핵심 도면 및 소스코드에 대한 접근 통제, 핵심 인력의 이직 관리 등 기술 유출을 막기 위한 강력한 독자 보안 시스템을 의무적으로 가동해야 한다.

이처럼 규제 주체에 따라 요구되는 보안 수준은 뚜렷하게 차등화된다. 일반 기업은 ISMS 인증과 기술적 보호조치 의무를 기본선으로 삼는 반면, 금융회사는 물리적 망분리와 전산실 접근통제 등 훨씬 구체적인 기술 요건을 준수해야 한다. 공공기관은 CC인증을 충족한 제품만 조달할 수 있고, 주요정보통신기반시설 운영자는 연간 취약점 평가와 보호계획 제출까지 의무화된다. 결국 보안 솔루션 공급자는 동일한 제품이라도 납품 대상 주체에 따라 충족해야 할 인증과 기술 사양이 달라지는 구조에 놓인다. 이처럼 규제 주체별로 요구되는 보안 수준이 세분화될수록, 이를 충족하기 위한 기술 솔루션의 구조도 단층이 아닌 다층으로 고도화된다.

주체에 따른 사이버 보안 체계

분류	대상 기관 및 주체	소관 및 감독 부처	핵심 적용 법령	주요 의무 및 규제 핵심 사항
공공기관 및 지자체	국가기관, 지방자치단체, 공공기관, 교육기관 등	행정안전부, 국가정보원, 개인정보보호위원회	전자정부법, 개인정보 보호법, 사이버안보 업무규정	행정안전부 구축·운영 가이드 준수 국정원의 지침 및 보안성 검토 감독 수령 국가용 보안요구사항(CC 인증 등) 충족 제품만 도입 가능 국정원 클라우드 보안검증 체계 통과 솔루션 채택 필수
일반 기업 및 온라인 서비스	웹사이트 운영사, 온·오프라인 고객 데이터 처리 기업 전체	개인정보보호위원회, 과학기술정보통신부	개인정보 보호법, 정보통신망법	기술적·관리적·물리적 보호조치 의무 (최상위 일반법) 일정 규모 이상 기업의 정보보호 최고책임자(CISO) 지정 및 신고 정보보호 관리체계(ISMS/ISMS-P) 의무 인증 및 유지
금융회사 및 핀테크 기업	전통 금융사, 전자금융업자(토스, 카카오페이 등 핀테크 스타트업)	금융위원회, 금융감독원	전자금융거래법, 신용정보법	물리적 망분리 의무화 (외부 인터넷망과 내부 전산망 단절) 전산실 출입통제 및 백업센터 구축 의무 개인신용정보의 엄격한 수집·이용·파기 기준 준수
국가 핵심기술 및 기반시설	발전소·교통·병원 등 인프라 운영 기관, 반도체·배터리 등 첨단기술 보유 제조·연구 기업	과학기술정보통신부, 산업통상자원부, 국가정보원 등	정보통신기반 보호법, 산업기술보호법	기반시설: 매년 전산 시스템 취약점 분석·평가 및 보호계획 제출 기술 보유 기업: 사내 연구망 분리, 핵심 도면/소스코드 접근 통제, 핵심 인력 이직 관리

자료: 한국IR협의회 기업리서치센터

심층적 구조

하나의 솔루션으로는 막을 수 없다

정보 보안의 심층적 구조

정보 보안은 다층적 구조를 띤다. 현대의 디지털 환경에서는 단일 방어벽으로 안전을 보장할 수 없기 때문이다. 과거에는 네트워크 경계 보안이나 PC 백신 정도가 보안의 전부로 여겨졌다. 그러나 클라우드 컴퓨팅, 모바일 기기, 사물인터넷(IoT)의 확산으로 방어해야 할 자산과 공격 표면이 급격히 확대됐다. 데이터는 이제 물리적 서버를 넘어 전 세계 수많은 가상 환경과 기기를 오가며 유통된다. 이 과정에서 공격자들은 시스템의 가장 취약한 지점을 집중적으로 파고든다.

이에 따라 현대 정보 보안은 임의의 방어막이 뚫리더라도 후속 레이어가 위협을 차단할 수 있도록 심층 방어(Defense in Depth) 구조를 기본 원칙으로 삼는다. 이를 뒷받침하는 보안 솔루션 분류 체계는 외곽에서 핵심 자산으로 수렴하는 일곱 가지 레이어로 구성된다.

첫째, 경계 보안(Perimeter Security)은 외부 인터넷망과 내부 업무망의 경계에서 외부 위협을 1차로 차단하는 영역이다. Secure DMZ를 통해 신뢰할 수 없는 외부 트래픽을 내부망과 분리하고, 경계 IDS/IPS와 방화벽으로 비인가 패킷을 실시간 탐지·차단한다. Anti-Virus·Anti-Malware 솔루션이 이 레이어의 대표적인 외곽 방어 수단이다. 물리 인프라가 가상화되고 경계가 소멸한 클라우드 환경에서는 경계 보안의 범위가 온프레미스를 넘어 클라우드 네트워크 경계로 확장된다. 클라우드 설정 오류와 취약점을 지속 모니터링하는 CSPM(Cloud Security Posture Management)과 가상머신·컨테이너 워크로드를 보호하는 CWPP(Cloud Workload Protection Platform)가 이 역할을 보완한다.

둘째, 네트워크 보안(Network Security)은 내부망으로 유입된 트래픽을 세밀하게 통제하는 영역이다. NAC(Network Access Control)로 접속 단말의 보안 상태를 검증하고, VPN으로 원격 접속 구간을 암호화한다. VoIP 보호와 무선 구간 보안도 이 레이어에서 함께 관리되며, NGFW(Next-Generation Firewall)가 단순 패킷 필터링을 넘어 애플리케이션·사용자 단위의 정밀 트래픽 제어를 수행한다.

셋째, 엔드포인트 보안(Endpoint Security)은 네트워크와 직접 연결되는 PC·모바일·서버 등 단말 기기의 무결성을 실시간으로 확보하는 영역이다. 엔드포인트 보안 정책 강제 적용(Endpoint Security Enforcement)과 패치 관리(Patch

Management)를 통해 알려진 취약점을 선제적으로 제거한다. 단말 내 행위를 실시간으로 모니터링하고 위협에 즉각 대응하는 EDR(Endpoint Detection and Response)과 행위 기반 탐지 기술로 알려지지 않은 위협까지 차단하는 NGAV(Next-Generation Antivirus)가 이 레이어의 핵심 솔루션이다.

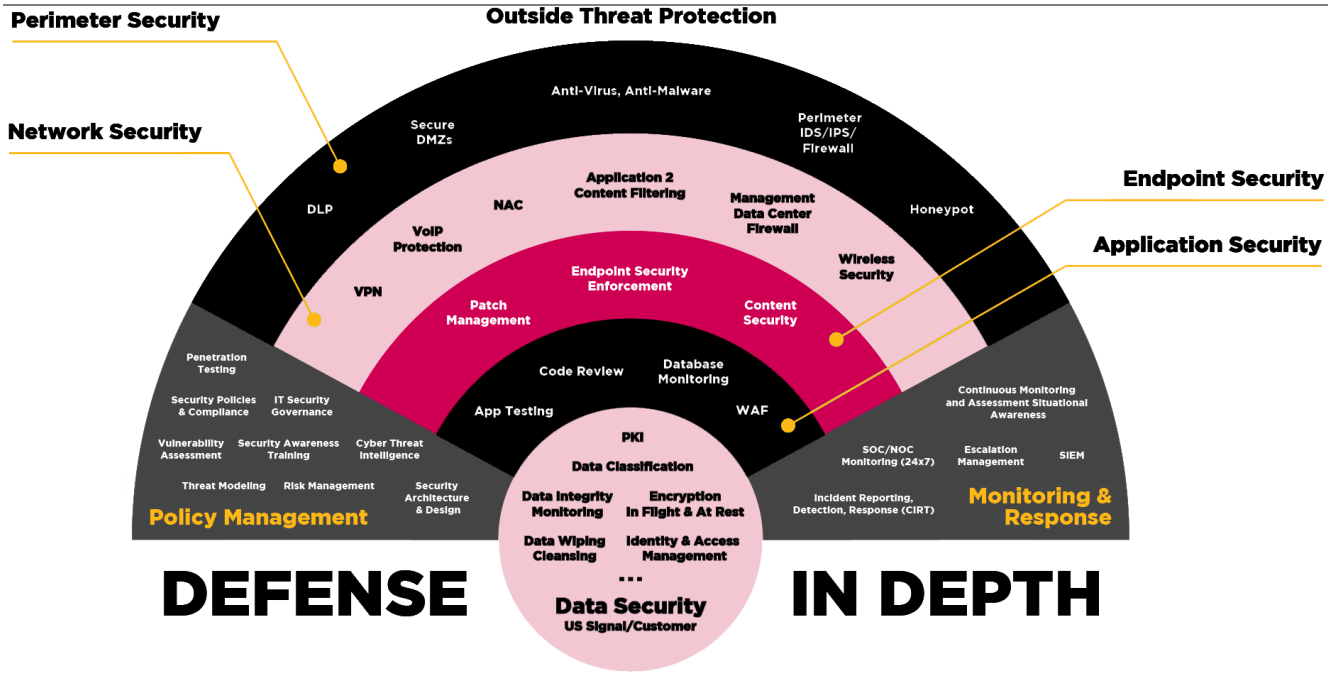
넷째, 애플리케이션 보안(Application Security)은 서비스와 데이터를 처리하는 애플리케이션 계층의 취약점을 방어하는 영역이다. 개발 단계에서는 코드 리뷰와 앱 테스팅으로 취약점을 사전 식별하고, 운영 단계에서는 WAF(Web Application Firewall)와 데이터베이스 모니터링으로 실시간 위협을 탐지·차단한다. 콘텐츠 보안 정책(Content Security)을 통해 애플리케이션에서 유통되는 데이터의 무결성도 함께 관리된다.

다섯째, 데이터 보안(Data Security)은 조직의 핵심 자산인 데이터 자체를 보호하는 최내곽 영역이다. 데이터 분류 체계를 기반으로 전송 중·저장 중 암호화(Encryption In Flight & At Rest)를 전 생애주기에 걸쳐 적용하고, DLP(Data Loss Prevention)로 화면 캡처나 외부 저장 매체를 통한 무단 유출을 탐지·차단한다. 문서 단위로 접근 권한을 통제하는 DRM(Digital Rights Management)은 데이터가 조직 외부로 반출된 이후에도 보호 효력을 유지한다. IAM(Identity & Access Management)으로 검증된 사용자에게만 최소 권한(Least Privilege)을 부여하며, SSO(Single Sign-On)로 복수 시스템에 대한 접근을 일원화해 인증 편의성과 보안성을 동시에 확보한다. 데이터 무결성 모니터링과 안전한 데이터 폐기(Data Wiping & Cleansing)까지 이 레이어에서 통합 관리된다.

여섯째, 정책 관리(Policy Management)는 위의 모든 기술적 레이어를 뒷받침하는 관리적·제도적 기반이다. 보안 정책 수립과 컴플라이언스 준수를 토대로, 취약점 평가·위협 모델링·위험 관리를 체계화한다. 임직원 보안 인식 교육과 사이버 위협 인텔리전스를 통해 인적 요인에 의한 보안 사고를 예방하며, 보안 아키텍처 설계와 IT 거버넌스가 전사 보안 체계의 일관성을 유지하도록 한다.

일곱째, 모니터링 및 대응(Monitoring & Response)은 이기종 보안 레이어 전반에서 발생하는 경보와 로그를 통합 수집·분석·대응하는 중앙 관제 영역이다. SOC/NOC의 24시간 상시 모니터링과 SIEM(Security Information and Event Management)으로 개별 레이어의 사각지대를 보완하고, AI 기반 위협 탐지 기술로 상관 분석의 정확도를 높인다. 탐지부터 격리·복구까지 대응 절차를 자동화하는 SOAR(Security Orchestration, Automation and Response)가 이 레이어의 대응 속도를 결정적으로 끌어올리며, 침해사고 탐지부터 대응(CIRT)·에스컬레이션 관리까지 일원화된 절차로 처리된다.

심층 방어 구조



자료: US signal, 한국IR협의회 기업리서치센터

국내 보안 산업 구조

정부 주도형 보안 모델

앞서 살펴본 규제 체계와 기술 레이어는 보안 솔루션 공급자에게는 시장 진입 장벽이지만, 이를 실제로 도입하고 운영해야 하는 기업 내 보안 담당자에게는 의사결정의 출발점이다. 정보보호최고책임자(CISO)를 비롯한 기업의 의사결정권자들이 예산을 집행하고 특정 보안 솔루션을 조달하기로 결정하는 과정은 법적 규제 준수 대응과 투자 효율성, 그리고 업무 생산성이 정교하게 얽힌 의사 결정을 필요로 한다.

우리나라는 공공, 금융, 민간 등 각 산업 영역의 가이드라인을 정부가 직접 제정하고 관리 감독하는 정부 주도형 보안 모델을 취하고 있다. 사고 발생 시 가이드라인 충족 여부가 면책의 핵심 기준이 되다 보니, 국내 기업의 CISO에게는 기술적 우수성이나 자율적인 위험 관리보다 당국이 제시한 법적 기준의 선제적 충족이 최우선 고려 대상이 된다.

두 번째 변수는 비용과 조직 내 거버넌스의 충돌이다. 의사결정권자들은 보안의 원래 목적, 총소유비용(TCO, Total Cost of Ownership), 그리고 현업 임직원의 불편함이라는 상충된 요소를 지속적으로 조율해야 한다. 아무리 안전한 솔루션이라도 다중 인증의 번거로움이나 파일 반출 절차의 지연이 과도하면 현업 생산성이 하락하고, 임직원들이 비인가 도구를 우회 사용하는 섀도 IT(Shadow IT) 현상으로 이어져 도리어 보안 사각지대를 키운다. CISO는 이 긴장 관계 안에서 통제 효율성이 가장 높은 솔루션을 한정된 예산으로 선택해야 하는 압박을 받는다.

국내 보안 산업
: 내수 및 공공 조달 중심의 단품

이처럼 촘촘한 규제 요건과 다층적 기술 구조가 맞물린 국내 환경은 보안 공급망의 체질을 해외 시장과 완전히 다른 형태로 고착화시켰다. 국가 주도의 사전 인증 제도와 물리적 망분리 규제가 국내 보안 시장을 내수 및 공공 조달 중심으로 폐쇄화시킨 것이다. 이를 글로벌 대형 보안 기업들이 포진한 해외 생태계와 비교하면 다음과 같은 기술적·상업적 특징이 나타난다.

첫째, 시장의 주요 동력 측면에서 한국은 공공 조달과 법적 의무 사항의 영향력이 절대적인 반면, 해외 생태계는 민간의 자율적인 수요와 자본 조달을 기반으로 성장한다. 국내 보안 업체들의 매출에서 공공 발주가 차지하는 비중은 이례적으로 높다. 공공기관이나 금융권이 규정 준수를 위해 국산 인증 제품을 우선 채택하는 구조여서, 국내 업체들은 정부 가이드라인에 맞춘 컴플라이언스 솔루션을 공급하며 안정적인 내수 기반을 확보해 왔다. 다만 이는 제한된 시장 내에서 가격 중심의 출혈 경쟁을 유발하며, 소프트웨어의 적정 가치를 인정받기 어렵게 만들어 기업의 연구개발(R&D) 재투자 재원을 제한하는 요인이 된다. 반면 미국이나 이스라엘 등의 해외 보안 생태계는 민간 기업들이 사이버 공격으로 인한 비즈니스 리스크와 법적 책임을 경감하기 위해 자발적으로 대규모 보안 투자를 집행한다. 이러한 민간 수요를 바탕으로 탄탄한 스타트업 생태계가 출현하며, 벤처캐피탈(VC)의 자본 투입과 인수합병(M&A)을 통해 기업 규모를 빠르게 확대하는 구조가 형성된다.

둘째, 제품의 확장성과 기술 아키텍처 측면에서 한국은 특정 기능에 특화된 단품(Point Product) 중심의 솔루션 비중이 높은 반면, 글로벌 기업들은 통합 플랫폼과 클라우드 기반의 생태계를 구축했다. 국내 보안 업체들은 물리적 망분리 의무를 충족하기 위한 망연계 솔루션이나 키보드 보안, PC 방화벽 등 규제가 명시하는 기술 요건에만 최적화된 개별 솔루션 발전에 집중해 왔다. 그러나 이러한 제품들은 글로벌 시장의 호환성을 확보하는 데 명확한 한계를 보인다. 이와 대조적으로 글로벌 보안 기업들은 네트워크, 엔드포인트, 클라우드 보안을 하나의 플랫폼으로 통합하여 공급한다. 경계 중심의 물리적 통제를 넘어 데이터와 사용자 정체성을 지속해서 검증하는 제로 트러스트(Zero Trust) 철학을 바탕으로, 모든 솔루션을 SaaS 형태로 다변화하여 전 세계 시장으로 공급을 확대하고 있다.

결론적으로 한국의 보안 업체 생태계는 공공 조달과 규제 환경을 발판 삼아 성장해 왔으나, 시장의 규모적 한계와 글로벌 표준 아키텍처와의 불일치라는 과제를 안고 있다. 특히 최근 생성형 AI와 대형 SaaS 도입에 대한 시장의 수요가 폭발하면서, 기존의 경직된 물리적 망분리 규제는 현업의 생산성을 가로막는 최대 걸림돌로 부각되었다. 이에 따라 정부 주도로 다층보안체계(MLS, Multi-Level Security) 도입과 금융권 망분리 규제 완화 등 전례 없는 제도적 변화가 시작되면서, 내수 컴플라이언스에 안주하던 국내 보안 업체들은 이제 클라우드 네이티브 전환과 플랫폼화라는 근본적인 체질 개선을 강제받는 변곡점에 직면해 있다.

국내와 해외 사이버 보안 시장 비교

비교 항목	국내 보안 시장	해외 보안 시장
주요 시장 동력	공공 조달 및 법적 의무 사항(규정 준수) 영향력 절대적 공공 발주 매출 비중이 높음	민간의 자율적인 수요와 자본 조달 기반 성장 비즈니스 리스크 및 법적 책임 경감을 위해 자발적 투자
시장 경쟁 및 환경	제한된 내수 시장 내 가격 중심의 출혈 경쟁 소프트웨어 적정 가치 인정 미흡으로 R&D 재투자 제한	탄탄한 스타트업 생태계 출현 벤처캐피탈(VC) 투자 및 활발한 M&A 를 통한 빠른 규모 확장
제품 및 기술 아키텍처	특정 기능에 특화된 단품(Point Product) 중심 솔루션 망연계, 키보드 보안 등 국내 규제 요건에만 최적화	통합 플랫폼 및 클라우드(SaaS) 기반 생태계 구축 네트워크, 엔드포인트, 클라우드 보안의 통합 공급
글로벌 확장성	국내 규제 맞춤형으로 글로벌 시장 호환성 확보에 한계	제로 트러스트(Zero Trust) 철학 바탕의 SaaS 형태로 전 세계 공급

자료: 한국IR협의회 기업리서치센터

2 국내 보안 산업의 변화

경계 보안에서 제로 트러스트로

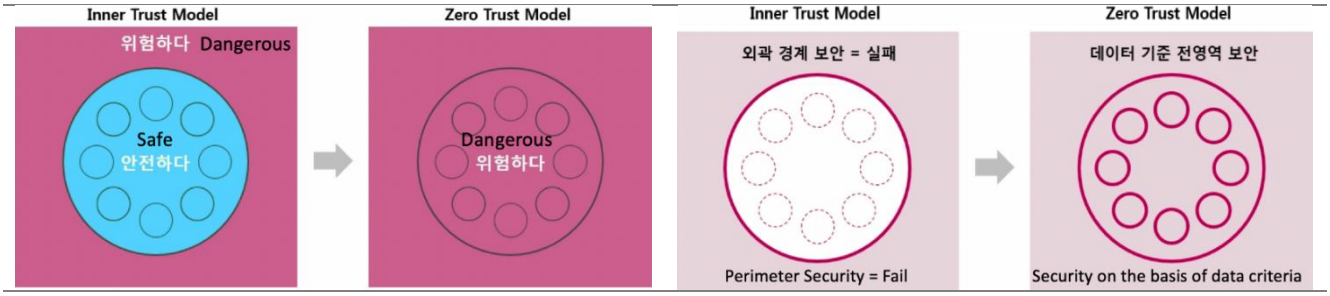
고전적인 경계 보안(Perimeter Security)은 내부 네트워크와 외부 공중망 사이에 단일 방어선을 구축하는 모델이다. 차세대 방화벽(NGFW, Next-Generation Firewall)과 침입탐지(IDS, Intrusion Detection System)·침입방지(IPS, Intrusion Prevention System) 시스템을 외곽에 집중 배치하고, DMZ(비무장지대)로 외부용 서버를 격리하며, VPN으로 원격 접속을 통제하는 구조다. 내부망 진입 이후의 트래픽은 원칙적으로 신뢰하는 방식이어서, 경계만 견고하게 유지하면 내부 자산은 안전하다는 전제가 수십 년간 기업 보안의 표준으로 작동했다.

한계는 클라우드 전환과 원격 근무가 일상화되면서 드러났다. 기업 데이터와 인프라가 사내 전산실을 벗어나 전 세계로 분산되자, 지켜야 할 자산 자체가 경계 밖으로 나가버리는 구조적 모순이 발생했다. 동시에 정상 계정을 탈취해 내부망에 침투하는 지능형지속공격(APT)과 공급망 취약점은 경계 모델의 치명적 맹점을 정확히 파고들었다. 외곽을 뚫으면 내부에서 자유롭게 이동할 수 있는 구조가 오히려 피해를 키웠다.

제로 트러스트는 이 경계 보안의 전제를 뒤집는다. "아무도 믿지 말고, 항상 검증하라(Never Trust, Always Verify)"는 원칙 아래, 내부·외부를 구분하는 경계선 개념을 폐기하고 모든 접근 경로를 잠재적 공격 노출면으로 간주한다. 단 한 번의 외곽 인증으로 내부 접근을 일괄 허용하는 구도 대신, 모든 사용자와 단말에 최소 권한(Least Privilege)만 부여하고 접속할 때마다 신원과 보안 상태를 실시간으로 검증한다.

중요한 것은 제로 트러스트가 특정 솔루션이 아니라 보안 철학이자 방법론이라는 점이다. 단기간에 완성되지 않으며, 기존 인프라와 레거시 보안 구조를 고려한 점진적 전환 전략이 필수적이다. 그리고 이 전환의 시급성을 결정적으로 끌어올린 것이 바로 초지능형 생성 AI의 부상이다.

경계 보안 vs 제로 트러스트



자료: 펜타 시큐리티, 한국IR협의회 기업리서치센터

AI는 제로트러스트 도입을 촉진

보안 위협의 구조적 전환: 초지능형 AI의 등장

에이전트형(Agentic) AI의 진화는 제로 트러스트로의 전환을 단순한 방향성이 아닌 시급한 과제로 만들고 있다. 앤스로픽(Anthropic)이 선보인 차세대 모델 클로드 미토스(Claude Mythos)는 그 변화를 극명하게 보여주는 사례로 주목받고 있다. 기존 AI가 취약점 코드 패턴을 학습하는 보조 도구에 머물렀다면, 미토스 급 프론티어 모델은 방대한 컨텍스트 창과 자율적 추론, 도구 호출실행력을 바탕으로 인간이 수십 년간 발견하지 못한 제로데이 취약점(Zero-Day Vulnerability)을 단 몇 분 만에 찾아낼 수 있는 것으로 보고되고 있다. 나아가 이를 악용할 수 있는 익스플로잇 코드(Exploit Code)까지 자율적으로 생성하는 것으로 알려졌다.

이 같은 초지능형 AI의 등장은 세 가지 차원에서 보안 사고의 폭발적 증가를 예고한다.

첫째, 공격 비용의 극적인 하락이다. 기존 방어 체계는 취약점이 많지 않고 탐지하기도 어렵다는 가정 위에 서 있었다. 특히 오래된 오픈소스나 중소기업 솔루션은 실제로 안전해서가 아니라, 공격자가 투입해야 하는 시간과 비용 대비 수익성이 낮아 방치되었을 뿐이다. 그러나 AI가 취약점 탐색을 자동화하면서 이 전제는 완전히 무너졌다. 그동안 공격 대상에서 비껴나 있던 소외된 시스템까지 전방위로 위험에 노출될 수 있다.

둘째, 방어자의 '유예기간(Window of Vulnerability)' 소멸이다. 과거에는 취약점이 발견된 후 패치가 배포되기까지 방어자가 대응할 수 있는 최소한의 시간이 존재했다. 이제는 AI가 취약점 탐지부터 자동 공격 도구 완성까지의 과정을 24시간 이내로 단축시키면서, 패치 중심의 사후 대응식 방어는 구조적으로 불가능해졌다.

셋째, AI 에이전트 보편화에 따른 '비인간 신원(Non-human Identity, NHI)'의 부상이다. AI 에이전트가 인간의 권한을 위임받아 파일 접근, 코드 실행, 외부 시스템 호출 등을 자율적으로 수행하는 환경이 도래했다. 이들의 신원 확인, 권한 위임 범위 설정, 행동 관측 등은 기존의 인간 중심 접근 통제 체계로는 대응이 어렵다.

결국 어떤 방어도 완벽할 수 없다는 전제에서 출발해야 한다. 침해가 발생하더라도 피해 범위를 최소화할 수 있도록, 실시간으로 맥락과 의도를 탐지하고 접근을 지속적으로 검증하는 제로 트러스트 아키텍처의 도입 필요성이 한층 더 뚜렷해진 시점이다. 이에 한국 정부는 이 철학을 국가 차원의 제도로 구체화하기 시작했다.

한국형 제로 트러스트의 제도화

정부와 금융권을 시작으로 제로트러스트 도입

N2SF와 다층보안체계, 그리고 4대 보안 주체의 대응

앞서 살펴본 제로 트러스트라는 거시적인 보안 철학을 국내 공공 및 금융 조달 시장의 현실에 맞게 구현한 국가 차원의 청사진이 바로 'N2SF(국가 망 보안체계, National Network Security Framework)'이다. N2SF는 2024년 9월 국정원이 '다층보안체계(MLS)'라는 이름으로 로드맵을 처음 공개한 뒤 명칭을 확장·변경하여 정립된 프레임워크로, 기존의 획일적 망분리 체계를 탈피하여 '데이터와 업무의 중요도 중심'으로 방어선을 재설계한다는 지향점을 갖는다. 정부는 이 N2SF를 통해 공공 영역의 정보 시스템을 세 가지 등급으로 분류하고 차등적인 보안통제를 적용함으로써 조달 시장에 실질적인 강제력을 행사하고 있으며, 이는 국내 정보보안의 네 가지 핵심 주체별로 다각적인 정책 변화를 촉발하고 있다.

첫째, 공공기관 및 국가·지자체는 이번 N2SF 도입의 가장 직접적인 영향권에 놓인다. 국가 시스템의 보안 등급은 데이터의 민감성에 따라 세 가지 등급으로 분류되어 차등적인 보안통제 기준을 적용받는다. 안보·외교·수사 활동 및 국민의

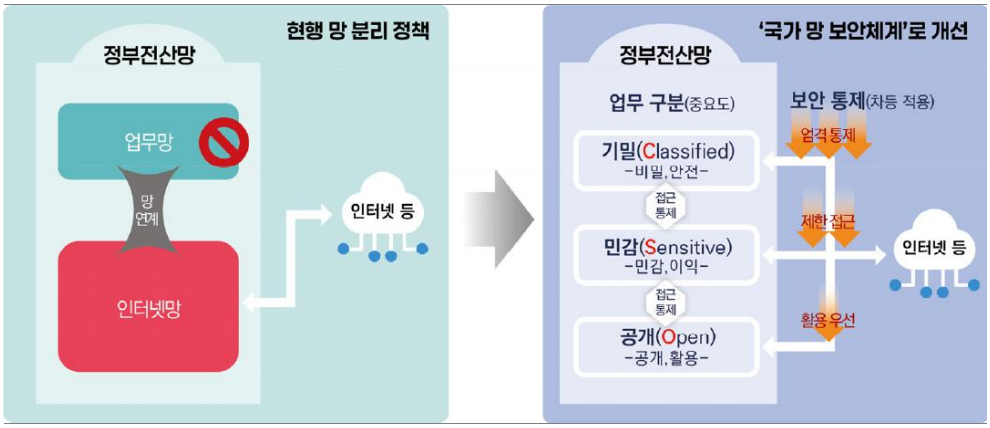
생명·안전에 중대한 영향을 미칠 수 있는 정보를 다루는 C(Classified·기밀) 등급은 기존의 엄격한 물리적 망분리 환경을 유지한다. 비공개 행정 서비스를 다루는 S(Sensitive·민감) 등급은 논리적 망분리를 포함한 다수의 보안통제 항목 충족을 전제로 클라우드 활용을 허용하는 완충 지대를 형성한다. 대국민 공개 데이터를 운용하는 O(Open·공개) 등급은 실무 규제를 과감히 완화하여 생성형 AI와 대형 SaaS 솔루션을 제약 없이 도입할 수 있도록 문호를 전면 개방한다. 정부는 현재 이러한 등급 분류 체계의 실효성을 검증하기 위해 KISA 주관으로 주요 공공기관을 대상으로 한 실증 사업을 추진 중이다.

둘째, 금융회사 및 핀테크 기업 역시 유사한 방향의 정책 전환 하에 놓이게 된다. 금융권의 망분리 규제 개선은 N2SF와 방향성을 공유하지만, 금융위원회가 2024년 8월 독자적으로 발표한 「금융분야 망분리 개선 로드맵」을 통해 별도의 정책 트랙으로 추진되고 있다. 그간 금융권의 혁신을 가로막던 획일적 망분리 규제가 데이터 중요도 기반의 차등 보안 통제 방식으로 고도화되고 있으며, 금융사들이 보안성을 확보하면서도 생성형 AI나 외부 SaaS 솔루션을 안전하게 금융 서비스에 결합할 수 있도록 유도하는 것이 핵심 방향이다.

셋째, 일반 기업 및 온라인 서비스 사업자에게는 민간 영역의 확산을 위한 맞춤형 제로 트러스트 전환 정책이 적용된다. 과기정통부와 KISA를 중심으로 실증 사업이 전개되고 있으며, 중소·중견 기업과 온라인 서비스 사업자들이 거대한 예산 투입 없이도 자사 서비스 환경에 제로 트러스트 구조를 단계적으로 이식할 수 있도록 「제로트러스트 가이드라인」(2023년 v1.0, 2024년 v2.0)을 보급하고 있다. 이와 함께 기업의 실제 환경에 제로 트러스트를 적용하는 도입·전환 컨설팅 지원도 병행 추진되고 있다.

넷째, 국가 핵심기술 보유 기업 및 주요 정보통신기반시설은 N2SF의 철학이 가장 절실한 영역이면서도, 동시에 적용이 가장 더딜 수밖에 없는 영역이다. 전력·에너지·제조 설비와 같은 OT 시스템은 가용성과 실시간성이 절대적 우선순위인 구조상, 패치 적용·통신 암호화·다중 인증 도입이 IT 환경 대비 현저히 제한되어 일반적인 제로 트러스트 원칙을 그대로 이식하기 어렵다. KISA는 2025년 12월 이러한 OT 특성을 반영한 「OT 환경의 제로트러스트 적용 안내서」를 국내 최초로 발표하며 개념적 토대를 마련했으나, 실증과 현장 검증은 이제 시작 단계다. 정책의 방향성은 확립됐지만, 실질적인 강제력을 갖춘 의무화 규정으로 이어지기까지는 추가적인 제도화 과정이 필요한 상황이다.

기존 망 분리 정책과 국가 망 보안 체계 비교



자료: 국가정보원, 한국IR협의회 기업리서치센터

점진적 변화가 현실적인 경로

국내 보안 산업의 현실적 전환 경로: 점진적 다변화와 양극화

초지능형 생성 AI의 위협과 정부의 다층보안체계(MLS) 도입, 금융권 망분리 완화가 맞물리는 현시점은 국내 보안 산업의 거대한 변곡점임이 분명하다. 그러나 정부 주도형 규제 환경과 독자적인 생태계가 오랜 기간 고착화된 한국 시장의 특성을 고려할 때, 글로벌 시장과 같은 급진적인 플랫폼화나 SaaS로의 전면 전환이 단기간에 일어날 가능성은 낮다. 향후 국내 보안 생태계는 기존 레거시 체제를 유지한 채 실제 산업 현장의 움직임과 맞물려 세 가지 현실적인 경로를 따라 점진적으로 재편될 것으로 전망된다.

첫째, 초기에는 관망과 눈치보기가 지배적인 기조를 이룰 것이다. 제로 트러스트는 특정 솔루션을 지칭하는 개념이 아니라 '아무것도 신뢰하지 않는다'는 보안 철학이자 설계 원칙이다. 정부가 가이드라인을 제시하고 실증 사업을 추진하고 있으나, 이를 실제 조달과 도입으로 연결하는 인증 기준과 검증 체계가 정착되기까지는 상당한 시간이 필요하다. 수요 기관 입장에서는 어떤 솔루션이 제로 트러스트 요건을 충족하는지, 기존 시스템과 어떻게 연계해야 하는지에 대한 명확한 답을 얻기 어렵다. 이에 따라 시장 참여자 대부분은 선도 기관의 사례와 정부의 후속 지침을 기다리는 관망 국면에 머물 가능성이 높다.

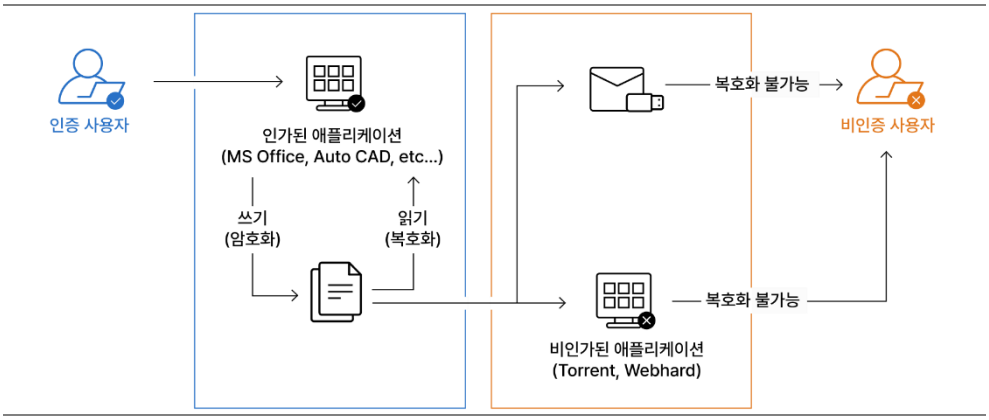
둘째, 관망이 걷히더라도 변화는 전면적이기보다 완만하게 진행될 수밖에 없다. 두 가지 구조적 제약이 작용하기 때문이다. 우선, 국산 인증 제품 중심의 공공·금융 조달 시장에서는 기존 단품 솔루션 공급사들의 기득권과 인터페이스 호환성 문제가 복잡하게 얽혀 있어 새로운 보안 아키텍처로의 전환 비용이 크다. 여기에 MLS 체계상 안보·핵심 행정 업무를 다루는 등급은 여전히 강력한 망분리 기조를 유지하며, 실질적인 규제 완화는 상대적으로 개방된 등급에 한정된다. 두 제약이 맞물리는 한, 시장 전반의 체감 변화는 제한적인 영역에서부터 단계적으로 나타날 수밖에 없다.
셋째, 솔루션 포트폴리오에 따라 공급사 간 희비가 갈릴 것이다. 이에 따라 단일 솔루션에 매출을 집중해 온 공급사는 해당 솔루션이 새로운 보안 패러다임에서 수요가 줄어들 경우 대체 수익원이 없어 직접적인 타격을 받을 것으로 보인다. 반면, 기존 레거시 솔루션으로 안정적인 수요 기반을 유지하면서 새로운 패러다임에 부합하는 솔루션을 선제적으로 준비해 온 공급사는 전환기의 수혜를 입을 가능성이 높다. 변화에 앞서 어떻게 대응해 왔는가가 개별 기업의 생존과 성장을 가르는 핵심 변수가 될 전망이다.

3 DRM 솔루션

DRM

DRM(Digital Rights Management)은 디지털 콘텐츠의 저작권을 보호하고 무단 사용을 방지하는 기술이다. 콘텐츠의 저작권 보호를 위한 DRM을 일반용 DRM 또는 CDRM(Commerce DRM)이라 부르고, 문서 보안용 DRM을 EDRM(Enterprise DRM, 기업용 DRM)으로 분류한다.

DRM 개념도



자료: 가비아, 한국IR협의회 기업리서치센터

DRM의 시작
:음악, 소프트웨어 불법 복제 방지

DRM은 CDRM에서 시작되었다. 2001년 미국의 음원 파일 공유 서비스인 냅스터의 MP3 무단 공유 사태를 계기로 음악이나 소프트웨어의 불법 복제 방지를 위해 개발되었으며, 현재는 영화, eBook, 게임, 라이브 스트리밍, OTT 콘텐츠 등 거의 모든 디지털 콘텐츠 분야에서 활용되고 있다.

CDRM은 단순히 파일을 보호하는 수준을 넘어, 구독 사용자만 콘텐츠를 사용할 수 있도록 제한하거나 특정 국가 및 지역에서만 접근하도록 통제한다. 또한 대여 기간이 만료되면 자동으로 접근을 차단하고, 동시 접속 기기 수를 제한하는 역할도 한다. 이와 달리, 데이터 전송 과정만 보호하는 일반 암호화 기술은 사용자 기기에 도착한 후 복호화된 파일이 남아 복제나 재배포의 위험이 있다. 반면, CDRM은 지속적으로 사용 권한을 제어하므로 일반 암호화보다 보안이 한 층 강화된 솔루션이다.

EDRM은 문서 DRM으로도 불린다. 기업 내의 문서, 영업 자료, 설계 도면과 같은 중요 정보자산을 보호하고 관리하는 기능을 한다. 회사의 문서 관리 시스템과 연동하여 구축하며, 문서를 열람할 수 있는 사용자별로 읽기, 수정 등의 권한을 차단하거나 제한한다. 아울러 화면 캡처 프로그램을 통한 무단 화면 저장이나 클립보드를 이용한 텍스트 복사 및 붙여넣기 등 유출 경로가 될 수 있는 모든 사용자 행위를 원천 제어한다. 또한 회사 외부에서의 접근을 통제하여 정보 유출을 방지하고, 외부 인력이 접근할 때도 엄격한 제한을 둔다. 문서를 작성한 본인이라 하더라도 권한이 없으면 삭제나 복사 등을 할 수 없다. 최초 작성자나 수정자가 누구인지 확인할 수 있는 감사 추적 기능도 제공한다. 여기에 워터마킹(Watermarking) 기술을 결합하면 인쇄물이 유출되었을 때 유포자를 추적할 수 있다. 디지털 워터마킹은 DRM의 기반 기술 중 하나로, 디지털 콘텐츠에 저작권자의 고유 마크를 삽입하여 문서의 위조나 변조를 막는 기술이다.
EDRM은 한 번 도입하면 전사 임직원의 업무 프로세스에 깊숙이 녹아들기 때문에, 고객사가 다른 브랜드로 쉽게 전환하지 못하는 강력한 '락인(Lock-in) 효과'를 가진다. DRM 솔루션이 적용된 문서를 열람하고 복호화하기 위해서는 해당 솔루션을 지속적으로 사용해야 하기 때문이다.

운영체제 변경은
새로운 DRM 솔루션을 요구

또한 EDRM 솔루션은 개인 PC마다 에이전트 프로그램을 설치해야 하는 특성상, 운영체제(OS) 환경이 바뀔 때마다 대규모 교체 주기를 맞이하곤 한다. DRM 기술은 소프트웨어의 단순 설치를 넘어, 컴퓨터 운영체제(OS)의 가장 깊숙한 핵심 제어 영역인 '커널(Kernel)' 수준에서 밀접하게 연동되어 작동하기 때문이다. 대표적인 사례가 바로 2019년에 발

생한 공공기관의 윈도우 10 업그레이드 특수다. 당시 마이크로소프트의 윈도우 7 지원 종료를 앞두고 대대적인 PC OS 교체 작업이 진행되었다. 이 과정에서 기존 DRM 솔루션도 윈도우 10 환경에 맞춰 업그레이드하거나 교체해야 하는 연쇄 수요가 발생했다. 여기에 국가정보원의 암호모듈 검증 필 인증제도가 국제공통평가기준(CC) 인증으로 대체되는 제도적 변화까지 맞물리면서, 2019년을 기점으로 국내 DRM 기업들은 기록적인 매출 성장과 호황기를 누렸다. 이러한 인프라 교체 주기는 DRM 기업의 실적이 퀀텀 점프하는 중요한 모멘텀이 된다.

최근 주목할 부분은 기존 핵심 고객사들의 IT 인프라가 클라우드 환경으로 전격 전환되고, 파트너사 및 협력사 간의 데이터 연동이 급증하고 있다는 점이다. 과거 사내 폐쇄망 중심의 구축형(On-Premise) DRM 환경과 달리, 하이브리드 워크(재택근무)와 외부 협업 환경 확산은 내부망을 벗어난 데이터에 대한 실시간 권한 제어 수요를 자극하고 있다. 이에 따라 주요 공급사들은 클라우드 보안 서비스(SaaS) 형태로의 비즈니스 모델 다각화를 추진 중이며, 이는 대기업 고객의 인프라 확장 대응력을 높이는 동시에 일회성 라이선스 중심의 사업 구조에서 탈피해 안정적인 반복 매출(Recurrent Revenue) 체력을 확보하는 계기가 될 것으로 보인다.

커널(Kernel)의 위치와 시스템 계층 구조도

자료: 한빛미디어, 한국IR협의회 기업리서치센터

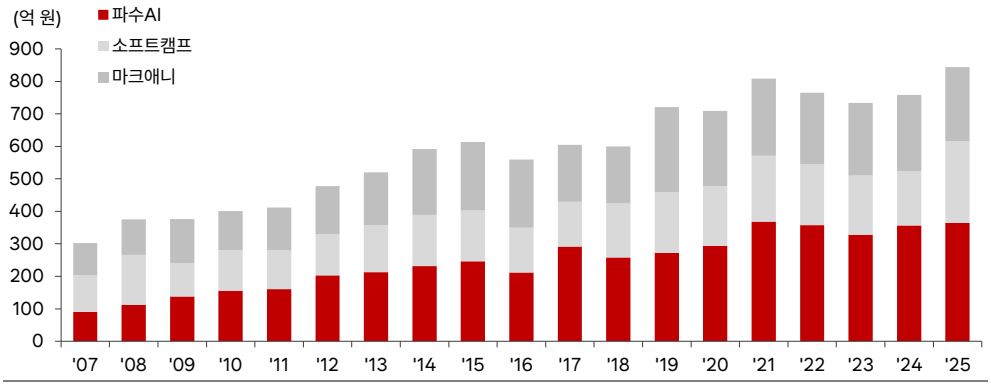
국내 DRM 솔루션 시장은 파수AI(FasooAI), 마크애니(MarkAny), 소프트캠프(Softcamp) 3사가 주도하고 있으며, 이외에 다수의 중소기업이 참여하고 있다.

파수AI는 1999년 삼성 SDS 사내벤처로 시작하여 2000년 분사·설립된 보안 솔루션 개발 업체다. 문서, 데이터, 애플리케이션 보안 분야에서 전문성을 보유하고 있다. 현재 통합문서보안(기업용 DRM), 민감정보 식별 및 통제 관리, 사용자 행동 기반 위험 관리, 애플리케이션 보안 솔루션 등을 제공한다.

마크애니는 1999년 설립된 보안 솔루션 개발업체로, DRM 및 위변조 방지, CCTV 영상 보안, 멀티미디어 콘텐츠 보호 솔루션에 특화된 기업이다. 2019년부터는 블록체인 분야에 진출하여 블록체인 기반 전자서명 기술 관련 특허를 10건 이상 취득했으며, 자체 개발한 DRM 솔루션으로 인도네시아, 두바이 등 해외 시장에 진출한 이력이 있다.

소프트캠프는 1999년 설립된 정보보안 업체로 기업용 문서 DRM, 키보드 보안 솔루션, 공급망 보안, 보안 클라우드 서비스 등을 주력으로 삼고 있다. 최근에는 스마트 공장의 공급망 보안, 원격 브라우저 격리(RBI)를 활용한 클라우드 보안 등 4차 산업혁명 핵심 기술을 적용한 정보보안 솔루션인 'SHIELDEX GateScanner' 제품을 출시하여 시장에 공급하고 있다.

DRM 3사 매출 추이


(억 원)
파수AI
소프트캠프
마크애니
900
800
700
600
500
400
300
200
100
0
'07
'08
'09
'10
'11
'12
'13
'14
'15
'16
'17
'18
'19
'20
'21
'22
'23
'24
'25

투자포인트

1 다층보안체계가 재점화하는 데이터 보안 모멘텀

제로 트러스트 전환으로 콘텐츠 보안의 위상이 급부상하고 있다. 과거에는 방화벽·VPN으로 외부망 진입만 막으면 충분했으나, 클라우드·SaaS 전환과 AI 에이전트 보편화로 보호 자산이 물리적 경계 밖으로 이동하면서 외곽 방어선은 무력화됐다. 지능형지속공격(APT)이나 비인간 신원 기반 우회 공격 앞에서는 네트워크·단말 보안만으로 유출을 막을 수 없다. 결국 파일 자체를 암호화하고 열람 권한을 실시간 제어하는 콘텐츠 보안이 제로 트러스트 아키텍처의 최후 방어선으로 재평가받고 있다.

과학기술정보통신부·KISA(한국인터넷진흥원, Korea Internet & Security Agency)가 발간한 제로트러스트 가이드라인 2.0은 글로벌 성숙도 모델과 미국 NSA(국가안보국, National Security Agency) 지침을 반영해 국내 환경에 최적화된 프레임워크를 제시한다. 보안 체계는 기존, 초기, 향상, 최적화의 4단계로 진화하며, 콘텐츠 보안도 수동 관리에서 출발해 중앙집중 제어를 거쳐 AI 기반 자동 분류·동적 최소 권한 정책 적용 단계로 고도화된다.

이와 같은 가이드라인의 단계적 이행 원칙에 발맞추어 기업들의 콘텐츠 보안 요구사항도 순차적으로 전개된다. 특히 정부가 추진하는 다층보안체계 도입과 맞물려 시장의 최우선 과제는 어떤 데이터가 어느 수준의 위험도를 가졌는지 식별하고 분류하는 것에서 출발한다. 데이터의 민감도를 국가 기밀, 민감, 공개 등급으로 분류하지 못하면 적절한 제로 트러스트 보안 정책을 적용할 수 없고, 클라우드나 인공지능 서비스의 도입 자체가 구조적으로 막히기 때문이다. 결과적으로 시장의 수요는 초기 비정형 데이터의 식별 및 자동 라벨링 솔루션에서 시작하여, 파일 자체에 거버넌스 통제권을 이식해 외부 유출 후에도 원격 제어가 가능한 솔루션으로 이어지며, 최종적으로는 사용자 신원과 접속 맥락을 실시간 분석해 동적으로 권한을 변경하는 맥락 기반 접근제어 솔루션으로 단계적으로 확장 적용될 전망이다.

파수AI의 데이터보안 강화 솔루션
1)FDR: 데이터 식별 및 분류
2)FRV: 사용자 행동 기반 관리

파수AI는 가이드라인의 성숙도 단계별 요구사항을 충족할 수 있는 제품 라인업을 갖추고 있다. 파수 데이터 레이더(FDR, Fasoo Data Radar)는 제로 트러스트 데이터 보안의 첫 단추인 식별 및 분류를 해결하는 핵심 솔루션으로, 기업 내에 방대하게 쌓여 있는 미분류 데이터와 방치된 파일들을 실시간으로 스캔하여 그 안에 담긴 민감도와 중요 정보를 평가한다. 패턴 매칭 및 문맥 분석을 통해 개인정보나 핵심 기술 자산을 자동으로 분류, 격리, 암호화 처리 및 저장함으로써 다층보안체계 환경 구축을 위한 필수적인 데이터 체계화 기반을 제공한다. 파수 리스크뷰(FRV, Fasoo Risk View)는 최적화 단계의 핵심인 맥락 기반 보안 정책과 위험 관리를 담당하는 사용자 행동 기반 리스크 관리 솔루션으로, 다양한 보안 로그와 문서 접근 이력을 연관 분석해 임직원의 정상적인 행동 패턴을 학습한 뒤 평소와 다른 대량의 문서 반출이나 비인가 시간대의 핵심 자산 접근 등 이상 징후를 실시간으로 탐지하여 내부자 위협이나 계정 탈취 리스크를 선제적으로 제어한다.

다층보안체계(MLS) 환경에서 DRM과 FDR·FRV는 각자 다른 보안 문제를 해결한다. DRM이 인가된 사용자의 파일 유출을 차단하고 권한 통제에 집중하는 반면, FDR은 그보다 앞선 단계에서 파일 내부 문맥을 분석해 기밀(C)·민감(S)·공개(O) 등급을 자동으로 식별·라벨링하고, FRV는 사용자 행동 패턴을 실시간으로 학습해 이상 징후를 탐지하는 동적 통

제를 담당한다. 따라서 이미 FED를 통해 강력한 암호화 기반을 확보한 기업이라 할지라도, N2SF 환경으로의 안착을 위해서는 데이터 레이더를 통한 식별·분류 체계와 FRV를 통한 행동 기반 통제가 추가로 갖춰져야 한다.

다층보안체계(MLS) 가이드라인의 본격적인 확산은 한동안 성장의 문턱에서 정체되어 있던 데이터 보안 사업 부문에 강력한 모멘텀으로 작용할 전망이다. 파수AI의 데이터 보안 부문은 2021년 275억 원으로 정점을 기록한 이후 오랜 기간 박스권에 갇혀 있었다. DRM 시장 성숙화와 구독형 매출 확대 전략이 맞물린 결과로, 2023년 197억 원, 2024년 198억 원, 2025년 207억 원 수준에 머물렀다.[2]

N2SF 확산으로 다층보안체계 도입이 본격화되면 구조적 변화가 시작될 것으로 기대된다. 기존 DRM 유지보수 중심의 매출에서 벗어나, 데이터 레이더의 식별·분류 신규 프로젝트와 FRV 기반 행동 분석 라이선스 확대가 동시에 진행되면서 데이터 보안 부문의 외형 성장이 재개될 전망이다.

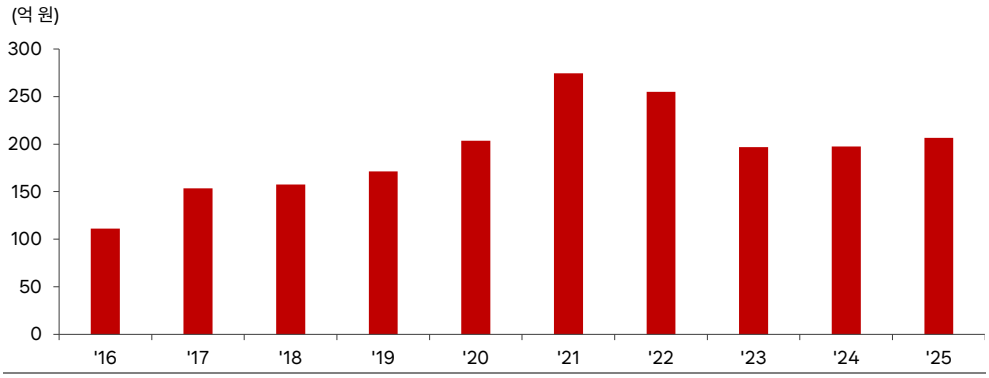
제로트러스트 성숙도 모델 2.0

	1. 기존(Traditional)	2. 초기(Initial)	3. 향상(Advanced)	4. 최적화(Optimal)
식별자 • 신원	• 온프레미스 ID 사용 • 패스워드 혹은 다중인증방식 • 수동접근 및 자격증명 관리	• 클라우드와 온프레미스 기반 ID 연계 • 다중인증 및 FIDO 기반인증 • 수동 및 정적 규칙 기반 위험 판단	• 컨텍스트 기반 ID 인증 • 일부 자동화된 및 동적 규칙을 이용한 위험도 평가 • 세션 기반 접근 지원	• 클라우드와 온프레미스 시스템 전반에 걸친 글로벌 ID • AI 기반 위험도 결정 및 지속적 보호 • 자동화된 적시·최소 권한 접근 적용
기기 및 엔드포인트	• 제한된 정책준수정보 • 단순하고 수동적 기기 목록 관리 • 수동적위협보호 기능 적용	• 대부분의 기기에 정책 준수 시행 메커니즘 사용 • 모든 기기에 대해 목록화 • 기기 보안솔루션 자동 관리	• 규정 준수 여부에 따른 접근 권한 부여 • 검증된 기기만 데이터 접근 • 자동화, 중앙집중식 위협 보호 및 자산관리 기능 통합	• 지속적인 기기 보안 상태 모니터링 및 검증 • 모든 환경에 걸쳐 자산 및 취약점 관리 통합 • 모든 기기에 대해 위협 보호
네트워크	• 경계분리 네트워크 구조 정의 • 알려진 위협 및 정적 트래픽 필터링 • 매우 중요한 애플리케이션 및 워크로드에 대한 기능 회복	• 소규모 경계를 통해 확장된 네트워크 구조 정의 • 내부 애플리케이션 모든 트래픽 및 외부 일부 트래픽 암호화 • 위험성이 없는 워크로드에 대한 탄력적인 네트워크 회복	• 마이크로 세그먼트를 통해 엔드포인트 및 애플리케이션 격리메커니즘 배포 • 비정상적인 데이터 흐름 격리 및 제거 • 자동화된 위험 인식 기반 동적 네트워크 규칙 생성	• 컨텍스트 기반 및 기계학습 기반 위협 보호 통합 • 암호화 민첩성 • 우선 순위 지정 가능한 동적 네트워크 규칙 생성
시스템	• 로컬 시스템 기반 ID/패스워드 등 단순인증 • 정적 속성 등 최소한의 권한 분리 정책 적용 • 온프레미스 시스템보안 패치 및 정책 수동 변경	• 독립적인 시스템으로 계정 관리 • 일부 중요도에 따르는 네트워크 세분화 • 온프레미스 및 클라우드 시스템에 대한 패치 수준 • 자동 확인 기능	• 동적 접근 권한 통제 • 등급 및 기능별 네트워크 분류 • 온프레미스 및 클라우드 시스템에 대한 자동화된 보안 패치	• 다중인증 및 신뢰도 기반 접근 인가 • 세분화된 리소스별 접근 정책 적용 • 온프레미스 및 클라우드 상의 모든 시스템 실시간 모니터링 및 자동화된 보안 패치
애플리케이션 및 워크로드	• 로컬 인가 및 정적 속성 기반 애플리케이션 접근 • 애플리케이션 워크플로우와 위협 보호에 대해 최소한의 통합 • 정적·수동테스트 수행	• 애플리케이션 워크플로우와 위협 보호에 대한 기본적인 통합 • CI/CD 파이프라인 DevSecOps, SBOM 적용 • 동적 테스트 방법 사용	• 확장된 컨텍스트 정보 및 최소권한 원칙의 애플리케이션 접근 • 애플리케이션 워크플로우와 위협 보호에 대한 강력한 통합 • 정기적인 자동화된 테스트	• 실시간 위험 분석을 통해 지속적 애플리케이션 인가 • 모든 애플리케이션에 사용자 및 단말 직접 접근 가능 • 자동화된 코드 배포 및 소프트웨어 검증
데이터	• 정적, 수동 데이터 분류 및 접근제어 • 온프레미스 및 암호화되지 않은 데이터 저장소 • 제한된 임시 데이터 분류	• 일부 자동화된 추적 기반 수동데이터 분류 및 목록화 • 최소한의 권한 요소를 통합한 데이터 접근 • 정적 레이블 및 수동 메커니즘 데이터 분류	• 속성에 기반한 최소 권한 제어기법으로 접근관리 • 저장소의 모든 데이터 암호화 • 레이블 지정 프로세스 계층화 및 데이터 목록화 자동화	• AI를 이용한 지속적인 데이터 분류 및 목록화 자동화 • 적시·최소권한 동적 데이터 접근 • 사용중인 데이터 암호화 및 최신 암호화 적용

자료: 과학기술정보통신부, 한국IR협의회 기업리서치센터

[2] 솔루션을 영구 라이선스로 판매하면 판매 연도에 매출 전액이 인식되는 반면, 구독형으로 전환하면 연간 일정 금액이 분산 인식된다. 구독형 비중 확대는 단기 매출 감소 요인으로 작용하나, 장기적으로는 수익 가시성과 안정성을 높인다.

파수AI 데이터보안 매출 추이



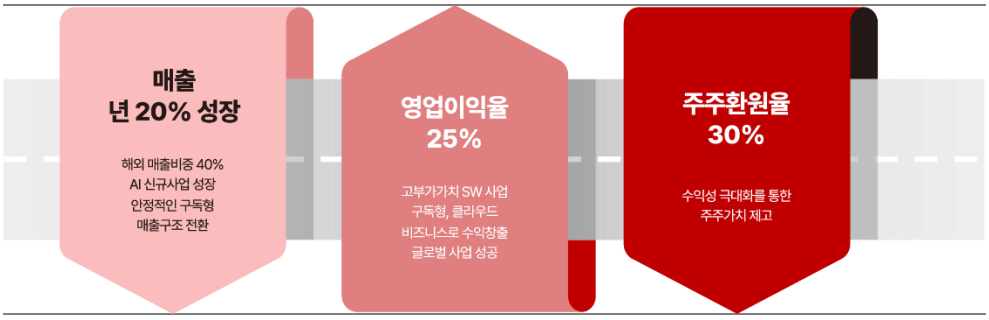
자료: 파수AI, 한국IR협의회 기업리서치센터

2 기업가치 제고 계획

파수AI는 2025년 6월, 2030년을 목표 연도로 하는 기업가치 제고 계획을 공시했다. 핵심 내용은 세 가지다. 연평균 매출 성장률 20%, 영업이익률 25%, 주주환원율 30%다.

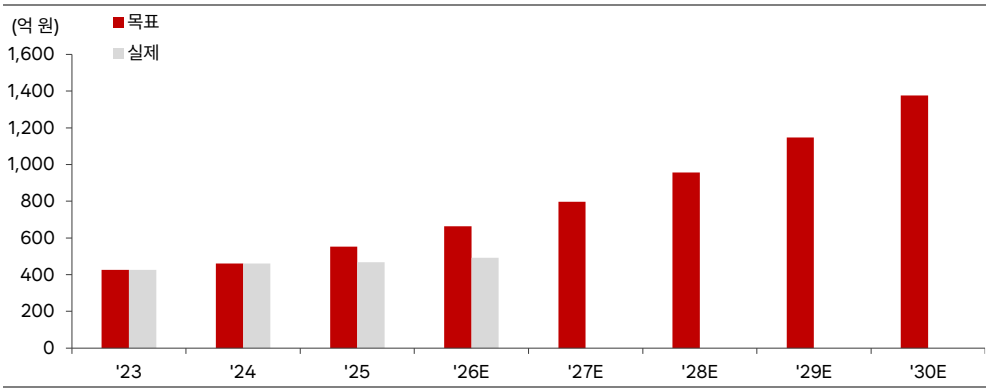
세 가지 목표 중 주주환원은 이미 궤도에 올라 있다. 2025년 배당성향은 42.5%로, 2030년 목표치인 30%를 이미 상회하고 있다. 반면 매출액과 수익성 목표는 현재 지표와 큰 간극을 보인다. 2025년 매출액 성장률은 1.2%에 그쳐 연평균 목표치인 20%에 미치지 못한다. 영업이익률 역시 2024년 8.5%에서 2025년 5.4%로 오히려 하락하며 목표치인 25%와 여전히 상당한 거리를 두고 있다. 결국 외형 성장을 통한 규모의 경제가 실현되어야만 고정비 부담을 낮추고 이익률을 끌어올릴 수 있다. 단순히 기존 사업의 비용을 줄이는 것만으로는 한계가 있는 만큼, 마진이 높은 신규 사업을 통해 매출 구조 자체를 다변화하는 전략이 병행되어야 한다.

파수AI 2030년 중장기 목표



자료: 파수AI, 한국IR협의회 기업리서치센터

2030년 매출 목표와 실제치



자료: 파수AI, 한국IR협의회 기업리서치센터

미국 시장, 기회이자 과제

2030년 목표 매출액은 1,377억 원으로, 2024년 461억 원 대비 약 3배 수준이다. 2025년 파수AI의 해외 매출은 20억 원으로 2030년 목표치 551억 원(2030년 매출의 40%)을 달성하기 위해서는 이미 진출해 있는 미국 시장에서 성공이 중요하다.

미국은 2021년 5월 바이든 행정부가 행정명령(EO 14028)을 통해 연방기관에 제로 트러스트 아키텍처 전환을 의무화하면서 시장의 방향이 빠르게 바뀌기 시작했다. 연방기관에는 2024년 9월까지 정체성·기기·네트워크·애플리케이션·데이터의 다섯 가지 제로 트러스트 목표를 달성하도록 요구했다. 전환이 완료된 것은 아니지만, 경계 기반 보안에서 데이터 자체를 보호하는 방식으로 무게중심이 이동하고 있다는 점은 파수AI에게 우호적인 환경이다.

다만 미국 시장 침투에는 현실적인 제약이 따른다. MS 365를 도입한 기업이라면 MS Purview를 통해 Teams, SharePoint, Exchange 등 자사 생태계 내에서 데이터 분류, 민감도 레이블 적용, DRM 기능을 기본으로 활용할 수 있다. 이미 MS 생태계 안에 보안 기능이 내재화되어 있는 셈이다. 그러나 MS Purview의 보호 범위는 MS Office 및 PDF를 포함한 약 20개 파일 형식에 한정되며, CAD·이미지·멀티미디어 등 비MS 포맷에 대한 지원은 제한적이다. 파수AI가 230개 이상의 파일 형식을 지원하며 SAP·Oracle 등 비MS 엔터프라이즈 시스템과 온프레미스 환경까지 커버한다는 점은, MS Purview가 닿지 못하는 영역에서 의미 있는 차별점이 될 수 있다. 다만 이 공간에서 고객사가 추가 도입을 결정할 만한 명확한 ROI를 제시할 수 있는지는 여전히 검증이 필요한 과제다. 글로벌 대형 고객사 레퍼런스가 아직 충분하지 않다는 점도 보수적인 현지 시장에서 넘어야 할 장벽이다.

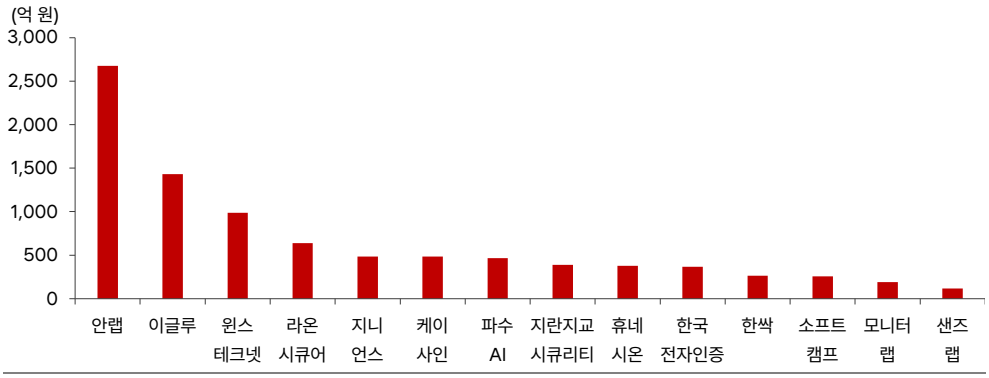
기업가치 제고 계획의 성패는 미국 시장에서의 성과로 귀결된다. 제로 트러스트로의 정책 전환과 MS Purview의 커버리지 공백은 파수AI에게 실질적인 진입 여지를 제공한다. 다만 현지화·레퍼런스 확보·추가 도입 명분 제시라는 과제가 남아 있는 만큼, 향후 미국 시장에서의 구체적인 수주 성과가 이 계획의 실현 가능성을 가늠하는 핵심 지표가 될 것이다.

2030년 매출 목표 달성 전략

자료: 파수AI, 한국IR협의회 기업리서치센터

2030년 국내 매출액 826억 원을 달성하기 위해서도 괄목할만한 성과가 필요하다. 국내 정보보안 시장은 특정 기능에 특화된 단품 솔루션 중심의 구조적 한계로 인해 개별 기업의 매출 규모가 크지 않다. 2025년 기준 상장사 중 연매출 1,000억 원을 상회하는 기업은 안랩과 이글루코퍼레이션 정도에 그친다. 2025년 447억 원의 매출을 기록한 파수AI가 5년 만에 두 배 가까운 국내 매출을 달성하려면, 기존 데이터 보안 사업의 점진적 확장만으로는 부족하다. 기업용 AI, DSPM 등 신규 솔루션에서 실질적인 매출 기여가 수반되어야 한다.

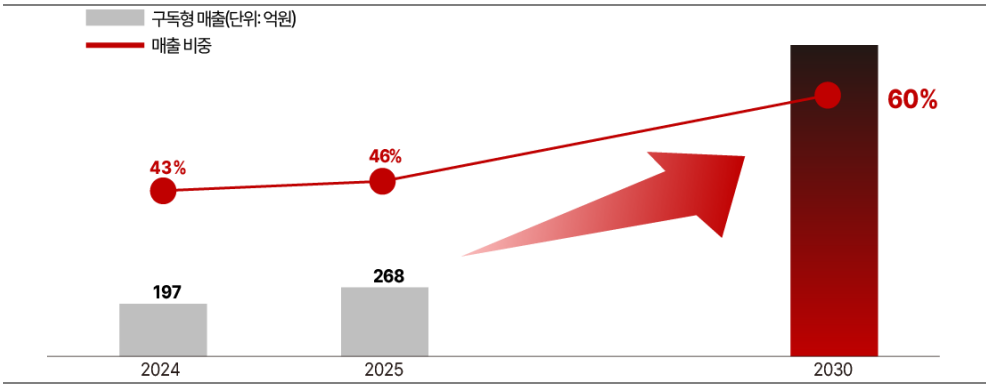
주요 정보보안 업체 매출액(2025년 연결 기준)



자료: 각사, 한국IR협의회 기업리서치센터

이와 병행하여 파수AI는 구독형 매출 비중을 2030년까지 60%로 끌어올리는 것을 목표로 하고 있다. 기존 영구 라이선스 계약을 연간 라이선스 방식으로 전환하는 작업은 이미 진행 중이며, 구독형 매출 비중은 2024년 43%에서 2025년 46%로 꾸준히 확대되고 있다. 90%를 넘는 유지관리 계약 갱신율이 기저를 받쳐주고 있다는 점을 감안하면, 구독 비중 60%는 달성 가능한 수준으로 보인다.

파수AI 구독형 비즈니스 전환 목표(2030년)



자료: 각사, 한국IR협의회 기업리서치센터

실적 추이 및 전망

1 지난 실적 점검

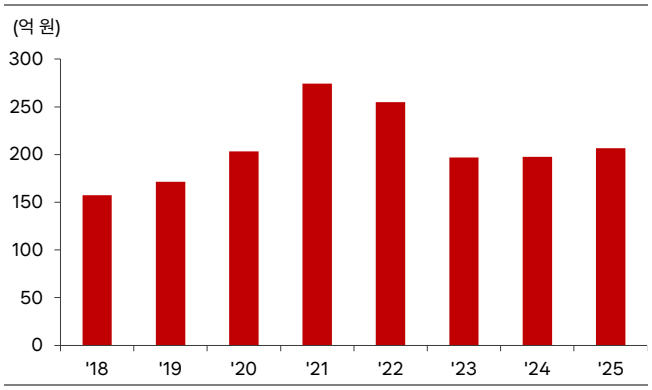
2025년 실적
매출액 467억 원(YoY +1%)
영업이익 25억 원(YoY -35%)

2019년 공공기관 및 기업들의 윈도우 10 업그레이드로 한 단계 도약한 매출액은, 코로나19로 인한 재택·원격근무 전환으로 2021년과 2022년에 추가 성장의 기회를 맞이했다. 잇따른 성장 동력이 폭발한 이후 이에 대한 반작용으로 데이터보안 부문의 매출은 2021년 275억 원을 정점으로 2023년~2025년에는 약 200억 원 수준에 그쳤다. 이에 더해 파수AI는 전략적으로 구독형 라이선스 판매 비중을 확대했는데, 영구 라이선스로 판매하면 판매 연도에 매출 전액이 인식되는 반면, 구독형으로 전환하면 연간 일정 금액이 분산 인식되어 단기 매출 감소 요인으로 작용했다.
그러나 누적된 설치 매출에 비례한 유지관리 매출이 2019년 77억 원에서 2025년 162억 원까지 확대되며 전사 매출액은 더디지만 성장을 이어갔다.

해당 기간에 2019년 말 202명이었던 직원 수는 2025년 말 281명까지 늘어났으며, 이에 따라 판관비 내 인건비는 2019년 90억 원에서 2025년 142억 원까지 증가했다. 연구개발비 규모 역시 2019년 32억 원에서 2025년 72억 원까지 확대됐다. 이 기간 파수AI는 Ellm, AI-R Privacy 등의 AI 제품을 개발하여 제품 라인업을 확대했다.

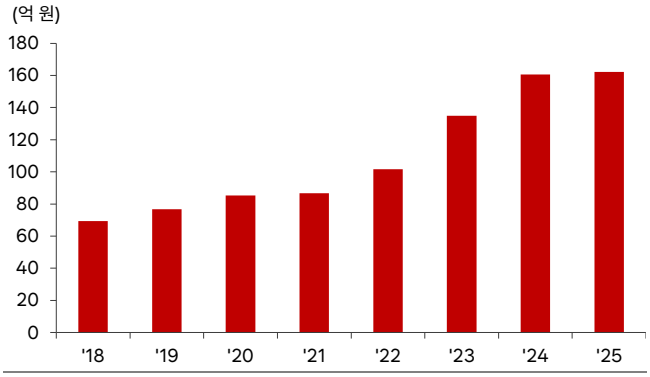
매출 확대가 가팔랐던 반면 비용 증가 속도는 완만했던 2022년에는 영업이익 52억 원(영업이익률 11.8%)으로 고점을 기록했으나, 이후 매출 정체와 비용 증가가 맞물리면서 2025년 영업이익은 25억 원(영업이익률 5.4%)에 그쳤다.

파수AI 데이터보안 매출 추이



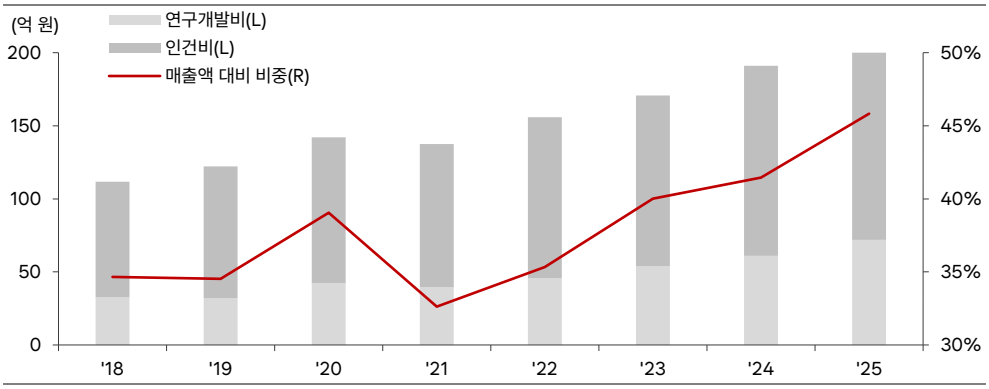
자료: 파수AI, 한국IR협의회 기업리서치센터

파수AI 유지보수 매출 추이



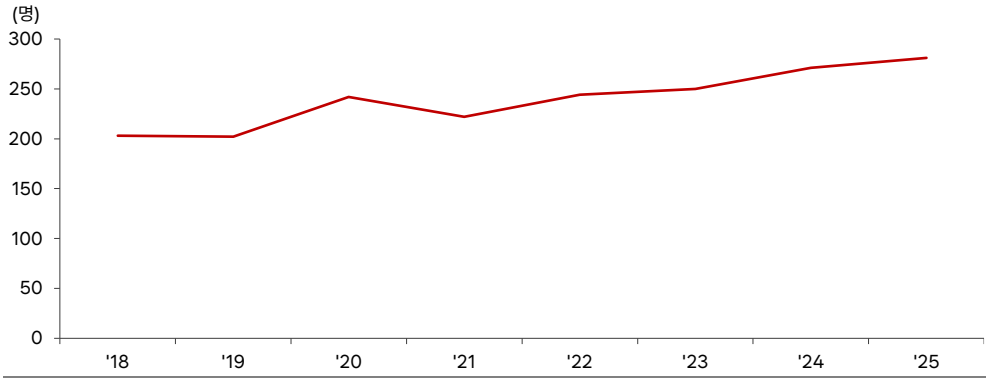
자료: 파수AI, 한국IR협의회 기업리서치센터

파수AI 연구개발비, 인건비 및 매출액에서 차지하는 비중 추이



자료: 파수AI, 한국IR협의회 기업리서치센터

직원 수 추이(연말 기준)



자료: 파수AI, 한국IR협의회 기업리서치센터

2026년 실적 전망

2026년 실적

매출액 492억 원(YoY +5%)

영업이익 31억 원(YoY +22%)

파수AI의 2026년 실적은 매출액 492억 원(YoY +5%), 영업이익 31억 원(YoY +22%), 영업이익률 6.3%(YoY +0.9%p)를 기록할 것으로 예상된다.

국가정보원은 2024년 9월 다층보안체계(MLS)를 처음 공개한 이후 이를 N2SF로 명명하고, 후속 가이드라인 제정과 실증사업을 이어가고 있다. 2025년 9월에는 'N2SF 보안 가이드라인 1.0'이 정식 발표됐고, 2026년 4월에는 총 45억 원(6개 과제 * 7.5억 원) 규모의 N2SF 도입 지원사업 입찰이 진행됐다. 정부 정책은 여전히 국내 정보보안 시장의 방향성을 결정하는 핵심 변수이나, N2SF는 아직 사업 초기 단계에 머물러 있다. 급변하는 보안 환경과 제로트러스트 강화 흐름 속에서도 국내 정보보안 산업은 특유의 생태계 구조로 인해 완만한 속도로 성장할 것으로 예상된다. 이를 반영하면 파수AI의 데이터보안 매출은 220억 원(YoY +6%), 애플리케이션 보안 매출은 88억 원(YoY +4%)으로 전망된다.

파수AI의 인력은 증가 추세를 이어가고 있다. 직원 수는 2023년 말 250명, 2024년 말 271명에서 2025년 말 281명으로 확대됐다. 급변하는 IT 인프라 환경에 대응하기 위한 기존 사업부의 연구개발 지속과 함께, 2024년 기업형 소규모 언어모델(sLLM) 솔루션 '일름(Ellm)' 출시 및 파로스네트웍스(OT·ICS 보안 전문)의 CPS(Cyber-Physical System) 사업부문 영업양수도 인수에 따른 인력 흡수가 주된 요인이다. 이에 연간 판매관리비 규모 역시 2023년 246억 원,

2024년 276억 원에서 2025년 300억 원으로 늘어났으며, 2026년에도 매출 확대에 대응하는 과정에서 전년 대비 16억 원 증가할 것으로 예상된다.

이로 인해 2026년 영업이익률은 6.3%로 전년 대비 0.9%p 상승하며 회복세를 보이겠으나, 판관비 부담으로 인해 2023년(8.9%)·2024년(8.5%) 수준에는 미치지 못할 전망이다.

2026년 1분기 실적

2026년 1분기는 매출액 90억 원(YoY +7%), 영업이익 -20억 원(전년동기 대비 적자 축소)을 기록했다. 분기별 변동성이 큰 애플리케이션 보안 매출이 10억 원(YoY +103%)을 기록했지만, 매출 비중이 가장 높은 데이터보안 매출은 36억 원(YoY -6%)에 그쳤다. 판매관리비는 77억 원으로 전년 대비 2억 원 증가했다.

파수AI 실적 추이 및 전망 (단위: 억 원)

구분	1Q25	2Q25	3Q25	4Q25	1Q26	2022	2023	2024	2025	2026E
매출액	84	107	104	171	90	441	427	461	467	**492**
데이터보안	38	45	33	91	36	255	197	198	207	**220**
애플리케이션 보안(종속회사 스패로우)	5	22	26	32	10	69	81	87	85	**88**
정보보호컨설팅	1	2	5	5	2	16	14	16	13	**16**
유지관리	40	38	41	43	42	102	135	161	162	**168**
매출비중										
데이터보안	45%	42%	31%	53%	40%	58%	46%	43%	44%	**45%**
애플리케이션 보안(종속회사 스패로우)	6%	20%	25%	19%	11%	16%	19%	19%	18%	**18%**
정보보호컨설팅	1%	2%	5%	3%	3%	4%	3%	3%	3%	**3%**
유지관리	47%	36%	39%	25%	46%	23%	32%	35%	35%	**34%**
영업비용(매출액-영업이익)	111	116	102	112	110	389	388	422	441	**461**
영업이익	-27	-9	3	59	-20	52	38	39	25	**31**
영업이익률	-32%	-9%	2%	35%	-22%	12%	9%	8%	5%	**6%**

자료: 파수AI, 한국IR협의회 기업리서치센터

Valuation

1 역사적 PBR

파수AI는 2026년 예상 PBR 1.1배로, 역사적 PBR 밴드 하단 수준에서 거래되고 있다.

정체 터널을 통과해 변화 초입으로

국내 DRM 산업은 윈도우 7 기술 지원 종료를 앞둔 2019년과 코로나19로 보안 수요가 급증한 2021년에 각각 정점을 기록한 이후 정체 국면에 진입했다. 같은 시기 글로벌 시장의 정보보안 강화 흐름에도 불구하고, 국내에서는 물리적 망분리 중심의 경직된 정책이 유지되면서 산업 구조의 변화가 다소 느린 편이었다. 그러나 2024년을 기점으로 N2SF 도입과 금융권 망분리 완화 등 새로운 보안 정책이 잇따라 발표되고 세부 가이드라인이 순차적으로 공개됨에 따라, 현재 정보보안 산업은 구조적 변화의 초입에 놓여 있다.

특히 제로 트러스트 환경에서 콘텐츠 보안이 강화되면서, 기업들은 당장 어떤 데이터가 어느 수준의 위험도를 가졌는지 식별하고 분류해야 하는 과제에 직면했다. 파수 데이터 레이더(FDR, Fasoo Data Radar)는 기업 내에 방대하게 쌓여있는 미분류 데이터와 방치된 파일들을 실시간으로 스캔하여 그 안에 담긴 민감도와 중요 정보를 평가할 수 있는 솔루션이다. 이에 따라 제로 트러스트 정책 강화 흐름과 맞물려 해당 솔루션에 대한 수요가 본격적으로 확대될 것으로 전망된다.

이처럼 한동안 정체되었던 파수AI의 데이터보안 사업이 긍정적인 전환의 계기를 맞이함에 따라, 주가 또한 역사적 PBR 하단 구간을 벗어날 수 있는 여건이 마련되고 있는 것으로 판단된다.

파수AI 역사적 PBR Band

자료: Quantiwise, 한국IR협의회 기업리서치센터

2 상대적 PBR

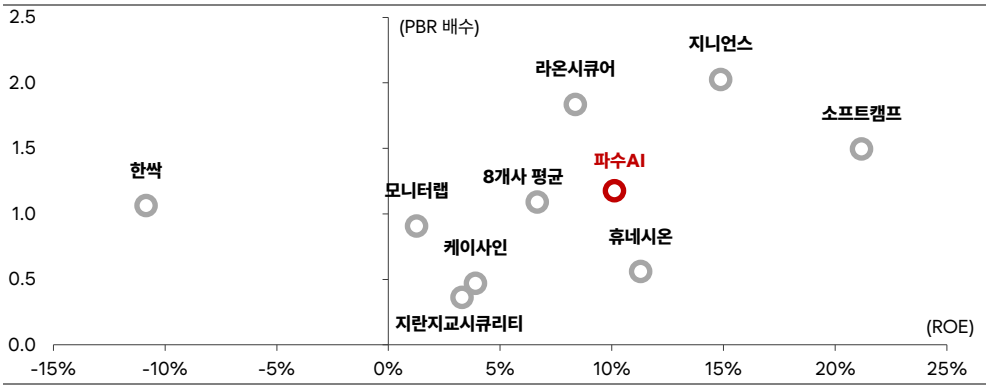
파수AI는 2026년 1분기말 BPS 기준 Trailing PBR 1.2배 수준에서 거래되어 비교 대상 기업 평균(1.1배)과 유사한 수준의 배수를 적용받고 있다. 비교 대상은 국내에 상장된 정보보안 업체 8개사로, 네트워크 보안·접근제어·인증·데이터보안 영역에서 파수AI와 매출 규모가 비슷한 기업들을 선정했다.

지난 12개월 실적(2026년 1분기말 기준) 측면에서는 이러한 Valuation 수준이 대체로 설명된다. 적정 PBR의 주요 변수인 ROE의 경우 파수AI는 10.1%를 기록하여 비교군 평균(6.7%)을 상회하고 있다. 다만 같은 기간 매출 성장률은 TTM 기준 2%에 그쳐 비교군 평균(13%) 대비 부진한 흐름을 나타냈으며, 이 두 요인이 상충하면서 결과적으로 배수상 프리미엄이 발생하지 않는 구조로 나타난 것으로 해석된다.

데이터 보안으로 무게 중심 이동

향후 전방 시장의 패러다임 변화 역시 파수AI의 Valuation에 영향을 미칠 요인으로 주목된다. 제로트러스트 아키텍처 논의에서 네트워크 경계 보안에 이어 데이터 중심 보안으로 무게중심이 이동하는 흐름은, 문서 DRM과 비정형 데이터 보안에 강점을 보유한 파수AI에 구조적으로 유리한 환경이다. 또한 생성형 AI 확산에 따른 기업 내 데이터 유출 리스크 증대는 문서 보안 솔루션 수요를 자극하는 요인으로, 파수AI가 보유한 AI 기반 데이터 분류·접근제어 기술의 차별화 가치가 재평가될 여지가 있다. 따라서 현재 평균 수준에 머물러 있는 Valuation 배수가 시장 환경 변화에 따라 점진적으로 재평가될 가능성이 있다.

동종업체 PBR-ROE(2026년 1분기 TTM 기준)



자료: Quantiwise, 한국IR협의회 기업리서치센터

동종업체 valuation

기업명	종가 (원)	시가총액 (억 원)	매출액(억 원) '24	'25	'2603 TTM	영업이익(억 원) '24	'25	'2603 TTM	영업이익률 '24	'25	'2603 TTM	ROE '24	'25	'2603 TTM	PBR(배) 25 (기말)	Trailing PBR
파수 AI	**3,655**	**428**	**461**	**467**	**472**	**39**	**25**	**32**	**9.2%**	**5.5%**	**6.9%**	**12.7%**	**7.3%**	**10.1%**	**1.3**	**1.2**
소프트캠프	4,410	220	169	257	263	-18	30	25	-7.8%	17.7%	9.5%	2.0%	27.9%	21.2%	2.3	1.5
휴네시온	2,940	282	369	377	383	32	48	45	11.7%	13.0%	11.9%	9.2%	11.8%	11.3%	0.7	0.6
한싹	3,145	343	205	263	256	-27	-19	-28	-7.9%	-9.5%	-10.5%	0.4%	-7.8%	-10.9%	1.6	1.0
지니언스	14,410	1,308	496	484	508	98	70	87	7.7%	14.1%	18.0%	20.3%	12.6%	14.9%	2.6	2.0
모니터랩	2,770	341	149	192	194	-6	9	7	-1.9%	6.3%	3.6%	5.7%	1.8%	1.3%	1.3	0.9
지란지교시큐리티	2,930	237	341	389	388	14	25	19	6.1%	7.3%	4.8%	-2.7%	3.7%	3.3%	0.5	0.4
케이사인	8,310	587	519	484	494	13	29	41	2.2%	5.6%	8.4%	1.9%	2.7%	3.9%	0.8	0.5
라온시큐어	8,850	983	625	638	623	20	28	37	2.0%	4.5%	5.9%	8.3%	6.5%	8.4%	1.8	1.8
정보보안업체 8 사평균			**359**	**385**	**388**	**16**	**27**	**29**	**1.5%**	**7.4%**	**6.5%**	**5.6%**	**7.4%**	**6.7%**	**1.4**	**1.1**

주: 종가는 2026년 6월 15일 기준

자료: Quantiwise, 한국IR협의회 기업리서치센터

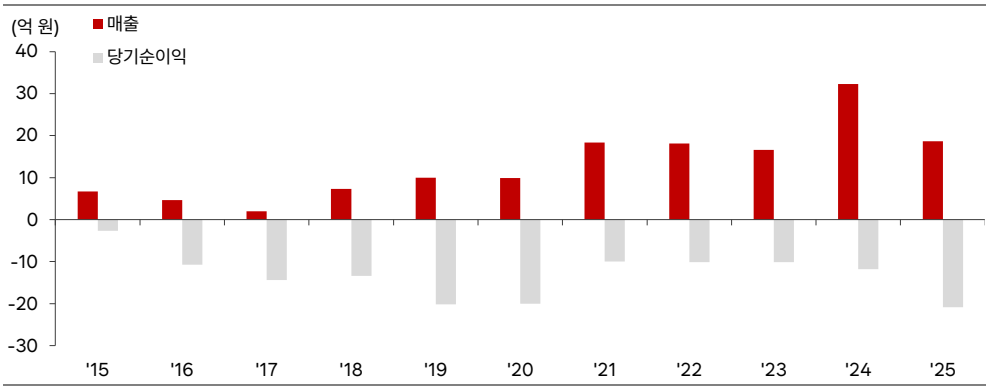
리스크 요인

1 심볼로직 출범과 AX 피벗 전략

파수AI는 2026년 6월, 기존 미국 법인(Fasoo, Inc.)을 현지 AI 플랫폼·컨설팅 기업 컨실릭스(Konsilix)와 합병해 AX(AI 혁신) 전문 법인 '심볼로직(Symbologic)'을 공식 출범했다. 초대 CEO는 AWS, Google Cloud, PwC 등을 거친 기업용 AI 전문가 롭 마라노(Rob Marano)가 맡았으며, 파수AI는 심볼로직을 통해 미국 중견·중소기업의 AX 수요를 선점한다는 전략이다.

다만 심볼로직의 출범 배경을 이해하기 위해서는 Fasoo, Inc. 시절의 실적을 먼저 짚어볼 필요가 있다. 2012년 캘리포니아에 설립된 이래 Fasoo, Inc.는 10년 이상 DRM 솔루션 중심의 미국 영업을 이어왔으나, 매출 규모와 수익성 모두 기대에 미치지 못했다. 2015년 이후 매출은 2~32억원 구간에서 등락을 반복했고, 당기순이익은 단 한 해도 흑자를 기록하지 못했다.

Fasoo, INC 연간 실적 추이



자료: 파수AI, 한국IR협의회 기업리서치센터

이러한 구조적 적자를 타개하기 위해 파수AI가 선택한 카드가 컨실릭스(Konsilix)와의 합병이다. 기존 Fasoo, Inc.의 사업 축이 DRM 솔루션 판매에 머물렀다면, 심볼로직은 데이터 보안·관리 역량 위에 AI 컨설팅과 에이전틱 AI 애플리케이션 구축 서비스를 결합한 AX 전문 법인으로의 피벗을 의미한다. 경쟁 강도가 상대적으로 낮은 미국 중견·중소기업 시장을 우선 공략 대상으로 설정한 것도 이 연장선상이다.

조규곤 파수AI 대표는 2026년 4월 기자간담회에서 심볼로직의 2027년 말 영업이익 흑자전환을 공개적으로 예고했다. 그러나 합병 이후 신규 시장 침투에 수반되는 초기 비용—컨설팅 인력 확충, 영업 인프라 구축, 브랜드 전환 비용 등—이 본격 집행될 경우, 단기 손익 측면에서는 추가적인 부담 요인이 될 수 있다.

한편 미국 매출 성장은 파수AI 기업가치 제고 계획의 달성 여부를 판가름할 핵심 축인 만큼, 손익과는 별개로 주시할 필요가 있다. 초기 비용 집행이 단기 손익을 압박하더라도 매출이 빠르게 확대된다면 2030년 목표 달성에는 긍정적으로 작용하지만, 매출 성장 속도마저 기대에 못 미칠 경우 밸류업 공약의 핵심 근거가 흔들릴 수 있다. 과거 10년간 누적 적자를 이어온 법인이 사업 모델 전환 이후 손익과 매출 두 축 모두에서 의미 있는 변화를 만들어낼 수 있을지, 그 진행 경과는 지속적인 모니터링이 필요한 대목이다.

포괄손익계산서

(억원)	2022	2023	2024	2025	2026F
매출액	441	427	461	467	492
증가율(%)	4.6	-3.3	8.1	1.2	5.4
매출원가	163	142	146	142	145
매출원가율(%)	37.0	33.3	31.7	30.4	29.5
매출총이익	279	284	315	325	347
매출이익률(%)	63.2	66.6	68.3	69.7	70.5
판매관리비	227	246	276	300	316
판관비율(%)	51.5	57.6	59.9	64.2	64.2
EBITDA	97	80	76	67	74
EBITDA 이익률(%)	22.0	18.9	16.6	14.4	15.0
증가율(%)	7.8	-16.9	-5.0	-12.1	10.1
영업이익	52	38	39	25	31
영업이익률(%)	11.8	8.9	8.5	5.4	6.3
증가율(%)	22.9	-26.6	2.2	-35.0	22.2
영업외손익	1	6	10	5	3
금융수익	6	10	13	9	4
금융비용	2	4	3	4	1
기타영업외손익	-3	-0	-0	-0	-0
종속/관계기업관련손익	0	0	0	0	0
세전계속사업이익	53	44	49	30	34
증가율(%)	39.0	-17.0	10.6	-38.1	12.7
법인세비용	0	-1	2	3	3
계속사업이익	53	45	46	27	31
중단사업이익	0	0	0	0	0
당기순이익	53	45	46	27	31
당기순이익률(%)	12.0	10.5	10.0	5.8	6.3
증가율(%)	28.4	-15.2	3.2	-41.0	14.7
지배주주지분 순이익	52	44	45	27	31

재무상태표

(억원)	2022	2023	2024	2025	2026F
유동자산	333	271	228	222	257
현금성자산	109	118	97	61	88
단기투자자산	124	79	35	45	49
매출채권	91	68	88	110	113
재고자산	0	0	0	0	0
기타유동자산	9	5	9	7	7
비유동자산	184	198	274	266	257
유형자산	34	20	42	26	15
무형자산	83	74	97	103	106
투자자산	25	60	89	93	95
기타비유동자산	42	44	46	44	41
자산총계	517	469	502	488	514
유동부채	117	68	75	75	79
단기차입금	30	0	0	0	0
매입채무	29	15	20	16	16
기타유동부채	58	53	55	59	63
비유동부채	75	52	60	32	34
사채	0	0	0	0	0
장기차입금	0	0	0	0	0
기타비유동부채	75	52	60	32	34
부채총계	193	119	135	107	113
지배주주지분	320	345	360	374	393
자본금	58	58	58	59	59
자본잉여금	91	93	93	94	94
자본조정 등	-12	-12	-21	-20	-20
기타포괄이익누계액	2	2	5	4	4
이익잉여금	180	203	225	237	256
자본총계	324	350	367	381	401

현금흐름표

(억원)	2022	2023	2024	2025	2026F
영업활동으로인한현금흐름	106	71	46	33	74
당기순이익	53	45	46	27	31
유형자산 상각비	16	17	20	22	21
무형자산 상각비	29	26	18	20	22
외환손익	1	1	1	2	0
운전자본의감소(증가)	-3	-30	-52	-56	1
기타	10	12	13	18	-1
투자활동으로인한현금흐름	-73	-8	-25	-40	-37
투자자산의 감소(증가)	5	-20	-23	-34	-2
유형자산의 감소	0	0	0	0	0
유형자산의 증가(CAPEX)	-1	-2	-5	-5	-10
기타	-77	14	3	-1	-25
재무활동으로인한현금흐름	-24	-54	-40	-29	-11
차입금의 증가(감소)	-10	-30	0	0	1
사채의증가(감소)	0	0	0	0	0
자본의 증가	0	0	0	0	0
배당금	0	-11	-11	-11	-11
기타	-14	-13	-29	-18	-1
기타현금흐름	-0	0	-1	-1	0
현금의증가(감소)	9	9	-20	-37	27
기초현금	100	109	118	97	61
기말현금	109	118	97	61	88

주요투자지표

	2022	2023	2024	2025	2026F
P/E(배)	20.3	25.2	12.7	19.4	13.7
P/B(배)	3.3	3.2	1.6	1.4	1.1
P/S(배)	2.4	2.6	1.2	1.1	0.9
EV/EBITDA(배)	9.2	11.6	6.3	6.5	4.1
배당수익률(%)	1.1	1.1	2.0	2.3	2.8
EPS(원)	448	377	384	228	261
BPS(원)	2,749	2,955	3,084	3,195	3,359
SPS(원)	3,793	3,663	3,949	3,992	4,204
DPS(원)	100	100	100	100	100
수익성(%)					
ROE	18.0	13.2	12.7	7.2	8.0
ROA	10.9	9.1	9.5	5.5	6.2
ROIC	32.5	27.2	24.3	13.3	17.4
안정성(%)					
유동비율	283.9	400.5	304.8	295.8	324.3
부채비율	59.5	34.1	36.9	28.2	28.2
순차입금비율	-53.3	-51.7	-26.7	-23.5	-29.9
이자보상배율	63.8	33.7	41.3	15.0	47.1
활동성(%)					
총자산회전율	0.9	0.9	0.9	0.9	1.0
매출채권회전율	4.7	5.3	5.9	4.7	4.4
재고자산회전율	N/A	N/A	N/A	N/A	N/A

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
파수AI	X	X	X

발간 History

발간일	제목
2026.06.17	파수-국내 매출 1위의 문서 보안 전문 기업
2025.05.29	파수-올해의 키워드는 AI, 글로벌 성과, 클라우드 전환
2022.03.28	파수-데이터보안 국내 1위 업체. 2022년 영업이익 YoY +94% 전망

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.