독립 리서치
GL RESEARCH

2025. 12. 17. 발간

사이버 보안 산업 리포트

연이은 대규모 정보 유출이 불러올 구조적 변화,
제도-수요-기술로 이어지는 성장 삼각편대

Analyst
박창윤, RA 김범태

現 지엘스토리 대표
금융투자분석사 포함 다수 자격 보유

前 메리츠증권, 아이엠투자증권

research@glstory.co.kr

지엘리서치
공식 홈페이지
QR코드 →

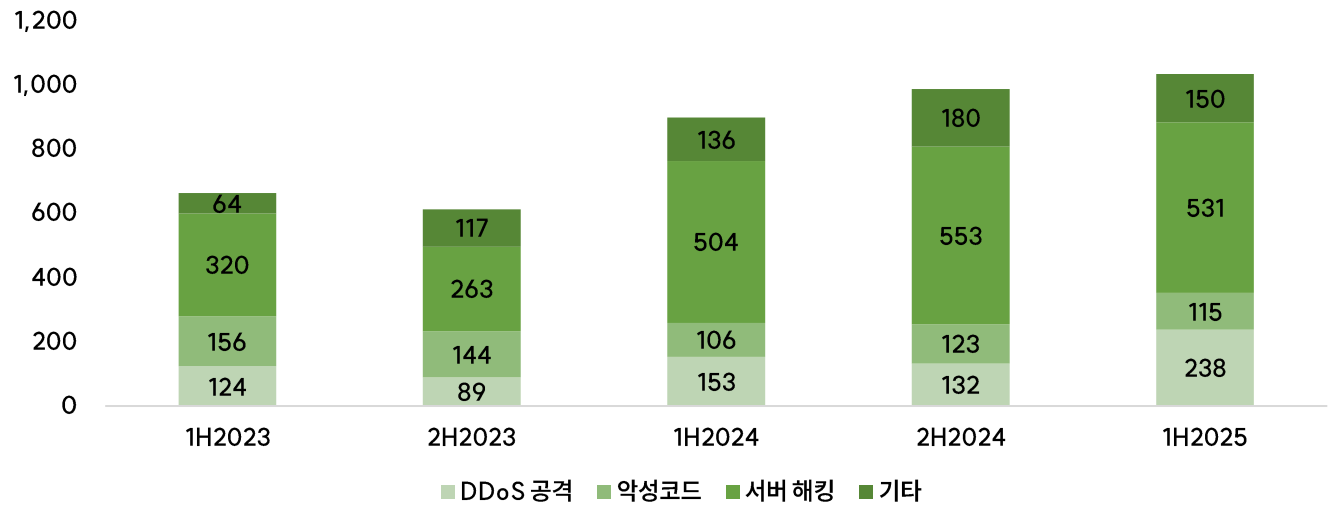
http://glstory.co.kr

Contents

1. AI의 도입과 가속화되는 사이버 공격

생성형 AI의 보편화 추세가 지속되며 에이전트 AI와 피지컬 AI로의 전환 국면에 진입하면서, 다양한 산업 전반에서 AI 도입이 빠르게 확산되고 있다. 한편 사이버 공격으로 인한 피해 사례 역시 증가하고 있다. 특히 2025년에는 국내 통신 3사 해킹 사고와 쿠팡의 대규모 고객 개인정보 유출 사태 등 중대한 정보보안 사고가 연이어 발생하며 기존 보안 체계의 한계를 명확히 드러냈다. 국가정보원은 지속적으로 증가하는 사이버 공격을 국가 안보 차원의 위협으로 규정하고 있으며, 이는 한국 보안 생태계 전반에 대한 근본적인 재정비가 필요함을 시사한다.

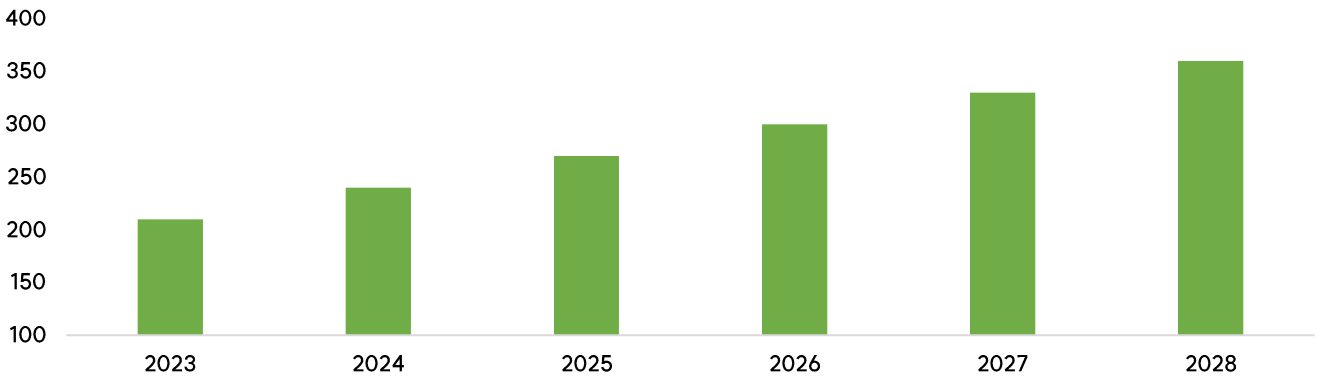
그림 1. 국내 사이버 침해사고 신고 통계 (단위 : 건)



자료 출처 : 한국인터넷진흥원, 지엘리서치

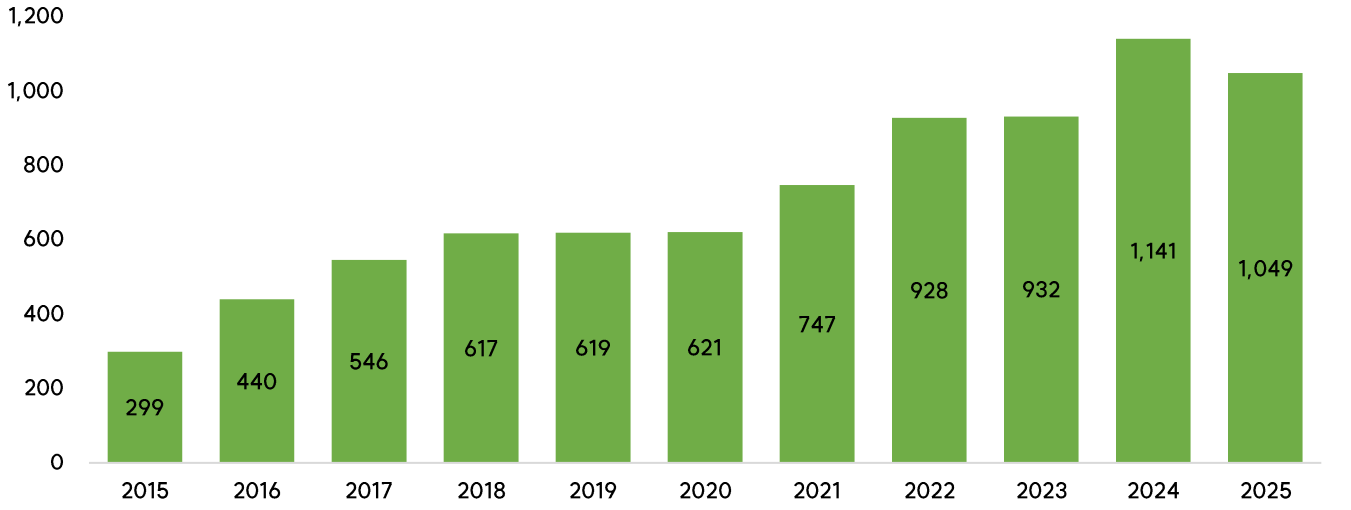
양자컴퓨터 기술의 발전으로 기존 공개키 암호체계(RSA·ECC)가 무력화될 가능성이 제기되면서, 글로벌 차원에서 양자 내성 암호(PQC) 도입을 위한 연구개발과 논의가 활발히 진행되고 있다. 여기에 AI 기반 사이버 공격의 고도화, OT 연결 확대, 클라우드 환경의 확산, 양자기술의 등장 등 사이버 보안 산업 전반의 구조적 변화는 향후 보안 투자 지출이 중장기적으로 지속 확대될 수 있는 환경을 형성하고 있다.

그림 2. 글로벌 사이버 보안 지출 성장세 (단위 : 십억 달러)



자료 출처 : IDC, 지엘리서치

그림 3. 과학기술정보통신부 – 정보보호, 사이버 보안 분야 R&D 예산 추이 (단위 : 억원)



자료 출처 :과학기술정보통신부, 지엘리서치

사이버 보안에 대한 필요성과 요구 수준이 지속적으로 높아짐에 따라 관련 예산 지출 역시 빠르게 증가할 것으로 예상된다. 이러한 환경 변화는 사이버 보안 산업 내 기업들에 대한 재평가 기회를 제공할 가능성이 크다. 궁극적으로 사이버 보안은 AI 기술의 발전과 병행해 동반 성장할 수밖에 없는 핵심 영역이다.

2. 2026년 주목할 사이버 보안 산업 트렌드

2026년 사이버 보안 산업의 핵심 트렌드는 크게 세 가지로 요약된다.

첫째, 제조·발전·정유·철강 등 핵심 산업 전반에서 **산업제어(OT) 시스템** 보안의 중요성이 빠르게 부각되고 있다. 기존 VPN·방화벽 중심의 원격접속 방식은 사용자 식별과 세분화된 접근통제가 어려워 구조적 한계를 노출하고 있으며, 이에 따라 OT 원격접속 통제, 망 연계 보안, 세션 모니터링 등을 포함한 안전한 OT 운영환경 구축 수요가 빠르게 증가하고 있다.

둘째, '지속적 검증'과 '최소 권한'을 핵심으로 하는 제로트러스트 보안 모델이 공공·금융·대기업을 중심으로 본격 확산되고 있다. 특히 클라우드 환경에서는 ID 기반 접근관리(IAM), 다중요소인증(MFA), ZTNA가 필수 보안 아키텍처로 자리 잡고 있으며, 국내 정책 및 규제 환경 또한 이러한 전환을 가속화하고 있다.

셋째, 양자내성암호(PQC)는 글로벌 차원에서 차세대 표준 암호체계로 부상하고 있다. 미국 NIST의 PQC 표준화는 통신·금융·공공기관을 중심으로 암호 모듈, VPN, 전자서명 및 인증 인프라 전반의 교체 수요를 촉발하는 초기 투자 사이클을 형성하고 있다.

3. 주요 기업 분석

위에서 제시한 세 가지 사이버 보안 산업 트렌드에 부합하는 국내 주요 기업으로는 망 연계·OT 보안 중심의 휴네시온, 양자내성암호(PQC)·인증·IAM 기술을 보유한 라온시큐어, OT 및 융합보안 컨설팅 역량을 강화하고 있는 싸이버원이 대표적이다.

1) 휴네시온 (290270)

공공·금융·민간 2,000여 고객사를 기반으로 10년 연속 국내 망연계 시장 점유율 1위를 유지하는 보안 인프라 전문기업이다. 망연계부터 접근제어·계정권한관리·NAC 등 국내 유일 풀 라인업을 구축해 고객사 맞춤형 설계와 강한 Lock-in을 확보하고 있다. 정부의 N²SF 전환, 공공·금융 클라우드 전환 확대 속에서 성능 증설·모듈 확장·유지보수 매출이 결합되는 구조적 성장 단계에 진입하고 있다.

2) 라온시큐어 (042510)

제로트러스트 기반 인증·접근관리 플랫폼(OnePass·OneGuard·wiseaccess)을 중심으로 공공·금융·대기업에 안정적으로 공급해 온 국내 대표 신원·접근보안 전문 기업이다. 동시에 OmniOne 블록체인 DID, IDaaS 신원인증, 프리미엄 모의해킹·PTaaS 등 고부가 서비스 사업을 확대하며 '신원 기반-전자보안 생태계'를 아우르는 성장 구조를 구축하고 있다. 글로벌 인증 수요 증가와 화이트햇 구독형 보안 확산이 동사의 중장기 성장 모멘텀을 강화하고 있다.

3) 싸이버원 (356890)

보안관제·보안컨설팅·클라우드 전환·보안솔루션을 아우르는 통합 보안 서비스를 제공하며, 자체 개발한 통합보안관제 플랫폼을 기반으로 효율성과 수익성을 강화하고 있는 정보보안 기업이다. 엑스큐어넷 인수를 통해 국내 대기업 고객사 기반을 확보하며 고객 포트폴리오를 확장했고, PROM SIEM·내부정보유출방지 솔루션을 앞세운 베트남 시장 진출로 해외 매출 다각화에 나서고 있다.

1. OT 보안

OT 보안, 우리의 생활과 밀접한 OT 시스템을 노리는 사이버 공격을 막는다

OT디지털전환가속
보안취약성확대

OT(Operation Technology) 시스템은 산업 설비의 운영과 제어를 담당하며, 하드웨어·소프트웨어를 통해 물리적 프로세스를 실시간 관리하는 기술이다. 과거에는 폐쇄형 네트워크로 운영됐지만 IoT, 빅데이터, 클라우드, AI의 도입으로 외부와 연결되는 '개방형 환경'으로 전환되면서 사이버 공격 노출도가 크게 높아졌다.

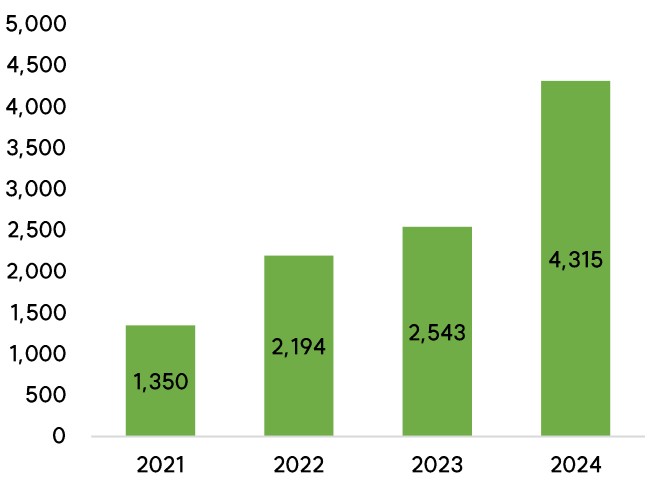
OT보안의본질
무결성,안전성,가용성확보

OT 환경에서의 사이버 공격은 단순한 정보 유출이나 업무 중단을 넘어 국가 기반 인프라와 산업 운영 자체를 위협할 수 있다는 점에서 파급력이 크다. OT 보안의 핵심은 산업제어시스템(ICS)을 포함한 실제 운영 환경의 **무결성, 안전성, 가용성**을 확보하는 데 있으며, 이는 데이터 보호를 중심으로 하는 IT 보안과 본질적으로 구분되는 영역이다. 최근 제조라인 자동화, 노후 설비의 디지털 관리, 교통·수처리 등 국가 인프라 전반의 디지털 전환이 가속화되면서 OT 보안의 전략적 중요성은 더욱 확대되고 있다.

글로벌OT시스템
사이버공격사례증가

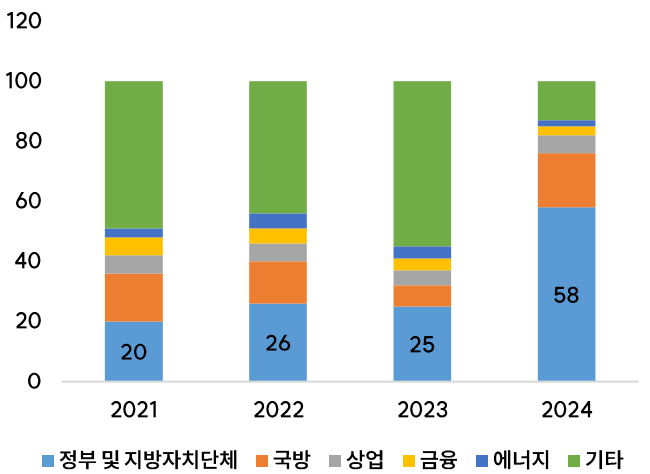
실제 공격 사례도 잇따르고 있다. 2025년 8월 노르웨이의 한 수력발전 댐에서는 해커가 웹 기반 제어 시스템의 권한을 탈취해 약 4시간 동안 수문이 열리는 사고가 발생했다. 또한 우크라이나는 러시아와의 전쟁 기간 중 2025년 상반기에만 3,000건이 넘는 사이버 공격을 받았으며, 이 중 상당수가 발전소·통신·운송 등 국가 핵심 인프라를 겨냥한 것으로 확인됐다. 이처럼 OT 시스템은 국가 안보와 산업 운영에 직결되는 영역으로, 향후에도 보안 강화를 위한 투자가 필수적인 전략 분야로 평가된다.

그림 4. 우크라이나, 사이버 공격 피해 건수



자료 출처 :우크라이나 국가사이버보호센터, 지엘리서치

그림 5. 우크라이나, 사이버 공격 피해 비중 (단위 : %)



자료 출처 :우크라이나 국가사이버보호센터, 지엘리서치

다양한 산업에 적용되는 AI, 없어서는 안될 OT 보안

OT보안의본질
무결성,안전성,가용성확보

산업 현장에서 인터넷과 AI 활용이 본격화되면서 IT와 OT의 통합이 빠르게 진행되고 있다. 제조업은 단순 자동화 단계를 넘어 데이터 기반의 지능형 생산 체계인 스마트 팩토리로 전환되고 있으며, 이는 기존의 '소품종 대량생산'에서 소비자 맞춤형 다품종 소량생산 체계로의 구조적 변화를 이끌고 있다.

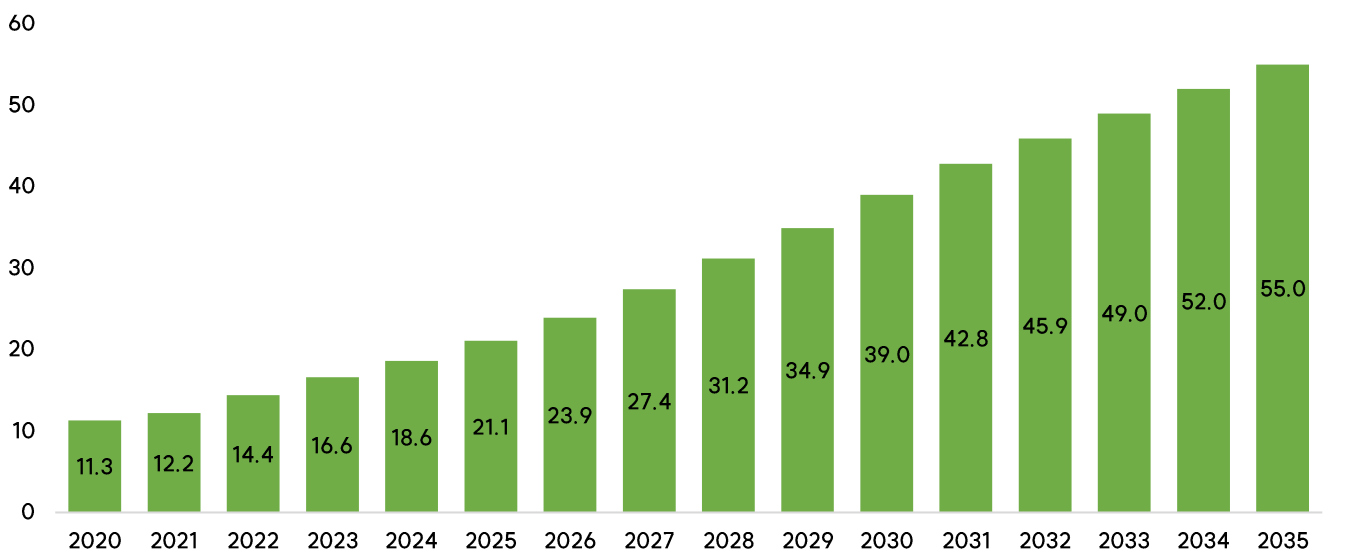
CPS구현으로생산지능화진전
동시에공격면확대

이와 함께 IT 기술은 공장 설비 중심의 OT 영역으로 확장되고 있다. 센서, 제어 장치, 로봇 등이 IoT 기반으로 연결되고, 현장 데이터를 실시간 분석해 생산 공정을 자동 조정하는 사이버-물리 융합 시스템(CPS)이 구현되면서 효율성이 크게 높아지고 있다. 반면 OT 시스템이 IT 네트워크, 클라우드, 원격 제어 환경과 연결되면서 외부 노출이 확대되어 사이버 취약성도 증가하고 있다. 최근에는 발전·교통·수자원·제조설비 등 공공 및 산업 인프라를 겨냥한 공격이 늘고 있으며, 이는 단순한 데이터 손실을 넘어 국가 시스템 마비로 이어질 위험을 내포한다.

OT특화보안기술
전략적중요성부상

이에 따라 OT 환경에 특화된 보안 기술 도입의 필요성이 더욱 부각되고 있다. OT 전용 프로토콜 분석, 실시간 이상징후 탐지, 물리적 공정 데이터를 활용한 비정상 행위 식별 등 고도화된 보안 기술의 중요성이 커지고 있으며, 물리 설비에서 기업 네트워크까지 이어지는 전 주기 통합 보호 체계 구축이 핵심 과제로 부상하고 있다.

그림 6. 글로벌 IoT 시장 전망치 (단위 : 십억 개)



자료 출처 : IoT – Analytics, 지엘리서치

OT 보안의 핵심 기술 요소

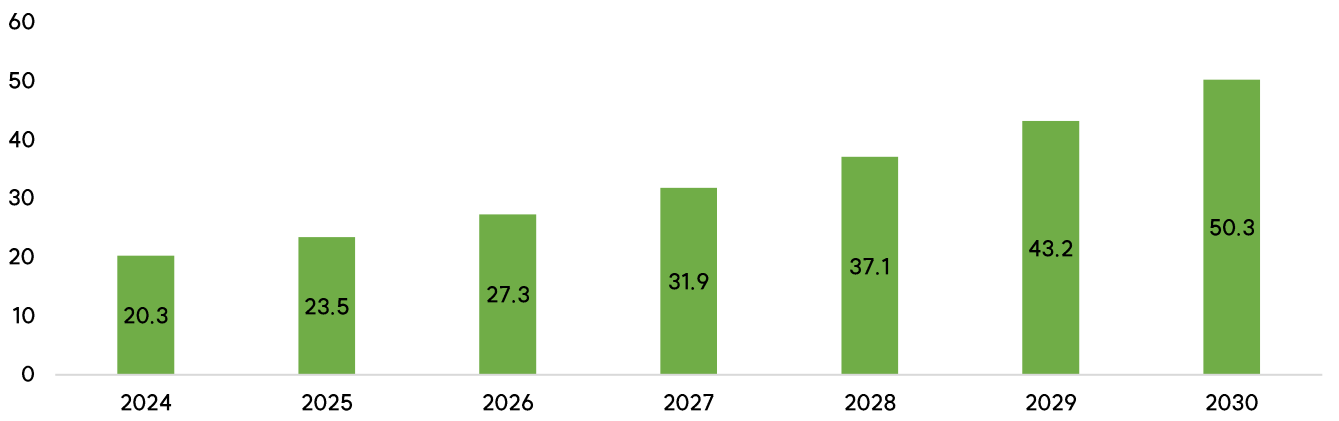
OT보안3대핵심기술
(1) 가시성및자산관리
(2) 위협탐지및분석
(3) 접근제어및보호

OT 보안의 핵심 기술은 세 가지로 구분된다. 첫째, **가시성 및 자산 관리**는 OT 네트워크에 연결된 수백~수천 개의 장비와 시스템을 식별·관리하는 기술로, 실제 산업 현장에서는 모든 자산을 정확히 파악하지 못하는 경우가 많아 필수적인 영역이다. 둘째, **위협 탐지 및 분석**은 OT 네트워크에서 발생하는 비정상 트래픽·행위를 식별해 공격 가능성을 조기에 탐지하는 기능이다. 셋째, **접근제어 및 보호**는 OT 시스템에 대한 접근 권한을 통제하고 외부 위협으로 부터 설비와 운영 환경을 보호하는 기술을 말한다.

글로벌OT보안시장
CAGR16%고성장

OT 보안 시장은 산업 디지털 전환이 본격화되면서 빠르게 성장하고 있다. 시장조사기관 Markets and Markets는 OT 보안 시장 규모가 2025년 234.7억 달러에서 5년 후 502.9억 달러로 확대될 것으로 전망하며, 연평균성장률(CAGR)은 약 16.5%에 달할 것으로 보고 있다.

그림 7. OT 보안 시장 성장 추이 (단위 : 십억 달러)



자료 출처 : Markets and Markets, 지엘리서치

OT보안시장성장요인

OT 보안 시장 성장을 견인하는 구조적 요인은 네 가지로 요약된다. **첫째, 스마트 팩토리 확산**으로 OT 네트워크가 클라우드·IoT와 직접 연결되면서 공격 표면이 크게 확대됐다. **둘째, 스마트시티, 로봇, 자율주행 등 물리 인프라의 디지털화**가 진행되며 실시간 데이터 제어의 안전성 확보가 핵심 과제로 부상하고 있다. **셋째, 국제 표준 준수 요구**와 함께 주요 국가들의 산업용 보안 인증 제도 도입이 강화되고 있다. 마지막으로 일본 JGC 플랜트 해킹과 같은 사이버-피지컬 사고 사례가 증가하며, **OT 보안이 기업의 필수 리스크 관리 영역으로 인식**되기 시작한 점도 시장 확대를 가속하고 있다.

그림 8. 산업 시설 사이버 공격 발생 지점 현황 및 사례

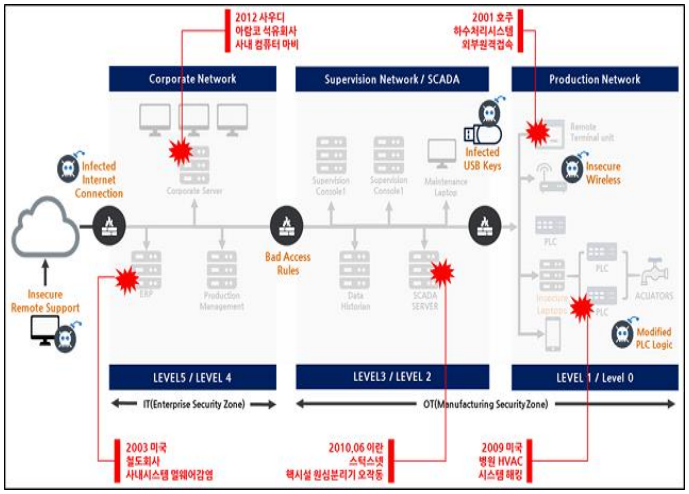


그림 9. 산업 시설 보안 위협 발생지점별 위협 요소

구분	상세 보안 위협
악의적 활동	서비스 거부, 멀웨어, 하드웨어 및 소프트웨어 조작, 정보 조작, 표적 공격, 개인정보 악용, 무차별 대입 공격
도청	중간자 공격, IoT 프로토콜 하이재킹, 네트워크 정보노출
물리적 공격	직,간접적인 시설 파괴
사고	의도하지 않은 데이터 또는 구성 변경, 장치 및 시스템 오용, 제3자에 의한 손실
고작/오작동	센서, 액추에이터의 고장 또는 오작동, 제어 시스템 고장 또는 오작동, 소프트웨어 취약점 악용
정전	통신 네트워크 중단, 전원 공급 중단, 지원 서비스 손실
위법	개인정보보호 위반, 계약사항 미이행
재해	자연재해, 환경재해

자료 출처 : 한국인터넷진흥원, 지엘리서치

국내OT보안정책강화
KISA가이드,정부예산지원확대

국내에서도 OT 보안 수요가 빠르게 증가하고 있다. 한국인터넷진흥원(KISA)은 '스마트 공장 사이버보안 가이드'를 마련해 자산관리, 접근통제, 데이터 보호, 사고 대응 등 세부 보안 기준을 제시하고 있으며, 산업통상자원부와 중소벤처기업부 역시 스마트 팩토리 보안 내재화를 위한 예산 지원을 확대하고 있다.

AI기반자율대응기술상용화

OT 보안은 AI·자동화·표준화가 결합된 융합 보안 체계로 발전하고 있다. AI 기반 딥러닝을 통해 비정상 트래픽을 자동 식별하고 위협 수준에 따라 자율 대응하는 기술이 상용화 단계에 진입했으며, 다중 인증·통합 인증 도입으로 사용자 신뢰성도 강화되고 있다. 또한 탐지–분석–대응 과정을 하나의 흐름으로 통합하는 보안 자동화 플랫폼이 확산되며 OT 환경 전반의 보안 운영 효율성이 높아지고 있다.

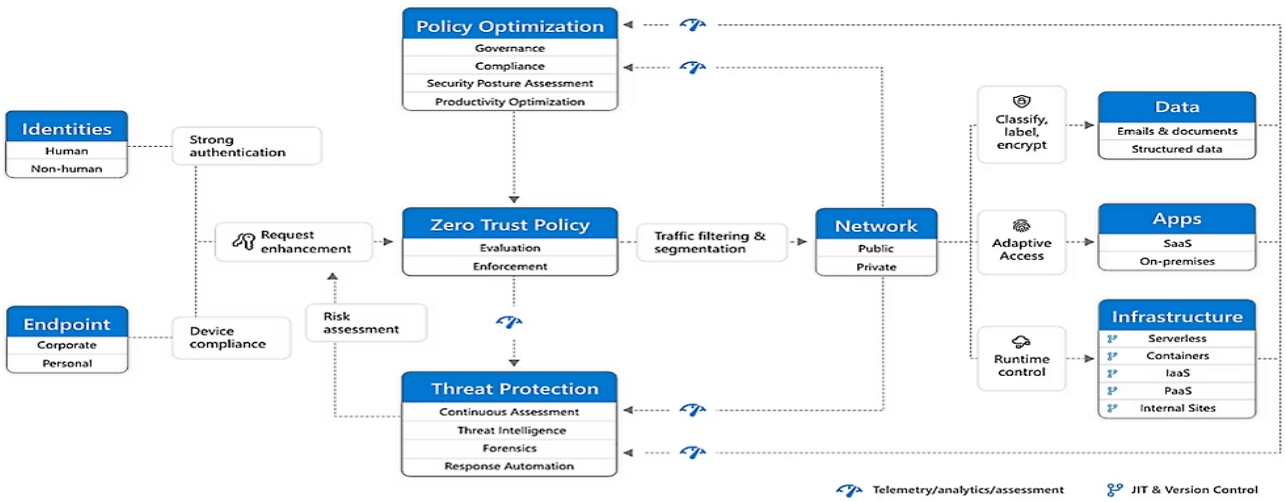
2. 제로트러스트 보안

제로트러스트 보안 이란?

경계기반보안의한계
제로트러스트보안모델부상

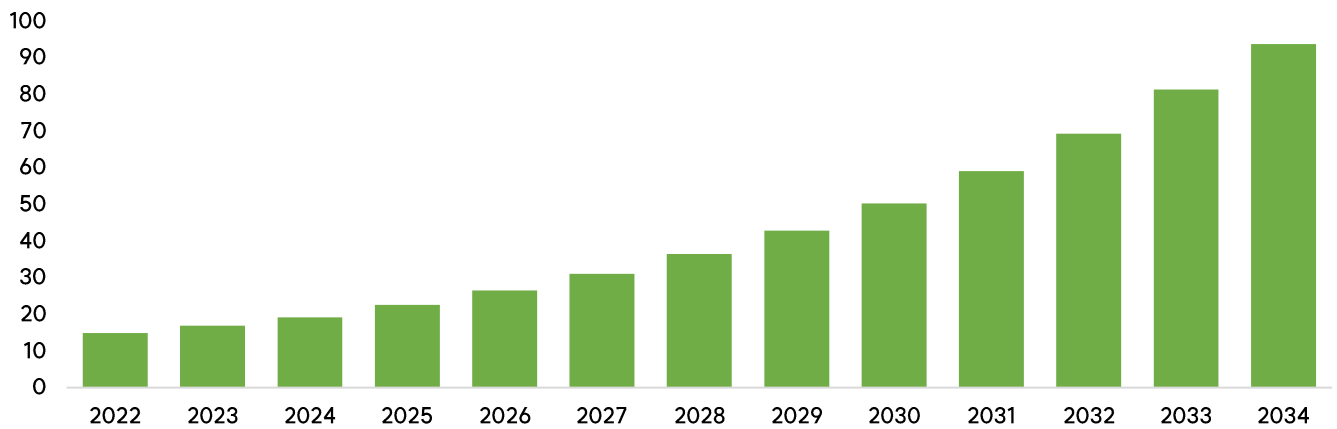
제로트러스트(Zero Trust)는 "기본적으로 아무도 신뢰하지 않는다"는 원칙을 기반으로 하는 보안 아키텍처다. 기존 경계 기반 보안이 내부 네트워크를 안전지대로 가정하고 외부만 방어했다면, 제로 트러스트는 내부·외부를 구분하지 않고 모든 사용자, 기기, 세션, 애플리케이션을 지속적으로 검증한다. 클라우드, 모빌리티, 원격근무 확산으로 경계가 모호해지면서 기존 방식만으로는 공격을 방어하기 어려워졌고, 이에 강력한 인증, 최소 권한, 행위 기반 정책을 결합한 제로 트러스트 모델이 글로벌 표준으로 자리 잡고 있다.

그림 10. 마이크로소프트에 적용되는 제로트러스트 보안 모델 구조



자료 출처 : 마이크로소프트, 지엘리서치

그림 11. 글로벌 제로트러스트 보안 시장 전망 (단위 : 십억 달러)



자료 출처 : GMI, 지엘리서치

제로트러스트확산
금융,의료,공공 중심

제로트러스트 보안은 금융, 의료, 공공 분야를 중심으로 빠르게 확산되고 있다. 금융 부문은 고객 데이터 보호와 규제 준수를 위해 적극 도입하고 있으며, 의료 부문 역시 민감한 환자 정보 보호를 위해 적용이 확대되고 있다. 공공 부문의 경우 N^2SF를 통해 데이터 등급 분류 및 평가 체계가 마련되면서, 다른 산업보다 빠른 속도로 제로 트러스트 도입이 추진될 것으로 전망된다.

제로트러스트핵심원칙
(1) 지속적인증
(2) 최소권한접근
(3) 마이크로세분화

제로트러스트는 **지속적 인증**, **최소 권한 접근**, **마이크로 세분화**를 핵심 원칙으로 한다. 지속적 인증은 사용자 세션을 일회성 인증이 아니라 실시간 위험 평가를 통해 계속 검증하는 방식이며, 최소 권한 접근은 직원·계약자·서비스에 필요한 만큼의 권한만 부여해 잠재적 피해 범위를 줄인다. 마이크로 세분화는 자원을 더 잘게 나누어 침해가 발생하더라도 lateral movement(수평 확산)를 차단하는 기술이다.

시장 조사업체에 따르면, 글로벌 주요 기관의 81%가 제로 트러스트 모델을 도입했으며 나머지 19% 또한 도입할 계획을 갖고 있다고 한다. 사실상 모든 기업이 제로 트러스트 모델을 도입할 것으로 전망된다.

그림 12. 제로트러스트 보안 모델 핵심 구성 요소

구성요소	정의	핵심 기능	목적 / 효과
IAM (신원 및 접근 관리)	사용자 계정·권한을 중앙에서 통합 관리하는 ZT 핵심 인프라	SSO 기반 단일 로그인 – RBAC/ABAC 권한 모델 – 통합 ID 저장소·인증 체계 – 계정 탈취·오남용 방지	모든 접속 요청의 "누가 접근하는가"를 검증하고 권한을 최소화
MFA (다중요소 인증)	비밀번호 외 2개 이상의 인증요소로 사용자 검증	지식/소지/생체 기반 인증 – 적응형MFA(위치·디바이스·위험도 기반)– FIDO 기반 패스워드 리스 인증	탈취된 비밀번호로는 침해가 불가능하도록 계정 방어력 강화
ZTNA (제로 트러스트 네트워크 액세스)	VPN 대신 사용자·디바이스가 허용된 애플리케이션만 접근하도록 제한	애플리케이션 단위 접근 제어 – 세션 단위 인증·인가 – SASE와 통합 운영	내부망 전체 오픈 없이 필요한 서비스만 최소 접근 → 공격 표면 축소
마이크로 세그멘테이션	네트워크를 워크로드·애플리케이션 단위로 세분화하여 내부 확산 차단	워크로드 기반 정책 – 세밀한 동서(East-West) 트래픽 제어– Lateral Movement 차단	침해 발생 시 내부 확산을 구조적으로 차단
정책 엔진 (Policy Engine)	사용자·디바이스·위험도 신호를 종합해 접근 허용 여부를 자동 의사결정	조건부 액세스– 위험 기반 정책 평가– 정책 관리자(PA)·정책 집행점(PEP)과 연동	실시간으로 "접근 허용/차단/추가 인증"을 결정하는 두뇌 역할
분석 및 모니터링	모든 인증·접속 이벤트를 실시간 분석해 이상행위 탐지 및 정책 자동 조정	UEBA·Threat Analytics – SIEM 기반 로그 분석– 이상행위 탐지 → 세션 차단·재인증	Zero Trust의 연속적 검증(Continuous Verification) 구현

자료 출처 : 산업 자료, 지엘리서치

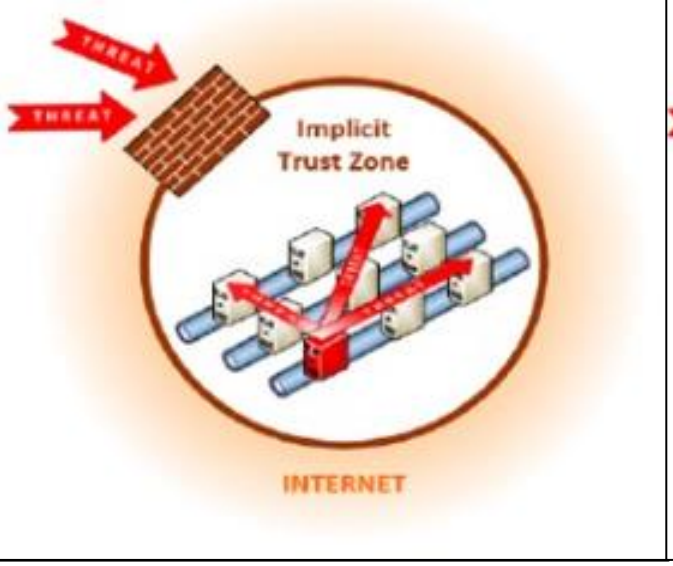
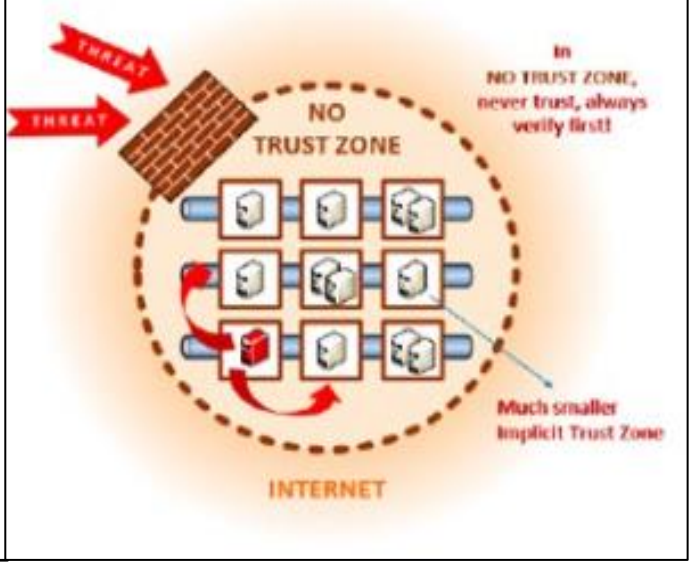
AI 도입으로 사이버 공격 표면 확대, 제로트러스트 보안 전략 부상

AI,원격근무,클라우드확산
사이버공격표면확대

AI 도입과 사이버 공격의 고도화로 제로 트러스트가 핵심 보안 전략으로 부상하고 있다. 코로나19 이후 원격 근무 확산과 클라우드 사용 증가로 기존의 내부 네트워크를 전제한 신뢰 기반 보안 방식의 한계가 드러나고 있는 상황이다.

기업 데이터는 온프레미스뿐 아니라 멀티클라우드, SaaS, IoT, 엣지 디바이스 등 다양한 환경으로 분산되었고, 구성원은 언제 어디서나 접속할 수 있게 되었지만 이는 동시에 공격 표면의 확대를 의미한다. 이로 인해 기업과 기관은 데이터 유출, 랜섬웨어 등 사이버 위협에 더욱 취약해지고 있다.

그림 13. 제로트러스트 보안 모델 핵심 구성 요소

제로 트러스트 도입 전 (경계 기반 보안 모델)	제로 트러스트 도입 후 (제로 트러스트 보안 모델)
• 경계를 기준으로 한번 인증된 기기 또는 사용자의 트래픽은 모두 허가 → VPN, 방화벽 등 • 내부자에게 높은 신뢰도를 부여하는 기존 모델의 약점을 공략하기 위해 내부자 권한 탈취를 통해 공격 사례 증가 우려	• 네트워크 혹은 물리적 위치, 기기에 상관없이 '무신뢰(Zero Trust)' 원칙 (Never Trust, Always Verify) • 강화된 인증 및 기기 상태 모니터링 등으로 지속적인 인증을 통해 전급 권한 부여
	

자료 출처 : 과학기술정보통신부, 지엘리서치

쿠팡 개인정보 유출 사태의 원인, 제로트러스트 보안과 내부 통제 관리도 핵심

쿠팡개인정보유출피해심화
내부통제시스템미흡

2025년 11월 18일 쿠팡 회원 약 4,500명의 이름·이메일·주소 등 개인정보가 유출된 사실이 언론을 통해 알려졌으며, 당시 쿠팡은 결제정보는 유출되지 않았다고 밝혔다. **그러나 이후 29일, 무단 노출된 고객 계정이 총 3,370만 개에 달한다고 발표하면서 유출 규모는 최초 보고 대비 약 7,500배 확대**되었고, 사실상 대부분의 고객 정보가 유출된 것으로 확인됐다. 이번 사태는 내부 직원에 의해 발생한 사고로, 쿠팡의 보안 체계가 외부 침입 대응에만 집중되어 있고 내부 통제 체계가 부재했다는 점이 핵심 원인으로 지적되고 있다.

쿠팡 개인정보 유출 사태와 관련해, 국회 과학기술정보방송통신위원회 현안 질의에서 이정헌 의원은 '제로 트러스트' 보안 원칙의 필요성을 강조했다. 이번 사고는 쿠팡만의 문제가 아니라, 국내 전반에서 제로 트러스트 보안 체계와 내부 통제시스템이 충분히 구축되지 않았다는 점을 드러낸 사례로 평가된다.

국내제로트러스트도입률8%

글로벌 사이버 보안 기업 옥타(Okta)에 따르면, 제로 트러스트 보안을 진행중인 국내 기업은 8%에 불과한 것으로 알려져 있다. 민간기업과 금융권에서 도입 논의가 증가하고 있지만, 여전히 미국 등 주요국 대비 현격한 격차가 존재한다.

그림 14. 쿠팡 개인정보 유출 사태 타임라인

시기	구체적 사항
2025.06.24	해외 서버를 통한 무단 개인정보 접근 시작
2025.10	내부 직원 퇴사 및 중국 출국
2025.11.20	쿠팡, 개인정보위원회에 신고 및 피해 계정 4,536건 발표
2025.11.29-30	쿠팡, 개인 정보 유출 피해 계정 3.370만 건으로 정정 및 유출 사실 인정

자료 출처 : 쿠팡, 산업 자료, 지엘리서치

3. 양자내성암호(PQC)

차세대 암호, 양자내성암호는 무엇인가?

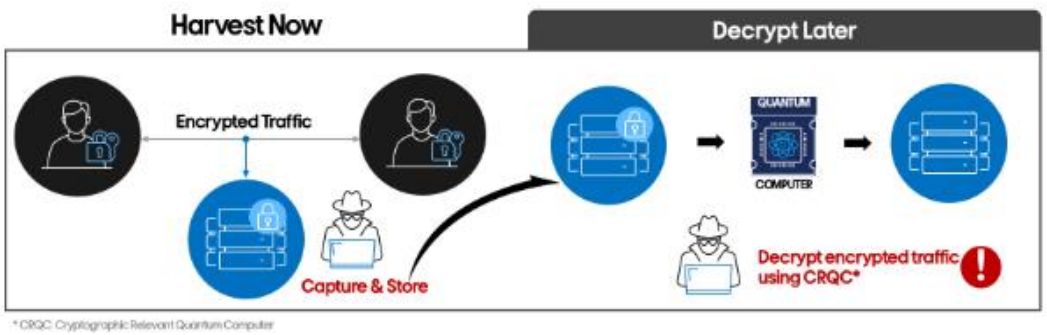
양자컴퓨터시대대비 PQC수요급부상

양자 내성 암호(PQC, Post-Quantum Cryptography)는 양자컴퓨터로도 해독이 불가능한 암호 기술을 의미한다. PQC는 양자 물리 기반 전송 기술인 '양자 암호(QKD)'와는 다른 개념으로, 기존 IT 인프라에 바로 적용할 수 있다는 점이 강점이 있다.

HNDL공격위협증가 금융,의료,공공중심 PQC대응필요

현재 널리 사용되는 공개키 암호(RSA, ECC)는 양자컴퓨터의 '쇼어 알고리즘'으로 해독될 수 있다는 위험이 제기되면서 PQC의 필요성이 부각되고 있다. 특히 금융·의료·국가 기밀 분야에서는 데이터를 먼저 탈취한 뒤, 양자컴퓨터가 상용화되면 해독을 시도하는 **HNDL(Harvest Now, Decrypt Later)** 공격 가능성이 커지고 있어 대응이 시급한 상황이다.

그림 15. HNDL 사이버 공격



자료 출처 : 삼성 에스디에스, 지엘리서치

그림 16. 양자내성암호 주요 기술 및 활용 분야

기술	PQC 활용 분야	장점	단점	NIST 표준 여부
격자 기반	KEM + 서명	속도, 안정성, 다양하게 쓰임	키/서명 크기 상대적 큼	표준(Kyber, Dilithium)
코드 기반	KEM	매우 안전, 빠른 복호	공개키 매우 큼	최종 후보 (Classic McEliece)
해시 기반	서명	장기적 안전성, 단순 원리	서명 크기 큼	표준(SPHINCS+)
다변수 기반	서명	빠른 서명	구조 공격 위험	탈락(Rainbow)
아이소제니 기반	키교환	키 매우 작음	보안 취약점	탈락(SIKE)

자료 출처 : 산업 자료, 지엘리서치

미국중심의PQC주도권 현시점필수보안체계정착

미국 국립표준기술연구소(NIST)는 지난해 양자 내성 암호 표준을 발표한 데 이어, 2025년 3월 코드 기반 알고리즘(HQC)을 표준 후보에 추가하며 표준화 범위를 확대하고 있다. 글로벌 기업들 또한 이에 맞춰 단계적 PQC 전환 계획을 추진 중이다. 특히 미국은 연방정부, 국방기관, 주요 은행, 클라우드 사업자가 PQC 연구·적용의 주도권을 확보하고 있어 표준화와 레퍼런스 시장을 선도할 가능성이 높다. 이들 기관을 중심으로 대규모 실증과 상업적 매출이 집중될 것으로 예상되며, 양자 내성 암호는 더 이상 미래 기술이 아니라 현재의 데이터를 보호하기 위한 필수 보안 체계로 자리매김하고 있다.

양자 내성 암호 시장 전망

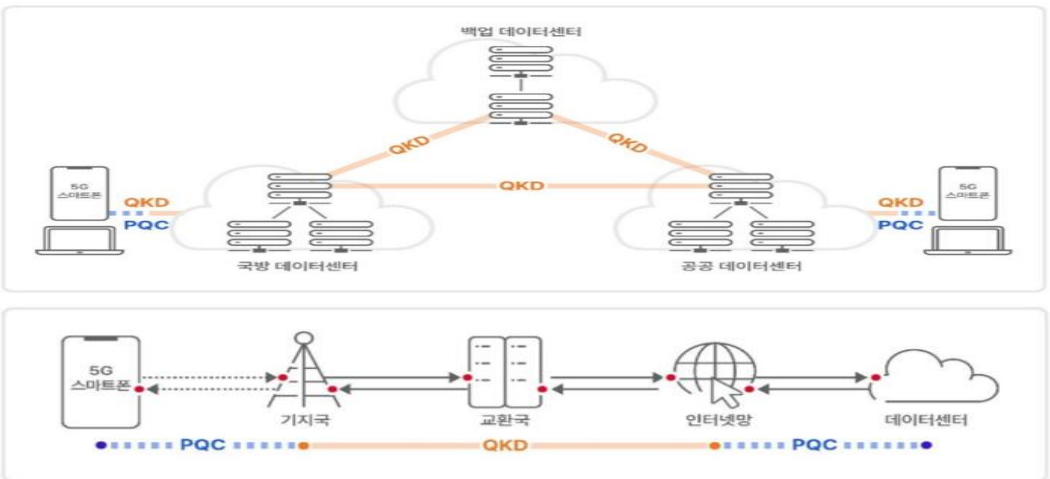
금융권중심PQC수요전망 CBDC,토큰화자산까지확산기대

양자내성암호(PQC) 수요는 금융 분야에서 가장 빠르게 확대될 것으로 전망된다. 계좌 정보, 거래 기록, 고객 데이터, 결제 인프라, 그리고 향후 확산될 CBDC·토큰화 자산 등은 장기 보존성과 높은 보안성을 요구하는 데이터이기 때문이다. 글로벌 중앙은행과 금융 감독기관이 양자 안전 보안 프레임워크를 제시하는 순간, 개별 기업의 선택을 넘어 금융권 전반의 일괄적 전환이 촉발될 가능성이 크다.

SKT,PQC활용보안제품출시

공공·국방·정부기관 역시 국가 신뢰성과 직결된 특성상 PQC 도입 속도가 가장 빠를 것으로 예상된다. 전자정부 시스템, 전자서명 인프라, 지휘통제망, 위성통신 등 국가 기반 인프라는 초기 구축 레퍼런스가 될 가능성이 높다. 또한 통신·클라우드·IDC 사업자는 네트워크 전송, 인증, API 보안, 멀티클라우드 연결 구간 등에 PQC 적용을 확대할 전망이다. 실제로 SKT는 지난해 'QKD-PQC 하이브리드 양자암호' 제품을 출시하며, PQC 표준 알고리즘과 양자키분배(QKD)를 결합해 하나의 장비에서 두 가지 방식의 암호화를 제공하는 기술을 상용화했다.

그림 17. SK텔레콤 양자보안 통신 모식도



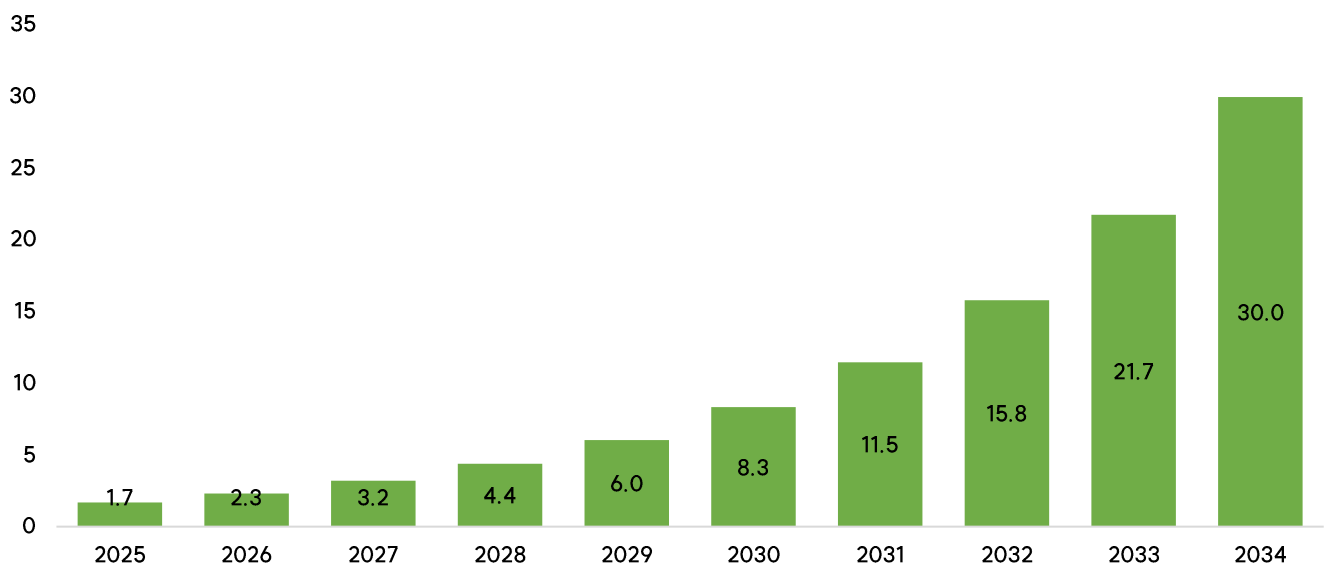
자료 출처 : SKT, 지엘리서치

제조, OT, IoT 영역에서는 장기 운영되는 설비의 특성상 "초기 설계 단계부터 PQC 내재화"가 요구에 대한 수요가 증가할 것으로 전망된다. 이는 산업용 장비 인증, 펌웨어 서명 검증, 원격 업데이트 보안(OTA) 등 실질적인 적용 영역으로 연결된다. 의료 및 헬스케어는 유전체 데이터·환자 기록처럼 민감하고 평생 유지되는 데이터 특성으로 인해 PQC의 핵심 적용처가 될 것이다. 또한 블록체인과 디지털 자산 생태계는 현재 ECC 기반 서명 체계 의존도가 높기 때문에 양자 위협 시 체인 신뢰가 직접 훼손될 수 있어, PQC 기반 계정 체계 및 신규 체인의 등장 가능성도 높다.

글로벌양자내성암호시장
25년~34년
CAGR37.72%성장

양자 내성 암호 산업은 초기 시장 형성 단계로, 현재 시점에서 전체 정보보안 투자 중 비중은 낮지만 중장기 성장률은 높을 것으로 전망된다. 시장 조사 업체 Precedence research에 따르면, 2025년 16.8억 달러에서 2034년 299.5억 달러, CAGR +38% 성장이 예상된다. 2030년 전후 까지는 글로벌 PQC 체계 도입이 시장의 핵심으로 존재하지만, 2030년 중반 이후부터는 PQ를 활용한 인증, 네트워크, 디바이스 보안 등 다양한 하위 영역에 내재화될 전망이다. 양자 내성 암호 시장은 단일 솔루션이 아닌 기존 사이버 보안 생태계 전체를 '양자 기술 기반 보안 구조'로 재편하는 것을 의미한다.

그림 18. 글로벌 양자내성암호 시장 규모 (단위 : 십억 달러)



자료 출처 : Precedence resaech, 지엘리서치

1. 국가 차원의 사이버 보안 육성 전략

범부처 '정보보호종합대책' 국가보안전략의 구조적 확장

정부는 2019년 '국가사이버안보전략'을 통해 국가 차원의 보안 정책 방향을 제시 했다. **이후 2025년 10월, 연속적으로 발생한 사이버 공격과 개인정보 유출 사태에 대응하기 위해 범부처 '정보보호 종합 대책'이 발표되면서 기존 전략이 한 단계 확장되었다.** 이번 대책에는 AI 에이전트 기반 보안 플랫폼 육성, 화이트 해커 인력 체계 재설계, 양자내성암호(PQC) 기반 국가 암호체계 전환 등이 포함되어 있다. 침해 대응을 넘어 차세대 디지털 인프라 전체를 보호하는 방식으로 정책 중심축을 재편하고 있다는 점에서 의미가 크다.

제로트러스트 가이드라인 공공, 민간 보안 구조 개편

정부와 한국인터넷진흥원(KISA)은 '제로트러스트 가이드라인 1.0·2.0'을 통해 공공 및 민간 조직의 보안 구조를 제로트러스트 모델로 전환하도록 유도하고 있다. 최소 권한 검증, 연속 인증, 환경 기반 접근 정책이 핵심 원칙으로 제시되었으며, 이에 따라 ZTNA, IAM/PAM, SASE, 마이크로 세그멘테이션 등 최신 보안 아키텍처가 사실상 필수 적용 기준으로 자리 잡고 있다. 결과적으로 보안 정책은 "접근을 허용한 뒤 감시하는 구조"에서 "접근 요청마다 신뢰 수준을 판단하는 구조"로 명확하게 전환되고 있다.

그림 19. 제로트러스트 가이드라인 1.0 과 2.0 비교

주요 내용	가이드라인 1.0	가이드라인 2.0 (기존 가이드라인에 추가된 사항)
제로트러스트 성숙도 모델	- 3단계 성숙도 수준 정의 - 기업망 핵심 요소별 20가지 기능 정의 (교차 기능 제외)	- '초기' 단계를 추가한 4단계 성숙도 수준 정의 - 기업망 핵심 요소별 27가지 기능 정의 (교차 기능 제외) 및 각 단계별 특징 구체화 - 기업망 핵심 요소 및 2가지 교차 기능에 대한 52가지 보안 세부역량 및 각 세부역량의 성숙도 수준별 특징 정의 - 성숙도 모델에 기반한 구현 방안 제시
제로트러스트 도입 절차	- 제로트러스트 아키텍처 도입 고려사항 정리 (성숙도 모델 관점 및 기업 내외부 환경 관점) - 총 5단계의 제로트러스트 아키텍처 도입 단계 제시 (준비 – 계획 – 구현 – 운영 – 피드백 및 개선) - OMB 각서를 참고하여 제로트러스트 구현에 따르는 핵심 요소별 초기 전략 제시	- 제로트러스트 아키텍처 도입 과정에서의 고려사항 구체화 (제로트러스트에 대한 명확한 이해 및 기업 내 인식 제고 등 추가) - 제로트러스트 도입 준비 단계 구체화 (업무 구체적 기술 및 예시 제시) - 제로트러스트 아키텍처 도입을 위한 조직 내 역할 및 목표 설정 방안 제시
기타	- 제로트러스트 구현에 관한 6가지 유스 케이스 및 목표·요구사항, 구현 방안 등 제시 - 제로트러스트 도입 후 보안 수준 평가 방안 없음	- 제로트러스트 도입 후 기업망 보안 수준을 평가할 수 있는 2가지 방안 제시 (성숙도 기반 도입 수준 분석을 위한 체크리스트, 침투시험 기반 제로트러스트 효과성 분석 방안)

자료 출처 : 한국인터넷진흥원, 지엘리서치

5대디지털산업중심 OT보안정책강화

정부는 국민 생활과 밀접한 5대 디지털 산업 '스마트공장, 자율주행 인프라, 디지털 헬스케어, 스마트시티, 실감 콘텐츠' 를 중심으로 OT 기반 보안 정책을 강화하고 있다. 산업별 위협 분석부터 취약점 진단, 보안 모델 개발, 확산까지 단계별 정책을 추진하며, 생산설비·의료장비·도시 인프라 등 물리적 시스템을 **운영 중단 없이 안전하게 유지하는 보안 체계** 구축이 목표다. 이는 기존 IT 보안 중심 접근으로는 한계가 있던 영역까지 정책적 적용 범위를 확장한 점에서 의미가 크다.

2035년까지 공공 인프라 PQC도입
한국형 PQC 알고리즘 표준화

정부는 암호체계 전환을 국가 전략 과제로 격상하며 양자내성암호(PQC) 도입을 본격화하고 있다. 2023년 7월, 국가정보원과 과학기술정보통신부는 '양자암호기술 발표전략'을 발표하며 2035년까지 국가 공공 인프라 전 구간을 양자내성암호(PQC) 기반으로 전환하겠다는 '범국가 마스터 플랜'을 공개했다. 2025년 초에는 한국형 PQC 알고리즘 4종이 최종 확정되어 국내 표준화 절차에 들어갔으며 에너지 – 의료 – 행정 3개 분야 시범 전환 사업도 27억원 규모로 추진되고 있다. 투자 규모와 추진 속도 면에서 미국 대비 부족한 점은 있으나, 공공과 민간 모두 PQC 기술 개발과 인프라 구축 속도를 높이고 있다.

그림 20. 양자내성암호 전환 추진 로드맵 – 관계부처 합동 마스터 플랜

자료 출처 : 국가정보원, 지엘리서치

2. 사이버 보안 인력 양성 정책 활성화

인력,생태계육성정책
정부보안정책의핵심

사이버 보안 수요가 증가하고 위협이 고도화되면서 정부는 **인력·생태계 육성**을 또 하나의 핵심 정책 축으로 삼고 있다. 정보보호 특성화대학, 보안대학원, 사이버레인지 등 다양한 인재 양성 프로그램이 운영되고 있으며, 공공기관·지자체 CISO 교육, 민관 합동 모의훈련, 사이버 위기 대응 훈련을 정례화해 조직의 대응 역량도 강화하고 있다.

또한, 정부는 보안 R&D 지원, ISMS-P·CSAP 기반의 인증 생태계 강화, 글로벌 진출 프로그램 등을 통해 국내 보안기업의 기술 경쟁력과 수출 확대를 뒷받침하고 있으며, 이는 단순한 인력 부족 해소를 넘어 MSSP, 보안 컨설팅·관제, 레드팀·훈련 서비스 등 서비스형 보안 산업 성장으로 이어지는 구조적 기반을 형성하고 있다.

그림 21. 정부 사이버 보안 정책 및 인력, 산업 육성 동향

정책 축	핵심 내용	기술 키워드	산업적 파급효과
국가 전략·거버넌스	국가사이버안보전략, 기본계획, 정보보호백서, 공세적 방어·핵심 인프라 복원력 강화	SOC 고도화, 위협 헌팅, 기반 시설 보호	국가 단위 규제·표준 상승 > 공공·금융·기간망 중심 CAPEX 확대
기술 영역별 정책	제로트러스트 1.0/2.0, SW 공급망 보안, ICS/OT 보안 가이드	ZTNA·IAM·SASE, DevSecOps·SBOM, OT 보안	최신 아키텍처 확산, 클라우드·OT 중심 신규 수요 증대
암호(PQC) 정책	PQC 전환 로드맵(2030/2035), 국산 PQC 알고리즘, 금융·공공 시범 적용	PQC 모듈, HSM, 키 관리, 암호 전환 솔루션	차세대 암호 전환 비용(CAPEX) 발생 > 중장기 성장 모멘텀
인력·산업 육성	정보보호 인재 양성, 사이버레인지, 모의훈련, 보안 R&D 확장	교육·훈련 플랫폼, MSSP, 레드팀·블루팀	인력 부족 해소 + 서비스형 보안(SaaS·MSSP) 성장 기반

자료 출처 : 과학기술정보통신부, 한국인터넷진흥원, 지엘리서치

Contents

V. 기업분석

휴네시온(290270, KOSDAQ)

국가망보안체계 정책 전환 구조적 수혜 + 차세대 보안 플랫폼 강화

라온시큐어(042510, KOSDAQ)

제로트러스트 기반 보안 솔루션 & 화이트햇 보안 서비스

싸이버원(356890, KOSDAQ)

통합보안관제 플랫폼과 M&A로 매출과 수익성 모두 잡는다

휴네시온(290270, KQ)

국가망보안체계 정책 전환 구조적 수혜 + 차세대 보안 플랫폼 강화

INVESTMENT
SUMMARY

국내 유일 망연계 풀 라인업 구축으로 시장 장악력 강화
2027년 SBOM 제도화 예정, SBOM 기반 공급망 보안모델 구축
국가망보안체계(N²SF) 최적화 보안 모델 준비 완료
SW 공급망 표준모델, 망연계 솔루션 제품군에 양자내성암호 기술 적용

Stock Data

2025. 12. 17 발간
2025. 12. 16 종가 기준

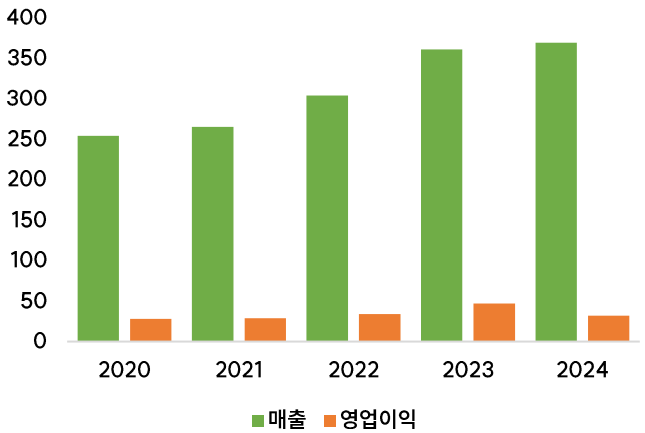
현재주가	3,955원
시가총액	380억원
발행주식수	9,607,672주
52주최고가	4,990원
52주최저가	3,135원
외국인지분율	2.33%
유동주식비율	48.73%
밸류에이션	
PER	7.22배
PBR	0.80배

보안, 개인 정보 유출 사고에 대응 가능한 망연계 풀 라인업 구축

휴네시온(이하 동사)는 공공-금융-민간 등 2,120여 레퍼런스를 보유한 국내 1위 망연계 솔루션 기업이다. 2025년 3분기 연결 기준 매출액 76.3억원(+18% YoY), 영업이익 2.4억원(흑자전환)을 기록했다. 4분기에 매출이 집중되는 계절성이 있어 2025년 연간 기준 최대 매출 달성이 예상된다. 최근 잇따른 통신, 금융권 사이버 보안 사고와 쿠팡 개인 정보 유출 사태로 인해 동사의 망연계 보안 제품군이 주목을 받고 있다.

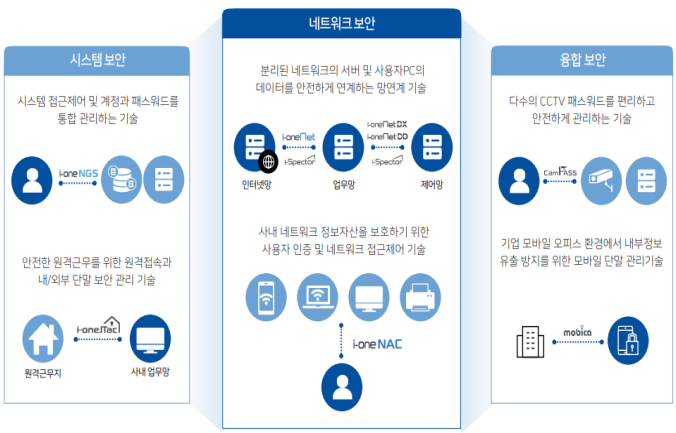
동사는 국내 유일 양방향, 일방향, 클라우드형 모두 제공하는 망연계 솔루션 포트폴리오를 보유하고 있으며 공공기관 망연계 시장에서 약 50% 수준의 점유율을 유지하고 있다. 금융·제조·국방 등으로 확장 기반을 마련해 고객 운용 편의성을 높이고, 강력한 Lock-in 효과를 창출하는 경쟁력으로 이어지고 있다.

그림 22. 휴네시온, 매출액과 영업이익 추이(단위 : 억원)



자료 출처 : 다트, 휴네시온, 지엘리서치

그림 23. 정보보안산업 핵심 플랫폼 사업영역 확대



자료 출처 : 휴네시온, 지엘리서치

국가망 보안체계(N²SF) 최적화 보안 모델 준비 완료

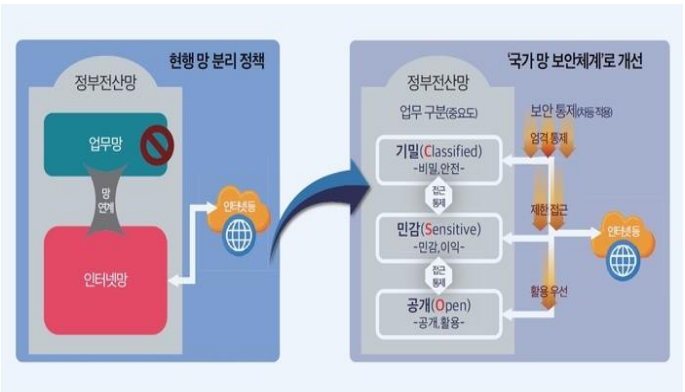
산업 전반에 사이버 위협이 확산되며 국내 보안 산업에도 새로운 정책 전환이 본격화되고 있다. 2025년 9월 30일, 국가정보원은 '국가망보안체계(N²SF) 보안 가이드라인 1.0' 정식판을 발표하며 기존의 획일적인 망분리 정책을 대체할 새로운 보안 패러다임을 제시했다.

이에 발맞춰 동사는 기존 망연계 보안 솔루션 경쟁력을 기반으로 N²SF 환경에 최적화된 망연계, 접근통제, 관리체계 보안 모델을 선제적으로 구축하고 있다. 이는 경계형 보안에서 제로 트러스트 기반 망연계 구조로 전환되는 정책 변화의 직접적인 수혜가 기대되는 부분이다.

그림 24. 보안산업 핵심 기술 보유 자회사 -AI, OT 보안 확대

자료 출처 : 휴네시온, 지엘리서치

그림 25. 기존 망분리 정책과 국가망보안체계 비교



자료 출처 : 국가정보원, 지엘리서치

SBOM 기반 공급망 보안 확장 및 양자내성암호(PQC) 적용

SBOM(Software Bill of Materials) 기반 공급망 보안 통합 위험관리 체계 구축은 사이버 공격에 대한 선제적 대응을 위해 필수적인 요소로 부각되고 있다. 미국·유럽 대비 국내는 아직 의무화 단계는 아니지만, 2025년 10월 발표된 '범부처 정보보호 종합대책'을 통해 2027년 전후 단계적 제도화 추진이 예고된 상황이다.

동사는 2025년 과학기술정보통신부·KISA 지원 'SBOM 기반 공급망 보안모델 구축 지원사업' 주관사업자로 선정되었으며, 망연계 솔루션 'i-oneNet'에 SBOM 생성·관리 체계를 내재화했다. 이를 통해 SW 개발-배포-도입 전 과정에서 잠재 위협을 사전에 식별하고 신속히 대응 가능한 공급망 보안 플랫폼을 구축하고 있다.

또한 동사는 자회사 오투윈즈를 통해 OT 보안 영역으로 사업을 확장하고 있다. 2025년 5월 글로벌 OT 제조장비 기업과의 파트너십을 기반으로 OT 보안 협력체계를 구축했으며, SBOM·HBOM 기반 산업제어시스템 공급망 보안 플랫폼 국제 공동 R&D를 통해 제품 경쟁력과 글로벌 진출 동력을 강화하고 있다.

아울러 양자내성암호(PQC) 및 동형암호 기술을 SW 공급망 보안 표준모델과 망연계 솔루션 제품군에 순차적으로 적용하며, 향후 동형암호 기반 기밀정보 유통 모델을 통한 글로벌 시장 진출을 목표로 하고 있다.

라온시큐어(042510, KQ)

제로트러스트 기반 보안 솔루션 & 화이트햇 보안 서비스

INVESTMENT
SUMMARY

정보보안 정책 강화, 제로트러스트 기반 인증 시장 성장 수혜 기대

OmniOne 기반 일본 증권사 중심 해외 매출 기여도 확대

정보 유출 사고 증가, 화이트햇 수요 증가에 따른 고성장 동력 확보

양자내성암호, AI 보안 기술 탑재 등 차세대 보안 플랫폼 신사업 추진

Stock Data

2025. 12. 17 발간
2025. 12. 16 종가 기준

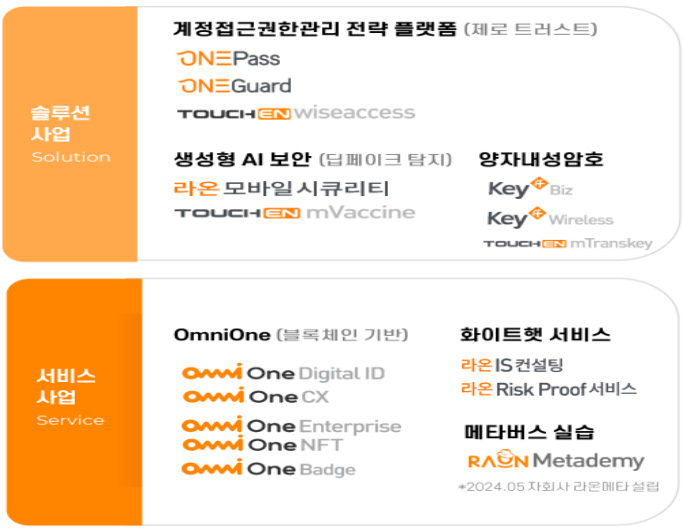
현재주가	9,400원
시가총액	1,058억원
발행주식수	11,205,174주
52주최고가	13,810원
52주최저가	8,950원
(수정주가)	
외국인지분율	1.92%
유동주식비율	57.39%
밸류에이션	
PER	24.65배
PBR	2.11배

국가 신원 인프라, 디지털 보안, 인증 생태계 연결하는 핵심 플레이어

라온시큐어(이하 동사)는 공공·금융·대기업과 일반 고객을 대상으로 다양한 보안 솔루션과 서비스를 제공하는 정보보안 기업이다. 동사는 모바일·PC 보안과 제로트러스트 기반 계정 접근 권한관리 플랫폼으로 구성된 솔루션 사업과 OmniOne 블록체인 서비스와 B2C IDaaS 신원인증 서비스, 화이트햇 컨설팅 등이 포함된 서비스 사업으로 구성되어 있다.

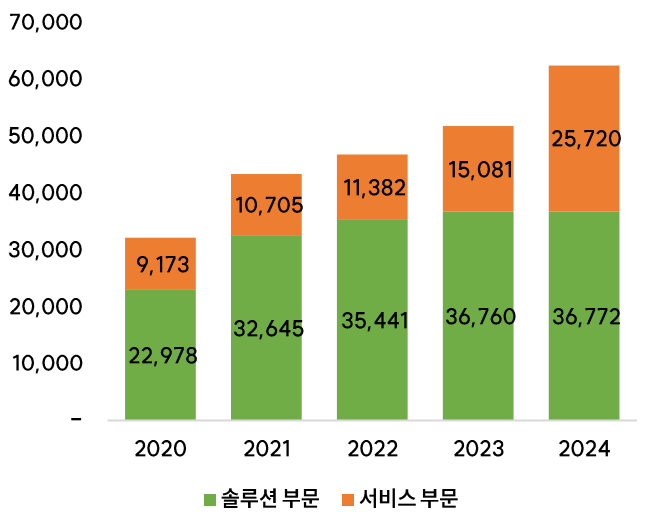
동사는 공공·금융·대기업과의 전략적 파트너십을 통해 솔루션 사업에서 안정적 매출 구조를 구축해 왔으며, 최근에는 OmniOne 블록체인 디지털 ID 서비스와 화이트햇 구독형 보안 서비스 등을 중심으로 서비스 사업을 확장하며 매출 성장을 가속화 하고 있다.

그림 26. 라온시큐어 사업영역



자료 출처 : 라온시큐어, 지엘리서치

그림 27. 사업부문별 매출액 성장 추이(단위 : 백만원)

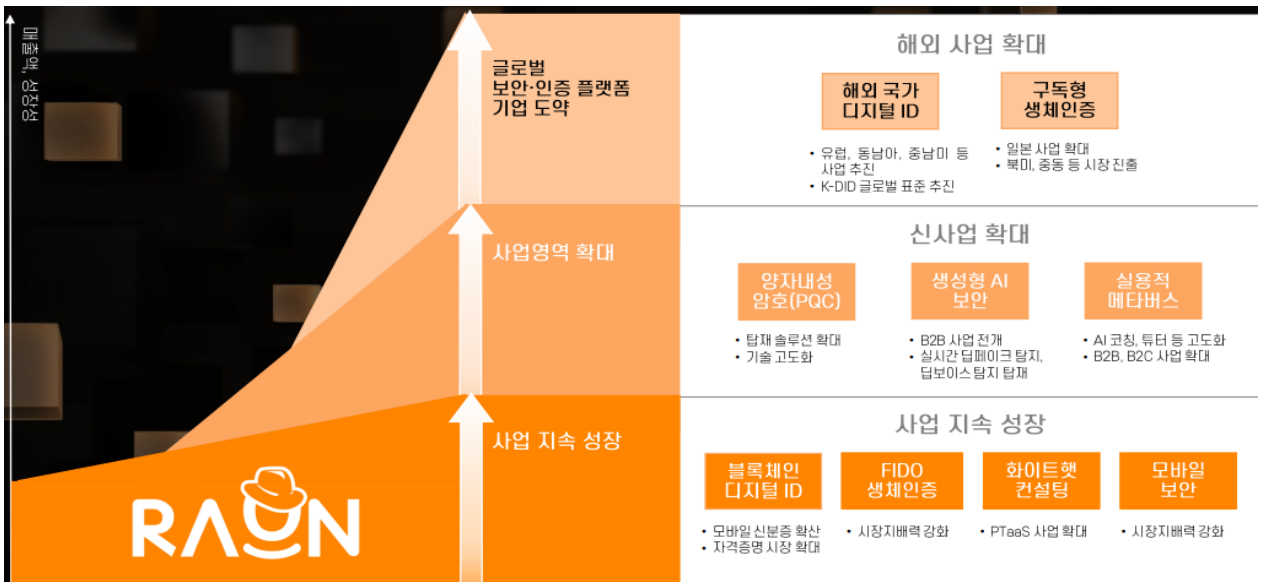


자료 출처 : 라온시큐어, 지엘리서치

안정적인 솔루션 사업 매출, 성장성의 기반

솔루션 사업은 제로트러스트 기반 모바일·PC 보안 플랫폼을 제공하고 있다. 이는 계정접근권한관리 및 단말 보안을 아우르는 플랫폼으로 OnePass(FIDO 기반 다중인증 플랫폼), OneGuard (통합 모바일 보안, 스마트워크 플랫폼), TouchEn WiseAccess(통합 계정, 권한관리 플랫폼) 등으로 구성되어 있다. 특히 OnePass는 일본 증권사 중심으로 도입이 확대되며 2025년 11월 기준 일본 월간 활성자수 940만 명을 돌파, 해외 수요 확대가 글로벌 성장으로 이어지고 있다.

그림 28. 라온시큐어 성장 전략 로드맵



자료 출처 : 라온시큐어, 지엘리서치

정보 유출 사고 증가, 화이트햇 수요 증가에 따른 고성장 동력 확보

동사의 화이트햇 컨설팅은 프리미엄 모의해킹 역량을 기반으로 공공·금융·대기업 고객 대상 모의해킹 서비스를 제공한다. 모의해킹은 실제 환경에서의 해킹을 통해 고객사별 대응 방안을 제시하는 서비스이며, 구독형 모의해킹 서비스 PTaaS는 상시적이고 지속적인 보안 테스트와 취약점 안내를 제공하는 플랫폼이다.

사이버 공격 및 대규모 정보 유출 사고 증가로 모의해킹 시장과 화이트햇 수요가 구조적으로 확대되고 있으며, 해당 부문은 동사의 핵심 신성장 동력으로 자리 잡고 있다.

싸이버원(356890, KQ)

통합보안관제 플랫폼과 M&A로 매출과 수익성 모두 잡는다

INVESTMENT
SUMMARY

통합보안관제 플랫폼 기반 운용 효율화 및 수익성 개선 기대
보안 컨설팅과 클라우드 전환을 아우르는 원스톱 서비스 역량 확보
엑스큐어넷 인수(2023년 8월)를 통한 고객사 다변화 효과 기대
동남아 시장 중심의 글로벌 진출 모멘텀

Stock Data

2025. 12. 17 발간
2025. 12. 16 종가 기준

현재주가	4,000원
시가총액	478억원
발행주식수	11,953,825주
52주최고가	5,420원
52주최저가	2,720원
외국인지분율	4.62%
유동주식비율	44.14%
밸류에이션	
PER	6.01배
PBR	1.14배

싸이버원, 안전한 IT 환경을 책임지는 종합 정보보호 전문 기업

싸이버원(이하 동사)는 보안관제, 보안 컨설팅, 클라우드 서비스, 보안솔루션 등의 사업을 영위하고 있다. 동사의 주력 사업인 보안관제 서비스는 클라우드, 온프레미스 방식으로 고객사의 니즈에 따라 원격, 하이브리드, 파견 형태로 운영 된다.

특히 통합보안관제 플랫폼(PROM SIEM)을 자체 개발·고도화함으로써 관제 운영의 자동화 수준을 높이고, 다수 고객을 동시에 처리할 수 있는 효율성과 시스템 가용성을 확보하고 있다. 특히 AI 기반 이상징후 탐지, SOAR 기반 자동화 대응 기능을 통해 관제 인력 의존도를 낮추는 동시에 운영 안정성을 강화하고 있다. 또한 악성메일 모의훈련(PROMATS), 취약점 진단·분석 및 대응 서비스 등 관제 연계 부가 서비스를 패키지 형태로 제공함으로써 기존 관제 고객 대상 추가 매출 창출이 가능할 것으로 기대된다.

그림 29. 싸이버원 주요 사업 부문

자료 출처 : 싸이버원, 지엘리서치

보안컨설팅·클라우드 전환을 아우르는 싸이버원의 서비스 경쟁력

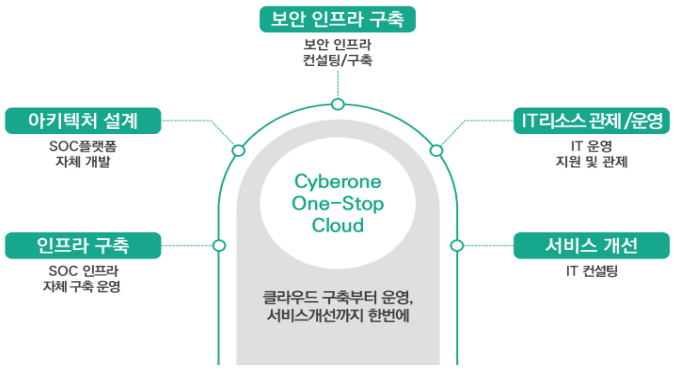
동사는 클라우드 및 IoT 관련 보안 컨설팅 서비스를 제공하고 있으며, 화이트햇 기반의 점검 및 대응 역량을 보유하고 있다. 경쟁사 대비 조직 규모는 크지 않지만, 공공기관을 대상으로 정보보호 컨설팅이 의무화되면서 매년 연말에 프로젝트 매출이 집중되는 경향을 보인다.

또한 동사는 기업 및 공공기관 데이터를 클라우드 환경으로 전환하고자 할 때 컨설팅부터 전환 설계, 시스템 구축·운영, 서비스 개선까지 전 과정에 걸쳐 원스톱 서비스를 제공하고 있다. 또한 AWS, MS Azure, 네이버 클라우드, NHN 등 주요 CSP와 파트너십을 체결하며 서비스 경쟁력을 강화하고 있다.

그림 30. 싸이버원 – 보안컬설팅 서비스

자료 출처 : 싸이버원, 지엘리서치

그림 31. 싸이버원 – 클라우드 서비스



자료 출처 : 싸이버원, 지엘리서치

엑스큐어넷 인수, 고객사 다변화와 해외 시장 진출 모멘텀

2023년 동사는 AI 기반 정보보안 솔루션 기업 '엑스큐어넷'을 인수를 완료했다. 엑스큐어넷은 기업의 내부 정보 유출 차단 보안 서비스를 제공하며 고객사 대부분이 국내 대기업으로 구성되어 있다. 공공기관, 금융기관, 인터넷/서비스 기업에 편중된 동사의 고객사 구성의 다변화가 기대된다.

2025년 2월, 동사는 베트남 하노이에서 동사의 통합관제 보안 솔루션 'PROM SIEM'와 엑스큐어넷의 내부정보유출방지 솔루션 'Venus/EMASS AI'를 소개하는 '내부정보보호 솔루션 세미나'를 개최하면서 현지 기업 관계자들 협력 기회를 마련했다. 이를 통해 동사는 해외 시장 진출과 4분기에 집중된 매출 계절성이 완화될 것으로 기대된다.

➢ Compliance Notice

- ◆ 동 자료에 게재된 내용은 조사분석담당자 본인의 의견을 정확하게 반영하고 있으며, 외부의 부당한 압력이나 간섭 없이 작성되었음을 확인합니다.
- ◆ 동 자료 종목의 경우, 작성자는 해당 기업의 주식을 보유하고 있지 않습니다.
- ◆ 당사는 본 자료를 전문투자자 또는 제3자에게 사전 제공한 사실이 없습니다.
- ◆ 본 자료는 개인투자자의 증권투자를 돕기 위한 정보제공을 목적으로 제작되었습니다.
- ◆ 본 조사자료의 지적재산권은 지엘리서치에 있으므로, 당사의 허락 없이 무단 복사, 복제 및 대여, 배포할 수 없습니다.
- ◆ 본 자료는 어떠한 경우에도 개인투자자의 증권투자 결과에 대한 법적 책임소재의 증빙자료로 사용될 수 없습니다.
- ◆ 본 자료는 투자 판단을 위한 정보제공일 뿐 해당 주식에 대한 가치를 보장하지 않습니다. 따라서 참고자료로만 활용하시기 바라며 유가증권 투자 시 투자자 자신의 판단과 책임하에 최종결정을 하시기 바랍니다.