AI의 위협으로 촉발된 사이버보안의 패러다임 대전환

EY한영 산업연구원

March 2026
Insight Report #26-070

EY한영
Shape the future with confidence

The better the question. The better the answer. The better the world works.

Contents

01

사이버보안 Landscape

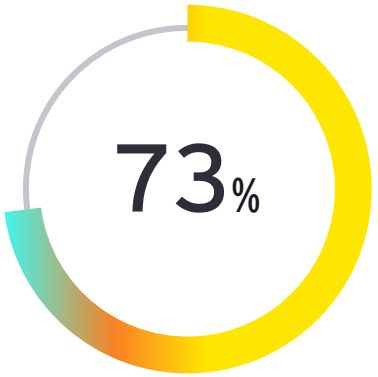
01

사이버보안의 전략적 중요성 확대

사이버 공격 피해 확산으로, C-Level에서 사이버보안 선제 대응이 핵심 경영 과제로 부상하고 있음

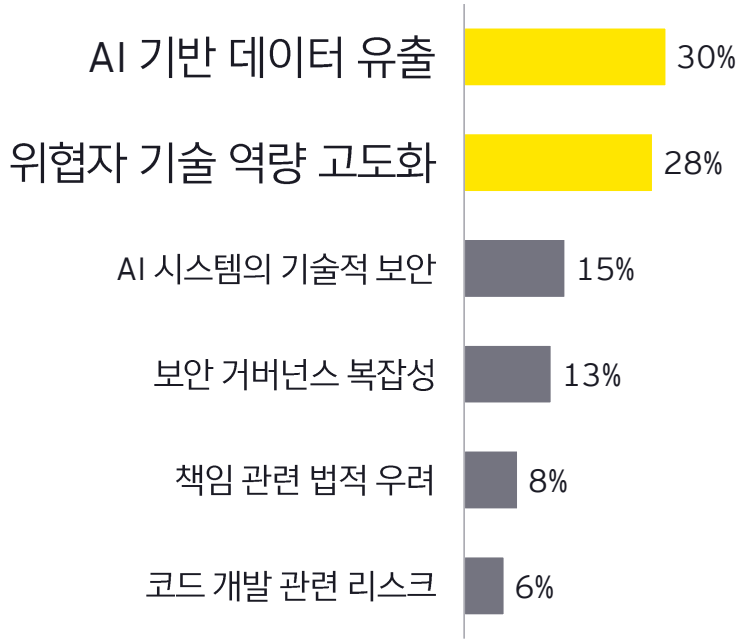
사이버 공격 발생 빈도 증가

최근 1년간 본인/ 동료 임원이
사이버기반 공격의
피해를 경험한 경영진 비중



AI 기반 위협 확산

CEO가 가장 우려하는 사이버보안 이슈



대응 긴급성 확대

81%

'26년 內 Zero Trust[1] 도입 예정 기업

>77%

사이버보안 투자 확대 예정 기업

1. 모든 사용자·기기·요청을 지속 검증해 최소 권한만 허용하는 보안 원칙

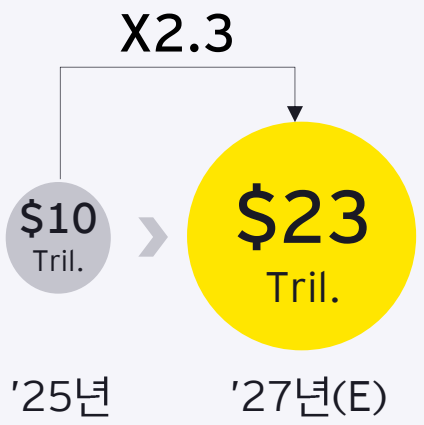
Source: WEF Cybersecurity Outlook (CEO 105명을 포함한 804명의 글로벌 리더 응답 기반 분석), Zscaler Risk Report (600명 이상의 글로벌 IT·보안 리더 대상 조사), Statista

사이버보안 사고의 기업 영향력 확대

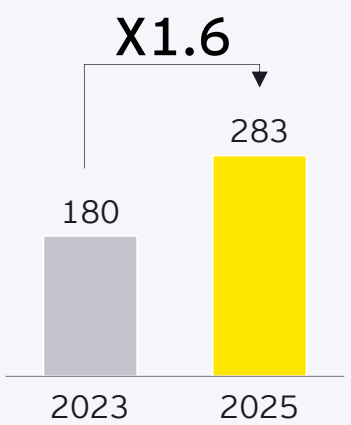
사이버보안 사고는 매출·신뢰·사업 지속성을 동시에 훼손하는 핵심 경영 리스크로 전환되고 있음

사이버 공격 피해의 범위·규모 확장

사이버범죄로 인한 글로벌 피해 금액



기업당 일일 사이버공격 시도 탐지 건수[1]



사이버 공격에 따른 Impact 사례

기업 차원

AT&T ['24년 3~7월]	8,600만 명 고객 데이터 유출	>177M USD **Settlement 비용**
JLR[2] ['25년 8월]	대형 랜섬웨어 공격으로 생산시설 6주 이상 중단	>2.5B USD **국가 경제적 피해[3]**
M&S ['25년 4월]	랜섬웨어로 공급망 운영 전반 마비	400M USD **매출 손실**

국가 차원

"Salt Typhoon" 사건 — 중국 정부 배후 해킹 그룹 ['21년~ 공격 추정]

- 수년에 걸쳐 80개국 대상 Verizon, AT&T 등 대형 통신사 및 정부기관 통신 인프라 공격

>600 **침해된 조직 수**

사이버보안 사고는 기업의 경쟁력·신뢰·사업 지속성을 결정하는 핵심 경영 리스크로 자리 잡고 있음

1. 보안 시스템이 탐지한 평균 공격·스캔 시도 이벤트 수 2. Jaguar Land Rover 3. 생산 중단으로 인한 차량 판매 감소와 이익 하락, 사고 대응 비용, 공급망과 지역 기업에 미친 영향 등을 포함한 손실 추정치
Source: Cybersecurity Ventures, Forbes, Check Point Research, IMF, EY Analysis

AI 사이버보안 시장 성장의 본격화

AI 사이버보안 시장은 투자 확대와 기술 고도화를 바탕으로, 빠른 성장 국면에 진입하고 있음

Key Drivers

1 **보안 투자 급증**

AI 관련 보안 기술 투자 확대 예정 IT 리더 비중

79%

2 **AI 위협 고도화**

'25년 사이버침해 확산 속도

전년 比 **65% 단축**

3 **AI 전문 보안 인력 수요 ↑**

전문 인력 수요 증가 → AI 보안 도입 시 평균 비용 절감 효과

2M USD

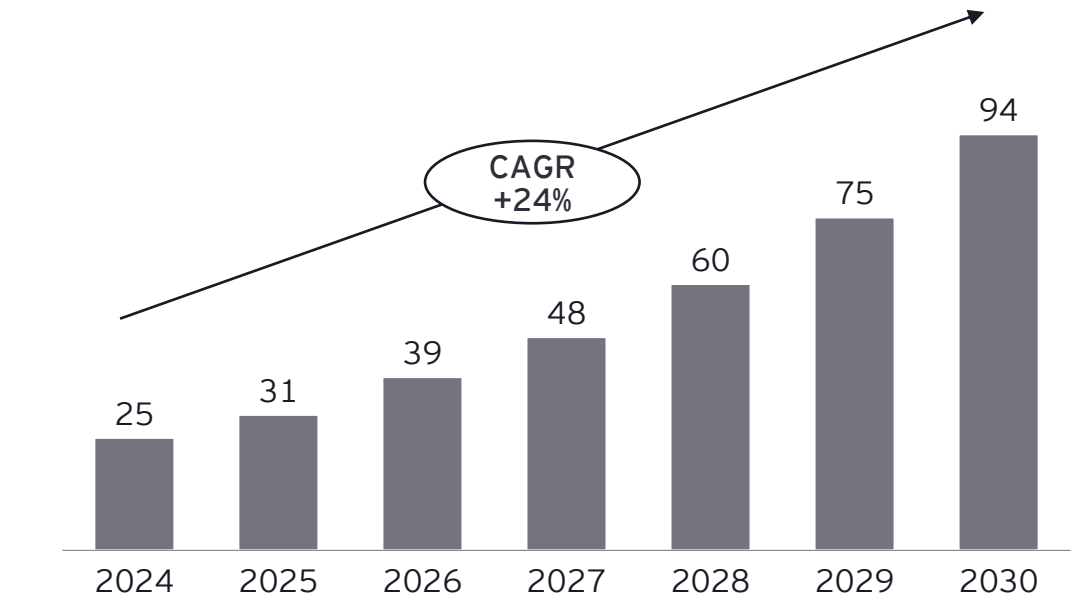
4 **자동화 기반 보안 확대**

자동화 및 상시 대응 보안체계 도입 기업 비중

>51%

AI 사이버보안 시장 규모

[단위: Bil. USD]



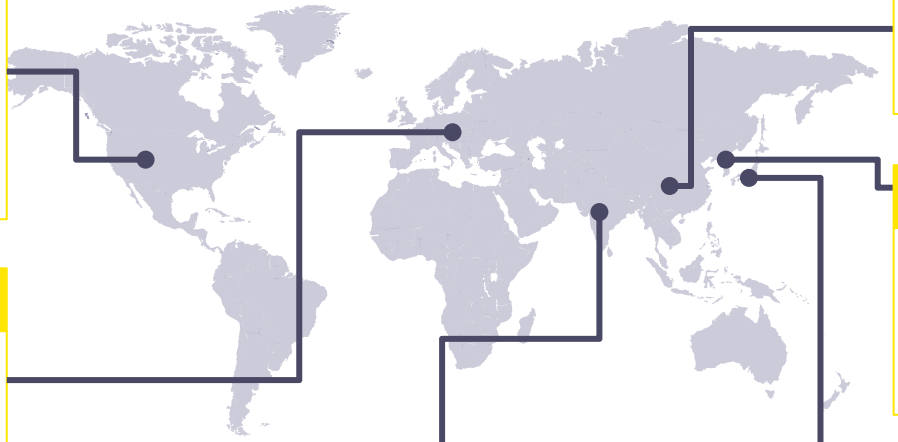
AI 기반 보안은 기존 보안의 한계를 보완하며 새로운 성장 축으로 부상하여 빠른 확장세를 보이는 중

Source: Grand View Research, Technavio, IBM, CrowdStrike, EY Analysis

AI 사이버보안의 정책·규제화

AI 사이버보안은 단순한 기술 대응을 넘어, 주요국 규제·정책 차원의 핵심 관리 영역으로 전환되고 있음

글로벌 각국의 규제·정책 환경 변화로 AI 보안 대응이 필수 요건으로 전환



미국

「 AI 행정명령 14110 」
- 안전·신뢰·보안을 중심으로 한 AI 개발·운영 기준 강화

「 National Security Strategy」
- AI·사이버를 국가안보 핵심 영역으로 명시

EU

「 EU Cybersecurity Strategy」
- 사이버공격 대응 강화 및 디지털 주권 확보, 회원국 간 공동 대응 체계 강화

「 AI Act」
- AI의 안전성·기본권 보호 보장 목적 법령
- 위험이 높은 AI 시스템 선별 및 통제

중국

「 Global AI Governance Initiative」
- AI 위험 수준 기반 평가체계 구축 및 지속가능한 글로벌 AI 생태계 조성 제안

한국

「 사이버보안 실태 평가지표 개정 」
- AI 보안과 N2SF[2] 중심의 위험관리 기반으로 전환, 기존 평가 체계 전면 개편

인도

「 DPDP[1] Act」
- AI 모델 학습·운영 과정에서 개인정보 보호 의무·책임 강화

일본

「 AI Governance Guidelines」
- 투명성·안전성·데이터 관리·책임 등 종합적 AI 거버넌스 가이드라인 제시

1. Digital Personal Data Protection 2. National Network Security Framework: 국가정보원이 도입한 차세대 보안체계로, 데이터 중요도(기밀·민감·공개)에 따라 보안통제를 차등 적용하는 프레임워크
Source: 각국 정부 및 규제기관 발표자료, EY Analysis

글로벌 주요
사이버보안 기업 현황

사이버보안 시장 참여 기업들은 기술·자문·운영 영역을 중심으로 구분되며, 일부 기업은 복수 영역으로 역할 범위를 확대하고 있음

Illustrative

「Advisory & Integration」 보안 전략·거버넌스·리스크 설계 및 시스템 통합

- 보안 아키텍처 설계
- 규제 대응 자문
- 침투 테스트
- ⋮

- IBM
- EY
- OPTIV
- GUIDEPOINT SECURITY
- CYDERES
- SAP
- CGI
- Accenture
- Capgemini

「Technology Solutions」 보안 기능을 제공하는 기술·제품·플랫폼 공급

- 네트워크 보안
- 클라우드 보안
- 계정 보안
- ⋮

- CISCO
- Google
- NVIDIA
- CYBERARK
- CROWDSTRIKE
- FORTINET
- Zscaler
- Paloalto
- Microsoft

「Operation & Response」 사이버 위협 탐지·분석·대응

- SOC[2] 운영
- MDR[3]
- 24/7 위협 모니터링
- ⋮

- IBM
- Trustwave
- KROLL
- ENSIGN Infosecurity
- AT&T Cybersecurity
- CROWDSTRIKE
- ECS
- Microsoft
- Secureworks

1. 보안 공급자들의 컨설팅·기술·운영 간 경계가 최근 융합되고 있어, 본 분류는 고정된 구분이 아닌 주요 제공 영역 기준 2. Security Operations Center 3. Managed Detection & Response
Source: EY Analysis

AI 특화 보안 솔루션 기업 부상

또한, 선도 기업들은 AI기반으로 고위험 공격 지점을 정밀하게 예측 및 대응하는 보안 역량을 고도화하고 있음

주요 기업별 사이버보안 솔루션 고도화 현황

Microsoft

「생성형 AI 기반 운영」

"Copilot for Security "

- 생성형 AI 기반 보안 위협 요약, 분석, 대응 안내

CISCO

「보안 자동화 플랫폼」

"Secure X"

- Agentic AI 기반 보안 플랫폼 구축, 글로벌 차원의 탐지·대응

Google

「AI 기반 위협 식별」

"Unified Security"

- Gemini AI 기반 피해 발생 전 위협 식별, 우선순위화, 조치

IBM

「위협 예측 AI」

"Predictive Threat Intelligence"

- 산업별 특화 모델 및 AI 활용, 잠재 위협 예측

CROWDSTRIKE

「침해 대응 고도화」

"Falcon Platform"

- 위협 10초 이내로 파악 및 빠르게 차단하는 역량 구현

FORTINET

「AI 위협 탐지, 대응 자동화」

"FortiAI 2.0"

- 자체 개발 AI를 자사 보안 플랫폼 전반에 탑재

Zscaler

「AI 기반 정보 유출 방지」

"Zscaler AI"

- LLM 연계 데이터 흐름 분석, 모니터링으로 정보 유출 방지

Paloalto

「보안 자동화 플랫폼」

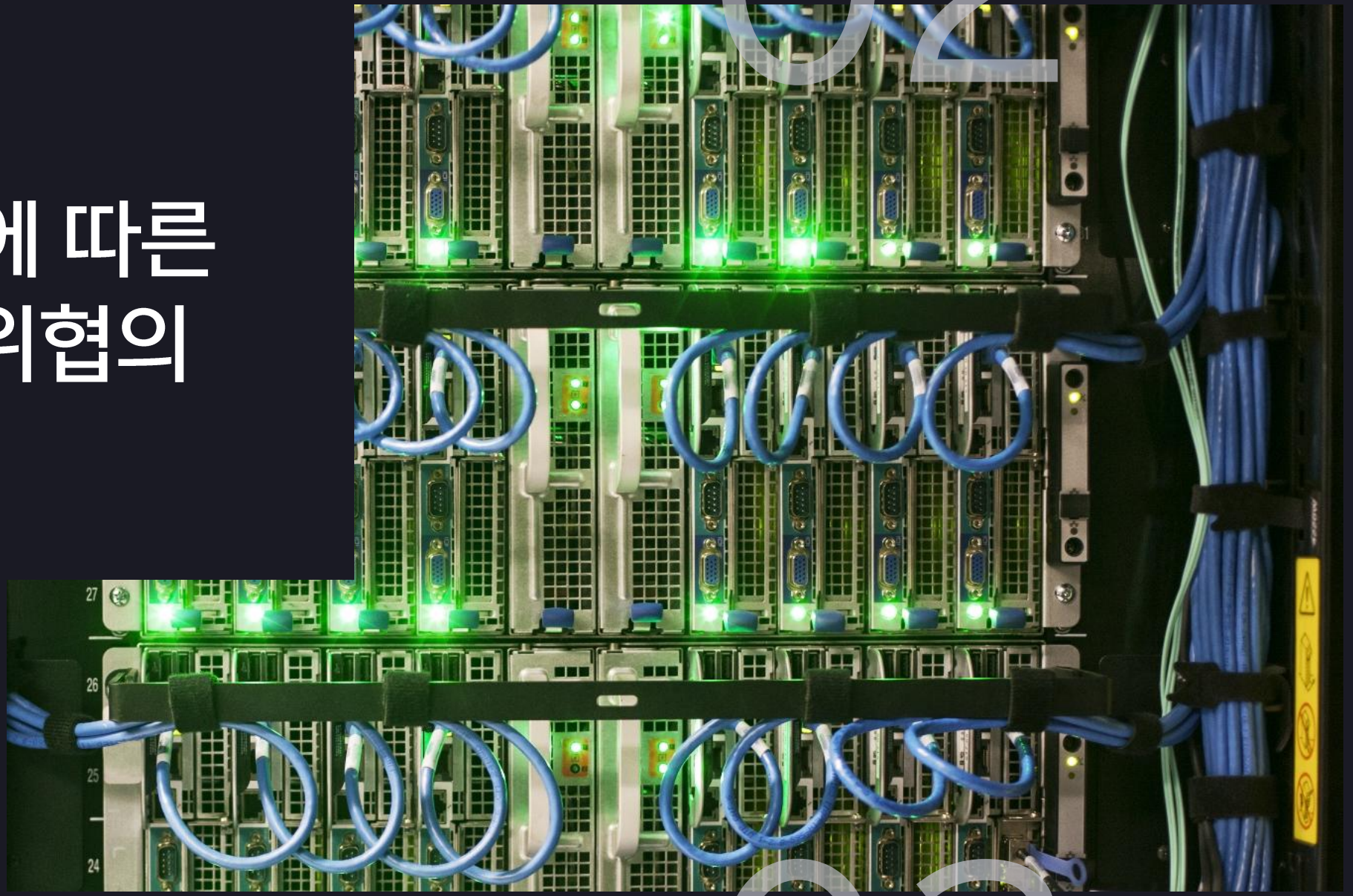
"Cortex XDR"

- Agentic AI 기반 위협 탐지 및 대응 역량 고도화

Source: EY Analysis

02

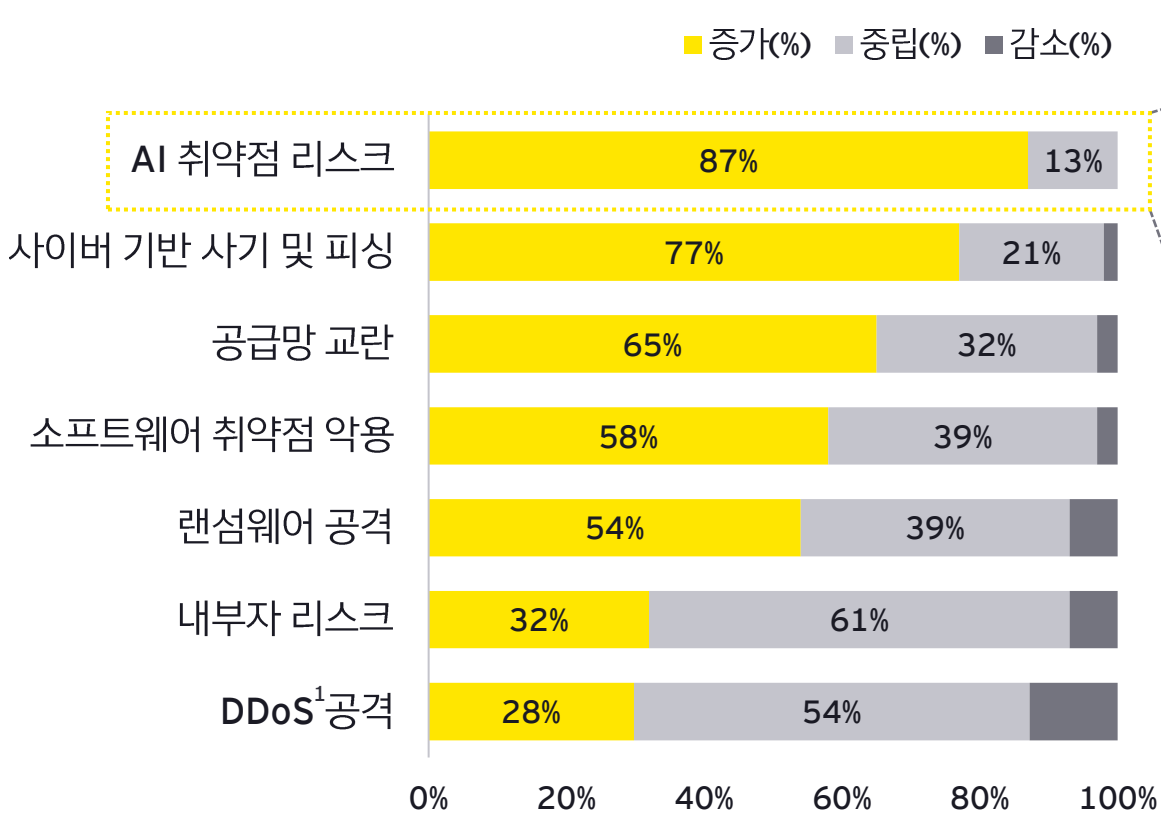
AI 확산에 따른 사이버 위협의 진화



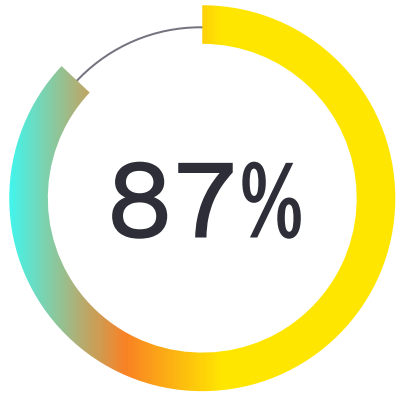
사이버 위협의 중심축 이동

최근 1년간 AI 취약점 리스크가 가장 빠르게 증가하며, 사이버 위협의 중심축이 AI 통제·검증 영역으로 이동하고 있음

최근 1년간 사이버 위협 수준 변화에 대한 기업 경영진의 인식 수준



AI 취약점[2] 리스크 증가 응답 비율



AI 취약점 리스크는 전통적 위협 유형인
랜섬웨어 54%(+33%p), DDoS 28%(+59%p) 比,
가장 높은 증가 응답률 기록,
위협 중심축이 AI 영역으로 이동함을 시사

1. DDoS(Distributed Denial of Service) : 분산된 다수의 장비를 활용, 목표 시스템에 대량의 트래픽을 유입시킴으로써 서비스 가용성을 저해하거나 중단시키는 사이버 공격 유형, 2. AI모델, 데이터, 입출력 처리 및 외부 연계 구조 등 AI 시스템 구성요소에서 발생 가능한 보안 취약성 및 악용 위험 요소를 의미
Source: WEF Global Cybersecurity Outlook 2026

사이버 공격 실행 구조 재편

AI 확산은 사이버 공격을 저비용·고속·대량 확산 구조로 전환시키고 있음

"AI 확산은 공격의 '경제성·공격 지점·확산 속도' 구조를 동시에 변화시킴"

01 공격 진입 장벽 하락

AI 기반 공격 설계 자동화 → 전문성 장벽 완화

- 공격 콘텐츠 생산 단가 하락(대량 생성·변형)
- 공격 준비 리소스 축소(정보 수집 및 준비 효율)
- 저비용 반복 실행 가능

"피싱·사칭 등 공격이 전체 침해 사례의 약 30~40% 차지"
- IBM X-Force('24) -

02 공격 지점 (Attack Surface) 확대

AI 모델·데이터 계층[1] 취약성 노출 증가

- 모델 입력 인터페이스(프롬프트)
- 모델 출력·후처리 계층
- 학습 데이터·파이프라인
- 외부 API·LLM 연계 구조

"2026년까지 기업의 80% ↑ Gen AI 도입 전망"
- Gartner('24) -

03 공격 속도·확산 가속

AI 기반 공격 실행 속도·확산력 증폭

- 자동 취약점 탐색·우선순위화
- 개인화 피싱·사기 메시지의 대량 전개
- 악성코드 변형·난독화 자동화

'취약점 악용 및 침해 확산 평균 소요 시간 단축 추세"
- Verizon DBIR('24) -

1. Layer(계층) : AI 시스템의 입력·모델·출력·데이터 처리 등 기능별로 구분한 구조적 구성 단계
Source: EY Analysis, WEF Global Cybersecurity Outlook 2026

공격 목표의 중심 이동

AI 환경에서는 보안 사고의 중심이 '시스템 침해'에서 '의사결정 과정·결과 왜곡'으로 확장되고 있음

사이버 보안 공격 목표 및 피해 매커니즘의 변화

구분	전통적 보안 사고 (시스템 침해 중심)	AI 환경 보안사고 (결과 왜곡 중심)
공격 의도	▪ 접근 권한 확보 ▪ 데이터 탈취 ▪ 서비스 가용성 저해	▪ 의사결정 결과 왜곡 ▪ 자동화 프로세스 교란 ▪ 정책 및 컴플라이언스 비준수 유도
공격 기법	▪ 계정 탈취(자격 증명 남용) ▪ S/W 취약점 기반 공격 ▪ 악성코드/랜섬웨어 배포	▪ 프롬프트 조작(Prompt Injection) ▪ 데이터 오염(Data/Model Poisoning) ▪ 출력 조작(Output Manipulation)
조직 영향	▪ 데이터 유출 ▪ 시스템 중단 ▪ 서비스 장애	▪ 자동화 의사결정 오류 ▪ 정책·규정 위반 리스크 ▪ 대외 신뢰도 훼손

AI 보안 사고의 구조적 특성

非 침해형 공격 유형	통제권 탈취 없이 결과 왜곡 발생 가능한 구조
입력값 조작 통한 통제 우회	프롬프트 조작 등 모델 통제 체계(정책·가드레일) 우회
리스크 탐지 가시성 한계	정상 운영 환경 內 탐지 난이도 증가로 식별 어려운 공격 패턴

Source: EY Analysis

AI 환경 보안 사고의 확산·가속화

검증되지 않은 AI의 판단이 API 및 자동화 시스템을 통해 연쇄 반영되며, 리스크가 빠르게 증폭됨

AI 환경의 사이버보안 사고 확산 매커니즘

데이터-AI 판단-API-자동화 시스템이 연결된 구조로,
단일 오류 판단이 내·외부 시스템 및 업무 프로세스로 즉시 확산

AI 환경 보안 리스크의 핵심은 '침해' 여부 자체보다는, '검증되지 않은 결과가 자동화 구조를 통해 확산' 되는데 있음

Source: EY Analysis

AI 환경에서의 기존 보안 통제 범위 한계

AI 환경에서는 서비스 연계 및 모델· 데이터 운영 영역에서, 기존 보안 전략의 적용 범위가 제한됨

AI 환경에서의 보안 리스크 구조적 변화

1 리스크 발생 영역 변화

기존 IT환경	AI 환경
네트워크 인프라	▪ API·서비스 연계 구간 ▪ 모델·데이터 운영 ▪ 자동화 기반 시스템
계정·권한 권리	
시스템·애플리케이션	

2 리스크 특성 변화

기존 IT환경	AI 환경
침투 기반 공격	▪ AI 판단 오류 기반 리스크 ▪ 모델 응답 왜곡 및 결과 값 자동 반영
권한 탈취 중심	
취약점 악용	

3 리스크 영향 범위 변화

기존 IT환경	AI 환경
시스템 단위 피해	▪ 내부 시스템 확산 ▪ 외부 서비스 연계 확산 ▪ 업무 시스템 영향 확대
데이터 유출	
서비스 장애	

AI 환경에서는 리스크 발생 구조 자체가 변화, 기존 IT 인프라 중심 보안 통제 체계의 적용 범위가 제한됨

Source: EY Analysis

AI 보안 대응 체계 분절

AI 보안 대응 체계는 기능·통제·책임이 분절된(Fragmented) 구조로 운영되어 통합 대응에 한계가 존재함

기업 내 AI 보안 운영 구조적 취약점 존재

- 모델·데이터·운영 기능 분산
- 기존 IT 보안 체계 중심 대응
- 외부 AI 서비스 연계 의존도 증가
- 전사 AI 거버넌스 및 책임 체계 미정립

분절 (Fragmentation) 지점 발생

기능 분절

- 보안·개발·데이터 기능 분산
- AI 운영 및 보안 통제 분리

통제 분절

- SIEM[1]·EDR[2] 중심의 기존 통제 한계
- AI 입력·출력·모니터링 미흡

책임 분절

- 모델 응답 오류 책임 불명확
- 외부 AI 서비스 사용 시 책임 경계 불명확

결 과

- 통합 대응 지연
- 정책·통제 기준 불일치
- AI 리스크 가시성 부족
- 사고 대응 혼선

AI 환경에서는 리스크 확산 구조와 분절된 보안 대응 체계 간 구조적 불균형 존재

1. Security Information and Event Mgmt.: 보안 이벤트 통합 관리 시스템, 2. Endpoint Detection and Response: PC·서버 등 단말 위협 탐지·대응 솔루션
Source: EY Analysis

AI 활용 확산에 따른 내부 리스크 확대

기업 내 AI 활용 확산은 데이터 통제 및 책임 구조의 공백이라는 새로운 내부 리스크를 야기하고 있음

기업 내 AI 활용 확산 현황

업무 내 AI 활용

非인가 AI[1] 사용 경험

월 223+

조직당 AI 정책 위반 평균 건수[2]

AI 활용 속도 > 통제 체계 정비 속도

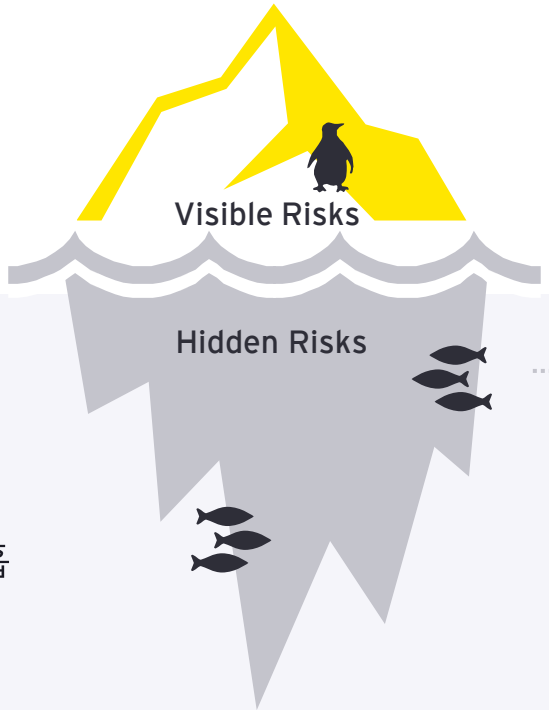
내부 AI 활용 리스크 유형

데이터 리스크

- 민감정보 외부 전송
- 외부 모델 데이터 잔존
- Shadow AI 사용

규제·컴플라이언스

- 데이터 보호 규정 위반
- 내부 정책 미준수
- 감사/법적 리스크



통제·가시성

- AI 사용 현황 파악 어려움
- 접근 권한/ 로그 관리 미흡
- 非인가 AI 사용

의사결정 리스크

- 미검증 AI 응답 활용
- 편향·왜곡 정보 적용
- 자동화 오류 확산

1. Shadow AI: 조직의 공식 승인·통제 절차 없이 임직원이 업무에 활용하는 외부 AI 도구·서비스를 의미 2. Netskope 고객 환경의 실제 데이터 정책 위반 로그 기반 산출
Source: EY Analysis, Microsoft Work Trend Index 2024, Netskope Threat Labs

글로벌 사이버보안 패러다임의 전환

AI 확산과 함께 사이버보안 패러다임은 사후 대응 중심에서, 상시 검증 및 통합 관리 체계로 이동하고 있음

보안 패러다임

외부 경계(Perimeter) 기반 신뢰 모델

Zero Trust 기반 상시 검증(Always Verify)/ 최소 권한 중심 접근 방식 강화

운영·프로세스

정기 점검·사후 승인 중심

지속적인 모니터링/ 위협 기반 분석 통한 선제적·연속적 방어

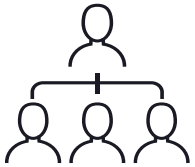
데이터·자산 통제

일반화된 통제 정책 일괄 적용

데이터 종류·민감도·사용 목적 등 세분화된 기준 기반의 정교한 통제 체계

조직·거버넌스

보안팀 중심 관리 및 책임



역할·책임 기반의 명확한 보안 거버넌스 정립 및 조직 전체의 공동 책임 체계

Source: EY Analysis

03

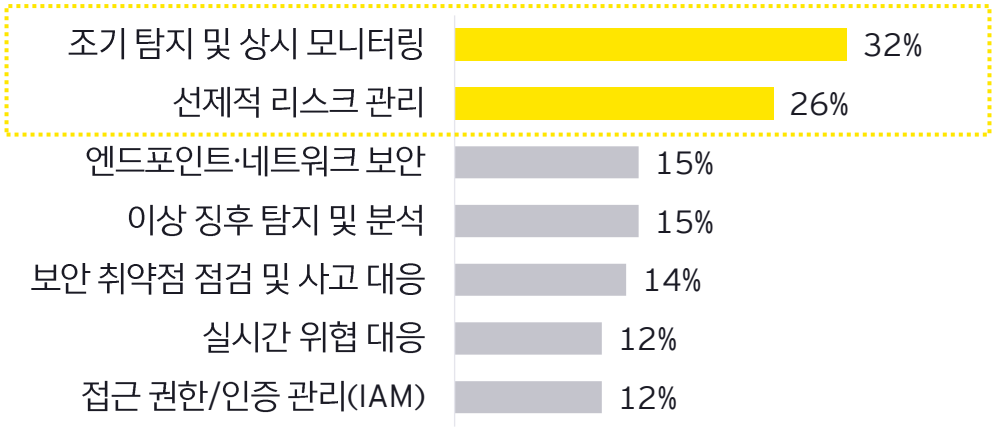
글로벌 사이버보안 역량 고도화 동향

AI 사이버보안
투자·운영 초점 재편

기업의 보안 투자는 개별 솔루션 중심에서 전사적 보안 프로세스 고도화로 재편되고 있음

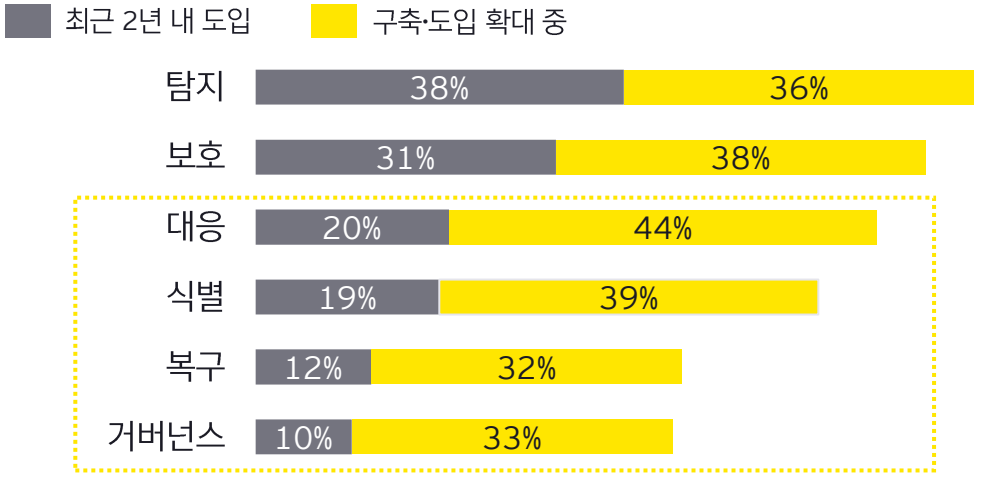
AI 보안 투자 우선순위

기업의 보안 투자 우선순위가
'원천 차단'에서 **'조기 탐지 및 선제적 리스크 관리'**로 이동



보안 프로세스 자동화 투자 현황

보안 활동이 개별 솔루션 중심 대응을 넘어,
'대응·복구·거버넌스'를 포괄하는 관리 체계로 확대



AI Cybersecurity는 기술 고도화를 넘어, 기업 전반의 운영 체계 수준을 결정 짓는 전략적 요인으로 부상

Source: EY Global Cybersecurity Leadership Insights study ('25년)

선도 기업 사이버보안 역량 고도화 전략

선도 기업들은 파트너십, M&A, 조직 재편 등 경영 차원의 의사결정으로 사이버보안 역량을 강화하고 있음

1 전략적 보안 파트너십

- 글로벌 보안 벤더 및 전문 기업과의 협력을 통해 신속히 기술·대응 역량 확보

2 M&A를 통한 역량 확보

- 핵심 보안 기술·플랫폼 보유 기업 인수로 단기간에 기술 역량 강화

3 핵심 영역 자체 개발

- 탐지·대응, AI 기반 분석 등 핵심 기술 내재화를 통한 역량 고도화

4 전사 거버넌스 강화

- AI 사용 승인 체계 및 전사 리스크 관리 기준 정립
- 조직 전반에 일관된 보안 정책·프로세스 통합 운영

5 CISO 권한 확대 및 조직 재편

- CISO의 전략·리스크 관리를 포함한 권한 및 영향력 강화
- 보안 의사결정 구조 및 협업 체계 재편

Source: EY Analysis

선도 기업 사이버보안 역량 고도화 사례 ①

글로벌 선도 기업들은 파트너십·M&A·내재화 전략을 통해 핵심 보안 기술·솔루션 역량을 확보하고 있음

1 전략적 보안 파트너십

Carrefour — corelight 파트너 社

내용 ML 기반 사이버공격 탐지 및 대응 기능 도입

기대 효과
- 대규모 리테일 네트워크 보안 가시성 확보
- 오탐 감소로 SOC 분석 효율성 증대, 위협 대응 시간 단축

TOYOTA TSUSHO — KEYFACTOR 파트너 社

내용 PKI[1] 기반 디지털 인증·암호화 기술을 그룹 밸류체인 전반에 적용

기대 효과
- 차량·IoT에 필요한 인증·암호화 체계 확보
- 자동차 外 제조영역까지 적용 가능한 확장형 보안 인프라 구축

2 M&A를 통한 역량 확보

Mastercard — Recorded Future 인수 社

내용 실시간 사기 감지·사이버보안 기능에 인수社 위협 인텔리전스 기술을 통합

기대 효과
- 결제망·금융 인프라 보안 강화
- 인수社 데이터 활용, AI 모델 정교화
- 보안·사기 방지 솔루션 경쟁력 확대

Servicenow — Armis, Veza 인수 社

내용 전사 서비스 內 Cyber Exposure 관리 역량 통합 (Armis) 및 아이덴티티 보안 강화 (Veza)

기대 효과
- 실시간 End-to-End 리스크 가시성 확보
- 보안 운영 자동화 역량 강화

3 핵심 영역 자체 개발

JP Morgan Chase

내용 내부 AI 기반 Fraud Detection 모델 개발

기대 효과
- 실시간 탐지 정확도 향상, 금융사기 피해 감소
- 오탐률 감소 및 규제 대응력 강화

TESLA

내용 차량용 OS 및 OTA[2] 보안 체계 자체 설계

기대 효과
- 즉각적 보안 업데이트로 취약점 대응 속도 확보
- SW/HW 수직 통합으로 보안 통제력 확보, 해킹 리스크 최소화

1. Public Key Infrastructure: 디지털 인증서와 공개키 암호기술을 활용하여 사용자·기기·시스템의 신원 검증, 데이터 암호화, 전자서명 검증을 수행하는 보안 인프라 체계
2. Over The Air: 유·무선 네트워크를 통해 차량 등의 소프트웨어·펌웨어를 원격으로 업데이트하는 기술

Source: EY Analysis

선도 기업 사이버보안 역량 고도화 사례 ②

글로벌 선도사는 전사 거버넌스 강화 및 CISO 권한 확대를 통해 사이버보안 대응 역량을 제고하고 있음

4 전사 거버넌스 강화

Microsoft

내용
- AI 시스템 개발·도입 시 단계별 승인·리스크 관리 프로세스 운영
- 6대 Responsible AI 원칙 기반 전사 정책·프로세스 일원화

기대 효과
- AI 오남용·윤리·보안 리스크 사전 차단, 글로벌 규제 대응력 향상
- 조직 전반의 일관된 정책 및 승인 프로세스 확보

SCHWARZ

내용
- 전사 임직원 58만 명 대상으로 주권형 Workspace[1] 로 일원화
- 사이버보안·데이터 주권 원칙을 그룹 차원에서 재정립 추진

기대 효과
- 업무환경·보안체계를 전사 동일 기준으로 통일, 보안 운영 복잡성 감소
- EU[2] 내 데이터 상주 및 백업으로 컴플라이언스 리스크 완화

5 CISO 권한 확대 및 조직 재편

SIEMENS

내용
- CISO 보고 체계를 이사회 직속으로 권한 상향 조정
- 분산된 보안 기능/조직을 중앙 사이버보안 거버넌스 체계로 통합

기대 효과
- CISO-이사회 직속 보고 체계로 보안 리스크 대응력·투명성 제고
- 보안 기능의 통합 관리로 전사 의사결정 속도 및 실행력 향상

Walmart

내용
- CISO를 부사장(EVP) 직급으로 격상 및 전사 보안 전략/리스크/운영 총괄 책임자로 역할 확대

기대 효과
- EVP·CISO 겸임 체계를 통해 보안·리스크 의사결정의 전략적 일관성 강화
- 단일 책임자 아래 기능 통합으로 보안 운영 효율 향상

1. 데이터를 특정 국가·지역에만 저장·암호화해 운영하며, 조직이 데이터 접근·보안을 직접 통제하는 협업 환경
2. EU는 GDPR·Schrems II 판결 이후 세계에서 가장 강도 높은 개인 데이터 보호·국외 이전 규제를 적용

Source: EY Analysis

04

국내 사이버보안 현주소

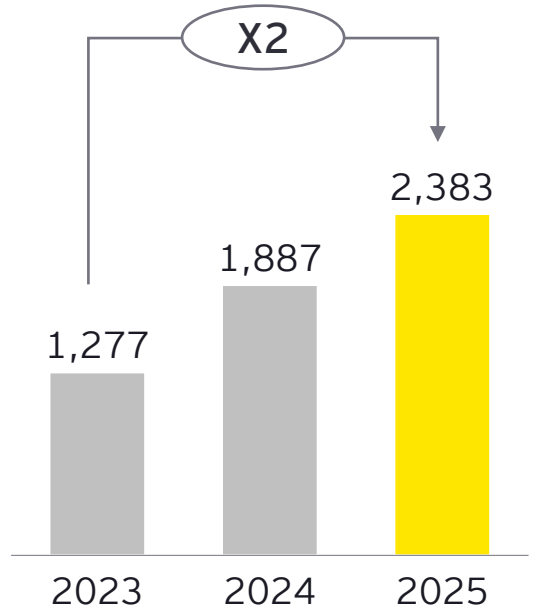
04

국내 사이버보안 사고 추이 및 대응 현황

국내 사이버보안 사고는 증가하는 반면, AI 기반 위협 대응 체계는 아직 초기 단계에 머물러 있음

국내 사이버 침해사고 추이

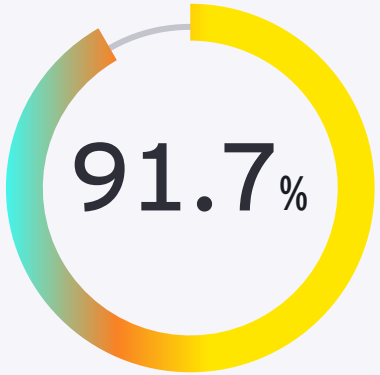
단위: 건



국내 기업 사이버보안 현황

Q AI 기반 공격에 대한 대응 역량 수준은 어느 정도인가?

"전혀 자신 없다"



사이버보안 준비도 '성숙' 수준 기업

3%

지난 1년간 AI 관련 보안 사고 경험 기업

83%

'25년 주요 사이버보안 사고 피해 규모

국내 인구 규모를 뛰어넘는 대규모 데이터 유출

> 7,000만 명

- 3,370만 명 유통사 A사
- 2,696만 명 통신사 B사
- 297만 명 카드사 C사
- 611만 명 게임 개발사 D사
- ...

Source: 과학기술정보통신부, KISA, IDC (아시아·태평양 지역 기업 보안/IT 의사결정자 대상 서베이), CISCO (30개국의 8,000명 이상의 보안 및 비즈니스 리더를 대상으로 한 사이버보안 준비 지수 서베이), EY Analysis

국내 기업의
사이버보안 미흡 원인

국내 사이버보안의 취약성은 단일 요소의 문제가 아닌, 조직·거버넌스·자원·시스템 전반에 걸친 구조적 한계에서 비롯됨

시스템 미흡 요인

거버넌스 체계 미비

79%

IT팀이 직원의 외부 AI 사용 여부를 파악하지 못하는 기업

- 민감 데이터 외부 노출 가능성 증가
- 보안 통제가 어려운 블라인드 존 발생

보안 시스템 파편화

66%

10개 이상의 개별 솔루션 사용으로 위협 탐지에 어려움을 겪는 기업

- 위협 탐지 정확도 및 속도 저하
- 사고 원인 추적/단일화된 대응 어려움

자원 부족 요인

보안 투자 부족

< 33%

IT 예산의 10% 이상을 보안에 배정한 기업

- 노후화된 보안 시스템 지속
- 사고 발생 시 피해·비용 증가

보안 인력 부족

97%

숙련된 보안 인력 수급에 어려움을 겪는 기업

- 사고 대응 속도 저하
- 신규 AI 기반 공격 대응 역량 부족

Source: Cisco, EY Analysis

05

전략적 과제 및 기업 시사점

05

AI 사이버보안 관리 프레임 재설계

AI 환경에서의 사이버보안 핵심은 AI 활용 全 과정에 대한 통제·관리 체계를 확보하는 데 있음

AI Cybersecurity 통제 범위

- 활용 목적, 범위 기준
- 데이터·모델 사용 경계
- 책임 및 의사결정 구조
- 운영 투명성·추적성
- 전사 리스크 통합 관리

"AI Cybersecurity는 AI 활용 전 과정에 대한 관리·통제 체계를 보안 오케스트레이션[1]을 통해 통합 운영하는 데서 출발함"

AI 사용의 허용 범위 정의

- 업무별 AI 활용 세부 범위·제한 조건 명확화
- 고위험 영역(고객 데이터·자동 의사결정 등)의 사전 분류

AI 책임 구조 명확화

- 모델 개발·운영·활용 조직 간 책임 구분 및 분리
- 사고 발생 시 의사결정 프로세스 사전 수립

AI 통제 단위 재정립

- 시스템 중심 단위 → 데이터·모델·출력 경로 단위로 통제로 전환
- 입력·출력 로그 상시 관리 체계 구축

AI 리스크 관리 체계의 전사 확장

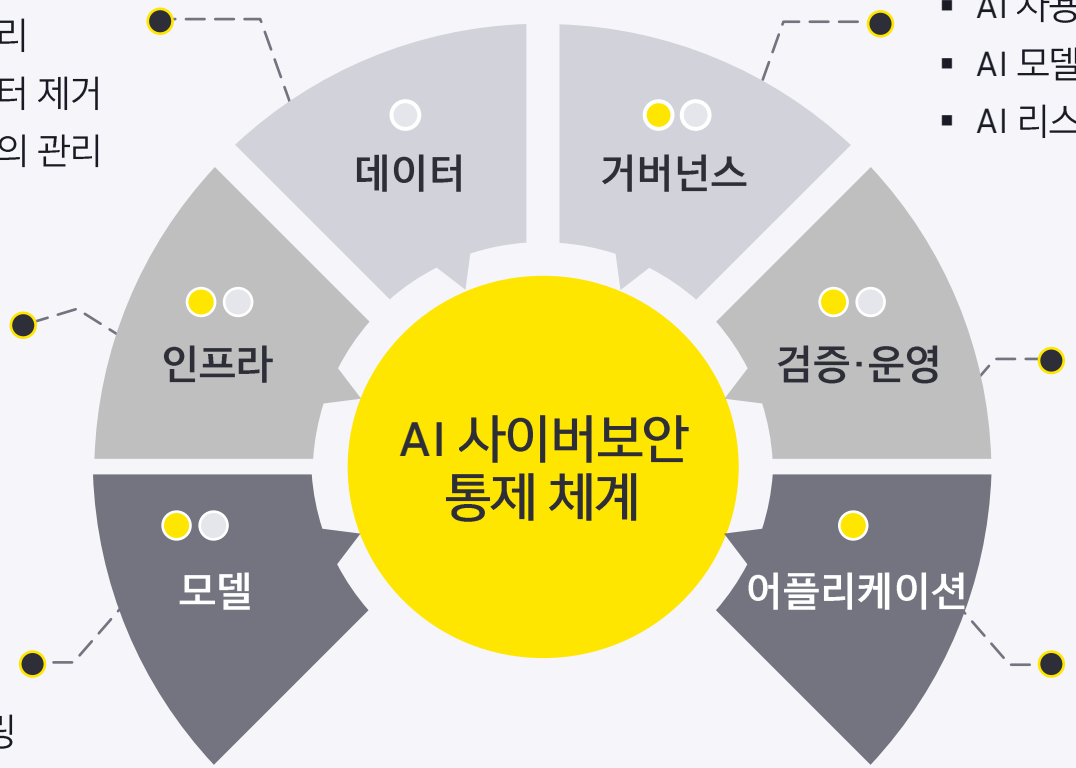
- IT 부서 중심 → 법무·리스크·현업 공동 관리 체계 수립
- AI 리스크를 기업 리스크 프레임에 편입

1. Security Orchestration: 여러 보안 시스템을 통합해 탐지·대응 등 보안 운영을 일관되게 관리하는 보안 운영 체계
Source: EY Analysis

AI 사이버보안 통제 범위 체계화

AI 보안 통제는 개별 시스템이 아닌, 데이터 모델·운영·거버넌스를 포괄하는 '全 주기 관리 체계'로 재정의되어야 함

적용 주체: 모델 개발 조직 모델 활용 조직



- 개인정보 최소화·비식별화 통제
- 학습 데이터 승인·적합성 관리
- 학습 데이터 정제·유해 데이터 제거
- 사용자 데이터 수집·활용 동의 관리

- AI 사용자 대상 보안·프라이버시 정책·교육 체계
- AI 모델·제품 보안 거버넌스 수립
- AI 리스크 식별·측정·모니터링 체계

- AI 모델·데이터 자산 목록 관리
- 모델·데이터 접근 권한 통제
- 모델·데이터 무결성 보호
- 보안 내재화 AI 개발 환경 조성 (Secure-by-default)

- AI 보안 모의해킹 및 적대적 테스트
- 취약점·보안 수준 저하 지속 관리
- AI 자산 위협 탐지·모니터링
- AI 보안·프라이버시 사고 대응 관리

- 입력 검증·적대적 프롬프트 차단
- 모델 출력 검증·유해 콘텐츠 필터링
- 적대적 학습·공격 내성 테스트

- 애플리케이션 접근·엔드포인트 통제
- 에이전트·플러그인 사용자 승인 관리
- 에이전트·플러그인 최소 권한 통제
- 사용자 투명성·통제 권한 관리

Source: EY Analysis

국내 기업 시사점

AI 경쟁력의 지속 가능성은 활용 확산 속도에 상응하는 보안 관리 역량 확보를 전제로 함

현황 진단

AI 활용 확대에 따른 보안 관리 수준 점검

- 다수 기업에서 AI 도입·활용 속도가 보안 체계 정비보다 빠르게 진행, 이로 인해 일정 시점 이후 AI **활용 자체가 리스크 요인으로 전환**
- 선도 기업일수록 AI **활용 계획과 보안 준비 수준을 동시 점검**

정책·기준 수립

AI 활용 범위 및 허용 기준 정립

- AI 활용은 확산되고 있으나, 허용·제한 기준은 명확하지 않은 경우가 다수
- 사고 발생 시 기술 문제가 아닌 **의사결정 기준 부재**가 원인으로 작용
- 글로벌 기업은 AI 사용 목적/범위별 기준을 선제적으로 정립

조직·책임 구조 정립

AI 보안 리스크 관리 책임 구조 정립

- 실제 보안사고는 해킹보다 **권한 관리, 사용 통제, 책임 구조 미비**에서 발생
- IT·보안 부서 단독 대응은 관리 공백을 확대
- AI 보안을 전사 리스크 관리 이슈로 다루는 기업이 증가

운영 통제

AI 시스템 보안 검증·모니터링 운영

- AI 시스템은 운영 과정에서 **입력, 데이터, 사용 방식 변화에 따라 리스크 특성이 달라지는 구조**
- 기존 도입 시점 중심의 일회성 점검 중심 보안 방식은 AI 환경에 부적합
- AI 보안은 도입 단계의 통제 설계와 운영 단계의 지속적 검증이 요구되는 영역

Source: EY Analysis

Contacts

EY한영 산업연구원

산업연구원장
권영대 파트너
young-dae.kwon@kr.ey.com

실무 총괄
김광현 상무
kwanghyun.kim@kr.ey.com

Team Member
김규민 매니저
gyumin.kim@kr.ey.com

Team Member
조아미 시니어
amy.killick@kr.ey.com

EY한영 Cybersecurity 전문가

Cybersecurity Lead
김상우 파트너
sang-woo.kim@kr.ey.com

Cybersecurity 담당
우문호 파트너
moonho.woo@kr.ey.com

Finance Security Lead
오준모 파트너
joon-mo.oh@kr.ey.com

EY한영 산업연구원 소개

국내외 경영 환경의 변화와 주요 산업 동향을 분석한 EY한영만의 인사이트를 제공합니다. 이를 통해 기업들이 급변하는 경영 환경 속에서도 주요 산업군의 변화와 트렌드를 선제적으로 파악하고,비즈니스 전략 수립을 할 수 있도록 지원하는 EY한영의 Think Tank의 역할을 수행하고 있습니다.

「산업별 인사이트와 전략적 시사점을 통해 시장 내 Thought Leadership을 선도」

1 산업 및 경영환경에 대한 연구과제 수행

- EY 글로벌 네트워킹을 통해 주요 산업·기능별 최신 리서치와 자료 확보
- 통합적 시각에서 산업별 주요 이슈를 분석한 리포트 정기 발간
- 시장 변화의 실질적인 영향력과 시사점을 분석하여 기업에 전략 방향성 제시

2 다양한 이해관계자 대상 지식 및 인사이트 공유

- 주요 산업 이슈 및 최신 경영 트렌드 중심의 세미나 정기 개최
- 업계 및 학계 등 대상 기관에 맞춤화된 강연을 통해 차별적인 경영 전략 제시

EY한영 마켓 인사이트

Insight Report 자료실 (Link)

Business Insights

Sector Insights

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

APAC No. 05001305
ED None

ey.com/kr