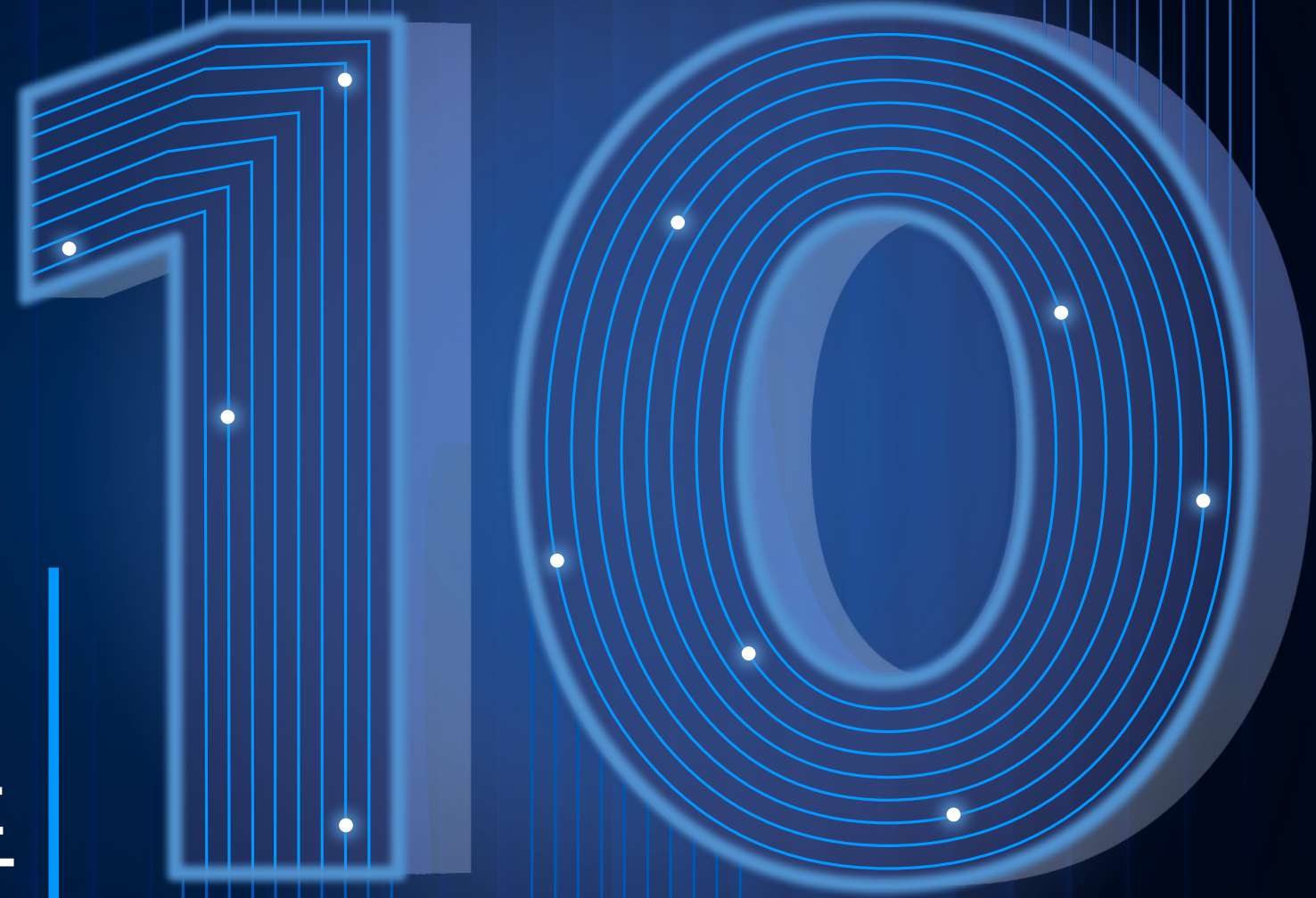


Gartner®



2026년 10대
전략 기술 트렌드

AI가 주도하는 초연결 세계에서 길을 찾다

2026년은 기술의 변화, 혁신, 위험이 전례 없는 속도로 확산되는 해가 될 것입니다. 가트너가 선정한 '2026년 10대 전략 기술 트렌드'는 단순한 기술 변화가 아니라, 비즈니스 혁신을 이끄는 촉매제이며 경영진의 적극적인 대응을 요구합니다.

올해의 트렌드는 AI 중심의 초연결 사회에서 단일 역량만으로는 충분하지 않다는 현실을 반영합니다. 가트너는 이를 바탕으로, 선도 기업들이 혁신하고 경쟁하며 가치를 보호하는 방식을 세 가지 주제로 제시했습니다.



설계자 (The Architect)

AI 네이티브 개발 플랫폼, AI 슈퍼컴퓨팅 플랫폼, 컨피덴셜 컴퓨팅 등을 통해 안전하고 확장 가능하며 유연한 디지털 기반을 구축합니다.



융합자 (The Synthesist)

다중 에이전트 시스템, 도메인 특화 언어 모델, 피지컬 AI 등 다양한 기술을 조율해 새로운 가치를 창출합니다.



개척자 (The Vanguard)

선제적 사이버 보안, 디지털 출처, AI 보안 플랫폼, 지리적 이전을 통해 신뢰와 거버넌스, 보안을 한층 강화합니다.

이 트렌드들을 살펴보고, 귀사의 전략적 목표와 어떻게 부합하는지, 지속 가능한 성장과 경쟁력을 위해 이를 어떻게 계획에 통합할 수 있을지 고민해보시기 바랍니다.



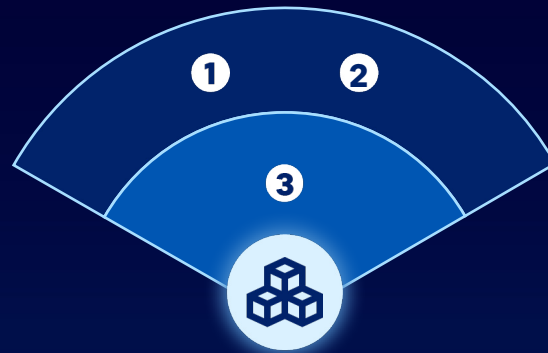
진 알바레즈 (Gene Alvarez)
가트너
비즈니스 및 기술 인사이트 총괄 부사장

가트너 2026년 10대 전략 기술 트렌드

가트너는 인공지능이 주도하는 초연결 세계에서 혁신을 촉진하고, 회복탄력성을 강화하며, 신뢰를 높일 수 있는 잠재력을 기준으로 10가지 트렌드를 신중하게 선정했습니다.

이 트렌드들은 기술 리더들이 깊이 있는 고민과 결단력 있는 실행을 통해 대응해야 할 전략적 과제들을 의미합니다.

● 현재 1-3년 ○ 가까운 미래 3-5년



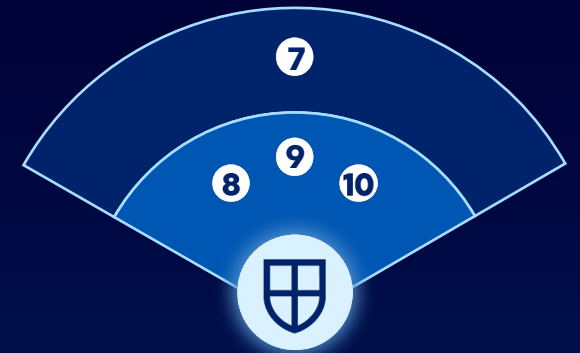
설계자

- ① AI 네이티브 개발 플랫폼
- ② AI 슈퍼컴퓨팅 플랫폼
- ③ 컨피덴셜 컴퓨팅



융합자

- ④ 다중 에이전트 시스템
- ⑤ 도메인 특화 언어 모델
- ⑥ 피지컬 AI



개척자

- ⑦ 선제적 사이버보안
- ⑧ 디지털 출처
- ⑨ AI 보안플랫폼
- ⑩ 지리적 이전



설계자

보안성 · 확장성 · 적응력을 갖춘
디지털 기반을 구축하세요.

혁신과 회복력을 가속화하려면 기술 리더들은 플랫폼과 인프라를 현대화해야 합니다.

‘설계자(Architect)’ 트렌드는 인공지능 중심의 초연결 세계에서 성공하기 위해 속도, 보안, 확장성을 가능하게 하는 AI 대응 기반(AI-ready foundation) 구축에 초점을 맞춥니다.

1



AI 네이티브 개발 플랫폼

무엇인가요?

AI 네이티브 개발 플랫폼은 생성형 AI를 활용해 소프트웨어를 이전보다 훨씬 빠르고 쉽게 제작할 수 있도록 돕습니다. 한 번의 프롬프트로 소프트웨어를 만드는 '원샷' 도구부터, 복잡한 기술 지식 없이도 개발이 가능한 '바이브 코딩' 도구, 그리고 여러 AI 에이전트가 협력해 소프트웨어를 완성하는 방식까지 다양하게 제공됩니다.

왜 주목받고 있나요?

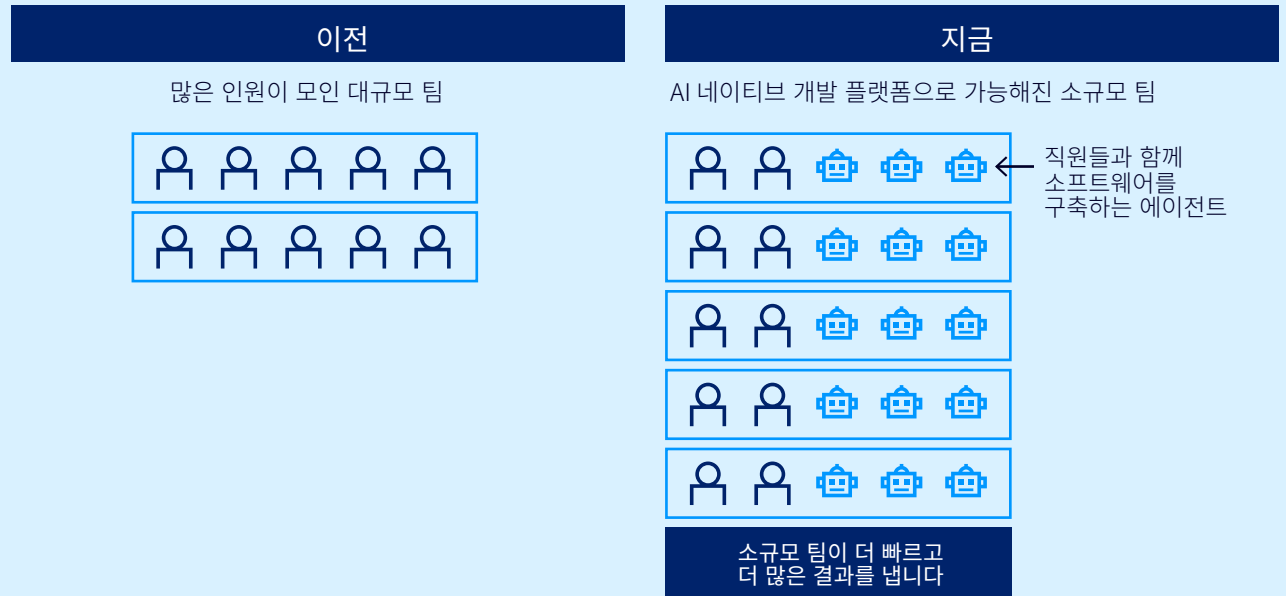
CIO는 빠른 소프트웨어 제공과 생산성 향상에 기대를 걸고 있으며, CEO와 CFO는 비용 절감의 가능성을 높게 평가합니다. AI 네이티브 개발 플랫폼은 '소규모 팀'이 동일한 자원으로 더 많은 애플리케이션을 개발할 수 있도록 지원합니다. 예를 들어, 2명으로 구성된 5팀이 동시에 5개의 앱을 출시하는 것이 가능해집니다. 이러한 트렌드는 CIO의 과제 해결에 도움을 주고, '구매 vs. 자체 개발'의 방향을 자체 개발로 전환하는 데 기여합니다.

앞으로의 전망

80%의 조직이 2030년까지 대규모 소프트웨어 엔지니어링 팀을 소규모 AI 보조(augmented) 팀으로 전환할 것입니다.

40%의 엔터프라이즈 애플리케이션 포트폴리오에는 2030년까지 AI 네이티브 플랫폼으로 개발된 맞춤형 애플리케이션이 포함될 것입니다. (2025년 2% → 2030년 40%)

소규모 팀



Source: Gartner

1



AI 네이티브 개발 플랫폼으로 성과를 실현하세요

속도 향상, 비용 절감, 혁신을 위한 실행 계획

실행 단계	1 플랫폼 전담팀 구성	2 보안 장치 구축	3 AI 네이티브 개발 시범 운영	4 AI 중심 사고방식 도입	5 팀 역량 강화 및 활성화
기대 효과	중앙 집중 관리로 표준화와 거버넌스가 일관되게 유지	안전하지 않거나 규정 미준수 코드의 위험 감소	가치를 입증하고 신뢰를 쌓을 수 있는 빠른 성과	빠르고 효율적인 제공, 혁신 역량 강화	더 넓은 도입과 효과적인 협업
실행 방안	AI 네이티브 플랫폼을 관리하고 적합한 AI 모델을 선정할 전담팀 구성	AI 거버넌스 플랫폼을 도입하여 코드 리뷰와 준수 여부 점검	생산성 향상을 검증할 수 있도록 저위험 프로젝트부터 시작	신규 개발 추진 시 AI 네이티브 도구를 우선적으로 활용	개발자와 비즈니스 파트너에게 프롬프트 엔지니어링과 거버넌스 교육을 실시

성과 달성을 이끄는 핵심 인물들

CIO	IT 파트너	비즈니스 파트너
<p>파트너: AI 중심 전략 및 거버넌스 프레임워크를 수립하세요.</p> <p>협업: 플랫폼 역량을 비즈니스 우선순위와 연계하세요.</p> <p>거버넌스: AI 네이티브 개발에 대한 준수와 보안 장치를 확보하세요.</p>	<p>플랫폼 엔지니어링: AI 네이티브 도구, 통합 및 성능을 관리하세요.</p> <p>보안: AI 거버넌스를 도입하여 코드 검토 및 리스크 관리를 강화합니다.</p> <p>구매: AI 네이티브 플랫폼 공급업체와 서비스를 평가하고 선정합니다.</p>	<p>제품 책임자: 도메인 전문성을 제공하고 AI 기반 솔루션의 효과를 검증합니다.</p> <p>재무: AI 네이티브 개발 추진을 지원할 수 있도록 자금 모델을 조정합니다.</p>

2



AI 슈퍼컴퓨팅 플랫폼

무엇인가요?

AI 슈퍼컴퓨팅 플랫폼은 첨단 AI 모델을 학습하고 운영하기 위해 필요한 막대한 처리 능력을 제공합니다. 이 시스템들은 고성능 컴퓨팅(HPC), 특화된 프로세서, 확장 가능한 아키텍처가 결합돼 데이터 집약적 작업을 효율적으로 처리합니다.

왜 주목받고 있나요?

기업들이 기존 인프라의 한계를 넘는 더욱 크고 복잡한 모델을 개발하면서, AI 슈퍼컴퓨팅에 대한 수요가 빠르게 증가하고 있습니다.

앞으로의 전망

40% 의 기업이 2028년까지 하이브리드 컴퓨팅 아키텍처를 도입할 전망입니다. (현재 8%에서 증가)

20 개 이상의 벤더가 2028년까지 슈퍼컴퓨팅 환경을 활용한 통합 개발자 플랫폼을 제공할 것으로 예상됩니다.

AI 슈퍼컴퓨팅 플랫폼



Source: Gartner

2



AI 슈퍼컴퓨팅 플랫폼으로 성과를 실현하세요

막대한 처리 성능을 이끌어내는 실행 전략

실행 단계	1 핵심 워크로드 식별	2 통합 소프트웨어 스택에 투자	3 단계별 통합 전략 수립	4 환경 전반에 걸친 개발 효율화	5 거버넌스 및 컴플라이언스 계획
기대 효과	가치 입증 및 내부 전문성 확보	통합 단순화 및 유연한 워크로드 배치	미래 대비 인프라와 인력 확보	전달 속도 향상 및 마찰 감소	리스크 감소 및 관리 강화
실행 방안	하이브리드 오케스트레이션을 활용한 파일럿 프로젝트 운영	기존 및 최신 시스템 전반에 개방형 표준을 도입	새로운 컴퓨팅 패러다임을 점진적으로 도입하고 IT 인력 교육을 실시	팀이 하이브리드 플랫폼과 조합형 아키텍처를 적극 채택하도록 독려	시스템 수준에서 보안 및 컴플라이언스 전략 설계

성과 달성을 이끄는 핵심 인물들

CIO	IT 파트너	비즈니스 파트너
<p>비즈니스 우선순위에 맞춘 하이브리드 오케스트레이션 전략을 수립합니다.</p> <p>워크로드 배치, 보안 및 컴플라이언스 관련 거버넌스를 확보합니다.</p> <p>비즈니스 리더들과 협력하여 영향력 높은 워크로드의 우선순위를 정합니다.</p>	<p>인프라 및 운영: 최신 가속기를 기존 시스템과 원활하게 연동합니다.</p> <p>보안: 다양한 아키텍처 환경에 맞는 거버넌스를 구축하세요.</p> <p>DevOps: 통합 소프트웨어 스택과 오케스트레이션 도구를 도입합니다.</p>	<p>제품: 하이브리드 컴퓨팅의 적용 사례(예: 시뮬레이션, AI 기반 앱)를 발굴합니다.</p> <p>재무: 단계별 통합과 지속 가능성 목표에 맞춰 예산을 조정합니다.</p> <p>운영: 핵심 프로세스에서 AI 기반 워크플로우에 대비하세요.</p>

3



컨피덴셜 컴퓨팅

무엇인가요?

컨피덴셜 컴퓨팅은 하드웨어 기반의 신뢰 실행 환경(TEE)을 활용하여 데이터가 처리되는 동안 외부 접근을 차단하고, 클라우드 제공업체조차 접근하지 못하도록 보호합니다.

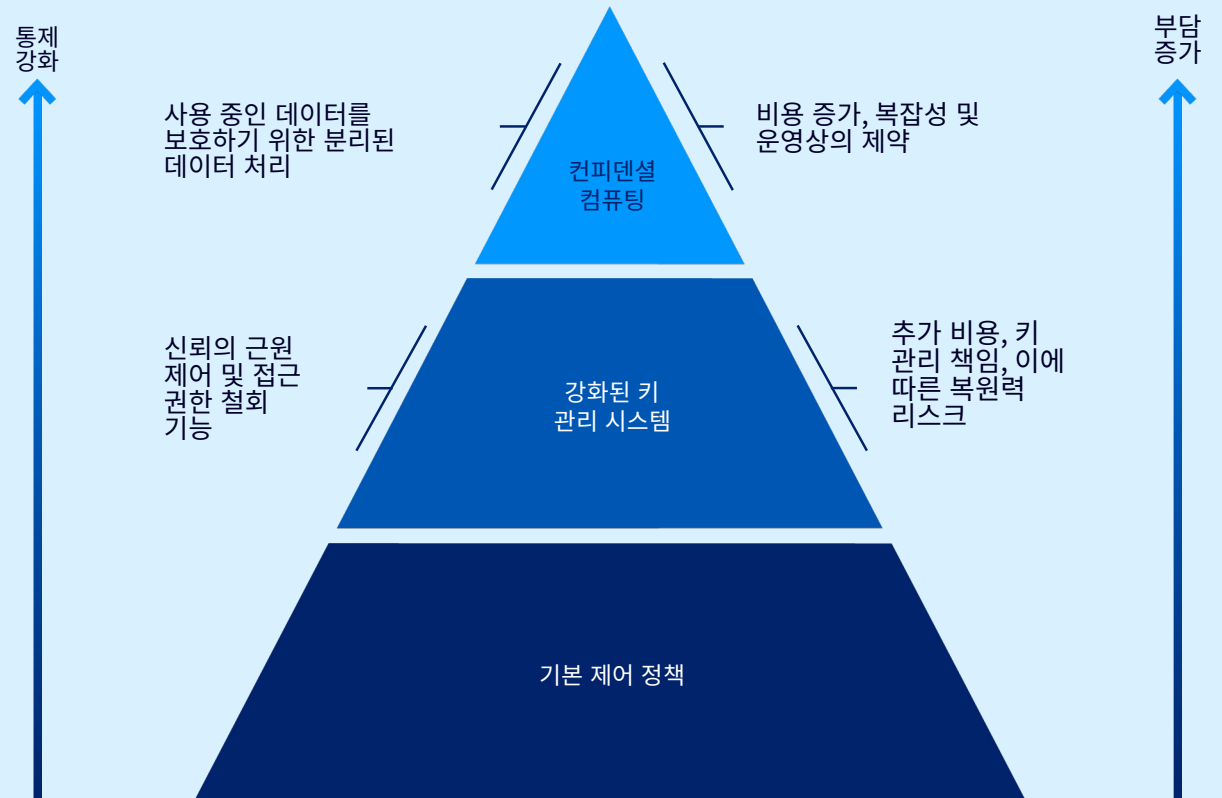
왜 주목받고 있나요?

더 엄격해진 개인정보 보호법, 데이터 현지화 규정, AI 도입 확산으로 인해 사용 중 데이터 보호가 필수가 되었습니다. 기밀 컴퓨팅은 민감한 업무에 맞는 안전한 클라우드 전략과 규제 준수를 가능하게 해줍니다.

앞으로의 전망

75% 의 데이터 처리가 컨피덴셜 컴퓨팅을 통해 2029년까지 보호될 것으로 예상됩니다.

클라우드 서비스 제공자(CSP)의 데이터 접근을 제한하기 위한 제어 장치



Source: Gartner

3



컨피덴셜 컴퓨팅으로 성과를 실현하세요

안전하고 규정에 부합하는 데이터 처리를 어디서나 실현하는 실행 계획

실행 단계	1 민감한 워크로드 감사 실시	2 AI 모델용 TEE 파일럿 실시	3 안전한 협업 환경 구축	4 독립적인 키 관리 체계 마련	5 통합 과정의 도전 과제에 대비
기대 효과	사용 중인 데이터 보호가 필요한 지점을 파악	기밀성과 지식재산 보호 강화	원시 데이터를 노출하지 않고 인사이트를 공유	데이터 접근을 완전히 제어	환경 전반에 걸친 원활한 배포
실행 방안	개인정보 보호 또는 지역화 규정이 적용되는 워크로드를 체계적으로 파악	독자적 및 오픈소스 AI 모델을 활용해 하드웨어 기반 신뢰 실행 환경(TEE)을 시험 운영	분석 및 BI 프로젝트에 기밀 컴퓨팅을 적용	조직이 직접 소유한 암호화 키 시스템을 도입	다양한 칩셋과 공급업체를 아우르는 오케스트레이션 전략을 수립

성과 달성을 이끄는 핵심 인물들

CIO

컨피덴셜 컴퓨팅 전략을 개인정보 보호, 컴플라이언스, 클라우드 목표와 연계하여 수립합니다.

법무 및 컴플라이언스 팀과 협력하여 데이터 지역화 및 주권 요건을 충족합니다.

TEE 거버넌스를 관리하고 기존 보안 프레임워크와의 통합을 보장합니다.

IT 파트너

인프라 및 운영:하이브리드 및 멀티클라우드 환경에 TEE를 배포합니다.

보안:인증 절차와 암호화 키 관리 시스템을 구축합니다.

DevOps 및 플랫폼:보안 컴퓨팅에 맞게 워크로드를 최적화하고 성능을 모니터링합니다.

비즈니스 파트너

컴플라이언스:관련 규제에 부합하는지 검증하고 감사 준비 상태를 점검합니다.

재무:보안 컴퓨팅 도입과 리스크 관리에 필요한 자금 계획을 수립합니다.

데이터 소유자:사용 중 보호가 필요한 민감한 워크로드를 식별하고 우선순위 프로젝트를 선정합니다.



융합자

다양한 기술을 융합해 새로운 가치를 창출하세요.

차별화의 새로운 원천을 발굴하기 위해, 기술 리더들은 도메인별 솔루션을 위해 특화된 모델, 멀티에이전트 시스템, 물리적 AI를 통합해야 합니다. '융합자(Synthesist)' 트렌드는 이러한 다양한 기술을 유기적으로 결합해 워크플로우, 제품, 경험 전반에서 혁신을 이끄는 적응형 지능형 생태계를 구축하는 데 초점을 맞춥니다.

4



다중 에이전트 시스템

무엇인가요?

다중 에이전트 시스템(MAS)은 다양한 역할의 AI 에이전트들이 협력하여 복잡한 작업을 처리하는 방식입니다. 각 에이전트가 특정 업무를 담당해, 기존의 단일 AI 솔루션보다 효율성과 확장성을 높입니다.

왜 주목받고 있나요?

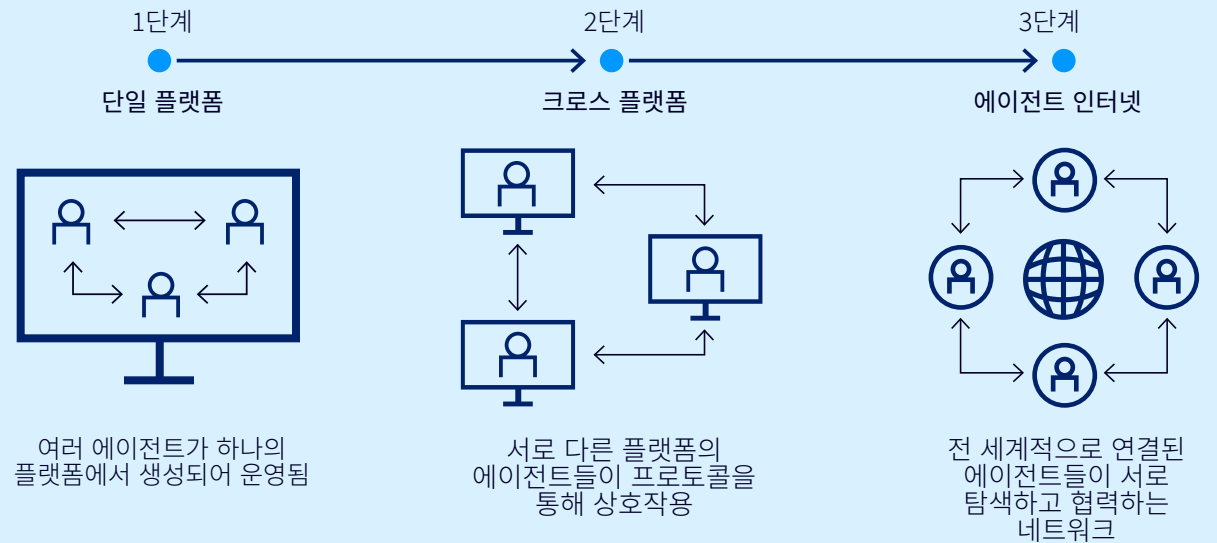
단일 에이전트 AI가 복잡한 과정을 처리하는 데 한계를 보이면서, MAS는 모듈형 자동화와 플랫폼 간 연동을 실현합니다. 1Q24~2Q25 동안 MAS 관련 문의가 1,445% 급증해 기업들의 관심이 빠르게 높아지고 있음을 보여줍니다.

앞으로의 전망

70%의 다중 에이전트 시스템이 2027년까지 특정 분야에 특화된 에이전트를 활용하게 돼 정확도는 향상되지만 조정의 복잡성은 증가할 것입니다.

60%의 다중 에이전트 시스템이 2028년까지 다양한 공급업체 간 상호운용성을 지원하게 돼 혁신과 유연성이 강화될 것입니다.

다중 에이전트 시스템의 진화



Source: Gartner

4



다중 에이전트 시스템으로 성과를 실현하세요

모듈형 자동화와 매끄러운 통합을 위한 실행 계획

실행 단계	1 고가치 활용 사례 식별	2 모듈형 에이전트 설계	3 거버넌스 및 가시성 구현	4 상호운용성 표준 적용	5 팀 역량 강화
기대 효과	측정 가능한 성과와 빠른 도입	신뢰성과 확장성 향상	리스크 감소 및 제어 강화	미래에도 유효한 MAS 투자 실현	효율적인 도입과 위험 최소화
실행 방안	MAS 파일럿을 위한 명확한 워크플로우로 시작	하나의 큰 솔루션 대신 특화된 에이전트를 구축	강력한 API 거버넌스와 모니터링 도구를 적용	다중 공급업체 협업을 위한 최신 프로토콜 활용	MAS 프레임워크와 변화 관리에 대해 직원 교육을 실시

성과 달성을 이끄는 핵심 인물들

CIO	IT 파트너	비즈니스 파트너
<p>가치가 높은 업무에 적합한 MAS 전략을 수립하고 비즈니스 우선순위와 연계하세요.</p> <p>에이전트 간 상호운용성, 보안, 컴플라이언스를 위한 거버넌스를 구축하세요.</p> <p>변화 관리 계획을 공유하여 구성원의 우려를 해소하세요.</p>	<p>플랫폼 및 DevOps: 모듈형 에이전트 설계 및 오케스트레이션 도구 관리</p> <p>보안: API 거버넌스를 적용하고 에이전트 상호작용을 지속적으로 모니터링합니다.</p> <p>통합팀: 상호운용성 및 가시성을 위한 표준을 도입합니다.</p>	<p>프로세스 책임자: MAS 파일럿을 위한 워크플로를 선정하고 결과를 검증합니다.</p> <p>재무: 예상치 못한 비용을 관리하고 가시성 도구에 투자합니다.</p> <p>운영: 사람과 에이전트의 협업과 교육 프로그램을 지원합니다.</p>

5



도메인 특화 언어 모델

무엇인가요?

도메인 특화 언어 모델(DSLM)은 특정 산업이나 업무 분야를 위해 전문 데이터셋으로 학습된 AI 모델로, 범용 대형 언어 모델(LLM)보다 더 높은 정확성과 규정 준수를 제공합니다.

왜 주목받고 있나요?

경영진은 AI에서 실제 비즈니스 가치를 요구합니다. DSLM은 오류를 줄이고, 도입 속도를 높이며, 금융·헬스케어·인사 등 핵심 업무의 비용을 절감합니다.

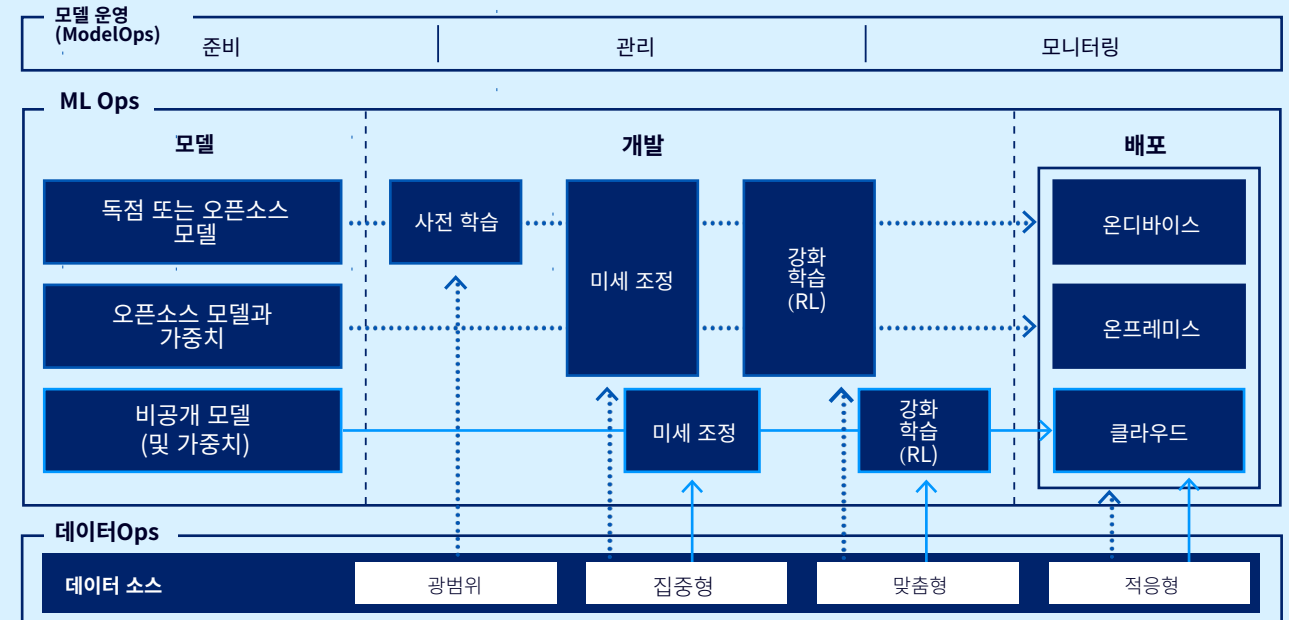
앞으로의 전망

60% 이상의 엔터프라이즈 생성형 AI(GenAI) 모델이 2028년까지 도메인 특화형으로 발전할 것입니다.

30%의 생성형 AI 워크로드가 2028년까지 온프레미스 또는 디바이스 내에서 도메인 특화 언어 모델을 활용해 운영될 것입니다.

DSLML 구축을 위한 다양한 경로

- 직접 운영할 수 있는 선택지 — 외부 API 연동



Source: Gartner

5



도메인 특화 언어모델(DSLM)로 성과를 실현하세요

정확하고 산업 특화된 규정 준수를 실현하기 위한 실행 계획

실행 단계	1 성공 사례 선정	2 데이터 거버넌스 강화	3 핵심 분야에서 DSLM 시범 운영	4 다분야 협업팀 구축	5 성과 모니터링 및 최적화
기대 효과	빠른 투자 회수와 정확성 향상	신뢰할 수 있고 규정에 맞는 DSLM 결과 제공	측정 가능한 비즈니스 가치 입증	원활한 통합과 도입 촉진	지속 가능한 성과와 비용 관리
실행 방안	일반 LLM이 성과를 내지 못하는 업무 프로세스에 집중	강력한 개인정보 보호와 품질 관리 체계 구축	금융, 헬스케어 또는 HR 프로세스 등에서 시범 적용	DSLМ 프로젝트에 IT, 분야별 전문가, 컴플라이언스 부서를 함께 참여	설명 가능성 및 컴플라이언스 프레임워크를 적용

성과 달성을 이끄는 핵심 인물들

CIO

규제가 적용되는 고가치 분야를 위한 DSLM 전략을 수립하세요.

정확성, 컴플라이언스, 설명 가능성을 위한 거버넌스를 확립하세요.

ROI 및 리스크 관리 목표와 DSLM 도입을 연계하세요.

IT 파트너

데이터 및 분석: 도메인별 데이터셋을 준비하고 품질을 유지하세요.

ModelOps: 모델 미세 조정, 모니터링 및 전체 라이프사이클 관리 체계 구축

Security: DSLM 도입 시 개인정보 보호와 규제 준수 철저히 이행

비즈니스 파트너

Domain experts: DSLM 결과의 정확성과 적합성 검증

Finance: DSLM 도입 예산 및 비용 최적화 계획 수립

Compliance: 법규 및 규정 준수 보장

6



피지컬 AI

무엇인가요?

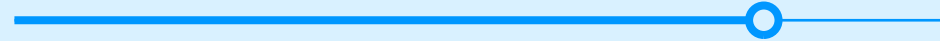
피지컬 AI는 로봇, 드론, 차량, 스마트 기기 등을 통해 실세계에 지능을 구현합니다. 센서, 작동기, AI 모델을 결합하여 다양한 물리적 작업을 자동화하는 시스템입니다.

왜 주목받고 있을까요?

기업들은 디지털 AI의 생산성을 실제 환경에도 적용하기를 원합니다. 2028년까지 상위 10개 AI 공급업체 중 5곳이 피지컬 AI 제품을 선보일 예정입니다.

앞으로의 전망

80% 의 참고에 2028년까지 로봇 또는 자동화 기술을 도입될 예정입니다.



AI 분류

사례



수요 예측



챗봇



추천 시스템

101100
010110
디지털 AI



AI
인공지능

피지컬 AI

사례



산업용 로봇



생체 모방 로봇/
범용 로봇



자율 기기



웨어러블
기기

Source: Gartner

6



피지컬 AI로 성과를 실현하세요

현실 업무 자동화와 생산성 극대화를 위한 실행 계획

실행 단계	1 운영 영역 점검	2 피지컬 AI 시스템을 시범 운영	3 분야별 협업팀을 구성	4 이해관계자에게 교육 제공	5 다중 에이전트 협업 계획
기대 효과	자동화와 비용 절감이 가능한 영역 파악	성과와 투자 대비 효과 검증	효과적인 관리 체계와 통합 운영	혼란과 잘못된 투자 방지	향후 변화에도 대응 가능한 도입
실행 방안	물류, 유지관리, 안전 업무 집중	실제 배포 전에 시뮬레이션과 디지털 트윈을 활용	IT, 운영팀, 엔지니어링 부서를 계획 단계에 포함	피지컬 AI, 임베디드 AI, 엣지 AI의 차이점을 명확히 구분	다수의 장치 관리를 위한 오케스트레이션 플랫폼을 탐색

성과 달성을 이끄는 핵심 인물들

CIO

피지컬 AI 전략을 운영 목표에 맞춰 수립하세요.

안전성, 신뢰성, 설명 가능성을 위한 관리 체계를 마련하세요.

운영 및 엔지니어링 부서와 협력하여 통합 및 리스크 관리에 힘쓰세요.

IT 파트너

인프라 및 운영: 물리적 AI를 IoT 및 기존 시스템과 통합하세요.

보안: 자율 시스템을 위한 보호 장치를 구축하세요.

데이터 및 분석: 시뮬레이션과 디지털 트윈 테스트를 지원하세요.

비즈니스 파트너

운영: 가치가 높은 활용 사례를 파악하고 성능을 검증하세요.

재무: 로봇 및 자동화 투자 예산을 편성하세요.

컴플라이언스: 안전 및 규제 기준을 반드시 준수하세요.



개척자

신뢰, 거버넌스, 그리고 보안을
한 단계 높이세요.

리스크와 규제 심사가 강화되는 시대에 신뢰는 타협할 수 없는 요소입니다. '개척자(Vanguard)' 트렌드는 선제적 보안, 투명한 거버넌스, 디지털 무결성을 강조하며, 이를 통해 조직이 평판을 보호하고, 규정을 준수하며, 이해관계자의 신뢰를 유지하면서 AI와 디지털 전환을 확장할 수 있도록 지원합니다.

7



선제적 사이버보안

이게 무엇일까요?

선제적 사이버 보안(PCS)은 첨단 AI 기반 기술을 활용해 사이버 공격을 사전에 예측, 차단, 무력화합니다. 전통적인 탐지와 대응을 넘어 한발 앞선 보호를 실현합니다.

왜 주목받고 있을까요?

AI 기반 위협이 폭발적으로 증가하며 네트워크, 애플리케이션, IoT 시스템을 겨냥하고 있습니다. 2029년까지 사전 대응형 사이버 보안을 갖추지 않은 기술 제품은 시장 경쟁력을 잃게 되며, 선제적 방어가 필수 요건으로 자리잡게 될 것입니다.

기술 및 서비스 제공업체를 위한 맞춤형 인사이트가 필요하신가요? 벤더를 위한 사전 예방형 사이버 보안에 관한 아티클을 확인해 보세요.

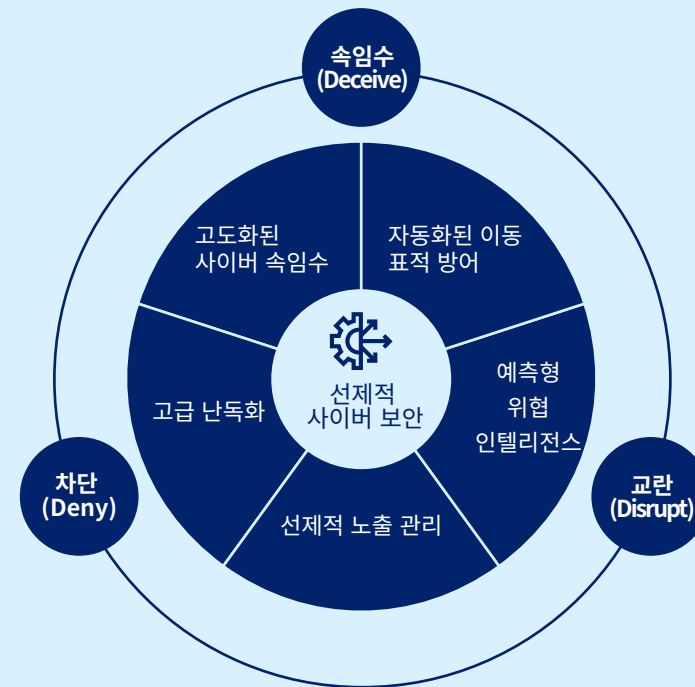
선제적 사이버 보안 솔루션, 지금 바로 구축하세요 .

앞으로의 전망

50% 의 보안 소프트웨어 지출이 선제적 보안 솔루션에 투입될 것으로 예상됩니다.

100만 건 이상의 보안 취약점이 매년 보고될 것으로 예상됩니다.

선제적 사이버 보안의 3D(Deceive, Deny, Disrupt) 전략



Source: Gartner

7



선제적 사이버보안(PCS)으로 성과를 실현하세요

위협 발생 전에 자산을 보호하기 위한 실행 계획

주요 단계	1 현재 보안 아키텍처 평가	2 고위험 영역에서 PCS 시범 진행	3 공급업체 선정 기준 수립	4 PCS 전략을 사내 확산	5 기존 보안 도구와 PCS 통합
기대 효과	취약점을 파악하고 PCS 투자 우선순위화	정량화 가능한 위험 감소 입증	장기적으로 유효한 PCS 도입을 보장	경영진과 이사회 차원의 지지를 확보	ROI를 극대화 및 도입 가속화
실행 방안	위험 분석 및 준비 상태 점검을 실시	예측형 위협 방지 및 기반 기술을 구현	선제적 대응 역량을 위한 상세 로드맵을 마련하세요.	PCS가 비즈니스에 미치는 영향과 투자 수익을 명확히 전달	현재 보안 및 컴플라이언스 프로세스와 PCS를 효과적으로 결합

성과 달성을 이끄는 핵심 인물들

CIO

주도적으로 수동적 보안에서 선제적 보안 전략으로의 변화를 이끌어갑니다.

PCS 역량을 위한 구매 기준을 정의하고, 임원진에게 교육합니다.

적극적인 방어 및 컴플라이언스 거버넌스를 감독합니다.

IT 파트너

보안: 위협 예측과 탐지 기술을 도입합니다.

인프라 및 운영: 클라우드, OT, 사이버-물리 시스템에 PCS를 통합합니다.

리스크 및 컴플라이언스: 개인정보 보호와 관련 규정 준수를 확실히 합니다.

비즈니스 파트너

재무: PCS 파일럿 및 장기 도입을 위한 예산을 편성합니다.

운영: 안전한 디지털 혁신 프로젝트를 지원합니다.

제품: 시장 차별화를 위해 선제적 보안을 제품에 내장합니다.

8



디지털 출처

무엇인가요?

디지털 출처는 BOM(구성 명세서), 인증 데이터베이스, 워터마킹과 같은 도구를 활용하여 소프트웨어, 데이터, 미디어의 출처와 무결성을 검증합니다. 이는 외부 구성 요소와 AI 생성 콘텐츠로 구축된 시스템의 투명성과 신뢰성을 보장합니다.

왜 주목받고 있나요?

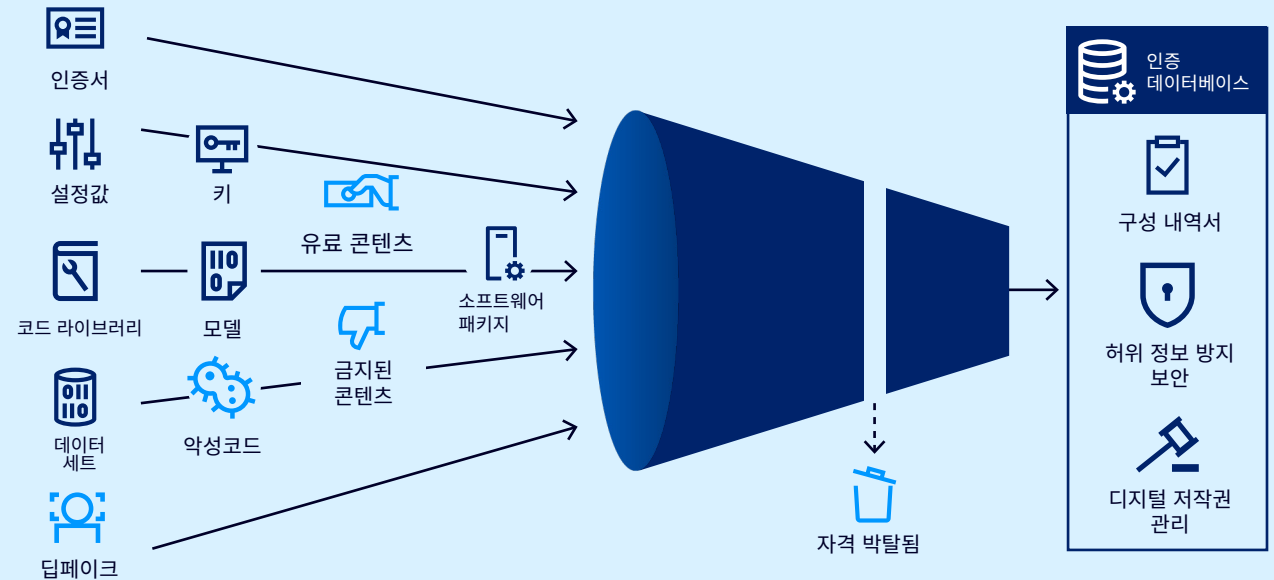
조직들은 코드 변조, 방치된 오픈소스 프로젝트, 딥페이크를 통한 허위정보 확산 등 점점 더 많은 위험에 직면하고 있습니다.

앞으로의 전망



늘어나는 규제(예: EU AI 법)는 AI 생성 콘텐츠에 워터마크와 출처 추적을 의무화하고 있습니다.

디지털 출처로 필터링하기



Source: Gartner



디지털 출처로 성과를 실현하세요

데이터와 콘텐츠의 진위를 검증하여 신뢰를 구축하는 실행 계획

주요 단계	1 BOMs(구성 명세서) 배포	2 검증 데이터베이스 구축	3 허위 정보 방지 솔루션 도입	4 디지털 워터마킹 적용	5 거버넌스 강화
기대 효과	소프트웨어의 출처 확인, 투명성 및 보안 강화에 기여	신뢰할 수 있는 중앙화된 출처 기록 확보	사칭 및 사기 행위로부터 보호	AI 콘텐츠 관련 규정 준수 확보.	법적·평판적 위험 감소.
실행 방안	소프트웨어용 SBOM, AI 모델용 MLBOM 도입	원본의 암호화된 서명 증거를 안전하게 보관	합성 신원 탐지 기능을 신원 위협 탐지 및 대응 계획에 통합	AI 생성 콘텐츠에 기계가 읽을 수 있는 형식으로 표시	IT, 컴플라이언스, 마케팅 팀 간의 협업을 강화

성과 달성을 이끄는 핵심 인물들

CIO

디지털 출처 전략을 수립하고 준수 및 위험 관리 정책과 연계합니다.

SBOM 및 인증 데이터베이스 구축을 총괄 관리합니다.

CISO 및 CMO와 협력하여 허위 정보 대응과 평판 보호를 추진합니다.

IT 파트너

DevOps: SBOM 및 MLBOM을 배포 파이프라인에 통합합니다.

보안: 허위 정보 방지 솔루션과 디지털 저작권 관리(DRM) 도입

데이터: AI 모델을 위한 학습 데이터 출처 기록

비즈니스 파트너

컴플라이언스: 새롭게 도입되는 규제 준수 보장

법무: 저작권 및 라이선스 준수 여부 검토

마케팅: 딥페이크 및 합성 콘텐츠로 인한 평판 리스크 관리

9



AI 보안 플랫폼

무엇인가요?

AI 보안 플랫폼(AISP)은 외부 AI 서비스와 자체 구축 AI 애플리케이션 모두를 안전하게 관리하는 통합 제어 기능을 제공합니다. 프롬프트 인젝션, 비정상 에이전트 행위, 데이터 유출 등 AI에 특화된 위험 요소들을 효과적으로 대응합니다.

왜 주목받고 있나요?

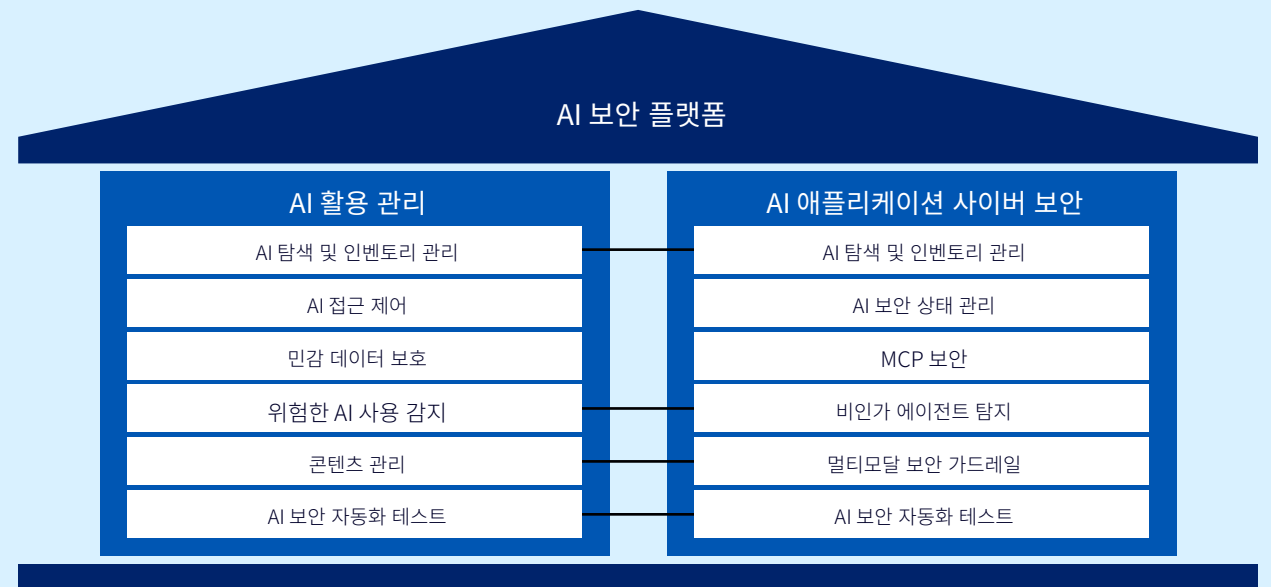
AI 도입이 빠르게 확산되면서 기존 보안 솔루션만으로는 AI 업무 흐름을 안전하게 지키기 어렵게 되었습니다.

앞으로의 전망

50% 이상의 기업이 2028년까지 AI 보안 플랫폼(AISP)을 도입할 것으로 예상됩니다.

80% 의 무단 AI 트랜잭션은 외부 공격이 아닌 내부 정책 위반에서 발생할 것으로 전망됩니다.

AI 보안 플랫폼 역량 맵



Source: Gartner



AI 보안 플랫폼(AISP)으로 성과를 실현하세요

진화하는 AI 기반 비즈니스 운영을 보호하기 위한 실행 계획

실행 단계	1 AI 위험 환경 평가	2 파일럿 AISP 솔루션 도입	3 통합 플랫폼 선호	4 보안 테스트 통합	5 공급업체 혁신 모니터링
기대 효과	현재 보안 체계의 취약점 파악	효과 및 투자 대비 성과 검증	관리 방식 단순화 및 복잡성 감소	프롬프트 인젝션에 대한 복원력 강화	신규 위협에 선제적으로 대응
실행 방안	AI 고유 리스크를 업무 프로세스 전반에 맵핑	위험도가 높은 AI 서비스와 맞춤형 애플리케이션부터 시작	AI 사용 관리와 애플리케이션 보안을 모두 지원하는 AISPs를 선택	자동화된 AI 보안 테스트를 파이프라인에 추가	스타트업과 기존 공급업체의 첨단 기능을 지속적으로 모니터링

성과 달성을 이끄는 핵심 인물들

CIO

설계 외부 및 맞춤형 AI 앱을 아우르는 AI 보안 전략을 수립하세요.

선택 통합된 AI 사용 관리와 애플리케이션 보안을 제공하는 공급업체를 선정하세요.

소통 AI 위험 현황과 준수 요구 사항을 이사회에 전달하세요.

IT 파트너

보안: 프롬프트 인젝션 및 비인가 에이전트 탐지를 위한 보호 장치를 배포하세요.

DevOps: AI 보안 테스트를 개발 파이프라인에 통합하세요.

인프라 및 운영: 클라우드와 온프레미스 환경 모두와의 호환성을 보장합니다.

비즈니스 파트너

컴플라이언스: AISP가 관련 규제 프레임워크(예: EU AI 법안)에 부합하도록 정렬합니다.

재무: 플랫폼 도입과 위험 완화에 필요한 예산을 수립합니다.

제품: AI 기반 서비스에 보안 기능을 내장합니다.

10



지리적 이전 (Geopatiation)

무엇인가요?

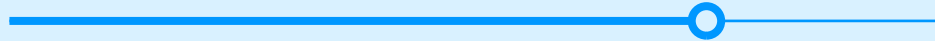
지리적 이전은 지정학적 리스크에 대응하기 위해 기업 데이터와 애플리케이션을 글로벌 퍼블릭 클라우드에서 소버린 클라우드, 지역 클라우드 공급업체, 자체 데이터센터로 이전하는 전략입니다.

왜 주목받고 있나요?

지정학적 불안정과 규제 요구로 인해, 기업들은 클라우드 의존도를 재점검하고 있습니다.

앞으로의 전망

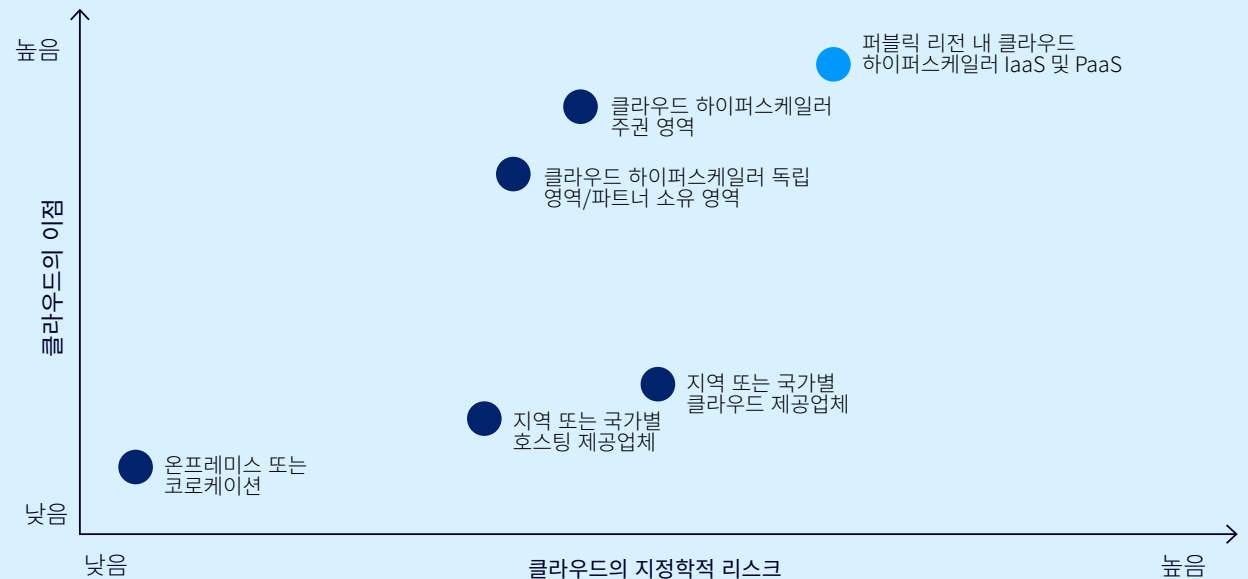
75% 의 기업이 2030년까지 워크로드를 지정학적으로 이전할 것입니다.



하이퍼스케일러와 로컬 사업자의 주권 클라우드 서비스가 빠르게 확대되고 있습니다.

클라우드의 이점과 지정학적 리스크

- 지리적 이전에 대한 대안
- 현재 일반적인 운영 형태



Source: Gartner

10



지리적 이전으로 성과를 실현하세요

핵심 디지털 업무의 현지화를 통한 리스크 완화 실행 전략

진행 단계	1 워크로드 중요도 평가	2 주권 클라우드 옵션 평가	3 하이브리드 전략 설계	4 거버넌스 통제 적용	5 지정학적 트렌드 모니터링
기대 효과	고위험 자산에 대한 지리적 이전 우선순위화	민첩성과 주권 간 균형 확보	복원력 및 성능 유지	컴플라이언스 및 보안 리스크 감소	변화하는 리스크에 선제 대응
실행 방안	업무의 민감도와 지정학적 위험성을 기준으로 점수를 산정	글로벌 하이퍼스케일러의 주권 클라우드와 지역 공급업체의 서비스를 비교	주권 클라우드를 온프레미스 또는 코로케이션과 연계해 활용	인증 및 주권 프레임워크를 도입	위험 환경이 변화함에 따라 업무 배치를 지속적으로 조정

성과 달성을 이끄는 핵심 인물들

CIO

지정학적 데이터 관리 전략을 정의하고, 주권·민첩성·회복탄력성을 균형 있게 설계하세요.

지역 공급업체와 글로벌 하이퍼스케일러의 주권 옵션 간 장단점을 평가하세요.

핵심 업무에 대한 위험 점수 산정과 컴플라이언스 준수 여부를 관리하세요.

IT 파트너

인프라 및 운영: 마이그레이션 경로와 기존 시스템과의 통합을 계획하세요.

보안: 주권 통제를 점검하고 규정 준수를 확보합니다.

클라우드 아키텍트: 업무 부담을 최적화하여 성능과 복원력을 높입니다.

비즈니스 파트너

컴플라이언스: 규제 변화와 주권 관련 지침을 지속적으로 모니터링합니다.

재무: 이전 비용과 위험 완화 투자를 예산에 반영합니다.

운영: 업무 부담 이동 중에도 지속적인 운영을 보장합니다.

실행 가능한 객관적 인사이트

IT 리더를 위한 다양한 무료 리소스와 도구를 확인해 보세요:



템플릿
IT 경영진을 위한 전략 기획 툴킷

한 장의 플래닝 템플릿으로 전략을 실행으로 연결하세요.

[템플릿 바로가기](#)



도구
가트너 벤치마킹 및 진단

더 스마트한 IT 의사결정을 위한 벤치마킹을 만나보세요.

[자세히 알아보기](#)



인사이트
2025 가트너 하이프 사이클™

2025 인공지능 하이프 사이클, 생성형 AI를 넘어 미래를 조망합니다.

[지금 살펴보기](#)



인사이트
AI 및 신기술에 관한 주요 질문

가트너 전문가가 최근 고객들이 자주 묻는 신기술 관련 질문에 빠르게 답변합니다.

[답변 확인하기](#)

이미 고객이신가요?
고객 포털에서 더 많은 리소스를 이용하세요. [로그인하기](#) ↗

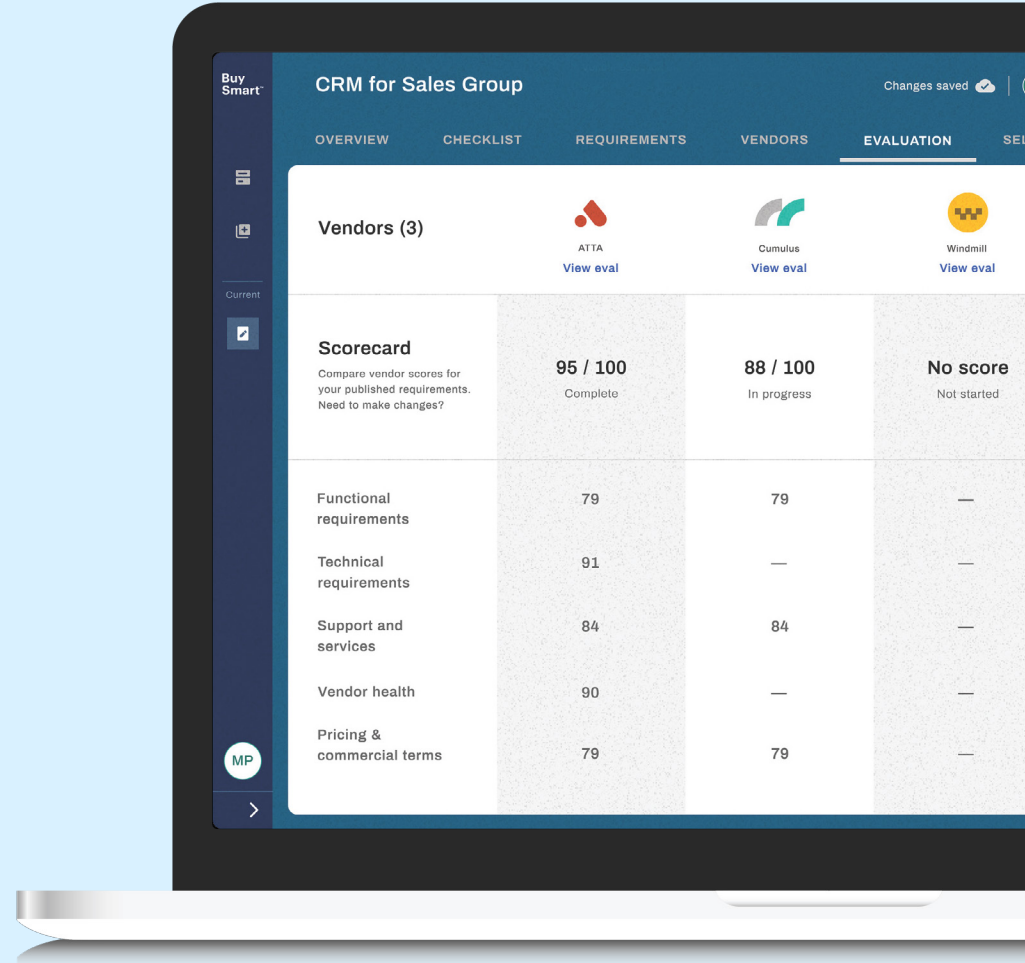


Gartner BuySmart™

팀의 기술 구매 결정을 더 쉽고 빠르게 만들어 드립니다

혜택 안내:

- 주요 기술 시장을 아우르는 100개 이상의 템플릿 이용 가능
- 미리 준비된 맞춤형 체크리스트와 요구사항 제공
- 팀의 업무 흐름을 한곳에서 지원하는 협업 기능
- 공급업체 선정에 신뢰를 더하는 표준화된 평가 시스템



[Learn More ↗](#)

Research

Shortlist

Evaluate

Negotiate

고객 지원 문의

실행 가능하고 객관적인 비즈니스& 기술 인사이트를 통해 미션 크리티컬 우선순위에 대해 더욱 현명한 의사 결정과 한층 강력한 성과를 이끌어내세요.

미국: 1 855 811 7593

해외: +44 (0) 3330 607 044

전문가에게 문의하기

최고정보책임자와 IT경영진들을 위한 가트너에 대해 더 자세히 알아보세요.

gartner.com/en/chief-information-officer

최신 인사이트를 계속 받아보세요



가트너 컨퍼런스에 참여해 보세요

[View Conference](#)