Gartner

Top 10 Strategic Technology Trends for 2026

Navigating an AI-powered, hyperconnected world

Technology leaders face a pivotal year in 2026, where disruption, innovation and risk are accelerating at unprecedented speed. The Gartner Top 10 Strategic Technology Trends for 2026 are more than technology shifts — they are catalysts for business transformation, demanding a C-Level response.

This year's trends reflect the realities of an AI-powered, hyperconnected world where no single capability is enough. They are organized into three themes that define how leading organizations will innovate, compete and protect value:

The Architect

Build secure, scalable and adaptive digital foundations with AI-native development platforms, AI supercomputing and confidential computing.

The Synthesist

Orchestrate diverse technologies — from multiagent systems to domain-specific language models and physical AI — to unlock new sources of value.

The Vanguard

Elevate trust, governance and security through preemptive cybersecurity, digital provenance, AI security platforms and geopatriation.

As you explore these trends, consider how they align with your organization's strategic ambitions and how they can be integrated into your planning to drive sustainable growth and competitive advantage.

Gene Alvarez
Distinguished Vice President, Business and Technology Insights, Gartner

Gartner Top Strategic Technology Trends for 2026

Gartner carefully selected these 10 trends based on their potential to drive innovation, strengthen resilience and elevate trust in an AI-powered, hyperconnected world.

They represent strategic imperatives that require thoughtful consideration and decisive action from technology leaders.

Now 1 – 3 years

Near 3 – 5 years

The Architect

1. AI-native development platforms
2. AI supercomputing platforms
3. Confidential computing

The Synthesist

4. Multiagent systems
5. Domain-specific language models
6. Physical AI

The Vanguard

7. Preemptive cybersecurity
8. Digital provenance
9. AI security platforms
10. Geopatriation

The Architect

Build secure, scalable and adaptive digital foundations.

To accelerate innovation and resilience, technology leaders must modernize platforms and infrastructure. The Architect trends focus on creating AI-ready foundations that enable speed, security and scalability — essential for thriving in an AI-powered, hyperconnected world.

1

AI-native development platforms

What is it?
AI-native development platforms use generative AI to create software faster and easier than ever before. These platforms range from “one-shot” tools that generate software from a single prompt, through “vibe coding” tools that enable software development without deep technical knowledge, to AI agents orchestrated together to create software.

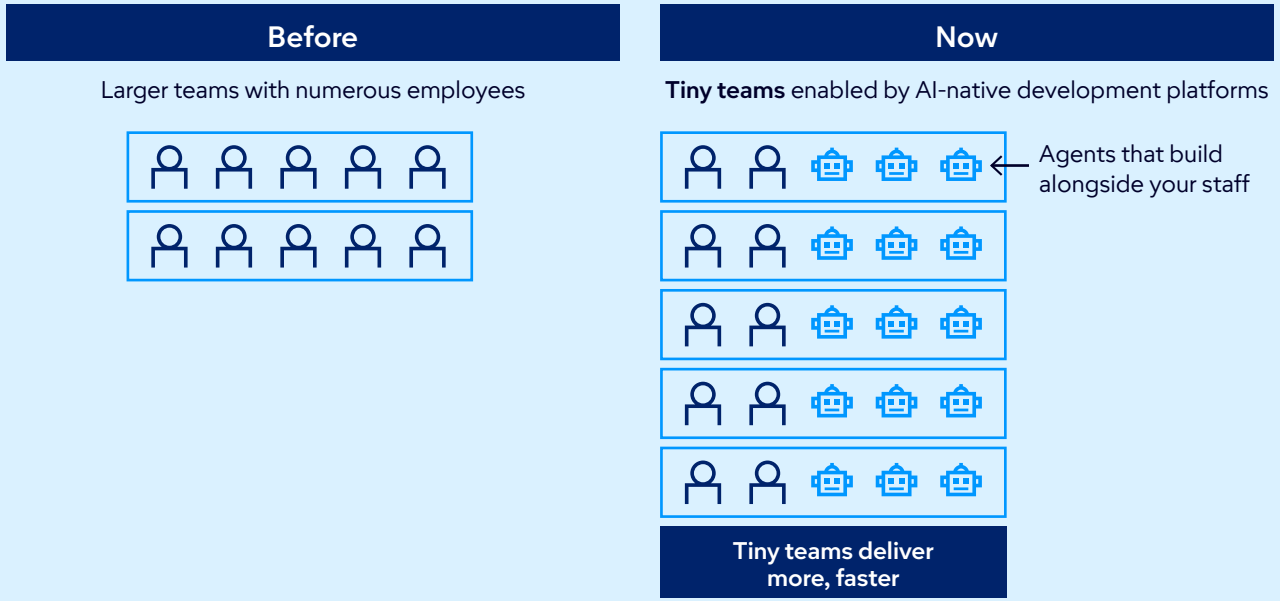
Why trending?
CIOs are enthusiastic about faster software delivery and productivity gains, while CEOs and CFOs recognize cost-saving potential. AI-native development platforms empower “tiny teams” to build more applications with the same resources — enabling, for example, five teams of two to deliver five applications at once. This trend helps CIOs address backlogs and shift the “build vs. buy” equation toward building.

What’s next

80% of organizations will evolve large software engineering teams into smaller, AI-augmented teams by 2030.

40% of enterprise application portfolios will include custom applications built using AI-native platforms by 2030 (up from 2% in 2025).

Tiny teams



Source: Gartner

1

Deliver results with AI-native development platforms

Action plan to boost speed, save costs and spark innovation

Steps	1 Establish a platform team	2 Implement security guardrails	3 Pilot AI-native development	4 Adopt an AI-first mindset	5 Upskill and enable teams
Expected outcome	Centralized oversight ensures consistent standards and governance.	Reduced risk of insecure or noncompliant code.	Quick wins that demonstrate value and build confidence.	Accelerated delivery and improved innovation capacity.	Broader adoption and effective collaboration.
Action	Form a dedicated team to manage AI-native platforms and select AI models.	Integrate AI governance platforms for code review and compliance checks.	Start with low-risk projects to validate productivity gains.	Prioritize AI-native tools for new development initiatives.	Train developers and business partners on prompt engineering and governance.

Key players to support implementation success

CIO

Partner: Define AI-first strategy and governance framework.

Collaborate: Align platform capabilities with business priorities.

Govern: Ensure compliance and security guardrails for AI-native development.

IT partners

Platform engineering: Manage AI-native tools, integrations and performance.

Security: Implement AI governance for code review and risk management.

Procurement: Evaluate and select AI-native platform vendors and services.

Business partners

Product owners: Provide domain expertise and validate AI-driven solutions.

Finance: Align funding models to support AI-native development initiatives.

2

AI supercomputing platforms

What is it?
AI supercomputing platforms deliver the massive processing power needed to train and run advanced AI models. These systems combine high-performance computing (HPC), specialized processors and scalable architectures to handle data-intensive workloads.

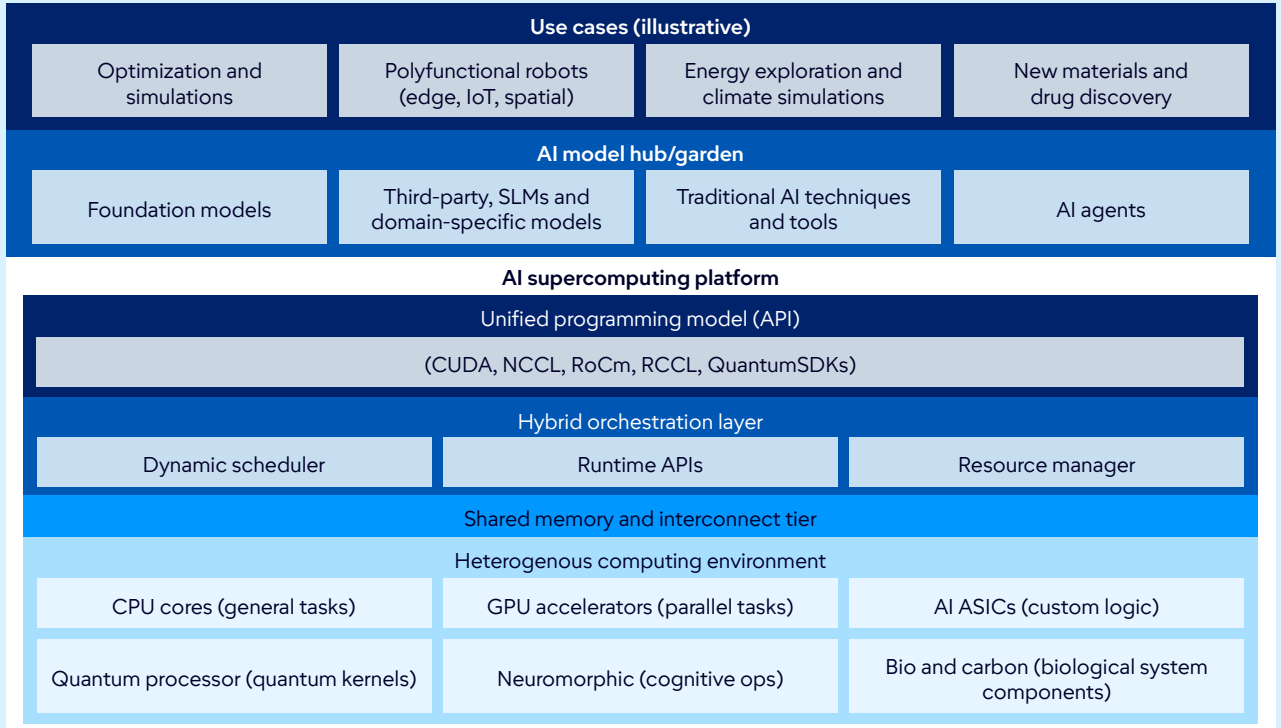
Why trending?
Demand for AI supercomputing is surging as organizations develop larger, more complex models that exceed traditional infrastructure limits.

What's next

40% of enterprises will adopt hybrid computing architectures by 2028 (up from 8%).

20+ vendors will offer unified developer platforms leveraging supercomputing environments by 2028.

AI supercomputing platform



Source: Gartner

2

Deliver results with AI supercomputing platforms

Action plan to unlock massive processing power

Steps	1 Identify high-impact workloads	2 Invest in unified software stacks	3 Develop phased integration strategy	4 Streamline development across environments	5 Plan for governance and compliance
Expected outcome	Demonstrate value and build internal expertise.	Simplified integration and flexible workload placement.	Future-ready infrastructure and workforce.	Accelerated delivery and reduced friction.	Reduced risk and improved oversight.
Action	Run pilot projects using hybrid orchestration.	Adopt open standards across traditional and emerging systems.	Introduce new compute paradigms gradually and train IT staff.	Encourage teams to adopt hybrid platforms and composable architectures.	Design security and compliance strategies at the system level.

Key players to support implementation success

CIO

Define a hybrid orchestration strategy aligned with business priorities.

Ensure governance for workload placement, security and compliance.

Partner with business leaders to prioritize high-impact workloads.

IT partners

Infrastructure and operations: Integrate emerging accelerators with legacy systems.

Security: Implement governance for multiarchitecture environments.

DevOps: Adopt unified software stacks and orchestration tools.

Business partners

Product: Identify use cases for hybrid computing (e.g., simulations, AI-enabled apps).

Finance: Align funding for phased integration and sustainability goals.

Operations: Prepare for AI-driven workflows in critical processes.

3

Confidential computing

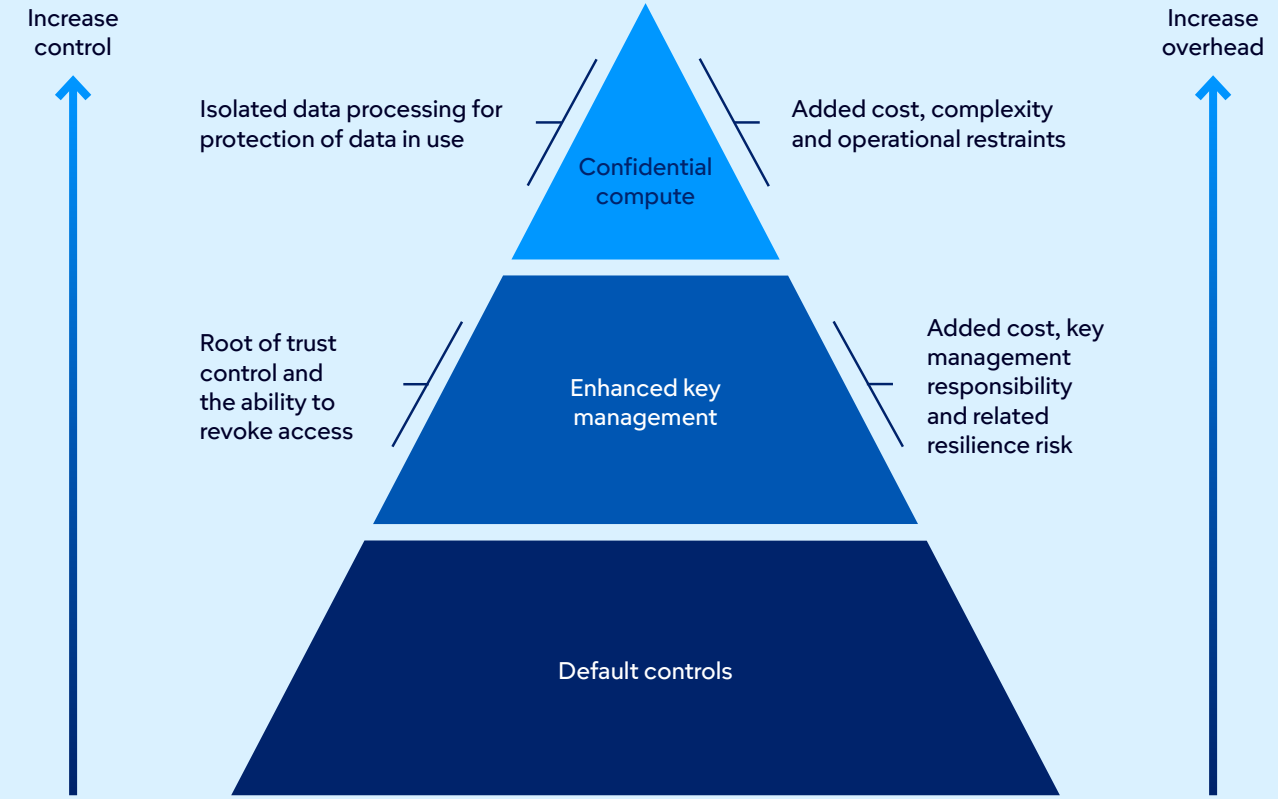
What is it?
Confidential computing uses hardware-based trusted execution environments (TEEs) to protect data while it's being processed, preventing unauthorized access — even from cloud providers.

Why trending?
Stricter privacy laws, data localization rules and AI adoption make in-use protection critical. Confidential computing enables secure cloud strategies and compliance for sensitive workloads.

What's next

75% of processing in untrusted infrastructure will be secured by confidential computing by 2029.

Controls to limit CSP data access



Source: Gartner

3

Deliver results with confidential computing

Action plan to ensure secure, compliant data processing everywhere

Steps	1 Audit sensitive workloads	2 Pilot TEEs for AI models	3 Enable secure collaboration	4 Establish independent key management	5 Prepare for integration challenges
Expected outcome	Identify where in-use protection is needed.	Strengthen confidentiality and IP protection.	Share insights without exposing raw data.	Full control over data access.	Smooth deployment across environments.
Action	Map workloads subject to privacy or localization rules.	Test TEEs with proprietary and open-source AI models.	Use confidential computing for analytics and BI projects.	Implement organization-owned cryptographic key systems.	Plan orchestration across multiple chipsets and providers.

Key players to support implementation success

CIO

Define a confidential computing strategy aligned with privacy, compliance and cloud goals.

Partner with legal and compliance teams to meet data localization and sovereignty requirements.

Oversee governance for TEEs and ensure integration with existing security frameworks.

IT partners

Infrastructure and operations: Deploy TEEs across hybrid and multicloud environments.

Security: Implement attestation processes and cryptographic key management.

DevOps and platform: Adapt workloads for confidential computing and monitor performance.

Business partners

Compliance: Validate adherence to regulatory mandates and audit readiness.

Finance: Align funding for confidential computing adoption and risk mitigation.

Data owners: Identify sensitive workloads for in-use protection and prioritize projects.

The Synthesist

Orchestrate diverse technologies for new value.

To unlock new sources of differentiation, technology leaders must integrate specialized models, multiagent systems and physical AI for domain-specific solutions. The Synthesist trends focus on orchestrating diverse technologies to create adaptive, intelligent ecosystems that drive innovation across workflows, products and experiences.

4

Multiagent systems

What is it?
Multiagent systems (MAS) use collections of specialized AI agents that collaborate to complete complex workflows. Each agent handles a specific task, improving efficiency and scalability compared to monolithic AI solutions.

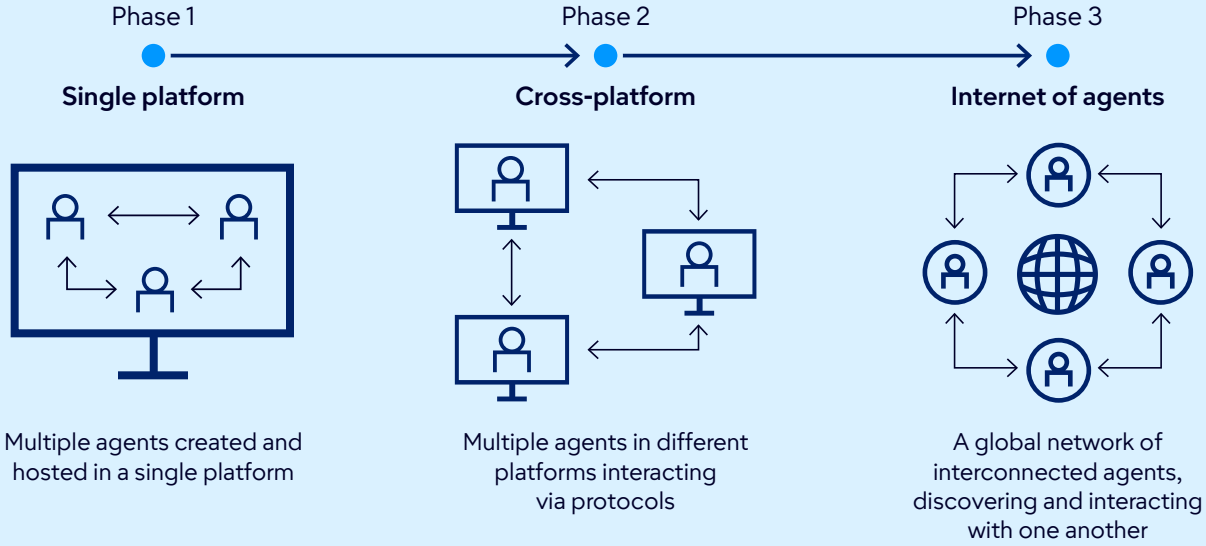
Why trending?
As single-agent AI struggles with multistep processes, MAS enable modular automation and cross-platform integration. We report a 1,445% surge in MAS inquiries from 1Q24 to 2Q25, signaling rapid enterprise interest.

What's next

70% of MAS will use narrowly specialized agents by 2027, improving accuracy but increasing coordination complexity.

60% of MAS will support multivendor interoperability by 2028, driving innovation and flexibility.

The evolution of multiagent systems



Source: Gartner

4

Deliver results with multiagent systems

Action plan to drive modular automation and seamless integration

Steps	1 Identify high-value use cases	2 Design modular agents	3 Implement governance and observability	4 Adopt interoperability standards	5 Upskill teams
Expected outcome	Measurable impact and faster adoption.	Improved reliability and scalability.	Reduced risk and better control.	Future-proof MAS investments.	Effective deployment and risk mitigation.
Action	Start with well-defined workflows for MAS pilots.	Build specialized agents instead of monolithic solutions.	Apply strong API governance and monitoring tools.	Use emerging protocols for multivendor agent collaboration.	Train staff on MAS frameworks and change management.

Key players to support implementation success

CIO

Define MAS strategy for high-value workflows and align with business priorities.

Establish governance for agent interoperability, security and compliance.

Communicate change management plans to address workforce concerns.

IT partners

Platform and DevOps: Design modular agents and manage orchestration tools.

Security: Implement API governance and monitor agent interactions.

Integration teams: Adopt standards for interoperability and observability.

Business partners

Process owners: Identify workflows for MAS pilots and validate outcomes.

Finance: Manage unpredictable costs and fund observability tools.

Operations: Support human-agent collaboration and training initiatives.

5

Domain-specific language models

What is it?
Domain-specific language models (DSLMs) are AI models trained on specialized datasets for specific industries or business functions, delivering higher accuracy and compliance than generic large language models (LLMs).

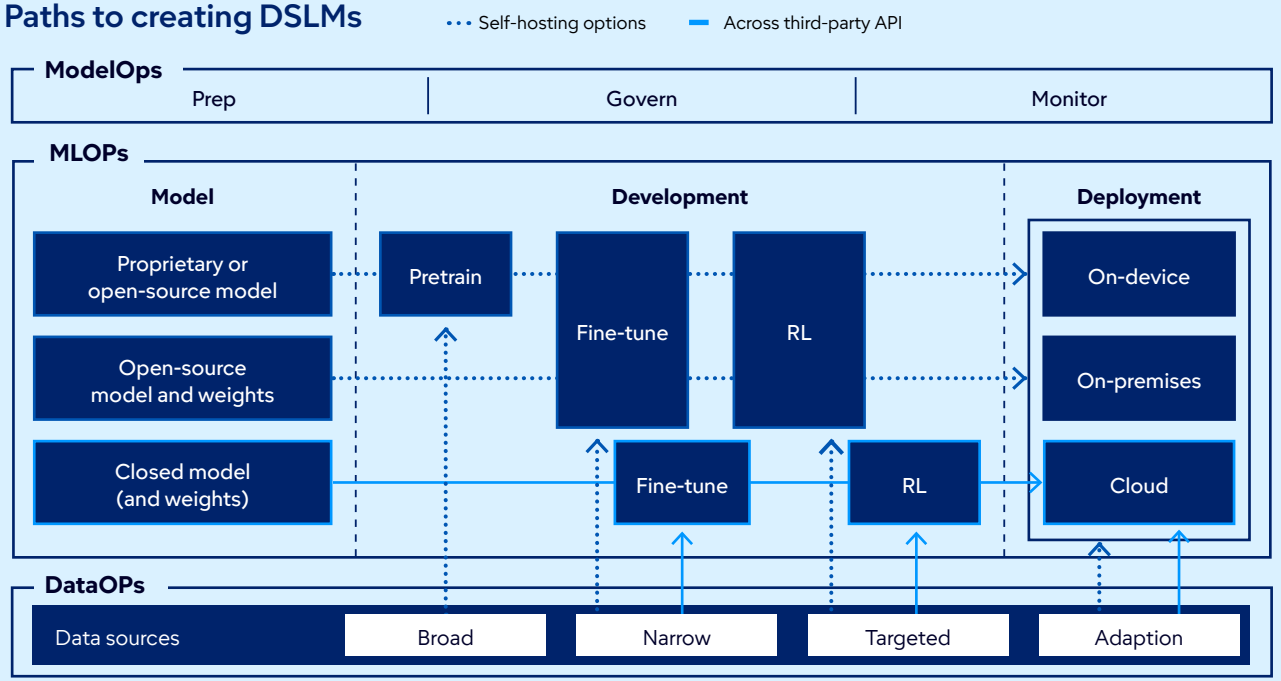
Why trending?
CIOs need measurable business value from AI. DSLMs reduce errors, accelerate deployment and cut costs for critical workflows like finance, healthcare and HR.

What's next

+60% of enterprise GenAI models will be domain-specific by 2028.

30% of GenAI workloads will run DSLMs on-premises or on-device by 2028.

Paths to creating DSLMs



Source: Gartner

5

Deliver results with DSLMs

Action plan to deliver precise, industry-specific compliance

Steps	1 Identify high-impact use cases	2 Strengthen data governance	3 Pilot DSLMs in critical domains	4 Build cross-functional teams	5 Monitor and optimize
Expected outcome	Faster ROI and improved accuracy.	Reliable and compliant DSLM outputs.	Demonstrate measurable business value.	Smooth integration and adoption.	Sustainable performance and cost control.
Action	Target workflows where generic LLMs underperform.	Implement robust privacy and quality controls.	Start with finance, healthcare or HR processes.	Include IT, SMEs and compliance in DSLM projects.	Apply explainability and compliance frameworks.

Key players to support implementation success

CIO

Define DSLM strategy for regulated and high-value domains.

Ensure governance for accuracy, compliance and explainability.

Align DSLM adoption with ROI and risk management goals.

IT partners

Data and analytics: Prepare domain-specific datasets and maintain quality.

ModelOps: Manage fine-tuning, monitoring and life cycle governance.

Security: Enforce privacy and compliance for DSLM deployments.

Business partners

Domain experts: Validate DSLM outputs for accuracy and relevance.

Finance: Budget for DSLM adoption and cost optimization.

Compliance: Ensure adherence to regulatory standards.

6

Physical AI

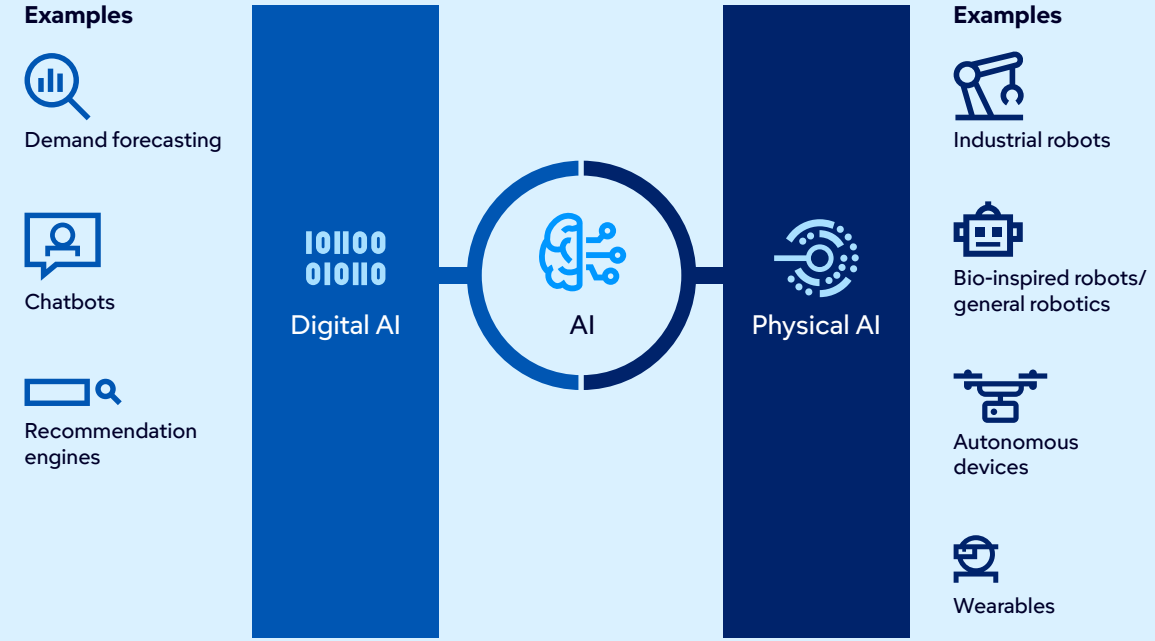
What is it?
Physical AI brings intelligence into the real world through robots, drones, vehicles and smart devices that sense, decide and act. These systems combine sensors, actuators and AI models to automate physical tasks.

Why trending?
Organizations want the productivity of digital AI applied to physical environments. By 2028, five of the top 10 AI vendors will offer physical AI products.

What's next

80% of warehouses will use robotics or automation by 2028.

Categorization of AI



Source: Gartner

6

Deliver results with physical AI

Action plan to automate real-world tasks and boost productivity everywhere

Steps	1 Audit operational domains	2 Pilot physical AI systems	3 Build cross-functional teams	4 Educate stakeholders	5 Plan for multiagent coordination
Expected outcome	Identify areas for automation and cost savings.	Validate performance and ROI.	Effective governance and integration.	Avoid confusion and misaligned investments.	Future-proof deployments.
Action	Target logistics, maintenance and safety workflows.	Use simulation and digital twins before live deployment.	Include IT, operations and engineering in planning.	Clarify distinctions between physical AI, embedded AI and edge AI.	Explore orchestration platforms for fleets of devices.

Key players to support implementation success

CIO

Define a physical AI strategy aligned with operational goals.

Ensure governance for safety, reliability and explainability.

Partner with operations and engineering for integration and risk management.

IT partners

Infrastructure and operations: Integrate physical AI with IoT and legacy systems.

Security: Implement safeguards for autonomous systems.

Data and analytics: Support simulation and digital twin testing.

Business partners

Operations: Identify high-value use cases and validate performance.

Finance: Budget for robotics and automation investments.

Compliance: Ensure adherence to safety and regulatory standards.

The Vanguard

Elevate trust, governance and security.

In an era of rising risk and regulatory scrutiny, trust is non-negotiable. The Vanguard trends emphasize proactive security, transparent governance and digital integrity — enabling organizations to protect reputation, ensure compliance and maintain stakeholder confidence while scaling AI and digital transformation.

7

Preemptive cybersecurity

What is it?
Preemptive cybersecurity (PCS) uses advanced AI-driven techniques to anticipate, disrupt and neutralize cyberattacks before they occur — moving beyond traditional detection and response.

Why trending?
AI-powered threats are growing exponentially, targeting networks, applications and IoT systems. By 2029, technology products lacking preemptive cybersecurity will lose market relevance as proactive defense becomes a universal requirement.

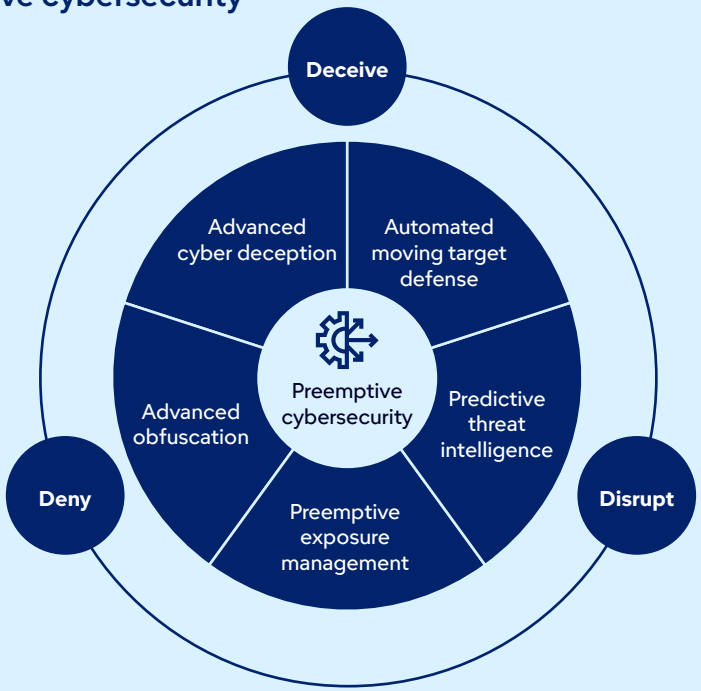
Need insights tailored to technology and service provider organizations? Read our article on preemptive cybersecurity for vendors, **Don't Delay in Building Preemptive Cybersecurity Solutions.**

What's next

50% of security software spending will go to preemptive solutions by 2030.

1M Documented vulnerabilities expected to surpass 1 million annually by 2030.

The 3 Ds of preemptive cybersecurity



Source: Gartner

7

Deliver results with preemptive cybersecurity

Action plan to protect assets before threats emerge

Steps	1 Assess current security architecture	2 Pilot PCS in high-risk areas	3 Define vendor selection criteria	4 Socialize PCS strategy	5 Integrate PCS with existing tools
Expected outcome	Identify gaps and prioritize PCS investments.	Demonstrate measurable risk reduction.	Ensure future-proof PCS adoption.	Build executive and board-level support.	Maximize ROI and accelerate adoption.
Action	Conduct risk analysis and readiness review.	Implement predictive threat prevention and deception.	Require detailed roadmaps for preemptive capabilities.	Communicate business impact and ROI of PCS.	Combine PCS with current security and compliance processes.

Key players to support implementation success

CIO

Champion a shift from reactive to preemptive security strategies.

Define buying criteria for PCS capabilities and educate executive peers.

Oversee governance for aggressive defense measures and compliance.

IT partners

Security: Deploy predictive threat prevention and deception technologies.

Infrastructure and operations: Integrate PCS with cloud, OT and cyber-physical systems.

Risk and compliance: Ensure adherence to privacy and regulatory standards.

Business partners

Finance: Allocate budgets for PCS pilots and long-term adoption.

Operations: Support secure digital transformation initiatives.

Product: Embed preemptive security into offerings for market differentiation.

8

Digital provenance

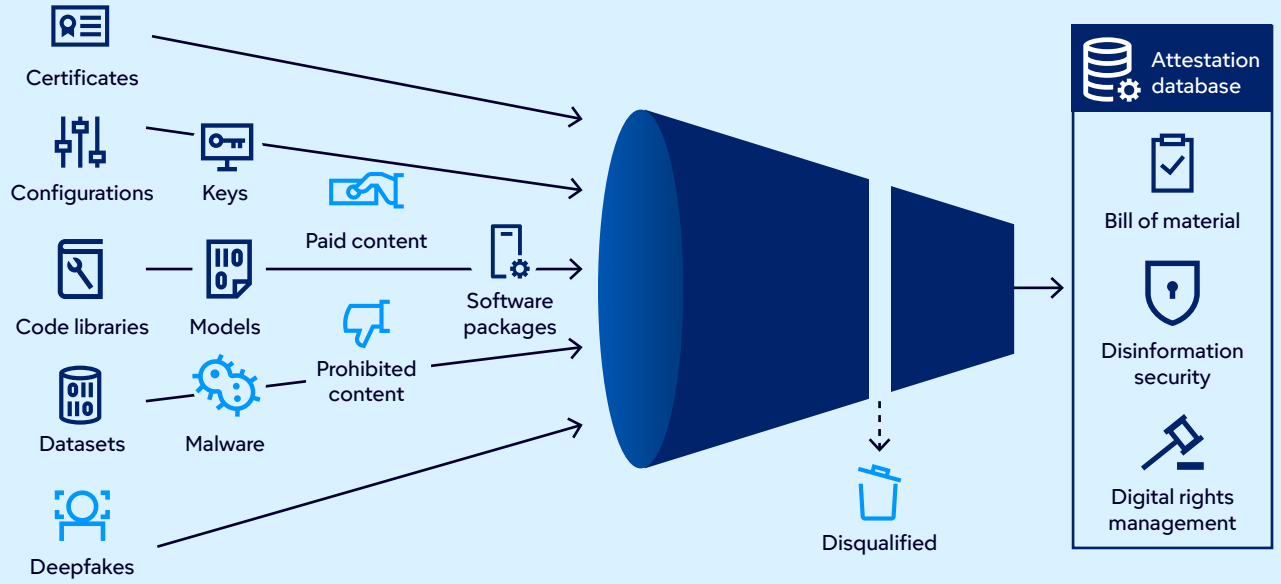
What is it?
Digital provenance verifies the origin and integrity of software, data and media, using tools like bills of materials (BOMs), attestation databases and watermarking. It ensures transparency and trust in systems built on third-party components and AI-generated content.

Why trending?
Organizations face rising risks from code tampering, abandoned open-source projects and deepfake-driven disinformation.

What's next

Growing regulatory mandates (e.g., EU AI Act) require watermarking and provenance tracking for AI-generated content.

Filter by digital provenance



Source: Gartner

8

Deliver results with digital provenance

Action plan to build trust by verifying data and content authenticity

Steps	1 Deploy BOMs	2 Implement attestation database	3 Adopt disinformation security tools	4 Apply digital watermarking	5 Strengthen governance
Expected outcome	Enables software provenance, transparency and security.	Centralized, trusted provenance records.	Protection against impersonation and fraud.	Compliance with AI content regulations.	Reduced legal and reputational risk.
Action	Implement software BOMs (SBOMs) for software and machine learning BOMs (MLBOMs) for AI models.	Store cryptographically signed evidence of origin.	Integrate synthetic identity detection into identity threat detection and response plans.	Mark AI-generated media in machine-readable formats.	Collaborate across IT, compliance and marketing teams.

Key players to support implementation success

CIO

Define a digital provenance strategy aligned with compliance and risk management.

Oversee implementation of BOMs and attestation databases.

Collaborate with CISO and CMO on disinformation response and reputation protection.

IT partners

DevOps: Integrate SBOMs and MLBOMs into delivery pipelines.

Security: Deploy disinformation security tools and digital rights management (DRM).

Data: Document training data lineage for AI models.

Business partners

Compliance: Ensure adherence to emerging regulations.

Legal: Validate copyright and licensing compliance.

Marketing: Manage reputational risks tied to deepfakes and synthetic content.

9

AI security platforms

What is it?
AI security platforms (AISPs) consolidate controls to secure both third-party AI services and custom-built AI applications. They address AI-native risks like prompt injection, rogue agent actions and data leakage.

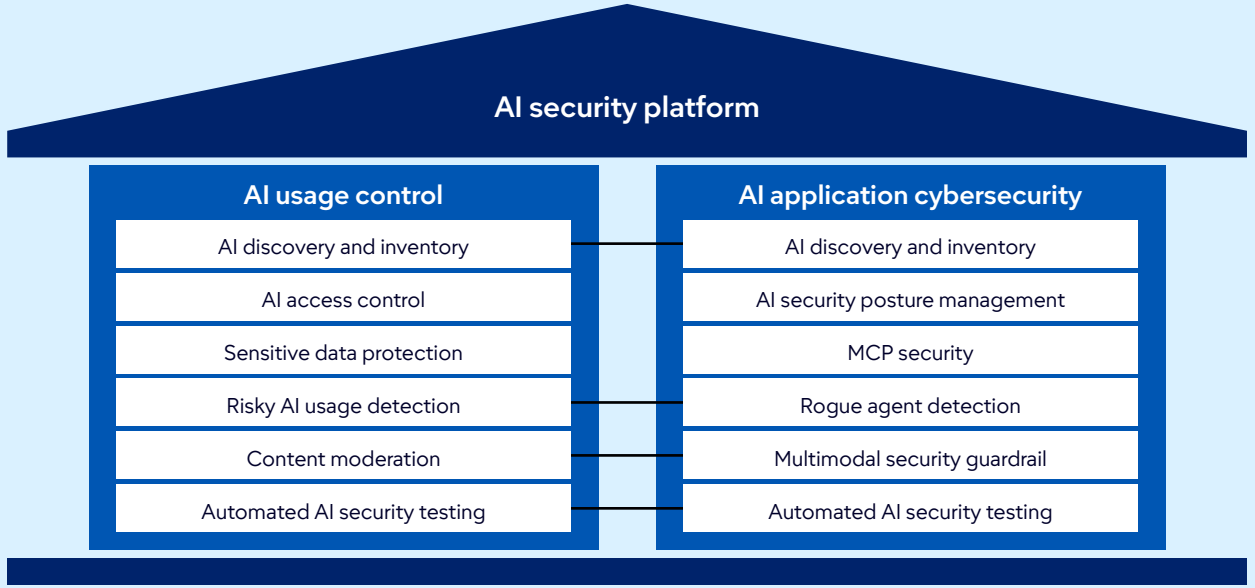
Why trending?
As AI adoption accelerates, traditional security tools fail to protect AI workflows.

What's next

+50% of enterprises will adopt AISPs by 2028.

80% of unauthorized AI transactions will stem from internal policy violations, not external attacks.

AI security platform capability mapping



Source: Gartner

9

Deliver results with AI security platforms

Action plan to safeguard evolving AI-driven business operations

Steps	1 Assess AI risk landscape	2 Pilot AISP solutions	3 Favor unified platforms	4 Integrate security testing	5 Monitor vendor innovation
Expected outcome	Identify gaps in current security stack.	Validate effectiveness and ROI.	Simplify management and reduce complexity.	Improve resilience against prompt injection.	Stay ahead of emerging threats.
Action	Map AI-native risks across workflows.	Start with high-risk AI services and custom apps.	Choose AISPs covering AI usage control plus app security.	Add automated AI security tests to pipelines.	Track startups and incumbents for advanced features.

Key players to support implementation success

CIO

Define an AI security strategy that spans third-party and custom AI apps.

Select vendors offering unified AI usage control and application security.

Communicate AI risk posture and compliance requirements to the board.

IT partners

Security: Deploy guardrails for prompt injection and rogue agent detection.

DevOps: Integrate AI security testing into development pipelines.

Infrastructure and operations: Ensure compatibility with cloud and on-premises environments.

Business partners

Compliance: Align AISPs with regulatory frameworks (e.g., EU AI Act).

Finance: Budget for platform adoption and risk mitigation.

Product: Embed security features into AI-enabled offerings.

10

Geopatriation

What is it?
Geopatriation is the relocation of workloads from global hyperscale clouds to sovereign or local environments to reduce geopolitical risk. It includes strategies like redeploying to sovereign cloud regions or repatriating workloads on-premises.

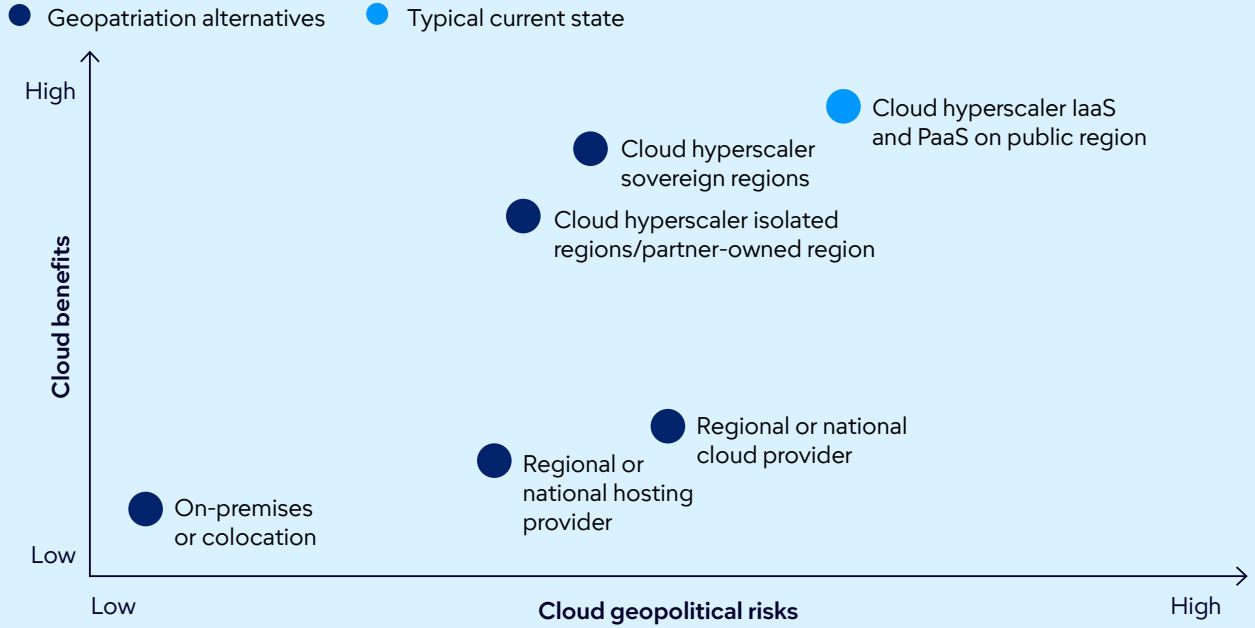
Why trending?
Geopolitical turbulence and regulatory mandates are driving organizations to reassess cloud dependencies.

What's next

75% of enterprises will geopatriate workloads by 2030.

Sovereign cloud offerings from hyperscalers and local providers are expanding rapidly.

Cloud benefits and cloud geopolitical risks



Source: Gartner

10

Deliver results with geopatriation

Action plan to reduce risk by localizing critical digital workloads

Steps	1 Assess workload criticality	2 Evaluate sovereign options	3 Plan hybrid strategies	4 Implement governance controls	5 Monitor geopolitical trends
Expected outcome	Prioritize geopatriation for high-risk assets.	Balance agility and sovereignty.	Maintain resilience and performance.	Reduce compliance and security risk.	Adapt strategy proactively.
Action	Score workloads based on sensitivity and geopolitical exposure.	Compare hyperscaler sovereign offerings vs. local providers.	Combine sovereign cloud with on-premises or colocation.	Adopt attestation and sovereignty frameworks.	Update workload placement as risks evolve.

Key players to support implementation success

CIO

Define geopatriation strategy, balancing sovereignty, agility and resilience.

Evaluate trade-offs between local providers and global hyperscalers' sovereign options.

Oversee risk scoring for critical workloads and compliance alignment.

IT partners

Infrastructure and operations: Plan migration paths and integration with legacy systems.

Security: Validate sovereignty controls and ensure compliance.

Cloud architects: Optimize workload placement for performance and resilience.

Business partners

Compliance: Monitor regulatory changes and sovereignty mandates.

Finance: Budget for migration costs and risk mitigation investments.

Operations: Ensure continuity during workload relocation.

Actionable, objective insights

Explore these additional complimentary resources and tools for IT leaders:

Template

Build an IT Strategic Plan

Turn strategy into action with this one-page planning template.

Access Template

Tool

Gartner Benchmarking and Diagnostics

Discover benchmarking that powers smarter IT decisions.

Learn More

Insights

2025 Gartner Hype Cycle™

The 2025 Hype Cycle for Artificial Intelligence goes beyond GenAI.

Explore Now

Insights

Trending Questions on AI and Emerging Technologies

Gartner experts share quick answers to recently asked client questions on emerging technologies.

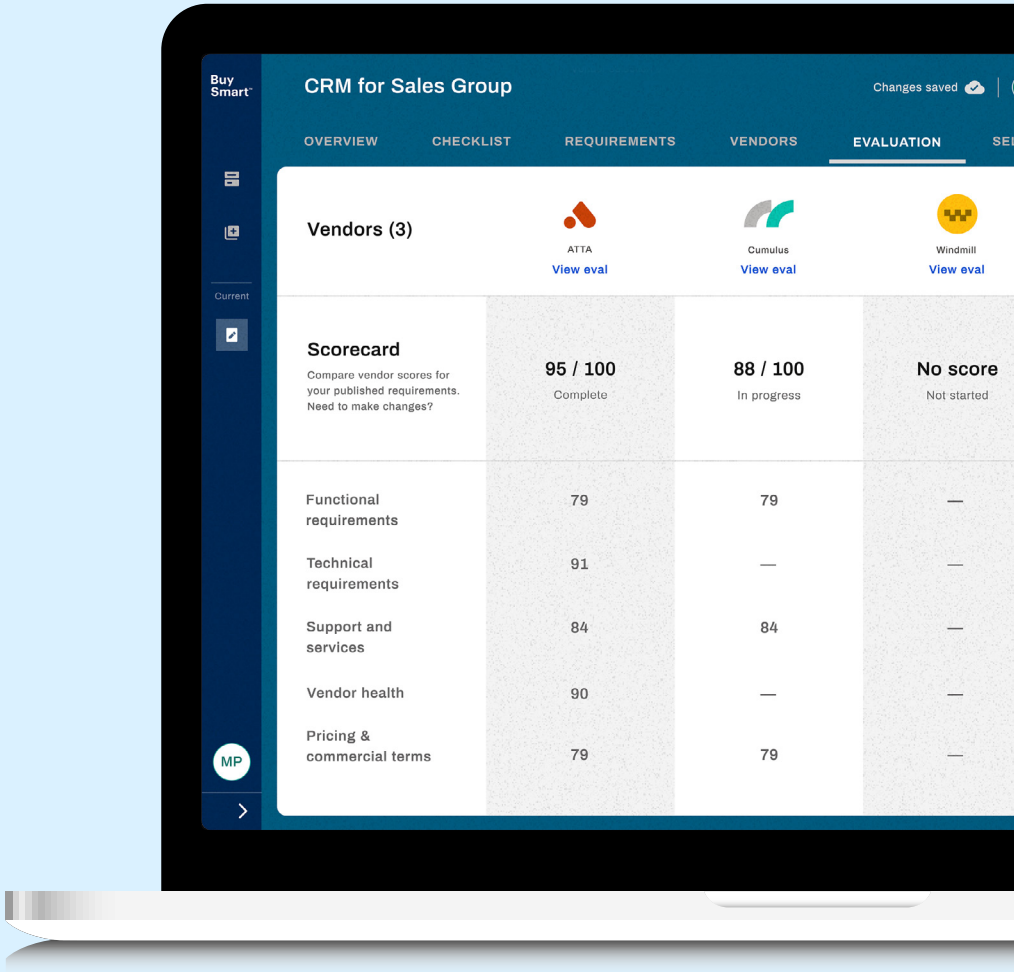
Review Answers

Already a client?
Get access to even more resources in your client portal. **Log In ↗**

Gartner®

Gartner BuySmart™

Streamline your team's path to better tech purchasing decisions



What you'll get:

- Access to 100+ templates covering top technology markets
- Predefined, fully customizable checklists and requirements
- Collaboration features to support your team's workflow all in one place
- Standardized scoring to build confidence in your vendor selection

Learn More ↗

Research Shortlist Evaluate Negotiate

Connect with us

Get actionable, objective business and technology insights that drive smarter decisions and stronger performance on your mission-critical priorities.

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Talk to a Specialist

Learn more about Gartner for CIOs and IT Executives
gartner.com/en/chief-information-officer

Stay connected to the latest insights

Attend a Gartner conference
View Conference

Gartner®