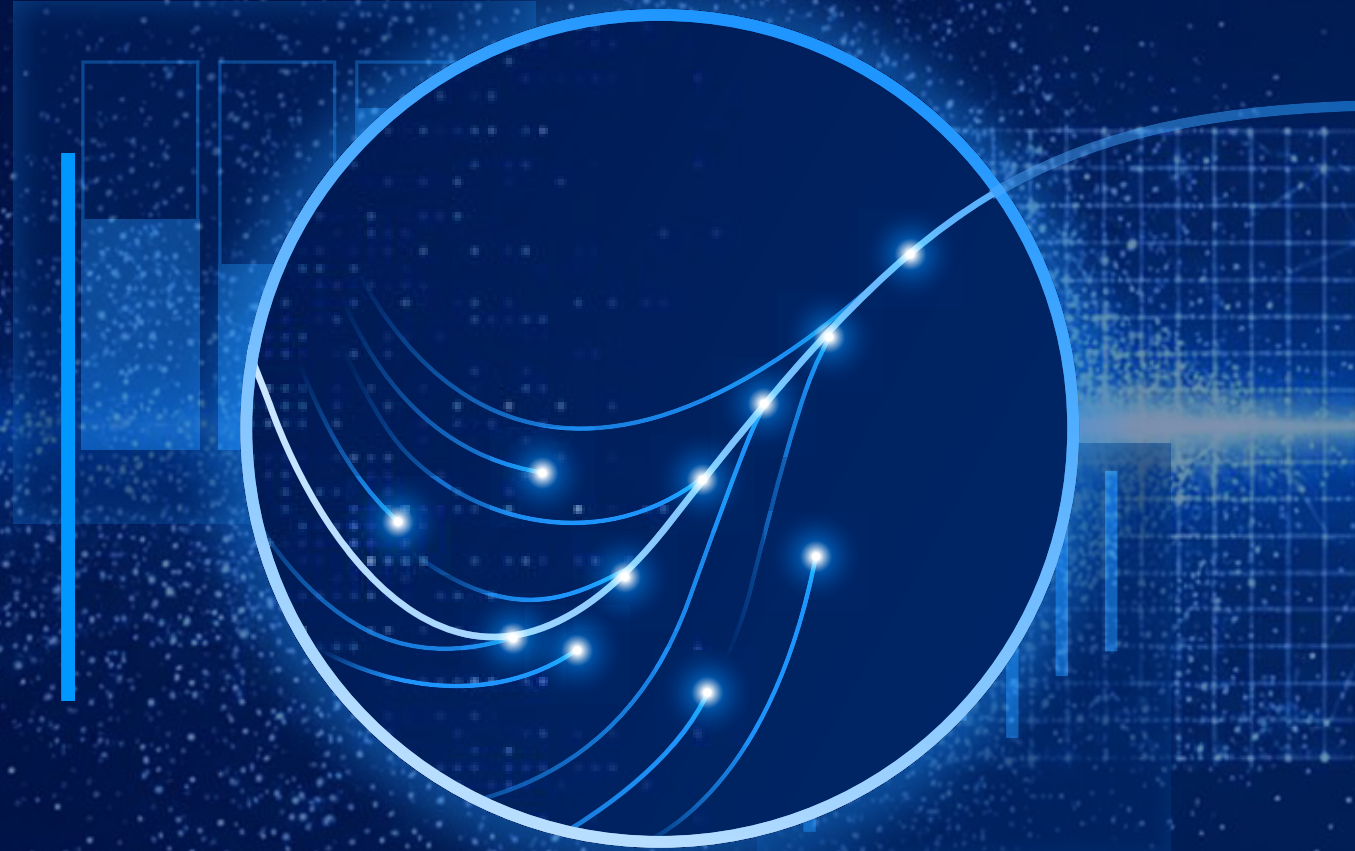


Top 10 Strategic Technology Trends for 2027



Mastering the new boundaries of machine behavior

It's no secret that technology leaders must safely lead their organizations into the autonomous era. While traditional IT relied on software scarcity, 2027 will deliver new levels of software abundance. Running static code will be replaced with the orchestration of autonomous machine workers, sensory AI and sovereign limits. Navigating this shift requires an immediate, C-Level focus across three operational fronts:

Leverage the nontextual AI frontier



Models that calculate, hear and simulate. Deliver specialized mathematical-, voice- and physics-based models that solve complex problems with deterministic precision and sensory depth.

Govern the autonomous agent platform



System-level control planes for trustworthy autonomy. Deploy platform-owned AI context systems, AI coding harnesses, AI secure identity systems and automated exposure remediation to securely constrain machine behavior and exposure.

Architect durable agility



Transitioning to sovereign, disposable and organic environments. Secure long-term independence using sovereign stacks, disposable applications designed for clean decommissioning and low-power biological computing.

The Gartner Top 10 Strategic Technology Trends for 2027 can help leaders build the boundaries needed to deliver trusted outcomes. 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

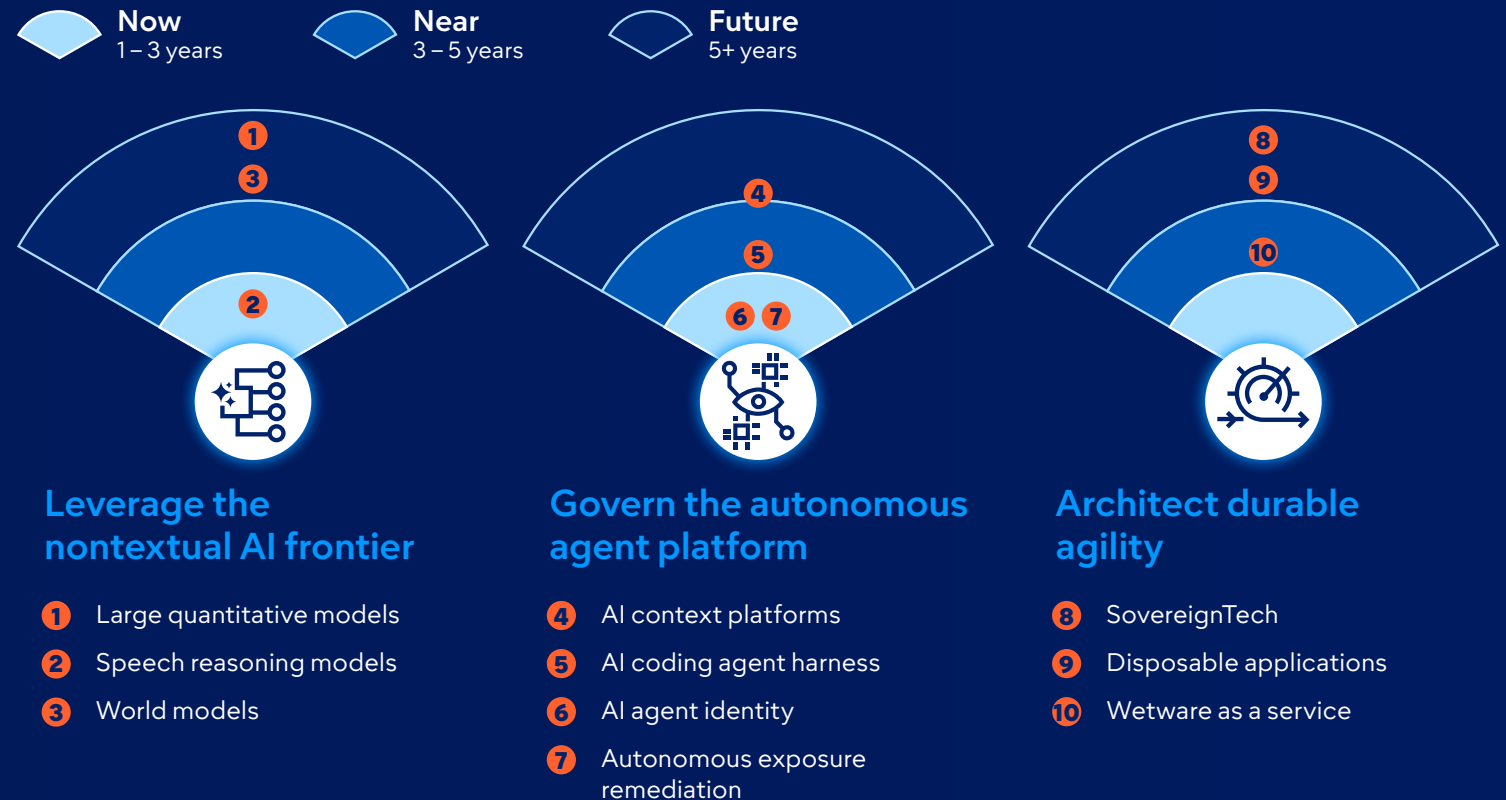
Distinguished Vice President, Business and Technology Insights, Gartner

Gartner Top 10 Strategic Technology Trends for 2027

Technology decisions require a balanced approach to immediate operational efficiency and long-term business survivability.

This multiyear outlook organizes the Gartner Top Strategic Technology Trends into sequential planning horizons to help you determine when to prepare, pilot and scale each capability.

Use these phases to align your technology roadmap with broader corporate goals, ensuring your business stays ahead of volatility while systematically upgrading its core capabilities.





Leverage the nontextual AI frontier

Models that calculate, hear and
simulate to solve complex problems

AI is expanding beyond text into speech, numbers and physical environments. But voice-native systems reasoning is shallower than text-based models, creating safety risks for businesses that rely on a single unsupervised voice model. These trends focus on complexity-based routing: fast models for routine tasks, deep reasoning for complex decisions.

Trend 1

Large quantitative models

What is it?

Modular, hybrid neural network architectures built to process and analyze quantitative data. They use deterministic calculations, established mathematical formulas, statistical methods and numerical algorithms to accurately model complex systems.

Why trending?

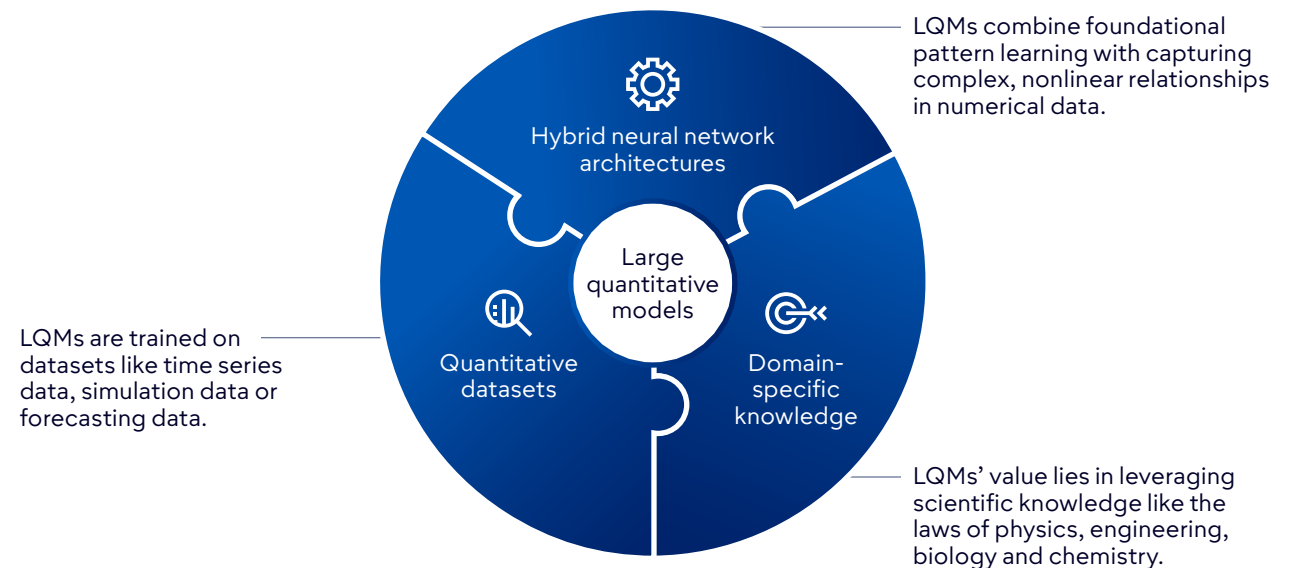
Rapid expansion of GenAI investments can't cover every business use case, especially numerical ones. Large language models (LLMs) fail at mathematical reasoning because they guess probabilistically. Large quantitative models (LQMs) are designed explicitly for numerical reasoning. They are far less resource-intensive, requiring significantly less memory, storage and compute. This specialized architecture provides a direct shortcut to rapid forecasting while slashing your reliance on expensive token-based inference.

What's next?

25%

By 2030, LQMs will replace LLMs in 25% of strategic forecasting and operational modeling tasks across major enterprise functions.

Core components of large quantitative models



Source: Gartner



Trend 1 | Large Quantitative Models

Delivering results with LQMs

Action plan to drive modular automation and seamless integration

Steps	1 Deploy hybrid AI architectures	2 Target high-value mathematical use cases	3 Establish robust data validation protocols	4 Adapt your ModelOps strategy
Expected outcome	A shortcut to rapid forecasting	Unprecedented business agility	Safe deployment of autonomous forecasting	Bypassed model retraining and lower compute costs
Action	Combine the conversational strength of LLMs with the deterministic analytical power of quantitative models.	Consider financial risk modeling, supply chain logistics, energy forecasting and agricultural soil analysis.	Ensure all numerical inputs remain flawless and prevent skewed forecasting models.	Continuously monitor deployments, prevent model overfitting and maintain high-yield operational efficiency.

Key players to support implementation success

 CIO

Lead: Establish a strategy for quantitative AI that improves forecasting, planning and operational decision making.

Invest: Prioritize high-value use cases where mathematical precision and predictive accuracy create competitive advantage.

Drive: Accelerate AI value by integrating LQMs into broader composite AI initiatives.

 IT partners

Data and AI teams: Build the data foundations, governance practices and model capabilities required for accurate forecasting and simulation.

Enterprise architecture: Establish scalable platforms that integrate LQMs with existing AI, analytics and business applications.

ModelOps and governance: Monitor model performance, data quality and explainability to maintain trust and reliability.

 Business partners

Operations leaders: Identify opportunities to improve forecasting, planning and operational efficiency.

Finance and strategy: Apply quantitative insights to scenario planning, risk management and investment decisions.

Business domain experts: Validate model assumptions, inputs and outcomes to ensure business relevance and adoption.

Trend 2

Speech reasoning models

What is it?

Voice AI systems that reason directly on audio, tracking context and intent across a conversation to determine what to do next. They bypass traditional text-transcription by reasoning and executing chained tasks, extending autonomous resolution to multiturn problem solving, context shifts and error recovery.

Why trending?

Voice remains the highest-volume enterprise interaction channel, but even a decade of customer support automation has failed to deliver sufficient accuracy, speed and resolution rates. Speech reasoning models close that gap at scale, making complex, judgment-intensive conversations viable to automate. This represents a fundamental architectural change that goes well beyond an incremental voice upgrade, extending even into physical AI where voice serves as the primary interface for robots and humanoids.

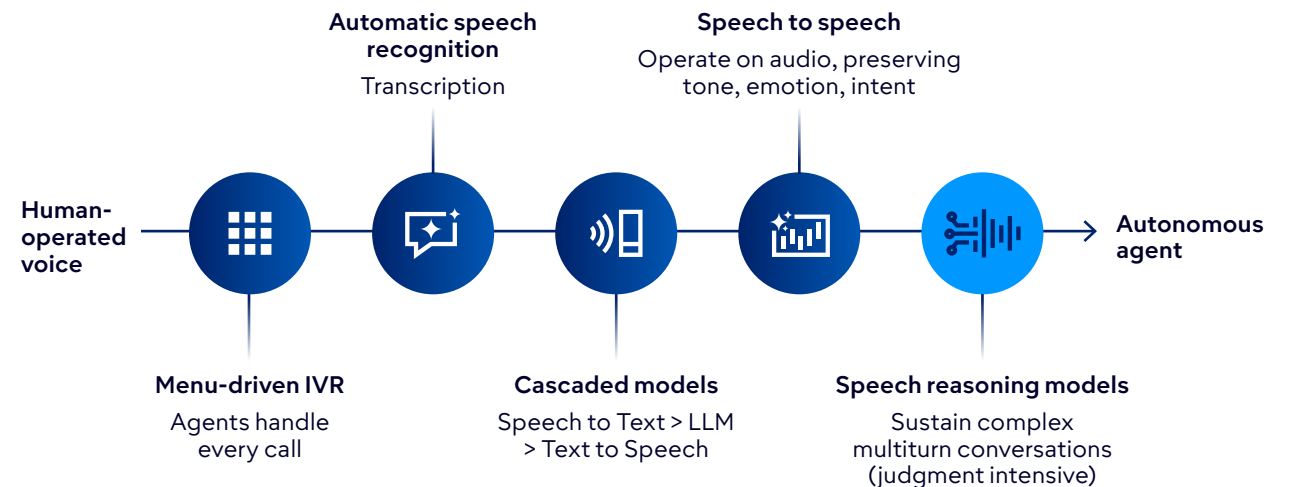
What's next?

70%

By 2030, over 70% of enterprise voice interactions will be handled autonomously by speech models, up from less than 10% in 2026.

The stages of speech evolution

Scaling human operations to agents



Source: Gartner



Trend 2 | Speech Reasoning Models

Delivering results with speech reasoning models

Action plan to drive modular automation and seamless integration

Steps	1 Draft strict requirements	2 Classify requirements by complexity	3 Inventory high-volume interactions
Expected outcome	Assess and confirm compliance readiness	A sharper build-or-buy strategy	Clear labeling standards
Action	Draft strict consent, privacy and audit logging requirements. Assign clear owners for each jurisdiction.	Classify voice interactions by complexity to route between low-latency tiers and deeper reasoning models.	Ahead of any domain adaptation work, catalog the highest-volume recorded voice interactions.

Key players to support implementation success

CIO	IT partners	Business partners
Lead: Establish a strategy for autonomous voice interactions across customer and employee experiences. Prioritize: Invest in conversational AI capabilities that improve service efficiency while maintaining trust and accuracy. Govern: Define policies for consent, privacy, compliance and responsible use of voice data.	Customer experience and AI teams: Design and deploy speech reasoning solutions that support complex, multiturn interactions. Data and platform teams: Manage voice data, model performance and domain-specific training assets. Security and compliance: Implement privacy controls, audit logging and governance for voice-based AI interactions.	Marketing and communications: Help define voice personas, conversational standards and customer trust requirements. Customer service leaders: Identify high-value use cases and validate interaction quality and resolution outcomes. Legal and compliance: Ensure adherence to consent, privacy and regulatory requirements across jurisdictions.

Trend 3

World models

What is it?

Computational systems trained on multimodal datasets to learn abstract representations of physical and virtual environments. They enable autonomous agents to simulate potential future states, predict outcomes and understand the consequences of their actions before execution.

Why trending?

Language models lack a native grasp of physical reality, causality and spatial logic. World models are progressively resolving this bottleneck by establishing a physics-first paradigm that allows machines to comprehend space, time and causality. Surging investments in robotics, autonomous vehicles and spatial computing are driving this cutting-edge development.

Although high computational costs currently restrict generalized deployment, model training costs will fall tenfold within three years, making enterprise simulations economically viable.

What's next?



By 2030, 40% of robotics applications will incorporate world models to drive optimal decisions in adaptive environments, compared with less than 1% in 2025.

World models: Different models for different worlds

Data science

The world is a probabilistic distribution. **Sample techniques:** MBRL, VAE, MAE, autoregressive, diffusion

Physics

The world is governed by physical laws. **Sample techniques:** physics simulator, expert system

Neuroscience

The world mirrors the human mind. **Sample techniques:** active inference, cognitive architecture

Graphics

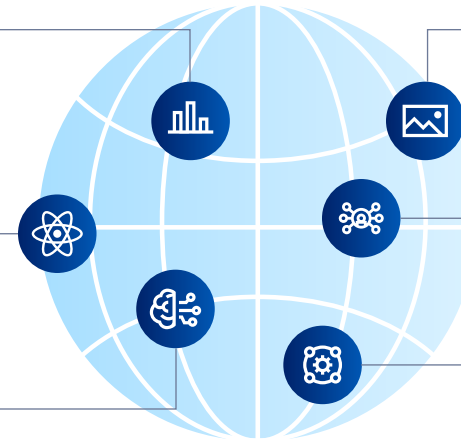
The world is a three-dimensional space. **Sample techniques:** spatial AI, 3DGS

Cybernetics

The world is a dynamic system and control loop. **Sample techniques:** MPC, JEPa

Social science

The world is collective intelligence. **Sample techniques:** complex system, multiagent system



Source: Gartner

Trend 3 | World Models

Delivering results with world models



Action plan to drive modular automation and seamless integration

Steps	1 Establish a five-year roadmap	2 Prove measurable business value	3 Build a deployment launchpad
Expected outcome	Industrialized intelligence and predictive foresight	Enhanced decision support and process optimization	Unprecedented decision automation
Action	Systematically invest in and operationalize world models.	Target high-impact and fast ROI scenarios in process optimization, productivity and safety.	Exploit multimodal capabilities and integrate synthetic data into end-to-end pipelines.

Key players to support implementation success



CIO

Lead: Develop a long-term strategy for leveraging world models to improve decision making, planning and intelligent automation.

Invest: Build the data, technology and talent foundations needed to operationalize world models at scale.

Drive: Demonstrate business value through improved forecasting, risk reduction and operational optimization.



IT partners

Data and AI teams: Build multimodal data pipelines that enable simulation, prediction and autonomous decision support.

Enterprise architecture: Create scalable foundations that support future world model deployment and integration.

Platform and engineering teams: Establish testing, validation and monitoring practices to ensure reliability and trust.



Business partners

Business leaders: Identify high-value use cases for scenario planning, forecasting and operational optimization.

Operations teams: Validate models using real-world processes and outcomes.

Finance and strategy: Support investments that improve resilience, productivity and long-term competitiveness.



Govern the autonomous agent platform

System-level control planes for
trustworthy autonomy

Developers are deploying digital workers that generate code, patch vulnerabilities and execute transactions in real time. But as machines produce software faster than teams can audit it, manual reviews become the primary bottleneck. These trends cover platform-owned governance: harnesses and semantic context engines that constrain what autonomous agents can see, use and produce.

Trend 4

AI context platforms

What is it?

This capability curates, integrates and delivers the dynamic background knowledge AI agents need to interpret inputs, make decisions and act in alignment with business objectives. It unifies scattered corporate knowledge into a machine-readable truth layer to ground autonomous digital workers.

Why trending?

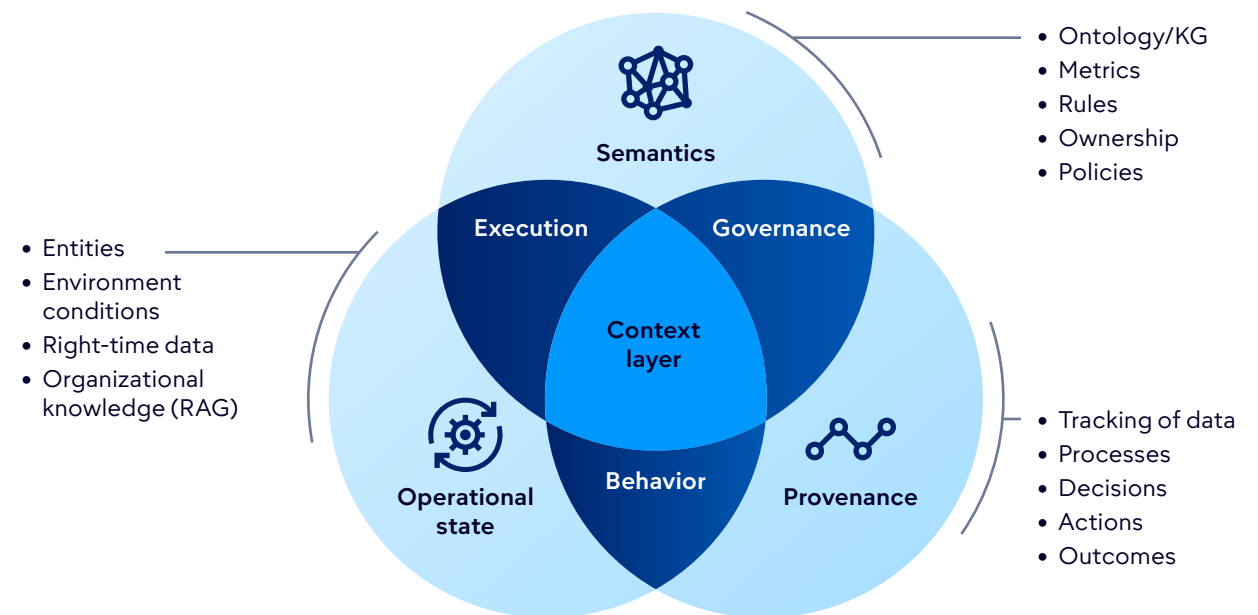
The rise of autonomous digital workers exposes legacy data limitations. While 42% of enterprises plan to deploy AI agents by the end of 2026, only 22% currently capture significant value from GenAI. This gap stems from fragmented operational knowledge, causing frequent hallucinations and prohibitive computing costs. To prevent stalled agentic deployments, organizations must deploy context platforms to systematically organize and prioritize business knowledge.

What's next?



By 2027, organizations that prioritize semantics in AI-ready data will increase agentic AI accuracy by up to 80% and reduce costs by up to 60%.

The 3 components of the context layer



Source: Gartner



Trend 4 | AI Context Platforms

Delivering results with AI context platforms

Action plan to drive modular automation and seamless integration

Steps	1 Form a phased maturity roadmap	2 Establish dual-ontology governance architecture	3 Enforce continuous, bi-directional ownership	4 Acquire knowledge engineering talent
Expected outcome	Progression from foundational capabilities to future-state semantics and knowledge	Improved AI accuracy and reduced costs	Interpretable, organized and secure knowledge	Self-serve, curated knowledge between AI agents and humans
Action	Centralize and structure policies before progressing to rule-based semantic automation.	Separate passive business rules from active, machine-generated decision traces.	IT maintains infrastructure while business units validate guiding policies.	Implement crucial semantic standards like RDF, OWL and SPARQL.

Key players to support implementation success

 CIO

- Lead:** Establish a strategy for enterprise context management to support trusted, scalable AI agents.
- Invest:** Build a shared context platform that enables AI initiatives to scale across the enterprise.
- Govern:** Define ownership, accountability and standards for business knowledge, context and AI outcomes.

 IT partners

- Data and AI teams:** Build and manage the context platform, including semantic models, knowledge graphs and governance controls.
- Enterprise architecture:** Establish standards for reusable and portable context across AI initiatives.
- Security and governance:** Implement controls for data quality, access, lineage, auditability and compliance.

 Business partners

- Business domain leaders:** Define, validate and continuously update the policies, rules and knowledge that guide AI agents.
- Operations leaders:** Identify high-value agent use cases and ensure context reflects current business processes and priorities.
- Risk and compliance:** Ensure contextual data aligns with regulatory and governance requirements.

Trend 5

AI coding agent harness

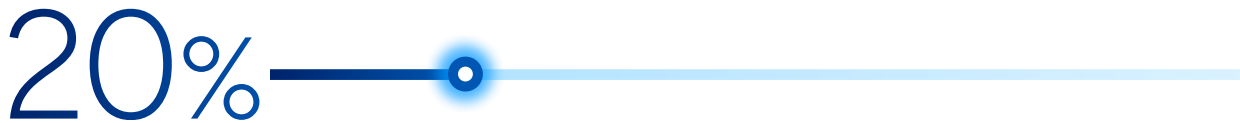
What is it?

A closed-loop system that governs autonomous developer behavior across the software development life cycle. It integrates coding platforms with enterprise context, model routing, verification gates and feedback loops to ensure software meets safety and compliance standards.

Why trending?

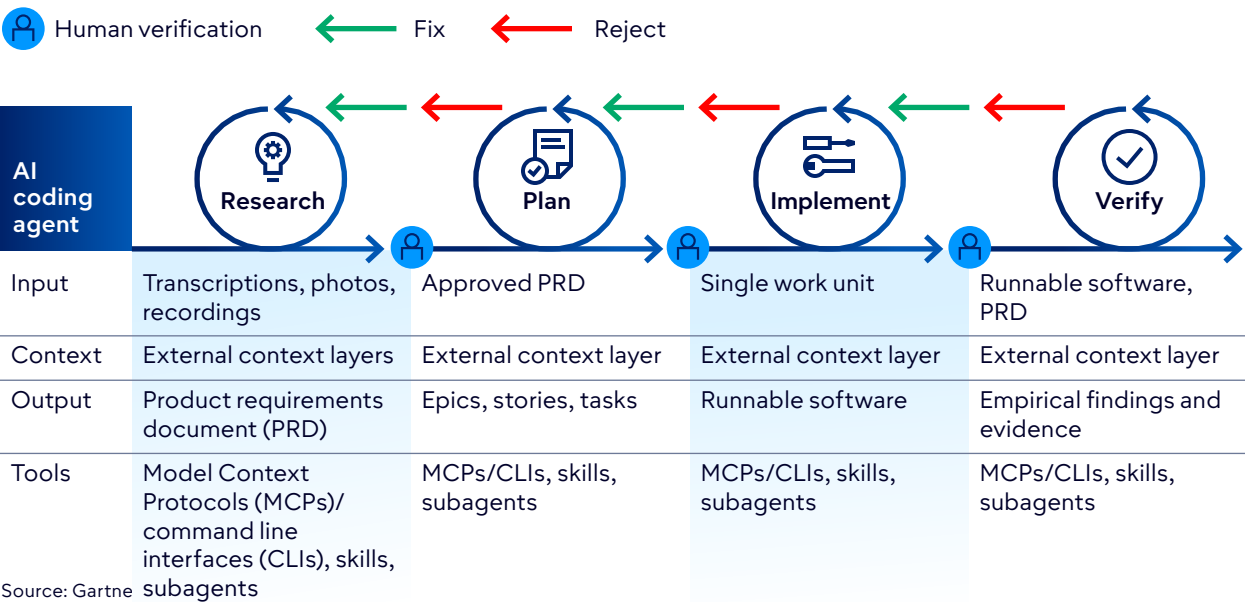
Coding agents are shifting from passive assistant tools into autonomous systems that execute software production work. However, scaling autonomous code generation without scaling validation shifts the bottleneck from writing code to proving that changes are safe, correct and maintainable. This ungoverned code generation rapidly compiles massive technical debt. Deploying harnesses sustains productivity by governing the entire software production system.

What's next?



By late 2026, autonomous coding agents will generate 20% of all public commits, making closed-loop harnesses mandatory to prevent critical software delivery quality failures.

The AI coding agent harness operates throughout the software development life cycle



Source: Gartne



Trend 5 | AI Coding Agent Harness

Delivering results with AI coding agent harnesses

Action plan to drive modular automation and seamless integration

Steps	1 Assign platform team ownership	2 Convert architectural standards and domain rules	3 Enforce automatic delivery backpressure
Expected outcome	Standardized enterprise software delivery	Contextual guidance for every agent	Unprecedented decision automation
Action	Consider coding agent harness configuration, model routing, approved tools, reusable workflows and verification policies.	Maintain machine-readable inputs that provide clear, codified knowledge documentation.	Run automated lint, test, security scanner and release-documentation gates before any code reaches human review.

Key players to support implementation success

 CIO	 IT partners	 Business partners
Lead: Establish AI-native software delivery as a strategic platform capability. Fund: Invest in a dedicated platform team to own harness configurations, standards and governance. Govern: Define risk, compliance and accountability requirements for autonomous software delivery.	Platform engineering: Own harness configurations, model routing, reusable workflows and developer experience. Architecture: Convert standards, design patterns and institutional knowledge into machine-readable context. Security and risk: Embed verification gates and protect the harness control plane from tampering and misuse.	Product leaders: Define requirements, domain rules and acceptance criteria for agent-generated solutions. Finance: Support long-term platform investment and measure value realization. Legal and compliance: Ensure autonomous delivery aligns with regulatory, audit and policy requirements.

Trend 6

AI agent identity

What is it?

A unique digital representation that actively governs autonomous digital workers across your organization. This framework correlates computational composite elements like model weights, prompts and credentials with runtime behaviors to establish continuous trust and human accountability.

Why trending?

AI agents expose massive vulnerabilities in legacy systems that can't deliver just-in-time access. Failing to secure these active digital workers immediately risks halting zero-trust deployments and derailing broader automation investments.

This urgent security crisis is driving rapid market consolidation as cybersecurity megavendors acquire specialized startups to deliver unified platforms that can govern human and machine actors.

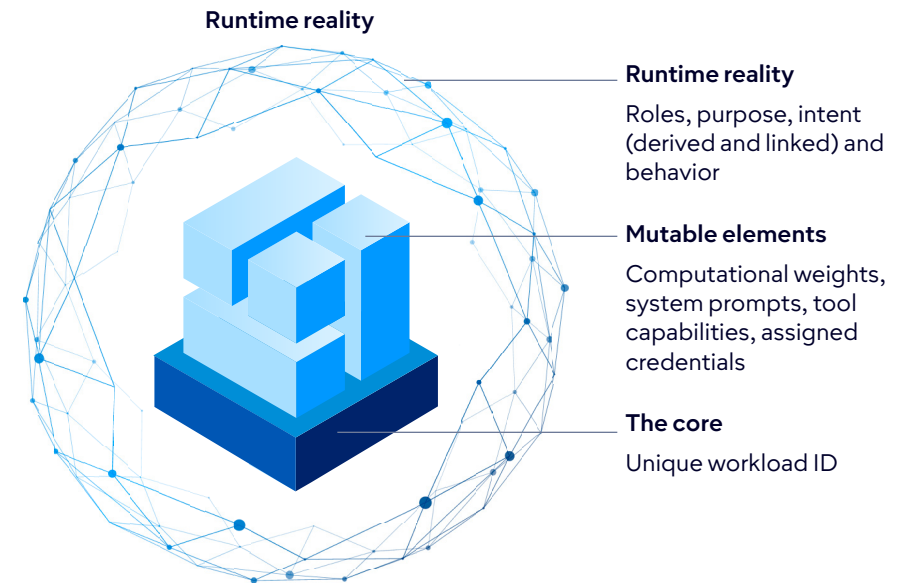
What's next?

25%

By 2028, 25% of enterprise security breaches will trace back to AI agent abuse due to unmanaged machine privileges and legacy credential practices. If organizations don't resolve these identity challenges, over half of their enterprise AI initiatives will halt entirely.

The evolution from human-centric to composite identity for AI agents

An AI agent's identity is constructed from mutable computational elements and requires an identity model that actively correlates that agent's identity with its runtime reality.



Source: Gartner



Trend 6 | AI Agent Identity

Delivering results with AI agent identities

Action plan to drive modular automation and seamless integration

Steps	1 Inventory all agent identities	2 Prohibit human credential sharing	3 Transition to composite identities	4 Demand converged identity platforms
Expected outcome	Identification of identity gaps	Clear ownership and auditability	Defined control requirements and taxonomies	A single control plane
Action	Discover, map and manage both sanctioned and shadow agents across your environments.	Issue unique, dedicated credentials to agents.	Enforce dynamic, policy-controlled access and zero trust policies.	Engage vendors to ensure management of both human and machine workloads.

Key players to support implementation success

 CIO	 IT partners	 Business partners
Lead: Establish an enterprise strategy for governing AI agents as digital coworkers. Prioritize: Invest in identity platforms that securely manage human, machine and AI agent identities together. Govern: Define accountability, risk tolerance and ownership for all AI agent workloads.	Identity and security: Implement composite identity models, least-privilege access and continuous verification for AI agents. Enterprise architecture: Establish standards for agent registration, credential management and policy-based authorization. Infrastructure and operations: Monitor agent activity, manage runtime controls and support secure deployment at scale.	Risk and compliance: Ensure AI agent activities align with governance, audit and regulatory requirements. Legal: Define accountability frameworks for agent actions and decision authority. Business leaders: Validate agent roles, permissions and acceptable use within business processes.

Trend 7

Autonomous exposure remediation

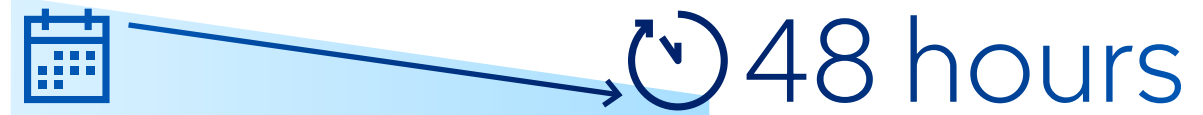
What is it?

An integrated set of capabilities that uses AI and automation to find, prioritize and fix security vulnerabilities across the enterprise digital estate. This system automatically deploys patches into production environments and initiates testing loops to safely roll back failed deployments.

Why trending?

The traditional defensive process is broken, leaving organizations with an average 50-day exposure window where vulnerabilities remain unpatched. By replacing slow, manual validation with continuous machine-speed defense, technology leaders transform vulnerability management from a passive queue into an active operational shield.

What's next?



By 2031, organizations deploying autonomous exposure remediation will reduce their average vulnerability containment window from weeks to within 48 hours.

Autonomous exposure remediation phases



Source: Gartner



Trend 7 | Autonomous Exposure Remediation

Delivering results with autonomous exposure remediation

Action plan to drive modular automation and seamless integration

Steps	1 Initiate narrow scope projects	2 Integrate vulnerability detection	3 Balance automated scanning	4 Conduct cost analysis early and often
Expected outcome	Safe testing and long-term scaling	Increased discovery volume	Improved performance and accuracy	Balanced security budgets
Action	Start with nonsensitive custom code bases to pilot automated patch generation and rollback capabilities to build experience.	Suggest real-time fixes directly into active software development loops.	Balance scanning with proportional prioritization practices to prevent overwhelming application teams with discovery queues.	Analyze compute costs and model token consumption to budget for unpredictable cybersecurity technologies.

Key players to support implementation success



CIO

Lead: Establish a roadmap for autonomous exposure remediation aligned to cybersecurity and business resilience objectives.

Prioritize: Invest in automation capabilities that reduce exposure windows and improve remediation speed.

Govern: Define risk thresholds, oversight requirements and accountability for automated remediation decisions.



IT partners

Cybersecurity: Identify priority use cases and implement AI-augmented vulnerability discovery, validation and remediation workflows.

Software engineering: Integrate automated testing, fix validation and remediation into development processes.

Infrastructure and operations: Support deployment, monitoring and rollback capabilities needed to safely automate remediation.



Business partners

Risk and compliance: Align remediation practices with governance, regulatory and audit requirements.

Product leaders: Balance remediation priorities with delivery objectives and operational risk tolerance.

Finance: Support investments that improve resilience and reduce the business impact of exploitable exposures.



Architect durable agility

Transition to sovereign, disposable
and organic environments

SaaS fatigue, provider lock-in and energy limits are turning absolute cloud dependency into an existential risk. Building a resilient business on foreign-controlled models is untenable when providers can restrict, modify or withdraw them overnight. These trends focus on sovereign architecture: legal and technical independence, disposable stacks and early pilots of biological computing.

Trend 8 SovereignTech

What is it?

Hardware, software, databases and AI models technically and legally architected to offer realistic exit strategies from critical providers. These technologies remain perpetually available to prevent lock-in and secure complete operational continuity.

Why trending?

Geopolitical friction and extraterritorial laws like the U.S. CLOUD Act pose real, immediate risks of sudden service cutoffs. Regulations like DORA contractually mandate proven cloud exit strategies and CADA prescribes strict sovereignty-enabling architectures. As AI automates professional tasks, massive subscription and API fees paid to foreign providers drain domestic wealth.

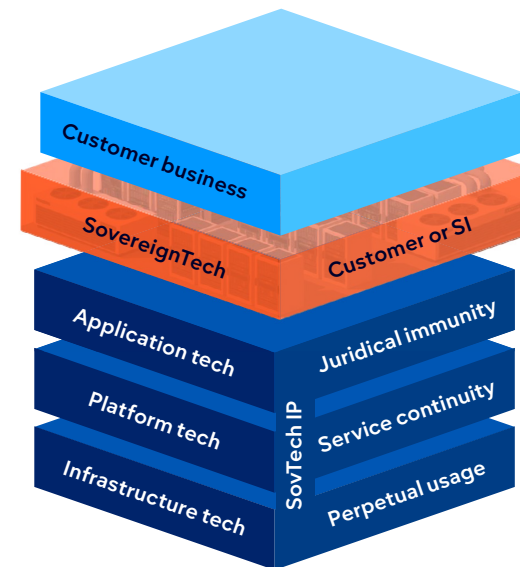
To secure long-term continuity and prevent proprietary data from being permanently absorbed into foreign model weights, leaders must establish technical and legal independence.

What's next?

75%

By 2030, over 75% of non-U.S.-based organizations will adopt digital sovereignty strategies, shifting critical workloads to reduce geopolitical and vendor lock-in risks.

What makes technology sovereign



SovereignTech (SovTech) assures your local operations will not collapse if a provider withdraws its IP, ensures AI-created value stays at home and secures your ability to act independently in a crisis.

What is it?

SovTech refers to technologies like cloud platforms, application code, servers, chips, databases, agents and AI models, technically and legally architected to enable realistic exit strategies from critical providers and remain perpetually available to customers to support real autonomy and resilience.

Source: Gartner

Trend 8 | SovereignTech

Delivering results with SovTech



Action plan to drive modular automation and seamless integration

Steps	1 Track distributed sovereign delivery models	2 Master lean innovation strategies	3 Monitor global sovereignty alliances	4 Directly engage technology providers
Expected outcome	Defined sovereignty requirements	Multiregional operational resilience	Identification and understanding of emerging standards	Minimal risk exposure
Action	Evaluate private, on-premises and ecosystem-driven alternatives to standard public clouds.	Use n-1 generation technology creatively and share capabilities reciprocally with trusted allies.	Consider the Trusted Tech Alliance and the EU Tech Sovereignty Package.	Assess provider appetite for sovereign delivery options and no-killswitch assurances.

Key players to support implementation success



CIO

Lead: Define a digital sovereignty strategy aligned to business continuity and operational resilience.

Prioritize: Evaluate critical technology dependencies and establish realistic exit and replacement strategies.

Govern: Balance innovation, risk and autonomy when selecting cloud, AI and technology providers.



IT partners

Enterprise architecture: Design systems that support portability, interoperability and provider flexibility.

Infrastructure and cloud: Assess sovereign, distributed and multipartner delivery models for critical workloads.

Security and risk: Test continuity plans and ensure compliance with evolving sovereignty and resilience requirements.



Business partners

Procurement: Evaluate providers based on resilience, exit options and dependency risks, not just cost and functionality.

Legal and compliance: Monitor regulatory requirements related to data, operational and technology sovereignty.

Finance: Support investments that strengthen long-term resilience and reduce single-provider risk.

Trend 9

Disposable applications

What is it?

Purpose-built software applications designed to be intentionally retired once their specific business purpose has been fulfilled or is no longer relevant. These temporary solutions operate as enterprise-grade applications with predefined lifespans, rather than permanent fixtures.

Why trending?

AI-powered vite coding tools are democratizing software creation, empowering both citizen and professional developers to rapidly generate customized applications for short-term operational needs. This shift allows deployment of targeted, temporary solutions with predefined lifespans instead of accumulating permanent, costly software assets.

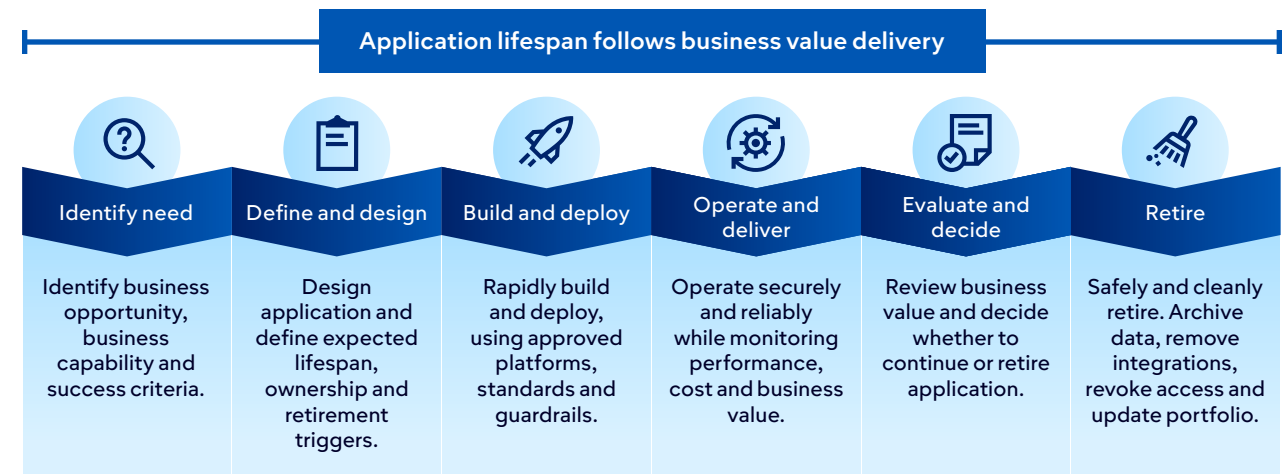
What's next?

80%

By 2030, widespread SaaS fatigue and AI-driven software abundance will force leading organizations to ensure 80% of new applications are disposable and easy to replace.

Disposable applications fundamentally alter how organizations buy, design and budget for software. Rather than maintaining legacy platforms indefinitely, the application portfolio becomes a dynamic system that continuously renews itself as redundant assets are retired.

The disposable application life cycle



Source: Gartner

Trend 9 | Disposable Applications

Delivering results with disposable applications



Action plan to drive modular automation and seamless integration

Steps	1 Audit your application portfolio	2 Establish a dedicated platform team	3 Position upcoming SaaS contract negotiations
Expected outcome	A roadmap for application modernization	Rapid software life cycle flows	Avoid vendor lock-in
Action	Classify which core capabilities require permanent software and which can be served by temporary, on-demand solutions.	Oversee, govern and manage the flow of transient assets across the enterprise.	Use renewals as leverage to reduce seat counts and secure open APIs.

Key players to support implementation success



CIO

Lead: Establish a disposable application strategy that aligns application lifespans with business value.

Invest: Fund the platforms, automation and governance needed to support rapid application creation and retirement.

Govern: Define accountability, ownership and life cycle standards across the application portfolio.



IT partners

Platform engineering: Provide the tools, guardrails and automation needed to build and retire applications at scale.

Enterprise architecture: Define standards that align governance to application risk, criticality and expected lifespan.

Security and operations: Manage application retirement, data life cycle requirements and security controls.



Business partners

Business owners: Define application objectives, expected lifespan and retirement criteria.

Finance: Shift funding models to support application creation, renewal and retirement.

Risk and compliance: Ensure governance and controls remain appropriate throughout the application life cycle.

Trend 10

Wetware as a service

What is it?

An emerging operational model that provides remote cloud-based access to living or synthetic biological systems for computation. These hosted organic processors utilize the natural plasticity of biochemical networks to run complex algorithms with extreme energy efficiency.

Why trending?

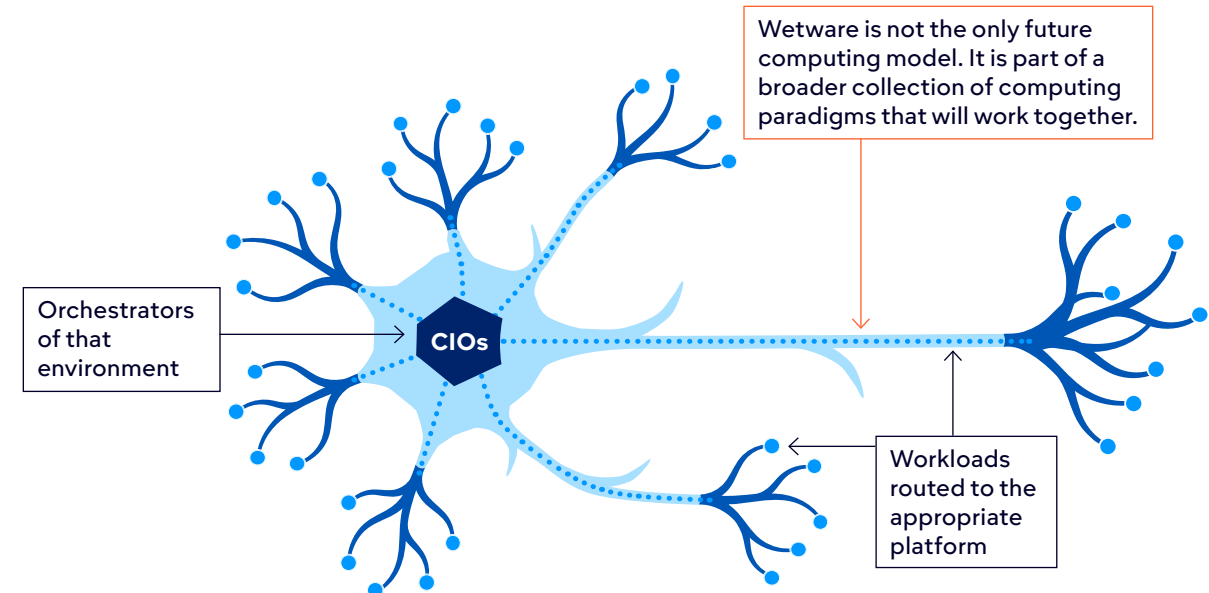
Traditional silicon computer hardware can't scale enterprise AI indefinitely due to unsustainable environmental and energy demands. Lab-grown biological neurons can perform goal-oriented computation with extreme efficiency, running complex pattern recognition algorithms on a fraction of traditional server power. Startups are bridging the physical science gap by hosting delicate biocomputers in remote, sterile laboratories. Biocomputing as a cloud-based subscription service allows organizations to launch immediate technical pilots without investing in capital-intensive wet labs or specialized neurological transport infrastructure.

What's next?

25%

By 2030, 25% of enterprise organizations prioritizing specialized low-power AI will deploy biological computing to bypass traditional silicon limits.

Wetware as a service as part of computing orchestration



Source: Gartner



Trend 10 | Wetware as a Service

Delivering results with wetware as a service

Action plan to drive modular automation and seamless integration

Steps	1 Audit software architectures	2 Establish low-risk cloud sandboxes	3 Convene an interdisciplinary task force	4 Design replication and redundancy policies
Expected outcome	Identification of high-return use cases	Safe piloting of volatile biocomputer lifespans	Bridge the talent gap	Safeguards that protect cognitive datasets and neurorights frameworks
Action	Identify high-consumption pattern recognition workloads suitable for redirection to low-power biological substrates.	Use remote subscription platforms to build early developer familiarity with living processors.	Combine software developers, neuroscientists and ethicists to fuse computer science and neurology.	Protect critical application data against volatile cell lifespans and sudden processor death.

Key players to support implementation success

 CIO	 IT partners	 Business partners
Lead: Establish a strategy for integrating biological computing into future AI and infrastructure roadmaps. Invest: Develop orchestration capabilities that dynamically route workloads across diverse computing platforms. Govern: Define risk, ethical and resilience frameworks for biological computing adoption.	Enterprise architecture: Identify workloads that could benefit from biological processing and hybrid computing models. Platform engineering: Build orchestration layers that manage workload routing across silicon, quantum, neuromorphic and biological processors. Security and risk: Develop controls for neurodata privacy, redundancy and business continuity.	Research and innovation teams: Evaluate opportunities to apply biological computing to complex optimization and discovery challenges. Legal and compliance: Establish policies addressing ethical use, intellectual property and emerging neurorights considerations. Finance: Support investment in next-gen computing.

Actionable, objective insights

Explore these additional complimentary resources and tools for IT leaders:

Tool

AI Use Case Insights

Explore, evaluate and prioritize 1,300+ proven AI use cases and real-world case studies.

Get Started



Tool

Gartner Benchmarking and Diagnostics

Prioritize, budget and optimize with tailored benchmarks for critical domains.

Get Started



eBook

The Gartner CIO Report

Explore the top CIO challenges, according to 12K+ of your CIO peers.

Download Now



Tool

AskGartner: Your AI-Powered Thought Partner

Get AI-powered access to analyst-vetted insights to build frameworks and speed up execution.

Get Started



Already a client? Get access to even more resources in your client portal. [Log In](#) ↗

Connect with us

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

U.S.: 1 855 322 5484

International: +44 (0) 3300 296 946

[Become a Client](#)

Leaders who know, choose Gartner. See how.
gartner.com/en/what-we-do

Gartner for CIOs
gartner.com/en/chief-information-officer/products/gartner-for-cios

Stay connected to the latest insights



Attend a Gartner conference
[View Conference](#)