Gartner

Defending Growth in the Age of AI

Build resilience, mitigate risk and maintain cybersecurity in the age of AI.

Build resilience, mitigate risk and maintain cybersecurity in the age of AI

The focus has shifted from “uptime” to “business defensibility.” Managing systemic exposure now decides if an enterprise captures growth or succumbs to a cascade failure.

63% of board members prioritize AI innovation to counter volatility, yet only 39% see cyber investment as a driver of shareholder value.

Managing exposure determines if you grow or succumb to failure. The Gartner stance is clear. CIOs must:

- → Move beyond traditional “perimeter” security to build an enterprise resilient by design against high-velocity risks
- → Replace reactive, technical checkboxes with a business-aligned foundation that treats security as a growth lever
- → Use identity-first security and outcome-driven metrics to ensure protection as the organization automates

Paul E. Proctor
Distinguished Vice President Analyst

Your roadmap to success

CIOs can no longer rely on perimeter-based security to manage enterprise risk. As AI accelerates automation and expands the attack surface, resilience must be designed into how the business operates — not layered on after the fact.

This requires a shift from reactive controls and technical checklists to a business-aligned cybersecurity foundation. Identity-first security, continuous verification and outcome-driven metrics enable CIOs to link protection to revenue, risk tolerance and operational performance — ensuring the enterprise stays secure as it moves faster.

Gartner supports CIOs in making this transition with confidence. By combining expert judgment with objective insights, Gartner helps CIOs architect adaptive security models, anticipate emerging threats and align every cyber investment to measurable business outcomes — protecting growth while enabling it.

1. **Revisit and modernize.**
2. Build a new cybersecurity foundation.
3. Reset your North Star.

4 key outcomes to consider in Step 1

- Audit technical debt to close visibility gaps.
- Baseline shadow AI to map unmanaged risk.
- Align security controls with strategic business goals.
- Map specific threats to relevant business priorities.

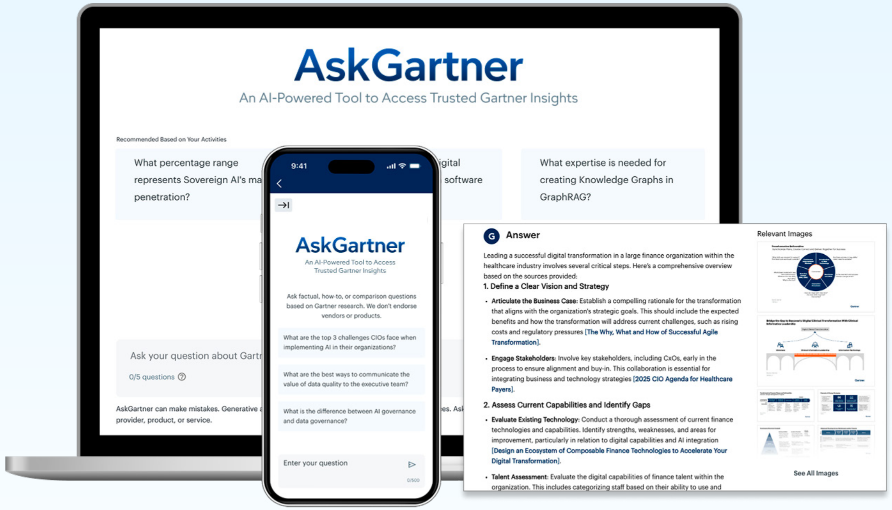
Key questions your CIO peers are asking Gartner

Gartner clients can ask questions like these directly on AskGartner.

Gartner clients can click to explore answers.

How can our organization secure generative AI implementations while maintaining speed to value?	Explore Answer ↗
What are the specific security risks and business implications of adopting AI-native technologies?	Explore Answer ↗
What are the essential cybersecurity metrics required to demonstrate defensibility to the board?	Explore Answer ↗
How much security is “enough” for our specific risk appetite and revenue goals?	Explore Answer ↗
How can IT operations be modernized to secure and support autonomous digital workflows?	Explore Answer ↗

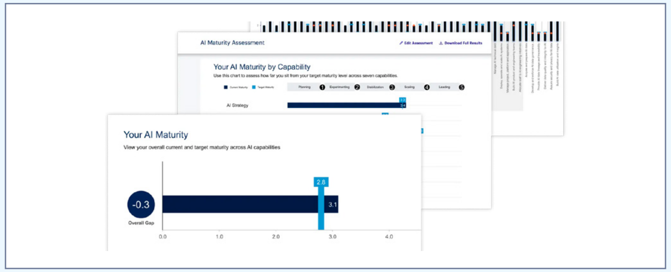
Your peers use AskGartner to answer these questions in minutes.



Learn More

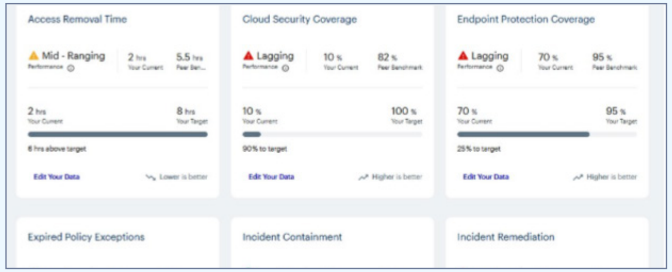
Gartner resources turn your priorities into plans and actions

Revisit and modernize.



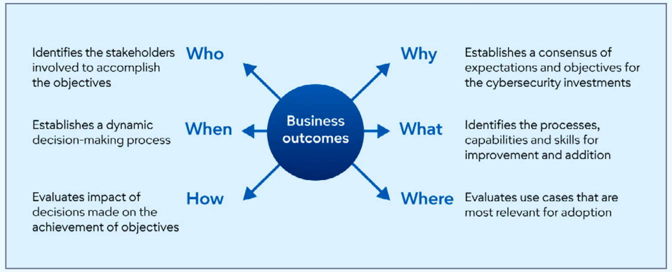
Gartner AI Maturity Assessment ↗

Build a new cybersecurity foundation.



Cybersecurity Business Value Benchmark ↗

Reset your North Star.



Cybersecurity Value: How CIOs Win C-Suite Support ↗

Engage with Gartner

- Connect with an analyst to baseline your outcome-driven metrics (ODMs) and establish protection-level agreements (PLAs).
- Engage with an Executive Partner to transition to a “sense-maker” leadership model and facilitate candid board-level dialogues.

Expected outcomes

- Defensible investment decisions through standardized ODMs
- Increased board confidence via risk-aligned PLAs
- Clear alignment of cybersecurity performance with enterprise business value

Who needs to be involved?

Cybersecurity is no longer a function — it is a coordinated leadership system. CIOs who succeed do not centralize control; they orchestrate alignment across risk, finance, security and business leadership to ensure resilience is built into how the enterprise operates. We have outlined the recommended functions to involve and their roles to ensure the best success in hitting the milestones.

CIO/Head of Technology ↗

Acts as the enterprise orchestrator of defensibility, aligning technology, risk and business leadership to ensure cybersecurity protects growth, accelerates innovation and delivers measurable outcomes.

CFO ↗

Sets the tone that cybersecurity is a growth enabler, aligning executive leadership around balancing innovation speed with enterprisewide resilience and defensibility.

Chief Data and Analytics Officer and Team ↗

Ensure AI and data initiatives are governed and secured by design, balancing innovation velocity with control over emerging risks such as model exposure, data leakage and unmanaged AI usage.

Chief Information Security Officer and Team ↗

Own the design and execution of an adaptive cybersecurity strategy, translating rapidly evolving threats into business-aligned risk decisions and measurable protection outcomes that scale with the enterprise.

Head of I&O and Team ↗

Embed resilience into enterprise platforms and operations, ensuring systems are designed not only to prevent disruption but to recover quickly and sustain performance under stress.

CEO and the Board ↗

Set enterprise expectations and accountability for defensibility by positioning cybersecurity as a growth enabler and requiring clear, outcome-driven visibility into risk, resilience and business impact.

Client Story

Aligning Information Security With Business Goals for a Sustainable Future

Mission-critical priority

Jukka Vuori, chief information security officer at SSAB, sought support from Gartner as the client worked to update and align their information security strategy with the company's transition to fossil-free steel. The client worked with Gartner to successfully achieve strategic objectives, enhancing their security program to support the company's greener future initiatives.

How SSAB leveraged Gartner resources

With Gartner guidance and support, the client refreshed their information security strategy to align with their transition to fossil-free steel. They also utilized Gartner budget efficiency tools to optimize resource allocation within their information security program and leveraged insights from conference sessions on risk quantification and outcome-driven metrics to effectively measure and manage risks.

Mission accomplished

With Gartner support, the client utilized the Gartner Priorities Navigator™ framework for CISOs to gain a holistic view and facilitate informed decision making by drilling down into specific topics and accessing relevant insights. Additionally, they leveraged Gartner tools and insights to support effective communication between the information security team and the organization's leadership.

Watch the full story ↗

Address your other mission-critical priorities

Accelerate AI enterprise value realization at scale.

Only 20% of AI initiatives currently deliver ROI and only 2% deliver disruptive value (return on future or ROF).

Manage costs strategically to spend smarter and scale faster.

Only **18%** of CIOs currently rate themselves as effective at dynamic reprioritization of resources, which is a significant driver of their ability to derive business value from technology investments.

Build the human-AI workforce.

45% more business value is driven by future-resilient talent strategies, yet only **36%** of CIOs are effective at building them.

Build resilience, mitigate risk and maintain cybersecurity in the age of AI.

77% of CIOs rate security and risk-related factors as top challenges to successfully implementing autonomous technologies at scale in their enterprise.

Modernize enterprise platforms to enhance agility and performance.

Only **54% (one in two)** of CIOs rate their IT organization as effective at equipping their enterprise with the required platforms and tools needed for investments.

Redesign IT operating model for effectiveness in turbulent times.

Only **24%** of CIOs report they have been highly effective at establishing an IT operating model that flexes with changing business needs.

Architect the next-generation enterprise for a tech-intensive future.

Only **31%** of CIOs rate themselves as effective at fostering ongoing enterprisewide, technology-enabled innovation.

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

Interested in becoming a client?

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

Stay connected to the latest insights

Gartner®