

# Master AI Cyber Risk & Governance

Adapt cybersecurity strategies for AI



# Accelerate enterprise AI value realization at scale

CISOs must empower their organizations to realize AI goals confidently, knowing they are built on secure principles.

By 2027, **90%** of successful AI implementations in cybersecurity will be tactical — task automation and process augmentations — rather than role replacing.

As AI scales, CISOs must mature governance to confidently pursue business-first AI goals, trading reactive checkboxes for an identity-first foundation that defeats high-velocity risks.

Master AI governance and security by executing these key steps:

- Define AI risk boundaries early to empower the organization to pursue AI goals built on secure principles.
- Implement AI-augmented defenses and robust visibility tools to protect against the risks of an autonomous economy.
- Measure the performance of AI investments and reduction of AI risk using business-aligned, outcome-driven metrics.

## Your roadmap to success

As AI becomes mainstream, CISOs must mature their governance processes to incorporate AI security enabling confidence to pursue business first AI goals at the same time as addressing the risks.

Gartner empowers organizations to confidently achieve business-first AI goals by defining early risk boundaries, implementing AI-augmented defenses and selecting trusted tools with strong security controls. CISOs master this priority by engaging Gartner analysts to refine strategies, utilizing Executive Partners for change management and leveraging the CISO's roadmap to securely scale AI usage.

### 1. Define AI risk boundaries and governance principles early.

2. Prioritize cybersecurity and IAM AI adoption aligned with business goals.
3. Select trusted tools with strong AI-enabled security controls.
4. Implement AI-augmented defenses and best-in-class AI risk visibility tools.
5. Measure performance of AI investments and reduction of AI-related risk.

### One key outcome to consider in Step 1

Understand the risks associated with the AI applications used and built by your organization. Build AI literacy to better understand how to leverage AI to benefit cybersecurity and IAM.

# Key questions to ask

Gartner clients can ask questions like these directly on [AskGartner](#).

How can I discover and secure the use of AI by the organization and craft AI policies that align to our organization’s risk tolerance?

[Explore Answer](#)

How do I respond to new cybersecurity regulations for AI, critical infrastructure and privacy and ensure my third parties maintain compliance?

[Explore Answer](#)

What steps do I take to best manage the risks associated with AI in my cybersecurity program?

[Explore Answer](#)

How can AI reduce my exposure to threats?

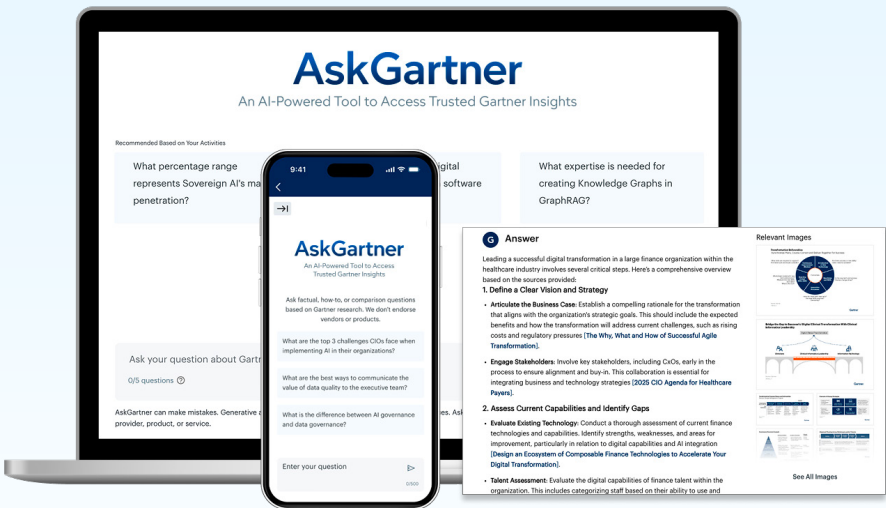
[Explore Answer](#)

What happens when posttype AI cybersecurity investment in the boardroom and C-suite turns into AI regret?

[Explore Answer](#)

Gartner clients can click to explore answers.

Your peers use AskGartner to answer these questions in minutes.



[Learn More](#)

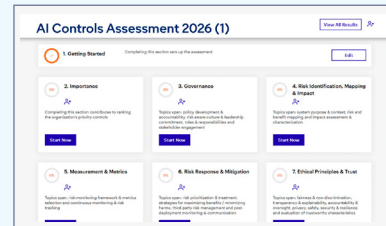
# Gartner resources turn your priorities into plans and actions

**Define AI risk boundaries and governance principles early.**



**AI Cybersecurity Leadership: 5 Steps to Secure Enterprise Innovation**

**Prioritize cybersecurity and IAM AI adoption aligned with business goals.**



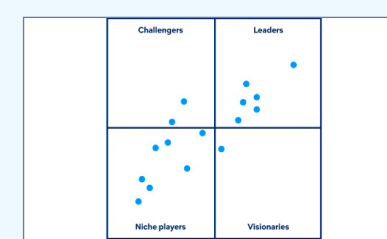
**AI Controls Assessment**

**Select trusted tools with strong AI-enabled security controls.**



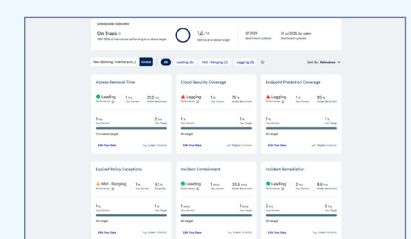
**Innovation Insight for AI Usage Control**

**Implement AI-augmented defenses and best-in-class AI risk visibility tools.**



**Magic Quadrant for Cyberthreat Intelligence Technologies**

**Measure performance of AI investments and reduction of AI-related risk.**



**Cybersecurity Business Value Benchmark**

## Engage with Gartner

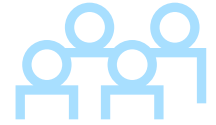
- Connect with an analyst to identify, review and refine your AI enablement strategy in cybersecurity.
- Get guidance from Executive Partners on change management best practices throughout your journey, including how to best overcome roadblocks along the way.

## Expected outcomes

- Build AI literacy in cybersecurity teams to enhance their ability to achieve tasks faster and reduce risk to the organization.
- Support AI initiatives across the business, becoming a trusted advocate for the secure use of AI.
- Understand the impact and mitigations for new and novel threats related to AI.

## Who needs to be involved?

The most successful organizations establish cross-functional teams for their cybersecurity for AI initiatives. We have outlined the recommended functions to involve and their roles to ensure the best success in hitting the milestones.



### CIO/Head of Technology ↗

Sets a clear enterprisewide AI ambition, finds use cases; quantifies benefits and risks, aligns teams and competencies, and drives innovation across the organization.

### Head of AI ↗

Develops, champions and executes the organization's AI strategy by overseeing AI use case selection and scaling, establishing governance and literacy, implementing solutions, monitoring market trends, building a world-class team and reporting on business impact.

### Chief Data & Analytics Officer And Team ↗

Lead the organization's AI data strategy by identifying use cases, establishing governance, developing new data value and ensuring data readiness for AI technologies.

### Head of Enterprise Architecture and Team ↗

Align AI structure and design with organizational value by guiding use cases and requirements, governing architecture investments, leading adoption decisions and architecting AI solutions.

### Software Engineering Leader and Team ↗

Drive AI integration by clarifying desired outcomes, establishing engineering best practices, transforming services with an AI-first approach and architecting software development to support AI objectives.

## Client Story

## Advancing Identity and Access Management With Strategic Guidance and Insights

### Mission-critical priority

As organizations adapt their cybersecurity strategies for modern challenges like AI, Darrell Jenkins, CISO at Clayton, faced a mission-critical priority centered on identity and access management (IAM), application control and operational resilience. As modernizing IAM programs is essential to enabling secure, identity-first cybersecurity that covers people, machines and AI agents, Jenkins needed to ensure his strategy was rock-solid to support safe enterprise growth.



### How Clayton leveraged Gartner resources

To navigate this complex technology landscape, Clayton utilized Gartner analyst consultations to receive one-on-one guidance, validate its strategic approach and evaluate vendors during the RFP process. It also leveraged targeted Gartner insights and benchmarking tools to precisely shape its identity and access management requirements.



### Mission accomplished

With Gartner support, Jenkins successfully validated the company's IAM strategy, received specific feedback on complex ROI calculations and ultimately secured vital executive buy-in and budget approval. Additionally, Gartner provided critical feedback during the implementation of services, which helped Clayton avoid cost overruns and execute its security initiatives with confidence.

[Watch the full story ↗](#)



## Address your other mission-critical priorities



### Build and evolve a resilient and agile cybersecurity program.

Only **14%** of non-executive directors are very or extremely confident in the effectiveness of current cyber risk assessments.



### Adapt cybersecurity strategies for AI.

**91%** of senior business leaders see AI as a value driver, making AI cybersecurity governance essential.



### Optimize cybersecurity technology and architecture effectiveness.

**75%** of CISOs identify budget or resource constraints as a challenge to meet their strategic objectives in the next six months.



# 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 CISOs

<https://www.gartner.com/en/cybersecurity>

Stay connected to the latest insights

