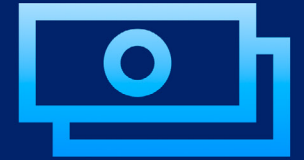




Prioritize Cybersecurity Investments to Deliver Business Outcomes

Optimize cybersecurity technology and architecture effectiveness.



Optimize cybersecurity technology and architecture effectiveness

Optimizing investments in cybersecurity requires a balance of effective technology selection, with a focus on cost-effectiveness. The pressures to reduce risk and demonstrate the value of cybersecurity and IAM investments to the organization's mission require balancing effective technology selection with efficient business enablement.

By **2027, 70%** of large organizations will face major cybersecurity incidents due to fragmented risk management, weak supply chain controls and poor integration of threat intelligence, leading to repeated disruptions and regulatory challenges.

Understaffed teams and fragmented risk management lead to repeated disruptions and increased breach costs. CISOs can no longer afford redundant capabilities or inefficient cybersecurity architectures.

Our stance is that CIOs must:

- **Define** business-justifiable requirements to match cyber and IAM investments directly with organizational capabilities
- **Select** cybersecurity and IAM tools that align with modern, future-ready architectures for long-term agility
- **Measure** current tool performance and cost with outcome-driven metrics to rationalize portfolios and reduce overhead

This guide equips CISOs to balance effective technology selection with efficient business enablement to cost-optimize cybersecurity.

Your roadmap to success

Optimizing cybersecurity investments demands precise technology selection and cost-effectiveness. To reduce risk and prove the value of cybersecurity and IAM tools, CISOs must balance effective technology deployment with efficient business enablement.

Gartner equips CISOs with actionable guidance, independent evaluation frameworks and critical insights to rationalize solution provider portfolios, prioritize technology investments and design future-ready cybersecurity architectures. CISOs maximize tool performance, eliminate redundant capabilities and cost-optimize cybersecurity architectures to enable secure business growth.

1. **Define business-justifiable cybersecurity and IAM technology requirements.**
2. **Select** cybersecurity and IAM tools to enable future-ready architectures.
3. **Automate** to reduce complexity and overhead.
4. **Measure** tool performance and cost to streamline investment strategy.
5. **Optimize** operations for efficiency and continuous improvement.

3 key outcomes to consider in Step 1

Establish precise organizational requirements to guarantee cybersecurity and IAM investments directly support business objectives.

Map investment objectives to technical capabilities to ensure selected tools deliver proven security performance and eliminate redundancy.

Optimize technology deployment to maximize resource utilization and secure the most efficient cost-to-value ratio for the enterprise.

Key questions to ask

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

How do I rationalize my cybersecurity vendor portfolio and ensure I am not paying for redundant capabilities?

[Explore Answer ↗](#)

How should we frame modern identity challenges and use cases to ensure we are aligned with emerging security standards?

[Explore Answer ↗](#)

How should I prioritize cybersecurity technology investments and staffing for my cybersecurity strategy and roadmap?

[Explore Answer ↗](#)

What should I set as budget for investment in infrastructure security tools and services?

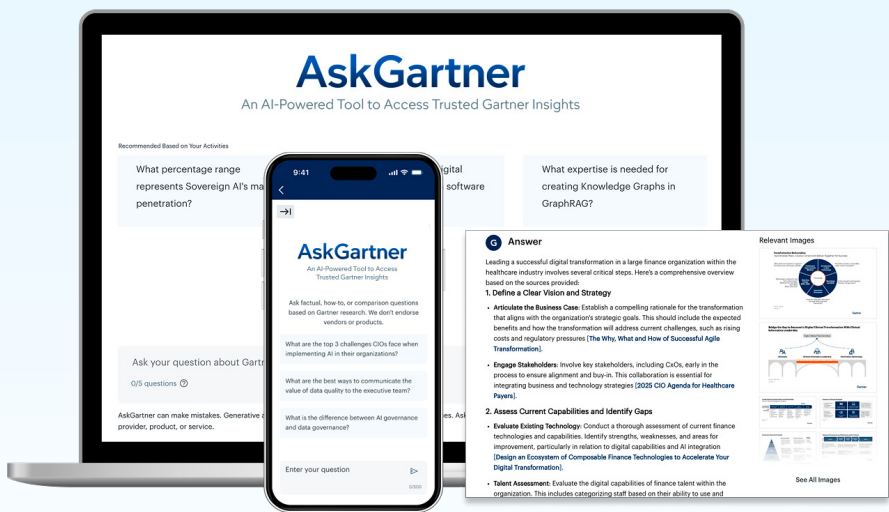
[Explore Answer ↗](#)

How can IAM strategies and principles be aligned with organizational goals to deliver business value?

[Explore Answer ↗](#)

Gartner clients can click to explore answers.

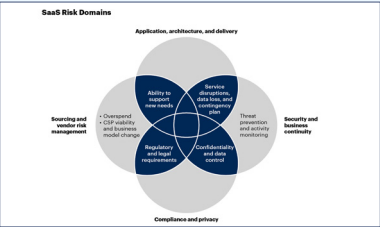
Your peers use AskGartner to answer these questions in minutes.



[Learn More](#)

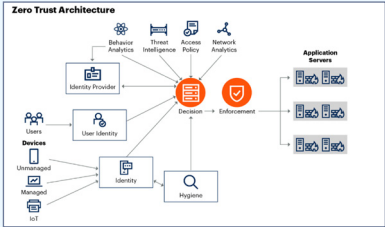
Gartner resources turn your priorities into plans and actions

Define business-justifiable cybersecurity and IAM technology requirements.



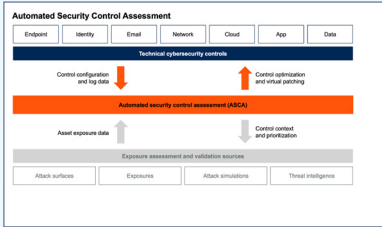
Strategic Roadmap for SaaS Security in the Age of AI ↗

Select cybersecurity and IAM tools to enable future-ready architectures.



How to Build Zero-Trust Architecture ↗

Automate to reduce complexity and overhead.



Innovation Insight: Automated Security Control Assessment ↗

Measure tool performance and cost to streamline investment strategy.



Accelerator for Cybersecurity Cost Optimization ↗

Optimize operations for efficiency and continuous improvement.



Gartner IT Score for Cybersecurity and Risk Management Framework ↗

Engage with Gartner

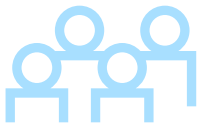
- Connect with an analyst to identify, review and refine your cybersecurity technology and architecture strategy.
- Get guidance from Executive Partner on change management best practices throughout your journey, including how to best overcome roadblocks along the way.

Expected outcomes

- Evaluate cybersecurity technologies and services from providers using unbiased independent frameworks.
- Build a cybersecurity technology consolidation strategy through understanding capabilities, roadmaps and future states.
- Create role efficiencies through the adoption of modern ways of working.

Who needs to be involved?

The most successful organizations prioritize cybersecurity investments to deliver business outcomes. 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 clear enterprisewide business outcomes and goals; quantifies benefits and risks, aligns teams and competencies, and drives innovation across the organization.

Head of AI ↗

Develops, champions and executes the organization’s technology 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 and Analytics Officer and Team ↗

Lead the organization’s technology optimization and architecture effectiveness 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 architectural effectiveness, optimization and architecture structure and design with organizational value by guiding use cases and requirements, governing architecture investments, leading adoption decisions and architecting business solutions.

Software Engineering Leader and Team ↗

Drive technology integration by clarifying business outcomes, establishing engineering best practices, transforming services with an outcome approach and architecting software development to support technology and capability objectives.

Client Story

Maximizing Security Efficiency and Business Alignment at Travelopia

Mission-critical priority

Travelopia sought support from Gartner as it aimed to enhance information and cybersecurity governance, risk management and compliance while delivering business value. The client worked with Gartner to gain actionable insights and guidance, leading to informed decision making and improved operational efficiencies.

**How Travelopia leveraged Gartner resources**

The information security director leveraged the CISO Effectiveness tool to identify strengths, weaknesses and growth opportunities. Additionally, board presentation templates helped the client align security initiatives with board priorities — a benefit especially valuable for someone new to the company.

**Mission accomplished**

The security director and Travelopia saved time and effort, allowing for informed decision making regarding license changes, ultimately avoiding unnecessary operational costs. Additionally, they were able to network with like-minded peers focused on business outcomes and alignment.

[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

