Gartner®

AI in Cybersecurity: Define Your Direction

Minimize disruption, manage risk and harness the value of AI.

Move past hype and maximize AI's value in cybersecurity

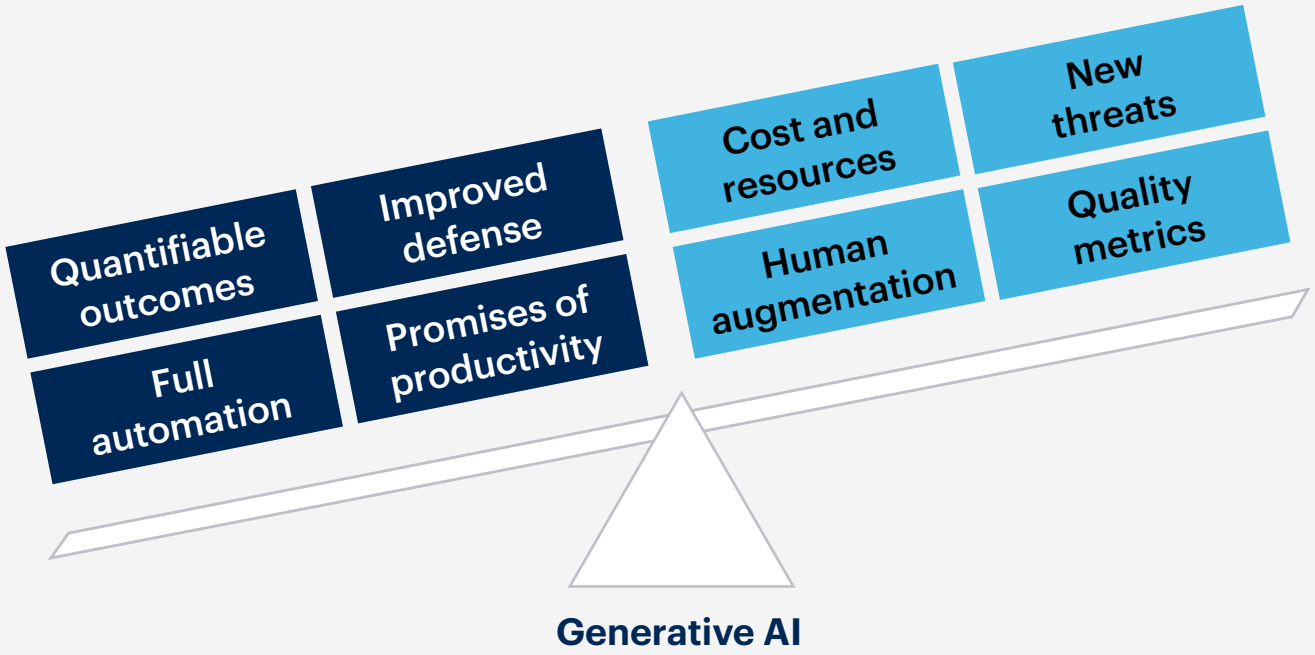
Hype around AI and generative AI (GenAI) in cybersecurity has disrupted business as usual. It's also adding new levels of risk and distraction to an already challenging security landscape. And despite the upheaval, AI hasn't yet fulfilled its promises.

Still, yesterday's disruption is tomorrow's opportunity. Beyond the hype lies real promise for harnessing AI's value.

AI can and will transform how organizations operate — including security. In the meantime, as the challenges of AI become more apparent and AI applications continue to mature, turn your focus toward:

- Rightsizing AI's impact
- Prioritizing key areas of risk
- Maximizing AI's value
- Anticipating future changes

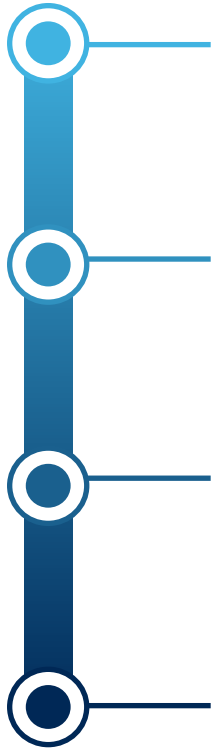
Balancing cybersecurity reality with GenAI hopes



Source: Gartner

Rightsize AI's impact

Our analysis reveals **nearly 90% of enterprises** are still researching or piloting GenAI, and most of those have yet to put AI TRiSM (trust, risk and security management) technical controls or policies in place — creating a wave of change for security. Leaders are feeling the effects in multiple ways:



Direct and urgent

- Unmanaged, uncontrolled use of confidential data in third-party applications
- Copyright infringement and associated brand damage

Direct and hyped as urgent

Early, exaggerated announcements designed to spark interest in GenAI

Indirect and scary

- Concerns about possible privacy risks and threat actors
- New attack surfaces emerging from disrupted business practices

Indirect and latent

- Ongoing GenAI adoption that requires ongoing security adaptation
- Upcoming regulations and compliance requirements requiring security team preparation
- Uncertainty on future skill gaps and talent challenges

Define your direction

Pivoting to GenAI will require new or modified governance principles, along with a well-defined cyber roadmap that integrates strong AI-focused considerations.

Your organization's scope of AI governance will depend on its maturity — but every organization can and should focus on the following three concurrent roadmaps:

1. **Adapt application security strategy to AI**
   Ensure you continue to implement secure development practices, while securing new attack surfaces at runtime and across the development cycle. Implement privacy-enhancing technologies and evaluate new GenAI techniques in application security.
2. **Integrate new AI technologies into cybersecurity**
   Factor the impact of today and tomorrow's AI into your three-year roadmap.
3. **Build AI considerations into risk management programs**
   Skill requirements will evolve. So will metrics, risk registers and exposure to threats.

Cybersecurity leaders' top 3 risk-related concerns about GenAI usage:

- Third-party access to sensitive data
- GenAI application and data breaches
- Erroneous decision making

Source: Gartner

Implement AI trust, risk and security management (AI TRiSM) solutions

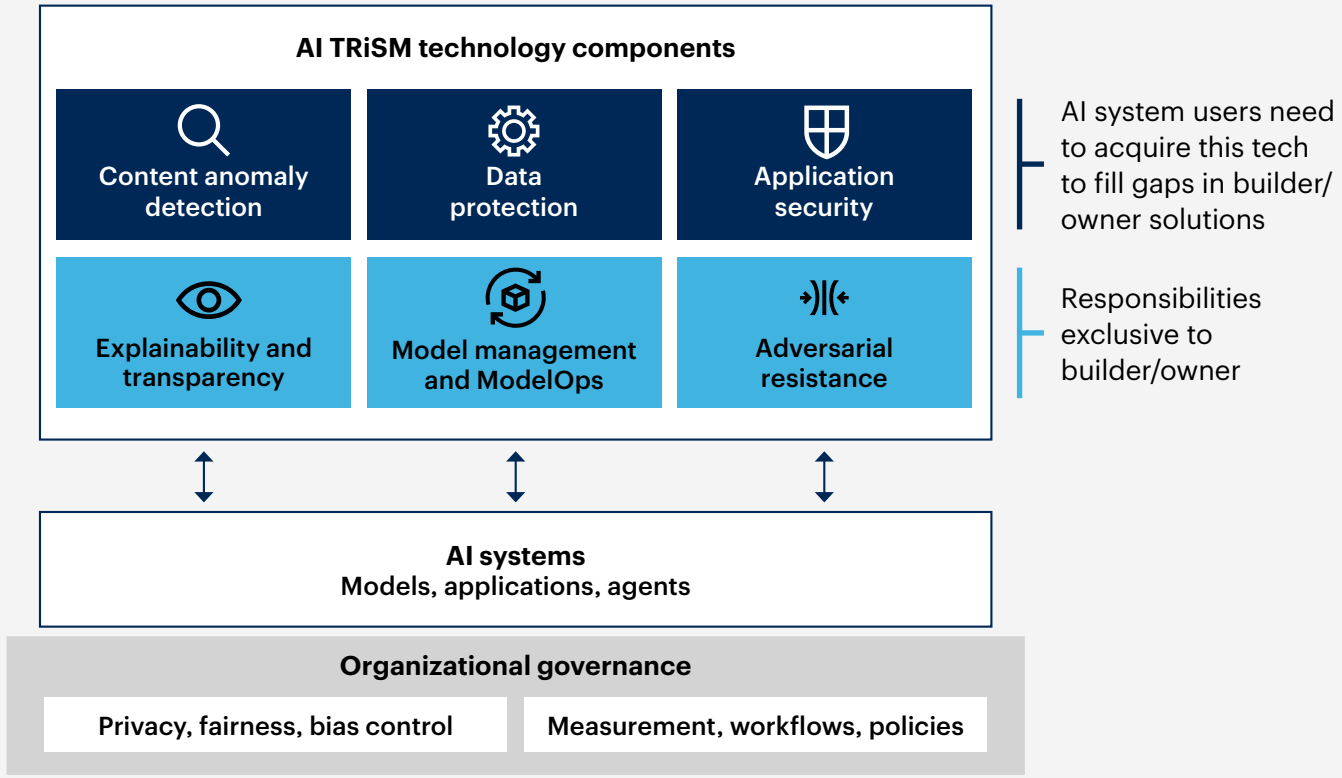
GenAI's risks intensify with the use of externally hosted large language models (LLMs) and other GenAI models that prevent enterprises from directly controlling their application processes, data handling and storage.

The risks also exist in on-premises models hosted and controlled by the enterprise, especially when security and risk controls are lacking.

Manage risk with AI trust, risk and security management (AI TRiSM) — a framework of controls and trust enablers that provide ongoing:

1. Content anomaly detection
2. Data governance and protection
3. Reduction of application security risks

AI trust, risk and security management technology



Source: Gartner

Prioritize securing GenAI applications

Ensure baseline security controls are in place for Web, SaaS, cloud infrastructure as a service (IaaS) and platform as a service (PaaS). Then take measures to secure GenAI applications.

Web and SaaS application consumption

- ☐ GenAI acceptable use policy (AUP)
- ☐ Checklist of security requirements to validate, approve and onboard SaaS applications
- ☐ Data security standard for how sensitive data needs to be protected in the public cloud
- ☐ Security service edge (SSE) product to secure web and SaaS usage

Cloud-hosted enterprise applications

- ☐ Security standard for how public cloud usage should be secured
- ☐ Cloud and web application security technologies
- ☐ Capabilities to secure custom-built applications
- ☐ Bot detection controls to ensure only humans use GenAI applications
- ☐ Capabilities to protect internal- or external-facing API endpoints

Focus on 3 key areas of risk

GenAI promises multiple benefits, including greater efficiency and productivity. It also introduces three new categories of risk.

Content anomaly detection

- Unacceptable or malicious use
- Hallucinations
- Inaccurate, illegal, copyright-infringing and other damaging outputs

Data protection

- Data leakage
- Compromised content and user data
- Privacy and data protection policy governance
- Privacy impact assessments
- Regional regulatory compliance

Application security

- Adversarial prompting attacks
- Vector database attacks
- Hacker access

Define your direction

AI TRiSM is a group effort; AI, security, compliance and operations should work together to implement new AI TRiSM measures. Get started with these actions:

- [ ] Set up an organizational task force or dedicated unit to manage your AI TRiSM efforts.
- [ ] Work across your organization to manage best-of-breed toolsets as part of a comprehensive AI TRiSM program.
- [ ] Define acceptable use policies. Establish systems to methodically record and approve user applications and document uses.
- [ ] Monitor usage continuously against stated objectives, and adjust usage parameters on an ongoing basis.

By 2026, enterprises that apply TRiSM controls to AI applications will consume at least **50% less** inaccurate or illegitimate information that leads to faulty decision making.

Source: Gartner

How CIOs can maximize GenAI's potential

GenAI promises to transform a wide range of security and business processes. Here's what CIOs should prioritize to maximize value:

- **Inventory, monitor and manage AI consumption** of third-party GenAI applications and features.
- **Update provider and technology selection requirements** to address privacy, copyright, traceability and explainability challenges.
- **Update AI application and data security practices** to integrate new attack surfaces.
- **Run proofs of concept before integrating GenAI into cybersecurity programs,** aiming to augment the work of humans, rather than replace them.
- **Monitor changes in the threat landscape** such as declines in detection accuracy and performance of existing security controls. Ensure you have access to the right intelligence on the changing threat landscape; scenario planning for future GenAI attacks is tricky and might not be the most profitable use of resources.

Through 2025, GenAI will cause a spike of cybersecurity resources required to secure it, causing **more than a 15% incremental spend on application and data security.**

Source: Gartner

How CISOs can maximize GenAI's potential

Here's what CISOs should prioritize to maximize value:

- **Evaluate these technologies like any other tools** to assess whether they create new risks with sensitive data.
- **Define what "good" looks like** to gauge how AI can improve existing security metrics without creating new ones.
- **Run experiments with new features** from existing security providers, starting with targeted and narrow use cases in the security operation and application security areas.
- **Apply the AI TRiSM framework** when developing new first-party, or consuming new third-party, applications leveraging large language models (LLMs) and GenAI.
- **Prepare and train your teams** for dealing with direct (privacy, IP, AI application security) and indirect (other teams using GenAI, such as HR, finance or procurement) effects stemming from GenAI uses across the enterprise.

By 2028, the adoption of generative augments will collapse the skills gap, **removing the need for specialized education from 50% of entry-level cybersecurity positions.**

Source: Gartner

Define your direction

Your next steps:

- ☐ **Evaluate** AI technologies and decide what "good" looks like for your organization.
- ☐ **Maintain and refine** good detection and response capabilities against uncertain and ambiguous threats.
- ☐ **Invest** in exposure management and threat intelligence to identify the most relevant threats.

One-third (34%) of organizations plan to deploy GenAI in the next 12 months.

Source: Gartner

Critical leadership roles to successfully set a strategy and implementation plan for AI

CIO/Head of Technology

CIOs are looked to by their CEO, peers and the board to develop a formal AI strategy (and/or name an AI lead) and successfully:

- Set an AI ambition for the whole enterprise and identify use cases and quantify benefits and risks
- Align business and technology teams and change organizational competencies to support AI
- Name an AI lead to orchestrate ideas and promote innovation

CISO/Security Leader + Team

Cybersecurity leaders must ensure that cybersecurity and data privacy are an integral part of AI strategy and successfully:

- Provide overall program oversight on security and risk
- Anticipate and take actions against unforeseen consequences such as data breaches or copyright violations
- Continuously update skills and readiness against new threats

CDAO/Data & Analytics Leader + Team

D&A leaders are expected to lead their organizations in setting the data for AI strategy and must successfully:

- Identify AI use cases for augmented analytics and data management
- Leverage existing D&A practices and establish D&A governance policies for AI
- Develop new sources of value from data leveraging AI
- Be AI-data ready

Enterprise Architecture Leader + Team

EA leaders are expected to drive tangible business value from AI and must successfully:

- Own the full AI infrastructure roadmap
- Govern AI technology architecture investment decisions
- Lead decision making about adopting AI solutions to drive business outcomes

Software Engineering Leader + Team

Software engineering leaders must understand the implications of AI technology in depth and successfully:

- Clarify the desired business outcomes for AI integration
- Establish AI engineering best practices across the organization
- Transform products, services and experiences and build an AI-first approach into roadmaps

Our research revealed several insights on how to **enable each role to take effective action toward valuable AI outcomes.**

	1 Establish an AI ambition that aligns to business goals	2 Select use cases and deploy tests	3 Incorporate AI into technology and business operations
CIO/Head of Technology	**Judiciously choose where to focus AI efforts** following Gartner best practices to select the highest-impact business metrics	**Align the business on pilots** based on potential business value and feasibility, looking for disruption potential while enabling strategic objectives	**Lead AI adoption for the enterprise** by making it an innovation practice with dedicated leadership, allocated resources and funding, guardrails, and governance
CISO/Security Leader + Team	**Stay ahead of sophisticated attackers** using AI behavior models to improve threat detection capabilities	**Identify the best use cases for AI** based on feasibility and risk reduction using Gartner's AI Prism for Cybersecurity	**More effectively manage AI risk** with teams working on AI projects evaluating cybersecurity considerations at each stage of development
CDAO/Data & Analytics Leader + Team	**Drive alignment** by quantifying expected value of AI to a specific KPI and establishing leading and lagging metrics to monitor	**More effectively prioritize use cases** by selecting business value dimensions, refining use cases, and driving engagement and decisions	**Efficiently drive AI delivery** by augmenting cross-functional teams with data experts, using the most appropriate techniques and keeping technical debt low
Enterprise Architecture Leader + Team	**Create an effective AI ecosystem** by identifying areas for deeper investigation and developing AI plans and strategies	**More strategically plan AI initiatives** using Gartner's four-step capability modeling approach for an optimal AI infrastructure	**Deliver target business outcomes and avoid failures** by following Gartner's five-phase approach to AI execution
Software Engineering Leader + Team	**Deliver world-class application development operations** by adopting AI-augmented software engineering practices	**Maximize the value of AI** by identifying areas of software testing where AI will be most applicable and impactful, such as in visual testing	**Generate breakthrough ideas** by combining human experts with generative AI to improve exploration and understanding of the solution space

Actionable, objective insight

Explore these additional complimentary resources and tools:

Insights
Cybersecurity Trends: Optimize for Resilience and Performance
See how top trends reflect the need for more agile and responsive programs.

Insights
Build a Resilient Cybersecurity Roadmap for Your Enterprise
Keep your team focused on projects that support business goals and address risks.

Tool
Gartner Cybersecurity Business Value Benchmark
Explore new standardized measures to benchmark vs. peers, mitigate risk and meet business objectives.

Webinar
Navigate Evolving Risks & Security Challenges in Enterprise AI Systems
Learn how to secure AI and implement required measures to prevent AI failures.

Access other AI insights from Gartner:

Building a Value-Driving AI Strategy for Your Business

Get AI Ready — What IT Leaders Need to Know and Do

AI-Ready Data Essentials

Cybersecurity and AI: Enabling Security While Managing Risk

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

Gartner

Advance your AI strategy by attending a Gartner conference

Join your peers to share valuable insights on how to communicate AI's opportunities and risks; strategize, pilot and scale; and manage AI's impact on enterprise software, talent and skills, risk, trust, and governance.

Don't miss out.

View the conference calendar today and find the conference that's right for you.

→ **View Security & Risk Conferences**

→ **View CIO & IT Executive Conferences**

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for Cybersecurity Leaders
gartner.com/en/cybersecurity

Stay connected to the latest insight

Attend a Gartner conference
View Conferences

Gartner®