Gartner

Top Cybersecurity Trends Heading Into 2027

1 CISOs expand software supply chain security to manage AI-augmented threats

2 Quantum decryption threats advance as organizations lag

Secure new frontiers

3 IAM adapts to secure and enable AI agents

4 Agentic AI demands program oversight

Transform governance

5 AI and cyber resilience redefine the CISO's remit

6 Technical debt undermines AI ambitions

Normalize AI adoption

7 AI breaks traditional cybersecurity awareness tactics

8 AI-driven solutions destabilize SOC norms

9 Frontier AI models transform vulnerability management

Secure new frontiers

1 CISOs expand software supply chain security to manage AI-augmented threats

59% of CISOs rank third-party and supply chain attacks among their top 5 threats for the next 12 months. The urgency: Business demand for faster AI system builds is pushing organizations to rely on open-weight and frontier models — plus the third-party components embedding them — without verifying their security posture.

2 Quantum decryption threat advances as organizations lag

Quantum computing will make conventional asymmetric cryptography unsafe by 2029–2030. With remediation requiring multiyear efforts, cybersecurity leaders must evaluate and adopt postquantum cryptography (PQC) solutions now.

3 IAM adapts to secure and enable AI agents

Machine identities are multiplying at an unprecedented rate — 94% of organizations report rising volumes, driven primarily by AI/ML adoption (52%) and autonomous agents (35%). These nonhuman actors are now a major adversary target. 58% of organizations have experienced incidents where AI-linked machine identities were compromised, causing moderate-to-significant business disruption (42%), financial loss (36%) and reputational damage (32%).

Transform governance

4 Agentic AI demands program oversight

CISOs can't slow AI initiatives as CEOs and CIOs push aggressive adoption to stay competitive. The pressure to buy AI agents and the ease of "vibe-coding" tools are too high to resist — yet only 16% of organizations have enforced workflows governing employees' use of third-party AI apps. The result: unmonitored "rogue automation" operating with excessive privilege.

5 AI and cyber resilience redefine the CISO's scope

Two disruptors are expanding CISO responsibilities: the shift from cyberprotection to cyber resilience and the urgent need to adopt and secure AI. The expanded scope often includes data governance, AI governance, privacy and business continuity — but for most CISOs, this shouldn't imply direct ownership of these domains.

6 Technical debt undermines organizational AI ambitions

49% of cybersecurity leaders cite technical debt as a major barrier to their top priorities. Executive pressure to deploy AI forces reliance on unstructured data repositories lacking adequate security governance and AI-ready controls — leading to data oversharing and unauthorized access.

Normalize AI adoption

7 AI breaks traditional cybersecurity awareness tactics

Existing security awareness efforts have failed to reduce risk exposure amid AI adoption. 60% of data breaches involve the human element, while 86% of organizations report having standalone, public SaaS GenAI apps in limited or broad production.

8 AI-driven solutions destabilize SOC norms

AI-driven security operations centers (SOCs) are creating uncertainty, fueled by cost mandates and overhyped promises. CISOs face a destabilized environment — staffing challenges, retraining pressures and uncertain AI tool costs — as leaders attempt to augment alert triage and investigation.

9 Frontier AI models transform vulnerability management

Traditional volume-driven vulnerability management was already misaligned with attacker timelines. Frontier AI has now created an unprecedented supply-side shock: As vendors and open-source projects use AI to uncover latent flaws, organizations face a heightened volume and frequency of urgent security updates.

Disclaimer: Trends are not ranked in order of importance.

Actionable, objective insights

Position your organization for success. Explore these additional complimentary resources and tools for cybersecurity leaders:

Conferences

Cybersecurity Conferences and Events

Join Gartner analysts and your peers to discuss the latest cybersecurity developments.

View Calendar ↗

Report

The Cybersecurity Executive Outlook

Benchmarks and insights to help you see around corners and guide your C-suite and board. Make decisions for the next quarter.

Download Now ↗

Insights

Cybersecurity and AI: Enabling Security While Managing Risk

AI's hype and promise in cybersecurity is offset by trepidation and risk. Here's where to focus.

Learn More ↗

Webinars

Explore Webinars Aligned to Your Priorities

Join Gartner analysts for live briefings or watch on demand.

Watch Now ↗

Become a Client

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

Learn more about Gartner for Cybersecurity Leaders ↗

Source: Gartner
© 2026 Gartner, Inc. and/or its affiliates. All rights reserved. CM_GTS_ 5333150

Gartner