

2025

Executive Summary

A message from the Conference Chair

Do you feel empowered to thrive in today’s environment and amplify the importance of IAM in your organization? We look forward to working with you as you enhance your cybersecurity posture and help your organization achieve its business objectives, and hope to see you at Gartner Identity & Access Management Summit 2026.

Sincerely,

Paul Rabinovich

Conference Chair and VP Analyst, Gartner

Top takeaways

- 1

Align your IAM program with the strategic objectives of your organization

Prioritize systems thinking as the guiding principle in your approach to IAM. Think about how introducing this tool or implementing that process helps you increase business agility and minimize loss and disruption. Improve business and security outcomes by developing a formal identity strategy, assigning owners to specific IAM functions, building bridges between IAM and security teams, and clearly communicating the business value of IAM to your C-Suite.

“IAM leaders can capture this strategic opportunity not merely to contribute, but truly to drive value for the business, for security, and for the organization as a whole.”

Zachary Smith,
Sr Principal, Research,
Gartner
- 2

Harness IAM to advance your zero-trust strategy

Align your zero-trust (ZT) and identity strategies. Make sure that the foundational IAM components such as identity lifecycle management, machine identity management, multifactor authentication, and privileged access management are in place before tackling-zero trust. Mature your identity, device, and application management to drive automation of zero-trust policies, a must-have for scaling your ZT implementation.

“Zero-trust is not about removing trust in people - it is about extending the right controls to the right people at the right time.”

Nathan Harris,
Sr Director Analyst,
Gartner
- 3

Move towards managed machine identity

Establish a long-term machine IAM initiative paying particular attention to workload identity, a significant source of risk for most organizations. Start by implementing basic capabilities such as broad discovery across multiple machine identity types on-premises and in the cloud. As no one vendor does it all, plan on pursuing a best of breed strategy focusing on managing secrets, certificates, SSH keys, workload identities, and runtime access by workloads.

“Machine IAM needs and constraints are different from human IAM. Establish a distinct machine IAM practice to address them.”

Erik Wahlstrom,
VP Analyst,
Gartner
- 4

Protect your systems against identity-based attacks

Establish identity posture management and identity threat detection and response (ITDR) practices to mitigate risk in an increasingly complex threat environment. Treat ITDR as a security discipline supported by, and providing value to, the IAM team. Focus on preventative measures such as detection, identity hygiene, and posture management.

“Ensure you balance your investment between prevention and detection, as these are well-served in the market today.”


Felix Gaehtgens,
VP Analyst,
Gartner
- 5

Navigate the generative AI disruption

Identify practical use cases where generative AI (GenAI) can be used to help IAM, such as audit and configuration. Implement a proof of concept and measure efficiency gains. To mitigate risks inherent in GenAI applications and assistants, implement retrieval-augmented generation (RAG) and augment prompts with properly entitled contextual data and identity guardrails. Monitor developments related to GenAI-amplified security risks such as deepfakes and enhanced phishing techniques.

“GenAI and IAM are driving forces to amplify business operations.”

Homan Farahmand,
VP Analyst,
Gartner



Save the date!

Join us 9 - 10 March 2026 in London for [Gartner Identity & Access Management Summit](#).