Gartner Identity & Access Management Summit

December 8 – 10, 2025

Gartner

2025 Executive Summary

Thank you, from the Conference Chair

We hope you feel empowered to thrive in this environment and recognize *identity at the core*, where IAM drives business resilience and enables secure interactions among people, machines, and organizations.

As the demands of your role continue to evolve, embrace the guidance you uncover to build scalable and efficient IAM infrastructures in today's complex environment.

We hope to see you at Gartner Identity & Access Management Summit 2026.

Sincerely,
Homan Farahmand
Conference Chair and VP Analyst, Gartner

Top takeaways

1 Implement IAM as the business control plane to enable resilient and secure digital services

IAM is essential to modern business, yet its value is often unrecognized due to budget limitations, communication issues, and insufficient decision-making authority for IAM teams. To change this perception, you should use outcome-driven metrics, storytelling, and clear strategy communication to advocate for greater recognition and decision rights.

"The apple does not exist without the core. Business does not exist without identity."

Michael Kelley,
Sr Director Analyst,
Gartner

2 Build organizational trust, orchestrate change, and raise awareness

Lead IAM transformation by building organizational trust, orchestrating change, and raising awareness as an active instigator and facilitator. Practice "unasking" to challenge assumptions, and focus on delivering a steady, foundational IAM product that generates business value through applied insight.

"Great managers are brilliant at answering the questions they are asked. Great leaders are brilliant at unasking the question."

Rebecca Archambault,
Sr Director Analyst,
Gartner

3 Adopt Gartner's identity fabric principles and taxonomy for IAM to evolve your deployment

Begin with focused use cases and IAM controls rather than attempting to tackle everything at once. Regularly validate your architecture, share identity data to provide better context between security and identity tools, and utilize zero-trust and cloud migration initiatives to secure additional resources.

"Zero-trust journeys require an *identity-first security* approach, and it must be powered by a *radically* modernized IAM infrastructure."

Erik Wahlstrom,
VP Analyst,
Gartner

4 Prioritize IAM for AI agents using current capabilities to meet immediate business needs

Extend IAM controls to AI agents by implementing workload identities, dynamic authentication, and fine-grained, context-aware authorization. Ensure robust governance, visibility, and secure multiagent collaboration while leveraging existing IAM protocols and maintaining human oversight as the central point.

"Proceed with caution! Tool calling and inter-agent calling protocols drive consistency and interoperability. However, they need to be matured and battle-tested, at the internet scale."

Homan Farahmand,
VP Analyst,
Gartner

5 Plan for centralized and complete identity and access visibility across all relevant environments

Implement a hybrid data architecture to address the requirements of identity visibility and intelligence (IVIP). Assess your analytics and AI capabilities to optimize their placement within your Identity Fabric, fully leverage existing IAM visibility and data management tools before adding new ones, and carefully evaluate IVIP solutions to ensure alignment with your business and security goals.

"Ultimately, the best data architecture for your identity fabric is a data fabric."

Nathan Harris,
Sr Director Analyst,
Gartner

6 Expand your authorization strategy

Cover commercial applications, infrastructure, and data platforms for improved agility and security. Prioritize and implement AMP use cases incrementally, starting with those that are most feasible and impactful. Adopt standards like AuthZEN to reduce vendor lock-in and enhance interoperability. Focus on strong policy lifecycle management and data integration to support accurate and effective authorization policies.

"AMPs can cover a larger number of applications and systems by including policy orchestration, increasing security, and reducing the risk of unauthorized access."

Paul Mezzera,
Sr Director Analyst,
Gartner

7 Evaluate and modernize your strategic access management tool

Incorporate third-party integrations as needed for covering legacy and nonstandard applications. Strengthen adaptive access policies and assess both built-in and third-party ITDR capabilities. Integrate detection, response, and posture management, and regularly review the resilience provided out-of-the-box by your access management solution to ensure it meets your needs.

"Access management is well understood and largely commodified. It doesn't mean it can't be improved."

Paul Rabinovich,
VP Analyst,
Gartner

8 Integrate ITDR into your IAM strategy and roadmap

Inventory current ITDR and observability tools and use NIST CSF 2.0 to identify gaps. Leverage existing solutions, clarify alert sources, and collaborate with leadership to optimize response processes. Ensure ITDR alerting and response are coordinated with broader cybersecurity efforts, extend ITDR practices beyond core identity systems, and foster a culture of continuous improvement.

"Identity threat detection and response is a *discipline* that protects the core identity infrastructure."

Mary Ruddy,
Distinguished VP Analyst,
Gartner

9 Adopt a "buy then build" strategy for CIAM tool selection

Evaluate options against the needs of each user group. Deploy CIAM in phases—starting with a robust platform, piloting with SSO and MFA, then adding usability features and scaling for compliance and personalization. Develop a flexible, long-term CIAM strategy that evolves in line with market trends to efficiently reach your maturity goals.

"CIAM is an orchestrator of various customer journey-time functions. Adopt a buy, build, and integrate approach for successful CIAM deployments."

Abhyuday Data,
Director Analyst,
Gartner

10 Reduce the risk of IAM technical debt by choosing interoperable tools

Prioritize resolving technical debt to boost IAM team agility, modernize IAM infrastructure with standards-based architecture, increase visibility through continuous identity discovery and observability, and improve IAM adoption by simplifying and making controls more flexible.

"IAM Architects should incrementally reduce technical debt to improve security, compliance, and operating efficiency."

Nat Krishnan,
Sr Director Analyst,
Gartner

Save the date!

Join us December 7 - 9, 2026 in Las Vegas, NV for Gartner Identity & Access Management Summit!

#GartnerIAM

Gartner