Identity Trends for 2026 & Beyond

Six trends shaping the future of identity and access management—jointly published by Ping Identity and Deloitte to help you future-ready your strategy in today's trust-nothing era.

Last Updated: November 1, 2025 7 min read

Table of Contents

The Future of Identity

How people interact with brands online has been upended due to advancements in artificial intelligence (AI), new fraud threats, and skyrocketing consumer expectations. It's become increasingly difficult for organizations to distinguish bad actors from legitimate users, and at the same time, people globally are losing confidence in organizations to protect their data.

Trust is eroding, and identity has become the foundation of security, experience, and verification.

Looking ahead to 2026, we've worked with Deloitte to come up with our top six trends on where identity and access management (IAM) is heading, and how organizations can future ready their identity strategies to build and maintain trust in today's "trust nothing" era.



> As agentic AI rapidly evolves, building trust with transparency, security, and user autonomy is essential. Organizations that adapt will detect threats faster, stay resilient, and drive lasting innovation in an era defined by verified trust.
>
> **Vikram Kunchala, Principal, Digital Trust & Privacy Leader**
> Deloitte

Global Trust Survey Findings

17%

of consumers trust the organizations managing their identity data

75%

of people globally are more concerned about their data security than five years ago

23%

worldwide are confident in their ability to spot a scam[1]

Trend 1: Managing AI Agents

AI Agents Will Break Outdated IAM

Agentic AI has evolved from experimentation to enterprise integration. Autonomous software entities now handle complex decision-making, execute workflows, and interact with APIs and applications on behalf of users and systems. From digital workers and API-driven assistants to Computer Using Agents (CUAs), these agents are driving measurable productivity and automation gains across industries.

The challenge ahead centers on trust, specifically, how organizations securely distinguish, authenticate, authorize, and govern these agents without resorting to brittle credential sharing or ineffective bot detection. Traditional IAM frameworks are buckling under the scale and unpredictability of agent behavior, pushing enterprises toward AI-aware identity systems that support authenticated delegation, dynamic entitlements, and human-in-the-loop oversight.

This evolution will be essential as agentic commerce emerges—a paradigm where personal AI agents independently shop, decide, and transact on behalf of consumers across channels. Identity systems will need to adapt to recognize and verify agents, enforce delegated authority, and sustain trust throughout agent-driven transactions. The next

frontier of identity management will likely be defined by how seamlessly organizations can manage trust between humans and autonomous entities.

> The rise of AI agents will continue to disrupt traditional e-commerce. This new channel will make consumers' lives easier by eliminating the friction of working across organizations and multiple channels to complete customer journeys, like brainstorming a trip, booking that trip, traveling, and then returning and remembering that trip.
>
> **Darryl Jones, VP of Consumer Product Strategy**
> Ping Identity

Ping Perspective

Integration Will Matter More Than Adoption

The value of agentic AI will be realized through deep integration with existing identity systems, not simply deploying new agents.

Identity Accountability Will Expand

As agents act on behalf of users and systems, organizations must extend identity accountability to every autonomous action taken.

Agent Identity Will Become Standard

Establishing verified, governable identities for AI agents will become a baseline expectation across enterprise IAM programs.

$42.5B

projected Agentic AI Market size by 2030, up from $5.1B in 2024—essentially doubling every two years.[2]

Trend 2: Securing Helpdesks

Helpdesks Could Be the New Top Target

Organized criminal groups now use fraudulent hires, insider recruitment, and AI-generated deepfakes to infiltrate organizations. These are low-tech, high-impact tactics that exploit people and processes, not passwords or code.

The helpdesk is an ideal entry point for social-engineering attacks against enterprise identity systems. As defenses around multi-factor authentication (MFA), single sign-on (SSO), and perimeter controls strengthen, attackers are shifting toward the human layer, exploiting helpdesk agents through convincing social engineering, AI-generated voice deepfakes, and urgency-driven manipulation. Breaches across industries, from hospitality to finance, increasingly trace back to compromised support interactions where attackers tricked agents into resetting credentials or disabling MFA.

Several factors amplify this risk: outsourced or remote staff may lack personal familiarity with end users, performance metrics prioritize speed over verification, and the high-pressure nature of support work leaves agents vulnerable to manipulation. Training can't close this gap; automated verification can.

In response, helpdesks should evolve into identity-aware security hubs. Real-time risk assessment and mandatory verification before account or device recovery will become standard. The organizations that reimagine the helpdesk as a proactive trust checkpoint, rather than a reactive support function, will help close one of the most exploited gaps in enterprise identity.

Ping Perspective

Redefine the Helpdesk as a Security Control

Treat every helpdesk interaction as a potential attack vector and embed identity verification into every support workflow.

Eliminate Password Dependencies

Removing passwords from recovery and verification workflows closes a key exploitation path used by social engineers.

Reset the Trust Baseline

Proactive re-onboarding and re-verification ensures identity records remain current and trustworthy across the enterprise.

3rd

largest GDP in the world—if cybercrime were a country, according to the World Economic Forum.[3]

Trend 3: Preventing Hiring Fraud

Hiring Fraud Will Continue to Be a Top Concern

AI has lowered the barrier to entry—anyone with bad intent and access to generative tools can fabricate convincing identities. The result: a surge in applicants using deepfakes to misrepresent themselves in your hiring process.

Bait-and-switch hiring, where the person who starts the job is not the one who interviewed, has become a prevalent tactic, often powered by AI-generated résumés, deepfake video interviews, and falsified credentials. These schemes thrive in large, fast-moving organizations that depend on remote and contract workforces, where traditional verification methods and static background checks fail to detect deception.

The underlying conditions are accelerating: the globalization of the workforce, compressed hiring cycles, and dependence on third-party platforms for sourcing and onboarding can weaken trust signals during recruitment. At the same time, adversaries are combining synthetic identities, fraudulent documentation, and compromised insiders to gain privileged access. This has created a new class of insider threat—one that passes surface-level checks and embeds itself before any anomalies appear.

Organizations that fail to evolve their hiring and verification practices could find their workforce perimeter increasingly porous and exploitable.

Ping Perspective

✓ Make Identity the Foundation of Hiring

Embed high-assurance identity verification at every stage of hiring and onboarding to prevent fraudulent applicants from entering the workforce.

Adopt High-Assurance Onboarding Workflows

Static background checks are no longer sufficient—continuous, multi-layered verification must underpin every onboarding process.

Issue Verifiable Digital Credentials

Reusable, tamper-resistant digital credentials reduce reliance on unverified documentation and strengthen workforce identity integrity.

220%

increase in IT worker hiring fraud incidents over the past year.[4]

Trend 4: User Autonomy & Decentralized Identity

User Autonomy Will Accelerate Decentralized Identity Adoption

The enterprise-centric identity model—where user data is siloed, duplicated, and controlled internally—is collapsing under its own weight. Consumers now expect ownership of their personal data, and regulators are enforcing that expectation through frameworks such as GDPR, CCPA, and emerging AI governance standards. Movements like open banking are accelerating demands for data portability and interoperability across sectors. Yet, most organizations still operate with fragmented identity records scattered across applications, regions, and third-party platforms.

This lack of integration creates unnecessary friction, inflates risk, and complicates compliance. Legacy architectures have become single points of failure and high-value targets for attackers. At the same time, trust is eroding: outdated identity records persist across disconnected systems, and individuals lack transparency into how their data is stored, shared, or monetized.

As the balance of control shifts toward the individual, enterprises should embrace decentralized, consent-based identity ecosystems. These systems will empower users to manage and verify their data directly while allowing

organizations to deliver secure, personalized experiences that comply with evolving global mandates. And as users delegate more tasks to AI agents, the same consent-driven principles will ensure those agents act only with verified intent.

Ping Perspective

Adopt Decentralized Identity to Reduce Risk

Shifting to user-controlled, decentralized identity ecosystems reduces the attack surface created by centralized data silos.

Prioritize Interoperability

Interoperable identity architectures improve security, compliance, and user experience across fragmented digital environments.

Build Trust Through Standards and Consent

Consent-driven frameworks ensure users and their AI agents act with verified intent, reinforcing trust at every interaction.

75+

countries have established some form of open banking regulatory framework.[5]

Trend 5: Quantum Computing

Quantum Computing Shifts From Concept to Capability

Quantum computing is moving from theoretical to tangible, challenging organizations to confront vulnerabilities in the cryptographic foundations of their identity systems. Advances in quantum processors and algorithms are shortening the timeline for breaking conventional encryption methods, threatening the integrity of long-trusted public key infrastructures and digital certificates.

This same computing power will also amplify AI's capabilities, accelerating analysis, automation, and simulation far beyond current limits. Enterprises that harness it will gain unprecedented efficiency, but malicious actors will leverage it too, finding new ways to breach and exploit organizations lacking resilient identity architectures.

Even if large-scale quantum attacks remain years away, the data being protected today, especially identity records and authentication keys, must withstand future decryption. Forward-looking enterprises are beginning to adopt quantum-resistant cryptography, modernize signing mechanisms, and inventory legacy algorithms. The transition will be gradual but essential; those who start early can maintain trust when quantum computing crosses from lab environment to operational reality.

Ping Perspective

Prepare for Quantum-Era Security Threats

Begin auditing cryptographic dependencies now to identify exposure to quantum-capable decryption before it becomes a crisis.

Anticipate Both Innovation and Exploitation

Quantum will accelerate both legitimate enterprise capabilities and adversarial attack sophistication—preparedness must account for both.

Act Now to Build Resilience

Adopting quantum-resistant cryptography and modernizing signing mechanisms today ensures identity systems remain trustworthy tomorrow.

100+

operational quantum computing systems expected worldwide by 2026.[6]

Trend 6: Verification & Zero Trust

Continuous Assurance Across Every Interaction

The strain on identity systems will likely intensify as enterprises expand across hybrid clouds, outsourced operations, and interconnected supply chains. The attack surface will grow, while long-standing weak points, like recovery workflows, onboarding processes, and access renewal, could be further undermined by AI-driven manipulation. With more users, vendors, and agents sharing systems and data, every assumed trust relationship may become a potential breach path.

Verified Trust is the journey from implicit to explicit to continuous trust—uniting identification, verification, authentication, and authorization in a single automated assurance loop. Verification can no longer function as a single checkpoint—it must evolve into a continuous control mechanism that validates every access request, credential reset, and privilege escalation with real-time assurance. The concept of verified trust will gain prominence as enterprises face tighter regulations, heightened audit expectations, and escalating costs from insider and social engineering attacks.

Organizations that operationalize verification, embedding it into workflows, automating enforcement, and measuring trust as a core performance metric will define the next stage of security maturity. In the years ahead, success will be measured by how confidently an enterprise can prove and manage who is accessing what, under what authority, and why.

Ping Perspective

Expect Mounting Pressure on Identity Systems

Expanding ecosystems, more agents, and deeper interconnections will continue to stress legacy identity architectures and expose new gaps.

Evolve Verification Into a Continuous Control

Every access request, credential reset, and privilege escalation must be validated in real time—not assumed at login.

Redefine Security Maturity Through Assurance

Organizations that measure and prove verified trust as a performance metric will define the next standard for enterprise security maturity.

50% faster

threat detection and response when organizations implement continuous verification.[7]

> In 2026, identity will become the universal language of accountability. Every action will need to show proof: who or what did it, under what policy, and with whose consent. Trust won't hinge on claims; it will hinge on proof. The organizations that can verify both identity and intent will define the new standard for digital trust.
>
> **Andre Durand, Founder & CEO**
> Ping Identity

Conclusion: It Starts & Ends With Identity

As new technologies, more sophisticated threats, and skyrocketing user experience expectations continue to fundamentally change how digital identities and access are managed, one thing remains the same: the organizations that can stay ahead of the trends have a significant opportunity to differentiate themselves in the market.

The ability to distinguish between legitimate users and bad actors and managing AI agents, while delivering seamless experiences, will set organizations up for success in 2026 and well into the future.

2026 Trends Summary

Managing AI Agents

IAM must account for the large increase in AI agents and be able to manage them as general users.

Securing Helpdesks

As the new primary attack vector for bad actors trying to infiltrate organizations, helpdesks should be a key focus for security teams.

Preventing Hiring Fraud

Make identity central to hiring and onboarding through high-assurance verification and reusable, verifiable digital credentials.

User Autonomy & Decentralized Identity

Adopt decentralized identity ecosystems that give users control over their data while improving compliance and trust.

Quantum Computing

Prepare for the quantum era by adopting quantum-resistant encryption and modernized signing mechanisms.

Verified Trust

Rising complexity and expanded ecosystems will demand continuous verification, automated assurance, and proof-based access to define security maturity.

[1]Ping Identity, Bridging the Trust Gap in the Age of AI

[2]Mordor Intelligence, Agentic AI Market Size and Share

[3]World Economic Forum, How AI-driven fraud challenges the global economy – and ways to combat it

[4]Fortune, North Korean IT worker infiltrations exploded 220% over the past 12 months, with gen AI weaponized at every stage of the hiring process

[5]CoinLaw, Open Banking Adoption Statistics 2025: Adoption, Innovation & Growth

[6]SpinQ, The Surprising Global Footprint of Quantum Computers in 2025

[7]CrowdStrike, Zero Trust Security Explained: Principles of the Zero Trust Model