

SECURITY ALERT:

USING IAM TO SAFEGUARD YOUR ORGANIZATION'S DATA

(2026 UPDATE)

A three-year retrospective and strategic forecast



Contents

Introduction	2
When, not if: The acceleration of continuous compromise	3
Identity: From infrastructure foundation to the enterprise operating system	4
The identity of things: Resolving the nonhuman identity crisis	5
The 2026 regulatory landscape: Managing global data sovereignty	6
Architecting the identity fabric beyond fragmented toolsets	7
Four critical IAM trends defining 2026	8
Final thoughts: Moving from identity debt to identity resilience	9



Introduction

The importance of [identity and access management \(IAM\)](#) has surged in recent years, as it has become a focal point of successful business operations. Just three years ago, we analyzed the state of IAM in the middle market, with a close look at the specific risks and strategies companies needed to monitor to implement an effective security stance.

IAM processes require constant attention and continuous oversight to stay ahead of persistent and accelerating threats. Therefore, our team has brought updated insights and strategic advice together in this guide, giving you the keys to developing a proactive, compliant IAM program that better controls who has access to your sensitive data.



2. When, not if: The acceleration of continuous compromise

In the 2023 RSM Middle Market Business Index Cybersecurity Special Report, we highlighted a stark reality: breaches are a given. At that time, our research found that ransomware attacks had risen from 23% to 35% in a single year, and the concept of “identity as the perimeter” was just beginning to take root in the middle market. Now, [the latest RSM Attack Vectors Report](#) confirms that this reality has shifted into a state of continuous compromise, driven by an unprecedented acceleration in attacker speed.

The differentiator now is the industrialization of artificial intelligence-powered attacks. Cybercriminals no longer spend weeks on manual reconnaissance; they use large language model (LLM)-enabled scripting to automate exploitation chaining and credential harvesting. This has shortened the window between initial access and full-scale data theft from days to minutes.

The 2023 versus 2026 identity landscape

- **Perceived risk:** Executive concern regarding identity-based threats is surging. This is no longer about simple malware; it is about impersonation. Attacker tactics now include real-time voice and video cloning to impersonate leadership during live virtual calls and browser-in-the-browser (BitB) attacks that capture credentials with near-perfect accuracy.
 - **The breach connection:** The RSM Attack Vectors Report revealed that identity-related weaknesses provided reliable access in 82% of offensive engagements in 2025.
- Attackers no longer target just human passwords; they target the machine-to-machine (M2M) secrets, application programming interface (API) keys and OAuth authorization tokens that power automated cloud pipelines.
- **The reaction gap:** Most security programs designed for a slower threat tempo are struggling. The reaction gap is the time between an AI-driven exploit (seconds) and a human-led response (hours). Bridging this requires defenders to move toward automated, AI-assisted response capabilities.

3. Identity: From infrastructure foundation to the enterprise operating system

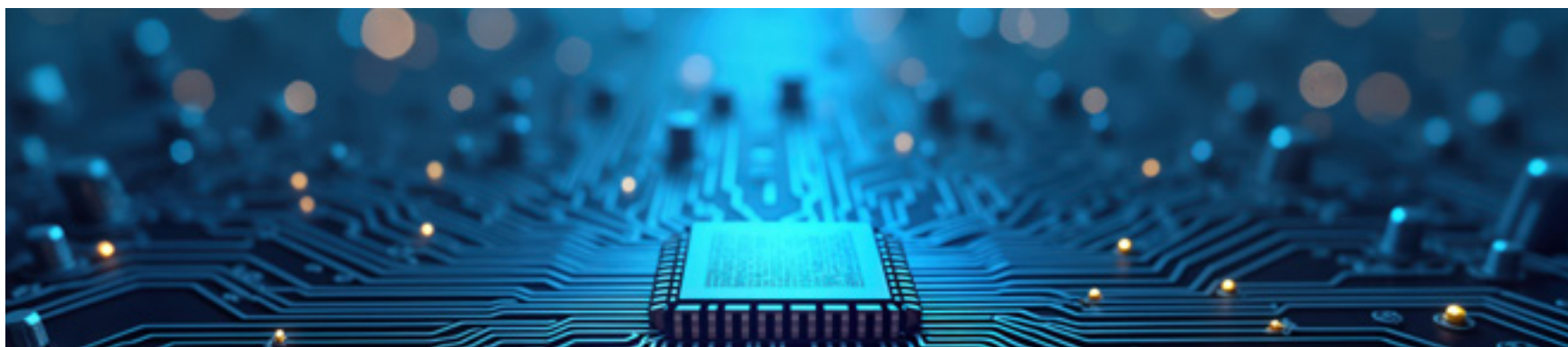
In 2023, we described IAM as the foundation of a house. In 2026, it has evolved into the operating system of the modern enterprise. With the complete dissolution of the network perimeter, identity is the only constant control plane across hybrid, multicloud and edge environments.

If you don't get the identity architecture right, no amount of firewalling can save the organization. Modern IAM is no longer a gate you pass through once; it is a continuous oversight mechanism that validates every single request.



The shift to continuous verification

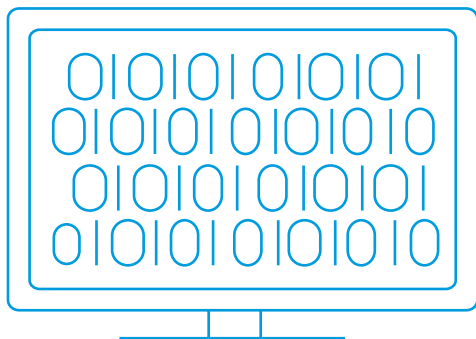
- **Continuous adaptive trust (CAT):** Legacy one-time logins are now a critical vulnerability. 2026 security relies on real-time behavior analysis—such as typing cadence, mouse movement and typical access hours—to ensure the entity behind the keyboard hasn't changed mid-session. If a user suddenly shifts from standard email to mass-downloading database files, the "operating system" must automatically step up authentication or terminate the session.
- **Identity threat detection and response (ITDR):** ITDR has moved from a niche concept to a primary defensive layer. It acts as a security camera for directory services, detecting identity drift—such as an Active Directory Certificate Services (AD CS) misconfiguration being exploited for stealthy persistence or the sudden elevation of a service account's privileges.



4. The identity of things: Resolving the nonhuman identity crisis

Our 2023 report warned of a false sense of security in the cloud and the rise of nonhuman identities. Since then, the growth of these entities has exploded, largely driven by the adoption of microservices and DevOps automation.

In modern cloud-native environments, nonhuman identities (NHIs)—including service accounts, bots and API keys—now outnumber human users by a ratio of 144 to 1.



- **Identity debt:** This explosion has created identity debt—a buildup of unmanaged, over-privileged accounts created by automated scripts. In 2025 testing, 78% of cloud-focused assessments revealed critical misconfigurations in these identities, such as hardcoded credentials in Lambda environment variables or publicly accessible S3 buckets.
- **Identity as code:** Security policies must be embedded directly into infrastructure as code (IaC). Without this, automated robots build servers with excessive permissions that remain active long after the server is destroyed. These ghost accounts create invisible back doors that bypass multifactor authentication (MFA) and allow for lateral movement across the enterprise.



5. The 2026 regulatory landscape: Managing global data sovereignty

Data privacy is now a global mandate with immediate penalties. The bright spotlight we discussed in 2023 has become a global floodlight, with an intense focus on transparency, consent management and the right to be forgotten applied to AI training data.

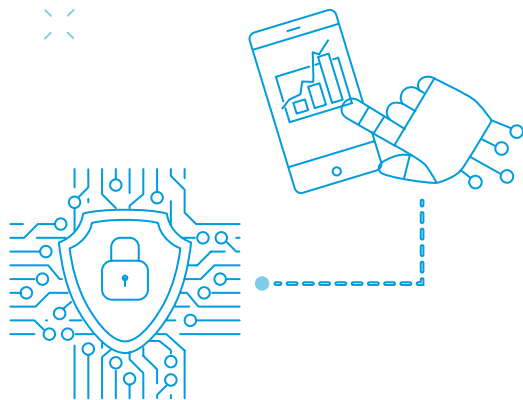


Key updates for 2026

- **The proliferation of state laws:** The patchwork of U.S. privacy laws has solidified. In addition to guidelines already established in 17 states, comprehensive mandates in Indiana, Kentucky and Rhode Island newly took effect in 2026, forcing middle market companies to manage data differently across state lines.
- **The end of right to cure:** Most regulators have removed the grace periods organizations relied on in 2023. Penalties for noncompliance are now immediate upon discovery of a violation.
- **The rise of government ID wallets:** In the U.S., nearly 75% of states now have active or developing mobile driver's license (mDL) programs. These are becoming a standard for selective disclosure, allowing users to prove an attribute (e.g., they are over 21 or hold a specific certification) without sharing their full address, name or Social Security number.

6. Architecting the identity fabric beyond fragmented toolsets

The market is saturated with AI-branded point solutions that solve isolated problems. For 2026, we no longer recommend a collection of tools but rather a unified identity fabric—an architectural approach that integrates single sign-on, governance and privileged access into a single, cohesive layer that works across all clouds and on-premises systems.



Modern selection criteria for 2026

- **Phishing-resistant MFA:** In nearly three-quarters of organizations using MFA, attackers identified practical bypasses using push-notification fatigue or session hijacking. 2026 requires a shift to the Fast Identity Online 2 (FIDO2) authentication standard or biometric approvals to ensure the physical presence of the user.
- **Just-in-time (JIT) access:** The permanent access models common in 2023 are now considered as extreme risks. Privileges must exist only for the duration of a task (e.g., a 15-minute window for a developer to fix a production bug) and expire automatically.
- **Multimodal liveness detection:** To defend against deepfakes, IAM tools must analyze micromovements, blood flow patterns in the face and unique vocal resonance to distinguish between a live human and a generative AI reconstruction.



7. Four critical IAM trends defining 2026

Trend 1: **Agentic AI governance**

Semi-autonomous agentic AI systems now execute transactions and access APIs independently. They require the same rigorous lifecycle management as human employees. In 2025, 73% of AI-integrated systems were found susceptible to prompt manipulation. Organizations must now manage identity for AI as a distinct governance pillar.

Trend 2: **High-assurance digital wallets**

U.S. midmarket companies are adopting government-issued digital IDs for high-assurance tasks like remote employee onboarding and secure customer verification. This allows businesses to verify identity with 100% certainty while storing significantly less personally identifiable information (PII), lowering their data breach liability.

Trend 3: **Post-hire continuous assurance**

Identity verification is no longer a point-in-time event. 2026 standards bind a verified person to their daily access using device posture and biometric signals to detect account-takeover risks from remote workers in real time.

Trend 4: **Deepfake and vishing defense**

As AI clones replicate executive voices in real-time calls, the new standard for sensitive requests (like help desk resets or wire transfers) is synthetic identity protection, analyzing linguistic patterns and signal origin to ensure a live human is on the other end.



8. Final thoughts: Moving from identity debt to identity resilience

In 2023, we said IAM isn't a sprint, but a marathon. In 2026, we have determined it is a continuous control plane. The organizations that succeed in this environment are those that have eliminated their identity debt and shifted from reactive patching to a proactive, identity-first architecture.

Secure digital identity with RSM

RSM provides IAM assessment and strategy development updated for the high-velocity AI era through our refined four-stage approach:

ASSESS:

We perform a deep-dive analysis of your current identity debt, identifying hidden nonhuman identities, over-privileged legacy accounts and AD CS misconfigurations that create stealthy attack paths.

ADVISE:

Our advisors design modern, scalable identity fabrics and governance frameworks tailored to your industry, business goals and the complex 2026 regulatory landscape.

IMPLEMENT:

Our certified engineers deploy phishing-resistant MFA, identity as code patterns and automated ITDR sensors to help ensure security is baked into your infrastructure from the first line of code.

MANAGE:

We act as a continuous extension of your team, providing the AI-assisted defensive capabilities, daily engineering support and threat hunting required to operate at the speed of modern threats.

+1800 274 3978
rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute assurance, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent assurance, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM, the RSM logo and *the power of being understood* are registered trademarks of RSM International Association.

© 2026 RSM US LLP. All Rights Reserved.