Simeio

Always-On Identity Access and Management:

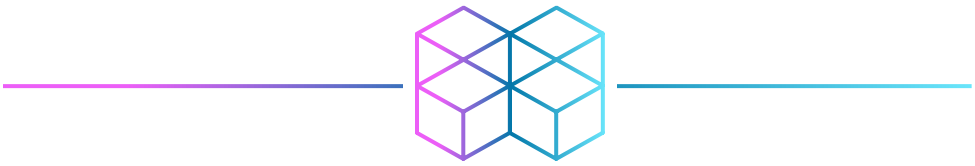
Closing the Execution Gap in IAM

Execution Gap = A disparity between the IAM risk mitigation capabilities organizations believe they have and the security outcomes they actually achieve.

Executive Summary

In today's hyperconnected enterprise, getting identity "right" the first time is not only impossible, it's obsolete thinking. The digital world never stands still: every cloud rollout, business acquisition, or threat innovation reshapes the landscape of who needs access to what, when, and from where. Yet most organizations are stuck with rigid, legacy IAM projects that can't keep up with the explosion of new users, devices, apps, and machine accounts. This leads to persistent security gaps, uncontrolled access, audit failures, and a mounting risk of breaches because business has changed, but identity strategies have not.

Always-On Identity is the only way forward. It transforms IAM from a static, project-based chore into a living, continuous discipline that evolves alongside the business. By automating access controls, detecting risk in real time, and integrating identity governance across every system and user, organizations regain control over the shifting ground of modern risk. A continuous identity program closes the "execution gap" by reducing breaches, ensuring compliance, unlocking agility, and empowering the business to grow with confidence. In a cyber world that never stops changing, the biggest risk is staying static. The boldest move is being always-on.



Why Always-On Identity Matters Now

For many organizations, identity is the new perimeter. **Access credentials are now the number one attack vector exploited in breaches.** Accordingly, identity systems are foundational to enforcing security policy, enabling workforce productivity, and ensuring regulatory compliance.

Despite this, **identity operations are too often handled like a one-time project** rather than a continuously managed function. Joiner-mover-leaver (JML) processes are run monthly. Access reviews happen quarterly. Privileged credentials go unmonitored between audit cycles. And automation is delayed due to cross-functional friction.

This outdated approach creates latency—between a business change and the corresponding identity change—and that latency is the source of real, measurable risk. Former employees retain access to sensitive systems for days or weeks after leaving. Contractors receive standing access that no one monitors. Third-party accounts persist long after the project ends. Meanwhile, attackers exploit this misalignment between business and security to move laterally, escalate privileges, and remain undetected.

Always-On Identity addresses these challenges head-on by treating identity as a continuously governed, monitored, and optimized discipline—integrated with threat detection, aligned to business objectives, and responsive in real time. **Rather than waiting for the next audit finding or breach to trigger action, Always-On Identity ensures that IAM processes are consistently operational,** continuously improving, and tightly coupled with enterprise risk management.

According to the Ponemon Institute, only 46% of organizations believe their IAM tools are effective at managing the user lifecycle.[1] That means **over half of enterprises are exposed to the very gaps that threat actors exploit.** In a related report from Cisco Talos, more than 60% of incident response engagements involved credential compromise.[2] These are not abstract risks—they are daily realities in enterprises that have not adopted a continuous IAM model.

Always-On IAM addresses latency challenges head-on by treating identity as a continuously governed, monitored, and optimized discipline.

ONLY **46%**

Of organizations believe their IAM tools are effective at managing the user lifecycle

Critical IAM Risk Statistics

30%

Unmanaged Identities

69%

Machine Identities Managed (vs. Human)

60%

Credential Misuse in Attacks

The Cost of Inaction

The consequences of IAM execution gaps are wide-ranging. In the best-case scenario, they cause delays and inefficiencies—slow onboarding, frustrated users, and missed audit deadlines. In the worst case, they lead to data breaches, compliance violations, reputational damage, and material financial loss. Unfortunately, these scenarios are increasingly common.

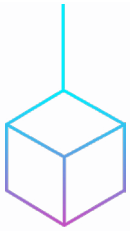
Consider this: SailPoint's Horizons report found that over 30% of digital identities in an average enterprise are unmanaged.[3] These include machine identities, service accounts, dormant credentials, and third-party access points. Many of these identities carry elevated privileges or persist outside the view of standard IAM tools.

In parallel, 72% of organizations report that machine identities are more difficult to govern than human ones—yet **69% say they now manage more machine than human accounts.**[4] This reversal has profound implications for risk, especially when automated processes and API integrations are granted broad access by default.

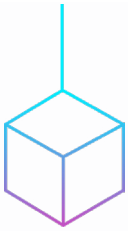
Meanwhile, organizations face mounting pressure from regulators, customers, and boards to demonstrate strong identity governance. Compliance frameworks such as SOX, HIPAA, GDPR, and NERC CIP require timely deprovisioning, access certifications, and demonstrable least-privilege enforcement. The more fragmented a company's identity infrastructure, the harder it becomes for them to produce comprehensive governance reports.

Compounding the problem is the well-documented cybersecurity skills shortage. IAM professionals are among the hardest roles to hire and retain, with recruitment cycles often exceeding six months.[5] According to IDC, the global IT talent gap could cost enterprises over $5.5 trillion in losses by 2026.[6] Even well-funded organizations may struggle to build the internal expertise required to operate a modern IAM program.

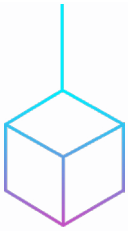
Delaying investment in IAM maturity carries hidden costs: the time spent chasing tickets, the impact of failed audits, the increasing likelihood of a preventable incident and the churn of overburdened staff. A 2024 study found that organizations spend 11 person-hours per identity-related audit.[7] The question isn't whether IAM maturity is necessary—it's whether your organization can afford to fall further behind.



Nearly a third of digital identities in an average enterprise are unmanaged. The bulk of these are complex machine credentials.



The more fragmented a company's identity infrastructure, the more time-consuming and difficult it becomes for their IAM staff to report on governance.



Delaying investment in IAM maturity carries hidden costs including the churn of overburdened staff at a time when IAM professionals are among the hardest roles to fill.

Components of Always-On Identity

At its core, Always-On Identity is an operational model. It is not a single product or platform. It is the strategic integration of people, processes, and technology to deliver identity outcomes consistently and continuously.

Identity Governance and Administration (IGA) is the foundation. Always-On IAM uses automated workflows to provision and deprovision access based on business logic. Role-based access control, entitlement catalogs, and policy-driven approvals ensure consistency. Regular access reviews, combined with analytics, provide visibility into access risks and violations before they escalate.

Privileged Access Management (PAM) is equally critical. Privileged accounts pose outsized risk. Always-On PAM ensures these accounts are tightly controlled—using just-in-time access, credential vaulting, session recording, and behavioral analytics. Monitoring is not limited to quarterly reviews—it is continuous and real-time.

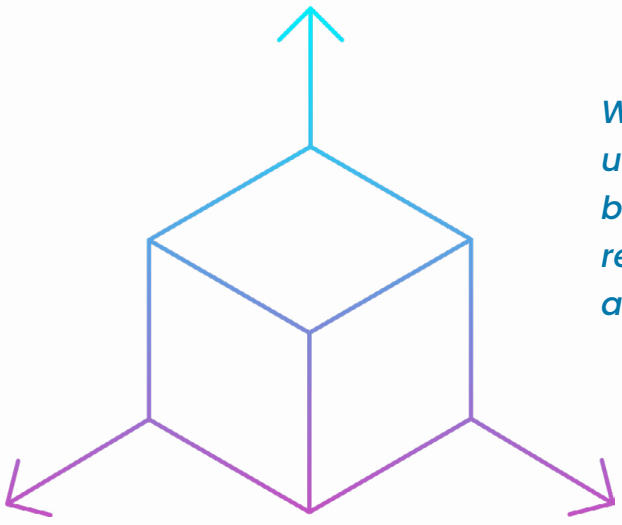
Authentication and Authorization must adapt to context. Adaptive MFA, single sign-on, and attribute-based policies allow organizations to grant or restrict access dynamically. When integrated with identity risk engines, these controls can block anomalous login attempts, enforce reauthentication, or elevate monitoring in real time.

Lifecycle Management connects identity to the business. When an employee joins, changes roles, or leaves, their access should adjust automatically—sourced from HR systems, approved through workflows, and deprovisioned without delay. Always-On IAM closes the loop between business systems and identity infrastructure.

Threat Detection and Response bridges IAM with security operations. Identity telemetry—login patterns, privilege escalations, failed access attempts—is a rich source of threat intelligence. Always-On Identity ensures these signals are captured, correlated, and acted upon through SIEM, SOAR, and UEBA platforms.

Scalability and Architecture must support today's IT complexity. Always-On IAM operates across cloud platforms, SaaS ecosystems, remote workforces, and hybrid datacenters. It integrates with DevOps, third-party contractors, and API gateways. It scales up without losing visibility or control.

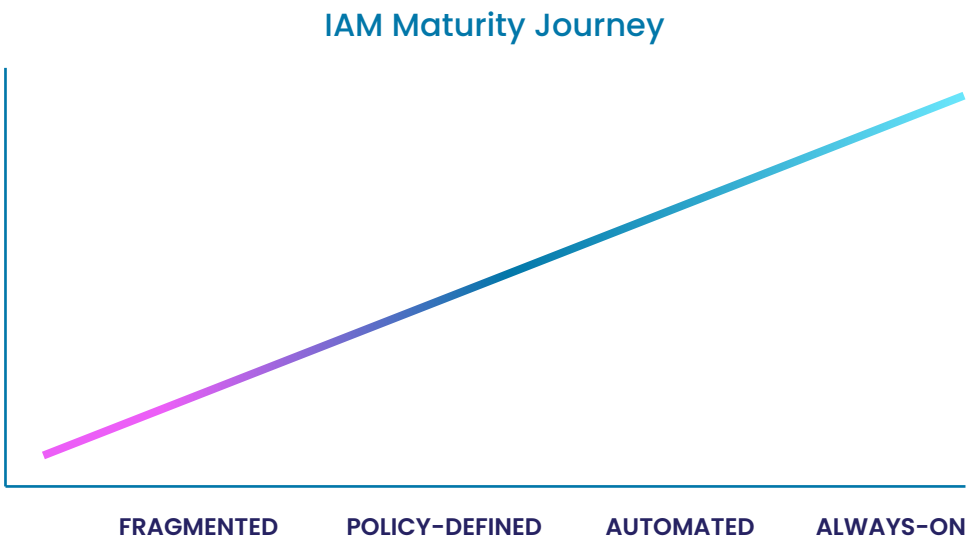
User Training and Awareness reinforces policy. Users are often the weakest link in identity security. Always-On IAM includes regular training, phishing simulation, and credential hygiene to keep users aligned with organizational risk policies.



When these components are integrated under a single governance model, IAM becomes a continuously improving system—responsive to change, resilient to disruption, and ready for next-level protection.

What Leading Enterprises Do Differently

Leading organizations do not wait for a breach or an audit failure to invest in maturity. They treat identity as a business priority and a maturity journey.



High-growth companies understand that Always-On IAM is not just a technical control—it is a strategic capability.

- **Faster Onboarding**
- **Self-Service Access**
- **Compliance Readiness**
- **Talent Gap Reduction**
- **Risk Insights & Remediation**

First, they align leadership around a shared vision for identity. CISOs, CIOs, compliance leaders, and business unit stakeholders agree on the importance of consistent access control, policy enforcement, and lifecycle governance. This alignment accelerates decisions and reduces friction.

Second, they centralize IAM responsibilities under clear governance. Rather than spreading ownership across disconnected teams, they establish a program office or center of excellence to standardize workflows, measure outcomes, and coordinate delivery.

Third, they invest in automation. Wherever manual processes persist—ticket-based provisioning, email approvals, Excel-driven access reviews—leading organizations replace them with workflow engines, approval hierarchies, and real-time policy evaluation.

Fourth, they integrate IAM with broader security architecture. Identity signals feed threat detection systems. IAM events trigger incident response playbooks. Privileged access is included in red-team exercises. Identity becomes a living part of the security operation, not a standalone tool.

Finally, they partner with expert providers to extend their capabilities. Managed IAM service providers (MSPs) like Simeio bring global scale, certified expertise, and continuous delivery models that internal teams alone cannot replicate. These partnerships accelerate maturity while reducing the burden on internal resources.

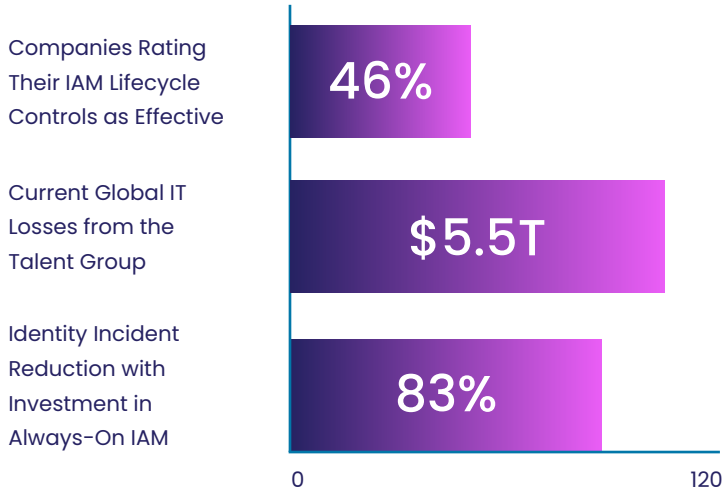
IAM as a Business Driver

When IAM works well, employees are onboarded quickly and accurately. Contractors receive access for only the time and systems they need. Mergers and acquisitions are integrated smoothly. SaaS adoption accelerates without increasing risk. Audit evidence is generated continuously, not retroactively.

Quantitative benefits are well-documented. A Forrester Total Economic Impact study of Okta[9] found that identity governance reduced onboarding time by 89%, cut audit preparation by 90%, and lowered help desk tickets by 12–15 minutes per user during access reviews.[8] Similarly, SailPoint reports that organizations that invest in identity maturity see 83% fewer identity-related security incidents.[9]

The financial case is reinforced by market growth. **The Identity Management Institute projects IAM spending to exceed $24 billion in 2025, growing at 13–14% CAGR.**[10] This reflects rising demand for continuous access management in a world where agility, security, and compliance must coexist.

IAM Readiness, Risk, and Results



Sources: Ponemon Institute, IDC, SailPoint

Always-On IAM delivers value beyond security. It improves operations, reduces friction, and supports growth.

Always-On IAM is not just an ideal. It is a critical operational platform that makes the business safer, faster, and more scalable.

14%

IAM spending is set to exceed $24 billion in 2025, growing at 13-14% CAGR.

Conclusion

IAM is not a static system. It is a dynamic, continuous discipline. As threats evolve and workforces become more distributed, the need for Always-On Identity has never been greater.

Organizations that delay modernization will fall further behind. **Those that act now will close execution gaps, reduce risk, and turn identity into a business driver.**

The path forward is clear. Start with a readiness assessment. Align leadership around a unified identity vision. Automate aggressively. Monitor continuously. And partner with experts who can deliver results.

Be Always-On. Get Access Right. Now.

info@simeio.com | www.simeio.com

Simeio

Getting Started with Simeio

Transitioning to Always-On Identity doesn't require a rip-and-replace strategy. It begins with a maturity assessment. Organizations must understand where their gaps exist—whether in lifecycle automation, privileged access monitoring, or policy enforcement—and prioritize improvements based on business risk.

Simeio helps organizations make this shift. As a global IAM MSP, Simeio delivers 24/7 identity operations, prebuilt integrations, and strategic consulting. Our Identity Orchestrator platform streamlines deployment. Our certified professionals bring deep expertise in SailPoint, CyberArk, Ping Identity, and other leading platforms. And our delivery frameworks accelerate time-to-value without overloading internal teams.

With Simeio, enterprises gain visibility into identity risk, automation of key workflows, and the ability to adapt quickly as business needs evolve.

One Simeio client, a global manufacturer, reduced provisioning time by 75% and eliminated 90% of manual access review effort within the first 12 months of engagement. These results are not the exception—they are the outcome of a structured, scalable, and Always-On IAM model.

> When IAM works right, no one notices. When it fails, everything is at risk.
>
> —Octavio Lopez, Solutions Architect, Simeio

info@simeio.com | www.simeio.com

Simeio

Always-On IAM Checklist for CISOs

Use this one-page guide to assess readiness and lead your organization through the adoption of Always-On Identity. This checklist helps CISOs plan, evaluate, implement, and maintain an IAM strategy that is continuous, scalable, and secure.

1. Preparation & Assessment

- [ ] Conduct a current-state IAM maturity assessment
- [ ] Identify execution gaps (e.g., deprovisioning delays, unmanaged identities)
- [ ] Quantify business risk and operational inefficiencies from IAM gaps
- [ ] Align key stakeholders (CISO, CIO, HR, Compliance, IT Ops)

2. Vendor Selection

- [ ] Define criteria for Always-On IAM delivery (24/7 monitoring, automation, scalability)
- [ ] Evaluate partners with experience in IGA, PAM, lifecycle automation, and threat response
- [ ] Prioritize vendor-neutral orchestration and support for multi-cloud/hybrid architectures
- [ ] Consider managed service providers (MSPs) to close resource and expertise gaps

3. Implementation

- [ ] Develop a phased roadmap (start with high-risk areas like privileged access and JML)
- [ ] Establish IAM governance structures (roles, policies, metrics)
- [ ] Integrate IAM with SIEM, SOAR, and HRIS/ITSM systems
- [ ] Pilot, validate, and document new workflows for continuous improvement

4. Operations & Maintenance

- [ ] Enable continuous access monitoring and policy enforcement
- [ ] Automate lifecycle events with real-time updates from authoritative sources
- [ ] Conduct quarterly governance reviews and risk analysis
- [ ] Maintain user training, access reviews, and executive reporting dashboards

---

Tip: Simeio account managers are skilled in developing a road map with our Certified & Certain assessment tools. Partner with Simeio to accelerate your journey to Always-On IAM with proven frameworks, expert staff, and measurable outcomes.

Citations

“Only 46% of organizations rate their IAM lifecycle controls as effective.” Source: Ponemon Institute / GuidePoint Security, “2025 IAM Maturity Report.” guidepointsecurity.com

“Over 60% of incident responses involve compromised credentials.” Source: Cisco Talos. veza.com/blog

“30% or more of digital identities go unmanaged.” Source: SailPoint, “2024 Horizons of Identity Security Report.” sailpoint.com

“72% of organizations say machine identities are harder to govern than human ones.” 69% of organizations manage more machine than human identities.” Source: SailPoint, Machine Identity Security Report. sailpoint.com

“IAM hiring cycles often exceed 6–9 months.” Source: Simeio market research and identity services data (internal benchmarks)

“$5.5 trillion in projected global losses due to the IT talent gap by 2026.” Source: IDC, 2024 IT Talent Shortage Forecast. Cited in: Multiple summaries, e.g. TechRepublic & Cybersecurity Dive

“Organizations spend 11 person-hours per identity-related alert.” Source: ITPro and ESG/ TechTarget Research (2024). itpro.com

“Up to 90% reduction in audit preparation time.” “IAM tools reduce help desk burden by 12–15 minutes per user.” Source: Forrester Total Economic Impact™ of Okta Identity Governance (2023). okta.com

“83% reduction in identity-related incidents with investment in IAM.” Source: SailPoint, Identity Security Adoption Study. sailpoint.com

“IAM market expected to exceed $24 billion by 2025.” Source: Identity Management Institute. identitymanagementinstitute.org