Is Your IdAM Strategy Still Fit for Purpose?

Four considerations as you build a secure yet scalable environment

Make better happen

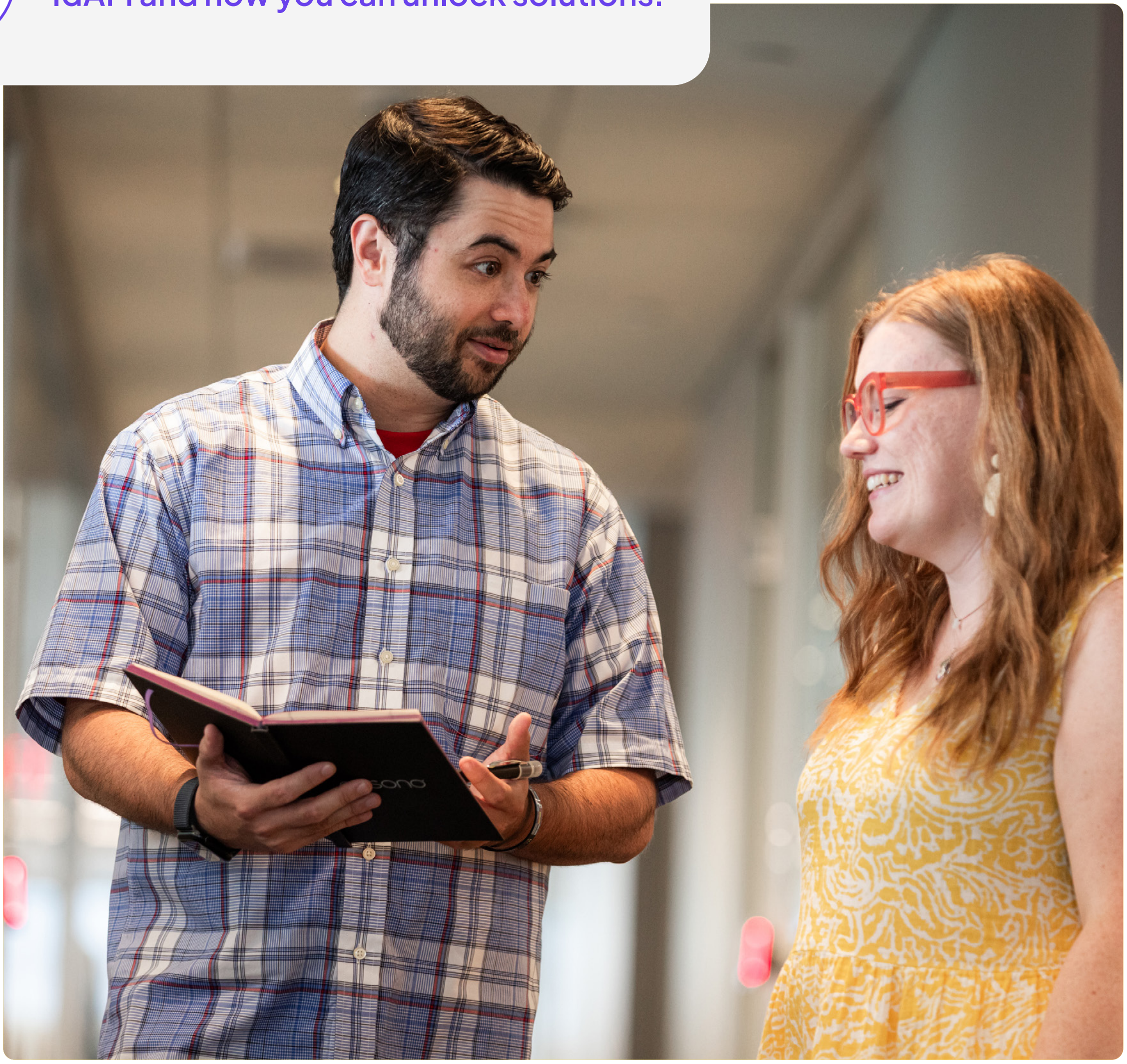
ensono.com

Introduction

With 61% of data breaches involving stolen workforce identities and privileged access credentials, identity and access management (IdAM) has become a critical component of cybersecurity. As organizations continue to modernize and evolve, their IdAM strategies must keep pace if they are to address the complexities of hybrid environments, AI-driven technologies, and increasingly stringent compliance requirements.

As the need for robust, scalable solutions grows, several new challenges are forcing organizations to rethink the way they manage identities and protect access. For IT leaders, the challenge lies in delivering secure, uninterrupted user access while ensuring scalability across diverse IT environments.

Learn about four major challenges of IdAM and how you can unlock solutions.



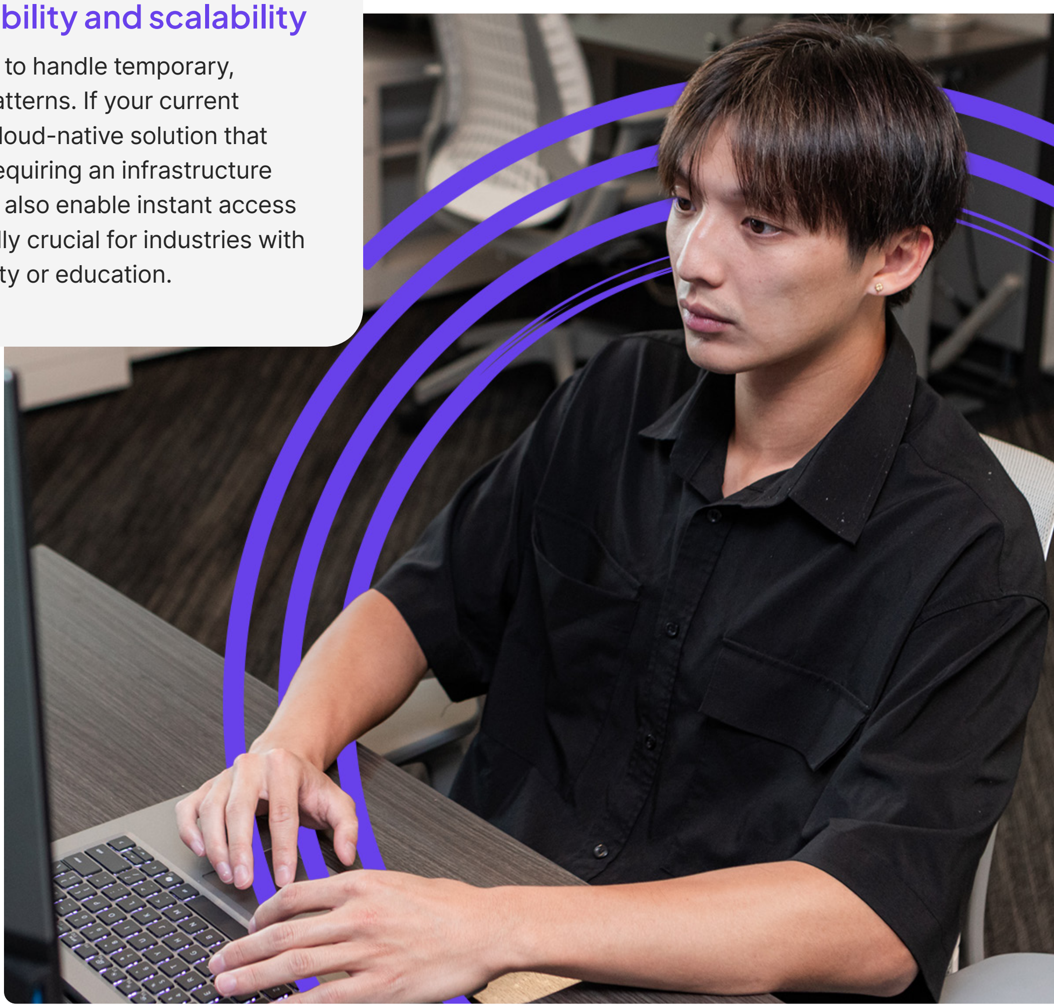
Challenge 1

Increasingly dynamic access needs

The transition to cloud infrastructure and software-as-a-service (SaaS) applications brings flexibility, scalability, and lower operational costs. And it presents new IdAM challenges. The distributed nature of cloud-hosted applications means organizations can no longer rely on traditional corporate firewalls for protection. And, while the cloud facilitates remote access, SaaS applications exposed over the internet often involve multiple device touchpoints and can be deployed across various geographies.

Solution: Look for flexibility and scalability

IdAM solutions need to be able to handle temporary, remote, and irregular access patterns. If your current system falls short, consider a cloud-native solution that can scale in real time without requiring an infrastructure overhaul. Many cloud solutions also enable instant access management, which is especially crucial for industries with high turnover, such as hospitality or education.



Challenge 2

Securing hybrid environments

Maintaining consistent and secure access across diverse cloud environments is a common struggle for IT teams. Native IdAM solutions from hyperscalers may seem like the obvious choice for organizations already invested in these ecosystems, but they often fall short beyond their most basic use cases.

Solution: Ensure comprehensive security

No single IdAM solution can comprehensively manage all levels of access and customization. Organizations should bridge gaps and ensure robust protection by supplementing hyperscaler solutions with platform-agnostic third-party IdAM tools. These tools can effectively secure complex environments while integrating and extending to meet your organization's specific needs.

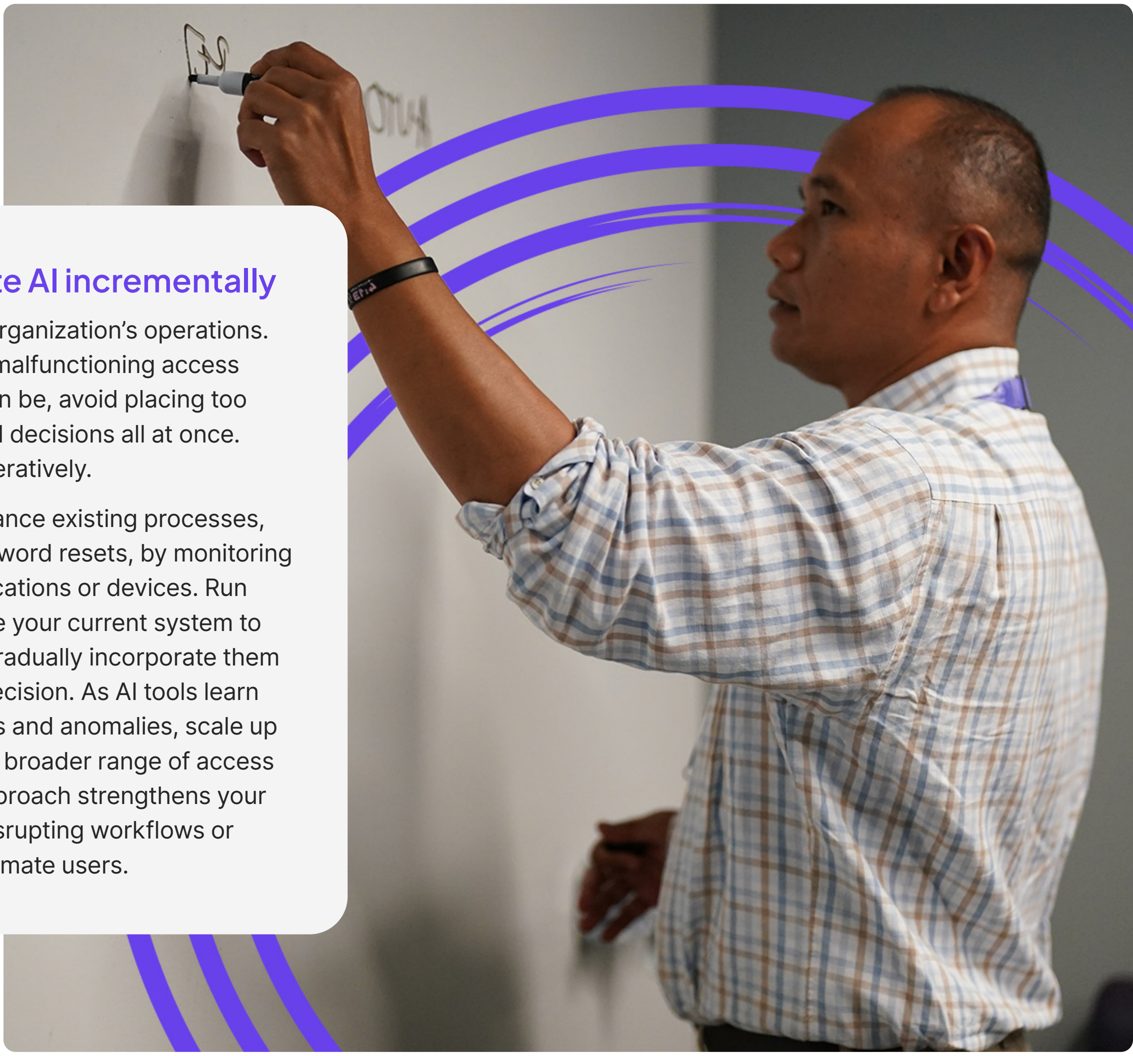
Each vendor has unique strengths and weaknesses, making them more or less suited for specific scenarios. While capability lists can help you create a shortlist of potential vendors, hands-on testing (e.g., PoC trials) is essential to evaluate a vendor's capabilities firsthand and ensure they offer the desired usability and coverage. Some vendors may appear to meet all requirements on paper, but their integrations might be disjointed and not work together as smoothly as expected.

Challenge 3

The rise of AI

While threat actors are using AI-powered tools to enhance their attacks, security leaders are leveraging these same technologies to defend against identity-based breaches.

AI can detect anomalous behavior, flagging suspicious access attempts before they escalate. In fact, **63% of security leaders** believe AI's most significant role in defending against identity-based breaches is identifying outlier behavior that signals potential threats. However, AI should enhance, not replace, existing IdAM infrastructure.



Solution: Integrate AI incrementally

IdAM is crucial to your organization's operations. Given how disruptive a malfunctioning access management system can be, avoid placing too much trust in automated decisions all at once. Instead, implement AI iteratively.

Start by using AI to enhance existing processes, such as logins and password resets, by monitoring events like unfamiliar locations or devices. Run risk predictors alongside your current system to monitor accuracy and gradually incorporate them as you tune them for precision. As AI tools learn from behavioral patterns and anomalies, scale up capabilities to monitor a broader range of access behaviors. A phased approach strengthens your IdAM system without disrupting workflows or causing friction for legitimate users.

Challenge 4

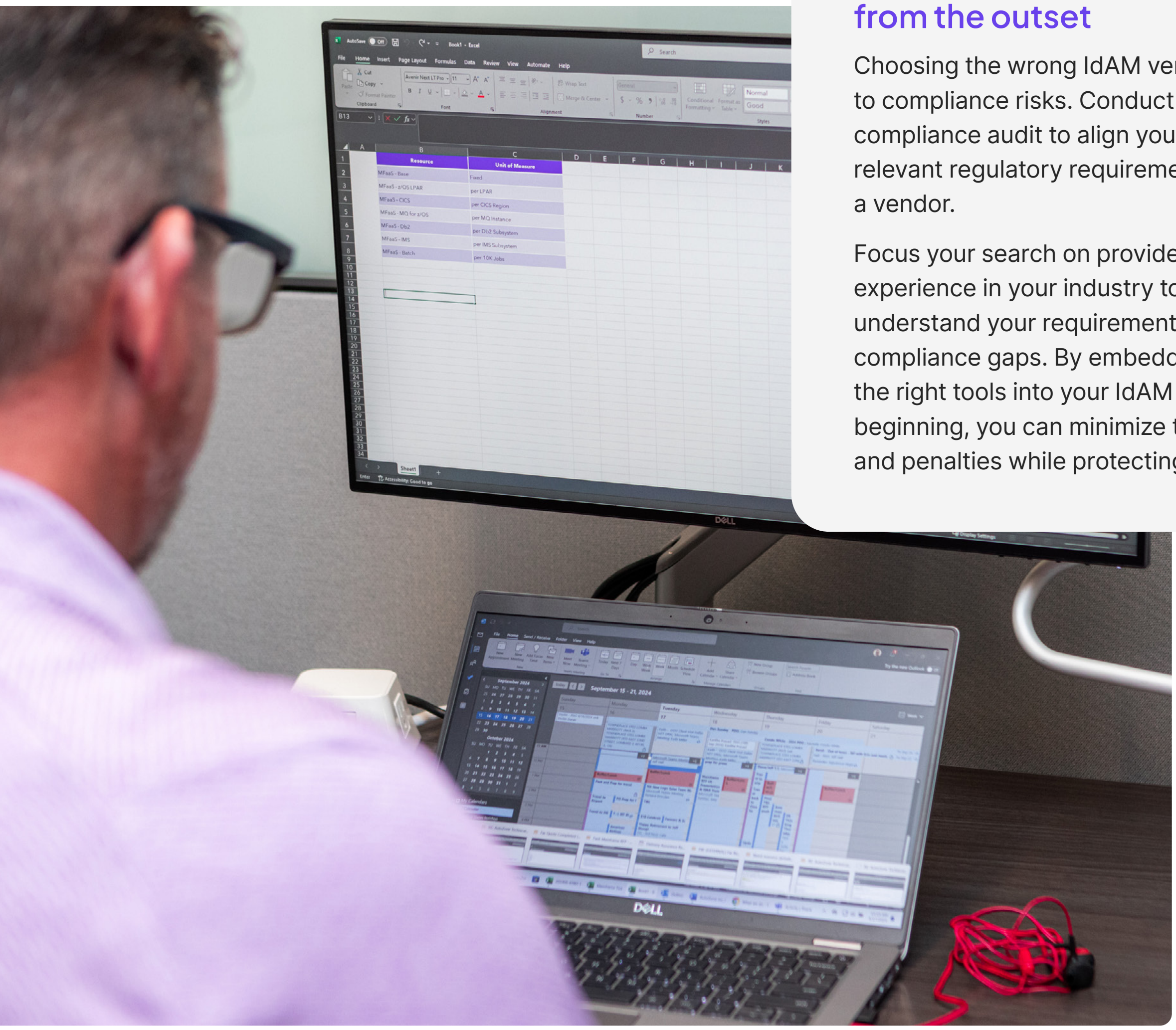
Navigating increasing compliance demands

As regulatory obligations like the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) evolve and expand, organizations face heightened scrutiny over how they manage identities and access to sensitive data. IdAM solutions are crucial for maintaining compliance, especially in sectors like finance where strict regulatory standards govern data access and storage.

Solution: Prioritize compliance from the outset

Choosing the wrong IdAM vendor can expose you to compliance risks. Conduct a comprehensive compliance audit to align your IdAM strategy with relevant regulatory requirements before selecting a vendor.

Focus your search on providers with recent experience in your industry to ensure they understand your requirements and help you avoid compliance gaps. By embedding compliance and the right tools into your IdAM framework from the beginning, you can minimize the risk of costly fines and penalties while protecting your data.



Adapting your IdAM strategy for long-term success

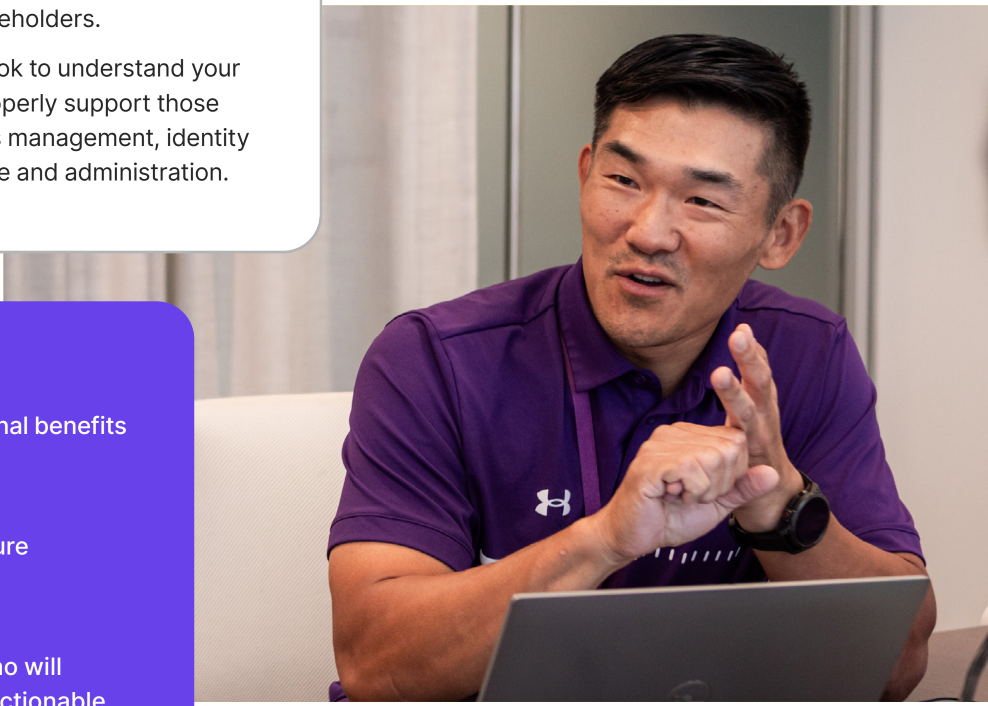
IdAM may seem straightforward, but it requires careful consideration and coordination among stakeholders from multiple areas of the business. As you refine your strategy, consider the trends and challenges impacting IdAM and take advantage of modern tooling and techniques.

Whether you're addressing dynamic access needs or closing security gaps in a hybrid environment, you must think beyond short-term fixes. Also, be careful to avoid taking a purely technical or security-centric approach to your IdAM solution. Modern IdAM tools provide evolving opportunities to improve customer experience, increase visibility into behavior, and reduce operational costs. By taking a proactive, long-term approach that accounts for your current and future requirements, you'll be better positioned to safeguard your digital assets and scale your IdAM solution to future demands.

Gain fresh insights into your IdAM strategy with a Rapid Assessment from Ensono

Ensono's IdAM Rapid Assessment is a two-week engagement during which our IdAM and business specialists collaborate with your technical and business stakeholders.

Through a series of workshops, we look to understand your strategic goals and how IdAM can properly support those goals. We explore the areas of access management, identity management, and identity governance and administration.



Together, we identify:

1. Opportunities to realize additional benefits
2. Risks and mitigation
3. Areas to improve security posture
4. Best fit technologies

At the end of the engagement, Ensono will deliver a detailed report containing actionable recommendations for improvements and savings.

Get in touch

To inquire about Ensono's IdAM Rapid Assessment, or our other IdAm solutions, please follow the link.

Contact us

ensono®

Make better happen