The $41 billion problem

How Access Management Complexity is Sabotaging Your Digital Transformation Strategy

OPNOVA

Table of contents

The Hidden Cost of Inefficiency: An Executive Insight

In the modern digital enterprise, speed, agility, and security are the cornerstones of success. Yet, a silent threat lurks within the operational fabric of many organizations, quietly draining resources and hindering growth: broken access management. This isn't just a minor IT inconvenience; it's a significant business problem with far-reaching consequences. In the world of Identity Governance and Administration (IGA), the market is saturated with a plethora of legacy systems and promising new startups, all claiming to offer the definitive solution to managing identities, entitlements, and access. The Identity and Access Management (IAM) market is projected to grow from USD 15.93 billion in 2022 to USD 41.52 billion by 2030, a testament to the growing recognition of its importance (Grand View Research, 2023). However, beneath the polished sales pitches and impressive product demonstrations, a fundamental and persistent challenge remains: the immense difficulty of implementation. This leaves businesses wrestling with persistent inefficiencies, unmet security needs, and a growing sense of frustration.

This white paper delves into the substantial business costs of a fractured access management strategy, uncovers the deep-rooted causes of this problem, and presents a clear, practical roadmap for modernizing identity governance. We will explore how to achieve this through intelligent integration and automation, without the need for a complete and disruptive overhaul of your existing systems. The goal is to illuminate a path forward, transforming access management from a source of friction into a strategic enabler of business velocity and security.

Why Integration Matters: The Strategic Value of Seamless Access

Despite widespread digital transformation initiatives, many businesses continue to be shackled by outdated and inefficient workflows for managing user access. The core of the problem lies in the frustrating inability of most current IGA tools to seamlessly integrate with the complex ecosystem of enterprise applications.
From legacy on-premises systems to modern cloud-based SaaS platforms and custom-built in-house applications, the technological landscape of any large organization is a heterogeneous mix. Existing IGA solutions, with their rigid architectures and limited integration capabilities, consistently fall short of their promises.

- This is due to a number of factors, including a lack of pre-built connectors for a long tail of applications;
- Inadequate or non-existent APIs that hinder orchestration and automation;
- The sheer complexity of the reasoning required to manage access for non-standard applications in critical workflows like employee onboarding, transfers, and offboarding.

This systemic failure inevitably leads to a highly inefficient and costly outcome: a reliance on redundant administrative work. While IGA platforms are often marketed as powerful engines for end-to-end automation, the reality for most organizations is far from this ideal. In fact, research shows that a considerable portion of IT help desk tickets are related to access management issues, such as password resets and access requests. This effectively transforms your expensive, state-of-the-art automation platform into little more than a sophisticated ticket-routing engine, a far cry from the promised land of seamless, hands-off automation.

What's at Stake: The Real-World Business Impact

The consequences of a broken access management system are not just theoretical; they have a tangible and substantial impact on the business.

Financial Losses

The costs associated with a flawed IGA strategy are substantial. The average cost of a data breach reached USD 4.88 million in 2024, a 10% increase from the previous year (IBM, 2024). The high initial investment in software and implementation, the ongoing costs of maintenance and support, and the significant resources required for customization and systems integration add to the financial burden.

Declining Operational Efficiency

The promise of automation is to free up human resources to focus on more strategic initiatives. However, when IGA tools fail to deliver on this promise, IT and security teams become overwhelmed by repetitive operational tasks. A survey by Expert Insights revealed that 35% of employees admit to working around their company's security policies to get their job done, highlighting the friction caused by inefficient access management.

Increased Security Risks

Perhaps the most critical consequence of a broken access management system is the increased risk to the organization's security posture. Verizon's 2023 Data Breach Investigations Report found that 61% of all breaches involved credentials. Furthermore, insider threats, both malicious and unintentional, are a growing concern. The Ponemon Institute's 2023 Cost of Insider Threats Global Report found that the average cost of an insider-related incident was USD 16.2 million, quadruple the average breach cost. Without a clear and accurate picture of who has access to what, it becomes impossible to enforce the principle of least privilege, a cornerstone of modern cybersecurity. This lack of visibility and control amplifies the risk of data breaches, insider threats, and non-compliance with industry regulations

Ultimately, the best-laid security plans and the most ambitious digital transformation initiatives can be undermined by inefficiencies in the back office.

Why Change Is Hard: Understanding the Resistance

Given the obvious risk created by a broken access management system, why do so many organizations struggle to address the problem? The reality is that most companies are not ignoring the issue, but they often feel trapped by a number of significant barriers:

Legacy Systems

Many organizations have invested heavily in legacy IGA solutions that are rigid, inflexible, and difficult to customize. The thought of ripping and replacing these deeply embedded systems is often seen as too risky and disruptive.

Dependence on Integrators

The traditional IGA market has long been dominated by a model that relies on armies of systems integrators to deploy and maintain their solutions. This has created a culture of dependence, reinforcing the idea that identity management is an inherently complex and expensive endeavor.

Fear of Disruption

The prospect of a large-scale overhaul of critical identity and access management systems is a daunting one for any organization. Concerns about disrupting business operations, impacting user productivity, and the potential for a failed implementation often lead to inertia.

Misconceptions about Automation

There is a common misconception that existing IGA tools provide true, end-to-end automation. In reality, they often do little more than shift the manual workload from one team to another. A survey by vSecureLabs found that while 44% of security experts believe an IAM solution is crucial to address security vulnerabilities, ease of integration remains a top concern for 72% of organizations.

Strategic Moves That Drive Change

To break free from the shackles of a broken access management system and transition to a more agile, secure, and efficient model, organizations need to adopt a new approach. The following four strategic moves can help you achieve this:

Move 1: Map and Modernize Your Access Landscape

The first step is to gain a clear and comprehensive understanding of your current access management landscape. This involves creating a detailed inventory of every application and system where access is managed, including:

- On-premises
- Legacy applications (e.g., mainframes, custom-built client-server applications)
- Cloud-based SaaS applications (e.g., Salesforce, Workday, Office 365)
- In-house custom applications
- Infrastructure components (e.g., servers, databases, network devices)

By mapping out these channels, you can identify the most critical and problematic workflows and prioritize them for automation.

Move 2: Automate with Integration and AI Agents

The key to unlocking true automation in access management is to leverage a modern integration platform that combines the power of AI with a flexible, application-agnostic approach. This involves:

- Workflow Automation: Automating complex, multi-step access request, approval, and provisioning workflows across multiple systems.
- AI-Powered Reasoning: Using AI and machine learning to handle the complex reasoning and decision-making required to manage access for non-standard applications and nuanced scenarios.
- Application-Agnostic Integration: Building a robust and scalable integration strategy that can connect to any application, regardless of its age, architecture, or whether it has an API.

Move 3: Create a Hybrid Integration Strategy

A one-size-fits-all approach to integration is doomed to fail in the complex and heterogeneous world of the modern enterprise. Instead, you need to adopt a hybrid integration strategy that combines a variety of different techniques to meet the unique needs of each application and system:

- API-based Integration: This approach connects modern, cloud-native systems via standardized interfaces known as APIs. It enables real-time, system-to-system communication—efficient and scalable—but depends on both systems supporting compatible APIs.
- Agent-based Integration: In environments where APIs are unavailable, software agents simulate user interactions with the system interface, automating tasks such as form inputs or navigation flows. This method is particularly useful for legacy or custom applications that lack direct integration options.
- Database and File-based Integration: This method facilitates data exchange through structured files (such as CSVs) or direct access to system databases. It is well-suited for batch processes or environments where systems are designed to interact through scheduled file transfers.

Move 4: Roll out the change in clear, access-focused steps

A successful transformation requires a structured and phased approach that allows you to demonstrate value at every stage:

- Pilot a Quick Win: Start by identifying a low-risk but high-impact workflow to automate. One example would be automating access requests for a single, critical application that is currently a major source of operational bottlenecks and user frustration.
- Prove the Value: Once you have successfully automated your pilot workflow, it is crucial to capture and communicate the results. This should include both quantitative metrics (e.g., reduction in time to grant access, decrease in help desk tickets) and qualitative feedback from users and stakeholders.
- Empower Business Users: To ensure long-term success and adoption, it is important to empower business users to take ownership of their own access management processes. This can be achieved by providing them with a low-code/no-code interface that allows them to customize workflows and rules without needing to rely on IT.
- Track Core KPIs: As you expand your automation efforts, it is essential to continuously

- monitor a set of core key performance indicators (KPIs) to track your progress and identify areas for improvement. These KPIs should include metrics such as the overall automation rate, the average time to fulfill an access request, and the number of access-related security incidents.
- Roll out in Controlled Phases: A phased rollout allows you to manage risk and ensure a smooth and successful implementation. You can start by tackling one department or application category at a time, gradually expanding your automation footprint across the organization....

From Access Control to Value Enablement: Future-Proofing Identity Governance

Ultimately, the goal of modernizing your access management is not just about improving efficiency or reducing costs. It's about transforming identity governance from a reactive, cost-centric function into a proactive, value-enabling capability.

ROI Highlight

Organizations leveraging AI in security see significant cost savings

$2.2M

Average cost savings per breach for organizations with extensive AI security automation (IBM, 2024).

In today's digital economy, the ability to quickly and securely provide your employees, partners, and customers with the access they need to do their jobs is a critical competitive advantage. **Organizations that leverage security AI and automation extensively see an average cost savings of USD 2.2 million per breach** (IBM, 2024).

Organizations that succeed in this endeavor will be those that are able to move beyond the traditional, siloed approach to access management and embrace a more holistic view of identity, security, and the user experience. They will be the ones that can redesign how value flows through their business, unlocking new levels of speed, agility, and innovation.

The IGA market is ripe for disruption, and the future belongs to those who are willing to challenge the status quo and embrace a new paradigm of intelligent, automated, and user-centric identity governance.

Next Steps: Start Your Access Management Transformation

Are you ready to break free from the constraints of your broken access management system? Are you ready to eliminate delays, reduce manual work, and future-proof your identity governance strategy? Contact our team of experts today to explore how an AI-powered automation platform can help you on your journey. Request a personalized demo to see how this innovative approach to access management can transform your organization and unlock new levels of business value.

References

- Expert Insights. (2024). *50 Identity And Access Security Stats You Should Know In 2025*.
- Grand View Research. (2023). *Identity And Access Management Market Size, Share & Trends Analysis Report*.
- Ponemon Institute. (2023). *2023 Cost of Insider Threats Global Report.*
- Verizon. (2023). *2023 Data Breach Investigations Report*.
- vSecureLabs. (2023). *25+ Identity and Access Management (IAM) Statistics to Know in 2023*.


OPNOVA