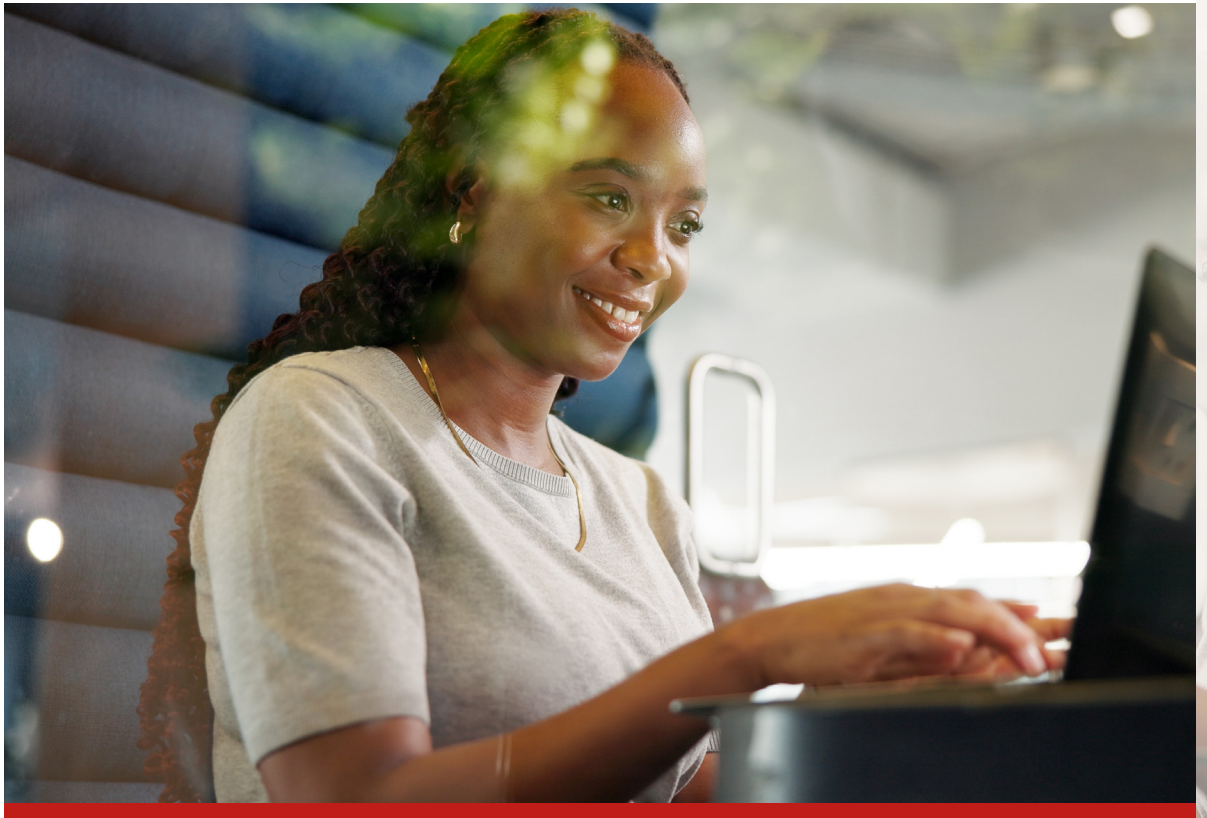


The agility mandate: Securing the enterprise at cloud speed

It may seem daunting to modernize and migrate a legacy system to the cloud. Yet delaying the process or choosing to stick with an on-premises identity solution presents significant roadblocks to enterprise agility and innovation.



Companies are dealing with a seemingly insatiable demand to adopt AI applications. Enterprise IT groups are under orders from the C-suite to enable these capabilities and foster rapid growth. But some organizations are hitting a roadblock as they try to adapt self-managed, premises-based identity architectures to cloud environments.

Legacy identity systems tend to be largely static and highly customized, making them ill-suited to dynamic cloud environments and unlikely to account for non-human entities such as AI agents.

As such, these older identity architectures are full of “identity debt,” a form of technical debt that enterprises need to address if they are to achieve the agility that AI demands. A practical solution is to migrate these legacy identity systems to a cloud-native platform that can turn identity into a business enabler.

The identity debt crisis

Identity debt arises from years of customizing on-premises identity systems to fit specific use cases, workflows, and requirements.

Consider a workflow that requires an elevated level of privilege, such as a customer refund request of \$15,000 due to a billing error. Such a request may require approval from a customer service manager and the finance department, as well as sign-off from accounting before any funds are released. Each step requires an identity check, and the entire process requires significant custom coding.

Perhaps even more complex is a situation where certain requirements must be met, for example, training in a healthcare environment. That requires checking a learning management system (LMS) to confirm that a given employee has completed a specific course within a specified time period. And the verification may have to happen periodically, such as annually. This process requires custom code in the identity system to complete these workflows and ensure employees have met all the requirements.

When an enterprise wants to move the identity environment to the cloud, all that custom code becomes identity debt. Further complicating matters is discovering all that custom code to ensure it's accounted for in the new environment.

The risks and complexity can create upgrade paralysis. As a result, organizations get stranded on older versions of identity platforms and miss modern features and security patches that cloud-based platforms continuously deliver.

In addition, enterprise IT groups end up spending valuable time on maintenance issues, including troubleshooting custom connectors to various applications, servers, and databases. Ultimately, these tasks leave the organization with less capacity to support new business initiatives and strategic projects – like AI.

The security reality: Defending the new perimeter

Upgrade paralysis can cause further risks, especially amid a shifting cybersecurity threat landscape. Attackers are armed with AI tools that enable them to more easily steal credentials from legitimate users. When successful, they can then log into your network, rather than hack in.

Agentic AI adoption can exacerbate the risks. Autonomous agents take actions on their own, just like employees. As such, these agents need to be governed and secured – just like employees. In effect, this new dynamic means identity is now the front line of cyber defense.

But legacy identity systems were never intended to handle dynamic entities like AI agents. They were built for a different era when companies provisioned resources that largely remained static. Companies issued periodic compliance reports as needed to prove they had a reasonable degree of security.



However, legacy systems lack the real-time visibility and dynamic control needed to detect anomalous behavior in the middle of a data stream or conversation. Such capabilities require modern identity management solutions that can correlate multiple data streams and apply real-time analytics to instantly detect risks, isolate threats, and dynamically adjust user privileges – including for AI agent “users” – before a breach or unauthorized data transfer occurs.

The prerequisite for an AI-driven future

Addressing the identity management issue is crucial if AI initiatives are to flourish.

The 2026 Foundry AI Priorities Study found that AI deployments are delivering significant ROI at many organizations. About half of the 538 IT decision-makers surveyed say they’re achieving meaningful productivity returns. “They’re also seeing cost savings and efficiencies, improved process automation, and gains in customer experience,” the report says.

Nearly all the participants (97%) say they are either investing in or planning to invest in AI tools. The top business objectives driving their AI investments are:

- **Improving employee productivity (55%)**
- **Strengthening data protection and privacy through AI (45%)**
- **Improving customer support or services (44%)**
- **Improving speed of development (44%)**
- **Enabling innovative/new product development (43%)**

However, the study also found that “integration of AI systems into existing IT environments is a common pain point.”

That pain certainly applies not only to the identity management issue but also to datasets. As the Foundry study suggests, C-suite executives are asking how AI and

machine learning (ML) can drive efficiencies and increase employee productivity. Enabling such gains requires AI to have access to massive, continuous datasets.

Yet legacy, premises-based identity systems trap critical data in localized silos, which can adversely affect AI initiatives. If an AI engine can't access all the relevant internal corporate identity data, it becomes far more difficult to detect issues that may be out of the norm.

A cloud-native identity platform, on the other hand, collects large amounts of access-related data from across the enterprise. That vast data store enables it to fully understand issues such as:

- **Who has access to data and systems**
- **When access permissions are typically granted**
- **How often permissions are used**
- **Which permissions are often granted together**

- **Which roles are typical for specific job functions**

- **Patterns associated with security incidents or compliance violations**

In essence, a cloud-native identity platform creates data gravity, which it then uses as fuel for AI systems to make intelligent access recommendations. Similarly, the platform can auto-generate compliance insights and identify dormant risks that humans may miss, such as still-active credentials for a long-retired employee.

By adopting a cloud-first identity architecture, organizations can establish a scalable, intelligent foundation for securely managing the explosion of human and machine identities that the next wave of computing is bringing.

Easing migration fears

Even when it's clear that migration to a cloud-based identity solution makes sound business sense, many organizations remain apprehensive about making the move.

One of the most common concerns is the risk of losing customizations, workflows, policies, and integrations they have spent years integrating into their premises-based identity systems. These may contain hundreds of business-specific rules governing access requests, approvals, compliance controls, and provisioning processes. The concern is that moving to a cloud-based identity platform will require them to identify, document, and reverse engineer these capabilities.

Historically, those concerns may have been well-founded. Traditional identity modernization projects may have involved months of manual discovery, requirements gathering, and costly consulting engagements. Teams had to analyze legacy configurations, map complex workflows, and rebuild them in a new environment. It was an effort fraught with the risk of misconfigurations and, consequently, delays in realizing value from the new solution.

Today, advances in AI and automation are fundamentally changing this equation. Modern identity platforms

can leverage AI-driven modernization methodologies to guide the transition. These methodologies use AI engines to analyze existing on-premises identity environments and identify key configurations, workflows, approval processes, and access policies. They can then translate the legacy configurations into cloud-ready artifacts. The entire modernization process, which may have once taken months, can be completed in a matter of weeks.

The benefits extend well beyond faster deployment. By automating large portions of the modernization process, organizations can begin realizing value from day one of the cloud identity deployment. This allows enterprises to achieve significantly faster time-to-value from their cloud identity investments. They can also achieve a lower total cost of ownership because AI-based automation reduces the likelihood of implementation errors and minimizes disruption to business operations. IT teams spend less time managing the upgrade and more time focusing on strategic initiatives that drive business outcomes.

Reclaim strategic enterprise agility

The impact of modernization becomes even more significant when viewed through the broader lens of enterprise agility. Removing identity debt means jettisoning the accumulated burden of outdated processes, fragmented systems, manual workflows, and technical complexity that slow innovation and increase operational costs.

Modernization also means entering a new world where identity is far easier to manage, with many tasks now automated. Assign a role to

a new employee, and the identity management tool can quickly assess what resources other employees in that role have and assign the appropriate access. If a manager wants to grant a user access to an application that may be outside the norm, an AI-driven cloud-based identity tool can quickly inform the manager of the risks inherent in doing so – and let the manager decide accordingly.

A cloud-based solution can also address mundane tasks, such as adding a description for an access permission or entitlement. This is especially useful when a resource name uses an IT-centric convention that isn't clear to nontechnical users, such as marketing executives. Historically, fixing this type of issue required manual documentation efforts involving every group that may need to access the resource. AI can dramatically speed up the process and improve decision-making, resulting in strengthened security because employees actually understand what access they're granting or reviewing.



Overall, a modern identity platform positions organizations to capitalize on the next wave of AI innovation. As enterprises begin deploying AI assistants, autonomous workflows, and agentic AI systems, identity becomes the control plane governing what agents can access, the actions they can take, and how their activities are monitored. Organizations burdened by legacy identity infrastructure will struggle to adopt these technologies safely and efficiently.

By modernizing identity and removing the constraints of legacy systems, enterprises can create the flexibility they need to respond quickly to changing business demands.

In short, they establish the foundation for true enterprise agility in an increasingly AI-driven world.

Stop letting legacy infrastructure dictate your business speed. Learn more about SailPoint Agentic Acceleration,[™] a methodology powered by SailPoint Virtual Architect[™] that transforms the move from IdentityIQ to SailPoint Identity Security Cloud. [See how](#) you can skip the manual heavy lifting and architect a seamless, cost-effective transition to the cloud.