IDC

SPOTLIGHT

Sponsored by: PwC

As today's security architectures continue to gain in complexity, the area of identity and access management is growing especially complicated. This complexity creates a huge challenge for organizations that want to switch from one IAM solution to another that offers more benefits.

The Value of Simplified Identity and Access Management Application Onboarding

August 2023

Written by: Philip D. Harris, CISSP, CCSK, Research Director, Governance, Risk, and Compliance Services

Introduction

Identity and access management (IAM) solutions have come a long way in the past 20 years. These solutions form the foundation of trust in information systems and infrastructure. They offer many benefits in improving the user experience, risk management, and systems administration of applications, networks, and endpoints.

Organizations see the greatest value in IAM solutions that are not only sustainable and cost effective but also simple to use, manage, and audit. This value is underpinned by foundational capabilities that help confirm only authorized users have appropriate privileges and access to infrastructure, network, and application resources.

AT A GLANCE

KEY TAKEAWAY

Centrally managing and automating a collection of application information can speed up application onboarding administration to popular identity and access management solutions. In addition, as a secondary benefit, this approach can make the transition between IAM solutions easier to consider when the need to change IAM providers becomes a necessity.

However, generating the value of IAM solutions does not come without challenges. These include application integration, streamlining business and IT processes, automating workflows, and change management.

Digital technologies have created new ways for organizations to do business, collaborate with colleagues and customers, and streamline processes. This digital acceleration has come with a dramatic increase in cybersecurity risk, highlighting the need for robust identity management. Companies need to make sure that the right people have the right access to their ever-growing list of applications. It's a process that has traditionally been long, complex, and expensive for each application. But that can change.

Application Onboarding Challenges

An effective IAM solution should offer capabilities such as onboarding and offboarding users, establishing and transferring resources and roles, understanding unique access control requirements, and grouping the identities and access roles appropriately. When done manually, these processes can be quite cumbersome, time-consuming, expensive, and prone to error. The value of an IAM solution is limited; however, when the system resources it's designed to protect aren't well accounted for or managed. When external systems and cloud services must be accounted for — and when consideration must be given to both internal and external users — these challenges are compounded.

Furthermore, the ongoing administration of IAM solutions can become problematic when introducing manual or time-intensive activities such as understanding the nuances of each application — the requirements for user and application access within the overall architecture, for instance. Given that applications change over time, it's necessary to understand how changes can impact user and application access requirements. For example, application A has undergone a major version change. As a result, application A will need access to database B. Ideally, this type of detail should be kept within the application documentation. However, this knowledge is often not available to key organizations such as IT or IAM administrative teams. Or imagine that application A has access to database B. This means that new user access control functionality requiring access changes is available in the user interface.

Application onboarding encompasses many of the aforementioned issues. It continues to be a challenge for IAM teams to fully onboard all applications in a timely manner, and the data collection itself becomes a major hurdle to overcome. Gathering the necessary contextual data to fulfill application onboarding can take anywhere from days to months, depending on the availability of documentation. Much of this data is located within a variety of places, such as the DevOps teams, the line of business, or within the application code itself.

Still, there's a missing piece to the puzzle of integrating applications with IAM solutions: the lack of a centralized repository. In such a repository, all the context for an application is managed and encoded in such a way that any IAM solution can easily gain access to it through an application programming interface (API) layer. This capability is vastly different from that of Lightweight Directory Access Protocol (LDAP) or Active Directory (AD). Most organizations rely upon the connectivity between IAM and LDAP or AD to confirm that their applications and systems are identified and managed. However, maintaining these repositories is difficult and offers little in the way of enabling other non-IT personnel to keep applications and systems maintained over time. With the rapid growth in the number of applications worldwide, these types of constraints make it challenging for IAM teams to keep up with the increasing workload.

A central repository provides the flexibility needed to access any IAM solution in the marketplace. It also enables the scalability to expand and contract based upon the organization's business needs as well as the extensibility necessary for collecting the contextual information that IAM solutions require. Such a repository is sustainable and can be maintained by either the business owner or DevOps. In addition, while a configuration management database (CMDB) works quite well for managing general system and application information, it has limitations. These include poor onboarding of applications and security for external users, devices, and applications. Due to its generally static nature, a CMDB is also expensive to install and reduces the flexibility needed for change.

IAM Application Onboarding Acceleration

A streamlined application onboarding process can help accelerate full deployment of an IAM solution. Moreover, it can help organizations prioritize which applications they onboard based upon compliance requirements, application user volume, and other factors. However, the onboarding process alone isn't enough. Organizations also need an ongoing — and consistent — automated methodology where they store, maintain, and manage application technical requirements and context. To achieve accelerated application onboarding, organizations need to gather this knowledge about applications and automate the flow into a centralized repository that has automated connectivity to their IAM solution.

Establishing an automated application onboarding methodology can help organizations confirm that they're managing — and maintaining — all relevant details, context, and requirements in one place. Having a capability like this also means that changes are captured and implemented within the IAM solution. The result is less application downtime, better accessibility for users when they need it, and critical application recoverability in the event it's necessary.

Organizations possess different applications to support business needs on an ongoing basis. Over time, this could result in an inventory of hundreds — or even thousands — of applications. Because of this, it's important that for sizable inventories, they're capturing application details, context, and requirements within a capability that's scalable.

Accomplishing this, however, can be quite difficult to manage. A change management automation workflow can make the collection of this information easier. It can also result in longer-term benefits that can be realized readily by application owners. For example, with the right technology and process, users will be able to access an application when they need it, especially when the user interfaces change. In the case of a major disruptive event, an organization's disaster recovery and business continuity teams would have the necessary information about an application. This would enable these teams to verify that the application is classified appropriately. In addition, knowing that an application is integrated with the chosen IAM solution can help reduce the complexity of onboarding — whether the organization stays with that IAM solution or migrates to another.

Migration to new IAM solutions can be a seamless activity that goes unnoticed by the organization. But this will require involvement from IT, DevOps, and the business because:

- APIs need to change — and applications, systems, and network accounts will need to be migrated to the new IAM system.
- IAM workflows and processes will need to change.
- Users and administrators will need to learn the new changes.

Movement of all the IAM data — users, access controls, and system, network, and application relationships — is what makes migration so fraught with issues. Not doing this in a highly organized way could render a company disrupted for a time. Leveraging a repository that can help organizations overcome many of these issues can play a significant role in making the management of applications much easier.

Benefits

For organizations, the benefits of an independent — and application-agnostic — onboarding repository include gaining the ability to:

- Enable secure application onboarding with efficiency and scalability.
- Address mission-critical application onboarding requirements.
- Automate manual workflows, while building a better experience for application owners.
- Integrate with leading IAM solutions to help mitigate cost.
- Maintain the relationships between applications, systems, and networks to take advantage of newer IAM solutions more freely.
- Build confidence and control through having a centralized view of what's onboarded and what's left.
- Get more from their IAM investments by getting applications onboarded faster and more securely.

- Decrease their cyberattack surface area and reduce the potential of security breaches.
- Save time and money by simplifying onboarding and making it a self-service.

Trends

Large corporations with dozens of applications for their ever-shifting workforces are putting themselves at an increased security risk and are creating more openings in their protection. Not just that — but their IAM teams are unable to provide a holistic overview of application onboarding to company leadership. And without an integrated application, solving the challenges of addressing cybercrime — or the cybersecurity needs of all stakeholders, including those at the board level — becomes significantly harder.

Many organizations have moved — or are considering moving — their IAM solutions to the cloud. The underlying rationale of cloud migration includes a need for increased scalability — in particular, for larger organizations — and for greater resiliency in the face of the post-pandemic landscape. These organizations are establishing methodologies for onboarding and are providing clarity on where they are in the process. They're looking for ways to manage a long, tiresome onboarding lift and automate menial tasks, while addressing cybercrime along with their cybersecurity needs related to onboarding.

Considering PwC

Connected Identity, a PwC product, embeds cybersecurity and identity management into an intelligent platform. This solution can help make onboarding faster, more secure, and less complex for organizations, while improving confidence, control, and business outcomes.

Connected Identity is designed and built to get systems up and running quickly with a more effective implementation process and a consistent user experience across all systems. It does this while capturing the inherent nuances and complexity of identity management. Its interoperability and portability also allow a smoother transfer of information between teams. With Connected Identity, organizations can enable better IAM services, such as provisioning access to the right people and access to the right things when they need them. And it can repeat the process for every new application.

Connected Identity enables fast integration of new applications in digital business ecosystems. With an easily repeatable process in place, companies can focus on creating value. This technology solution will work with SailPoint, Okta, ForgeRock, Microsoft, and Saviynt — and, in the future, with privileged access management (PAM) providers such as CyberArk.

Connected Identity is a critical part of a cybersecurity strategy, and as such, its benefits go beyond IT and application owners. When people and business units are up and running with the right levels of access to necessary applications on day one, the user experience is improved, collaboration and efficiency happen sooner, and more can get done. Connected Identity enables better workflows, improved security, and greater ROI from an organization's investments in its people, processes, and technology.

Challenges

Solution sales are different from services sales. PwC's entrance into the solution sales space will be an important initiative for the company's sales staff to take on. Achieving success in the marketplace with this new offering will require staff training and effective change management, two of the areas where PwC excels.

Conclusion

Digital transformation brings great promise to organizations, but it also increases the surface area for cyberattacks — attacks that often come from identity management issues. Application onboarding to IAM solutions can be an arduous process — often customized by application and system. And the growing number of applications at any given organization presents increased access challenges. Seeking out a solution that can simplify application onboarding can significantly reduce the cybersecurity risks that could result from inaccurate or incomplete application information. The right solution can help organizations establish secure onboarding to an IAM solution.

About the Analyst

Philip D. Harris, CISSP, CCSK, *Research Director, Governance, Risk, and Compliance Services*

Phil Harris is the research director for GRCS. He is responsible for developing and socializing IDC's point of view on governance, risk, and compliance across people and processes focused on creating a foundation of privacy and trust with enterprises, IT suppliers, and service providers.

MESSAGE FROM THE SPONSOR

PwC's Connected Identity solution, designed and built by cybersecurity and identity management leaders, redefines access management. Connected Identity makes the process streamlined, transparent and speedier—and establishes an onboarding methodology that applies across applications. Interoperability means that information is exchanged seamlessly, with consistent controls across applications and systems. Onboarding new people and new systems is finally a good experience. And with people and systems up and running faster and more securely, organizations can see the impact of their investments more quickly.

For more information visit https://www.pwc.com/us/en/products/connected-identity.html.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.