Modern Identity Management: A Platform Approach

Deploying IGA on a Business Platform Can Improve Security and Streamline Identity and Governance Tasks

By Jack Poller, Enterprise Strategy Group Senior Analyst
November 2022
Contents

Background ............................................................................................................................................................................ 3
IAM Trends ........................................................................................................................................................................... 3
Identity Security Challenges .................................................................................................................................................. 4
The Rise of Platforms .......................................................................................................................................................... 5
Clear Skye and the ServiceNow Platform .......................................................................................................................... 5
The Bigger Truth ................................................................................................................................................................. 7
Background

Identity management is a complex component of an organization’s security profile. The responsibilities for managing user, customer, workload, and third-party identities can be distributed between HR, IT, cybersecurity, and line-of-business (LOB) teams, which presents challenges for security and business alignment. As a result, identity management is becoming an increasingly large part of the cybersecurity budget as organizations struggle with identity and access management (IAM), customer identity and access management (CIAM), and cloud infrastructure entitlement management (CIEM) in their desire to improve the overall user experience.

IAM Trends

An organization’s digital identities have become increasingly complex—so much so that over 60% of enterprises currently rely on managed service vendors, professional services, or both just for their IAM needs. This complexity is compounded by the distributed responsibility for diverse types of identity, including customers, workloads, third parties, and employees, who may each have different teams managing their identities for their respective use cases (see Figure 1).¹

Figure 1. Primary Owner of Identity and Access Management Programs

<table>
<thead>
<tr>
<th>Which of the following has primary responsibility for these different areas of your identity and access management programs? (Percent of respondents)</th>
<th>IT</th>
<th>Security</th>
<th>HR</th>
<th>Multiple groups with equal responsibility</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud infrastructure entitlement management (N=240)</td>
<td>55%</td>
<td>17%</td>
<td>8%</td>
<td>20%</td>
<td></td>
</tr>
<tr>
<td>Identity-as-a-service (N=229)</td>
<td>51%</td>
<td>19%</td>
<td>10%</td>
<td>18%</td>
<td></td>
</tr>
<tr>
<td>Federated identity and single sign-on (SSO) access management (N=266)</td>
<td>50%</td>
<td>21%</td>
<td>12%</td>
<td>17%</td>
<td></td>
</tr>
<tr>
<td>Multifactor authentication (N=285)</td>
<td>49%</td>
<td>25%</td>
<td>6%</td>
<td>19%</td>
<td></td>
</tr>
<tr>
<td>Privileged access management (N=191)</td>
<td>46%</td>
<td>23%</td>
<td>9%</td>
<td>21%</td>
<td></td>
</tr>
<tr>
<td>Identity risk services (N=202)</td>
<td>45%</td>
<td>26%</td>
<td>9%</td>
<td>19%</td>
<td></td>
</tr>
<tr>
<td>Third-party risk services (N=160)</td>
<td>44%</td>
<td>21%</td>
<td>12%</td>
<td>23%</td>
<td></td>
</tr>
<tr>
<td>Identity governance and administration (N=231)</td>
<td>43%</td>
<td>24%</td>
<td>12%</td>
<td>21%</td>
<td></td>
</tr>
<tr>
<td>Customer identity and access management (N=274)</td>
<td>42%</td>
<td>18%</td>
<td>13%</td>
<td>25%</td>
<td></td>
</tr>
<tr>
<td>Secrets management (N=165)</td>
<td>39%</td>
<td>30%</td>
<td>8%</td>
<td>22%</td>
<td></td>
</tr>
<tr>
<td>Identity proofing, verification, and affirmation (N=241)</td>
<td>34%</td>
<td>30%</td>
<td>14%</td>
<td>22%</td>
<td></td>
</tr>
</tbody>
</table>

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

¹Source: Enterprise Strategy Group Complete Survey Results, Securing the Identity Perimeter with Defense in Depth, June 2022. All research in this white paper was taken from this complete survey results set, unless otherwise specified.
Identity governance and administration (IGA) provides visibility, separation of duties, role management, attestation, analytics, and reporting to traditional identity administration activities, including account, credential, user, and device provisioning and management.

These activities have become more visible and more important as workloads shift to the cloud, and organizations now depend on hundreds of homegrown and commercial SaaS and cloud apps, resulting in many silos of identities. Since each app has a different concept of access and authorization, oversight of identities and access activity throughout the organization becomes difficult.

A recent research survey by TechTarget’s Enterprise Strategy Group (ESG) that looked at securing identities demonstrates the evolution of how enterprises view identity management, from pure IT operations to improving security and efficiency. Some key findings include:

- Privileged access management (PAM) is growing in popularity and is one of the top five IAM tools used by 90% of respondents. PAM was noted particularly for increasing security without increasing user friction and helping with compliance and regulatory obligations.

- Single sign-on (SSO), in a similar fashion, also increases security, reduces friction, improves the overall user experience, and increases compliance, which is why a majority of organizations now mandate SSO.

- IGA efficiency gains are coming from integration with IT services and applications, as almost two-thirds (64%) are integrating IGA with IT help desk ticketing systems, customer service support management systems, asset management systems, software licensing systems, and other IT services and applications.

Identity Security Challenges

Research by Enterprise Strategy Group (ESG) highlighted the importance of securing identities. Nearly half of organizations (46%) have suffered a breach due to identity-related threats, 36% of respondents have suffered a breach due to permission-related threats, and 37% have suffered a breach due to workload/model deployment related threats.

Because applications are distributed across multiple IT on-premises, public cloud, and software-as-a-service environments, organizations end up with multiple silos of identity and many organizations have multiple identity records for a single individual or entity. Multiple identity records mean there may be no single source of truth, individuals may be given improper—and often too permissive—access privileges, and the risk of attack rises as some records may not be properly secured.

The lack of a consolidated, optimized identity solution is also frustrating to organizations, with many dependent on numerous SaaS or on-premises identity management solutions to manage the sprawling and ever-growing set of business-critical applications. This is why organizations are expanding their use of IGA to cover new use cases: over the next 12-18 months, 54% expect to expand use of their existing IGA; 54% expect to extend IGA to support more cloud, hybrid, and SaaS apps; 50% expect to expand their IGA purview to include workload identities; and 50% expect to integrate IGA with business and process automation.

As organizations deploy more applications, determining the correct level of access for every identity becomes more challenging. Thus, admins often over-permission identities under the mistaken assumption that too much privilege is better than preventing work from getting done due to lack of access, despite the increased risk of attack. This practice increases risk as over-permissioned and under-used identities feature prominently in breaches and attacks.
More applications distributed in more environments increases complexity and the administrative workload. Even small organizations can be overwhelmed by the volume of identity-related tasks, and as complexity and scale increase, the need for automation becomes increasingly clear. Thus, a large majority (88%) of respondents said that their organization is likely to enable automated remediation and removal of excessive, unneeded, and unused permissions and entitlements to help reduce the attack surface.

Solving these identity issues has been a persistent thorn in IT’s side. Many organizations have tried several times with a variety of different solutions and now find themselves five years into a three-year project to address these issues with no end in sight and without having achieved their desired outcomes.

These challenges highlight the growing need to put identity where it belongs: on a business workflow platform.

**The Rise of Platforms**

Spreadsheet and email-driven identity solutions are haphazard, slow, impossible to manage and govern, and prone to human error. Using multiple identity applications often results in overlapping functionality that requires duplicate efforts, increasing resource dependencies and costs and the probability of governance gaps while frustrating users and IT teams alike. For these reasons, medium to large organizations prefer automating identity-related tasks just as these organizations automate other IT management workflows.

The current state of the art solution for business process automation is a digital businesses platform. Organizations are using business platforms to digitize, connect, and automate siloed processes to optimize workflows across IT, human resources, security operations (SecOps), applications, and more. With a business platform, all management operates on a single data plane—a single source of truth—avoiding duplication and fostering cooperation and communication among departments, people, and activities. Business platforms eliminate latency issues and help ensure all functionalities and capabilities are available in a single solution, removing the need for context switching to manage various aspects of the environment.

Identities are key fundamental components of the IT environment, and every application and system, whether on-premises or in the cloud, relies on identities for controlling access. Thus, IGA needs to live in the same place that organizations manage the rest of their environment, and it’s now time to add IGA to business platforms so that identity management can integrate with other management activities and take advantage of the benefits of business platforms.

Deploying IGA as a native application on a business platform can simplify operations, increase efficiency, and improve the overall user experience by providing a common look and feel and operational workflow for all environment management activities. This facilitates IGA expansion to support cloud, hybrid, and SaaS workload identities and integration with business process automation.

IGA running on a business management platform also helps the organization consolidate identity silos with the goal of evolving to a single source of truth for identity information, which helps increase accuracy, reduce workloads, and enable organizations to leverage automation to increase security and efficiency.

**Clear Skye and the ServiceNow Platform**

Because, at its core, identity secures workflows, and business platforms are where workflows live, Clear Skye has built an identity governance application on the ServiceNow Platform, a major platform that operates as a single, unifying foundation for digital business. This enables ServiceNow to provide enhanced identity lifecycle management and governance over a broad range of vertical markets and industries.
Clear Skye reduces security risks by ensuring organizations can implement the principle of least privilege access, whereby only the right people have the right access to the right applications at the right time to do their jobs, no more and no less. Using a data warehouse specifically designed for identity that tracks profiles, accounts, entitlements, roles, requests, approvals, identity tasks, and the relationship between all of these components enables organizations to consolidate all identity data into a single source of truth. With this unified view of identities, organizations can extend and expand IGA to cover all identities throughout the enterprise.

The combination of Clear Skye and ServiceNow provides customized access request capabilities tuned to existing approval workflows, eliminating the need for additional training since users manage identities using the same user interface (UI) and ServiceNow workflows they use to manage other parts of the environment.

Delivering Clear Skye as a ServiceNow application also simplifies and automates entitlement management for users joining, moving, or leaving the organization, and automation can consider organization, department, role, job functions, and other factors. The inclusion of IGA Flow Spoke enables new and existing workflows to benefit from identity actions in a no code/low code environment, where workflows are quickly and easily changed without needing ServiceNow developers to invest time and effort developing custom code.

With Clear Skye, there is no need to waste a lot of time repeating previous efforts since the familiar ServiceNow Platform makes it easy for admins to connect to IT and HR services on-platform. Other benefits of Clear Skye on ServiceNow include:

- **Faster time to value**—organizations can see the results of deploying Clear Sky on ServiceNow immediately. No forklift upgrades are needed, and Clear Skye eliminates the need for complicated onboarding and training of admins since users already know how to use ServiceNow applications.

- **The elimination of identity silos**—which reduces duplication, over-permissioning, and the attack surface enterprise-wide and helps organizations correctly diagnose and remediate errors as they arise.

- **A consistent user experience**—employees can focus on their tasks at hand and not have to learn a new application, user interface, or methodology when managing identities.

- **Lower overall costs**—increasing utilization by adding additional solutions to the ServiceNow Platform reduces acquisition costs and the administrative overhead of managing multiple platforms while increasing the efficiency of IT staff, ensuring highly trained specialists can use their knowledge to focus on the most important tasks.

- **Integrations**—Clear Skye seamlessly links to ServiceNow Integration Hub with instant connectivity to nearly 100 other business applications, enabling admins to expand the purview of IGA to the organization’s critical business applications.

- **Customizable User Interfaces**—admins can leverage the Service Portal to create UIs that are easily understandable by ServiceNow LOB users. These updated UIs provide easier ways to use Clear Skye and reduce the number of support requests to IAM teams.

- **Reporting**—Clear Skye leverages ServiceNow’s reporting framework that offers the capability to visualize different metrics and time series data via easy-to-read pie charts and graphs and provides the ability to create custom reports on the relationships between identity and access.
The Bigger Truth

Historically, managing identities was the responsibility of HR—when an employee joined or left the organization, HR created the appropriate identity. As the IT infrastructure expanded, moved to the cloud, and became more complex, responsibility for identity management shifted to IT. And with the rise of ransomware and other identity-related cyber-attacks, organizations are concluding that identities are intimately intertwined with security. Thus, in many organizations, multiple groups share responsibility for managing identities and using manual methods or multiple overlapping identity solutions is fraught with many issues.

Organizations are now shifting to an integrated and unified business platform for multiple groups to manage the IT environment, on-premises and cloud apps, and business functions, such as HR. Integrating the management functions into a single platform reduces human errors, increases efficiency, enables automation, reduces administrative workload, and lowers costs. Thus, it’s time to enable IGA to realize these benefits by adding identity management to the platform.

Clear Skye has done just that, building an IGA solution on the ServiceNow Platform. Using Clear Skye IGA, organizations can rapidly coalesce identity information into a single source of truth while leveraging the consistent user experience, automation, and built-in connectors to enhance and expand IGA throughout the organization’s IT environment. Organizations looking for faster time to value in securing, managing, and governing all identities in their enterprise while lowering overall costs and increasing efficiency should take a serious look at Clear Skye IGA.