Enterprise Strategy Group™

TECHNICAL VALIDATION

Simeio Identity Orchestrator

Improving Identity Security Posture and Regulatory Compliance

By Alex Arcilla, Principal Analyst – Validation Services
Enterprise Strategy Group

May 2025

Contents

Introduction

This Technical Validation from Enterprise Strategy Group evaluates Simeio Identity Orchestrator. We specifically evaluate how this platform can help organizations improve their identity security posture.

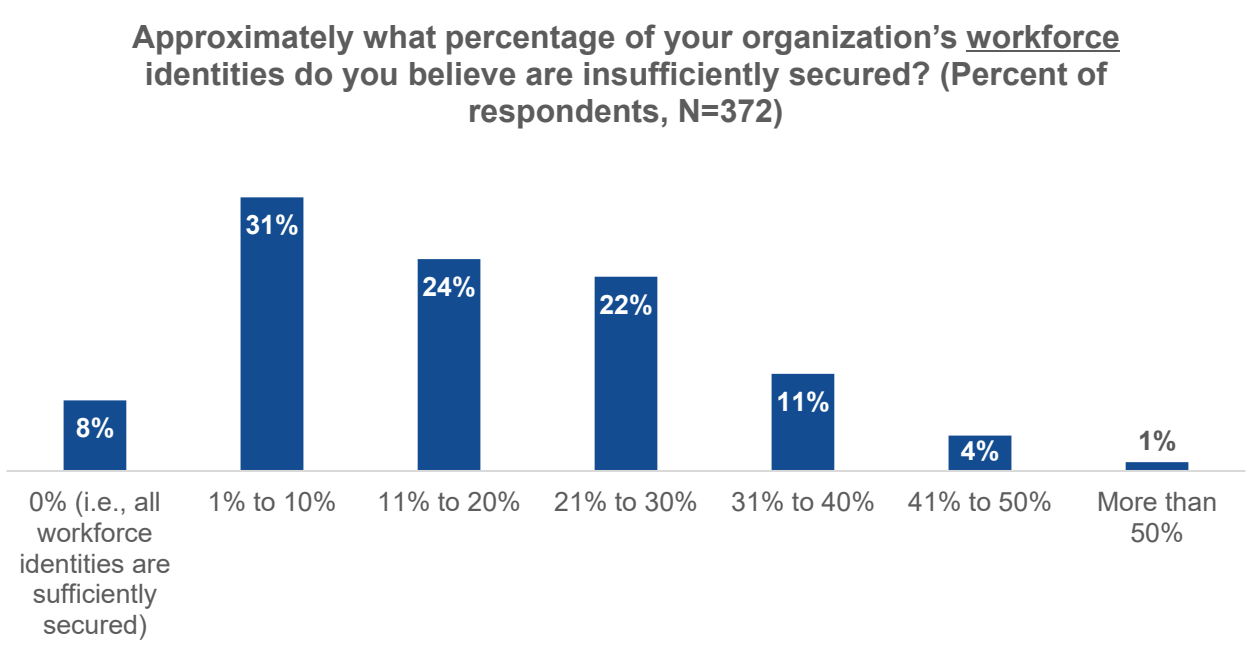
Background

Organizations can experience employee growth and/or an increase in the number of applications used due to events such as mergers and acquisitions or lines of business implementing applications without going through IT. A common result is that the number of identities is bound to increase. According to Enterprise Strategy Group research, 57% of organizations expected the number of workforce identities to increase between 11% and 40% over the next year.[1]

Part of this increase is due to the presence of multiple workforce identities for individuals, as experienced by 89% of organizations surveyed. This is likely occurring due to organizations implementing multiple identity and access management (IAM) tools, which creates multiple identity silos.

Unfortunately, the increase in workforce identities have opened unintended gaps in an organization's identity security posture. The same research showed 57% of organizations believed that between 11% and 40% of their current workforce identities are insufficiently secured (see Figure 1).

Figure 1. Percentage of Insufficiently Secured Workforce Identities



Source: Enterprise Strategy Group, now part of Omdia

Securing user access to business applications is necessary as a first line of defense from bad actors infiltrating an organization. Yet, inconsistencies across multiple identities held by a single identity can easily be exploited. While organizations have implemented numerous identity security tools to mitigate these inconsistencies, 72% of organizations agreed that deploying these tools has taken much longer and/or been more complex than initially

[1] Source: Enterprise Strategy Group Complete Survey Results, *The State of Identity Security*, May 2024. All Enterprise Strategy Group research references and charts in this technical validation are from this report.

planned. Unfortunately, such obstacles prevent organizations from closing security gaps that emerge in light of multiple workforce identities. Additionally, organizations cannot realize how these siloed tools can complement each other, as each has been designed for a specific purpose.

Simeio Identity Orchestrator

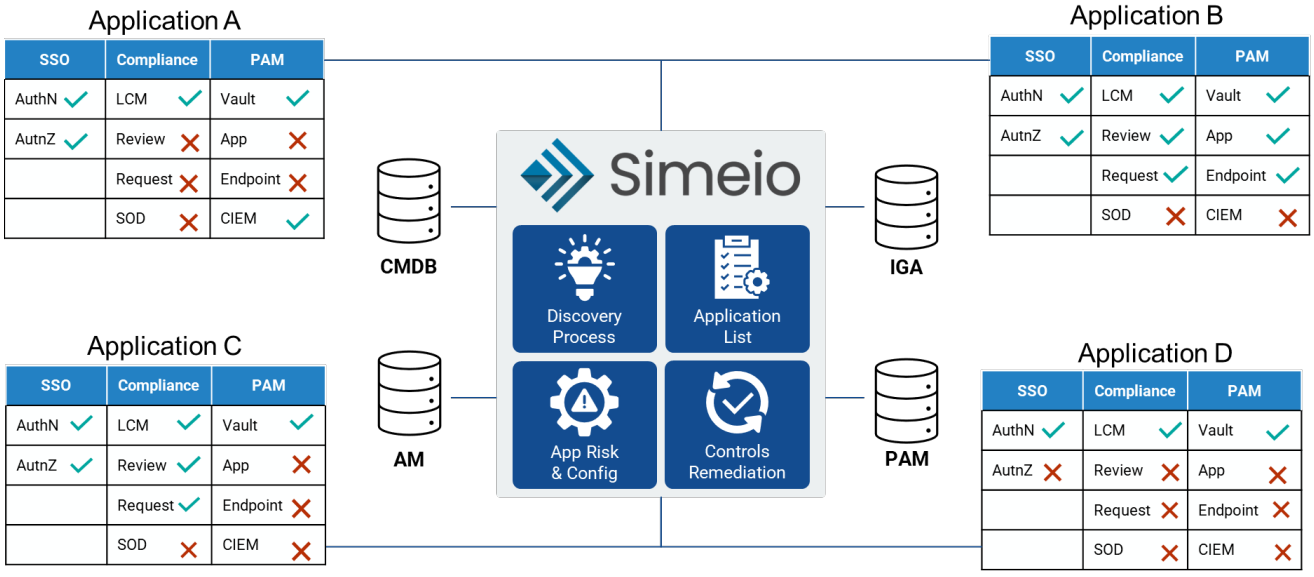
The Simeio Identity Orchestrator (IO) is designed to help organizations gain the necessary visibility and control over all existing and new applications and identities. With Simeio IO, organizations can bolster their identity security posture and regulatory compliance.

Delivered via SaaS, the platform integrates and unifies policies, controls, and processes across the following identity security tools (see Figure 2):

- **Access management** (AM) for managing authentication and authorization of users and devices so that they are allowed access to specific data, applications, and/or IT infrastructure.
- **Identity governance and administration** (IGA) for automating access to applications and data by assigning the proper roles and access level without incurring security and compliance risk.
- **Privileged access management** (PAM) for governing how and when special access to applications, data, and IT infrastructure is given beyond that of a standard user. This assumes that all users are initially assigned the "privilege of least access."

With Simeio IO, organizations can pinpoint and reconcile controls related to AM, IGA, and PAM against the identities managed by individual IAM tools and technologies. Simeio's platform can easily scale to manage multiple identities as the number of applications and assets grows to meet evolving business needs.

Figure 2. Simeio IO



Source: Simeio and Enterprise Strategy Group, now part of Omdia

All capabilities of the Simeio IO platform are accessible via a centralized interface. Organizations no longer need to switch between IAM tool-specific interfaces when establishing and managing identify security. The integration of capabilities from individual identity security tools unlocks value, as organizations can pinpoint identity misconfigurations and identity hygiene issues more quickly. The centralized visibility can also help organizations continuously audit their environment and monitor regulatory compliance.

With automated and self-driven workflows, Simeio IO simplifies how organizations inventory applications and assets used across organizations and manage the various identity controls across applications and infrastructure. Application and asset owners can review and remediate identity security control gaps via self-service capabilities, thus increasing operational efficiency while decreasing security and compliance risk.

Enterprise Strategy Group Technical Validation

Enterprise Strategy Group validated how organizations can fortify their identity security posture with Simeio IO. We specifically reviewed how Simeio can increase operational efficiency via self-service and automated workflows, reduce access risk, and discover additional areas of risk via AI-driven analytics and recommendations.

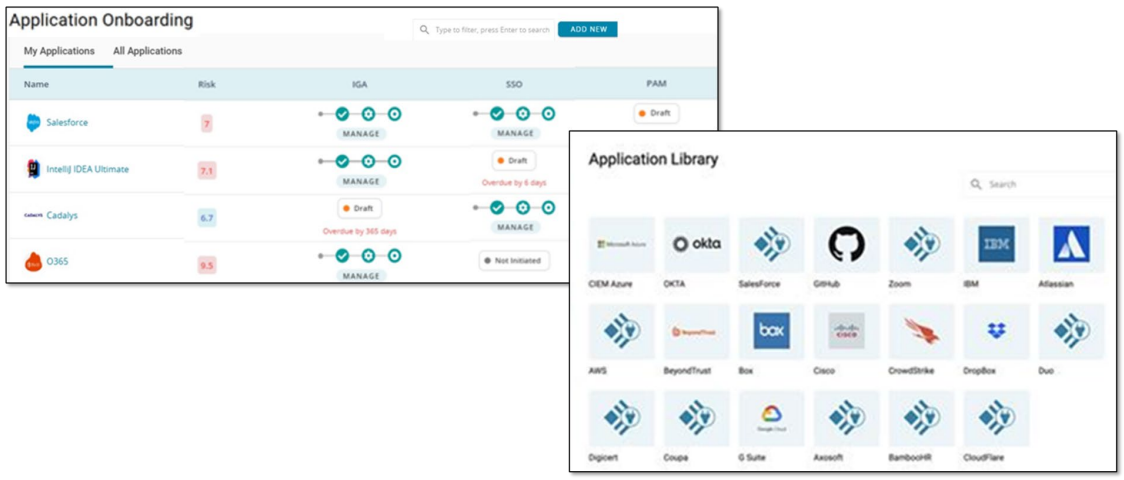
Increasing Operational Efficiency When Inventorying Applications

Tracking all applications used within an organization is typically a tedious and time-consuming process. The inefficiency hampers organizations from determining which identity security controls should be in place for these applications. Simeio IO can reduce the time spent inventorying applications and pinpoint security controls to be implemented. Time to onboard applications decreases, leading to reduced operational expenses.

Enterprise Strategy Group Analysis

To onboard an application, Enterprise Strategy Group navigated to the page listing onboarded applications in Simeio IO, the Application Library (see left of Figure 3). We clicked on the “Add New” button and manually created an application for monitoring the status of identity security controls in place across three domains: AM, IGA, and PAM. We could also use available plugins representing IAM tools and technologies that are integrated with Simeio IO to automatically ingest controls already in place.

Figure 3. Onboarding New Application and Its Identity Security Configuration



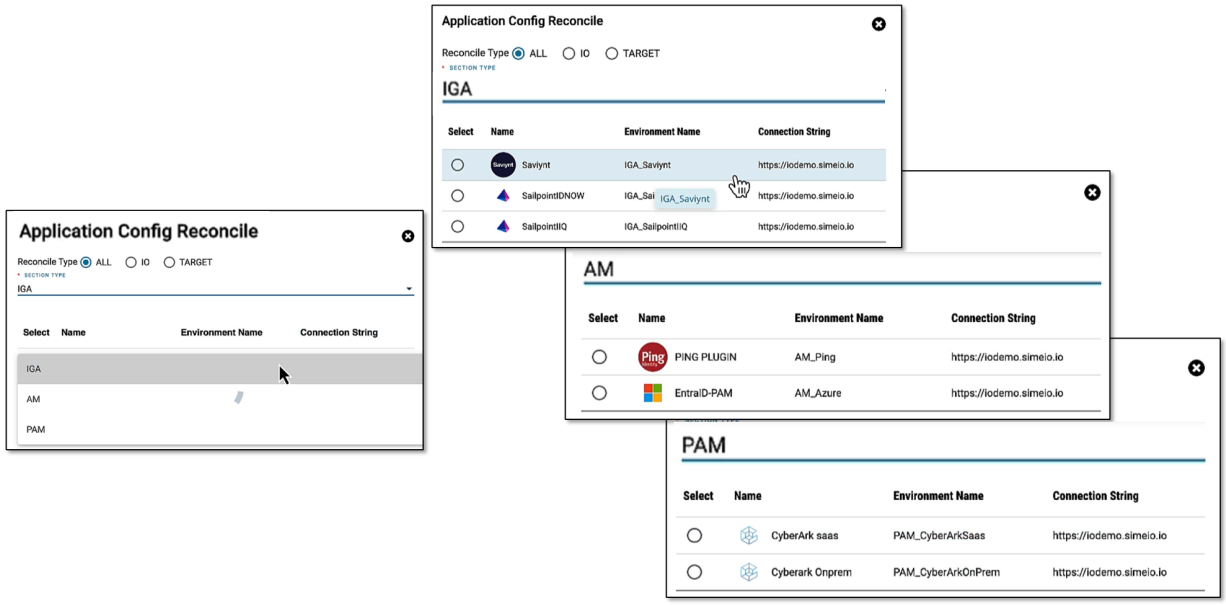
Source: Enterprise Strategy Group, now part of Omdia

An inventory of applications can also be onboarded automatically by connecting to an existing configuration management database, which contains application details or existing AM, IGA and PAM systems.

We proceeded to reconcile the application configuration profiles by discovering which controls are in place governing AM, IGA, and PAM. From an existing list of Application Reconciliation jobs, we clicked on the button “New Job” to begin this process.

For each domain, we selected the source(s) of application configuration details that would input the security controls used. Separate pages were available to select domain-specific details (see Figure 4).

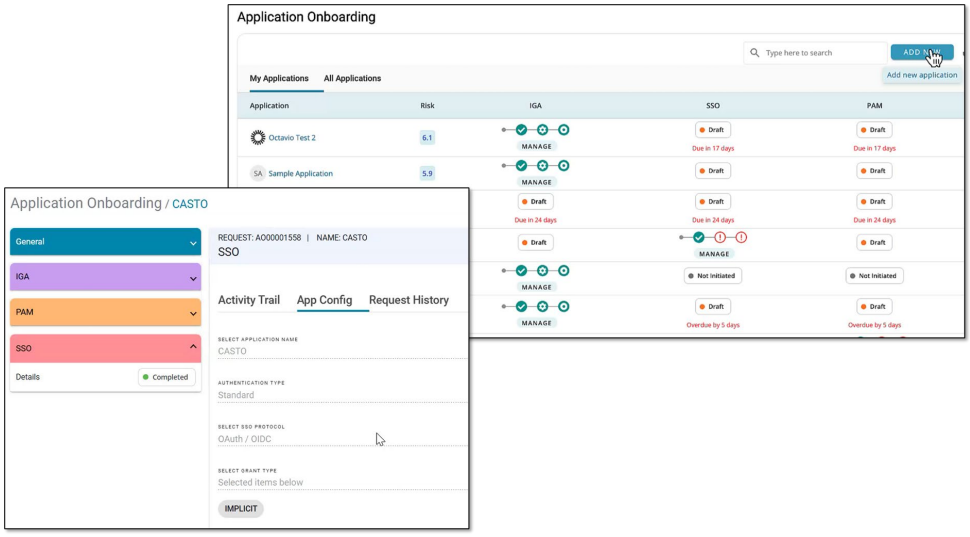
Figure 4. Reconciling Application Configurations for AM, IGA, and PAM



Source: Enterprise Strategy Group, now part of Omdia

Once an application was discovered, Simeio IO displayed its onboarding status and showed controls already in place (see Figure 5). Each onboarded application revealed if all necessary controls were in place for each domain (IGA, AM, PAM). "Draft" status indicated that an application was in the process of being manually inputted, while completed green circles denoted that all application controls were completed. Due dates and overdue notices were also displayed for reminding end users to fill in missing security controls (e.g., if controls are needed to prepare for an internal audit).

Figure 5. Self-driven Workflows for Completing Application's Identity Security Configuration



Source: Enterprise Strategy Group, now part of Omdia

As we navigated through Simeio IO, Enterprise Strategy Group took note of the built-in self-service workflows. We observed how the workflows simplified the onboarding of new applications (like the one we manually created) along with existing identity security controls. Application owners would not need to wait for a centralized IAM program team to complete these tasks and could take immediate action to establish the needed identity security controls.

We also saw how the predefined questions assisted in completing the application's identity security configuration. Questions were presented in business-friendly terms, regardless of the underlying IAM tool or technology supporting the application. This demonstrated how Simeio IO was designed to translate answers into parameters that the underlying tool or technology needs to establish AM, IGA, and PAM controls.

The simplicity exhibited by Simeio IO also revealed that organizations no longer need to rely on subject matter experts of IAM tools and technologies to perform this work. Application owners are empowered to establish a baseline of identity security control.

Why This Matters

Establishing solid identity security across an organization first requires a complete application inventory and the current status of their AM, IGA, and PAM controls. Completing this task can be tedious and time-consuming, given the number of existing applications and the separate tools that are used for identity security, specifically for AM, IGA, and PAM.

Enterprise Strategy Group validated that Simeio IO can greatly simplify how organizations can onboard applications and register the AM, IGA, and PAM controls already in place. We observed how quickly we could input an existing application, assess the completeness of the supported identity security domains, and flag the work to be completed by application owners. With Simeio IO, organizations can reduce the time and cost of inventorying applications, thereby reducing the time to assess and resolve security gaps.

Reducing Identity Security Risk via Centralized Visibility and Remediation

While organizations may believe that they have secured access to all applications, there can be overlooked controls to implement. Unfortunately, establishing this view is difficult to compile and verify, especially when relying on individual tools and manually driven methods. Once a complete application and asset inventory is established, organizations can assess their identity security posture. With centralized visibility across all applications, Simeio IO can assess this posture more quickly and efficiently than cross-referencing multiple single-purpose identity tools. Using Simeio IO can reduce the time to pinpoint gaps in an organization's identity security posture.

Enterprise Strategy Group Analysis

Enterprise Strategy Group first navigated to the webpage showing the current status of an organization's identity security program posture (see Figure 6).

Figure 6. Status of Current Identity Security Program Posture

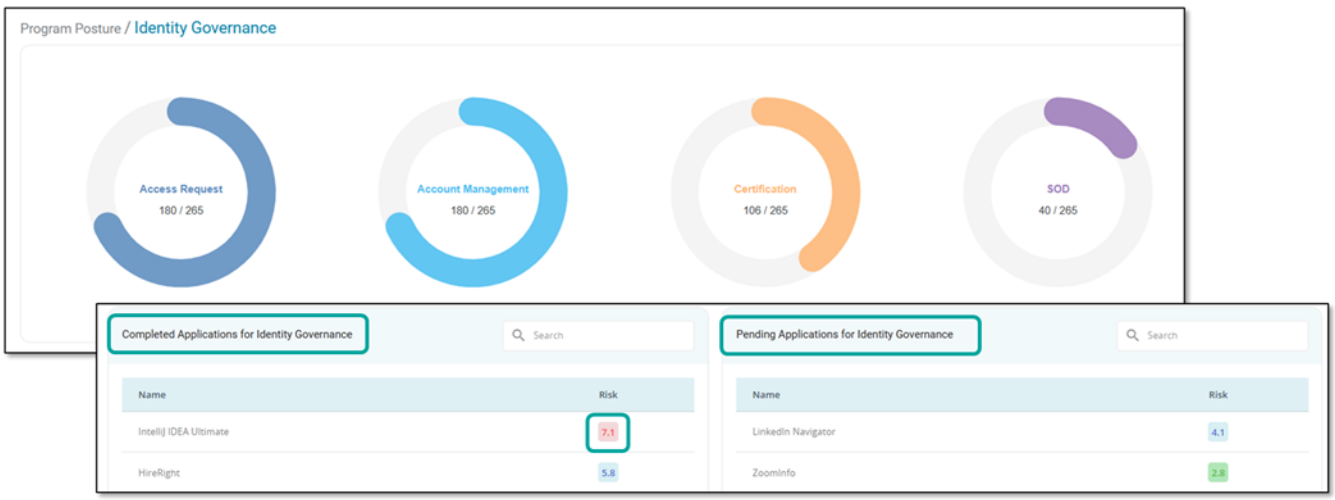
Source: Enterprise Strategy Group, now part of Omdia

Of the 265 onboarded applications, this dashboard noted the number of applications that had security controls in place for each domain. Simeio IO tracked:

- AM controls such as single sign-on and two-factor authentication.
- IGA controls such as access request, certifications, and segregation of duties.
- PAM controls such as vaulting and application security.

We then drilled down into each domain and saw controls already enabled for individual applications, along with a risk score for each completed application and pending applications (i.e., those waiting for all controls to be enabled), as show in Figure 7. The risk score assessed an application's risk, factoring in the criticality of the application to the business and the data the application contains. For example, an application that accesses personally identifiable information (PII) would be scored higher. Scoring would help an organization to prioritize if an application needs more attention when securing its identity posture.

Figure 7. Detailed View of Identity Governance Controls in Place

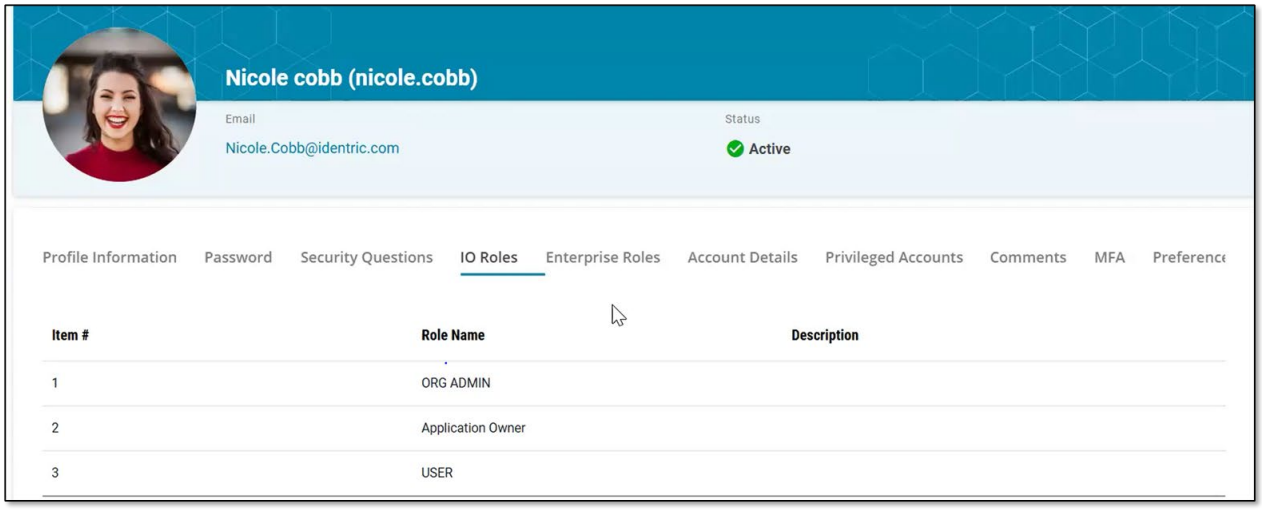


Source: Enterprise Strategy Group, now part of Omdia

These views can be used by both IAM teams and application owners to track their progress of establishing all AM, IGA, and PAM controls.

Centralized visibility is also achieved via showcasing an individual user's access across all applications and devices (see Figure 8). Each tab displayed details such as assigned roles defined in the platform and roles within the organization, along with individual application accounts and privileged accounts.

Figure 8. Identity Convergence for an Individual



Source: Enterprise Strategy Group, now part of Omdia

Why This Matters

Without a complete view of identity security posture, organizations cannot locate the security gaps they need to close. Yet, obtaining this view becomes time-consuming and cumbersome when needing to gather and cross-reference data from multiple identity security tools.

Enterprise Strategy Group validated that Simeio IO provides the centralized visibility that organizations can use to quickly identify gaps within their identity security posture. We observed that Simeio IO summarized the number of applications that fulfilled each security control related to AM, IGA, and PAM. For applications that had yet to satisfy all controls associated with any domain, we could drill down to a specific application and determine the remaining controls to be established. Simeio IO could also provide visibility into individual users, specifically their access to applications and privileged access.

Establishing Strong Identity Hygiene With AI-based Analytics

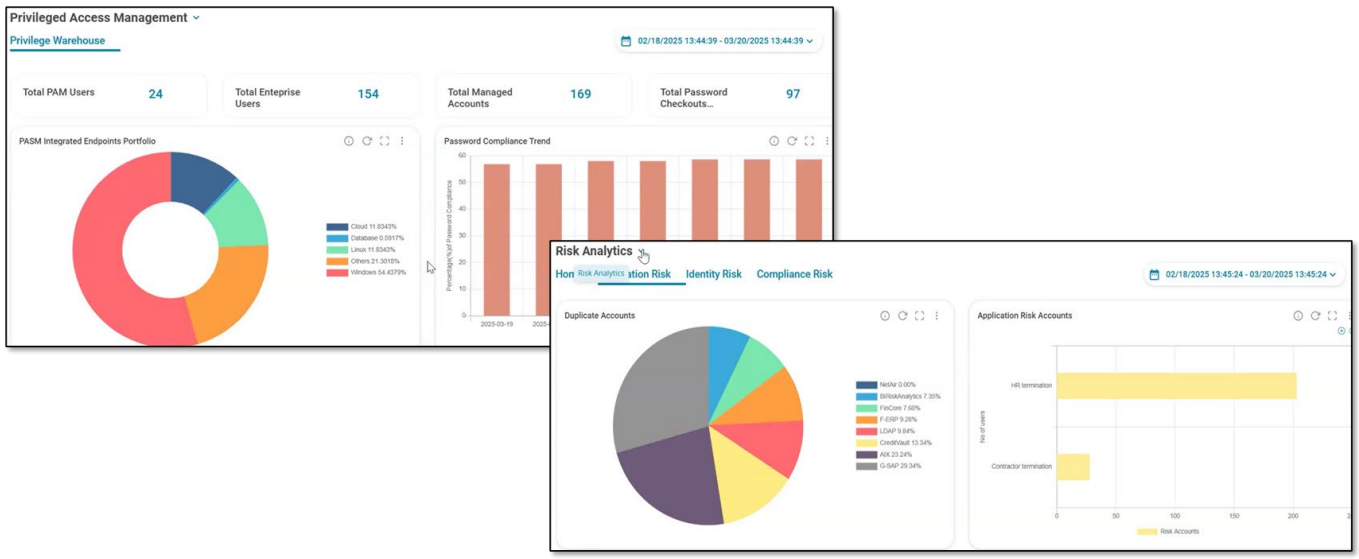
With Simeio IO, organizations can generate insights with data integrated across the AM, IGA, and PAM domains. Analyzing this integrated data can provide insights into previously overlooked identity security gaps as well as establish strong identity hygiene, beyond what Simeio can identify with its applications inventory and centralized visibility.

Enterprise Strategy Group Analysis

Enterprise Strategy Group first viewed the analytics focusing on each domain. The top left of Figure 9 displays statistics related to PAM, such as password compliance over time. Using this domain view can help an organization monitor the effectiveness of PAM security controls to date.

Because Simeio IO collected data from the underlying identity security tools and technologies used within an organization, we could generate analytics using the integrated data (see bottom right of Figure 9). For example, an organization could calculate statistics highlighting previously overlooked gaps, such as duplicate accounts (e.g., those that bad actors could exploit) and departments with accounts presenting application risks (e.g., containing sensitive employment data). With Simeio IO, all analytics and related views were customizable.

Figure 9. Analytics Revealing Additional Security Gaps



Source: Enterprise Strategy Group, now part of Omdia

Why This Matters

Generating analytics using data from individual IAM tools and technologies can provide insights into identity security gaps and identity hygiene issues. However, analyzing data across these tools and technologies can uncover previously overlooked gaps, thus highlighting remediation opportunities.

Enterprise Strategy Group validated that Simeio IO can generate insights into identity security gaps beyond the platform's application onboarding capability and centralized visibility. We saw how Simeio IO can perform analytics using data specific to the AM, IGA, and PAM domains or data integrated from the IAM tools and technologies already used within an organization.

Conclusion

Bolstering an identity security posture is a given in today's business climate, as employees access multiple applications and devices. Organizations have responded by implementing a combination of identity security tools and technologies, yet their coverage is inconsistent across applications and devices, leading to control gaps and hygiene issues. Unfortunately, the "patchwork" coverage leads to identity security gaps and vulnerabilities that can be easily exploited. Uncovering exactly where these gaps lie can be hindered by cross-referencing data gathered from individual IAM tools and technologies along with manually inventorying assets and applications.

On the other hand, Simeio IO can help organizations bolster their identity security posture while eliminating the need to implement multiple point tools and manual workarounds. Simeio IO has been designed to simplify the discovery and remediation of identity security gaps specifically related to AM, IGA, and PAM. Organizations using Simeio IO can onboard applications, download security controls that are already installed, and highlight other controls to be implemented. Operational efficiency increases while mitigating outstanding security risk.

Throughout our evaluation, Enterprise Strategy Group validated that organizations can use Simeio IO to:

- Reduce the time and effort typically required to inventory existing applications and assets and resolve multiple identities assigned to individuals.
- Locate existing gaps in controls that should be in place to control AM, IGA, and PAM, without the need to coordinate findings from individual IAM tools and technologies.
- Discover other security gaps via AI-based analytics of integrated data that can be overlooked.

Simeio IO can help to remove the complexity encountered when establishing and fortifying an organization's identity security posture. Based on our observations, Enterprise Strategy Group recommends looking closely at Simeio IO for help efficiently uncovering and closing identity security gaps.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com