WHITE PAPER

Strengthening Identity Security Posture With Identity Orchestration

Overcoming Silos to Improve Identity Security

By Todd Thiemann, Senior Analyst
Enterprise Strategy Group

April 2025

This White Paper from Enterprise Strategy Group, now part of Omdia, was commissioned by Simeio and is distributed under license from TechTarget, Inc.

Contents

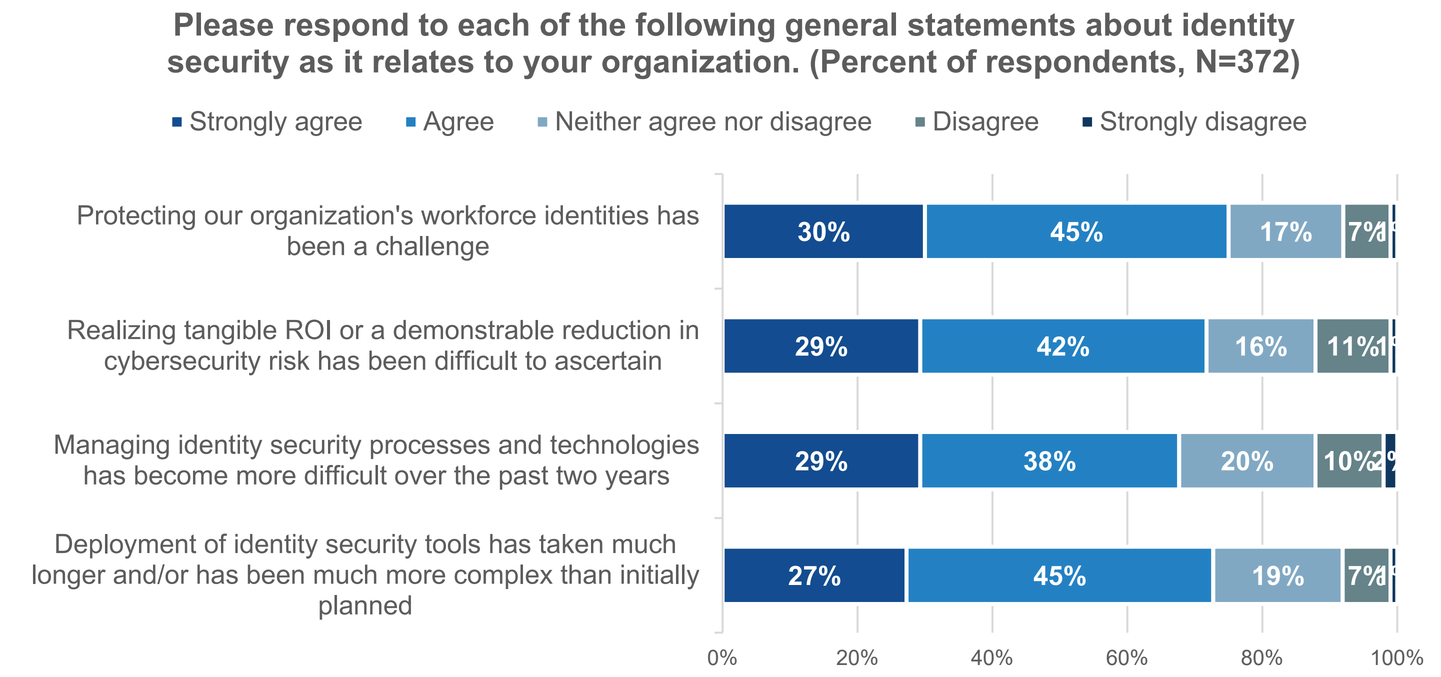
Executive Summary

Enterprise identity security teams today navigate a collection of disparate identity and access management (IAM) tools that provide key identity services, including identity governance and administration, access management, and privileged access management (PAM). Tasks like onboarding business applications can become complex and burdensome as teams maintain consistency and take manual steps across their siloed tools. Identity orchestration across IAM services provides a path to accelerate and scale application rollouts while ensuring compliance, controlling risk, and reducing the burden on enterprise security teams and application business owners.

The Enterprise Identity Solution Silo Problem

Identity teams are highly motivated to secure the enterprise identities and ensure that the right identities have the right access to enterprise data, applications, and infrastructure, but their task has grown more challenging. They are finding that protecting workforce identities is challenging, demonstrating ROI and risk reduction is problematic, and managing identities has become more difficult over the past two years (see Figure 1).[1]

Figure 1. Identity Security Across Tool Sets Is Challenging



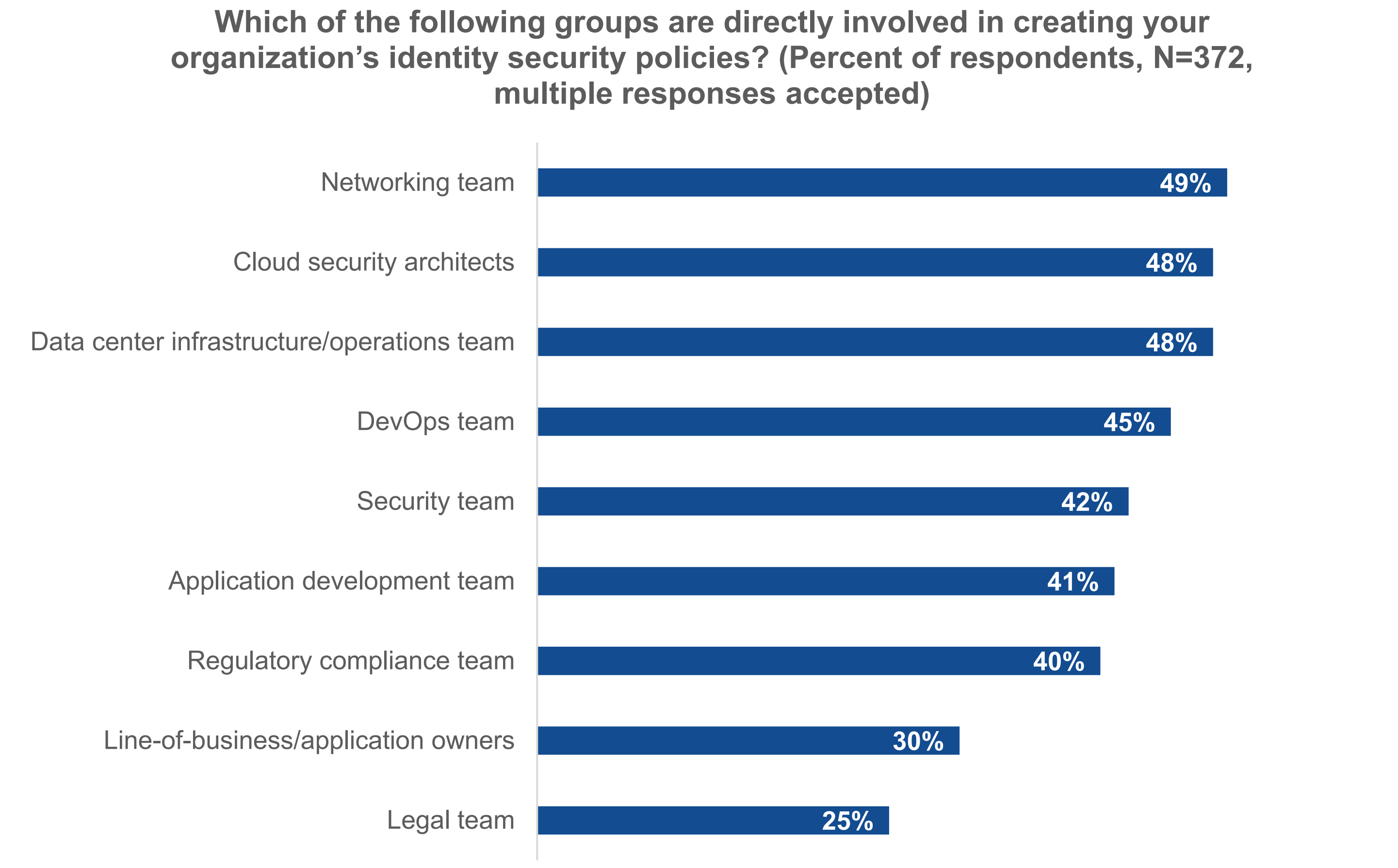
Source: Enterprise Strategy Group, now part of Omdia

The pain that identity security teams face has been increasing. When asked about the ability to roll out tools, 72% of respondents to research from Enterprise Strategy Group, now part of Omdia, indicated that they either agree or strongly agree that deploying identity security tools has taken much longer and/or has been much more complex than originally planned. Additionally, 67% agreed or strongly agreed that managing identity security processes or technologies has become more difficult over the past two years.

[1] Source: Enterprise Strategy Group Research Report, *The State of Identity Security*, July 2024. All Enterprise Strategy Group research references and charts in this white paper are from this report.

Identity security teams typically employ a portfolio of IAM tools to get their jobs done. This identity technology stack requires coordination across a variety of constituents to establish policies and roll out identity security functionality (see Figure 2). The variety of tools used across these constituents contributes to a cumbersome process for rolling out support for new business applications in a way that controls risk and maintains compliance.

Figure 2. Identity Security Policies Are a Team Sport



Source: Enterprise Strategy Group, now part of Omdia

While the concept of an uber identity security platform is an attractive concept, today's reality is that enterprises have typically deployed a mix of tools across different identity domains. Enterprises have gradually deployed distinct technologies to solve their specific business challenges, and that evolution has resulted in multiple identity security silos.

Identity security services include access management, identity governance and administration, PAM, and cloud IAM. Services might consist of a single tool in each identity security area, multiple tools inherited as a result of mergers and acquisitions (M&A), or one tool for cloud identity and another tool for on-premises requirements.

Enterprises are judicious in deciding on the tooling they use and have spent considerable time, money, and resources to customize and deploy their identity tool set. But the different identity services need to be coordinated to enforce security policy, maintain visibility, and facilitate threat detection and response. That coordination can consume precious time and resources.

The challenge of rolling out new applications continues to cause consternation and drain resources for identity teams. While each domain of identity security may individually function well, gaps emerge between silos that cause security and compliance issues and burden security teams with coordination activities.

Enterprise IAM programs are hindered by manually driven policies between silos and separate management. For example, not all access management users have credentials vaulted in a PAM system, leaving a key security control not fully leveraged.

Another more nuanced example lies in how organizations measure the ROI and impact from access management and PAM projects. Access management in the form of single sign-on (SSO) and multifactor authentication (MFA) are broadly applicable projects affecting all application users—possibly hundreds or thousands of users. The benefits of such projects include reducing password resets, help desk tickets, and authentication-related friction that can deliver a measurable ROI in the same quarter. This makes business justification for access management relatively straightforward, with the improved productivity being readily apparent.

In contrast, PAM is typically deployed to a subset of applications and infrastructure, and a subset of users often comprised of IT and application administrators. This can result in a lack of visibility if an application secured with access management controls is secured with PAM controls that may include appropriate access. While PAM is a critical control for mitigating cyber-risk, its narrow adoption makes it harder to justify in terms of a financial ROI.

The result of this dynamic is a potential security gap, with organizations investing in access management for broad usability but not applying the same rigor to PAM. This can leave important privileged accounts and service credentials unprotected. The issue is not just about cost, but rather about recognizing that the risk reduction from PAM is as important as the efficiency gains from access management.

Challenges in Bridging Service Silos

Bridging identity services silos poses various orchestration challenges for identity teams, and those challenges can be divided into four main areas.

Inventorying Applications

Enterprises can frequently leverage their existing configuration management database (CMDB) to obtain an inventory of applications. However, CMDBs can be infrastructure-focused with inadequate information about applications. An alternative to using a CMDB is using other tooling like Active Directory or access management tools to understand the application portfolio. Accumulating the app inventory can be challenging due to flux caused by M&A that results in unknown applications or integrating legacy, homegrown applications.

Prioritizing Application Integration

Once the application portfolio is understood, identity teams need to rank and prioritize what apps should be integrated. Prioritization needs to take into account a variety of factors, including security risk, usage frequency, compliance requirements, business objectives, the application user base, decommissioning plans, and resourcing. Teams also need to consider the impact to the enterprise when the availability, integrity, and data confidentiality is compromised.

Onboarding and Identity Controls

Onboarding apps is frequently a cumbersome process without an easy way to establish appropriate controls and configuration across identity, governance, and administration (IGA); access management; and PAM. Identity teams need to coordinate with application owners to properly implement controls. While teams can manually handle a small number of applications, scaling application onboarding to tens or hundreds of apps can prove impossible for even the most talented teams using existing, manual processes. Application onboarding can also prove to be expensive if external consulting and integration services become part of the project.

Maintaining Policy Compliance

Particularly for larger enterprises, maintaining and measuring compliance is required to accommodate internal governance or external compliance requirements. Identity security tools mitigate risk, but compliance is a frequent driver for identity security teams. For example, Sarbanes Oxley compliance requires periodic user access reviews to ensure that access to systems affecting financial records remains appropriate.

Policy compliance activities run the gamut, including:

- Enforcing MFA and measuring how many apps are controlled via MFA.
- Enforcing password rotation.
- Visibility to compromised passwords.
- User access reviews for contractors by the contractor sponsors.
- User entitlement reviews.

However, much of today's reporting can be manual because content and context does not exist across tools.

Identity security teams risk being overwhelmed as they onboard apps and infrastructure, implement identity controls, and try to manually maintain consistency across their tool portfolio. They risk being overwhelmed as the backlog of business applications accumulates and there are not enough resources to coordinate onboarding with application owners and maintenance of the existing portfolio of tools and applications.

Identity Orchestration: Key Factors to Consider

There are multiple factors to consider when determining how to solve the identity security posture challenges across a fragmented identity ecosystem. Following are some of the characteristics to look for in any orchestration solution to overcome this challenge:

- SaaS-based solution consistent with enterprise mandates that enables rapid updates and scalability.
- Consistent coordination across IAM service silos (IGA, PAM, access management).
- Facilitation of rapid app deployment by controlling configuration through the onboarding process to improve time to value.
    - Avoid integrations and professional services costs associated with custom adaptors.
    - Streamline currently manually driven application onboarding tasks through automation and self-service capabilities so application and infrastructure teams can add more value to other areas.
    - The capability to build a common identity process and data fabric.
    - Re-evaluate priorities to see if budget previously spent on integration services can be more productively used elsewhere.
- Achievable visibility and reporting.
    - Improve security posture by highlighting security risks.
    - Facilitate compliance.
    - Improve visibility to inform problem-solving constituents.
- Ability to scale horizontally across the application.

- Understand and quickly ensure remediation of identity control gaps.

While enterprises can achieve these outcomes with manual identity orchestration, a manual approach cannot scale at the rate of applications, identities, and identity transaction data that needs to be analyzed. The manual approach can divert resources from the business objectives of making the enterprise operate more efficiently with reduced risk and improved compliance. Simeio's solution applies machine learning and AI to analyze and provide recommendations, and help teams move beyond the status quo to achieve their goals.

Overcoming Identity Silos: The Simeio Identity Orchestrator

Simeio has focused its technology development efforts on unifying siloed identity tools with a unified identity service orchestration platform.

Simeio Identity Orchestrator (IO) was designed to give identity teams the control, automation, and insights they need without complexity. It recognizes the heterogeneous complexity of today's identity ecosystem and overcomes that challenge with pre-built integrations across IGA, access management, and PAM.

Simeio IO configures various IAM controls, monitors, and integrates by implementing individual IAM platforms for the major IAM service domains—access management, IGA, and PAM. The self-service tool empowers application owners to drive the process and frees up identity teams to do more impactful work. Additionally, Simeio IO controls customization expenses by avoiding additional investments to build identity processes for each application.

Some of the key functionalities that Simeio IO provides include:

- **Streamlining application onboarding and lifecycle management** for every app in the enterprise portfolio by connecting business applications to all identity controls and services across IGA, access management, and PAM. It automates remediation of security control gaps and ensures continuous identity governance by proactively updating IAM configurations.
- **Automating remediation of control gaps** with pre-built templates that provide process consistency and efficiency.
- **Continuous identity control lifecycle management** that updates settings within IAM tools as applications evolve. This approach streamlines identity security processes by maintaining control configuration versions, detecting and notifying on changes to controls and configurations.
- **Comprehensive reporting by centralizing audit evidence and compliance reports** across IAM domain tooling to streamline audit efforts and maintain real-time control visibility.

Simeio IO enables enterprises to maintain their controls consistently across IAM platforms, tools, and applications. With Simeio IO, businesses can unify fragmented identity processes, eliminate security blind spots, and accelerate secure access at scale.

Conclusion

Solution gaps are inevitable, as enterprises choose the best identity security solutions for the various IAM domains. The challenge for identity teams lies in improving security by quickly rolling out applications with appropriate controls to meet their risk and compliance objectives.

While existing tools add tremendous value, bridging siloes and streamlining application onboarding processes improve security posture, reduce risk, and accelerate application rollouts.

Identity orchestration is low-hanging fruit, a quick win that enables enterprises to get a better ROI from their existing investments while alleviating the strain on identity security teams and application owners.

Information contained in this publication has been obtained by sources Informa TechTarget considers to be reliable but is not warranted by Informa TechTarget. This publication may contain opinions of Informa TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent Informa TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, Informa TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

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