S&P Global
Market Intelligence

451 Research Market
Insight Report Reprint

Agentic AI complicates an already complicated picture around nonhuman identities

Highlights from VotE: Information Security

August 25, 2025

by Daniel Kennedy

The Voice of the Enterprise: Information Security, Identity Management 2025 survey highlights security leaders' key concerns related to identity security.

Introduction

The Voice of the Enterprise: Information Security, Identity Management 2025 survey highlights security leaders' key concerns related to identity security. It examines the growth in managing nonhuman identities, focuses on various authentication methods, especially the increase in multi-factor authentication, and explores the drivers and barriers for this growth. Additionally, it identifies the key features fueling advancements in customer identity and access management, as well as in identity threat detection and response.

THE TAKE

Nonhuman identities (NHIs) — such as machine identities, service accounts and application credentials — have always been a distinctive part of identity management, where approaches focus on persistent credentials for human users rather than emphasizing ephemeral access for machine users. With some reports indicating that NHIs outnumber human identities 50 to one, managing the sprawl of these identities, including permissions that maintain the principle of least privilege and knowing who owns what, has always been a challenge for security teams. Yet, NHIs are a vital component of automation strategies. Some key challenges include a lack of visibility into their activity and related difficulties in auditing, over-permissioning, and even application security issues, such as secrets management. The rise of agentic AI, especially agents acting on behalf of users, promises to make an already complex issue even more complicated. In fact, agent behavior blurs the line between human users and NHIs. Two-fifths (41%) of enterprises are already using third-party security tools to help manage NHIs, 18% are running proof-of-concept projects, and another 15% plan to implement them within the next six months.

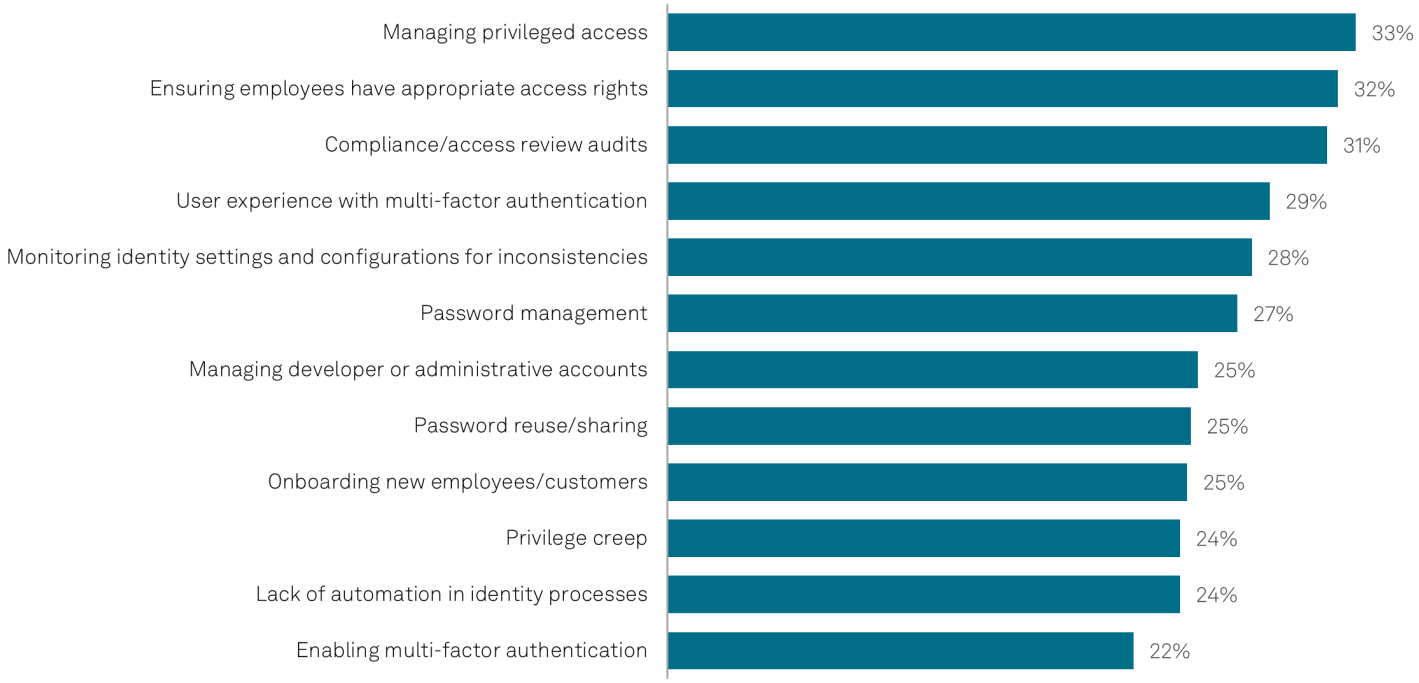
Summary of findings

The impact of AI in identity is not limited to the management of NHIs. Username and password combinations remain the most common authentication approach (cited by 56% of respondents). However, the second most popular approach is now authenticator apps for multi-factor authentication (MFA), which increased from 35% in 2024 to 47% this year. This may be due to mobile push-based MFA, the fourth most common authentication method, being susceptible to fatigue attacks. Still, it is also widely used because it offers a level of convenience for users. The 2023 attack by the Scattered Spider cybercriminal group on MGM Resorts and Caesars Entertainment involved social engineering and manipulation of human controls around identity, such as reset processes. However, the emerging concern for MFA is how attackers use AI to undermine authentication methods. In 2018, researchers at the University of Florida showed how AI-generated synthetic fingerprints can beat biometric authentication. Andre Kassis and Urs Hengartner published Practical Attacks on Voice Spoofing Countermeasures in 2021, demonstrating weaknesses in voice authentication. Criminal services for MFA bypass using some of these techniques are beginning to appear.

The cost of failing to implement MFA properly can be significant, as the City of Hamilton in Ontario discovered earlier this summer when the city government realized that what they believed to be $5 million in covered costs from their 2024 ransomware attack would not be covered by their cybersecurity insurance policy. The reason given is that coverage doesn't apply to losses caused by the absence of MFA. Although city staff were aware of the MFA requirement since 2022, some departments resisted its implementation, according to their technology vendor. Hamilton is not alone; the number one barrier to MFA adoption continues to be usability and user experience issues, cited by 30% of respondents in this survey. User experience with MFA is the fourth most frequently mentioned pain point in identity management overall (29% of survey respondents). Ransomware continues to be an active threat, especially for local governments. The city of St. Paul, Minnesota, is currently facing an attack that prompted the deployment of the state's National Guard cybersecurity unit. The most cited response in the field of identity management to such attacks is the implementation of MFA (cited by 60% of respondents), so it is clear why insurance companies are so focused on that capability, followed by enhanced auditing (40%) and privileged access management (PAM) implementation (38%).

PAM remains a top pain point, as shown in Figure 1. This is similar to 2024, and this issue serves in part as a driver of M&A. While CyberArk, recently acquired by Palo Alto Networks for $24.1 billion, is primarily described as an identity platform offering various identity security solutions, it is also a leading PAM vendor. It combines into a Palo Alto Networks security offering that focuses on an integrated platform approach to providing a variety of security product offerings across network security, security operations, and cloud security. Ensuring employees have proper access rights (32%) and facilitating compliance or access review audits (31%) are among the top three challenges. Large language models may hold promise for the latter, specifically in automating the review of user access rights and identifying excessive or unnecessary permissions.

Figure 1: Top-cited identity management pain points



Q. What are your organization's key pain points when it comes to identity management or governance? Please select all that apply.
Base: All respondents (n=589). Note: Showing top 12 responses.
Source: 451 Research's Voice of the Enterprise: Information Security, Identity Management 2025.

While much of the identity management field centers on enterprise solutions related to various aspects of identity (e.g., authentication, access control and single sign-on), customer identity and access management (CIAM) focuses on how customers access an enterprise's services. Typically, CIAM strategies include reduced sign-on capabilities for users. The primary driver for implementing third-party CIAM offerings is far and away the security and protection of customer data (cited by 53% of survey respondents). Compliance with privacy requirements (39%) and preventing misuse of an enterprise's online resources (38%) are also among the top reasons.

Identity threat detection and response (ITDR) uses various tools and techniques to safeguard user identities and systems. It emphasizes continuous monitoring of user activity to identify suspicious or unusual actions, automated responses when possible and integration with other security tools like common security operations center systems. The leading features that set ITDR offerings apart are their detection and response abilities (48% of citations), providing security for Entra ID (44%), and preventing privilege escalation (41%). ITDR is also being adopted as a strategy to build resilience against ransomware (41%).

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia-Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html