Keeper Security Insight Report

Identity Security at Machine Speed

May 2026

Overview

Identity now underpins how modern enterprises operate. It governs workforce access, machine interactions, service accounts, automation workflows and AI-driven processes across cloud and hybrid environments. What was once a directory-based function has evolved into operational infrastructure with a ballooning cyber attack surface.

As identity ecosystems expand to include both human and Non-Human Identities (NHIs), governance must extend across a broader and more dynamic landscape. Nearly 89% of senior IT leaders report that managing this growing identity footprint is challenging, reflecting the scale and complexity of modern environments. At the same time, identity authority is often distributed across systems with 96% citing disconnected or poorly integrated security tools as creating exploitable gaps, underscoring the oversight required to maintain consistent enforcement.

This expansion intersects directly with monitoring. In environments where automation executes continuously and identities operate at machine speed, real-time visibility becomes increasingly consequential. Yet 72% of organizations report that credential misuse is not detected in real time, with most identifying unauthorized privileged access within hours rather than minutes – if not days, weeks, months or even years.

Keeper Security's research, conducted among 3,200 cybersecurity decision-makers and senior IT leaders across North America, Europe, Asia-Pacific and the Middle East, examines how organizations are adapting to these infrastructure shifts. It analyzes identity growth, distributed authority, privilege maturity and detection tempo in environments where execution increasingly occurs at machine speed. Together, the findings provide a current-state view of identity governance at scale and the structural forces shaping enterprise security in 2026.

89%
find managing identity growth challenging

96%
cite disconnected tools creating exploitable gaps

72%
cannot detect credential misuse in real time

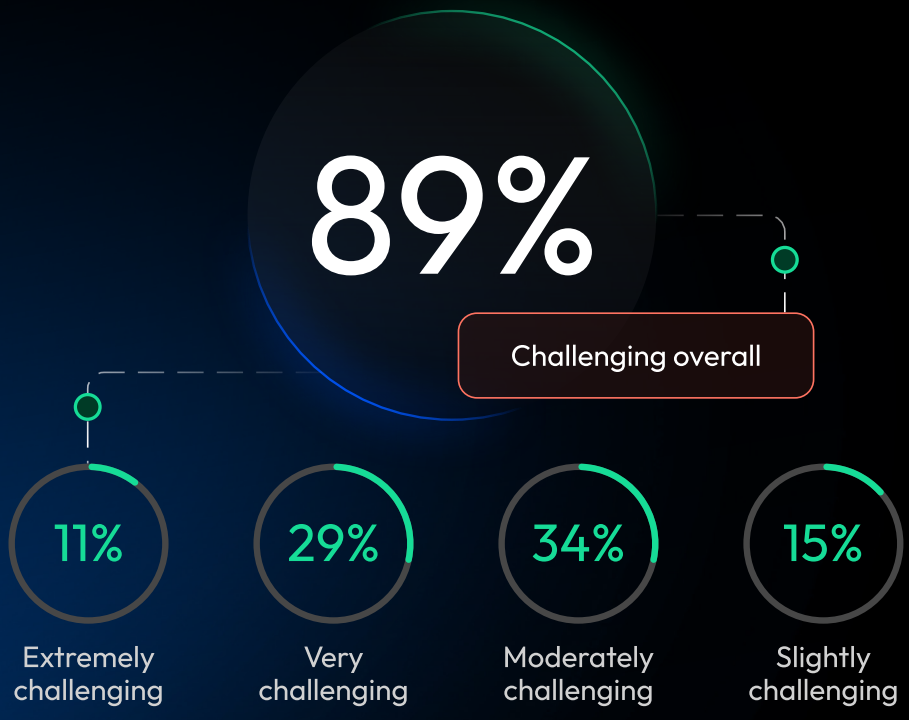
Identity is Now Enterprise Infrastructure

Identity is no longer just a user authentication function. It is the operational layer through which modern enterprises execute. Every employee login, contractor access request, API call, service account, automation workflow and AI-driven process relies on identity to authenticate, authorize and record activity.

This shift has been gradual, but its implications are structural. Identity now mediates access across cloud platforms, SaaS applications, AI agents, development pipelines and infrastructure environments. It governs not only who can access systems but also how machines interact, how services exchange credentials and how automation executes at scale. The result is an expansion in both volume and complexity.

A significant majority of organizations (89%) report that managing the growing number of identities across their environments is challenging, as these identities now span employees, contractors, third parties and NHIs such as service accounts and machine credentials.

Growth is no longer tied solely to workforce onboarding cycles. Each new system, automation script or Artificial Intelligence (AI) integration introduces additional authentication events, credentials and access pathways. Identity ecosystems have become continuous and interdependent rather than linear and discrete.



AI further accelerates this expansion. Generative copilots, orchestration engines and AI-driven analytics systems interact directly with business-critical infrastructure by authenticating, retrieving data and executing commands through defined credentials and permissions. As AI adoption increases, so does the number of NHIs operating within enterprise environments. Organizations recognize that AI-related identity risk extends beyond employee behavior.

Top AI-Related Identity Governance Gaps

56%
Employees using AI and inadvertently sharing sensitive information

44%
Lack of governance for AI-driven access and automation

43%
AI-related NHI management and security

42%
Lack of visibility into AI tools employees use

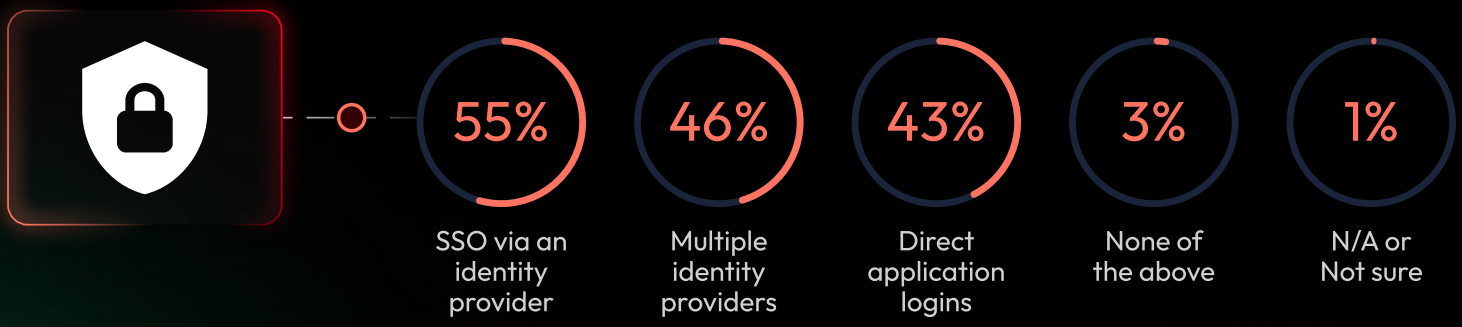
While 56% express concern about the inadvertent exposure of sensitive information, more than four in 10 identify governance-specific gaps, including oversight of AI-driven access, management of AI-related NHIs and visibility into AI tool usage. This suggests that AI-related risk is not confined to user error. It reflects the need to extend identity governance into automated and machine-driven workflows, where privilege, visibility and oversight must operate consistently across human and non-human identities.

Identity now underpins a hybrid ecosystem of human and machine identities operating simultaneously across distributed infrastructure. As that ecosystem expands, governance must extend beyond workforce identity management to a broader, more integrated security and control model.

Concern about employee misuse varies by region

67%	55%
64%	55%
62%	52%
56%	51%
56%	51%

Identity Security and Control is Fragmented



As identity volume expands, authority over identity has extended across systems. Organizations introduce identity providers, cloud access controls and privileged access platforms over time, typically in response to immediate operational or regulatory requirements. These systems now coexist within the same environment, yet they do not always function as a single, unified control layer.

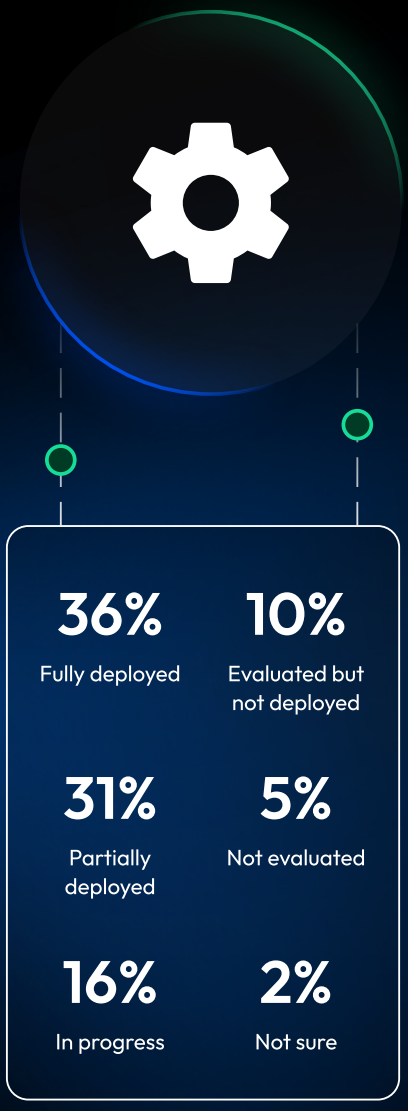
The distribution is visible in authentication patterns. While 55% of respondents report using Single Sign-On (SSO) through an identity provider, 46% operate multiple identity providers and 43% still allow direct application logins outside centralized enforcement.

These figures reflect an environment in which identity decisions are not confined to a single authority. Authentication, privilege assignment and session monitoring may be governed by different systems depending on infrastructure boundaries. Policies may be consistently defined yet applied unevenly, and logging may exist across platforms without originating from a unified source of truth.

This dynamic is reinforced by perception: **96%** say disconnected or poorly integrated security tools are creating exploitable gaps. The concern is less about the presence of controls than about their coordination. When identity authority is distributed, alignment becomes an operational effort rather than an architectural property.

As identity assumes a central role in enterprise execution, the distribution of control carries greater implications. Security and governance depend not only on the strength of individual systems but also on how coherently those systems function together.

Privilege Expansion Without Full Maturity



Privileged access management deployment status

As identity authority becomes distributed, privilege emerges as a defining control point. Privileged access is no longer confined to a small set of administrative accounts. It now extends to automation pipelines, service identities and machine-driven workflows, where elevated permissions are often required for routine operational tasks. Cloud-native infrastructure relies on defined access roles to function, and AI-enabled systems interact directly with sensitive datasets and production environments. The distinction between operational and privileged identities has become less pronounced as these interactions scale.

Adoption of Privileged Access Management (PAM) reflects recognition of this shift, yet implementation maturity varies. Globally, 36% report that PAM is fully deployed, while 31% indicate partial deployment and 16% report active implementation. In effect, **64%** do not yet operate with fully consolidated privileged access governance.

Privilege expansion continues as new systems come online, API integrations accumulate, NHIs increase and cloud roles multiply across environments. Where privileged workflows remain partially centralized, visibility and enforcement may differ between systems, reflecting the structure of the underlying architecture.

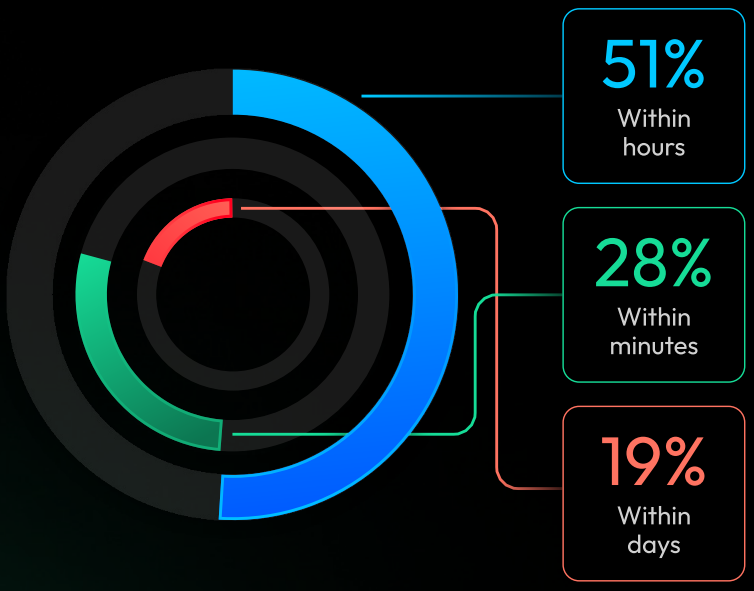
The issue is not the importance of privilege, which is widely acknowledged. It is the consistency of control over privileged access. When centrally governed, privilege provides auditability and policy alignment. When authority is distributed without uniform oversight, measurement and management become more complex. As identity assumes an infrastructural role, privilege becomes its most sensitive layer, and governance maturity determines whether that layer functions predictably across the enterprise or varies according to system boundaries.

Detection Operates on a Different Tempo

As identity becomes enterprise infrastructure and privilege expands across environments, monitoring shifts from a supporting function to a defining one. Yet detection does not always operate at the same pace as execution. Nearly three-quarters (72%) of organizations cannot detect credential misuse in real time, with most identifying unauthorized privileged access within hours rather than minutes.

Detection speed is shaped less by intent than by architecture. When identity security authority and privilege enforcement are distributed across systems, monitoring depends on stitching together signals rather than observing activity through a consolidated lens. Log aggregation, session recording and cross-platform analysis introduce delays that reflect structural design rather than operational oversight.

Time to Detect Credential Misuse

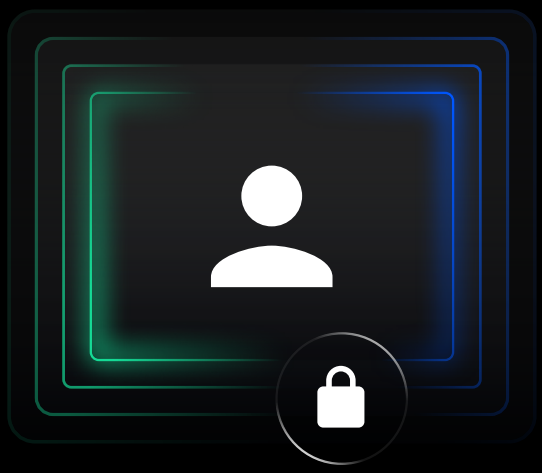


This becomes more pronounced as automation scales. Authentication events occur continuously, service accounts generate non-human activity patterns and privileged workflows extend into CI/CD pipelines and cloud-native services. In such environments, the ability to detect activity in real time is determined by how cohesively identity governance, privilege enforcement and monitoring operate together.

Detection tempo serves as a practical indicator of integration. The more identity functions as a unified control layer, the more closely monitoring can align with execution speed.

Identity Security at Scale

As identity ecosystems have grown to include humans and machines acting in parallel, governance has extended across multiple systems. Authentication, privilege enforcement and monitoring were introduced at different stages of infrastructure growth, often to solve discrete problems. Over time, this has produced a distributed model of authority rather than a single, consolidated cybersecurity control plane.



Privilege now operates within automation pipelines, service identities and AI-enabled workflows, narrowing the distinction between operational and elevated access. Monitoring capability mirrors this structure. Where identity governance is integrated, activity can be evaluated with minimal delay. Where it remains distributed, response timing reflects the coordination required across systems.

Identity has evolved from a directory-based function into operational infrastructure. Its scale is continuous rather than episodic, and its authority is no longer centralized by default. Governance maturity is increasingly defined by coherence – how consistently authentication, privilege and monitoring function together across environments.

About Keeper Security

Keeper Security is the global leader in zero-trust and zero-knowledge identity security, protecting passwords, passkeys, secrets, endpoints and privileged access for thousands of organizations and millions of users worldwide. To learn more, visit **Keepersecurity.com** or contact us at **communications@keepersecurity.com**.

Methodology

The research was conducted by Censuswide in 2026, among a sample of 3,200 professionals who are cybersecurity decision makers/managers+ and who work in IT Security, Executive Leadership or DevOps (500 respondents in the UK, US, France, Germany, Japan, APAC (Australia, India, New Zealand, China) and 200 in the Middle East). Censuswide is a member of the Market Research Society (MRS) and the British Polling Council (BPC), and a signatory of the Global Data Quality Pledge.