

Rethinking Identity Lifecycle Management in the Age of AI

The Governance Gap Is Widening

The security environment has fundamentally changed. Organizations now operate in cloud-first, application-heavy environments where access is distributed across hundreds or thousands of systems. Infrastructure has evolved, applications have multiplied, and the identities accessing those resources have expanded far beyond traditional employees.

Today's identity landscape includes seasonal and contract workers, partners, service accounts, workloads, and AI agents. Employees change roles faster and more frequently. Access needs shift continuously. Any identity, human or nonhuman, can quickly become a privileged identity through direct assignment, inherited entitlements, or accumulated access over time.



Figure 1. Types of identities

Identity is one of the most valuable targets for threat actors. Recent research showed that 87% of organizations had over two identity-related breaches in the past year.¹ Attackers target credentials, permissions, and privilege escalation because identity sits at the center of how work gets done. As a result, identity has become the new security perimeter.

This shift has significant implications. As organizations invest in stronger security postures and adopt new security platforms, identity governance and lifecycle management can no longer operate as isolated compliance tools. They must be treated as foundational components of the identity security strategy.

Modern identity lifecycle management (LCM) has become more than only onboarding and offboarding users. It now entails continuously aligning access with business needs as identities join, move, change roles, and leave, as well as addressing access drift and privilege accumulation over time. Without continuous governance, least privilege cannot be enforced, and security teams are left managing risk reactively.

Idira™ Identity Security Platform, by Palo Alto Networks, addresses this reality. It considers LCM as an always-on, AI-driven governance capability that integrates directly into the broader identity security platform and its corresponding solutions for managing critical security programs. These programs can include privileged access, single sign-on (SSO), just-in-time (JIT) access, and AI agent discovery and governance.

Access Delayed Is Often Access Diverted

Access governance challenges both create security risks and affect productivity. When employees cannot quickly obtain the access required to do their jobs, work slows down. And, when access processes become too slow, users often find ways around them. Among employees, 65% admit to bypassing access rules because governance is too slow.²

1. *Unit 42 Global Incident Response Report 2026*, Palo Alto Networks, February 17, 2026.

2. *2025 Identity Security Landscape*, CyberArk, May 2025.

How do organizations make access governance go faster? Cloud adoption and application sprawl have dramatically increased the number of access decisions organizations must manage. Each new application introduces its own entitlement model, permissions, and risk. Identity sprawl compounds this challenge. Organizations must govern access for a growing mix of employees, contractors, service accounts, machine identities, and AI-driven processes.

At the same time, identities are more dynamic than ever. Employees change teams, responsibilities, and tools frequently. Contractors come and go. AI agents and automated workflows operate continuously, often with elevated permissions. Access that was appropriate yesterday might be excessive today.

This can create persistent access drift and privilege creep. Temporary access becomes permanent. Exceptions accumulate. Over time, access no longer reflects the real needs of employees, and it doesn't reflect least privilege or just-enough privilege.

Roles Can't Solve the Problem

Most organizations use roles to simplify access decisions, but they aren't sufficient on their own. Roles lack the granularity needed to reflect real-world work patterns. Modern employees often work across multiple systems, projects, and responsibilities that change frequently. Capturing this reality in static roles quickly becomes complex and restrictive.

As organizations grow, the number of roles often multiplies rapidly. Each application, team, or function introduces new variations. Maintaining these roles requires constant tuning as identities, responsibilities, and entitlements evolve. Even with significant effort, roles frequently fall out of sync with how the work is performed.

At modern scale, roles alone cannot keep pace with the dynamic nature of identities, applications, and access needs. Instead of simplifying governance, they often create an administrative burden while still failing to enforce least privilege.

Neither Can Legacy Identity Governance and Administration

Even when organizations attempt to govern access through roles, traditional identity governance and administration (IGA) platforms struggle to govern the full application estate. Legacy IGA was designed for environments where the number of critical applications was limited, centrally managed, and relatively stable. These systems rely heavily on deep integrations and custom connectors to manage access across applications.

In modern environments, application portfolios grow rapidly and change all the time. Traditional IGA connector development can be slow and manual, delaying application coverage and creating governance blind spots. As organizations pursue least privilege, JIT access, and zero standing privileges (ZSP), these gaps become even more problematic. Without broad coverage and continuous intelligence, security teams are forced to rely on manual processes and reactive controls that cause access delays and cannot keep pace with the speed and security needs of modern organizations.

Lifecycle Intelligence with Continuous Automation

Idira Identity Security Platform addresses these challenges through AI Profiles, which bring real-time intelligence to identity governance. AI Profiles analyze real access patterns across users and peer groups to determine what access is appropriate for a given role or job function. Instead of relying solely on static roles, governance decisions are informed by how access is used across the organization. As identities, applications, and responsibilities change, AI Profiles continuously adapt to reflect those changes.

This enables preapproval of appropriate access and dramatically reduces review fatigue. In practice, organizations can reduce buy up to 75% of unnecessary review decisions while increasing confidence in outcomes.³ Access requests are evaluated in context, based on how similar identities use applications and entitlements, rather than relying on static assumptions.

AI-driven governance is also critical for operationalizing least privilege, JIT access, and ZSP. By continuously understanding access needs, Idira Identity Security Platform helps organizations grant access only when required, for the appropriate duration, and with clear justification.

Automation is applied intelligently. Rather than forcing deep integrations everywhere, Idira Identity Security Platform uses a combination of API-based connectors, robotic automation, and on-premises integration to govern access across virtually any application. This approach delivers coverage without sacrificing speed or flexibility.



Figure 2. Lifecycle management: Continuous intelligence to manage access

Modern Workforce, Modern Risk: Governance Beyond the Traditional Workforce

Modern organizations must govern access for more than just people. Service accounts, machine identities, workloads, and AI agents now represent a significant portion of the identity landscape.

AI agents introduce new risks because they act autonomously, often at scale, and are controlled by human owners whose access decisions also require governance. Governing these identities requires continuous visibility into both the identities themselves and the humans who design, deploy, and manage them.

AI agents change the landscape, but they don't change the best practices. Security teams must still enforce appropriate access across humans and machines alike, as well as have full visibility into AI agents, which is another required platform capability.

IGA Alone Isn't Enough

IGA exists to help organizations govern access across the identity lifecycle. It includes provisioning and deprovisioning access, enforcing approval workflows, enabling self-service requests, conducting access reviews, and producing audit-ready evidence.

When implemented effectively, IGA supports the principle of least privilege by ensuring that access is granted intentionally, reviewed regularly, and removed when no longer needed. Automation reduces manual effort and human error.

However, least privilege is no longer a static goal. Many organizations are actively adopting JIT access, ZSP, and time-bound permissions to reduce risk. These initiatives are at different stages of maturity across organizations, but they all share a common requirement: Access decisions must be continuous.

Manually managing JIT approvals, privilege elevation, and access revocation at scale is operationally expensive. Without strong governance, these controls become fragmented and difficult to sustain. IGA must provide the intelligence layer that understands who needs what access, when, and why, across the entire lifecycle.

³. Based on internal research and findings.

Adopt a Platform Strategy for Risk Reduction and Continuous Intelligence

Governance alone cannot reduce identity risk. Any identity can become privileged, intentionally or unintentionally. Effective identity security requires governance to work alongside privileged access controls and access management.

Idira Identity Security Platform delivers an identity security platform that unifies governance, privilege controls, and access management. Governance insights inform enforcement decisions, while privileged access controls apply those decisions consistently. Access management ensures policies are executed across environments for both human and nonhuman identities.

For identity and access management teams and broader security leaders, including those evaluating identity as part of a larger security platform strategy, this integration is critical. Identity is the connective layer across cloud, applications, and infrastructure. A siloed IGA solution cannot deliver continuous visibility or enforce least privilege at scale.

By unifying governance, privilege controls, and access management, organizations gain continuous insight, enforceable least privilege, and audit-ready evidence in an environment where identity is the security perimeter.

Closing the Gap Between Intent and Access

Modern identity security requires more than defining policies. It requires continuously ensuring that access reflects real business needs across every identity, application, and privilege boundary. As organizations adopt principles such as least privilege, JIT access, and ZSP, the gap between security intent and operational reality becomes harder to manage without intelligent automation.

Identity governance and lifecycle management play a critical role in closing that gap. By continuously understanding who needs what access and aligning entitlements with real-world behavior, organizations can reduce risk while enabling the business to move quickly.

The webinar “[Right Intentions, Wrong Access](#)” explores these challenges and practical approaches in more depth. We invite you to watch it to learn how modern identity environments create governance blind spots and how AI-driven lifecycle management can help maintain least privilege in dynamic environments.

To explore all the ways Idira can secure the identities across your organization, visit <http://www.paloaltonetworks.com/idira>.

About Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI, and Identity. Trusted by more than 70,000 customers and powered by Unit 42® threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at www.paloaltonetworks.com.



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
idira_wp_rethinking-id-lifecycle-mgmt_043026