Idira Human Identity Security

Secure Your AI-Ready Workforce with a Unified Identity Security Platform

Weak identity security posture plays a material role in 90% of all breach investigations.[1] Increasingly, organizations are exposed to the uncontrolled privilege gap. This dangerous blind spot is created by taking a disconnected approach to modern privileged access management (PAM), using separate tools for identity and access management (IAM) and identity governance and administration (IGA).

Idira™ Human Identity Security, by Palo Alto Networks, replaces this fragmentation with a unified platform that's built for the speed of modern business. By connecting intelligent discovery, smart controls, always-on governance, and the power of automation, Idira delivers a unified platform to secure your decentralized workforce and AI-driven workflows.

Fast Facts

Human identities are projected to grow by **56%** over the next 12 months, drastically expanding the attack surface.[2]

1. *Unit 42 Global Incident Response Report 2026*, Palo Alto Networks, February 17, 2026.
2. *2026 Identity Security Landscape*, Palo Alto Networks, May 11, 2026.

The Identity Landscape Has Fundamentally Transformed

For decades, organizations have managed their identities through three disconnected silos: IAM for access, PAM for administrators, and IGA for compliance. This fragmentation has created the uncontrolled privilege gap—the vulnerability risks between siloed tools that attackers exploit to move laterally and escalate privileges.

Idira Human Identity Security is built on a foundation of proven market leadership and has been recognized by Gartner® as a Leader in the 2025 Magic Quadrant™ for PAM.[3] This approach to modern PAM replaces fragmented point solutions with a unified, AI-native operating model. By converging data and policy engines across IAM, PAM, and IGA, Idira secures every human user, from the IT admin to the sales manager, across your entire organization.

99%

of cloud identities carry excessive permissions, a gap known as "governance drift."[4]

Furthermore, 96% of human identities possess access levels far beyond what is required for their actual job functions.[5]

Today's Privilege Reality Outpaces Legacy Tools

Legacy identity management tools were built for a world of static perimeters and a smattering of IT admins. Today, however, every human identity carries privilege risk based on the data and systems each person can access:

- **Fragmented tools:** When IAM, PAM, and IGA solutions don't communicate with each other, security teams lose visibility. For instance, an employee might pass a standard IAM login check while holding excessive entitlements in an IGA tool. Attackers thrive in these blind spots.
- **Standing privilege, standing risk:** Traditional least privilege models still leave access persistent when no task is being performed. If a credential is compromised at 2:00 a.m., the attacker has a wide-open door to sensitive data, regardless of whether the affected user is working.
- **Scale of human risk:** Everyone, from marketing managers to financial analysts, hold privileges, and all are potential risk vectors. Human teams that work manually can't keep pace with the demands of modern cloud and SaaS environments.

The Idira Solution: Discover, Control, Govern

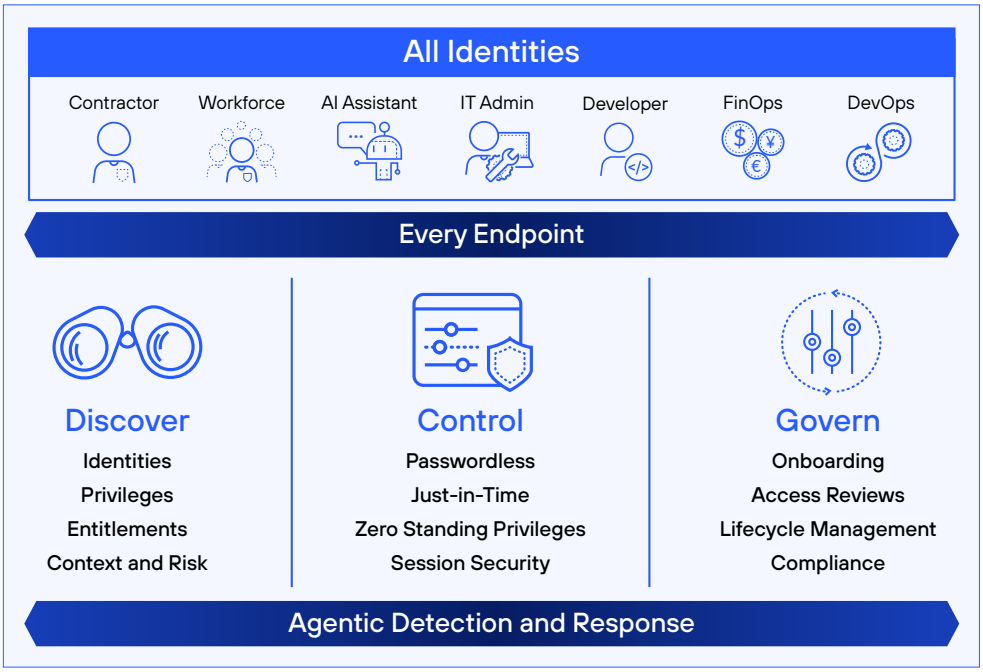

Figure 1. Idira Identity Security Platform

3. *2025 Gartner® Magic Quadrant™ for Privileged Access Management*, CyberArk, October 2025.
4–5. Palo Alto Networks, *Unit 42 Global Incident Response Report 2026.*

Idira Human Identity Security delivers a unified platform built for your AI-ready workforce across every environment your business runs on. The platform transforms a disjointed collection of tools into a single, continuous operating model.

61%

of privileged access requests are still fulfilled without using secure JIT or ZSP methods, leaving doors open for attackers.[6]

Discover Privilege Everywhere

- **Proactively and automatically scan on-premises, cloud, and SaaS environments** to build a live, correlated inventory of every human identity, entitlement, and access path.
- **Map privilege sprawl and permission creep** to uncover and prioritize unmanaged risks.
- **Maintain a single source of truth** to accurately map the blast radius across complex environments.

Control Access in Real Time

- **Shift from static, persistent access to zero standing privileges (ZSP)** by dynamically provisioning and revoking entitlements based on context.
- **Use just-in-time (JIT) access** to elevate privileges at the exact moment of need for the task at hand.
- **Protect the workforce** with phishing-resistant, passwordless multifactor authentication (MFA).
- **Implement continuous session isolation, monitoring, and recording** to know which users and third-party vendors accessed what, when, and why for complete session control and auditability.

Continuously Govern Access

- **Automate user access reviews:** Replace manual spreadsheets with AI-assisted workflows that reduce reviewer fatigue, surface risk, and deliver audit-ready evidence packages with full traceability.
- **Automate Joiner-Mover-Leaver processes** with AI-driven access recommendations to grant the right access faster and reduce excessive privilege from day one.
- **Proactively monitor risks:** Continuously evaluate access across human and machine identities to detect segregation of duty (SoD) conflicts, orphaned accounts, and risky entitlements with actionable risk remediation.

Key Capabilities

	Discover	Control	Govern	Intelligence
Strategic Capability	Attack Path and Risk Mapping	Adaptive, Risk-Based Access	Automated, Always-on Compliance and Lifecycle Management	Context-Driven Remediation and Response
Technical Highlights	Proactively reduce risk across your on-premises, cloud, and SaaS environments. By finding and monitoring every identity, entitlement, and access path, you can map permissions and attack paths, apply context to understand the scope of access, and prioritize remediations based on the potential blast radius.	Control access from the endpoint all the way through the session. Protect against preauthentication and postauthentication threats using real-time phishing-resistant MFA, JIT, and ZSP access models.	Automate user access reviews and the full Joiner-Mover-Leaver lifecycle with AI-driven recommendations to enforce least privilege and deliver audit-ready evidence. View unified identity and entitlement data to eliminate visibility gaps. Automatically detect SoD conflicts and orphan accounts with real-time alerts and remediation.	Use AI to connect identity risk with your unique environment. Get clear recommendations and the evidence behind them, from onboarding guidance to flagging suspicious activity and removing unneeded privileges. Speed up your response time and reduce manual cleanup.

6. Palo Alto Networks, *2026 Identity Security Landscape.*

From Uncontrolled Privilege to Unified Modern PAM

Human identity security cannot be managed effectively in silos or through fragmented tools. By consolidating IAM, PAM, and IGA, you can move from a reactive posture to a proactive, comprehensive defense that eliminates the uncontrolled privilege gap.

No persistent standing access to exploit, unmanaged credentials to steal, or hidden entitlement risks. Modern PAM capabilities support the AI-ready workforce across a single operating model that secures every human identity.

To explore all the ways Idira can secure the identities across your organization, visit 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.

"Fragmentation isn't just a visibility issue; it's a speed issue—identity tool silos delay incident response by an average of 12 hours per incident."[7]

Primary Use Cases for Securing Human Identities

1. **Eliminate Standing Access and Static Credentials**
   Secure the authentication layer with phishing-resistant passwordless MFA and remove persistent privileges with ZSP and JIT access models across hybrid cloud infrastructure.
2. **Enforce the Principle of Least Privilege at the Endpoint**
   Prevent lateral movement and credential harvesting by removing persistent local administrative rights, using on-demand elevation to secure sensitive applications and data.
3. **Automate the Identity Lifecycle**
   Automatically provision or revoke access throughout the user lifecycle. Remediate orphaned accounts, access drift, and policy violations throughout the Joiner-Mover-Leaver process.
4. **Detect and Respond to Identity-Based Threats in Real Time**
   Detect and neutralize active identity-based threats with real-time monitoring. Use behavioral analytics and automated playbooks to remediate credential misuse, privilege escalation, and account takeovers before they escalate into a breach.

7. Palo Alto Networks, *2026 Identity Security Landscape.*

paloalto NETWORKS

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

idira_sb_human-identity-security_042226