

Idira Human Identity Security At a Glance

Every User Is Privileged. Secure Them.

Identity-based techniques drive 65% of initial access.¹ The challenge only continues to increase as organizations manage risk through disconnected tools across identity and access management (IAM), privileged access management (PAM), and identity governance and administration (IGA). This disconnect creates the uncontrolled privilege gap and dangerous fragmentation that allows attackers to compromise standard employee accounts, exploit unmonitored privileges, and move laterally to target mission-critical infrastructure.

Applying Modern PAM Principles

Idira Human Identity Security unifies modern PAM capabilities with IAM and IGA into a single platform built for your AI-ready workforce. Through intelligent discovery, smart controls, and always-on governance, your decentralized workforces and AI-driven workflows can move faster while you reduce identity risk.

No matter where you do business, from on-premises to the cloud and everywhere in between, Idira secures every user—from the first endpoint authentication to the last privileged action. Idira provides the speed and precision that modern identity security demands.

Foundational Capabilities

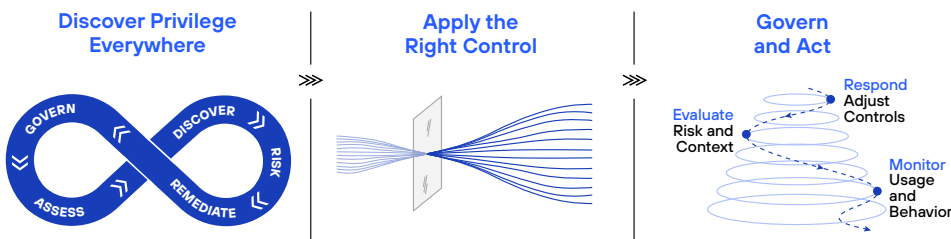


Figure 1. Foundational capabilities of modern PAM

Discover Every Identity, Entitlement, and Role

Proactively reduce risk through organization-wide scanning and attack path mapping.

- **Continuous discovery:** Track every user identity from employees to contractors and vendors or service accounts across on-premises, cloud, SaaS, endpoints, and applications.
- **Real-time inventory:** Maintain a current view of every account, entitlement, and credential with full context. Uncover privilege sprawl and hidden admin rights across IAM roles and SaaS platforms to reduce visibility gaps.
- **Risk assessment:** Correlate who has access, where they have access to, why they have access, and how risky it is against behavior and potential blast radius.

Control Access Across the Complete User Journey

Enforce privilege dynamically based on context and risk, providing a single, centralized control plane for administrators.

- **Remove endpoint risks:** Eliminate local admin privileges and replace them with on-demand, policy-based elevation.
- **Deliver phishing-resistant authentication:** Provide an end-to-end passwordless experience with phishing-resistant multifactor authentication (MFA) and workforce password management.
- **Eliminate standing access:** Use just-in-time (JIT) access scoped to the task or secure access through dynamic credential vaulting and rotation.
- **Secure sensitive sessions:** Isolate, monitor, record, and audit every sensitive session across infrastructure, cloud consoles, and SaaS in real time.
- **Stop attacks:** Use Identity Threat Detection and Response (ITDR) to analyze signals from endpoints and authentication workflows to identify and stop anomalous behavior before attackers move laterally.

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

Idira Human Identity Security

At a Glance

Govern Access Where Privilege Never Outlives Intent

Ensure governance is continuous and grounded in the privilege that exists, from the moment an identity is created to its last action.

- **Automate Joiner-Mover-Leaver events:** Use AI to define and automate granting the right access to ensure identities are secure at birth and access remains appropriate throughout the Joiner-Mover-Leaver lifecycle. Automate provisioning policies and actions to reduce effort and orchestrate ticketing and approval workflows.
- **Simplify access reviews:** Replace manual access reviews with AI-assisted certifications that reduce manual effort and automate the end-to-end reviewer workflow.
- **Proactively remediate drift:** Maintain a unified view of human and machine identities to discover and remediate orphan accounts or overprovisioned access before they become risks.
- **Generate audit-ready evidence:** Automatically capture every access request, privilege granted, activity review, and deprovisioning log to generate an audit-ready evidence package.

Accelerate Actions with AI Reasoning and Recommendations

- **Accelerate operations:** Transform time-intensive tasks into streamlined workflows that significantly speed up provisioning and reduce the manual effort required for remediation and governance.
- **Human-in-the-loop design:** Focus human oversight on high-risk identities and behavioral anomalies, while the platform automates routine work.
- **Ask any question:** Use AI available in any workflow to ask why an identity is high risk or if an entitlement is appropriate. Get well-reasoned answers and supporting evidence grounded in your environment's full identity context.

What Sets Idira Apart

- **No more silos. Just Idira:** Idira combines intelligent discovery, smart controls, and always-on governance to close security gaps, allowing you to move faster and reduce risk with modern PAM.
- **Accelerate automation:** Use agentic AI to analyze access patterns and generate job-appropriate AI profiles, slashing the time required for access certifications.
- **Eliminate standing privileges:** Create ephemeral privileges that exist only for the duration of a task, leaving nothing behind for an attacker to exploit, across every environment your business runs on.
- **Secure the entire human access journey:** Extend enterprise-grade protection, including session isolation and credential rotation, to every identity in the organization.

Implement Modern PAM with Idira

Privilege is everywhere. It moves and changes at a speed and scale that fragmented tools cannot keep up with.

Idira Human Identity Security is specifically designed to meet the identity security demands of decentralized workforces, accelerated access cycles, and AI-driven workflows. With unified modern PAM capabilities, you can eliminate gaps and blind spots, while keeping your business productive.

See how Idira can secure every user identity in your organization.

[REQUEST A DEMO](#)