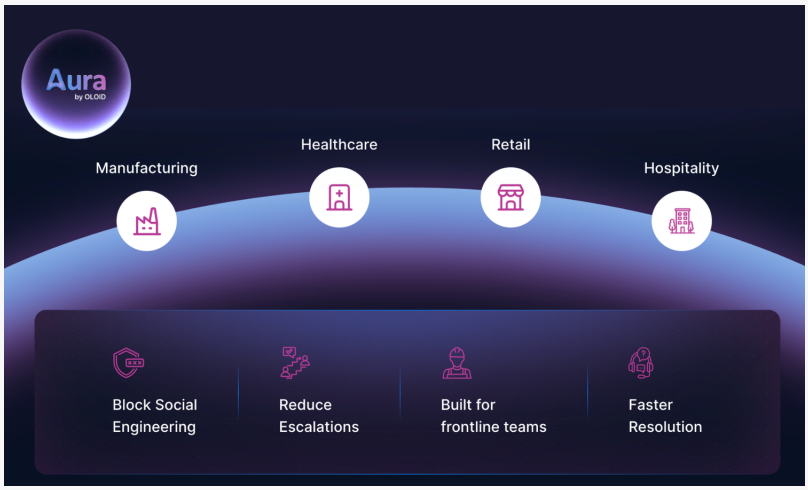
OLOID Introduces Aura, an AI Identity Assurance Agent for Critical Workforce Identity Processes

Structured Enterprise Preview Program Now Open for Organizations Extending Identity Enforcement Beyond Login



OLOID Aura is a purpose-built AI agent designed to establish employee identity in real time when help desk requests require higher assurance—from password resets to MFA resets, access changes, and sensitive HR updates.

SUNNYVALE, CA, UNITED STATES, March 2, 2026 /EINPresswire.com/ -- OLOID today announced Aura, a policy-enforced identity assurance platform designed to verify workforce identity before high-risk transactions are executed. Aura is being introduced through a structured enterprise preview program for select organizations seeking to enforce identity assurance at the transaction layer across IT, HR, and workforce systems.

As enterprises continue to strengthen authentication at login, a critical security gap remains: verifying identity when sensitive actions are requested after access has already been granted. Payroll updates, MFA resets, privilege modifications, contractor enablement, timecard edits, and credential recovery workflows frequently rely on static knowledge-based questions or manual checks, methods increasingly targeted through social engineering.

> Aura extends identity enforcement beyond authentication and into workforce operations.”
>
> *Mohit Garg, Co-founder & CEO of OLOID*

Aura establishes identity assurance at the moment of action, not just at authentication.

A Policy-Enforced Identity Gate at the Transaction Layer

Aura operates as an API-driven enforcement layer that integrates directly with service desk platforms, IAM workflows, HR systems, and workforce

applications.

It is invoked through event-based triggers, such as ticket creation, access request submission, payroll change initiation, device enrollment workflows, or credential recovery actions, before a high-risk transaction is executed.

When a request is initiated, Aura:
1. Classifies the transaction type
2. Evaluates organizational assurance policies
3. Determines the required verification strength
4. Executes the appropriate identity verification workflow
5. Returns a cryptographically signed, programmatically verifiable assurance decision (approve, deny, or escalate) to the originating system

The originating system validates Aura's assurance signal before completing the transaction.

This creates a deterministic, policy-enforced identity control point at the transaction layer, extending governance beyond login authentication and into operational workforce workflows.

Risk-Based Verification Aligned to Transaction Sensitivity

Aura supports multiple intelligent verification paths, allowing enterprises to match assurance strength to request sensitivity and workforce context.

For lower-risk interactions, Aura generates dynamic, role-aware verification prompts informed by real-time HRIS and IAM signals. These adaptive challenges replace static security questions while maintaining speed and minimal friction through chat or voice.

For higher-risk transactions, such as payroll modifications, direct deposit changes, elevated system access, or contractor enablement, Aura automatically escalates assurance strength. This may include document-based identity verification through an organization's preferred vendor, with real-time confirmation returned to the initiating system before the transaction proceeds.

In environments where HR or badge photos are maintained, Aura can securely compare a live selfie against authorized records using liveness detection. Biometric artifacts generated during the session are deleted immediately after verification.

By unifying these verification methods under a deterministic, policy-driven enforcement framework, Aura enables risk-based identity control at the transaction layer without overburdening legitimate workers.

What "AI-Powered" Means in Practice

Aura uses AI to classify transaction intent, dynamically assemble contextual verification prompts, and adapt assurance requirements based on workforce and policy signals.

Core enforcement logic remains deterministic and policy-driven, ensuring consistent, auditable decision-making aligned to enterprise security standards.

AI enhances contextual awareness and adaptability, while policy engines govern final authorization decisions.

Built for Frontline and Distributed Workforces

Aura is purpose-built for workforce-heavy environments where shared devices, BYOD realities, distributed teams, and seasonal labor are common. In these settings, device-bound identity signals are often limited, making post-login transactions particularly vulnerable to impersonation attempts.

Aura supports identity assurance across high-impact workflows, including:

* Credential recovery and MFA re-enrollment
* Sensitive access requests and role modifications
* Contractor and seasonal workforce enablement
* Payroll, benefits, and direct deposit changes
* Workforce record and time-related adjustments
* New device enrollment verification

By embedding identity verification directly into operational workflows, Aura helps organizations reduce social engineering exposure, lower unnecessary escalations, and preserve audit integrity without slowing legitimate workers.

Engineered for Security and IAM Teams

Aura includes a managed control plane that securely orchestrates policy evaluation, verification workflows, and system integrations across HR platforms, IAM solutions, workforce applications, and external identity verification providers.

The architecture is built around:
* Strict session-based processing
* Zero persistent biometric template storage
* No retained personal identification artifacts
* Role-based access controls
* Real-time assurance signal validation

“Aura extends identity enforcement beyond authentication and into workforce operations,” said

Mohit Garg, CEO & Co-founder at OLOID. “Enterprises need identity assurance at the moment critical identity-related actions are requested on an ongoing basis, not just when users log in. Aura provides a policy-enforced control layer without introducing new data risks.”

Aura Enterprise Preview Program

The structured Aura enterprise preview program is designed for CISOs, IAM leaders, HR technology teams, and security architects evaluating stronger enforcement controls across high-risk workforce transactions.

Preview participants will:
* Integrate Aura into a defined transaction flow (e.g., payroll changes, credential recovery, privilege modification)
* Configure policy-driven assurance rules aligned to internal security standards
* Connect HRIS, IAM, and workforce systems via API and event triggers
* Evaluate measurable impact on social engineering exposure, escalation rates, and resolution speed

The preview enables organizations to validate transaction-layer identity enforcement before broader deployment. Organizations interested in participating in the Aura Preview Program can sign up here.

About OLOID

OLOID is a passwordless authentication platform purpose-built for frontline and shared-device environments. Trusted by global enterprises across healthcare, manufacturing, retail, and critical infrastructure, OLOID enables fast, secure access using biometrics, badges, and mobile credentials, without passwords. Powered by AI-driven identity intelligence, OLOID integrates with leading identity providers and enterprise systems to deliver frictionless authentication, strong compliance, and real-world operational impact. Learn more at www.oloid.com

Garima Bharti Mehta
OLOID INC.
+1 800-711-9123
email us here
Visit us on social media:
LinkedIn
Facebook
X

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.