

OLOID Brings Aura to Workday Agent System of Record to Strengthen Identity Assurance for Sensitive Workforce Requests

OLOID Aura extends identity assurance to sensitive workforce workflows, including password resets, credential recovery, and access-related support requests.

SUNNYVALE, CA, UNITED STATES, June 8, 2026 /EINPresswire.com/ -- OLOID today announced

“

With Aura now added to Workday Agent System of Record, organizations can apply stronger, policy-enforced identity assurance in the moments where trust matters most.”

Madhu Madhusudhanan, Co-founder & CTO, OLOID

that [Aura](#), its recently launched AI Identity Assurance Agent, has been added to [the Workday Marketplace](#), extending identity assurance into sensitive workforce workflows such as password resets, credential recovery, and access-related support requests.

Aura was introduced by OLOID as a policy-enforced identity-assurance platform designed to verify workforce identity before high-risk actions are completed. OLOID seamlessly registers with Workday ASOR and brings the capability into a broader enterprise framework for governing and managing AI agents used across workforce

operations.

Workday Agent System of Record (ASOR) is designed to help organizations securely register, manage, govern, and measure AI agents, including third-party agents, in a unified environment with greater visibility, accountability, lifecycle management, and analytics. As organizations begin deploying more AI agents across HR, IT, finance, and workforce operations, ASOR provides a structured control layer for managing how those agents are introduced and used across the enterprise.

“As organizations deploy more AI agents across workforce operations, governance, visibility, and trust become increasingly important,” said Mohan Rajagopalan, Senior Director of Product Management, Workday AI Platform. “Workday Agent System of Record is designed to help customers manage this emerging agent ecosystem, and partners like OLOID are bringing valuable specialized capabilities such as identity assurance into that framework.”

Bringing Identity Assurance into the Agentic Workforce

As enterprises continue to strengthen authentication at login, an important area of focus is verifying identity when high-risk actions are requested after access has already been established.

Password resets, account recovery, support escalations, and access-related employee requests are still frequently handled using static security questions, manual review, or agent discretion, methods that can be vulnerable to impersonation and social engineering.

Aura is designed to help establish identity assurance at the moment of action, not just at authentication.

With its addition to Workday ASOR, Aura extends that control into emerging AI-driven workforce workflows where trust, verification, and accountability remain essential.

What Aura Does

Aura is designed to help organizations verify workforce identity before sensitive actions are completed, particularly in workflows where support teams, workforce systems, or service channels are asked to act on behalf of an employee.

These workflows may include:

- * Password reset
- * Credential recovery
- * Account unlock
- * Access restoration
- * Sensitive support escalations
- * Workforce identity verification for high-risk requests

By embedding policy-driven identity verification directly into these moments, Aura helps organizations reduce exposure to social engineering while preserving a faster, lower-friction experience for legitimate workers.

Risk-Based Verification Aligned to Workforce Context

Aura supports multiple verification methods that can be selected dynamically based on request sensitivity, workforce context, and organizational assurance policy.

Depending on the workflow, verification can include:

- * AI-generated security questions informed by workforce and contextual signals
- * Identity document verification for higher-assurance scenarios
- * HR photo-based identity verification where employee records support visual comparison
- * Chat, voice, or video-based interactions to support flexible workforce experiences

This allows organizations to move beyond static knowledge-based authentication and apply a more adaptive, risk-based approach to workforce identity verification.

Why This Matters in Workday ASOR

As organizations begin managing AI agents more like digital workers, identity trust becomes a critical part of agent governance.

Aura adds an important layer to that model by focusing on supporting one of the most sensitive operational trust considerations in workforce systems: verifying identity before a high-risk workforce action is approved or fulfilled.

By bringing identity assurance into Workday ASOR, organizations can extend governance beyond login and into the employee-facing workflows where trust decisions continue to carry operational and security consequences.

What “AI-Powered” Means in Practice

Aura uses AI to help classify request types, assemble contextual verification workflows, and determine the most appropriate identity assurance path based on policy and workforce signals.

Core assurance and decision logic remains policy-driven and deterministic, ensuring that verification outcomes remain consistent, auditable, and aligned to enterprise security requirements.

AI enhances contextual awareness and adaptability. Policy governs the assurance decision.

Built for Workforce-Heavy Environments

Aura is designed for organizations supporting frontline, shared-device, distributed, and non-desk workers, environments where identity is often challenged not only at login, but during support and recovery workflows.

In these settings, support teams are frequently required to make trust decisions in real time, often without strong verification controls.

By introducing automated, policy-based assurance into those interactions, organizations can:

- * Reduce identity risk during reset and recovery workflows
- * Strengthen protection against impersonation and social engineering
- * Improve confidence in workforce-facing support interactions
- * Support more secure identity operations without adding unnecessary friction

“Enterprises have made significant progress strengthening authentication at login, but many sensitive workforce actions still rely on varying levels of identity checks after access has already been established,” said Madhu Madhusudhanan, Co-founder & CTO, OLOID.

“With Aura now added to Workday Agent System of Record, organizations can apply stronger, policy-enforced identity assurance in the moments where trust matters most.”

Extending Workforce Identity Beyond Login

Aura’s addition to Workday ASOR builds on OLOID’s broader work to modernize workforce identity across frontline and operational environments.

As AI agents take on a larger role in workforce workflows, OLOID believes identity assurance must extend beyond authentication and into the actions where workforce trust continues to carry operational and security consequences.

About OLOID

OLOID is an AI-powered passwordless authentication platform tailored for frontline & mobile employees. Fortune 500 companies in manufacturing, retail, healthcare, pharmaceuticals, and other frontline industries rely on OLOID to securely authenticate deskless workers on shared devices and applications using physical identity factors such as facial recognition, NFC, RFID badges, etc., all while meeting strict security and regulatory requirements. Headquartered in Sunnyvale, California, OLOID is backed by leading investors including Dell Technologies Capital, Yaletown Partners, Honeywell Ventures, Okta Ventures, Unusual Ventures, and Emergent Capital.

For more information, visit www.oid.com.

Garima Bharti Mehta

OLOID INC.

+1 800-711-9123

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/917381882>

EIN Presswire’s priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something 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.

