Saviynt

Customer Story

UKG Unifies Identity Security for a Complex, AI-Forward Enterprise

How a global HCM leader replaced fragmented identity tools with a unified identity security platform — eliminating standing privileges, consolidating 150,000+ identities, and laying the groundwork for AI-era governance.

UKG

Company:
UKG (Ultimate Kronos Group)

Industry:
Software

Segment
Enterprise

Saviynt Capabilities:
- Identity Governance & Administration (IGA)
- Privileged Access Management (PAM)
- Zuma

A Post-Merger Identity Challenge at Scale

Founded through the merger of Kronos and Ultimate Software in 2020, UKG is one of the world's leading providers of human capital and workforce management software. Serving more than 85,000 organizations across 150+ countries and generating approximately $5 billion in annual recurring revenue, UKG's platform supports the frontline workforce that makes up roughly 80% of the global labor market.

But the business success of that merger created a formidable identity security challenge. Combining two large, independently operated SaaS companies meant inheriting two complete, and often incompatible, stacks of identity systems, processes, and tooling. The result was a sprawling environment with up to 10 separate identities per user, three competing Privileged Access Management (PAM) tools running in parallel (CyberArk, BeyondTrust, and a homegrown solution), multiple identity providers including ForgeRock, and fragmented access control mechanisms across a global infrastructure.

For Ajitha Choudary, Vice President of Global Security Engineering and Identity & Access Management at UKG, the mandate was clear: consolidate and modernize before the complexity became a liability.

> **"Like many large enterprises formed through mergers, we had multiple identity processes, technologies, and control models that had evolved over time. Our focus was on simplifying the environment, improving visibility into who had access to what, automating manual processes, strengthening governance, and ultimately reducing identity-related risk."**
>
> **Ajitha Choudary**
> VP of Global Security Engineering and Identity & Access Management, UKG

Building a Unified Identity Control Plane

After engaging GuidePoint Security to assess their identity posture, UKG's team identified two strategic priorities: establishing a strong identity governance and administration (IGA) foundation, and converging PAM and IGA into a single platform. The unified IGA + PAM offering and native support for Google Cloud Platform (GCP) were important factors, but what ultimately set Saviynt apart was its forward vision on non-human and agentic identity security. UKG wasn't just looking for a platform that could support where they were — they wanted a partner aligned on where identity security was heading, particularly as AI began reshaping the threat and governance landscape.

Phase 1: Get the Basics Right

UKG began by automating core Joiner-Mover-Leaver (JML) processes, establishing a reliable identity lifecycle foundation and eliminating the manual provisioning burden that had accumulated across two organizations. Core enterprise applications including Workday and Active Directory were onboarded first, followed by custom-connector applications, and finally databases.

Phase 2: Eliminate Standing Privilege

With the lifecycle foundation in place, UKG turned to the more strategic goal: eliminating standing privileged access entirely. By implementing Just-in-Time (JIT) privilege elevation through Saviynt's converged PAM capability, UKG moved to a zero-standing-privilege model. Today, every domain admin and privileged user request is granted dynamically, for the minimum duration required, and revoked automatically. No standing admin access remains in the environment.

Consolidating three separate PAM tools into the Saviynt platform also resolved significant operational complexity, eliminating redundant integration points, inconsistent policy enforcement, and the overhead of maintaining disparate systems.

Phase 3: Identity Rationalization at Scale

Running in parallel with the tooling consolidation, UKG undertook a comprehensive identity rationalization effort: collapsing multiple accounts per user, consolidating identity providers under a single UKG.com domain, and decommissioning redundant
or orphaned identities. The result was a reduction from more than 150,000 identities to fewer than 25,000, an 83% decrease that dramatically reduced UKG's attack surface and eliminated credential sprawl across the enterprise. The entire transformation was executed in 18 months with minimal
disruption to end users.

> **"The transformation is not about technology — it's about educating your user base on why just-in-time access matters, what risks it reduces, and how it actually enables them. As long as you have the right automated tools in place, there is no reason to have standing privileges."**
>
> **Ajitha Choudary**
> VP of Global Security Engineering and Identity & Access Management, UKG

Security, Efficiency, and Compliance at Scale

The outcomes of UKG's identity modernization program have been measurable and significant across security posture, operational efficiency, and compliance.

83%	40%	73%	100%
Reduction in total identities (150K+ → <25K)	Reduction in provisioning time	Reduction in audit findings	Elimination of standing privileged access (JIT-only)

Access review cycles that previously required large teams of manual reviewers are now automated through Saviynt, accelerating certification campaigns, reducing human error, and freeing the identity team to focus on higher-value governance work. Onboarding and offboarding processes that once stretched over days have been dramatically compressed. Audit findings dropped by 73%, a direct result of consistent, policy-driven governance replacing fragmented manual processes.

The cost impact has been equally meaningful. Retiring CyberArk, BeyondTrust, and multiple legacy IGA tools, along with decommissioning the homegrown provisioning system, has generated multi-million-dollar savings in licensing, integration maintenance, and operationalverhead.

> **"What attracted us to Saviynt was not the ability to support where we are today, but where we wanted to go in the future. We wanted to be aligned with a platform that could give us a single pane of glass across all of our identities — human, non-human, and agentic."**
>
> **Ajitha Choudary**
> VP of Global Security Engineering and Identity & Access Management, UKG

Looking Ahead: Identity as the Control Plane for AI

For UKG, the work is far from complete. With a robust IGA and PAM foundation now in place, the team has turned its attention to what Choudary considers the defining challenge of the next era: governing AI identities.

UKG views AI identity security governance through two lenses: using AI to make identity security more proactive
and risk-intelligent, and governing the growing population of AI agents and machine identities that now operate across the enterprise. Non-human identities, including service accounts, API keys, secrets, certificates, and increasingly autonomous AI agents, are growing exponentially faster than human identities, and traditional governance models were not built to keep pace.

UKG has already established initial visibility into its AI identity landscape and is now advancing toward lifecycle governance, policy enforcement, and privileged access controls for agent identities. The goal is to treat AI agents with the same rigor as human identities: clear ownership, defined lifecycles, least-privilege access, and continuous monitoring.

> **“Before you can govern AI, you need visibility and you need owners. You need to know what AI identities exist, who is accountable for them, and what they are accessing. Without that foundation, you cannot manage risk. Identity will become the primary control plane for AI, and the organizations that establish visibility and ownership first will be the ones that can scale and innovate confidently.”**
>
> **Ajitha Choudary**
> VP of Global Security Engineering and Identity & Access Management, UKG

What drew UKG to Saviynt as a long-term partner, beyond integrated IGA and PAM, was Saviynt’s forward vision on non-human and agentic identity governance, and its willingness to co-develop solutions rather than push pre-packaged answers. Ajitha and her team are design partners for Zuma, the enterprise AI-NHI Identity Security platform which provides the foundation for trusted AI adoption, enabling UKG to securely scale innovation while moving from AI sprawl to AI confidence.

> **“Before you can govern AI, you need visibility and you need owners. You need to know what AI identities exist, who is accountable for them, and what they are accessing. Without that foundation, you cannot manage risk. Identity will become the primary control plane for AI, and the organizations that establish visibility and ownership first will be the ones that can scale and innovate confidently.”**
>
> **Ajitha Choudary**
> VP of Global Security Engineering and Identity & Access Management, UKG

About Saviynt

Saviynt is the identity security platform built to secure the modern enterprise. With Zuma, its complete AI security platform, Saviynt helps organizations build, run, and scale AI with confidence. The world’s leading brands trust Saviynt to reduce risk, improve visibility, and support compliance while enabling business agility. For more information, please visit **www.saviynt.com.**

Saviynt

Headquarters
1301 E El Segundo Blvd, Suite D
El Segundo, CA 90245 USA

310.641.1664
info@saviynt.com
www.saviynt.com