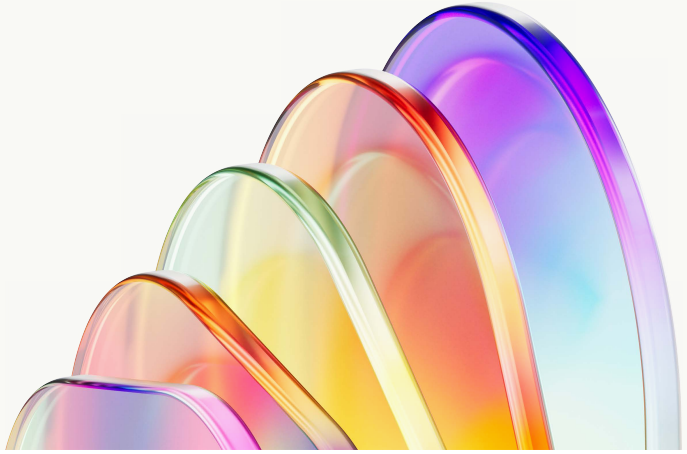
Saviynt

IBM | aws

Solution Guide | Identity Watch

Uncover The Risks Hiding in Your Identity Environment

Discover, prioritize, and remediate risk across AI agent, non-human, and human identities — before attackers find what you're missing.



The addition of AI agents to the enterprise has made an already complex identity security challenge exponentially harder. Identity programs built for human users now must account for autonomous agents and non-human identities spread across on-premises, cloud, and multi-cloud environments.

Without visibility into every identity and the access it holds, risk compounds unknowingly. Disconnected IGA platforms, PAM tools, security solutions, and SaaS applications can't correlate risk across the full environment, leaving organizations exposed in unknown ways.

Introducing Identity Watch from AWS, IBM, and Saviynt

Identity Watch is a structured assessment that completes the risk landscape picture. It discovers and inventories every identity in your environment — human, non-human, and AI agent — evaluates risk and access, and delivers prioritized remediation guidance that security teams can act on in a single, unified engagement.

User registration and third-party onboarding

Onboard contractors, partners, and vendors with a single governed workflow through delegated administration that gives partner organizations the ability to manage their own users while Saviynt maintains centralized policy control. Every third-party identity is registered, governed, and subject to the same controls as internal users from day one.

Discover and inventory every identity. Identity Watch continuously discovers human, machine, and AI agent identities across cloud, SaaS, and on-premises environments — building a complete, auditable inventory of ownership, access, and associated risk, including shadow AI.

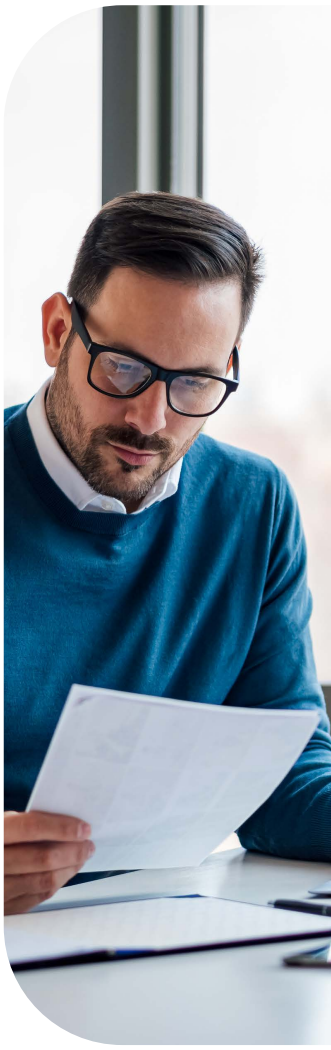
Assess posture across all identity types. A strategic analysis identifies risk and control effectiveness across your entire identity landscape. The assessment uncovers dormant accounts, toxic entitlement combinations, orphaned credentials, broken access workflows, and unauthorized access routes.

Identify active risk. The assessment goes beyond configuration gaps to evaluate behavioral signals — anomalous access patterns, MFA/PAM bypass indicators, unusual agent activity, and identities deviating from baselines — surfacing active risk that static audits miss.

Prioritize and remediate with context. At the end of the assessment, risk findings are scored, prioritized, and delivered with clear remediation guidance. Contextual activity mapping shows exactly how service accounts, users, and AI agents access critical systems so security teams can triage with precision rather than chasing false positives.

Identity Watch maps identity risk and control posture against NIS2, DORA, the EU AI Act, and other regulatory requirements so you can see how well you are maintaining compliance.

Deliver findings to every audience. Technical remediation reports give security operations teams the specifics they need to act. Executive-level findings give board and audit stakeholders evidence of governance posture. Both are generated from the same underlying assessment data.



Identity Watch Helps Uncover

- Dormant accounts and inactive identities holding active credentials
- Terminated users or decommissioned agents with active access
- Toxic entitlement combinations that enable lateral movement and escalation
- Active users with inactive managers operating without oversight
- Anomalous access patterns deviating from peer group baselines
- Shadow AI that can be brought under governance
- Revocation gaps where access removal is operating outside acceptable SLAs

Key Solution Benefits

- **Gain full visibility into every human, machine, and AI agent identity across your environment**
- **Surface hidden risks — dormant accounts, toxic entitlements, shadow AI — before they're exploited**
- **Identify active threat indicators that static audits and periodic reviews routinely miss**
- **Accelerate remediation with prioritized findings and clear guidance delivered within hours**
- **Demonstrate compliance with NIS2, DORA, the EU AI Act and other regulations**
- **Deliver board-ready governance evidence — not just technical reports**

About Identity Watch

Identity Watch is a joint solution between AWS, IBM, and Saviynt, built on proven infrastructure, powered by continuous identity posture management, and driven by intelligent threat detection — delivering the foundation organizations need to govern AI agent, non-human, and human identities at scale.

Next Step

- To learn more about Identity Watch or schedule an assessment, please reach out to your IBM, Saviynt, or AWS account team.

Saviynt

Headquarters
1301 E El Segundo Blvd, Suite D El Segundo,
CA 90245 United States

310.641.1664
info@saviynt.com
www.saviynt.com