



# Identity and Data Security, United

Access governed by what data actually means to your business

As AI agents, service accounts, and APIs expand the modern attack surface, disconnected identity and data governance tools leave security teams blind to who — or what — has access to sensitive information. Cyera and Saviynt close this gap by unifying data classification and identity security through shared telemetry and AI-powered insights. The result: complete visibility across identity and data layers, consistent least-privilege enforcement, accelerated compliance, and proactive risk remediation across cloud, on-premises, and hybrid environments.

## Smarter identity governance through data and access intelligence

Strengthen your security posture by merging data classification and identity security intelligence across all identities — human, non-human, and AI — to enable precise, risk-based access decisions and accelerated remediation. Agentless data discovery and classification surfaces sensitivity, location, and security controls across key assets, while mapping regulatory categories such as PII and GDPR data directly to roles and entitlements. Prioritized remediation recommendations target toxic access combinations, over-privileged accounts, and dormant access to sensitive data — so your team eliminates the highest-risk exposures first and triggers micro-certifications where they matter most.

## Right-size access based on data sensitivity and regulatory context

Enable just-in-time access provisioning for shared accounts and elevated privileges, ensuring users only access sensitive data when necessary. As employees change roles, transfer departments, or leave the organization, dynamically adjust access based on actual data sensitivity, not just application entitlements. Prioritize remediation efforts with highly accurate, risk-based recommendations that help you right-size permissions and enforce least privilege at scale. Automate reviews of high-risk identities and sensitive data, reducing review fatigue while ensuring comprehensive audit trails and continuous governance.

- **Gain holistic visibility across identities, data, and access pathways**
- **Enforce least privilege with time-bound, policy-driven access controls**
- **Prioritize remediation by data sensitivity and toxic access combinations**
- **Dynamically adjust access as roles and responsibilities change**
- **Maintain continuous compliance with streamlined reviews and complete audit trails**

## Maintain continuous compliance and audit readiness

Use AI-driven automation to map sensitive and proprietary data to global regulatory frameworks with high precision, ensuring compliance decisions are grounded in accurate, contextual data intelligence. Streamlined review campaigns confirm access remains appropriate and compliant, while policy-driven controls handle access revocation, privilege right-sizing, and separation of duties enforcement — no manual tickets required. A complete timeline of every change to an identity's access keeps your team audit-ready at all times.

USER	USER NAME	FIRST NAME	LAST NAME	ACCTKEY	ACCOUNT NAME	ENDPOINT NAME	LAST LOGON DATE	IN
10	MJohnson	Merry	Johnson	20452	MJOHNSON	SAP	Jan 01, 1970 12:00 AM	12
10	MJohnson	Merry	Johnson	50536	MJOHNSON	OracleEBS	Feb 09, 2001 12:00 AM	9C
12	mleo	Michael	Leo	26915	MLeo-da95d	SAP	Jan 01, 1970 12:00 AM	10
18	TStark	Tony	Stark	21963	tstark	SAPECC	Oct 08, 2001 12:00 AM	12
10	MJohnson	Merry	Johnson	37553	MJOHNSON	SAPECC	Jan 01, 1970 12:00 AM	2C
11	JHenry	James	Henry	26908	JHenry-db999	SAP	Jan 01, 1970 12:00 AM	19

**Merry Johnson**  
MJohnson • Inactive Days: 120

Enriched by **CYERA**

**Warning:** This dormant account has access to sensitive files

Data Categories

- PII: 3
- PCI: 1
- PHI: 2
- Business & IP: 4

Files (9)

- HR\_Information.docx (Very Sensitive)
- OneDrive / HR
- Confidentialdata.docx (Very Sensitive)
- OneDrive / AD\_Folder
- Business & IP

Ingesting Cyera data classification information into Saviynt streamlines risk identification and remediation.

### About Cyera

Cyera is the world's leading AI-native data security platform, giving organizations a complete view of where their data lives, how it's used, and how to keep it safe, so they can reduce risk and unlock the full value of their data, wherever it is. Cyera is backed by more than \$1.3 billion in funding from top-tier investors including Accel, Coatue, Cyberstarts, Georgian, Lightspeed, and Sequoia. The company's unified data security platform helps businesses discover, secure, and leverage their most valuable asset - data - and eliminate blind spots, cut alert noise, and protect sensitive information across the cloud, SaaS, databases, AI ecosystems, and on-premise environments. Recent innovations like Cyera's AI Guardian solution and Omni DLP extend this platform with adaptive, AI-native data loss protection, bringing real-time intelligence and contextual understanding to how data moves and is used across the enterprise.

### Next Step

- Learn more by visiting [www.saviynt.com](http://www.saviynt.com)
- Schedule a **demo** to experience posture-led security

### About Saviynt

Saviynt's AI-powered identity platform manages and governs human and non-human access to all of an organization's applications, data, and business processes. Customers trust Saviynt to safeguard their digital assets, drive operational efficiency, and reduce compliance costs. Built for the AI age, Saviynt is helping organizations safely accelerate their deployment and usage of AI today. Saviynt is recognized as the leader in identity security, with solutions that protect and empower the world's leading brands, Fortune 500 companies, and government institutions. For more information, please visit [www.saviynt.com](http://www.saviynt.com).



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

310.641.1664  
info@saviynt.com  
www.saviynt.com