

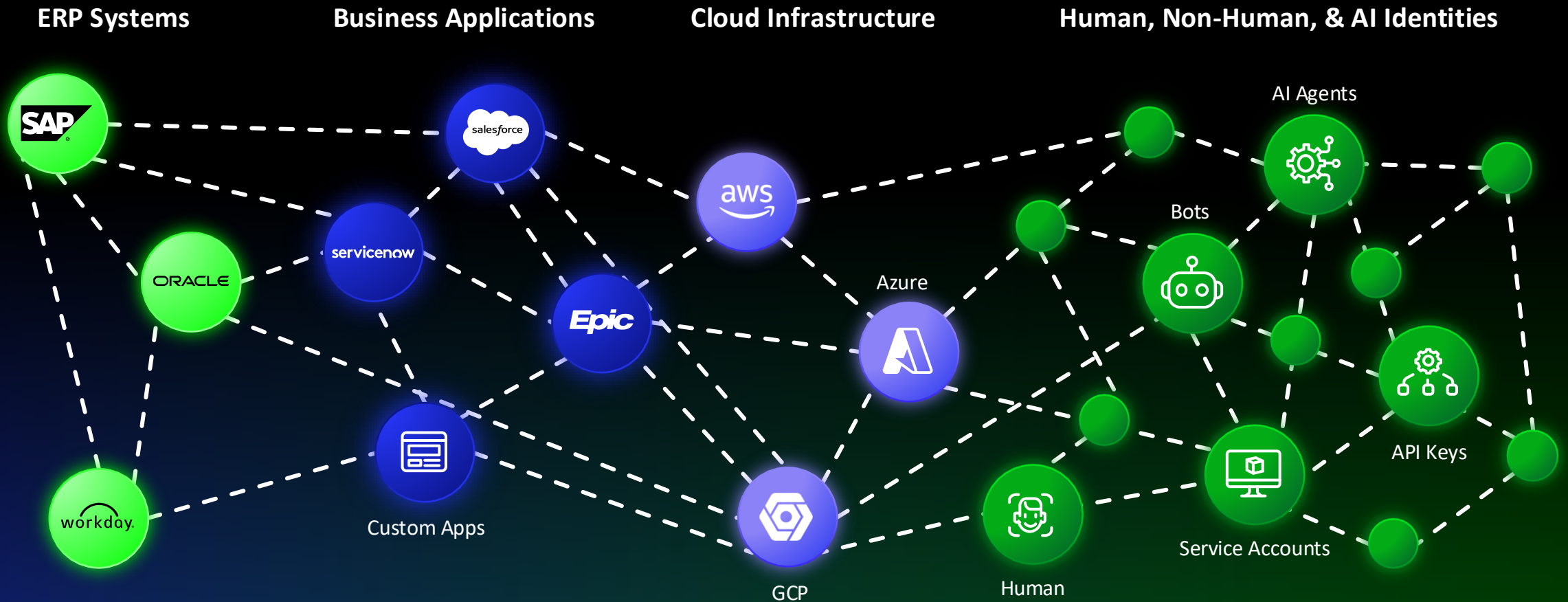


SAP Security and Governance at an Inflection Point: *Rethinking the Model*

October 2026



Enterprise access risk spans your entire application and infrastructure ecosystem

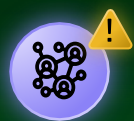
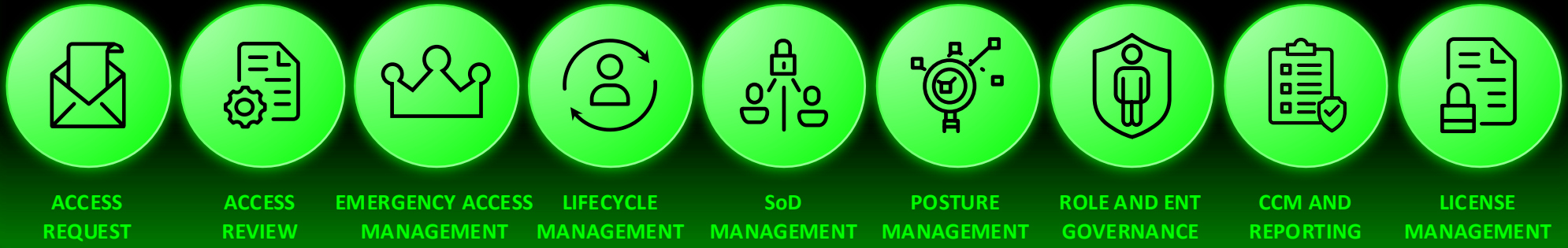


The ERP ecosystem is in flux...

Is it a disruption or an opportunity?



Why Saviynt for mission critical apps and platforms?



The security model is very complex, unique and hierarchical



Security typically managed in silos by point solutions—misses enterprise identity context and cross-app risks



Misses managing all types of non-human and agentic identities



Longer, intensive audits and Higher cost of compliance



Saviynt: a global leader in Identity Security

Company scale



1,400+ employees



625+ enterprise customers



100M+ identities governed

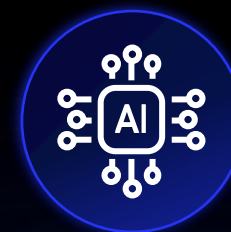


98% customer retention

Platform positioning



100% cloud-native



AI-powered identity security platform



Unified governance across applications, cloud, and infrastructure

Identity Governance • Application Access Governance • Privileged Access • Identity Security Posture

What independent analysts say

Saviynt named a leader in SAP Access Control and Security by KuppingerCole



Saviynt named a leader in Business Application Risk Management by KuppingerCole



Saviynt Reviews by Gartner Peer Insights (4.8/5)



80+ verified reviews • Application Access Governance
400+ verified reviews • Saviynt Identity Cloud Platform

Top-rated in SAP Identity Security vs.
SAP GRC • Pathlock • Others

Saviynt for SAP

Agentic AI Workflows

Posture Management

Lifecycle Management

SoD Management

Transaction Monitoring

Emergency Access Management

Access Request and Review

License Intelligence

Access Gateway



MCP Aware Services



Identity Security Data Fabric

Identities (human, non-human, agents) + MCP servers

Access

Configurations

Policies

Events

Usage

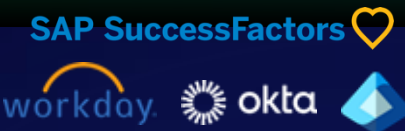
Assets



Discover, classify, manage, monitor



Identity
Sources



IaaS



Multi-Agent
Frameworks



SaaS/ERP



Vector
Databases



Managed AI/
LLM Providers



Third-Party
Security Providers



Saviynt SAP 2025 Clean Core Certification


SAP Certified
for clean core with SAP S/4HANA Cloud

Certified integration validated for
security, upgrade, and compliance
reliability

[SAP Certified Solution Directory Listing](#)
[Saviynt Announcement](#)

ABAP Conditional Clean Core (Level C)

Aligned to SAP's new rating system

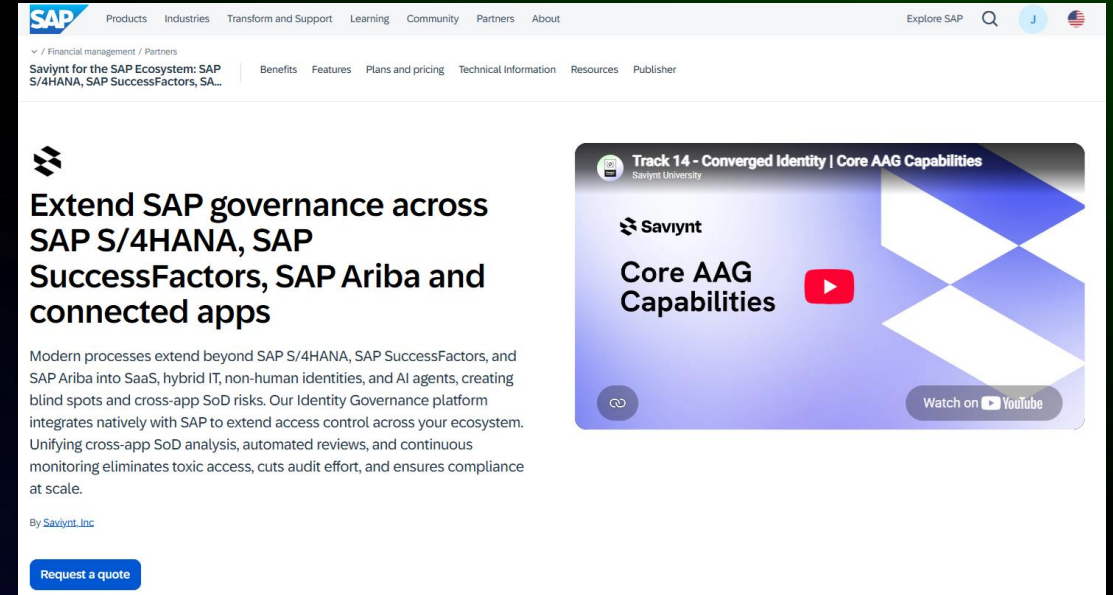
Passed CVA security and uninstall requirements

Upgrade-safe without custom-code remediation

Certified for SAP S/4HANA 2023 as well

AVAILABLE

SAP Store



Extend SAP governance across SAP S/4HANA, SAP SuccessFactors, SAP Ariba and connected apps

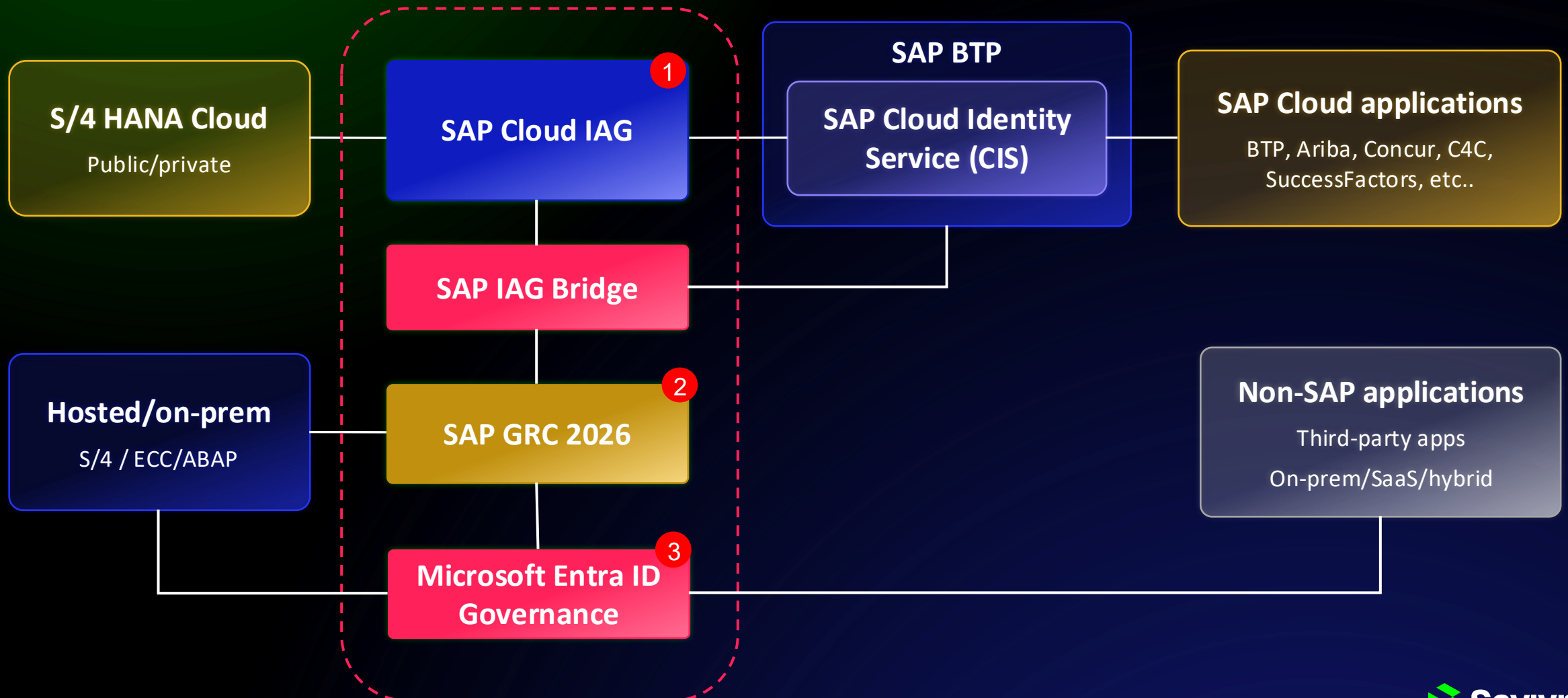
Modern processes extend beyond SAP S/4HANA, SAP SuccessFactors, and SAP Ariba into SaaS, hybrid IT, non-human identities, and AI agents, creating blind spots and cross-app SoD risks. Our Identity Governance platform integrates natively with SAP to extend access control across your ecosystem. Unifying cross-app SoD analysis, automated reviews, and continuous monitoring eliminates toxic access, cuts audit effort, and ensures compliance at scale.

By Saviynt Inc

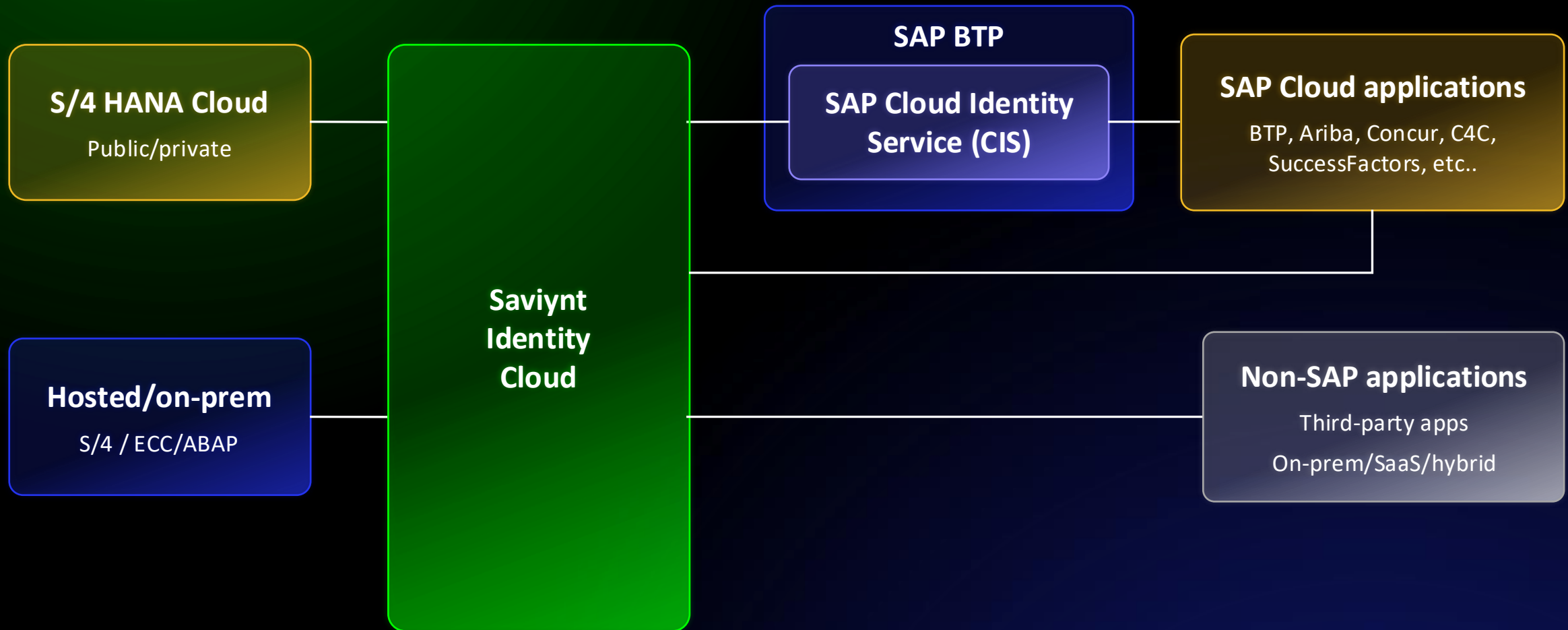
[Request a quote](#)

Easy to find. Easy to procure.

Future Reference Architecture from SAP



IAM & GRC Simplification with Saviynt for SAP



Violations Workbench (SoD)

For intelligent analysis and collaborative risk remediation



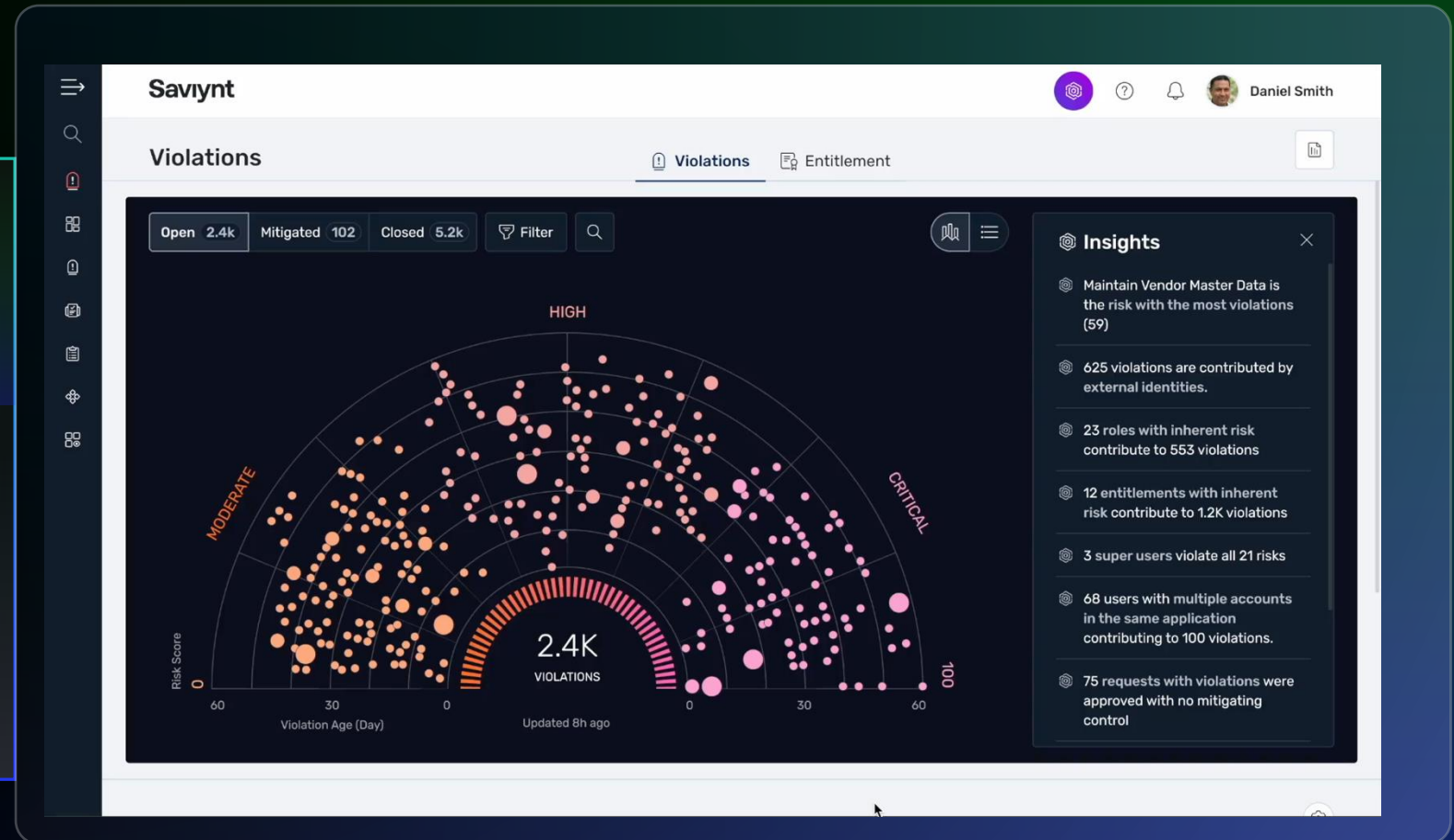
Risk Owner

“

How do I help the business prioritize SoD violations?

How can I continuously monitor sensitive access (SA), SoD and other security controls?

”



Violations

Violations

Entitlement



Open 2.4k

Mitigated 102

Closed 5.2k

Filter



Insights



Supplier Master Data vs. Process Payments is the risk with the most violations (59)

625 violations are contributed by external identities.

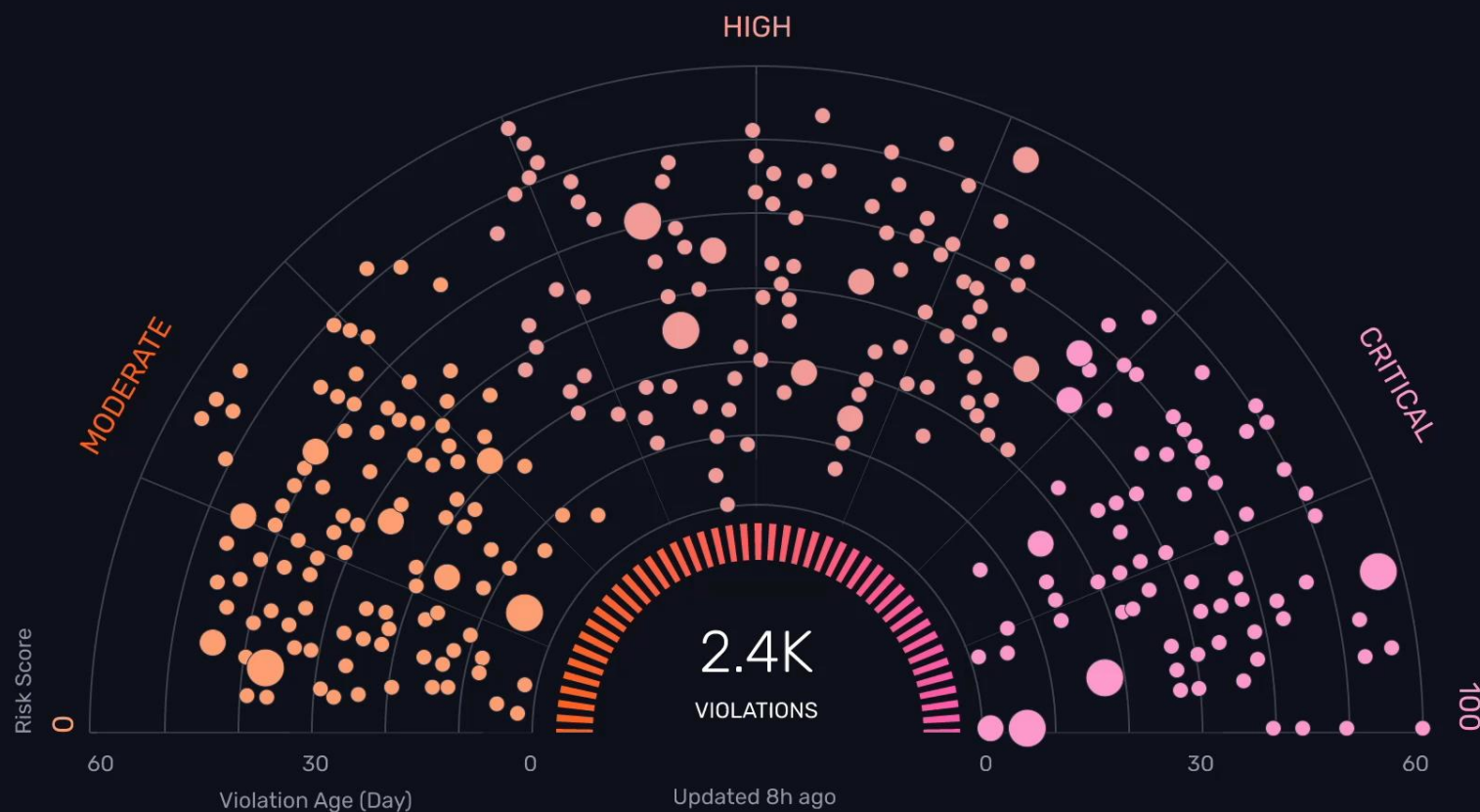
23 roles with inherent risk contribute to 553 violations

12 entitlements with inherent risk contribute to 1.2K violations

3 super users violate all 21 risks

68 users with multiple accounts in the same application contributing to 100 violations.

75 requests with violations were approved with no mitigating control



Violations

\$ Exposure

Violations

All

Realized

Potential

TOTAL EXPOSURE

\$119.0M

REALIZED • ACTUAL

\$36.0M

POTENTIAL • AT RISK

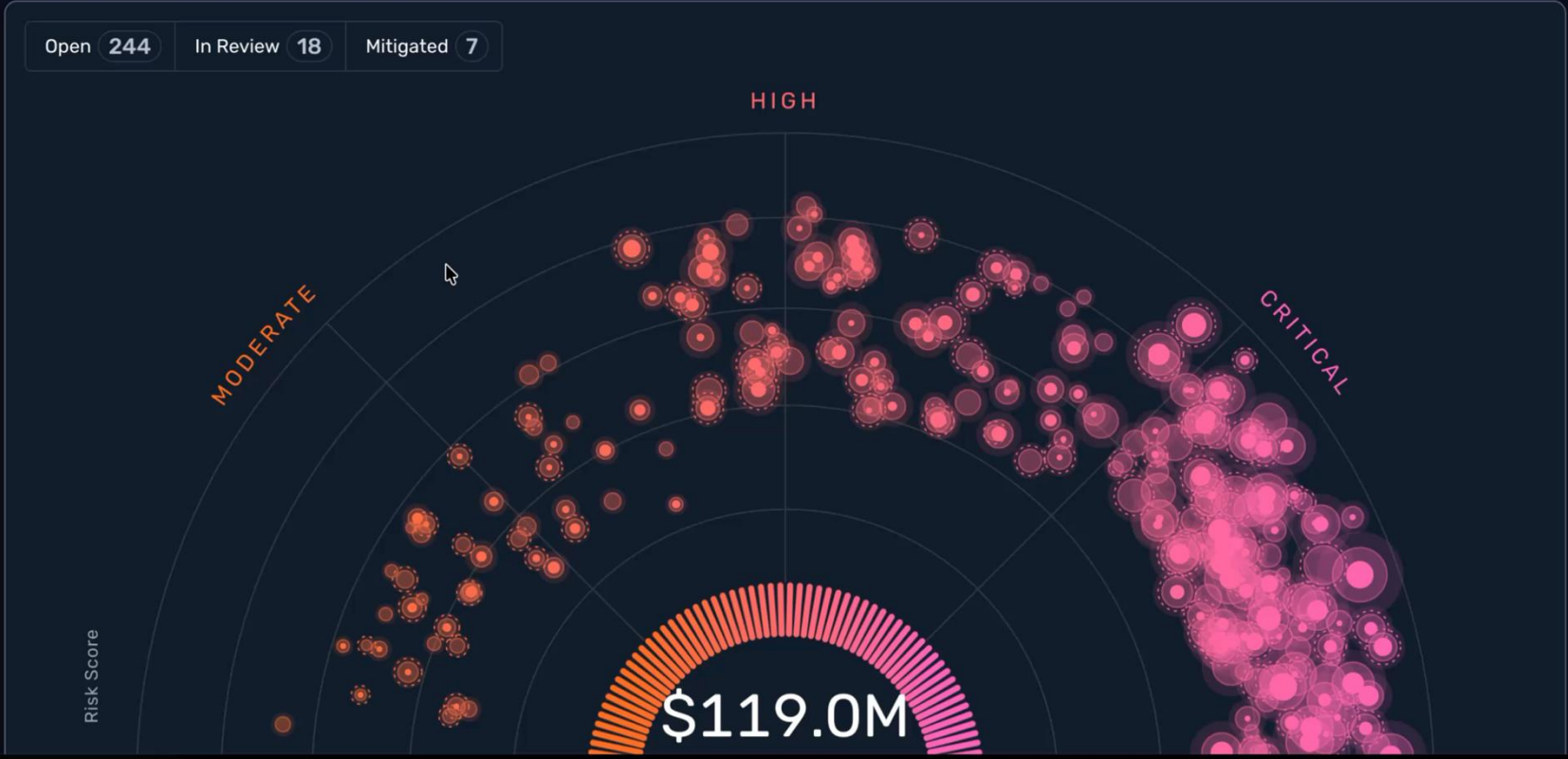
\$83.0M

VIOLATIONS

244

IDENTITIES • TXNS

27 • 3,184



Exposure by risk

Aggregated from every violating user's transactions. Click to filter.

Post Journal Entries and Approve Journal Entries

\$26.8M

\$6.8M realized • \$20.0M potential • 30 violations • 17 users

Maintain Vendor Master Data and Approve Invoice

\$24.9M

\$8.2M realized • \$16.7M potential • 32 violations • 19 users

Approve Time Entries and Process Payroll

\$22.4M

\$7.0M realized • \$15.3M potential • 33 violations • 19 users

Maintain Bank Details and Execute Payment Run

\$18.3M

\$4.9M realized • \$13.4M potential • 30 violations • 17 users

Intelligent Emergency Activity Log Monitoring

For tracking and assurance of high-risk access activities



Privileged Asset Owner

“

How can I quickly review the emergency access activities?

How do I know if there are any anomalies?

”

SAP

SAP S/4 Hana, EAM_SAPFFID

Details

Audit Fail

Audit Pass

Insights

Filter

Sort

Column

Requested T-Codes

Risk Analysis

5

Low

100% display-only T-code executed

No critical changes detected

No policy violations observed

No suspicious activity during session

User followed expected behavior patterns

Recommendation

If everything looks good, mark this session as reviewed and compliant.

Audit Pass

03/26/2025, 13:31

Logon successful (type=A, method=P)

T-Code

Session Manager

Severity

Medium

Audit Class

Logon

Log ID

00001

03/26/2025, 13:31

Transaction SE37 Started

T-Code

SE37

Severity

Low

Audit Class

Transaction start

Log ID

00001

03/26/2025, 13:31

Transaction PFCG started

T-Code

PFCG

Severity

Low

Audit Class

Transaction start

Log ID

00001

03/26/2025, 13:31

Generic table access call to USR02 with activity 02 (auth. check: passed)

T-Code

USR02

Severity

Low

Audit Class

Transaction start

Log ID

00001

03/26/2025, 13:31

Dynamic ABAP code: Event -, event type II, check total ZSAVIYNT_LOGDATA_TEM...

T-Code

SU01

Severity

Low

Audit Class

Other

Log Type

00001

© 2026. Saviynt Inc. All Rights Reserved.

Saviynt

Identity compliance with license intelligence

For aligning application access with license entitlements and business value

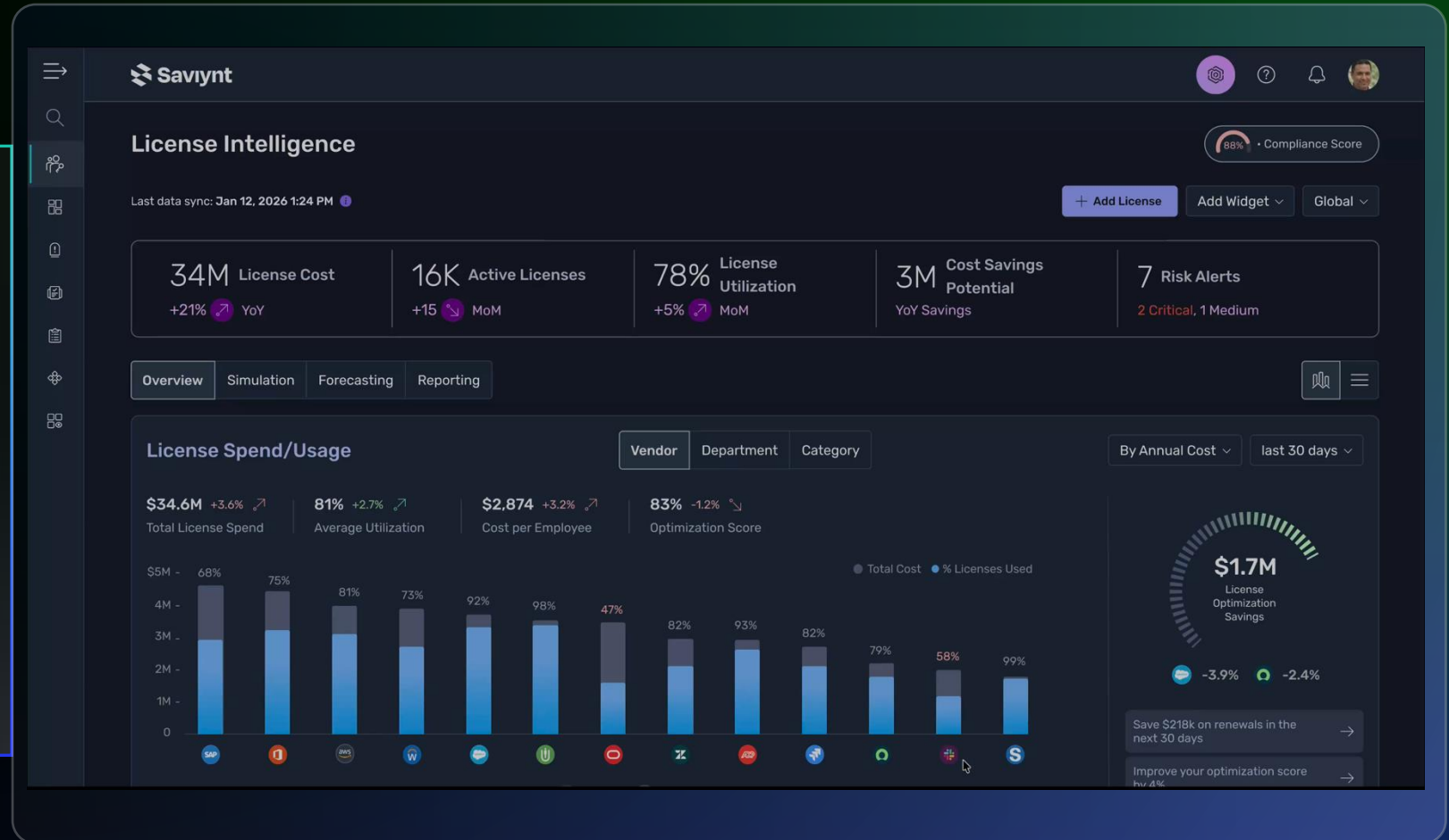


Application Owner

“

Am I assigning the right licenses based on how users actually access and use my applications?

”



Cross Application Risk Visibility

For identifying risks across SAP and Non-SAP landscape

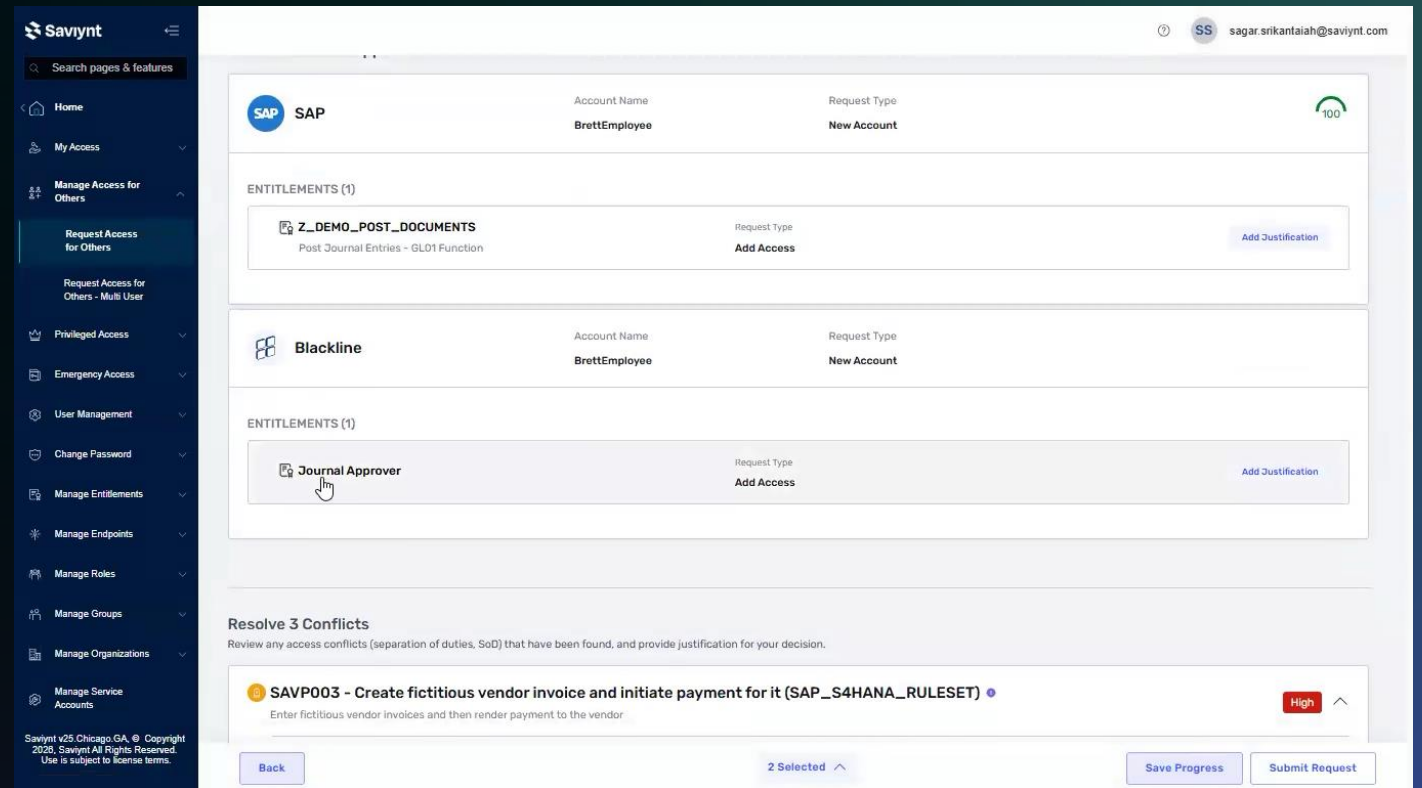


Compliance Owner

“

How can I understand risk landscape across different applications - SAP and Non-SAP?

”



The screenshot displays the Saviynt web application interface. On the left is a dark blue sidebar with a search bar and a list of navigation items: Home, My Access, Manage Access for Others, Request Access for Others, Request Access for Others - Multi User, Privileged Access, Emergency Access, User Management, Change Password, Manage Entitlements, Manage Endpoints, Manage Roles, Manage Groups, Manage Organizations, and Manage Service Accounts. The main content area is white and shows two sections for access requests. The first section is for 'SAP' with 'Account Name: BrettEmployee' and 'Request Type: New Account'. It lists one entitlement: 'Z_DEMO_POST_DOCUMENTS' with 'Request Type: Add Access' and an 'Add Justification' button. The second section is for 'Blackline' with the same account name and request type. It lists one entitlement: 'Journal Approver' with 'Request Type: Add Access' and an 'Add Justification' button. Below these sections, a 'Resolve 3 Conflicts' section is visible, showing a conflict titled 'SAVP003 - Create fictitious vendor invoice and initiate payment for it (SAP_S4HANA_RULESET)' with a 'High' risk level. At the bottom, there are buttons for 'Back', '2 Selected', 'Save Progress', and 'Submit Request'. The top right corner shows the user's profile and email: 'sagar.srikantiah@saviynt.com'.

Intelligent Access Certification

For aligning application access with license entitlements and business value



Access Reviewer

“

Need help in going through
access of all my reportees

”

The screenshot displays the Saviynt web application interface. At the top, the header shows the Saviynt logo and a user profile icon. Below the header, the page title is "Certification for SAP Access Reviews". A navigation sidebar on the left contains icons for home, search, reports, settings, and a clock. The main content area features a "Certification List" section with buttons for "Refresh Progress" and "Export". Below this is a table with columns: DUE IN, CAMPAIGN NAME, CERTIFICATION NAME, TYPE, START DATE, CERTIFIER, and ACTION. The table contains one entry for "SAP Access Reviews" with a due date of "79 Days" and a certifier "margaretmanager (Margaret Manager)". The action column shows a "Resume Certification [0%]" button. At the bottom, it indicates "Showing 1 to 1 of 1 entries" with pagination controls.

DUE IN	CAMPAIGN NAME	CERTIFICATION NAME	TYPE	START DATE	CERTIFIER	ACTION
79 Days	SAP Access Reviews	SAP Access Reviews - margaretmanager (Margaret Manager)	User Manager	Mar 08, 2025	margaretmanager (Margaret Manager)	Resume Certification [0%]

Thank You

