



SAP Cloud Identity Services supporting Agentic AI and SAP-managed Scenarios

[SAP User Groups Events](#)

PUBLIC

July 16th 2026



Agenda

01

Introduction

SAP Cloud Identity Services and their role for the Autonomous Enterprise

02

Agent Identity & SAP Business AI Platform

Agent Governance & Security with the Cloud Identity Services

03

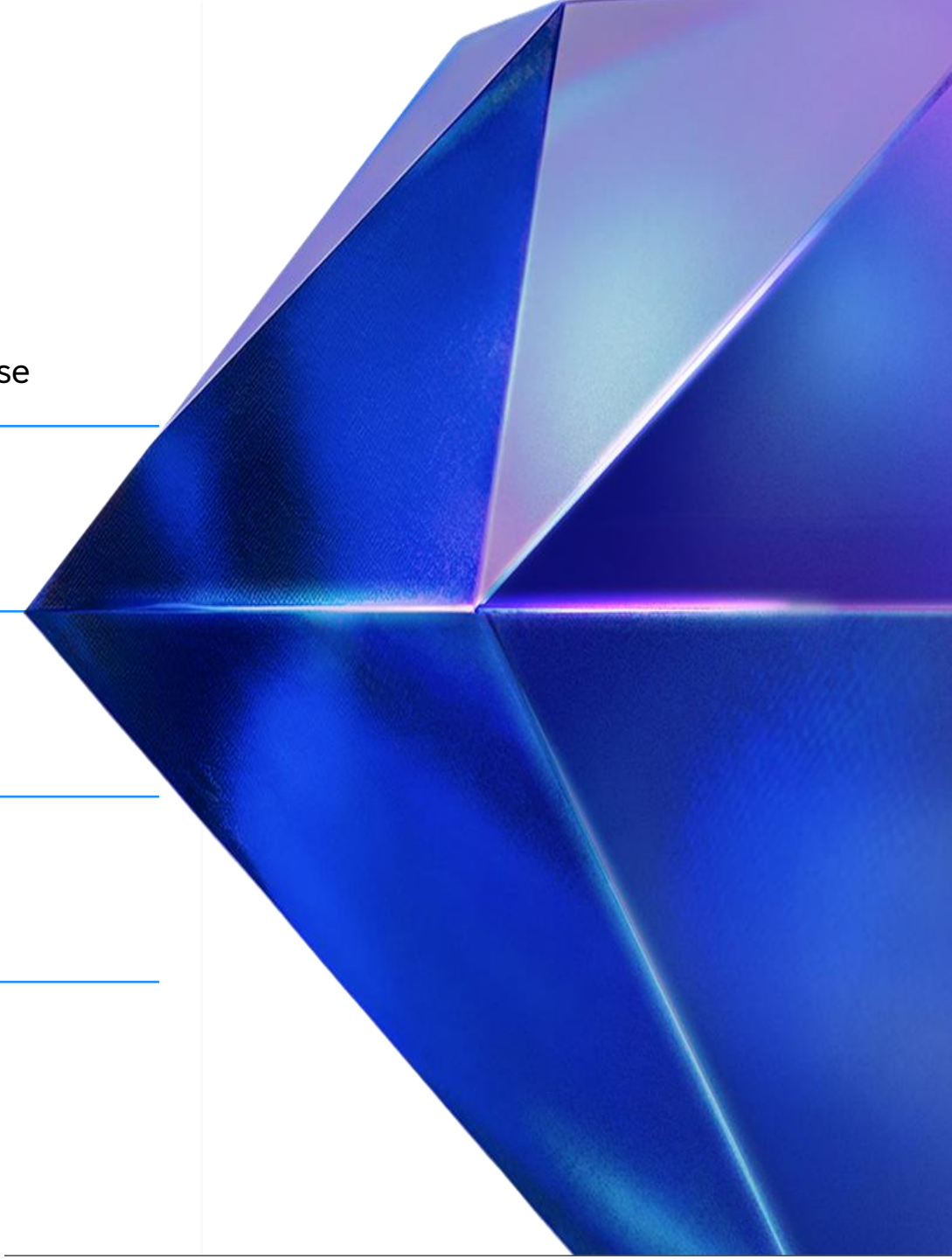
SAP Managed Scenarios

Changes in the shared responsibility model

04

Summary

Key Takeaways



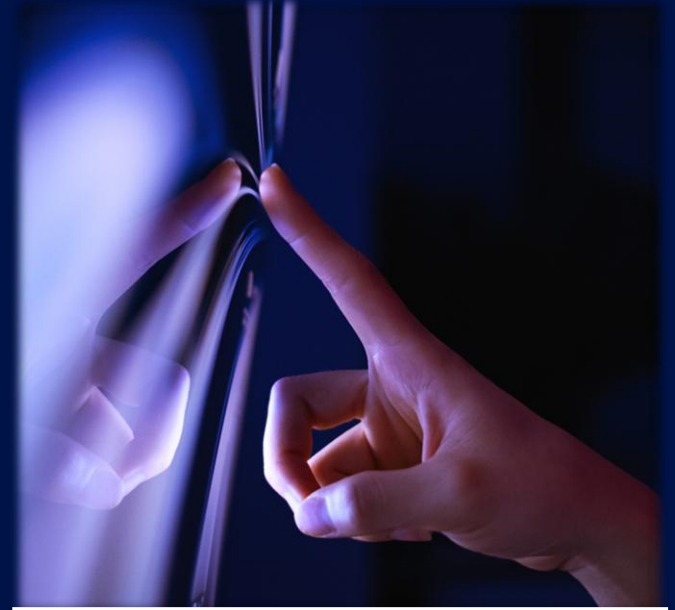
Key Areas of Identity Access Management



**Consistent identity
lifecycle management**



**Authorization
Management**



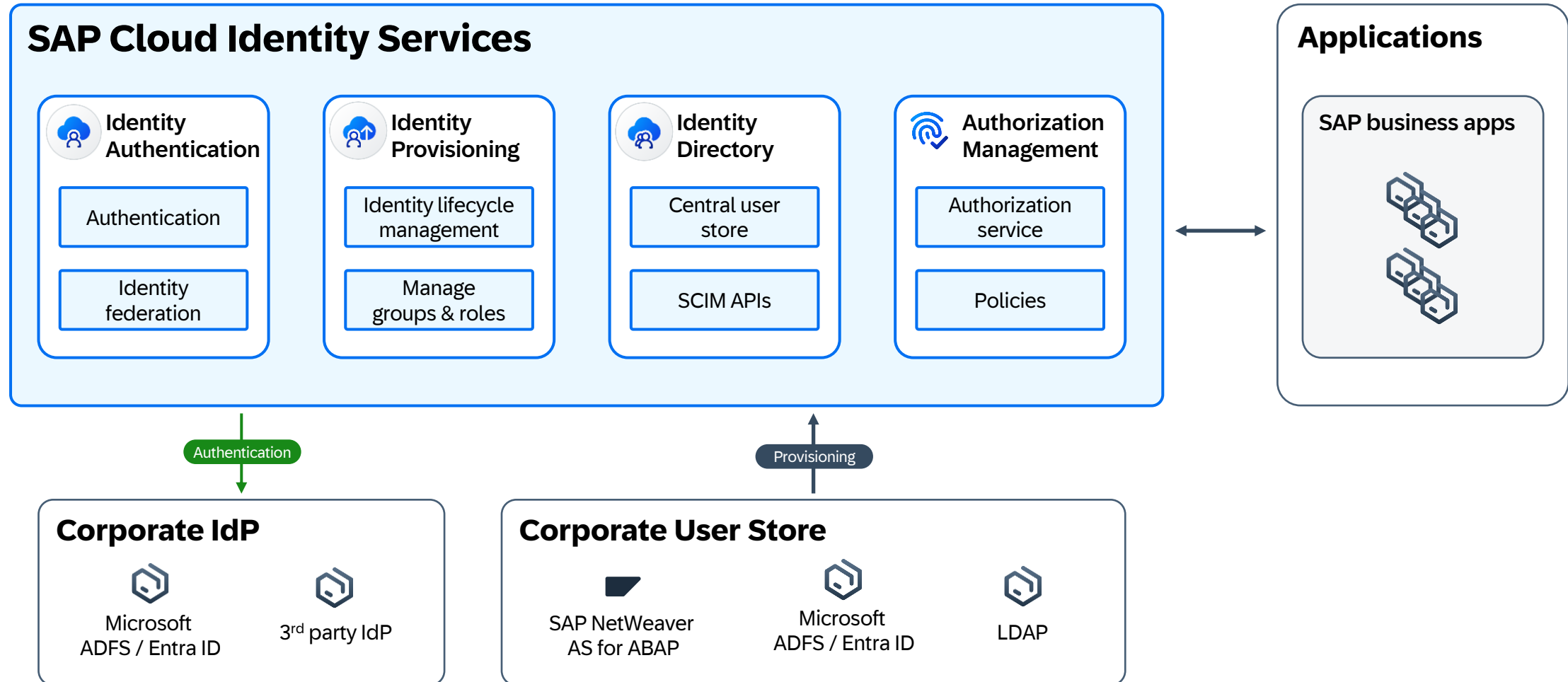
**Authentication and
Single Sign-on**

Consistent Security and Identity Access Management established with SAP Cloud Identity Services

The SAP Cloud Identity Services are a key component to ensure Consistent Security and Identity Management for SAP solutions with:

- Central user store for SAP cloud applications (Joule!)
- Consistent protocol support for customer IAM (SAML/OIDC, FIDO, SCIM, ...)
- Consistent security feature set for SAP cloud applications
- Authentication broker for multiple IdPs
- Application specific attribute mapping and enrichment of tokens by corporate IdP
- Feature support for non-standard integration scenarios
- Adoption of new technologies
e.g. step-up-authentication, context-based authorizations

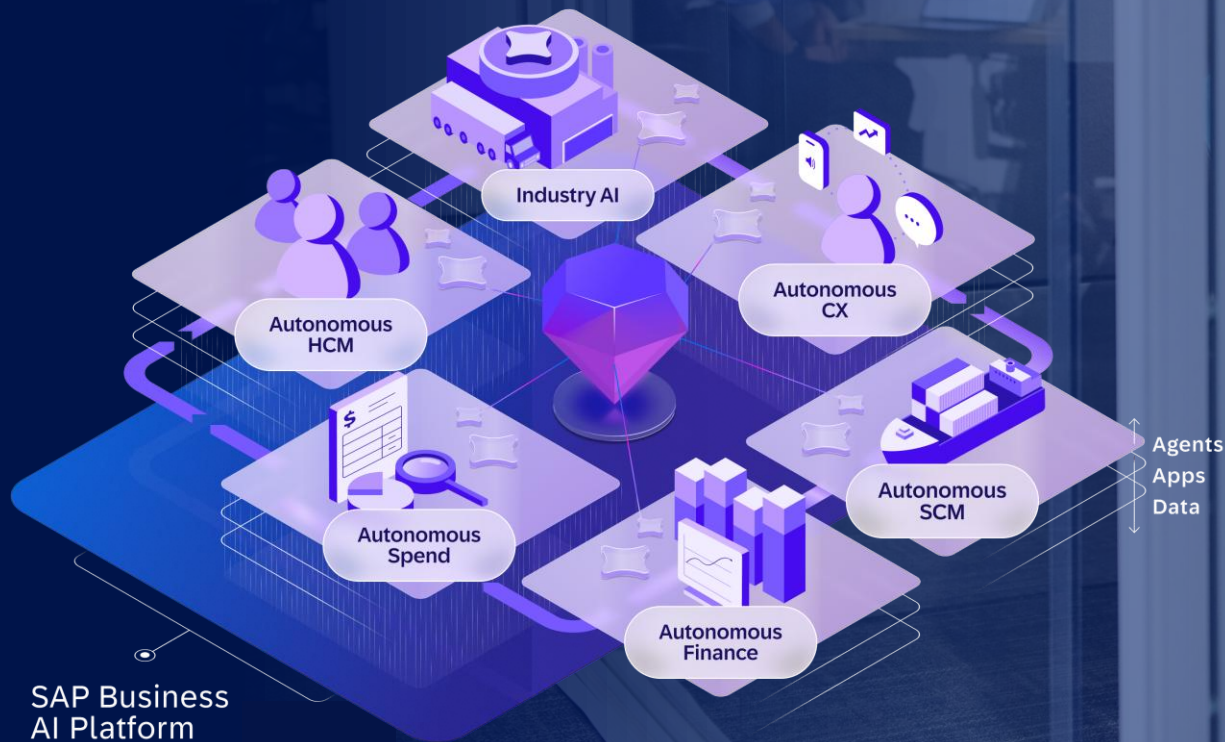
SAP Cloud Identity Services



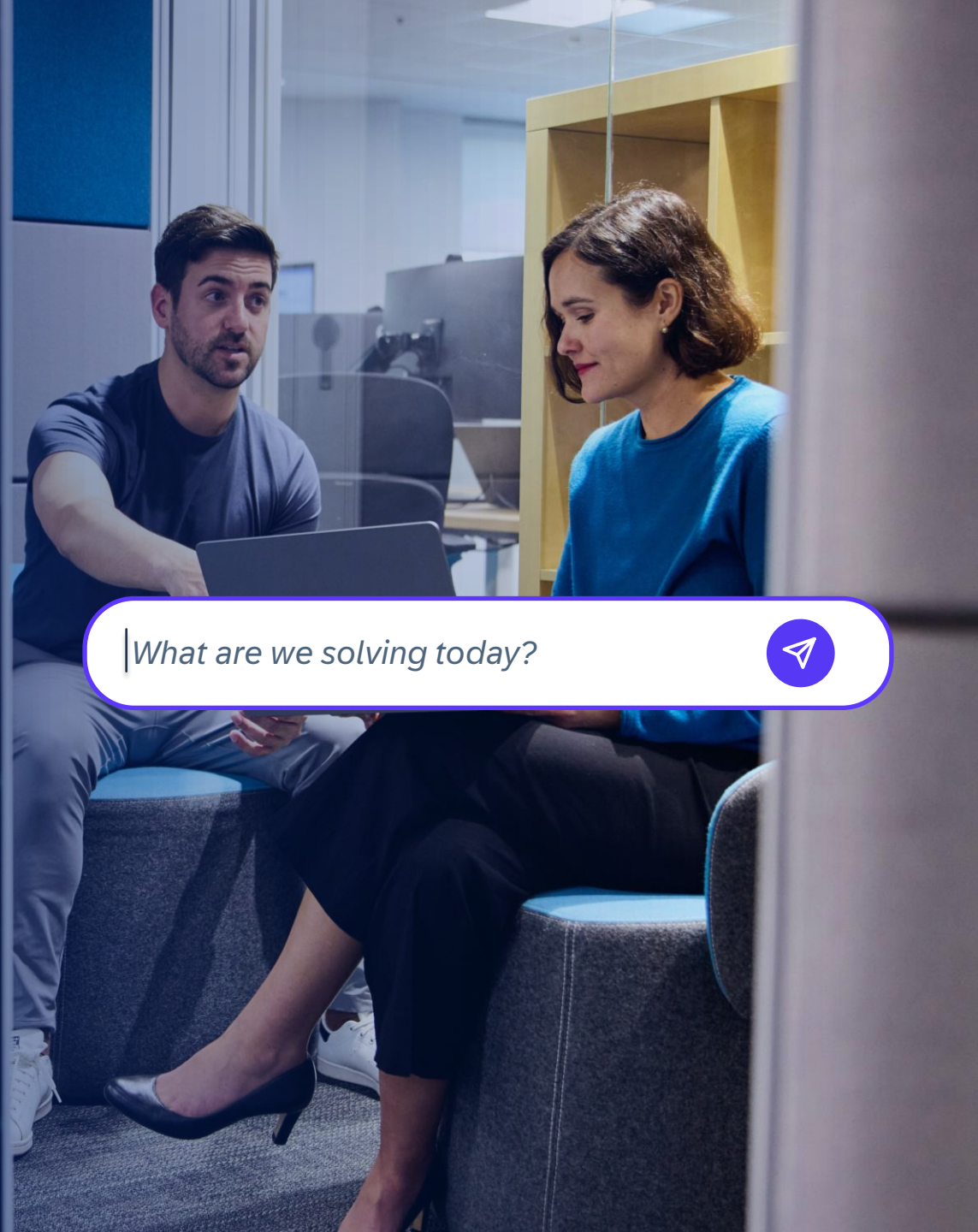
The Beginning of Better.

Welcome to the Autonomous Enterprise

People set the direction. AI executes.



|What are we solving today?



Agenda

01

Introduction

SAP Cloud Identity Services and their role for the Autonomous Enterprise

02

Agent Identity & SAP Business AI Platform

Agent Governance & Security with the Cloud Identity Services

03

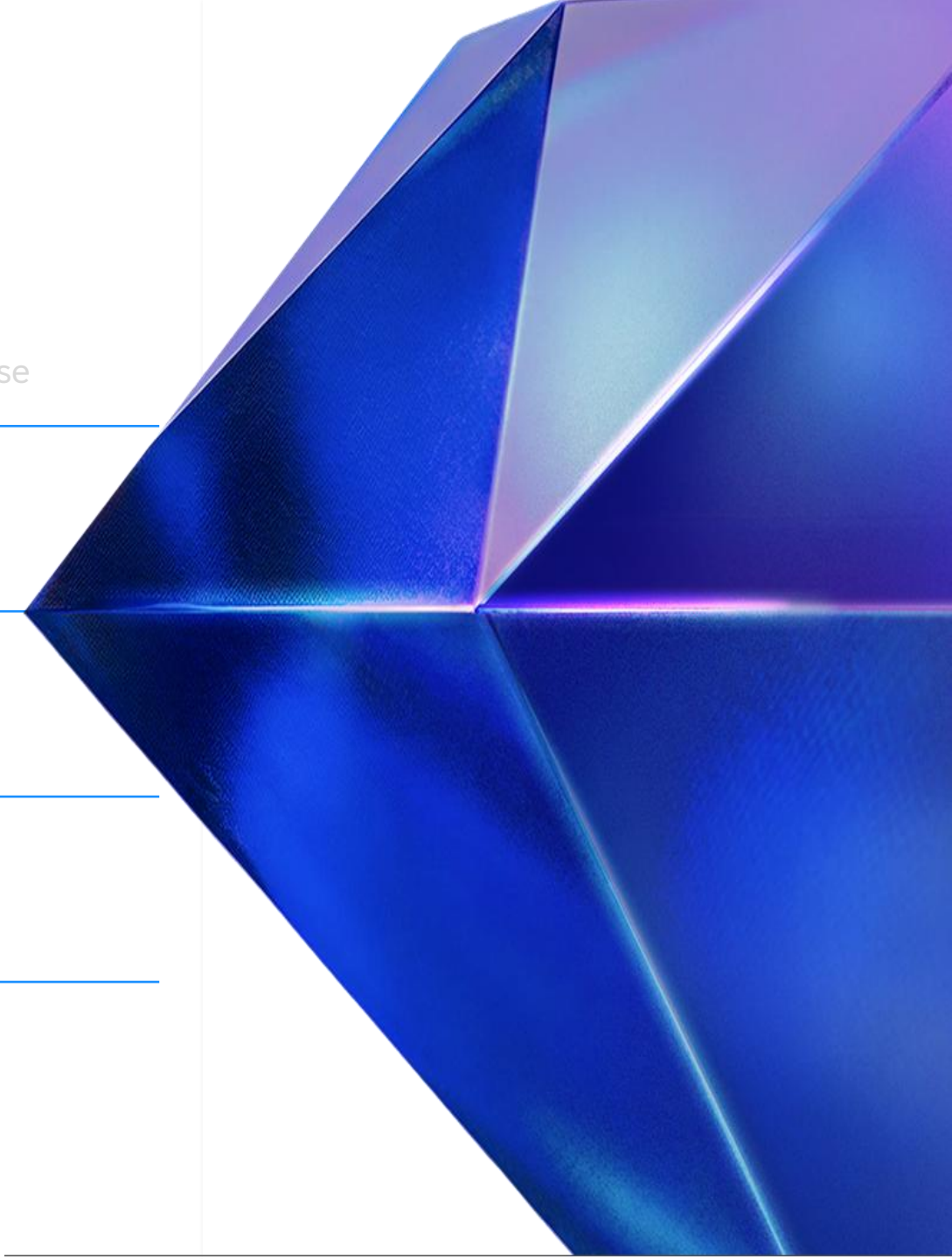
SAP Managed Scenarios

Changes in the shared responsibility model

04

Summary

Key Takeaways



Joule



Finance



Spend



SCM



HCM



CX



Industry AI

SAP Autonomous Domains



accenture



Capgemini



IBM



... And more

Partner Agents



... And more

Third-party AI Agents

SAP AUTONOMOUS SUITE



Build

Joule Studio



n8n



Vercel



CURSOR



Claude Code



CURSOR

... And more

SAP Integration Suite



Contextualize & Reason

SAP Knowledge Graph



Business Data



Business Process



Industry

SAP & Non-SAP Models



PRIOR



OpenAI



cohere



... And more

SAP Business Data Cloud

SAP and Non-SAP
Business Data Fabric



... And more



Govern

SAP AI Agent Hub



Google



... And more

Value Realization

Joule Studio Runtime



Identity, Access, Security

SAP BUSINESS AI PLATFORM

Security is a Must for Business AI Scenarios

Strong execution in compliance, security, and integration is not overhead.
It is the operating system of trust in SAP's new reality



AI agents introduce a new class of identities that often sit outside traditional IAM design* (without reuse)



Change in defence posture balance

Direct connectivity to production data

Misconfiguration or compromise can turn into large-scale data breach



Agents are:

- ✓ Indeterministic
- ✓ Ambitious
- ✓ Use every credential they find
- ✓ Have memory
- ✓ Are supportive to get „social engineered“

Agent Identity

Agents...

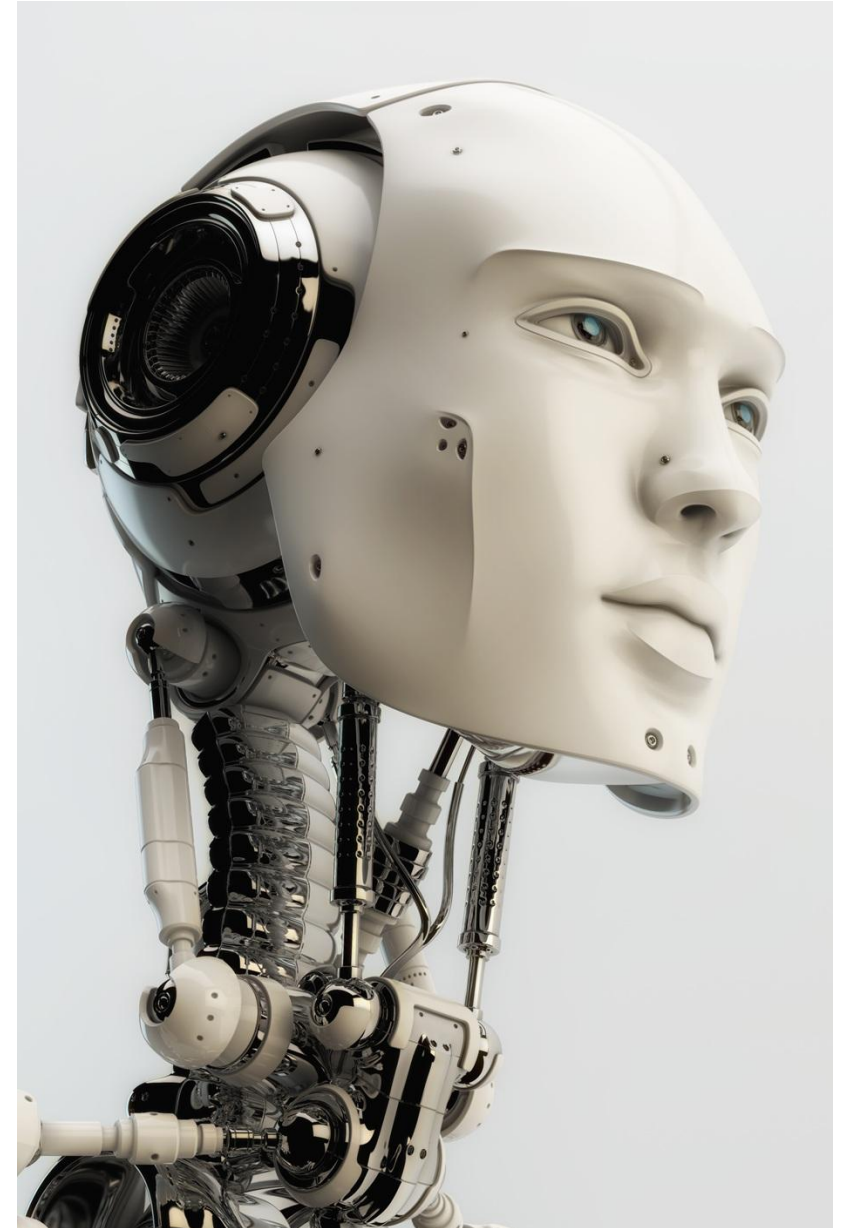
- are applications (deterministic)
- use LLMs (indeterministic)
- have a feedback loop and a memory

Main scenarios

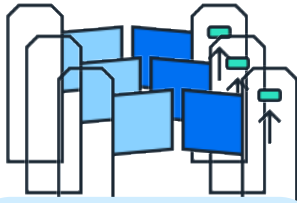
- Agent identity acts in the name of the human identity
- Agent identity acts on its own

Artifacts in SAP Cloud Identity Services

- Application with trust to SAP Agent Gateway
- Agent user with a (global user) ID
- Policy- & role-assignments



Business AI Platform – Authorization checks

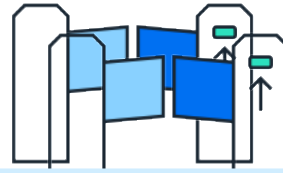


1/3 Agent-Access

WHAT: Check if the Human-Identity or Agent-Identity is allowed to use the agent.

WHERE: SAP Business AI Platform
(SAP Agent Gateway)

HOW: Token-check about policy-assignment in
SAP Cloud Identity

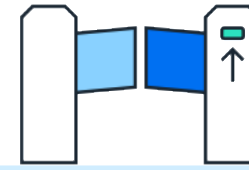


2/3 Scoped-Authorizations*

WHAT: Functional policy enforcement when an agent calls a tool/API/MCP.
Scoped authorization approach to intersect Agent-Identity- with Human-Identity-access

WHERE: SAP Business AI Platform
(SAP Agent Gateway)

HOW: SAP Cloud Identity Services intersect
"scoped authZ" into the token



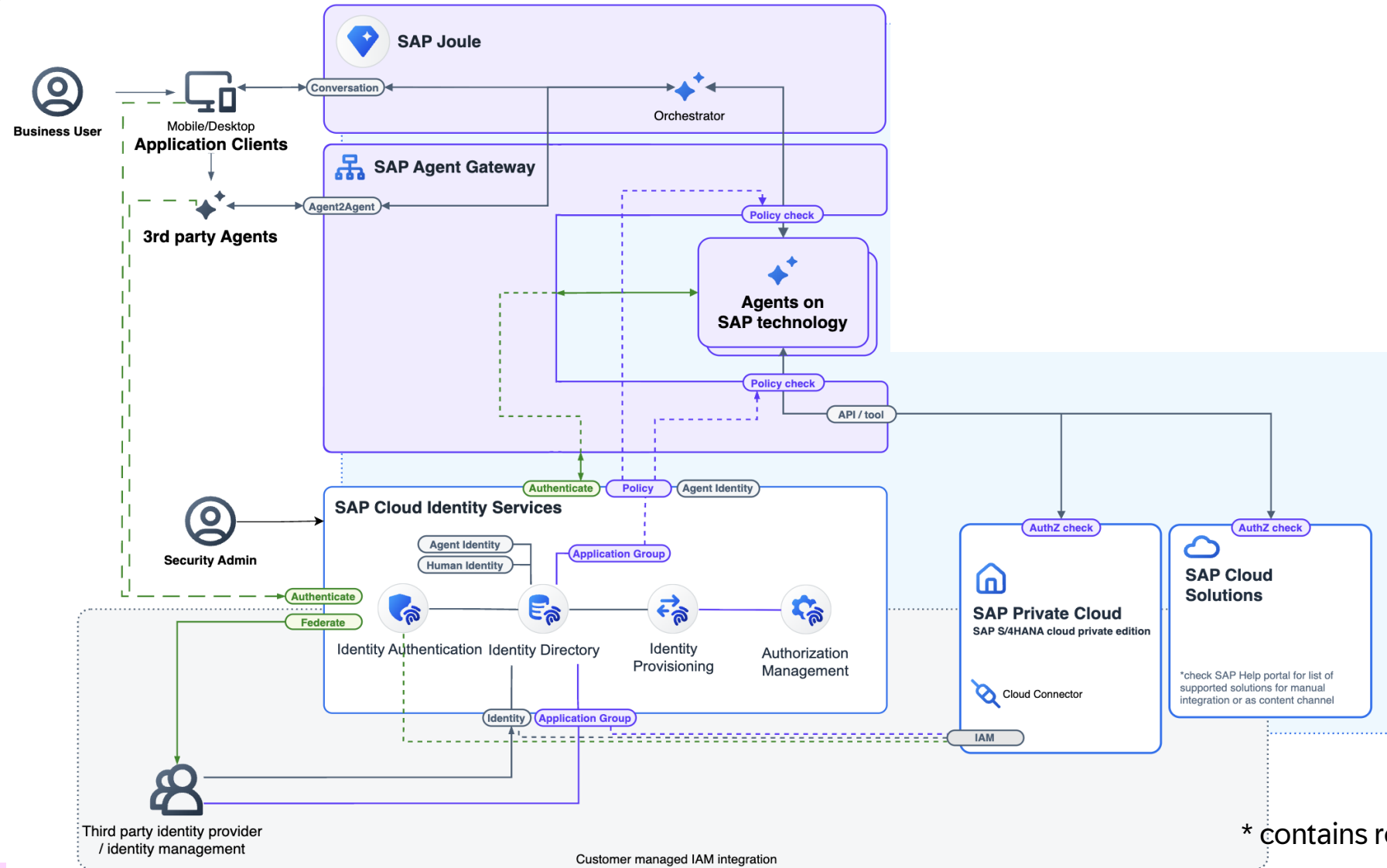
3/3 Application-Authorizations

WHAT: Detailed authorization check including attribute restrictions in the SAP application based on the application-specific authorizations.

WHERE: SAP application

HOW: Authorization-Check
with application engine

Agent Identity



Agent Configuration

Labs preview
final UI in preparation

The screenshot displays the SAP Cloud Identity Services Administration Console. The browser address bar shows the URL: `https://rado-ids.sci-lab.cc.eu-dc-1.cloud.sap/admin/#/agents/5ul9c034-ef41-4f6e-95dc-9dc53f21f0dc/agentAuthorizations`. The page header includes the SAP logo, "Cloud Identity Services", "SANDBOXES", and the user "ids". The navigation menu contains "Home", "Users & Authorizations", "Applications & Resources", "Identity Providers", and "Monitoring & Reporting".

The main content area is divided into two sections. On the left, the "Agents" section shows a search bar and a list of agents:

Agents (3)		Create	Delete	⚙️
☐ Display Name	Authorized to Access Applications			
☐ AGW				
☐ My Agent	SAP SuccessFactors			
☐ SAP Agent	S4 Hana 1 more			

On the right, the "My Agent" section shows details for the selected agent:

My Agent Manage Agent Delete

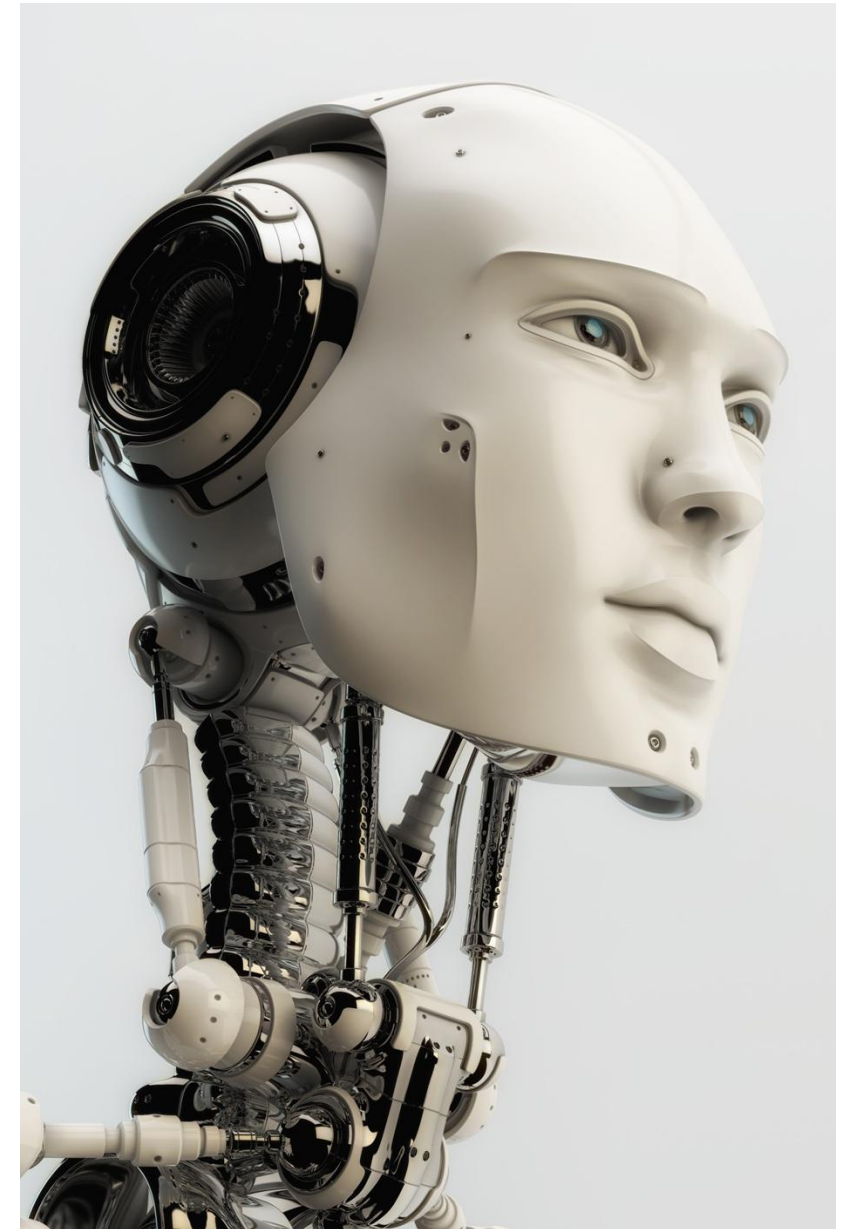
Created On: 08/Jun/2026 09:26 Owner: dummy
Last Modified: 09/Jun/2026 07:11

The "Authorizations" tab is active, showing a table of policies:

Policies			Search	Q
Application	Permissions	API		
SAP SuccessFactors	write	CE_API_CREDIT_REQ_0001		

Agent Governance

- SAP Agent Hub
 - Gives the insights into the landscape
- SAP Joule Studio
 - Allows agent creation out of a conversation
- SAP Agent Gateway
 - Encapsulates the agent communication
- SAP Cloud Identity Services
 - Holds the **Agent Identity**
 - Offers the policy management
 - Issues tokens to agents for SAP



Agenda

01

Introduction

SAP Cloud Identity Services and their role for the Autonomous Enterprise

02

Agent Identity & SAP Business AI Platform

Agent Governance & Security with the Cloud Identity Services

03

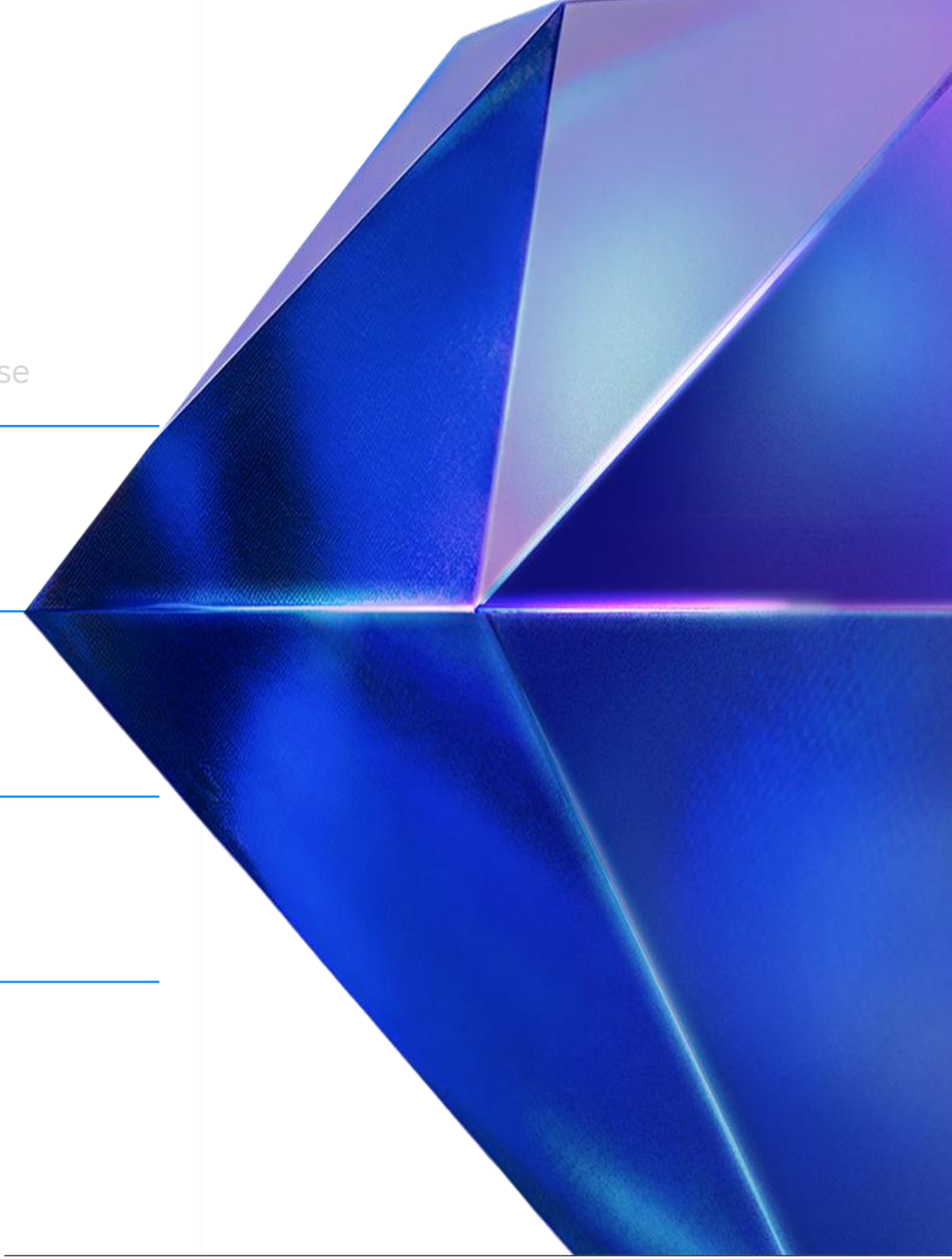
SAP Managed Scenarios

Changes in the shared responsibility model

04

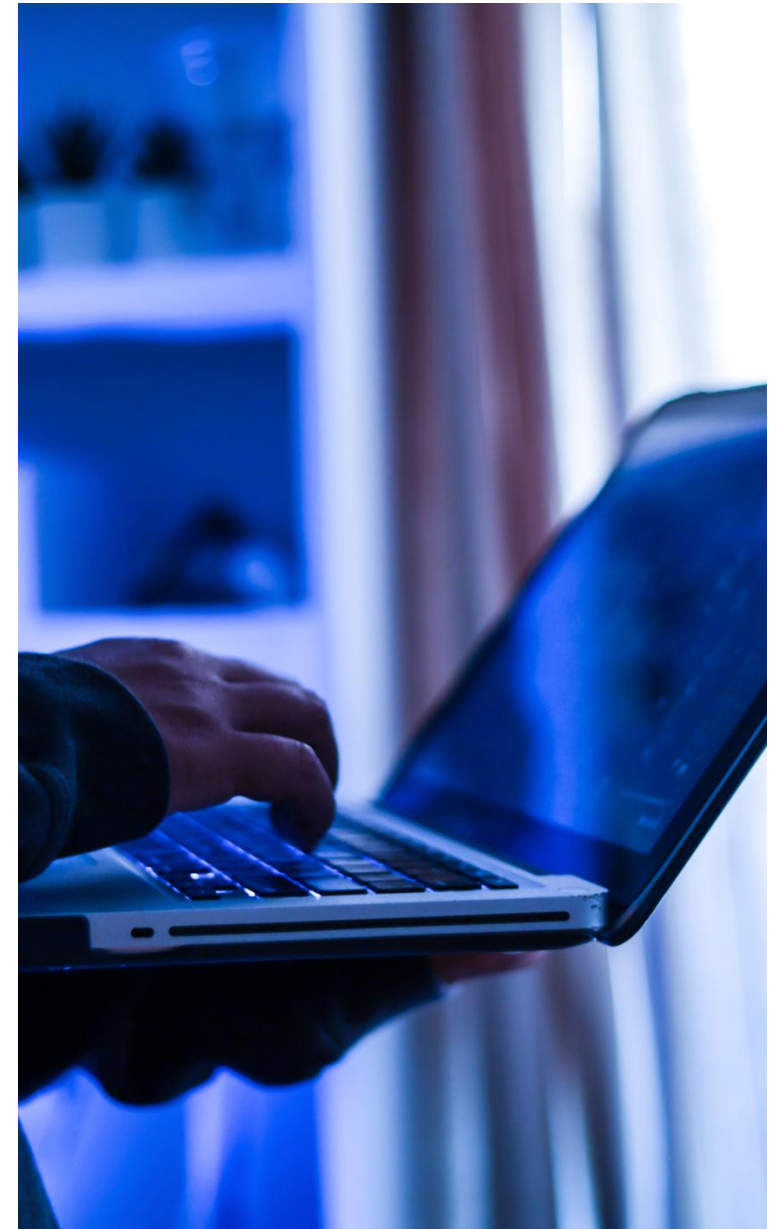
Summary

Key Takeaways



SAP-managed

- Your business decisions what to integrate
- SAP4ME management UI
 - Tenant / Solution activation
 - Integration selection
- Technical SAP2SAP integration
- Shared responsibility regarding monitoring & operations

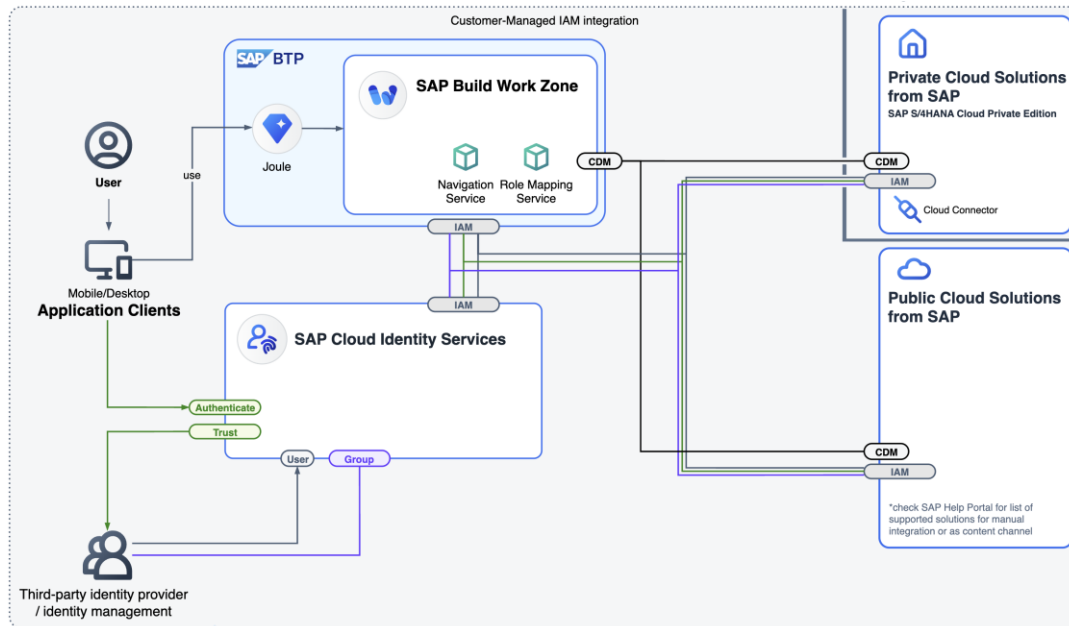


(SAP-managed) Joule

Customer-managed Joule

From Customer configures every bit and piece of the tenant and integration lifecycle.

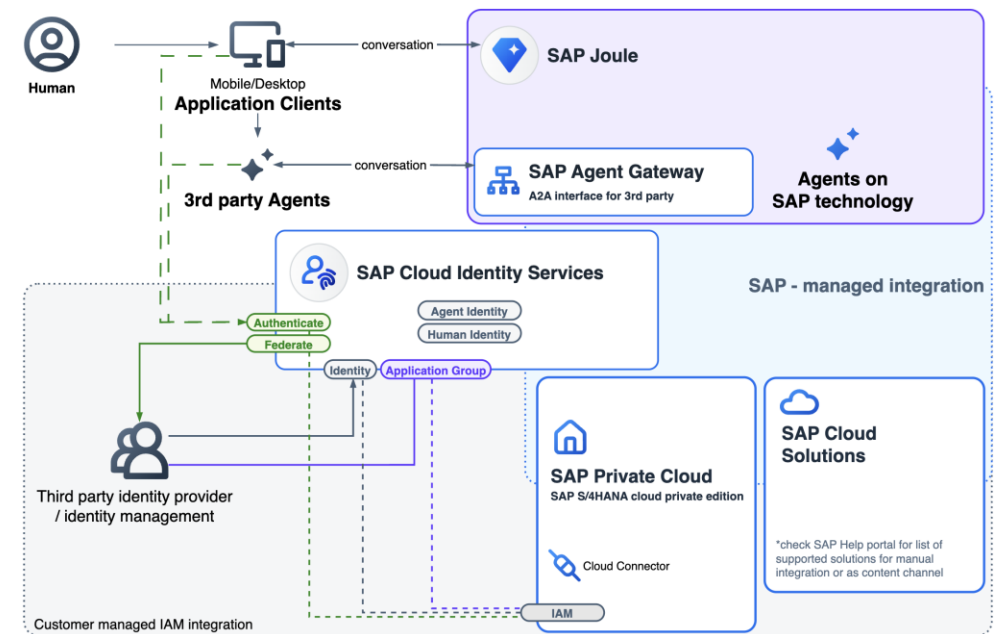
High effort for customers & SAP - slow project



SAP-managed Joule

To Customer activates Joule in SAP4ME, uses Cloud Identity Services. SAP manages the tenant & integration lifecycle.

Activate Joule once, consume it in SAP applications



SAP managed Suite applications aspects

01

Initial provisioning of Suite applications

02

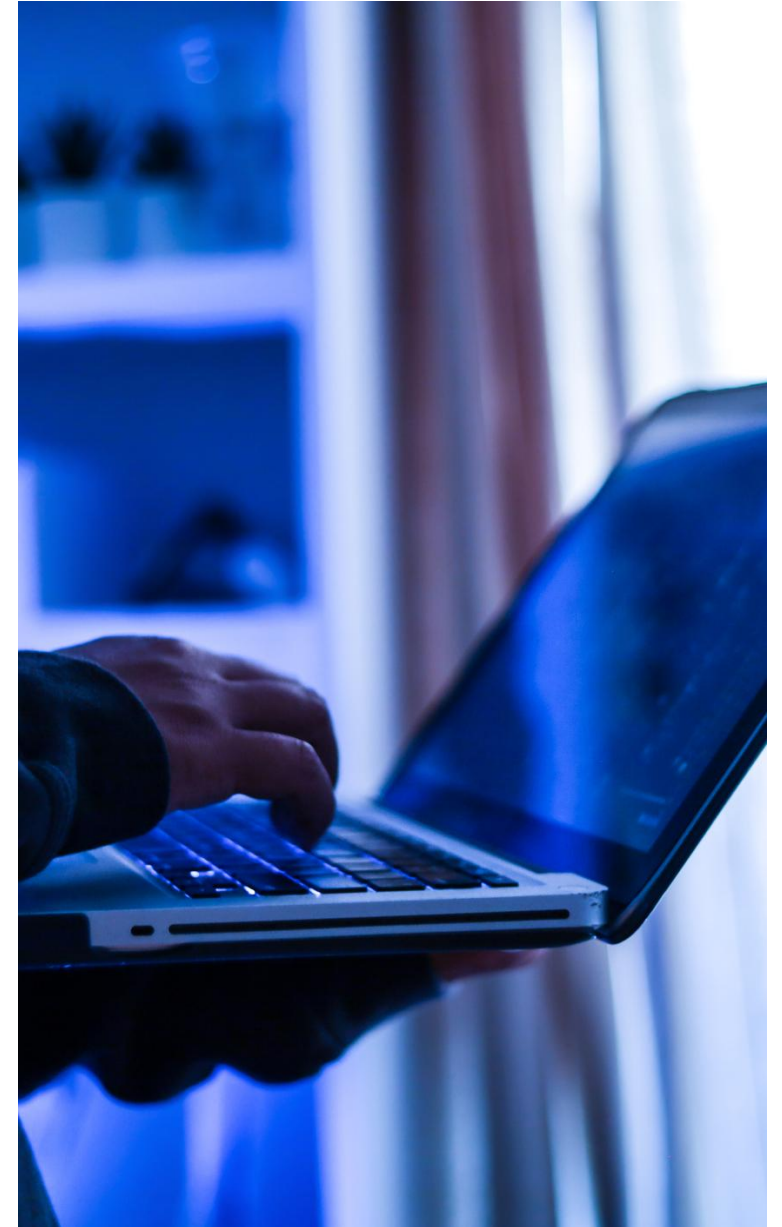
Configuration of Authenticating Identity Provider

03

Authorization management

04

Identity lifecycle management



Initial Provisioning of Suite Applications

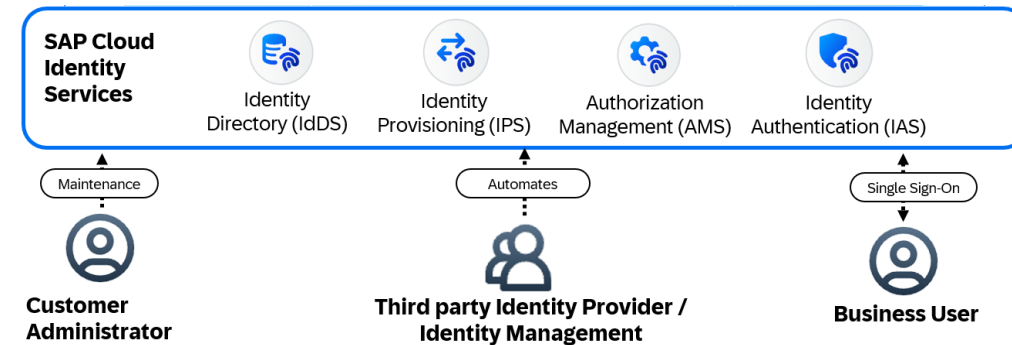
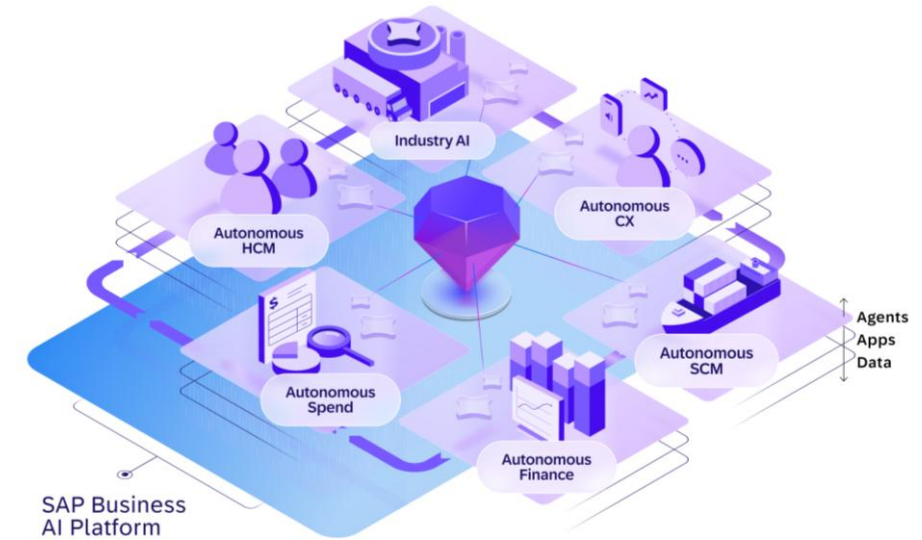
Administrator logs on to SAP 4 Me and triggers provisioning of the Suite applications:

- initial application roles are created in the applications
- **SAP-managed** IAM integration set-up established

IAS set-up as the authenticating identity provider for the applications

SAP-managed IPS jobs for user and user role assignments are scheduled

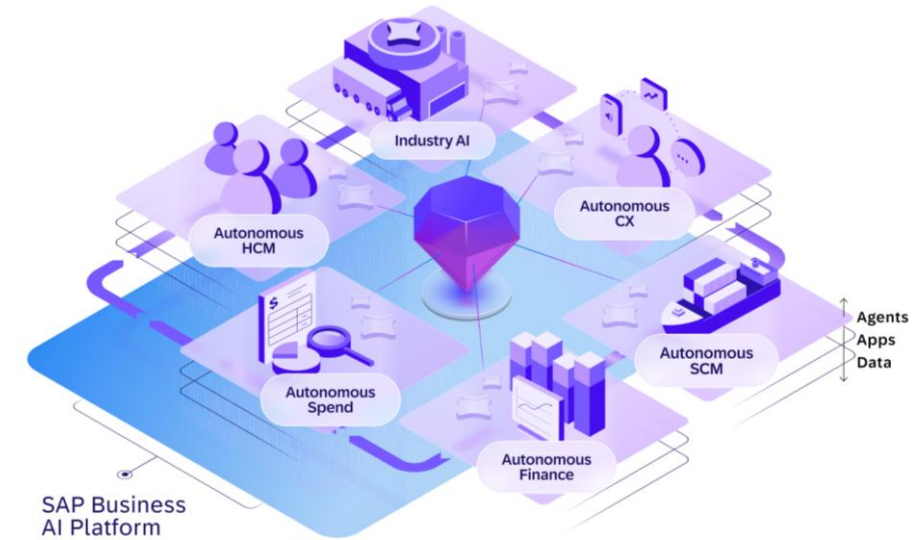
Administrator can add additional users required for initial system setup in SCI*) and maintains user-role assignments based on published (initial) application roles from the applications



Configuration of Authenticating Identity Provider

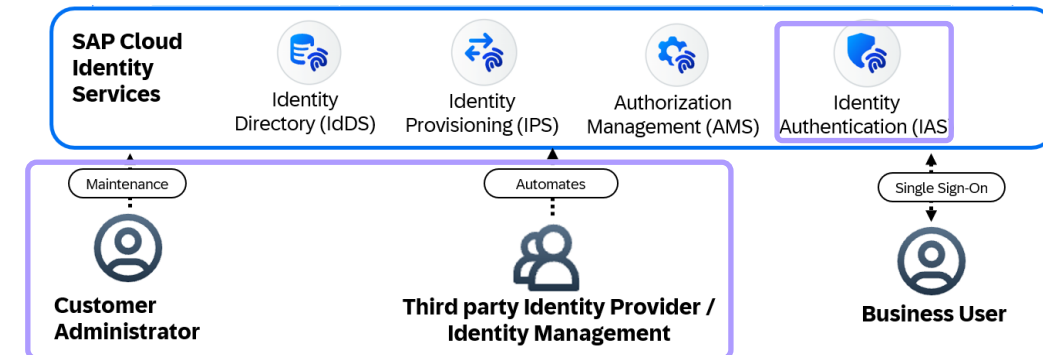
Administrator can

- configure in SCI for the provisioned applications the third-party IdP as the authenticating identity provider. The IAS acts as a proxy to delegate the authentication to the corporate IdP
- or use IAS directly as the authenticating identity provider for the SAP applications



Administrator can manage in IAS customer specific details of the application, mostly on Suite level

- Risk based authentication rules
- Policies (passwords, terms of use, privacy)
- Branding and Layout



Not required technical details in IAS will be hidden for the customer

Authorization Management

Administrator defines/maintains authorizations

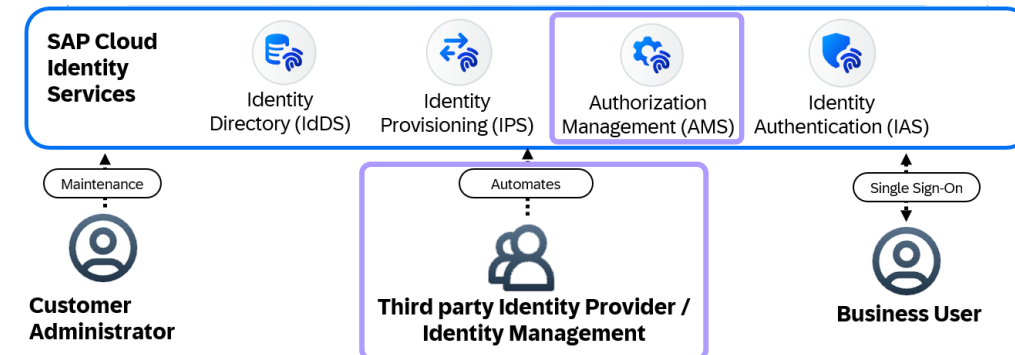
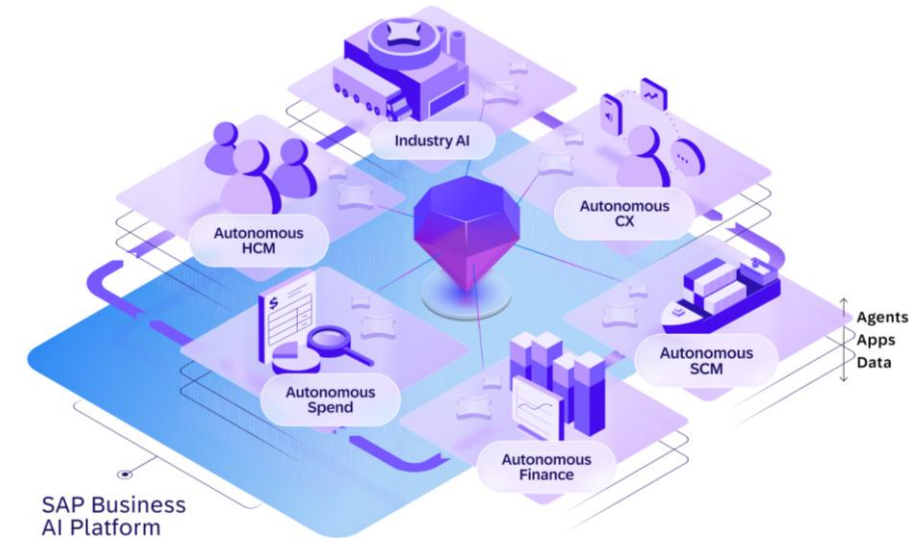
- in SCI for XSUAA / AMS based BTP applications
- in the respective SAP Cloud applications for non BTP based applications

Composite roles are created based on published application roles

- either in third-party IDM
- or directly in Identity

In SCI [composite roles](#) are planned to be supported. They are a collection of groups.

The administrator has an overview of the maintained authorizations across SAP applications in a central point.



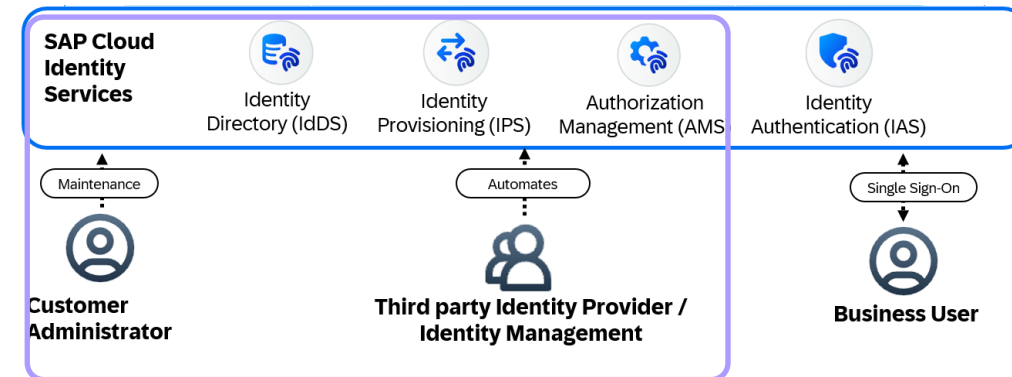
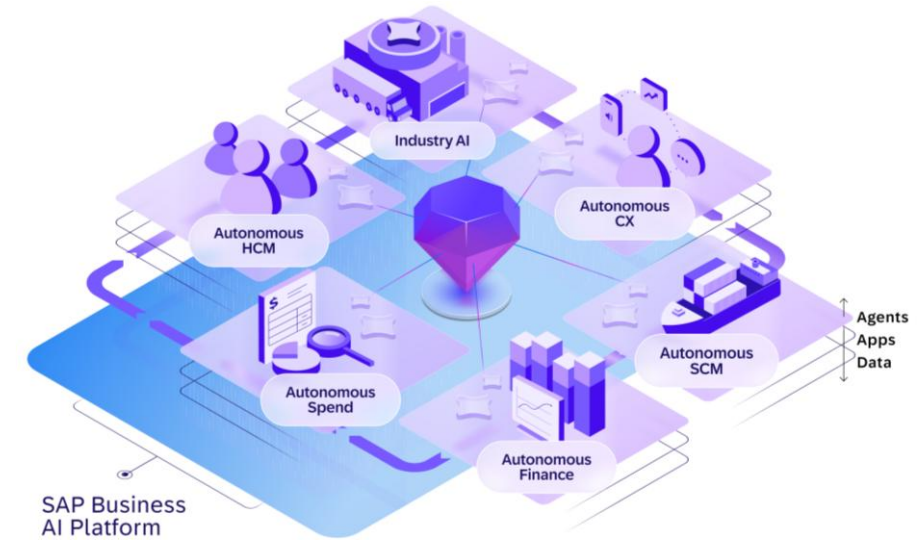
Identity Lifecycle Management

With a (third-party) IDM tool

- HR administrator creates employee in SAP SFSF
- Corresponding user is created in third-party IDM
- Admin assigns roles to the user in third-party IDM
- User and role assignment information are replicated to SCI (customer managed). Replication to all connected SAP applications (SAP managed)

Without a (third-party) IDM tool

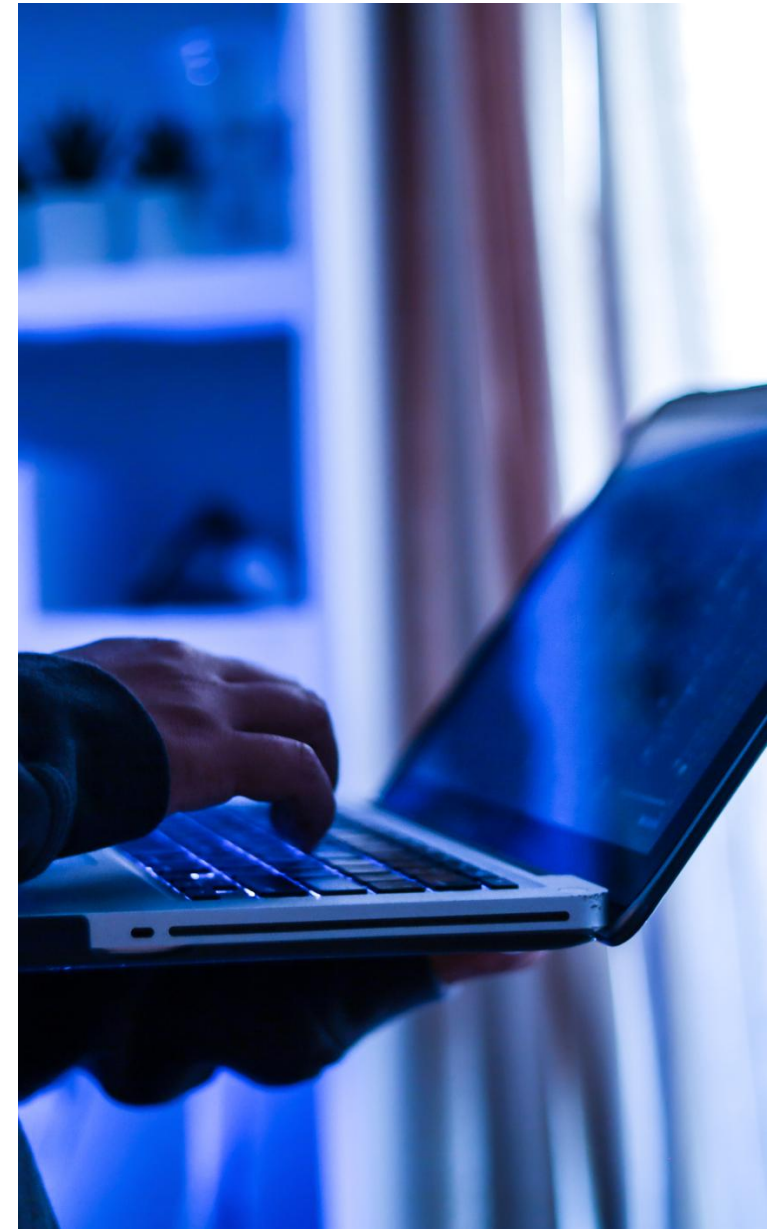
- HR administrator creates employee in SAP SFSF
- SFSF integrates directly with SCI for user creation
- Admin assigns roles to the user in SCI –replication from SCI to all connected SAP applications (SAP-managed)



One more thing: Landscape considerations

- SAP managed Joule will be a Singleton Joule instance per customer
- SAP Cloud Identity Services
 - holds the Agent Identity
 - offers the policy management
 - issues tokens to agents for SAP

⇒ Following the SCI default tenant model is recommended



Agenda

01

Introduction

SAP Cloud Identity Services and their role for the Autonomous Enterprise

02

Agent Identity & SAP Business AI Platform

Agent Governance & Security with the Cloud Identity Services

03

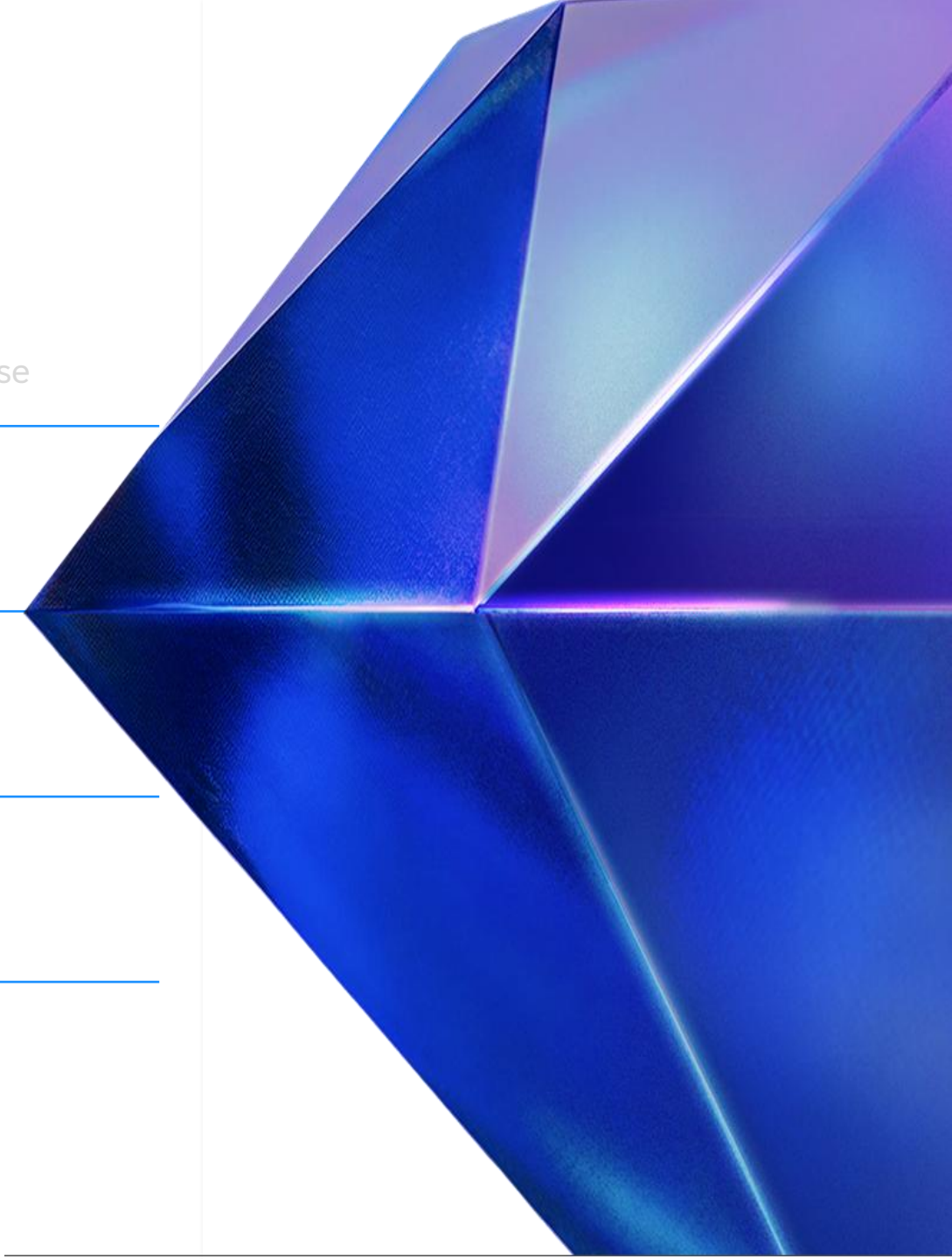
SAP Managed Scenarios

Changes in the shared responsibility model

04

Summary

Key Takeaways



Key Takeaways

01

SAP Cloud Identity Services will hold the **Agent Identity**. It will offer policy management and token issuing for agents.

02

SAP-managed IAM setups ensure a fast and secure path towards realizing the vision of an Autonomous Enterprise

03

SAP Cloud Identity Services default tenant model is recommended for **SAP-managed Joule**



Speakers



Sonia Petrescu
SCI Product Manager



Marko Sommer
SCI Product Manager

