Harness the Power of SAP GRC Across Your Entire Landscape, Options for Cloud and Non-ABAP Systems

James E. Roeske, CEO
Customer Advisory Group

Las Vegas

2024

SAPinsider

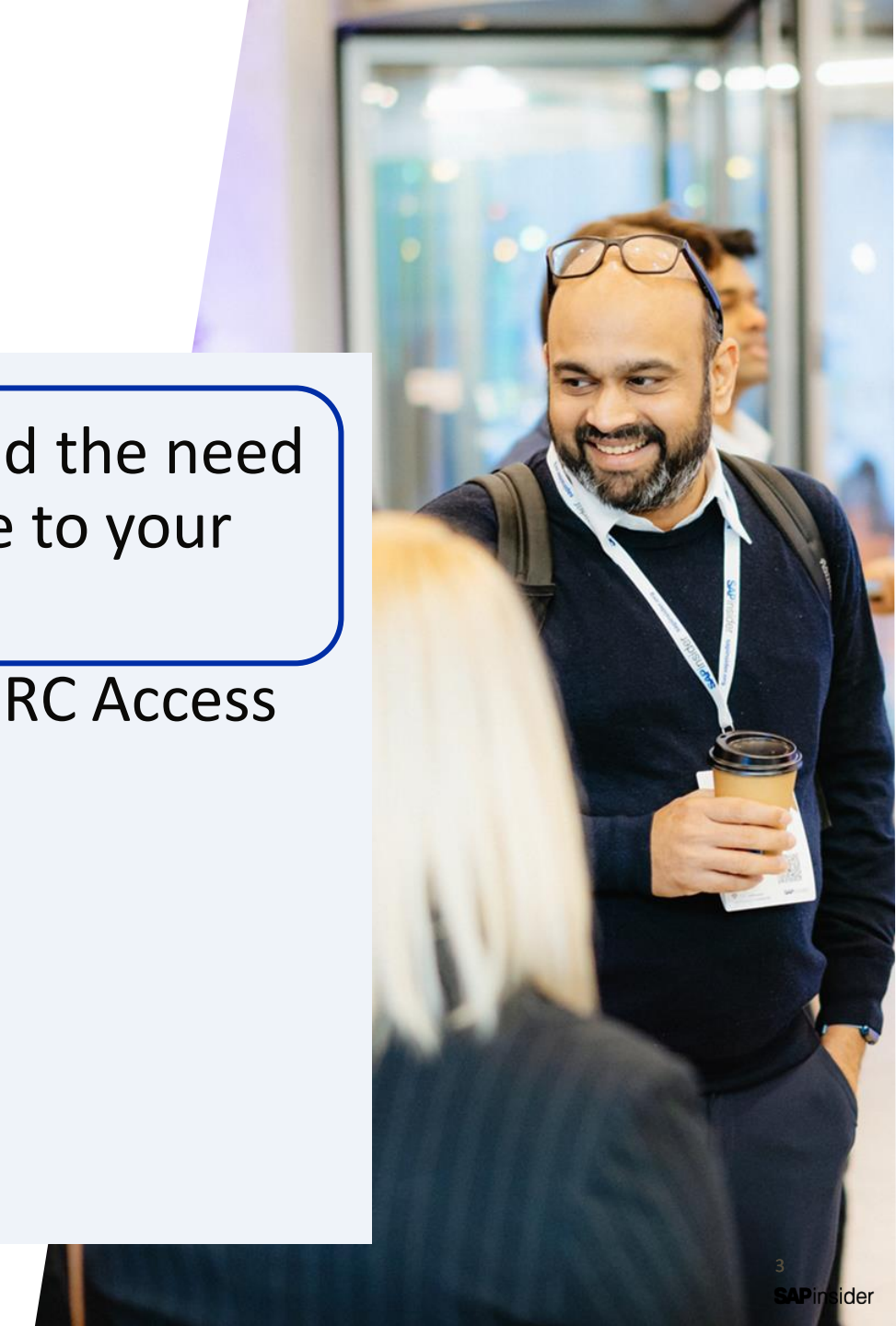
In This Session

Risk analysis across your entire landscape of business systems is critical for accomplishing compliance, especially as audits are becoming more in-depth year after year. Discover the technical options of how SAP GRC can communicate and analyze Cloud, Non-ABAP and Non-SAP systems. By attending this session, you will learn:

- Provide a clear explanation of the functionality capabilities of SAP GRC Access Control when integrated with a Non-SAP or Non-ABAP based system.
- Offer a detailed review of the 3 primary technical alternatives of connectivity, their Pro's and Con's, and implementation requirements of the options available to GRC customers to allow SAP GRC to interact with Cloud, Non-ABAP and Non-SAP based systems

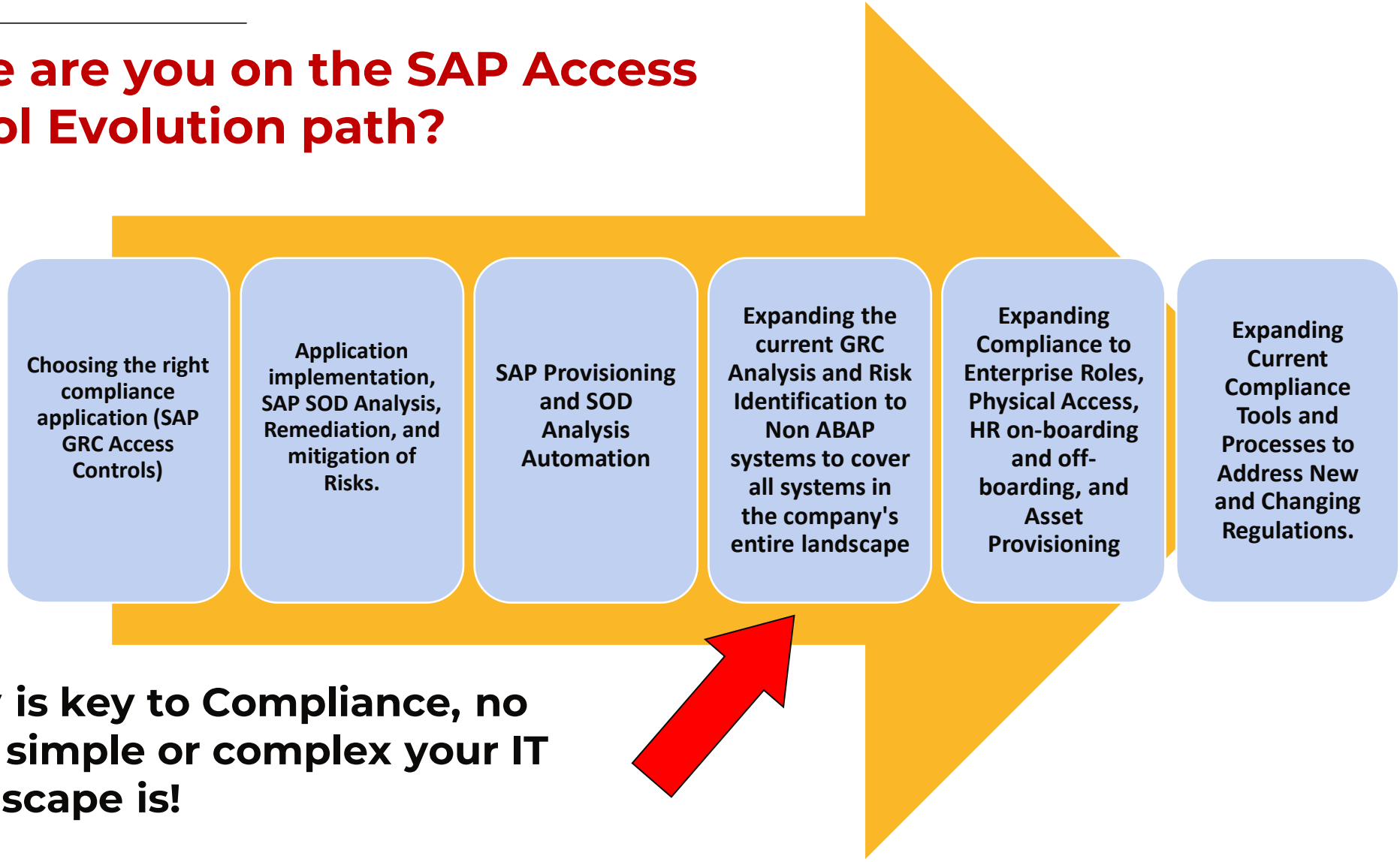
What We'll Cover

- Evolution of a GRC customer and the need to grow and expand compliance to your entire Landscape
- 3 Options for Connecting SAP GRC Access Control to Non-ABAP systems
- Which Option is Best for You?
- Wrap-Up



The Evolution of a Typical Access Controls GRC Customer.

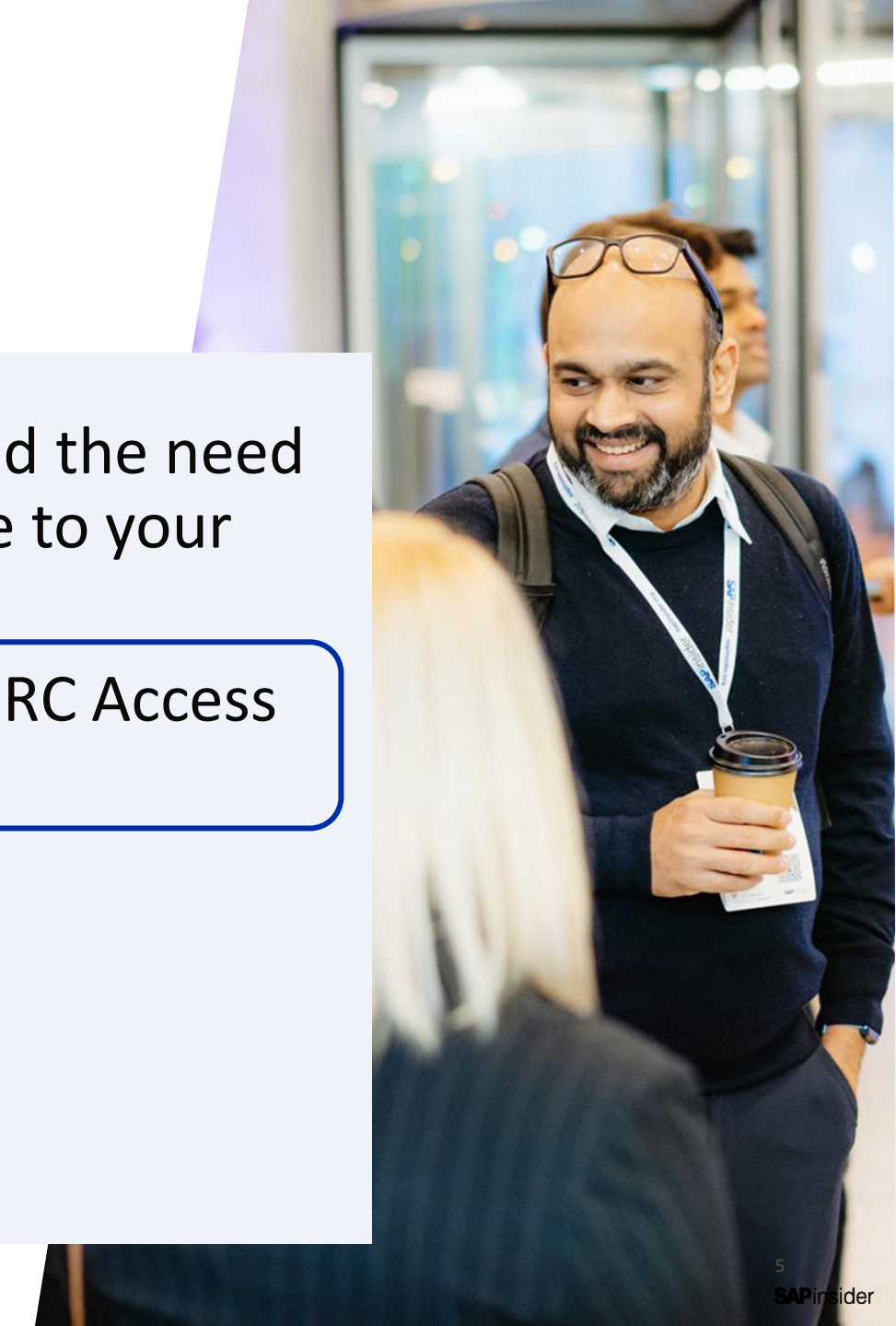
Where are you on the SAP Access Control Evolution path?



Consistency is key to Compliance, no matter how simple or complex your IT system landscape is!

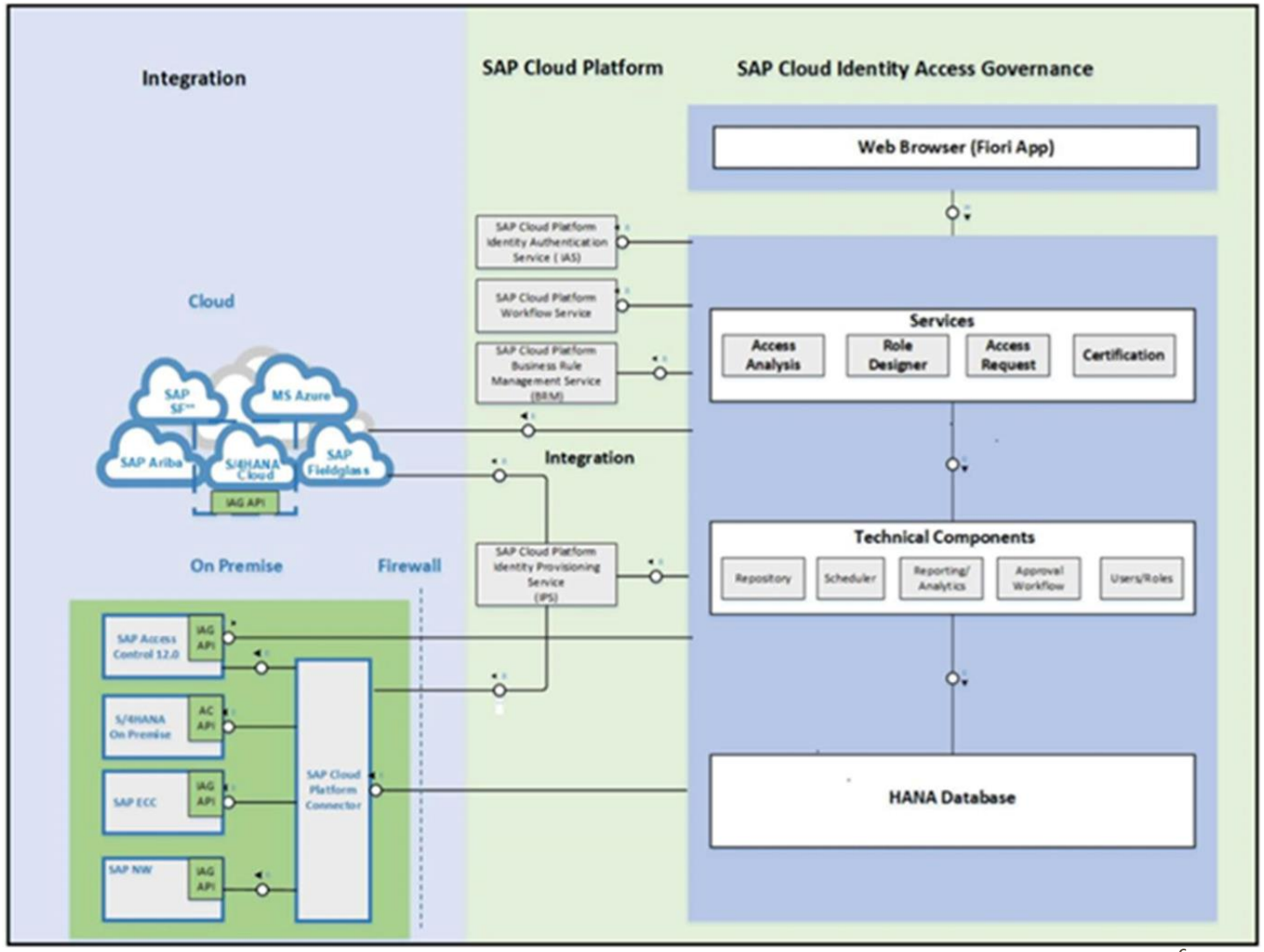
What We'll Cover

- Evolution of a GRC customer and the need to grow and expand compliance to your entire Landscape
- 3 Options for Connecting SAP GRC Access Control to Non-ABAP systems
- Which Option is Best for You?
- Wrap-Up



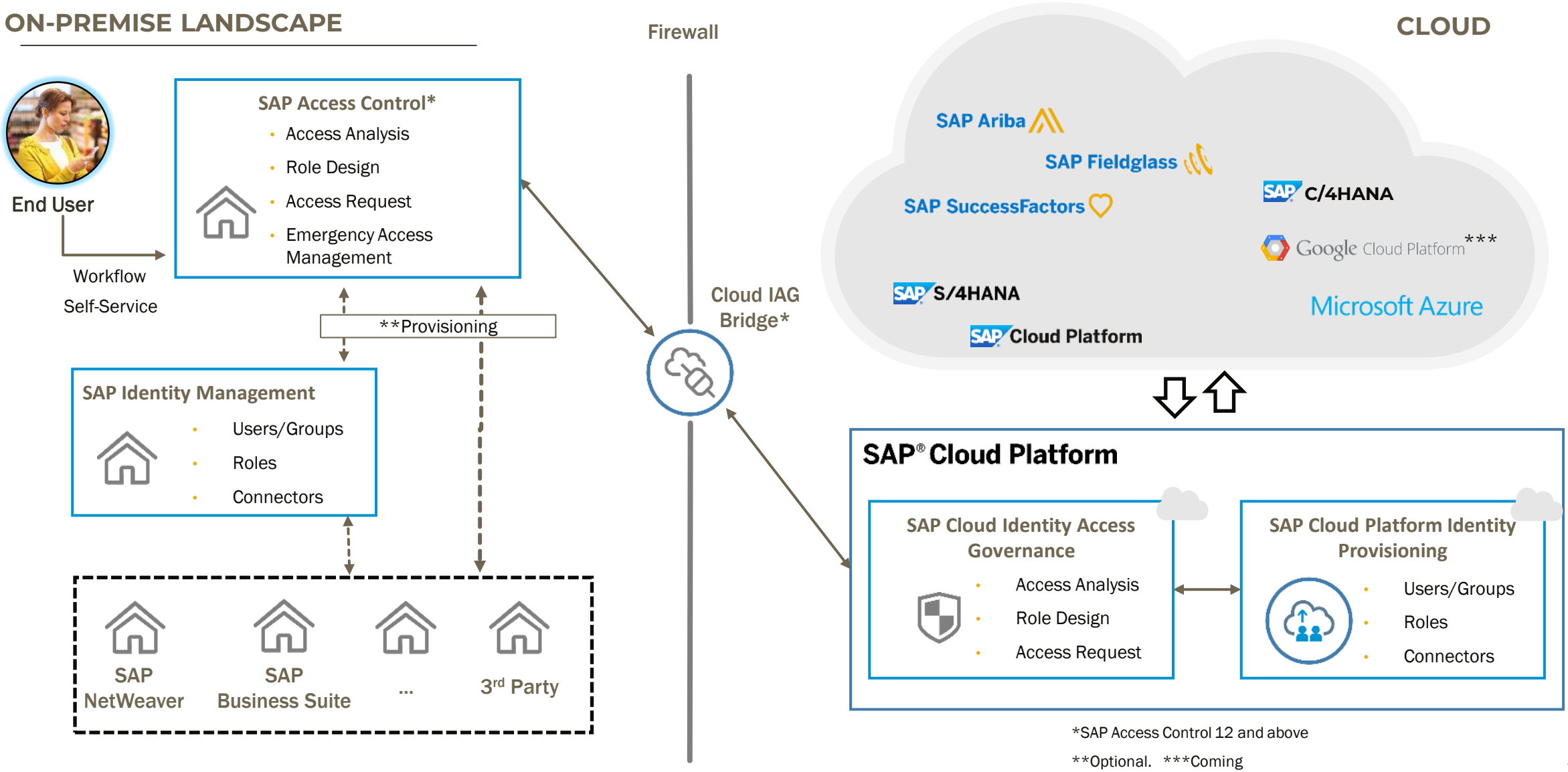
Option #1: SAP Cloud Identity Access Governance & Cloud IAG Bridge

- Is a Cloud application only
- Uses IAG API's for connectivity
- Connects to both SAP Cloud and On-Premise applications
- SAP Fiori is the only application interface
- SAP HANA is the only Database supported



Source: SAP

Hybrid Identity and Access Governance – AC + IAG



*SAP Access Control 12 and above

**Optional. ***Coming

Source: SAP

SAP Cloud IAG - Integrated Provisioning for Hybrid Landscapes

Cloud

On premise

- **SAP SuccessFactors**
- **SAP ABAP (on-premise)**
- **SAP Ariba**
- **SAP Fieldglass**
- **SAP S/4HANA Cloud**
- **SAP S/4HANA (on-premise)**
- **Microsoft Azure Platform**
- **SAP Marketing Cloud**
- **SAP Integrated Business Planning**
- **SAP Analytics Cloud**
- **SAP Cloud Foundry**
- **LDAP System**
- **SAP Identity Authentication**
- **SAP Cloud Platform**
- **....**

- Seamless access governance across hybrid landscapes
- Automated access request approval and provisioning based on HR events
- Expanded system connectors for key business applications on-premise and cloud
- S/4 HANA native integration including rule content and support for new authorization model

Key benefits

Increased scope for provisioning across hybrid landscapes

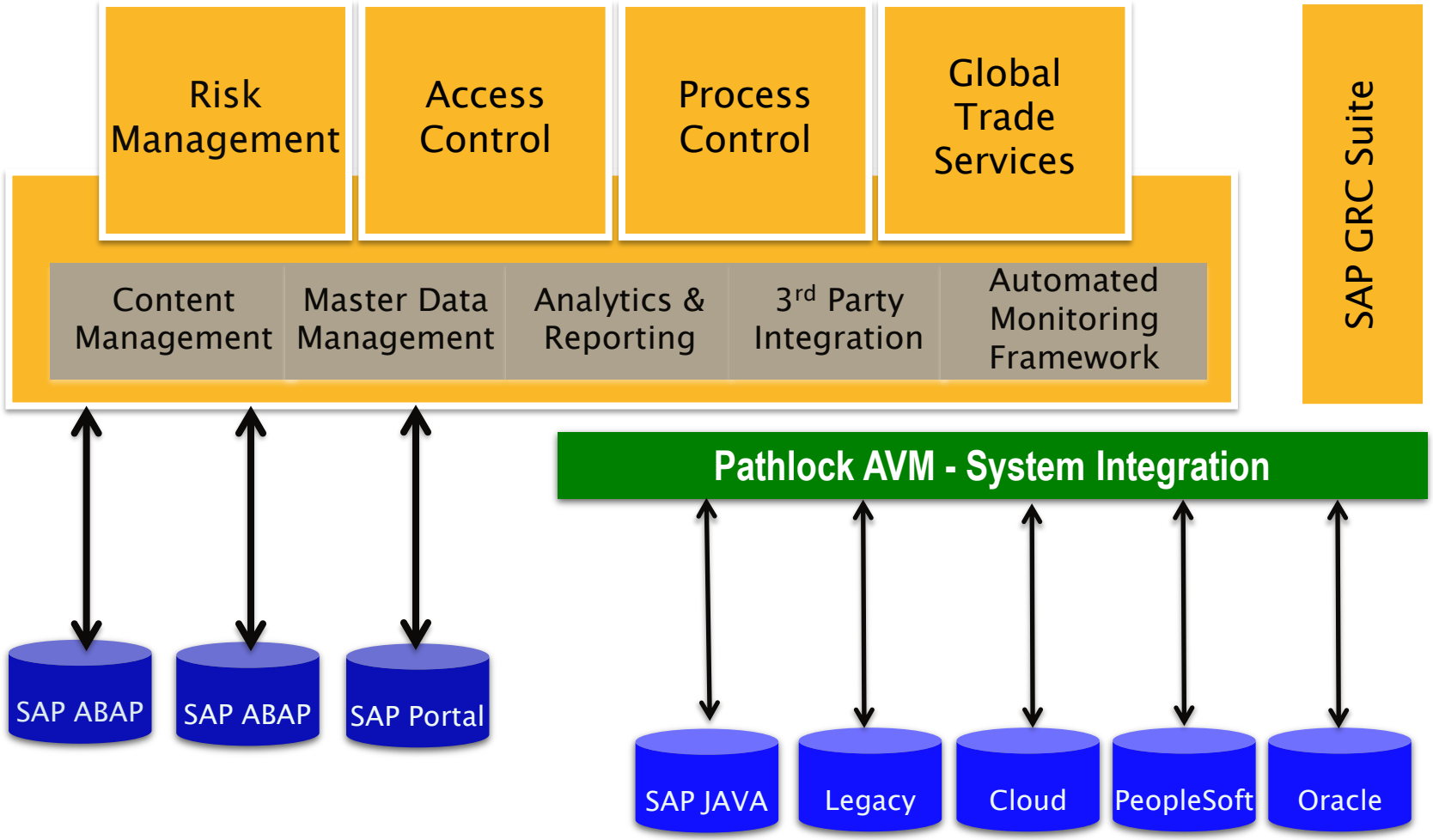
Simplified architecture leveraging common components

Enable and govern users for processes that span multiple applications

Source: SAP

Option #2: Pathlock Access Violation Management System Integration Edition

- Extend the capabilities of SAP Access Control across additional business applications and IT systems, eliminating administrative silos and enabling a more complete picture of user access across the organization.
- SAP Access Violation Management enables real-time risk analysis and provisioning, user access reviews, role management, and emergency access management to on-premise and cloud-based enterprise applications.



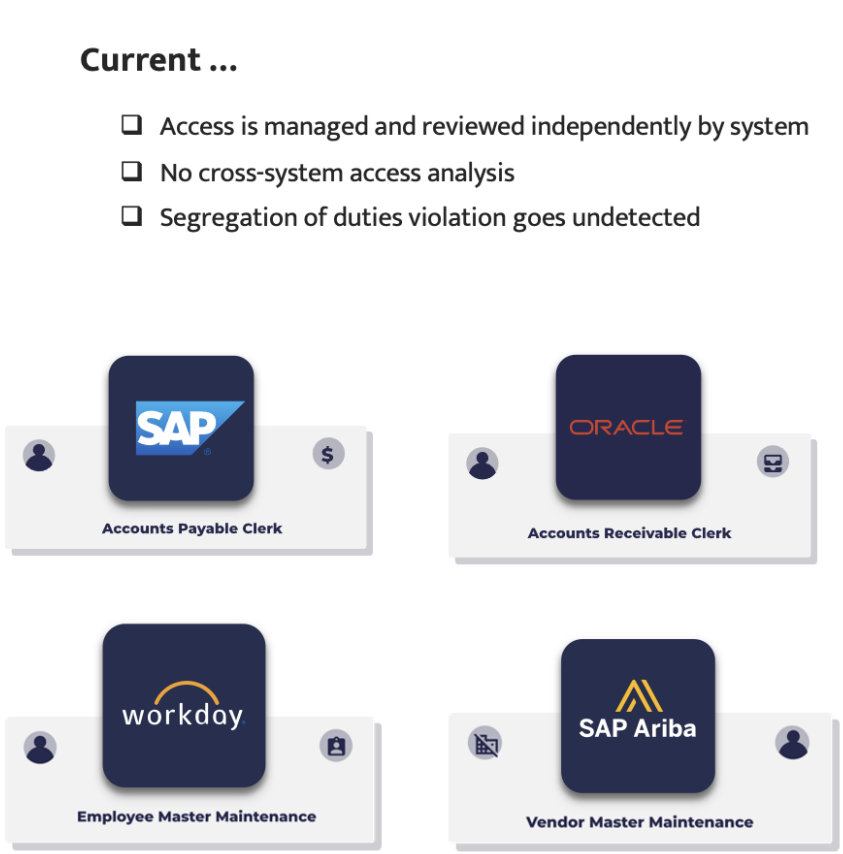
Option #2: Pathlock Access Violation Management System Integration Edition

Uncover access risk & review user entitlements across applications

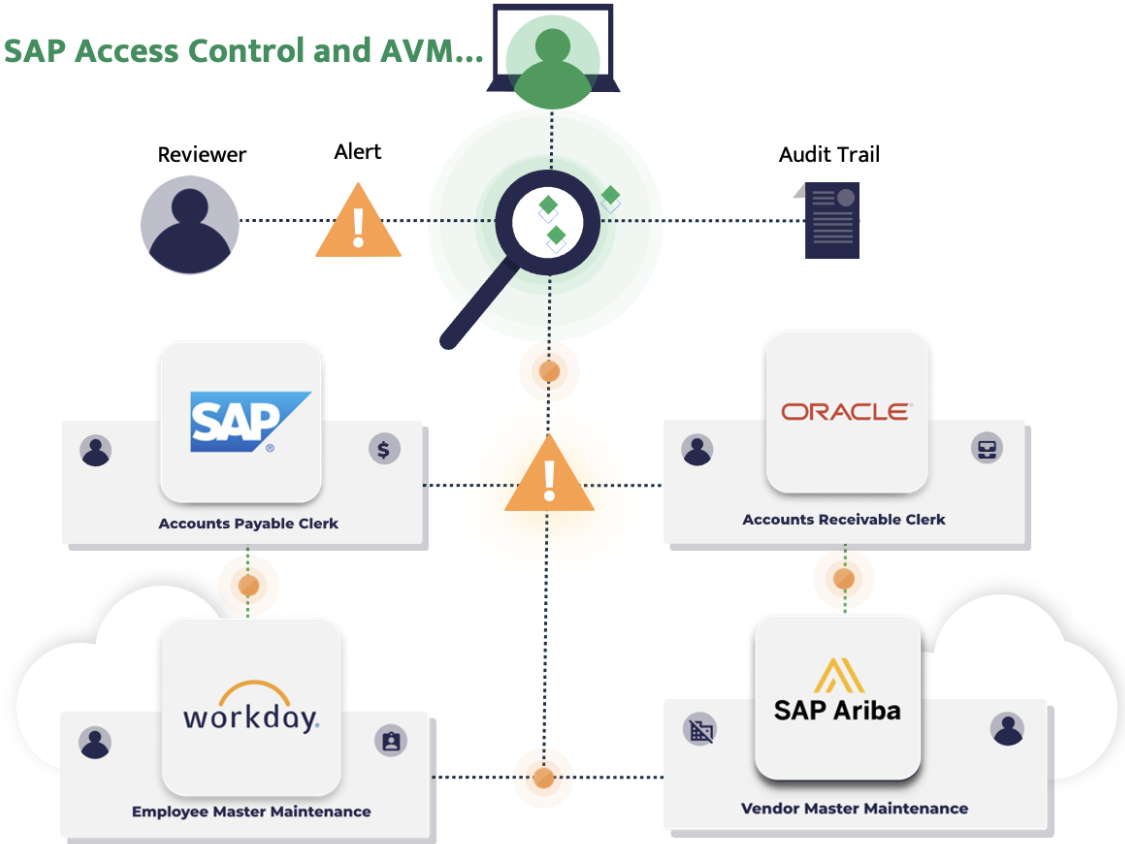
With a single pane of glass for identity and access governance

Current ...

- ❑ Access is managed and reviewed independently by system
- ❑ No cross-system access analysis
- ❑ Segregation of duties violation goes undetected

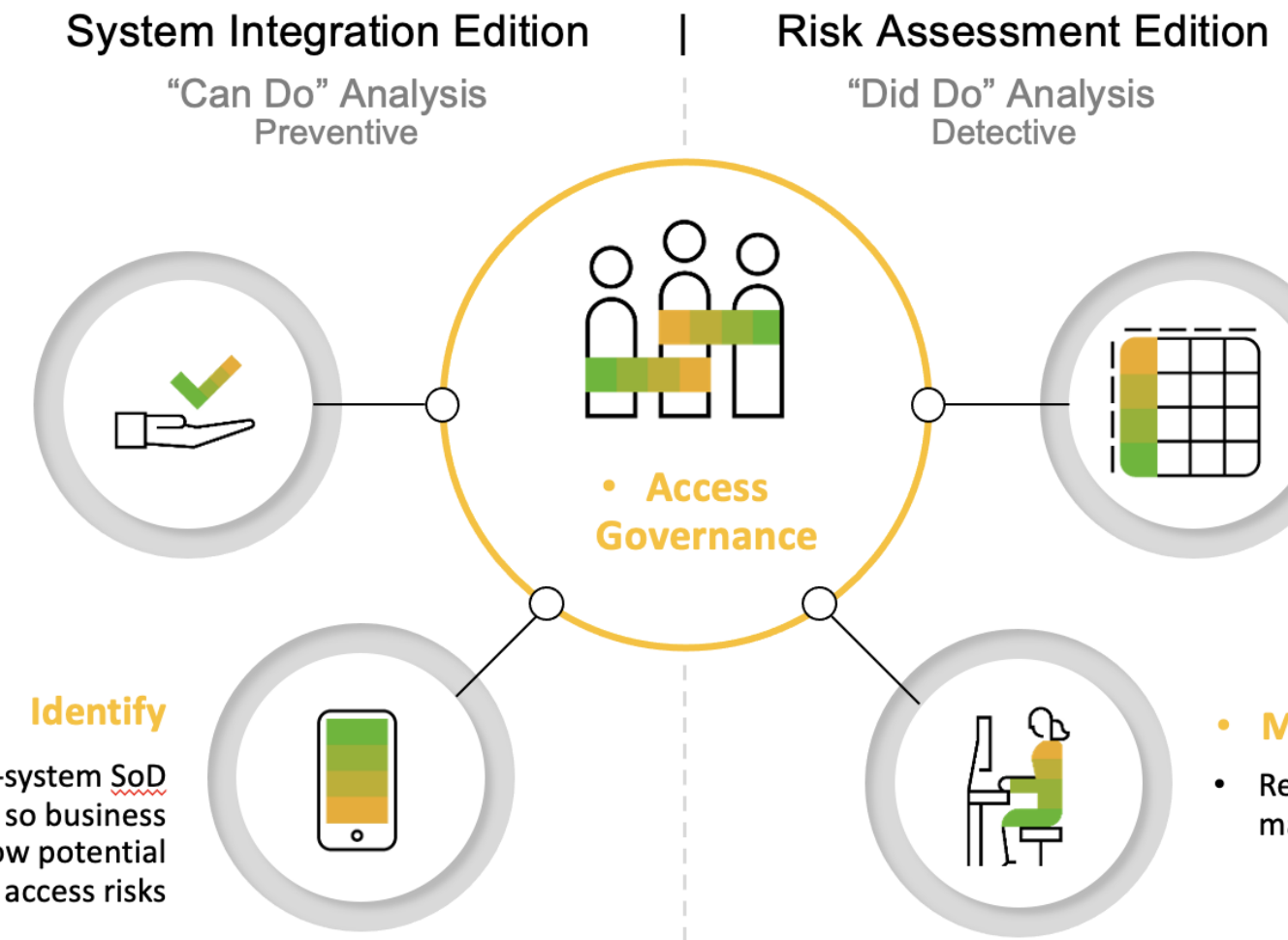


SAP Access Control and AVM...



Source: Pathlock AVM Integration Edition 2023

Option #2: Pathlock Access Violation Management System Integration Edition Plus Risk Assessment Edition



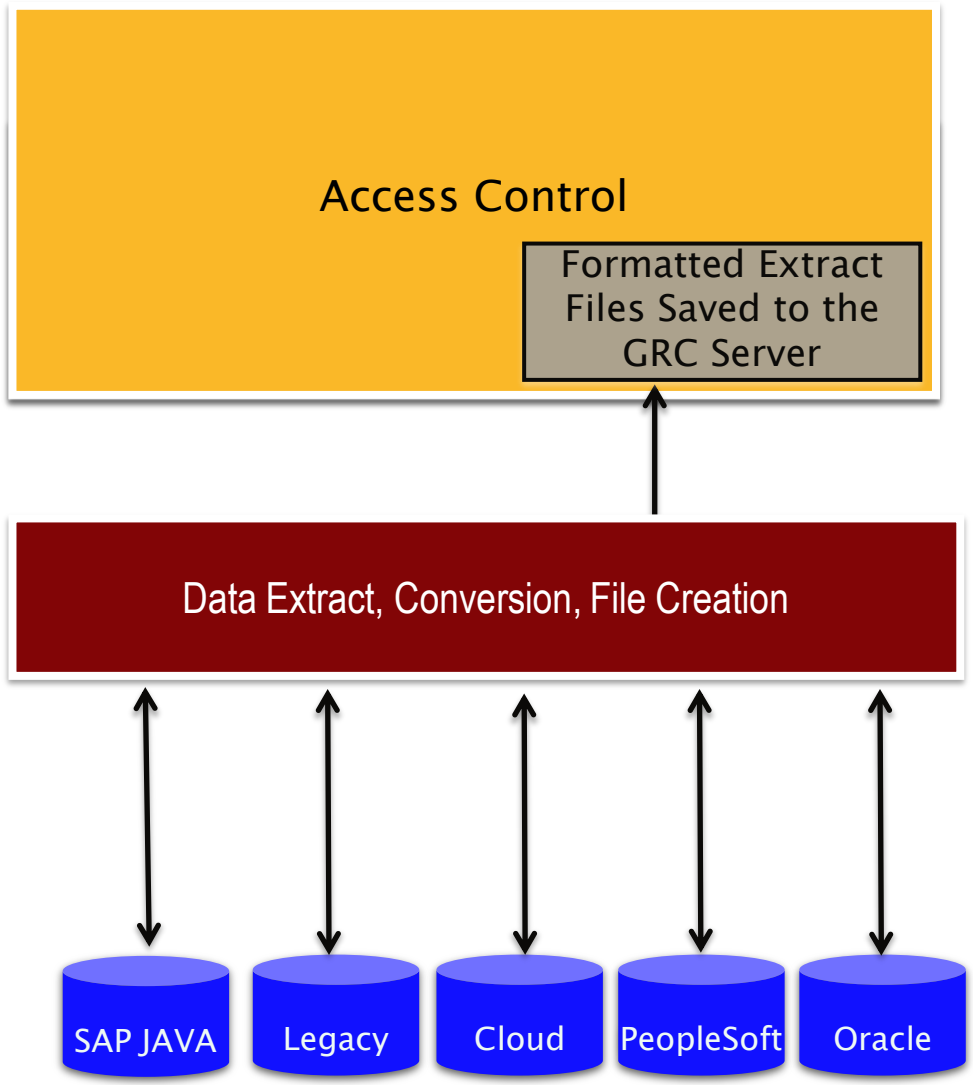
- **Extend**
  - Extend the capabilities of SAP Access Control across enterprise systems
- **Identify**
  - Identify cross-system SoD violations so business owners know potential access risks
- **Mitigate**
  - Act on what matters based on financial impact
- **Monitor**
  - Review user business transactions for materialized SoD violations

Source: SAP

Option #3: File System for Legacy Extraction Method

- Ideal for Customers that require SoD Analysis, Risk Mitigation assignment, and User Access Review functionality for Non-SAP and Non-ABAP systems for compliance purposes, but do not require the full functionality of Access Provisioning, Role Management, or FireFighter for those systems.

- The “File System for Legacy Extract Method” is NOT Real Time. It relies on data to be extracted on a consistent and regular basis which can then be read by SAP Access Control.



GRC 12.0 File Based Connector

- The File method basically allows a user to create and store files on the GRC server that contain the information that GRC needs to perform Repository Object Synchronizations and SoD Analysis
- 11 separate files are required, which contain all the data SAP Access Control requires
- Please note – Action Usage is NOT included as a data value for the legacy file extract process.

File	File ID
Permission Master Data	LEGACY_PERMISSION
Action Master	LEGACY_ACTION
Role Master	LEGACY_ROLE
Role-Action	LEGACY_ROLE_ACTION
Role-Permission	LEGACY_ROLE_PERMISSION
Profile Master	LEGACY_PROFILE
Profile-Action	LEGACY_PROFILE_ACTION
Profile-Permission	LEGACY_PROFILE_PERMISSION
User Master	LEGACY_DEFAULT_USER
User Action	LEGACY_USER_ACTION
User Permission	LEGACY_USER_PERMISSION

GRC 12.0 File Based Connector

- The Key is to build a consistent and regularly scheduled extraction process that places the data in the proper format that SAP GRC can read and is expecting.

- This option does NOT provide “Real Time” results! Rather, your results will be based on the last successful extract of the data saved on the GRC server for that system.

Old Data means inaccurate SoD Results!

User Action File

Field	Data Field Type	Field Size	Field Values	Sorting	Req'd	Description	Transformation
User ID	String	50	CAPS	Sort Ascending Order1	Yes	User ID	Unique record = The combination of columns 1–3 (User ID, Roles, and Action From) must be unique
Role Name	String	100	CAPS	Sort Ascending Order2	Yes	Role Name	
Action From	String	50	CAPS	Sort Ascending Order3	Yes	User Action	
Action To	String	50	CAPS		No	User Action, only applicable if User Action has range From/To	If this value does not exist for source system, leave blank
PROFILE	String	20	CAPS		No		If this value does not exist for source system, leave blank
Composite Role Name	String	100	CAPS		No	Composite Role Name (leave blank if unavailable)	If this value does not exist for source system, leave blank.

GRC 12.0 File Based Connector

- The file extract process has the ability to analyzing risk all the way down to the “Permission” and “Permission Value” level just like the Real Time Plugin method.

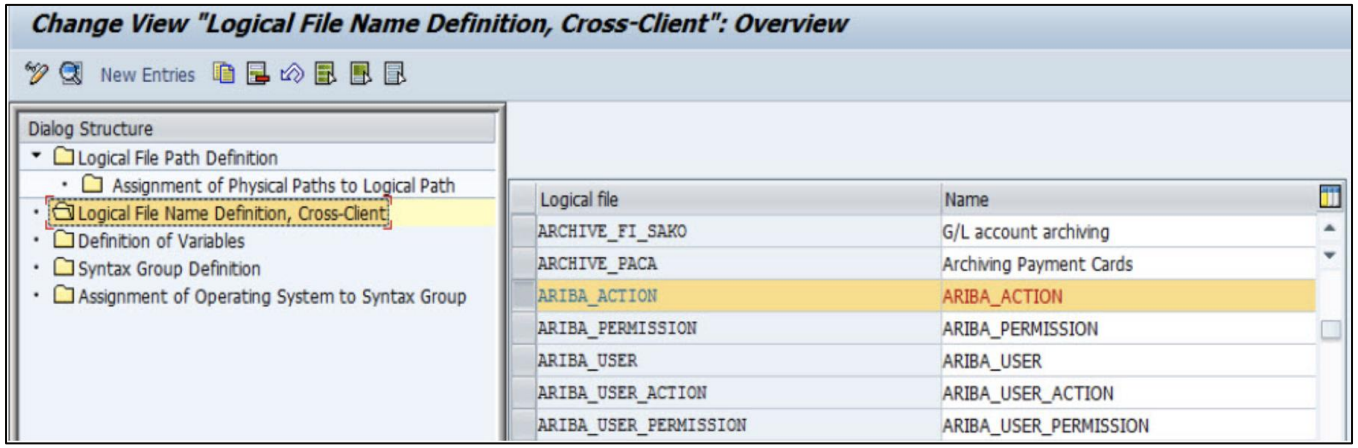
- Most Non-SAP systems do not follow the same concept of having “T-codes”, “Authorization Objects”, and Auth Values, therefore you must map the authorization concept of the Non-SAP system to align with “Actions” and Permissions” that SAP GRC can understand.

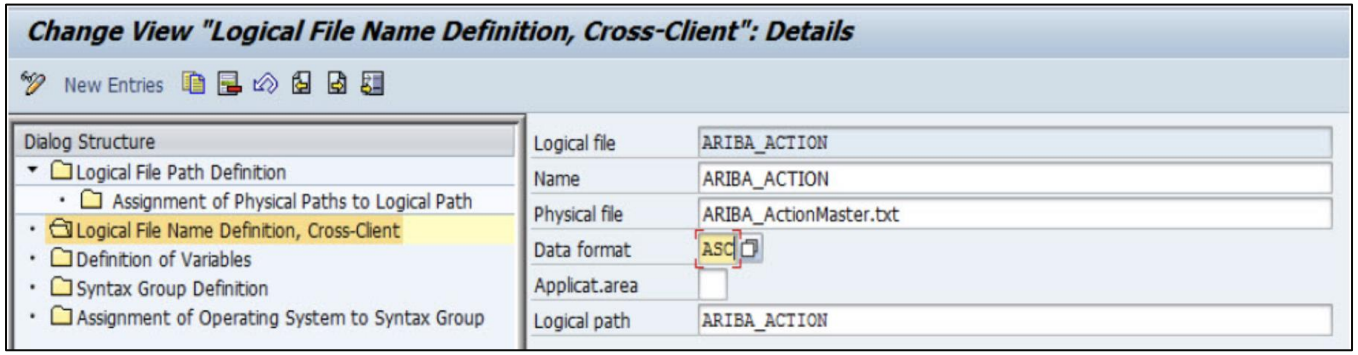
- This Mapping is also necessary for the Rule Building process you will need to do in your existing GRC Rule Set to include the Non-SAP systems.

Role Permission File							
Field	Data Field Type	Field Size	Field Values	Sorting	Req'd	Description	Transformation
Role	String	100	CAPS	Sort Ascending Order1	Yes	Role Name	
PERMISSION (Resource Name||Resource Ext.)	String	100	CAPS	Sort Ascending Order2	Yes	Role Permission (Permission Object/Field),required if applicable	ACTION and PERMISSION field that use || with no space in between
Auth Group	String	20			Yes	Auth Group	
Value From	String	50	CAPS		Yes	Permission Value	
Value To	String	50	CAPS		No	Permission value, only applicable if User Action has range From/To	If this value does not exist for source system, leave blank

GRC 12.0 File Based Connector

- These 11 files then get stored on the SAP GRC server in one consistent location, file format, and naming convention. SAP GRC then knows where to always retrieve the data for that particular “Legacy File” connector when a SoD analysis or Synchronization job is run for that particular connector.



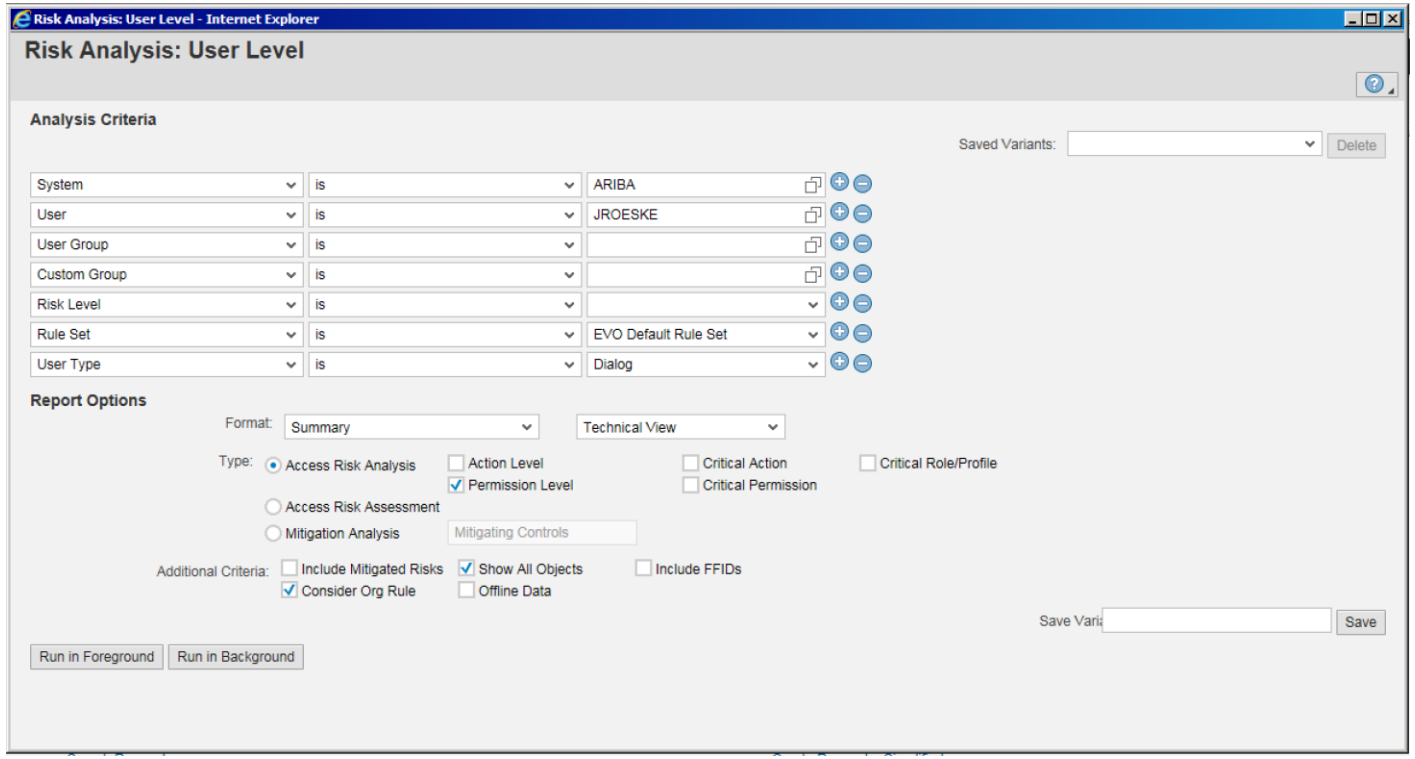


GRC 12.0 File Based Connector

Once you have completed the following:

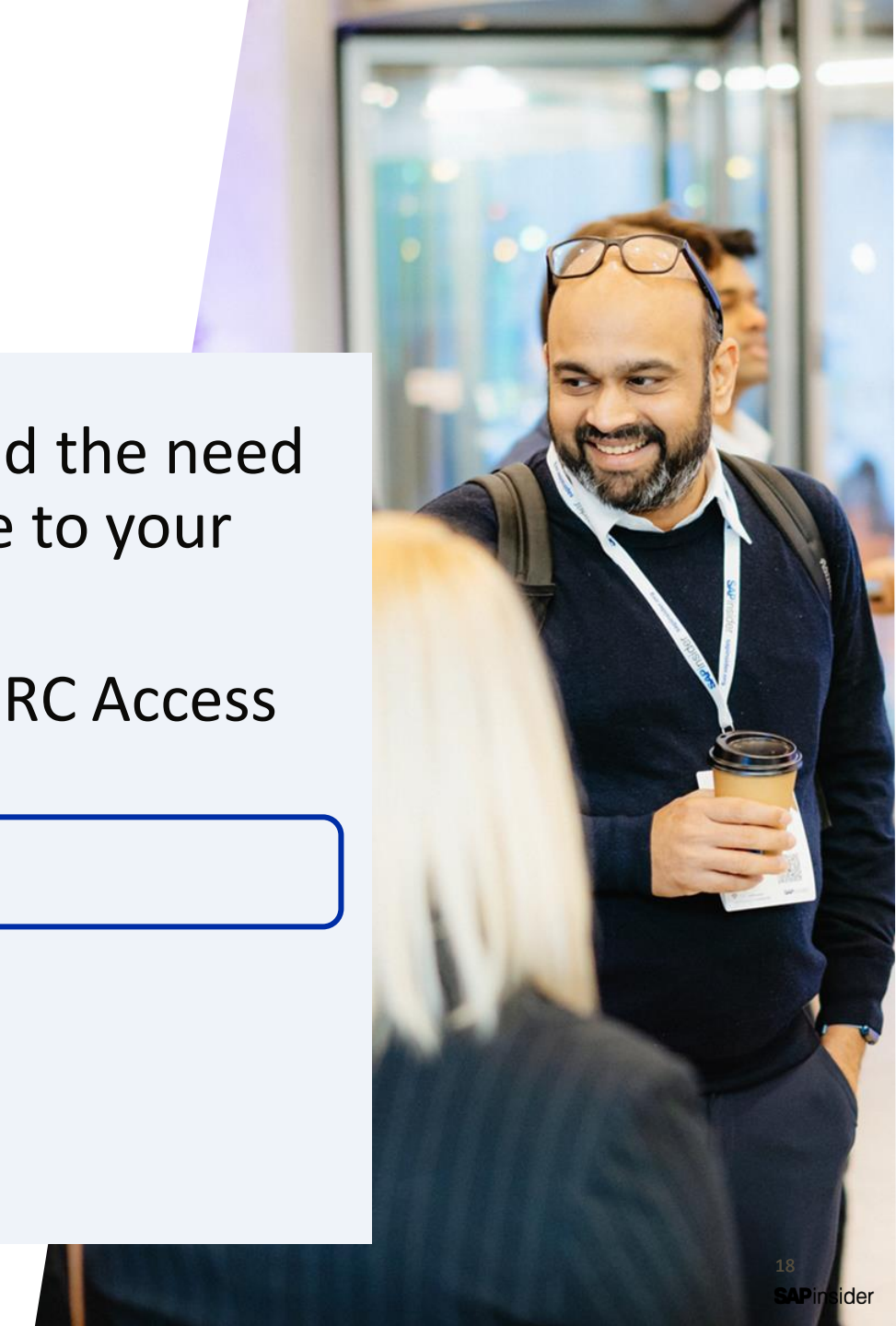
1. Connector configuration
2. Mapping of Actions and Permissions concept in GRC to the security structure of your Non-SAP system
3. 11 files have been successfully formatted and loaded
4. The Ruleset has been augmented to include Non-SAP Actions and Permissions in the Functions and Single and/or cross systems Risks have been configured.
5. Executed Repository Object Sync job for the new system

You are now ready to run risk analysis for the new Non-SAP system!



What We'll Cover

- Evolution of a GRC customer and the need to grow and expand compliance to your entire Landscape
- 3 Options for Connecting SAP GRC Access Control to Non-ABAP systems
- Which Option is Best for You?
- Wrap-Up



Which Connectivity Option is Right For You? Well, It Depends!

Finding the right option for you really boils down to identifying what your priorities are today, and for the future.

Here are some key questions to ask:

- Are you needing the ability to run BOTH Risk Analysis as well have Provisioning capabilities to your Non-ABAP based Systems in SAP GRC Access Control?
- Is ”Real Time” Risk Analysis essential for your requirements or would the data extraction method be acceptable?
- Are your Non-ABAP systems Cloud only, and compatible with SAP Cloud IAG?
- What are your future plans for connecting Compliance relevant systems? Do you need a connector platform that will cover your current needs and scale for the future too?
- Are you looking for more then just connector capabilities but also utilize extended functionality such as financial impact assessment of risk etc?

Things to Consider No Matter Which Option You Choose:

The “Clicky Clicky” is Easy, the “Thinky Thinky” is the Hard Part!

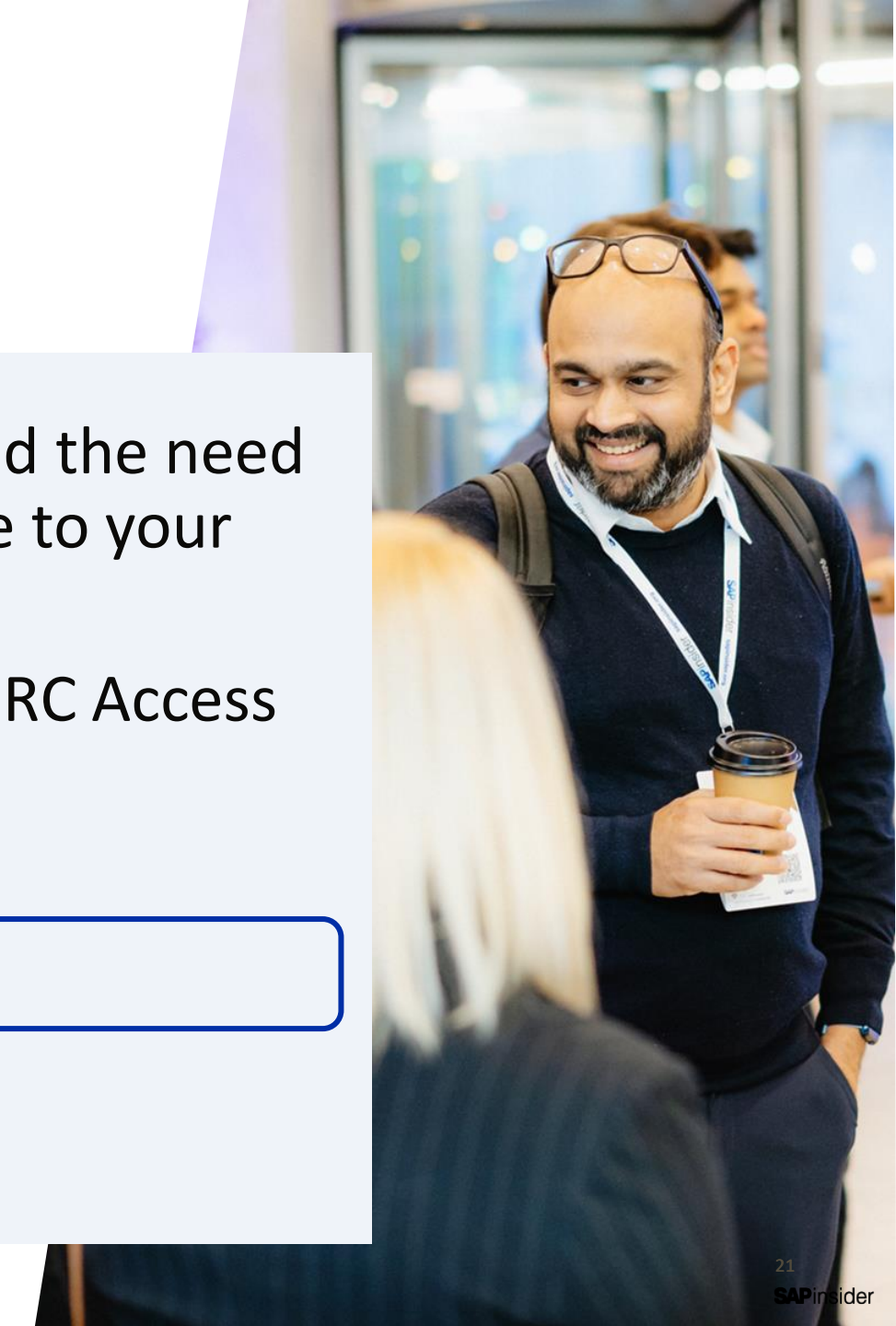
The “Clicky Clicky” is usually the easy part to connect SAP GRC to a Non-SAP or Non-ABAP system using either SAP Cloud Identity Access Governance, Pathlock AVM, or the File Based method……

But!

The “Thinky Thinky” of making sure you have a consistent and automated extract process, correctly mapped Actions and Permission for a nontraditional Security concept, as well as a correctly configured Ruleset to identify risk is the hard part!

What We'll Cover

- Evolution of a GRC customer and the need to grow and expand compliance to your entire Landscape
- 3 Options for Connecting SAP GRC Access Control to Non-ABAP systems
- Which Option is Best for You?
- Wrap-Up



Where to Find More Information

- https://help.sap.com/docs/SAP_CLOUD_IDENTITY_ACCESS_GOVERNANCE?locale=en-US&task=implement_task
  - SAP Cloud IAG Integration Scenario Documentation
- http://wiki.scn.sap.com/wiki/display/GRC/Legacy+System+Configuration+and+Risk+Analysis
  - File System for Legacy Extraction Configuration Summary
- https://me.sap.com/notes/2068247
  - 2068247 - Delivered Adapters with SAP Regulation Management by Pathlock and SAP Access Violation Management by Pathlock
- http://pathlock.com/wp-content/uploads/2016/12/SAPAccessViolationManagement-system-integration-editionInfoSheet.pdf
  - Download the SAP Access Violation Management, System Integration Edition Info Sheet

Key Points to Take Home

- It is very important to have compliance processes that are consistent across your entire organization and applicable to all compliance relevant systems in your IT infrastructure.
- For most Customers, their compliance road map began with focusing on SAP environments first. Now it is time to evolve and expand current compliance standards, functionality, and reporting to Cloud, Non-ABAP and Non-SAP compliance relevant systems.
- SAP GRC was built to provide a platform to support non-SAP and non-ABAP connectivity, and SAP is continuing to expand that ability both through product enhancements and partner collaboration.
- Pathlock Access Violation Management - System Integration Edition provides the most comprehensive Real Time functionality for connecting non-SAP and non-ABAP systems to SAP GRC.
- If SoD Analysis is the priority and Real-time information is not essential, then File System for Legacy extraction can provide significant benefit to a customer.

Thank you! Any Questions?

- LinkedIn: **http://www.linkedin.com/in/jamesroeske/**
- Twitter: **http://twitter.com/Roeskinator**

Please remember to complete your session evaluation.

SAPinsider

SAPinsider.org

PO Box 982Hampstead, NH 03841

SAPinsider comprises the largest and fastest growing SAP membership group with more than 800,000 members worldwide.