SAP Security in Hybrid System Landscapes

Alessandro Banzer, Xiting

Hendrik Heyn, Xiting

SAPinsider 2023

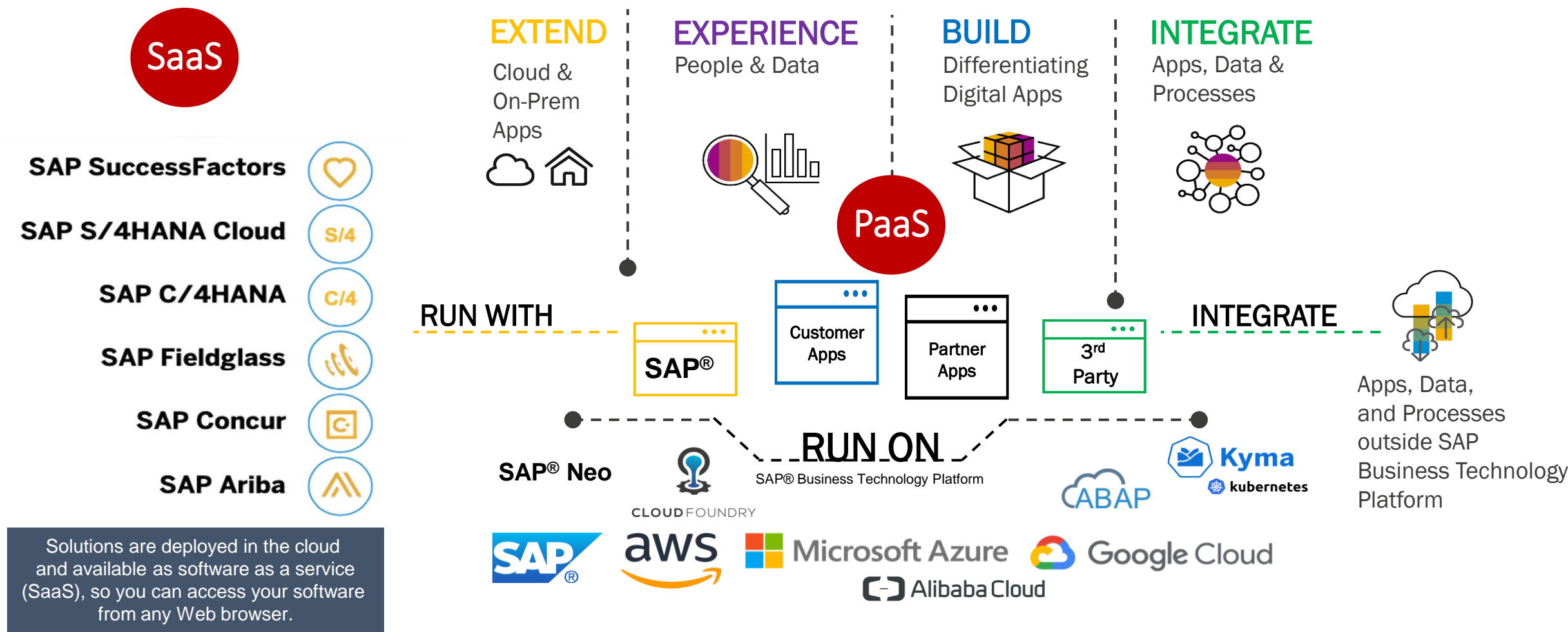SAPinsider

In This Session

- Complexity of hybrid landscapes
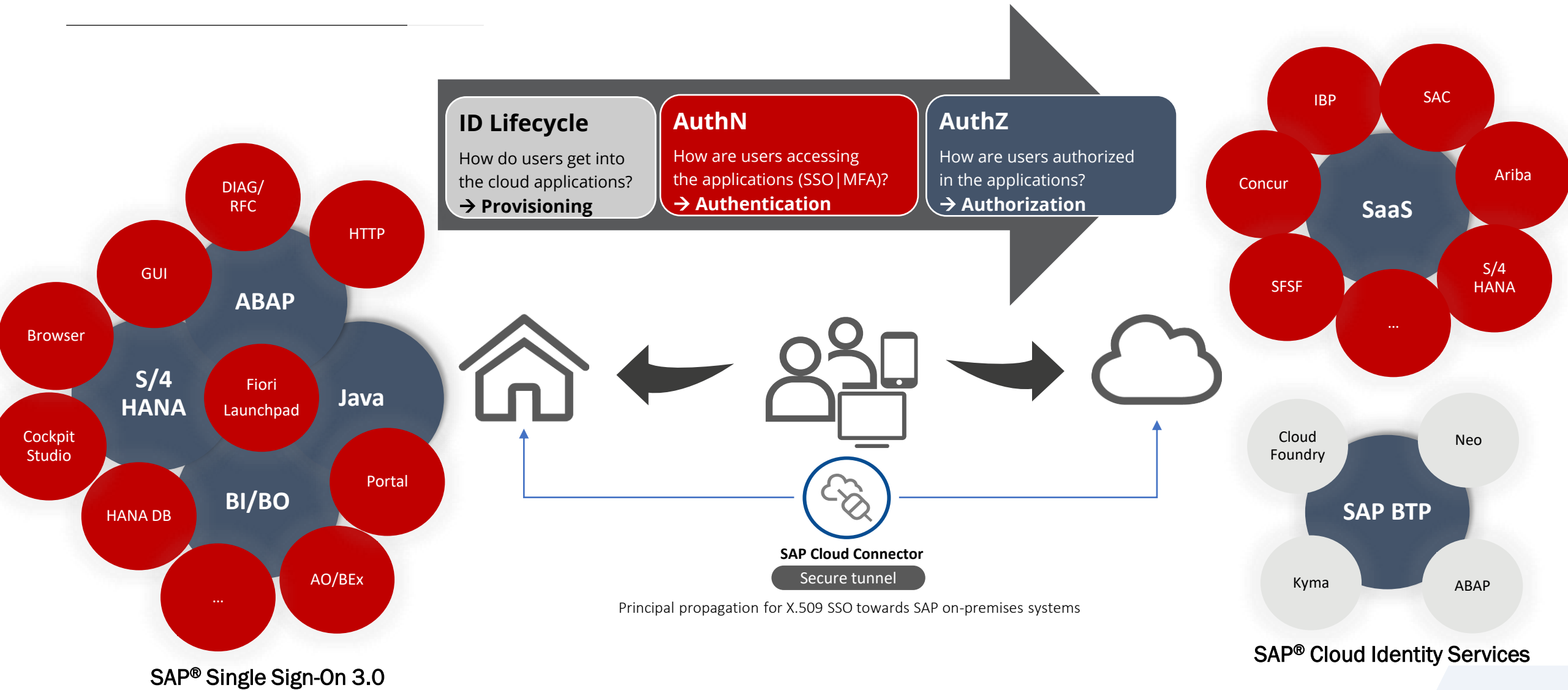- Xiting's solutions
- Practical use cases and applications

SAPinsider

Agenda

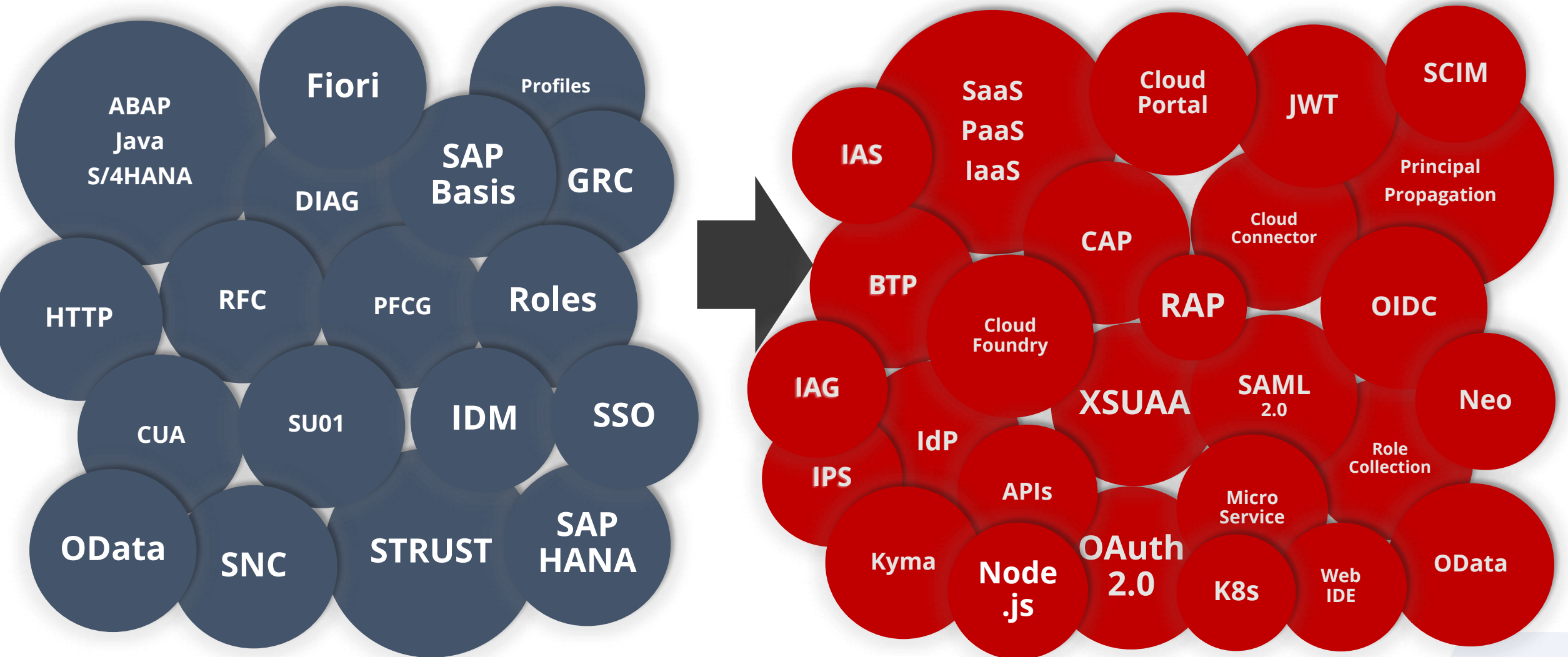- Complexity of Hybrid Landscapes
- Typical Use Cases
- Solutions
- Wrap-Up

Hybrid Landscapes

SaaS

SAP SuccessFactors
SAP S/4HANA Cloud
SAP C/4HANA
SAP Fieldglass
SAP Concur
SAP Ariba

Solutions are deployed in the cloud and available as software as a service (SaaS), so you can access your software from any Web browser.

EXTEND
Cloud & On-Prem Apps

EXPERIENCE
People & Data

BUILD
Differentiating Digital Apps

INTEGRATE
Apps, Data & Processes

PaaS

RUN WITH

SAP®

Customer Apps

Partner Apps

3rd Party

INTEGRATE

Apps, Data, and Processes outside SAP Business Technology Platform

SAP® Neo

RUN ON
SAP® Business Technology Platform

CLOUD FOUNDRY

ABAP

Kyma
kubernetes

SAP

aws

Microsoft Azure

Google Cloud

Alibaba Cloud

SAPinsider

Typical Challenges

ID Lifecycle

How do users get into the cloud applications?
→ **Provisioning**

AuthN

How are users accessing the applications (SSO | MFA)?
→ **Authentication**

AuthZ

How are users authorized in the applications?
→ **Authorization**

SaaS: IBP, SAC, Concur, Ariba, SFSF, S/4 HANA, ...

ABAP: DIAG/RFC, HTTP, GUI
S/4 HANA: Browser, Cockpit Studio, Fiori Launchpad
Java, BI/BO: HANA DB, Portal, AO/BEx, ...

SAP Cloud Connector
Secure tunnel

Principal propagation for X.509 SSO towards SAP on-premises systems

SAP BTP: Cloud Foundry, Neo, Kyma, ABAP

SAP® Single Sign-On 3.0

SAP® Cloud Identity Services

SAPinsider

New Technology -> New Terminology

Typical Challenges and Use Cases

- Unified Security Architecture for Hybrid Landscapes

  - Unified Concepts and Guidelines

  - Unified Identity and Access Management

  - Cross-System Risk Monitoring incl. Segregation of Duties (including non-SAP)

  - Unified Security Monitoring

  - Unified Handling of Threats

Xiting's Solution

- **Access Governance**
  - Cross System SoD & Rulesets
  - Access refinement and remediation
  - Role mining and business roles
  - Emergency Access / Elevated Access
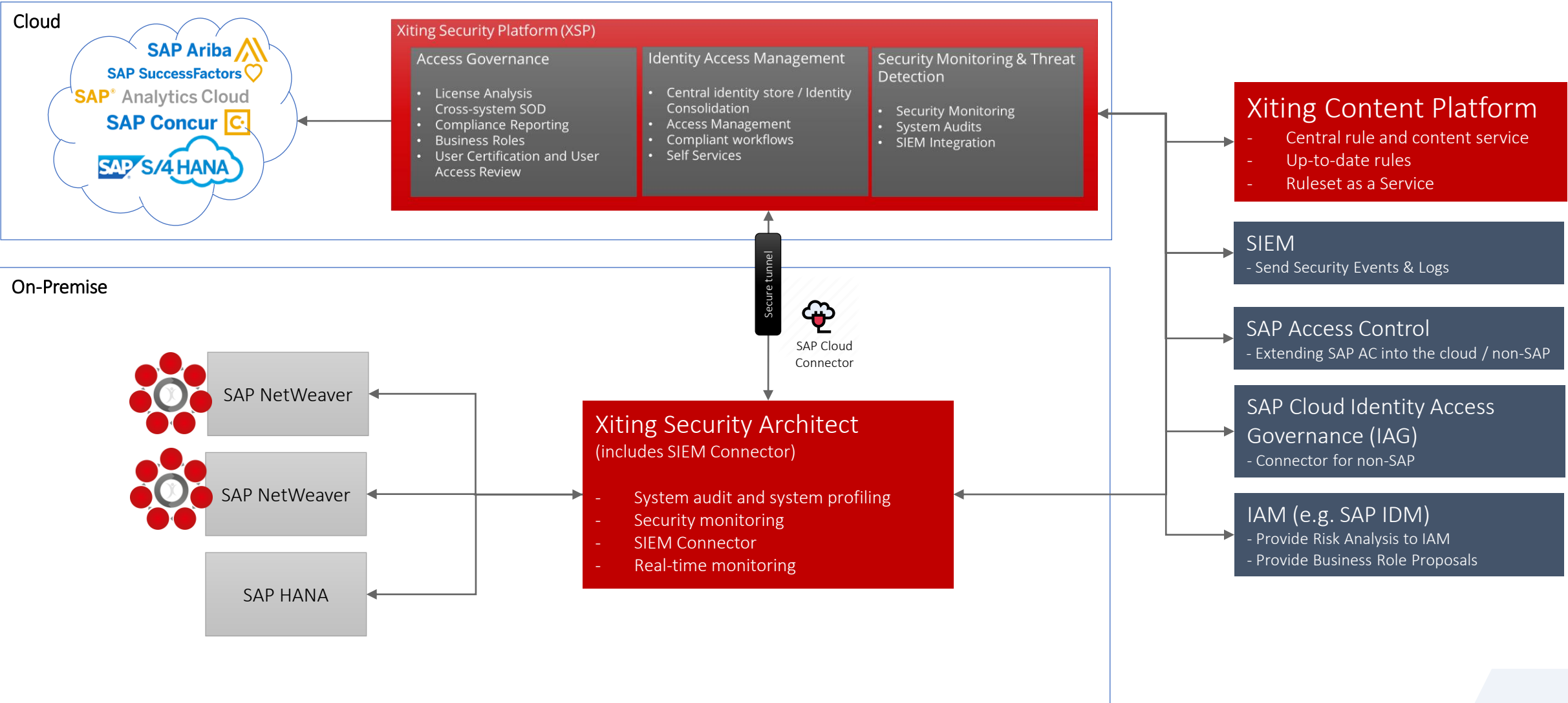 - Security Audits (internal/external)

- **Security Monitoring & Threat Detection**
  - Central Security Monitoring for all SAP applications
  - Real-time Alerting
  - SIEM Integration
  - Insider Threats and Fraud Detection
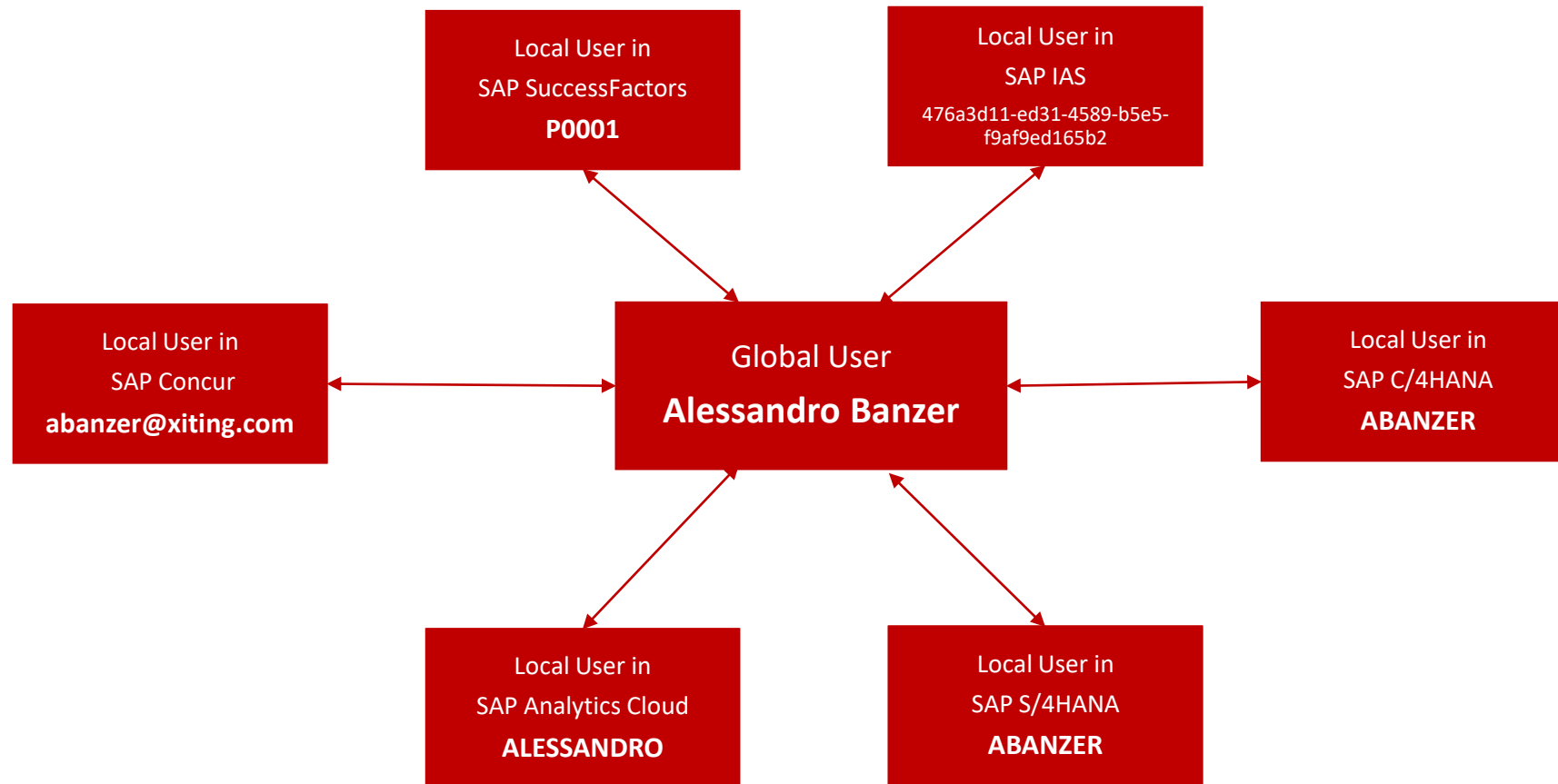
- **Identity Access Management**
  - Consolidated identities
  - Compliant access provisioning to all SAP and non-SAP applications
  - SOD and critical authorization simulation during workflow
  - User access reviews and recertification of access

Xiting's Solutions

Cloud

SAP Ariba
SAP SuccessFactors
SAP® Analytics Cloud
SAP Concur
SAP® S/4 HANA

Xiting Security Platform (XSP)

Access Governance
- License Analysis
- Cross-system SOD
- Compliance Reporting
- Business Roles
- User Certification and User Access Review

Identity Access Management
- Central identity store / Identity Consolidation
- Access Management
- Compliant workflows
- Self Services

Security Monitoring & Threat Detection
- Security Monitoring
- System Audits
- SIEM Integration

Xiting Content Platform
- Central rule and content service
- Up-to-date rules
- Ruleset as a Service

SIEM
- Send Security Events & Logs

SAP Access Control
- Extending SAP AC into the cloud / non-SAP

SAP Cloud Identity Access Governance (IAG)
- Connector for non-SAP

IAM (e.g. SAP IDM)
- Provide Risk Analysis to IAM
- Provide Business Role Proposals

On-Premise

Secure tunnel

SAP Cloud Connector

SAP NetWeaver

SAP NetWeaver

SAP HANA

Xiting Security Architect
(includes SIEM Connector)

- System audit and system profiling
- Security monitoring
- SIEM Connector
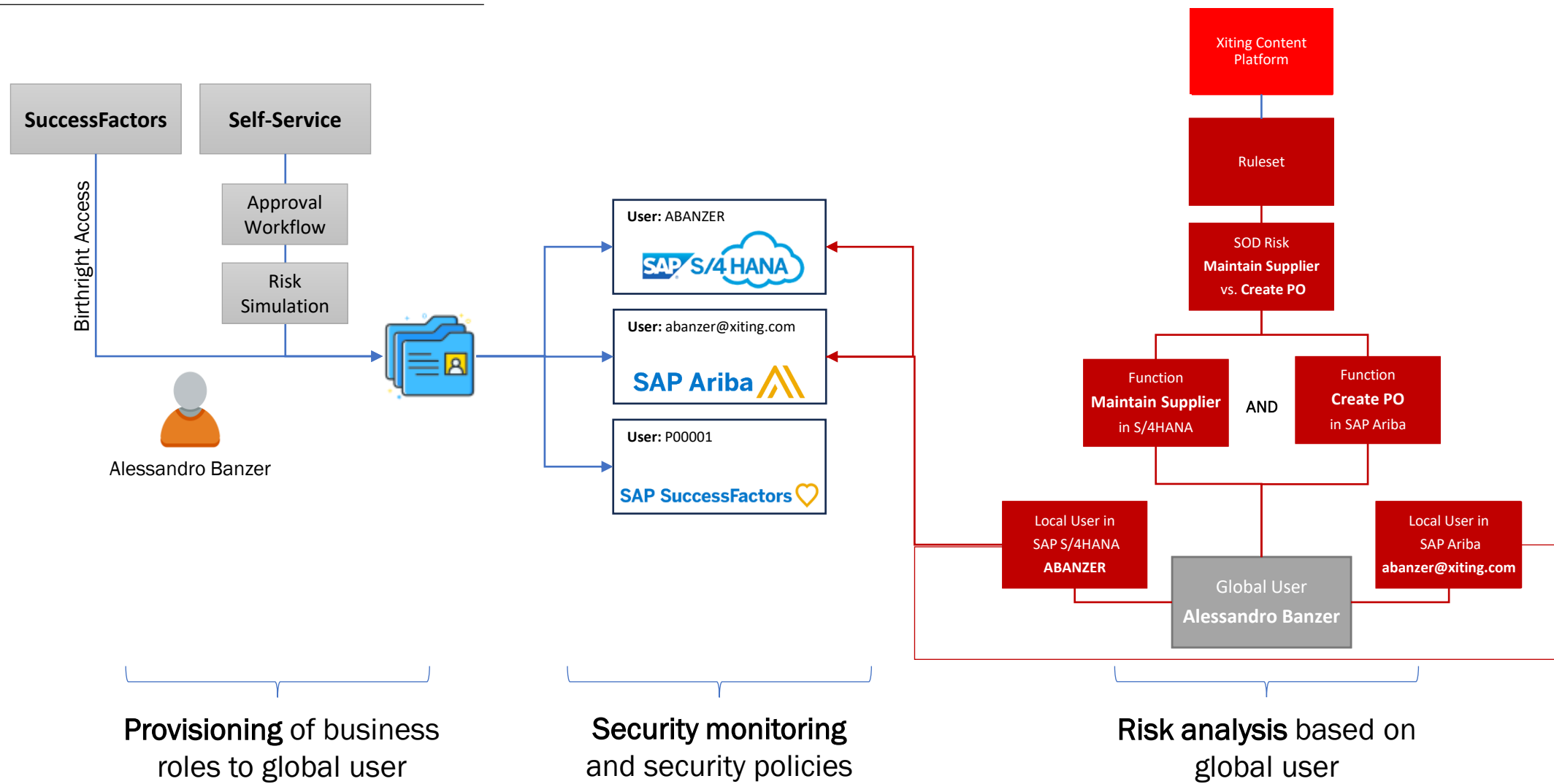- Real-time monitoring

SAPinsider

Xiting Security Platform – Identity Consolidation

- Consolidation of decentralized identities into the same persona

Xiting Security Platform – Utilizing Consolidated Identities

Provisioning of business roles to global user

Security monitoring and security policies

Risk analysis based on global user

Wrap up

- Challenges in hybrid landscapes are similar but different than on-prem

- Identity lifecycle is important to get users in and out of applications

- Authorizations and authentication more important than ever due to outside facing applications

- Don't neglect security monitoring and proper security strategy

Where to Find More Information

- SAPinsider.org
- https://xiting.com/en/leveraging-iga-for-enhanced-security/
    - Leveraging IGA for enhanced security: an overview and the unique offerings of Xiting
- https://xiting.com/en/whitepaper-sap-security-hardening/
    - Whitepaper: Security Hardening – Implement Security by Design and Zero Trust Follow

Key Points to Take Home

- Acknowledge the complexity and begin with a best-practice workshop.

- Ensure proper implementation of cloud applications into the identity lifecycle processes.

- Rethink identities and utilize proper implementation practices.

- Risk analysis requires updated rule definitions for cloud applications.

- Proactive security monitoring and security policies for future-proof compliance and access governance.

Thank you! Questions?

Alessandro Banzer

CEO Americas, Xiting

abanzer@xiting.com

LinkedIn

Hendrik Heyn

CEO Global/Germany, Xiting

hheyn@xiting.com

LinkedIn

Please remember to complete your session evaluation.

SAPinsider

in 🐦 📷

SAPinsider.org

SAPinsider comprises the largest and fastest growing SAP membership group worldwide, with more than 750,000 global members.

SAPinsider