RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **STR-R03**

# Epic Journey of an Enterprise Cloud Transformation While Building Security

**Helen Oakley, CISSP, GPCS**

Senior Product Security Architect, SAP Global Security
**SAP**

@e2hln
/in/helen-oakley

# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

**www.sap.com/contactsap**

© 2022 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/trademark for additional trademark information and notices.

# Content

- 30,000-foot view
- Walking Through the Transformation
- Cloud Transformation and Security: Use Cases
- Takeaways, you can apply in your organization starting today

RSAConference2022

# 30,000-foot view

# 30,000-foot view: SAP

Hundreds of products across six main portfolio categories

Cloud, On-Premise, Hybrid solutions

Wide range of technologies, programming languages

# Mindset Shift

| From | To |
| --- | --- |
| Moment in time | Journey |
| Fit to gap | Fit to standard |
| Monolithic | Modular |

**Digital transformation is not a destination,**
**it's a continuous journey.**

# Common Industry Challenges

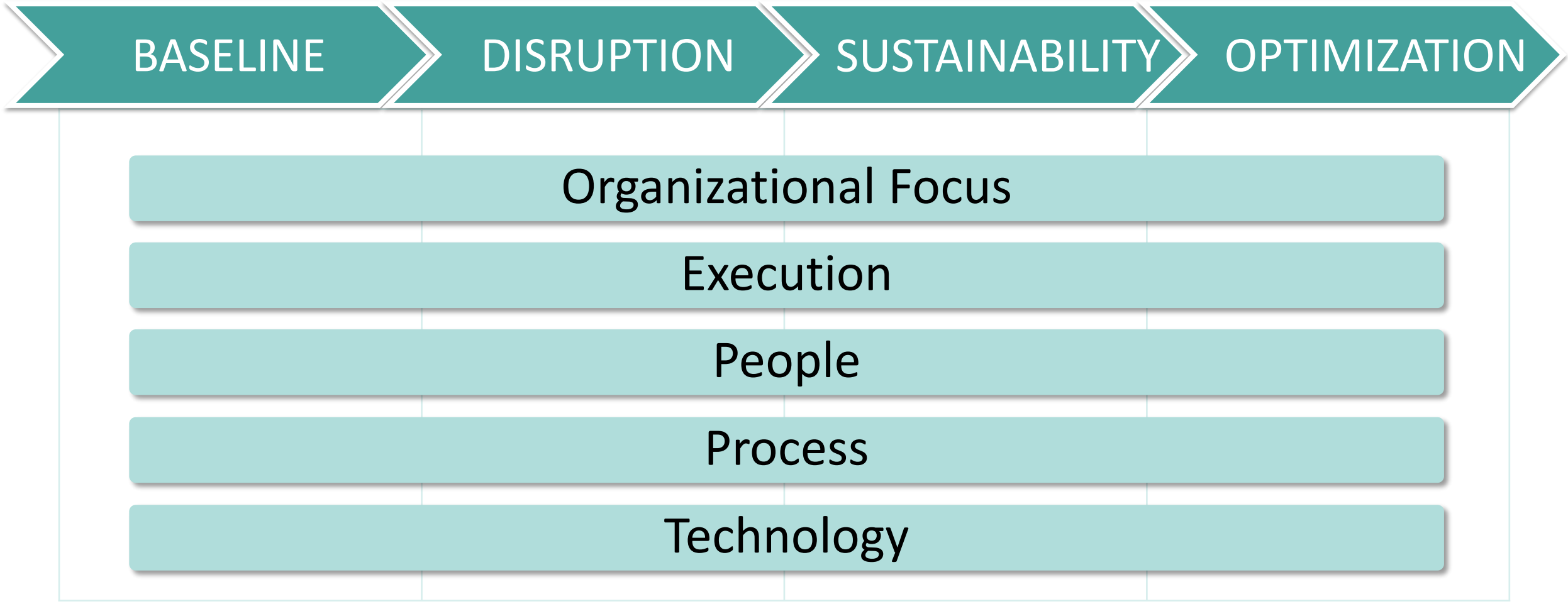
- Complex, hybrid IT landscapes and increasing technical debt
- Shortage of developers (drives LCNC* trend), shortage of security professionals, and limited time
- Evolving security threats

*LCNC: low-code and no-code (solutions)

RSAConference2022

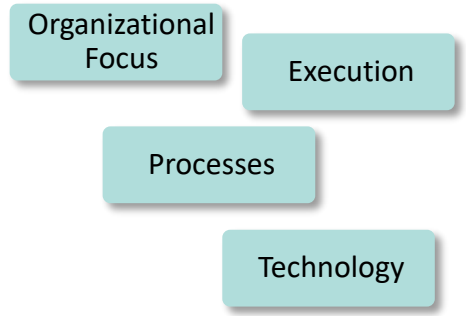
# Working Through the Transformation

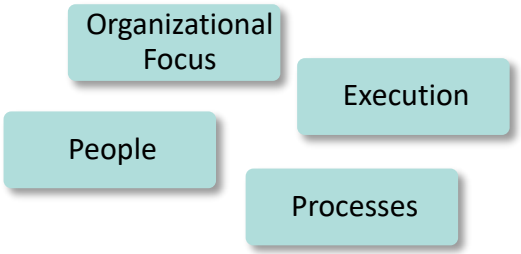
# Enterprise Security Transformation

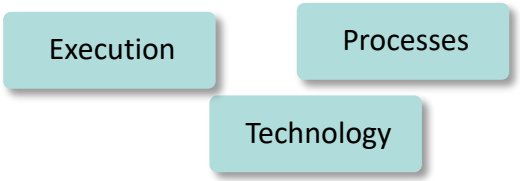


# Security Challenges with Cloud Transformation

| Common Industry Challenges | Translated Security Challenges |
| --- | --- |
| Complex, hybrid IT landscapes and increasing technical debt | · Security controls must handle a mix of technologies and integration<br>· Software supply chain risks (third party, open source, dev infrastructure) |
| Shortage of professionals (especially, on security side), and limited time | · Lack of security culture<br>· The need for harmonized processes |
| Evolving security threats | · The need for proactive approach and streamlined response |



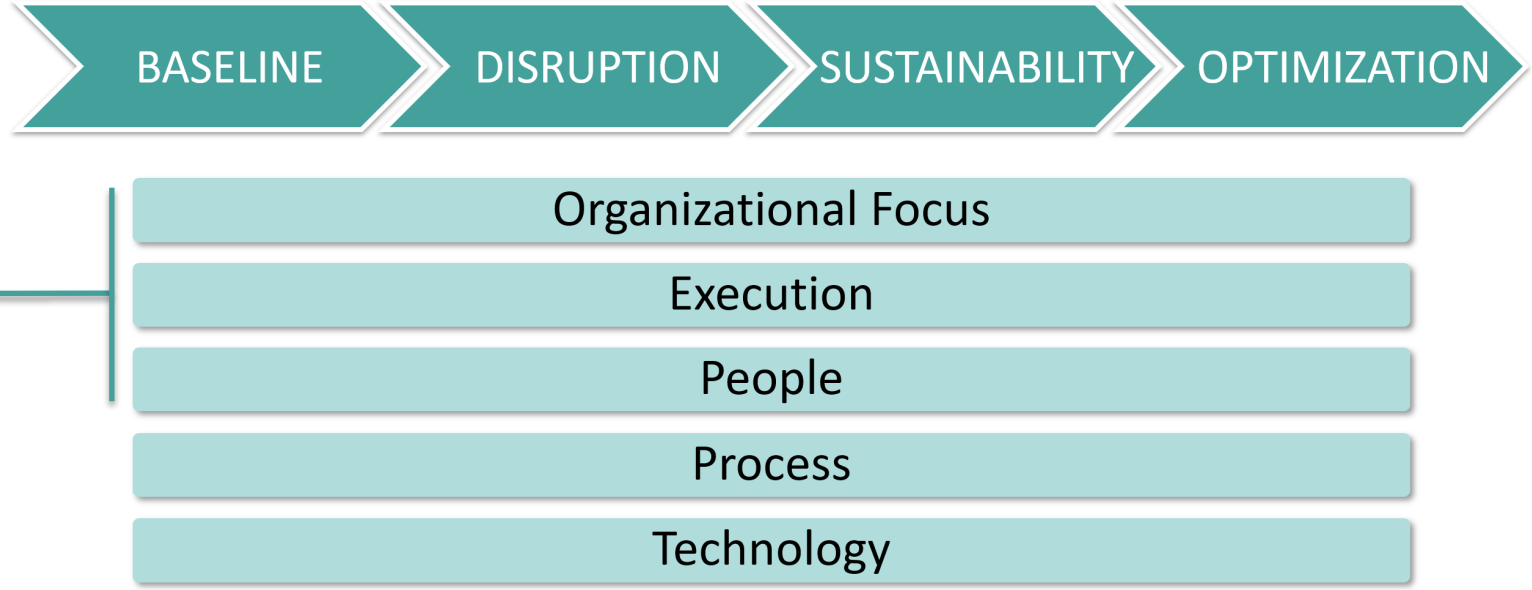



# Working through the Security Challenges with Cloud Transformation

## Security Challenge Areas:

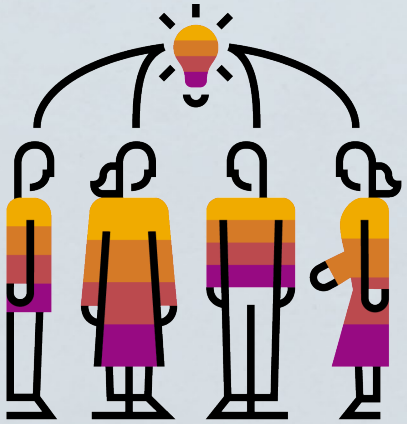
1. Security Culture
2. Processes
3. Technology



RSAConference2022

# Working Through the Transformation

## Security Culture



# Security Culture

- Security is a matter of quality
- Education, make it fun
- Cybersecurity hygiene
- Continuous improvement
- Risk assessment
- Zero-defect approach
- Testing & validation
- Collaboration, security champions

To develop and operate secure software, we need to change our development culture, looking beyond the technology, at the organization that created it.

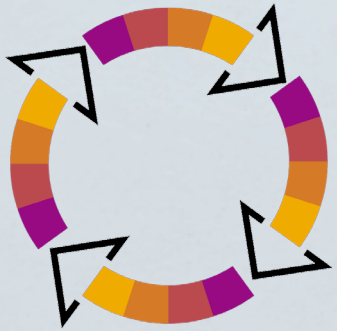
The change has to start with **people**.

Security Culture Toolkit: https://www.sap.com/about/trust-center/security.html?pdf-asset=c8573354-f87d-0010-bca6-c68f7e60039b

RSAConference2022

# Working Through the Transformation

## Processes



# Transformation of Security Requirements

## Foundational

- Secure against untrusted Input
- Secure Communications
- Secure Identity Management and Authentication
- Secure Cryptography
- Secure Audit Logging
- Secure by default & by design
- Data Protection & Privacy
- Secure Authorizations
- Secure Storage

## Cloud security

- Secure against untrusted Input
- Secure Communications
- **Secure Identity Management and Authentication +**
- Secure Cryptography
- **Secure Audit Logging +**
- Secure by default & by design
- **Data Protection & Privacy +**
- **Secure Authorizations +**
- **Secure Storage +**
- **Secure Operations**
- **Secure Multi-Tenancy**

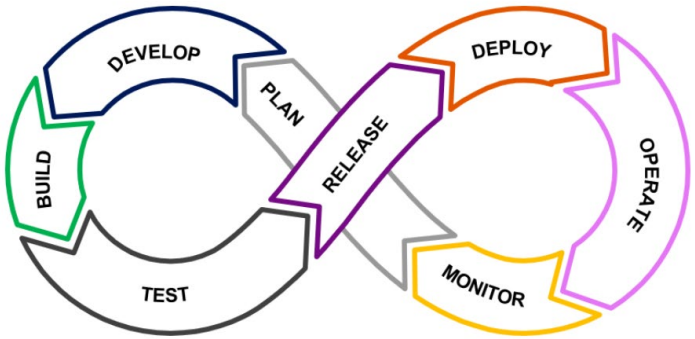
# Transformation of Secure Processes

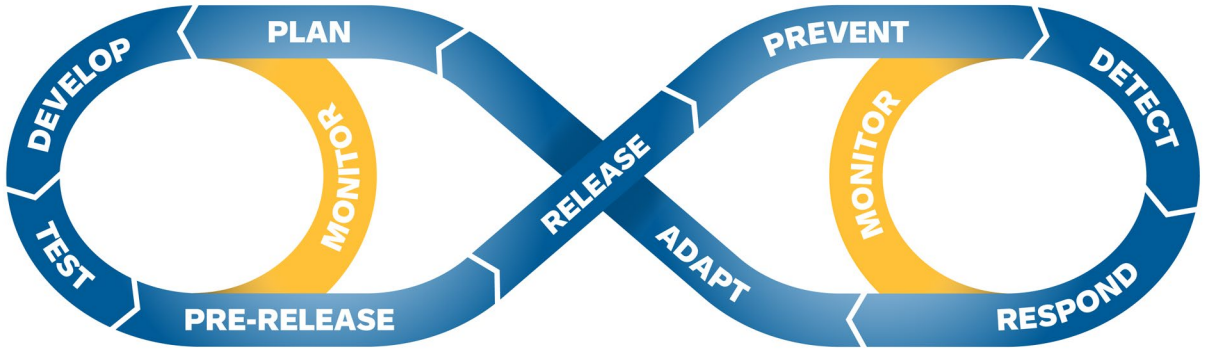
Secure Software Development and Operations Lifecycle (aka Secure SDOL)

## From Linear…

Provided foundational guidance for security activities throughout development lifecycle (risk-based approach, recommendations)

## To Continuous…




**Gen1**: Introduced continuous approach towards secure development and operations (risk-based, contract-based requirements, recommendations)

**Gen2**: Optimized continuous approach towards secure development and operations (contract-based, mandatory requirements, software supply chain safeguards, etc.)

# Continuous Compliance

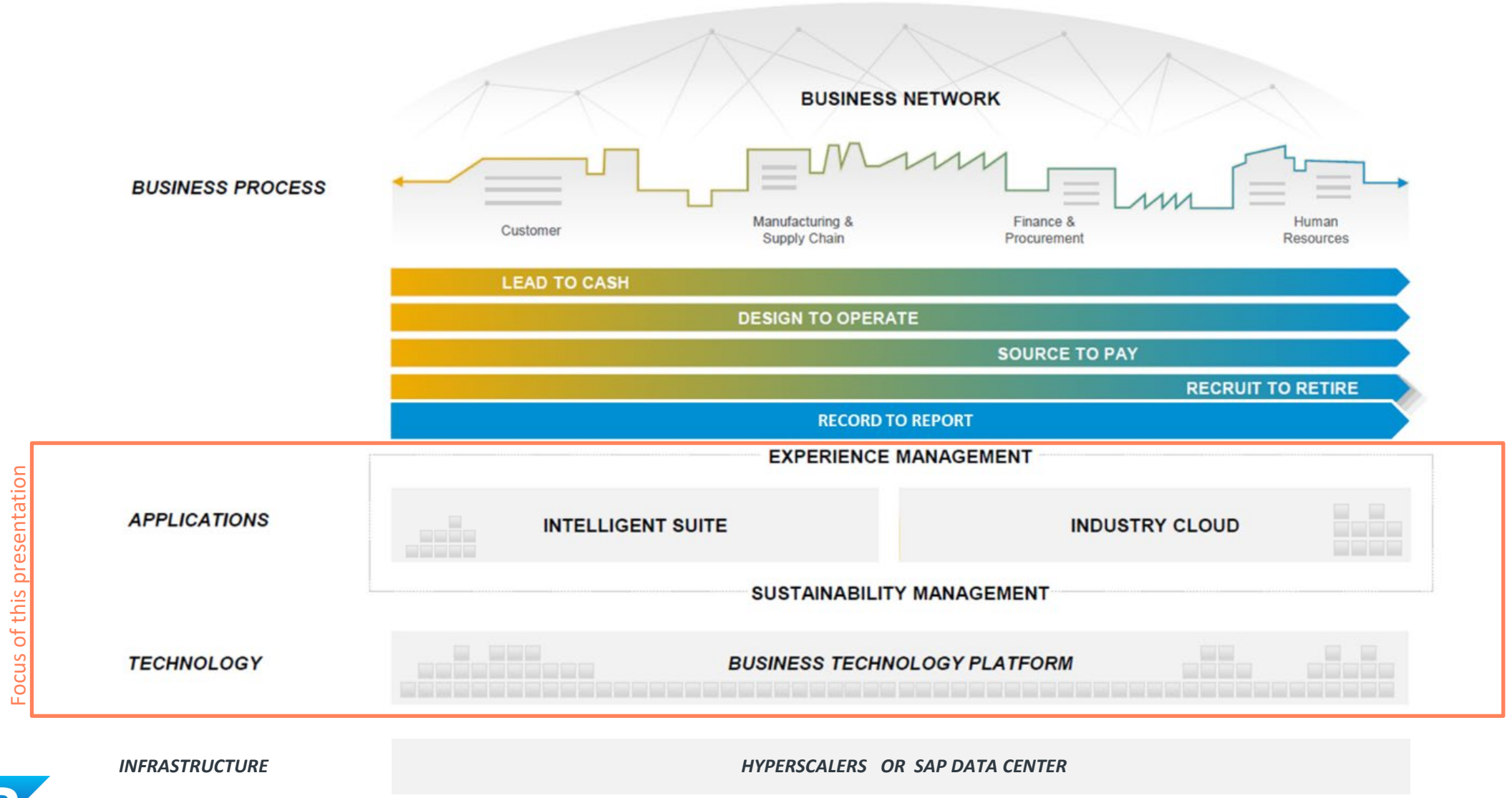
- Controls mapping to:
  - Security requirements
  - Secure Software Development and Operations Lifecycle
- Onboarding procedure
- Accountability (dev teams)
- Centralized support

RSAConference2022

# Working Through the Transformation

## Technology

# SAP Reference Architecture




https://www.sap.com/documents/2020/02/520ea921-847d-0010-87a3-c30de2ffd8ff.html

# Integration through SAP Suite Qualities

SAP's Cross Product Architecture (CPA) workstreams

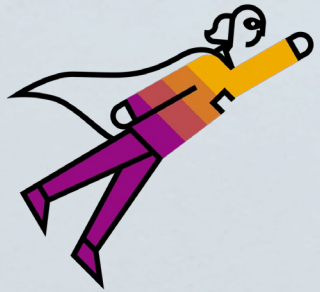
- Aligned domain models
- Consistent security & identity management out-of-the-box
- Coordinated lifecycle management

https://www.sap.com/documents/2020/02/520ea921-847d-0010-87a3-c30de2ffd8ff.html

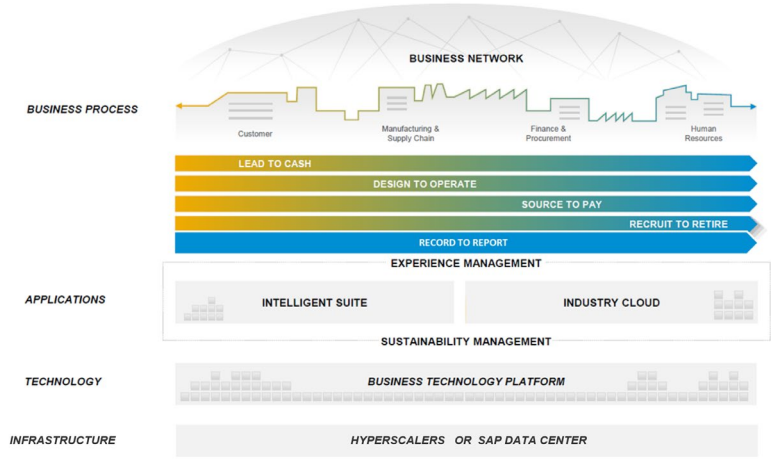
RSAConference2022

# Cloud Transformation and Security

## Use Cases



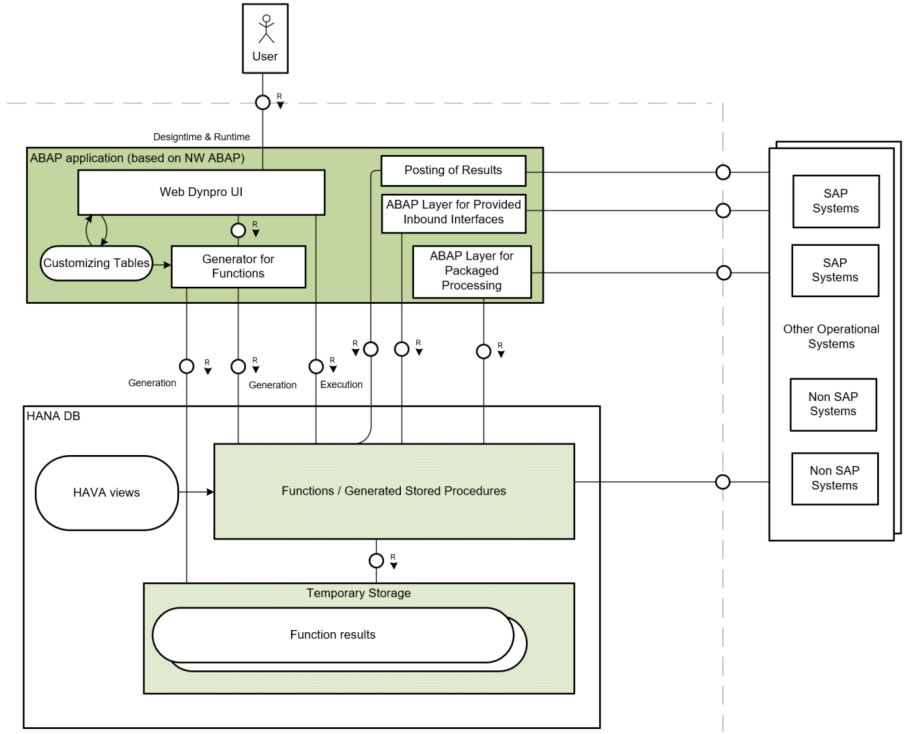
# Use Case 1: Intelligent Suite



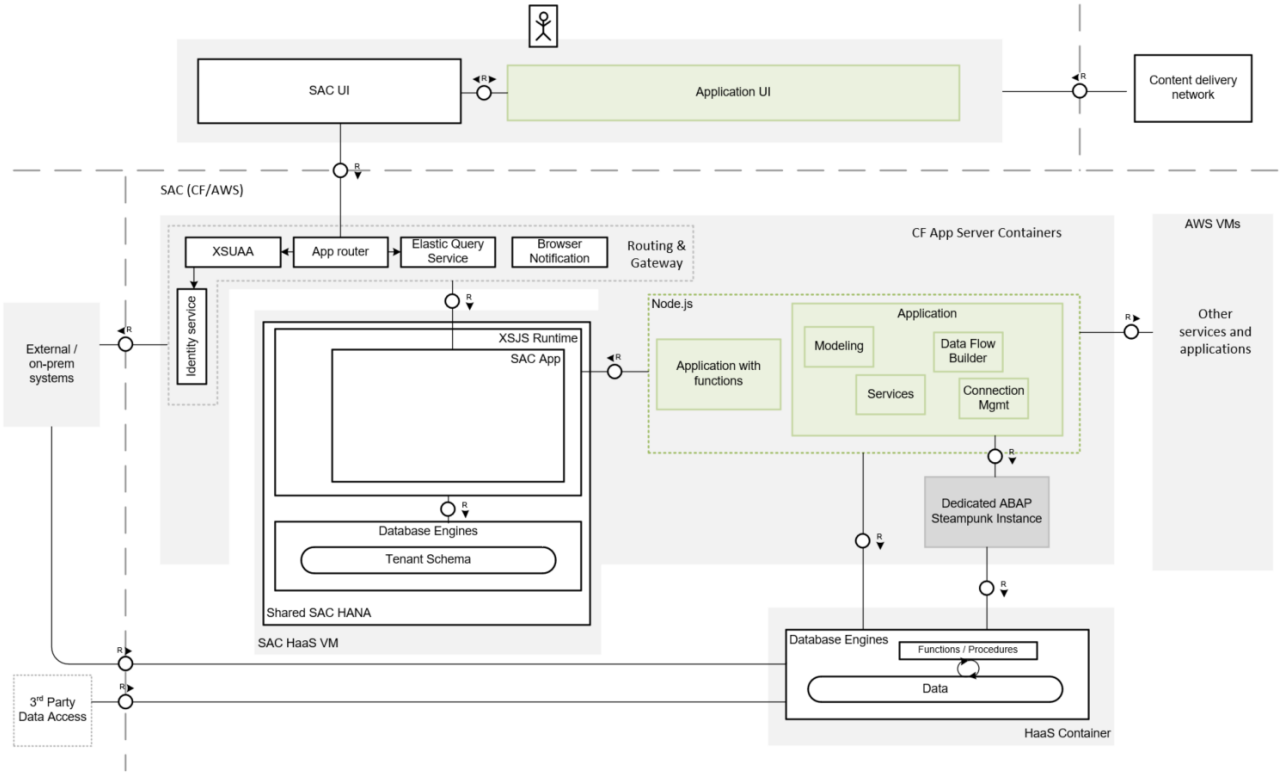
# Use Case 1: Reference Architecture for Transformed Application

From ABAP on-prem to Node.js native cloud

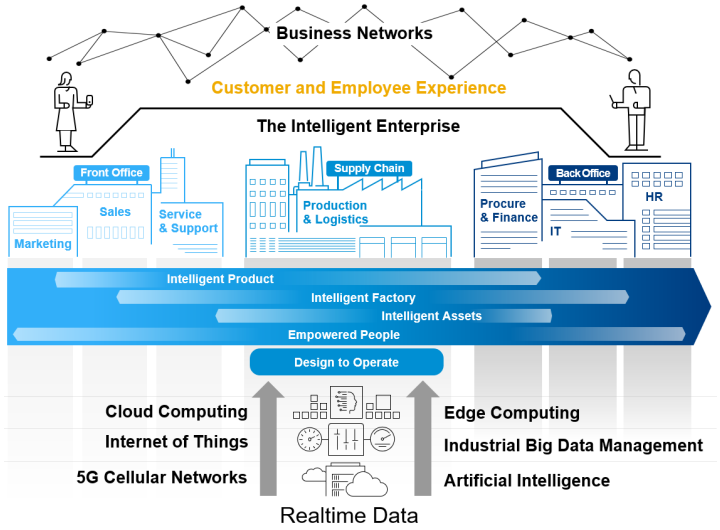
## Before: on-prem



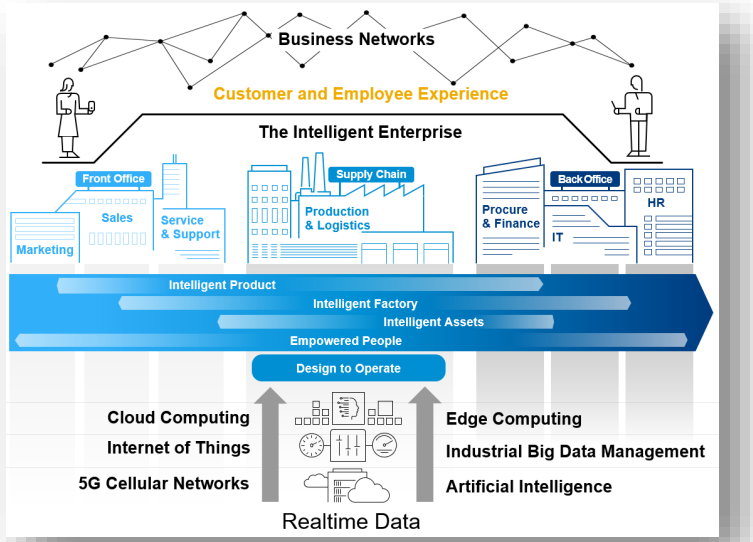

## New: cloud

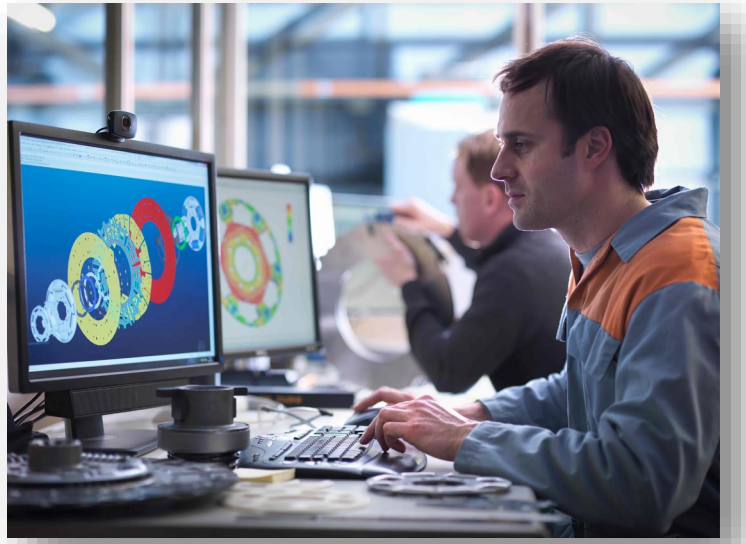


# Use Case 2: Industry 4.Now



# Use Case 2: Security Challenges for Industry 4.Now



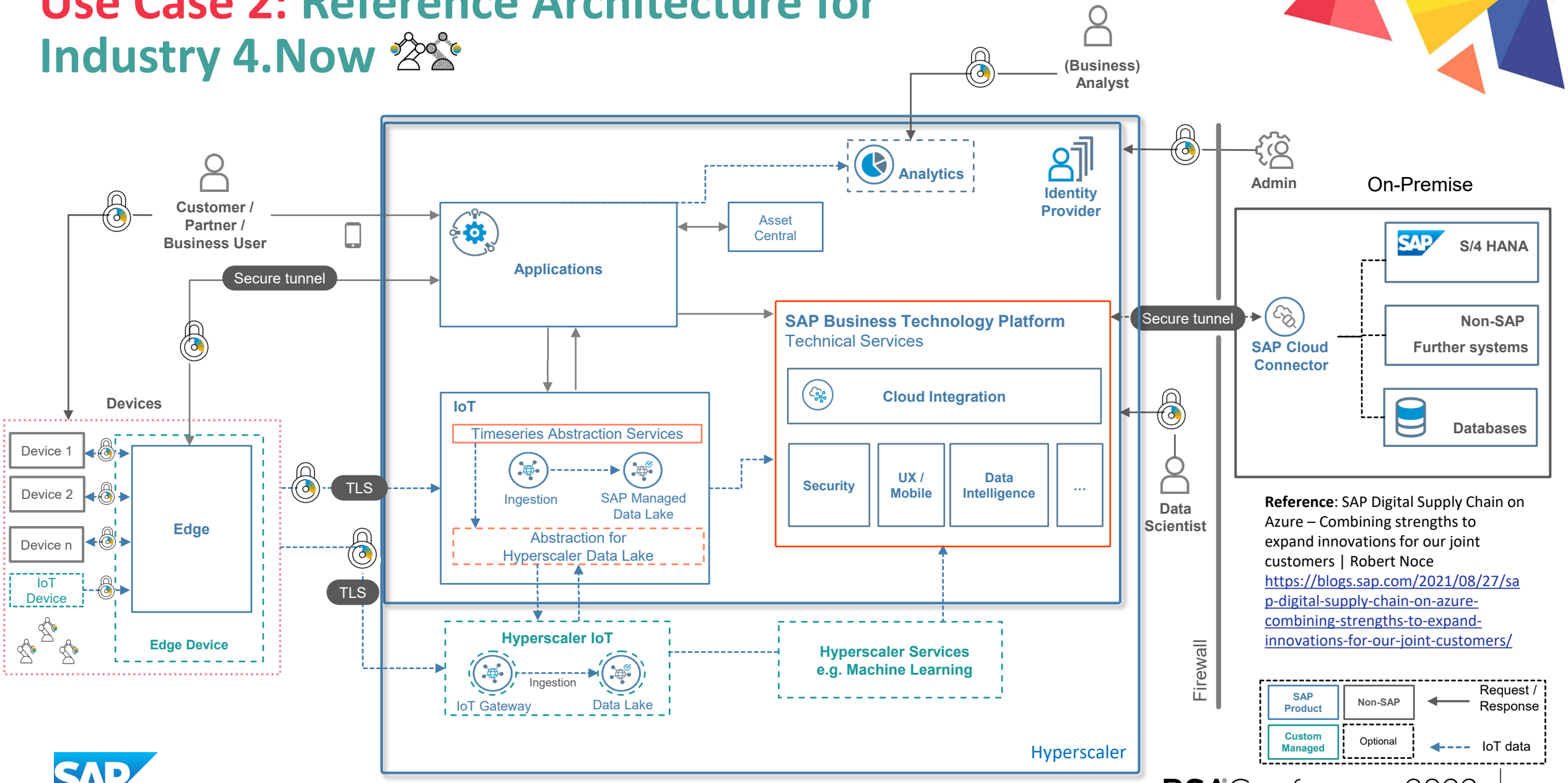


Landscape Complexity

Digitization of Industrial Technology

Intellectual Property Concerns

# Use Case 2: Reference Architecture for Industry 4.Now

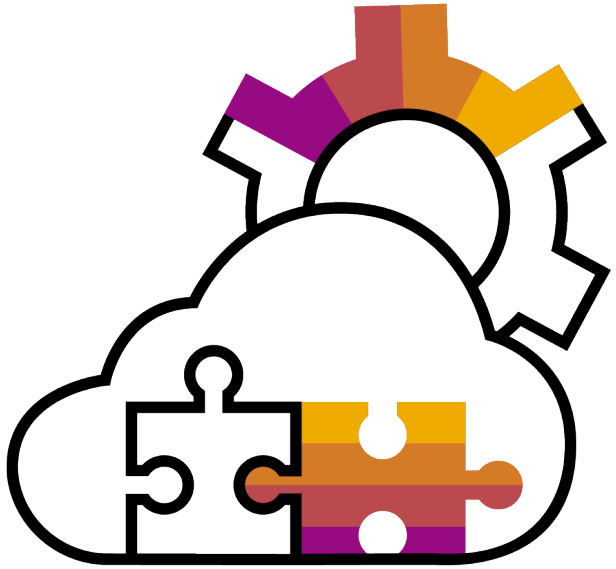



**Reference**: SAP Digital Supply Chain on Azure – Combining strengths to expand innovations for our joint customers | Robert Noce https://blogs.sap.com/2021/08/27/sap-digital-supply-chain-on-azure-combining-strengths-to-expand-innovations-for-our-joint-customers/

# Use Cases Summary: Security at SAP

Build-in security at every level of organization, connected security to business objectives

- Built-in security capabilities and processes
- Incorporated latest technical services (qualities) for integration or security capabilities
- Onboarding to operations and audit services



RSAConference2022

# Takeaways

# Apply what you've learned

Step forward to the higher level of security maturity at your organization.

## 1. Security Culture

- Connect security to business objectives
- Security Culture Toolkit: www.sap.com/about/trust-center/security.html?pdf-asset=c8573354-f87d-0010-bca6-c68f7e60039b

  or use tinyURL: **tinyurl.com/SecurityCultureToolkit**

## 2. Process

- Integrate, automate, improve
- Threat model DevOps processes and tooling

## 3. Technology

- Perform risk assessment: application, infrastructure, 3rd party
- Build security into everything; defense in depth; foundation
- SAP's transformation: www.sap.com/documents/2020/02/520ea921-847d-0010-87a3-c30de2ffd8ff.html

  or use tinyURL: **tinyurl.com/TransformationRoadmap**

# Thank You

**Helen Oakley**, CISSP, GPCS

@e2hln

/in/helen-oakley

SAP Global Security

www.sap.com/about/trust-center.html

THE BEST RUN SAP