



# SAP Premium Engagement Session

## Cybersecurity

September 23, 2021

PUBLIC

# Agenda

- Welcome Session by Nina Schertinger
- [Identity and Access Governance, Data Protection and Privacy, Cybersecurity, Enterprise Risk and Compliance](#) by Arndt Lingscheid
- [How Can Premium Engagements Support](#) by Natascha Lalor
- Wrap up by Nina Schertinger





# Overview IAG, DPP, Cybersecurity & Enterprise Risk and Compliance

Arndt Lingscheid  
09, 2021

PUBLIC

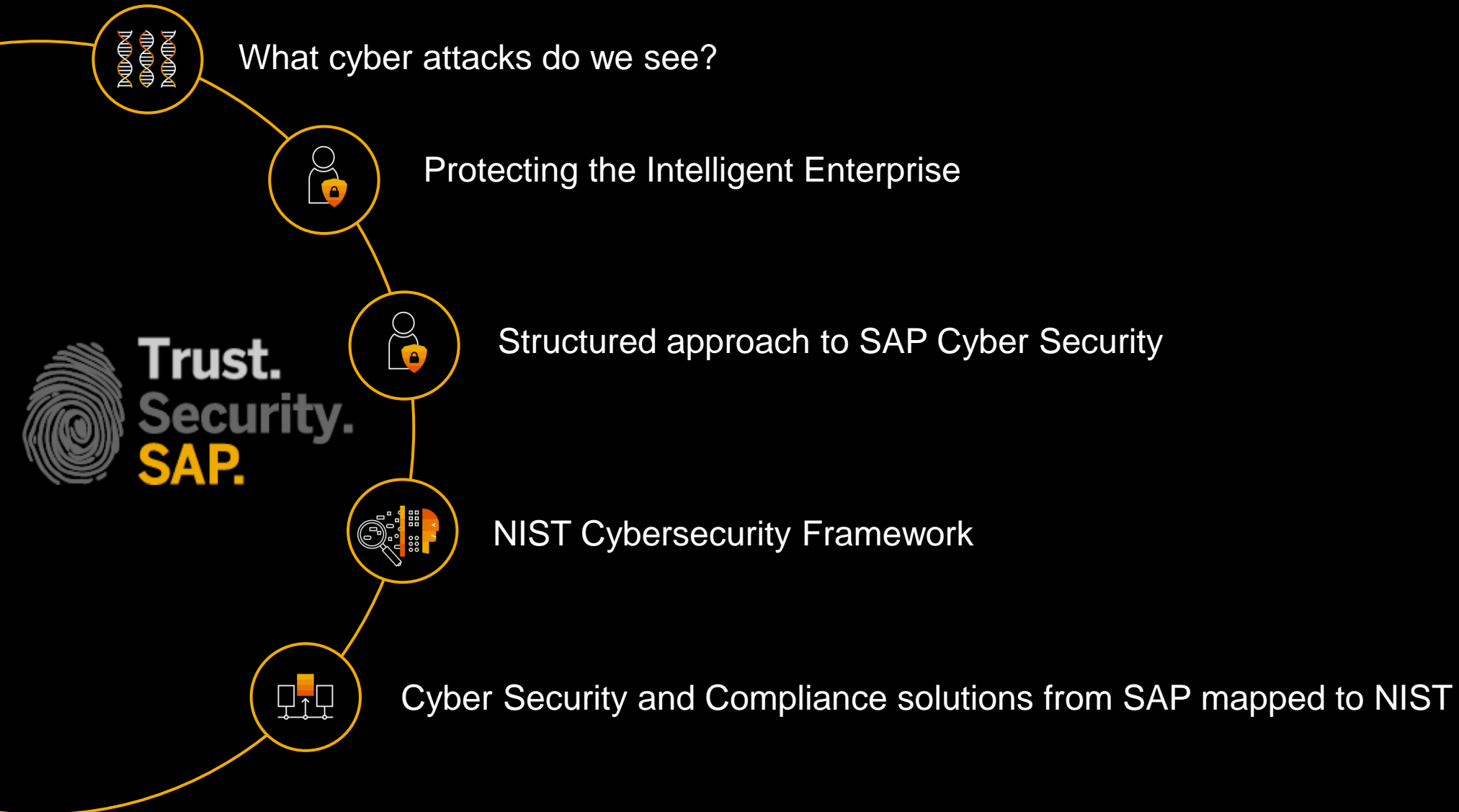
# Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP's intentional or gross negligence.

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, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

# SAP Solutions for Cyber Security and Data Protection

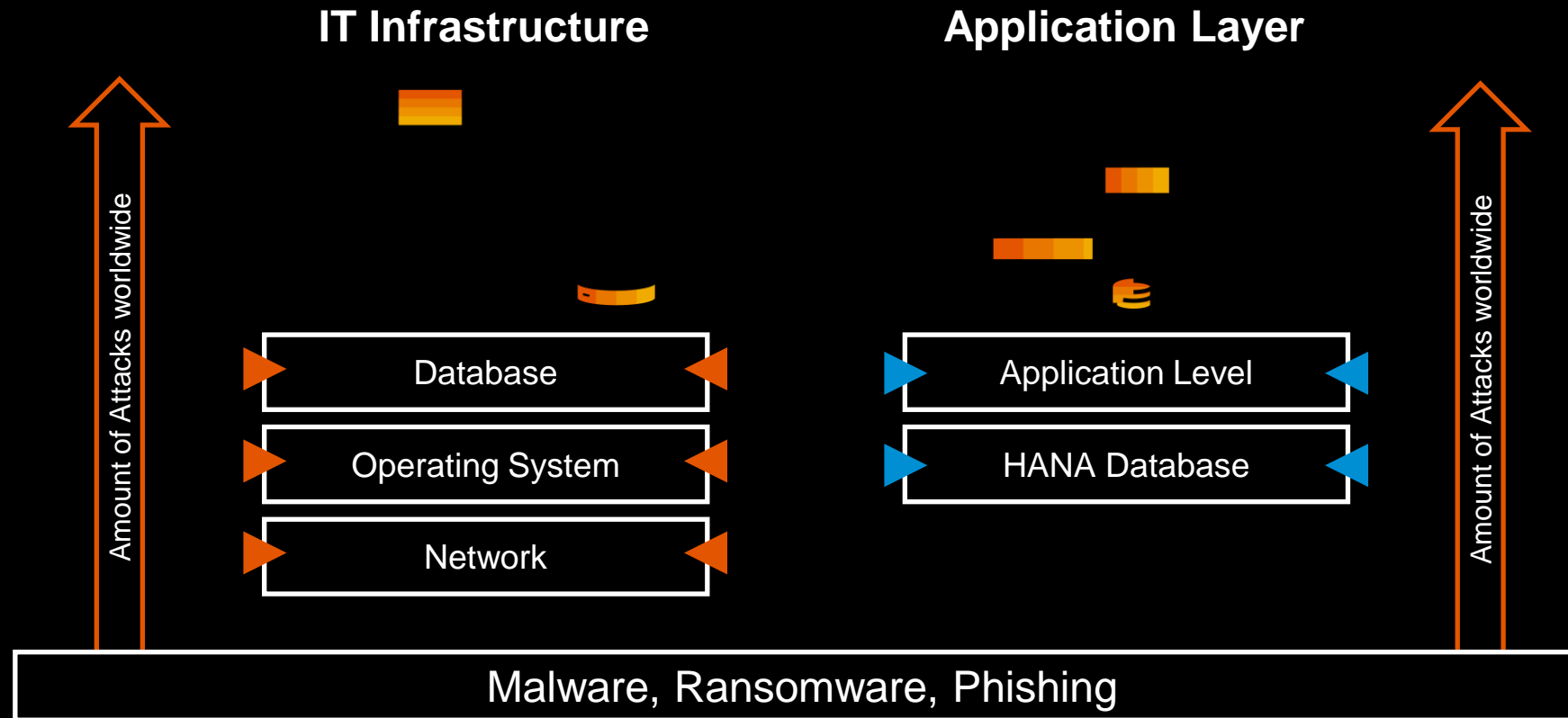






Systems are under attack

# IT Infra s vs. Application



Analysts e.g. from insurance companies rate cyber attacks as the biggest risks for enterprises worldwide within the top 10 Business Risks.

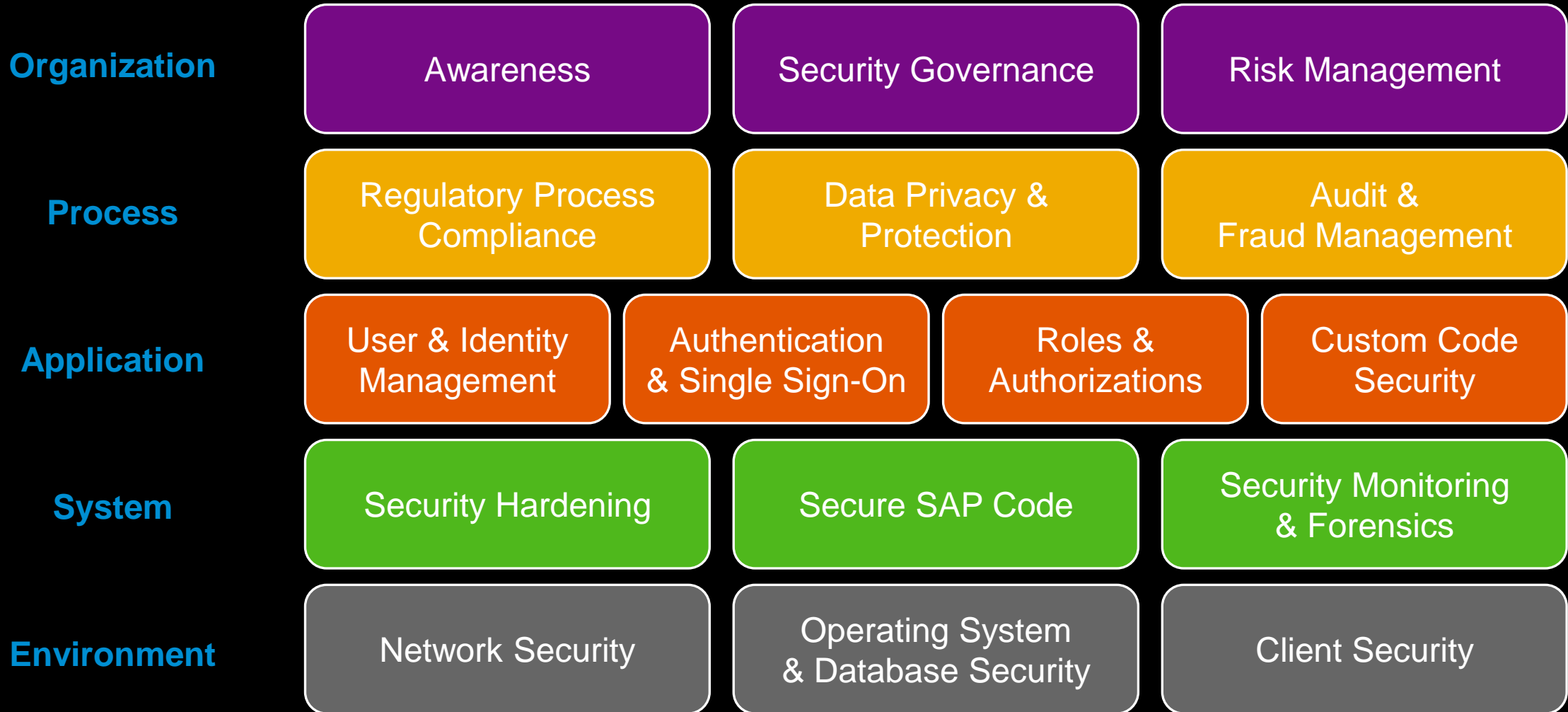
# Sobering Statistics

- Businesses that had not deployed security automation saw an average total cost of **\$6.03 million**, more than double the average cost of a data breach of **\$2.45 million** for businesses that had fully deployed security automation.
- **\$5.52 million average total cost of a breach** at enterprises of more than 25,000 employees
- **Mega Breaches:** In breaches of more than 50 million records, the average cost was **\$392 million**, more than 100 times the average.
- The time to contain a security breach on average is **280 days**.
- Lost business costs **\$1.52 million** accounted for nearly **40%** of the average total cost of a data breach.
- It's not a question of experiencing a data breach. It's only a question WHEN!  
(The percentage chance of experiencing a data breach within two years was 29.6 percent in 2019.)

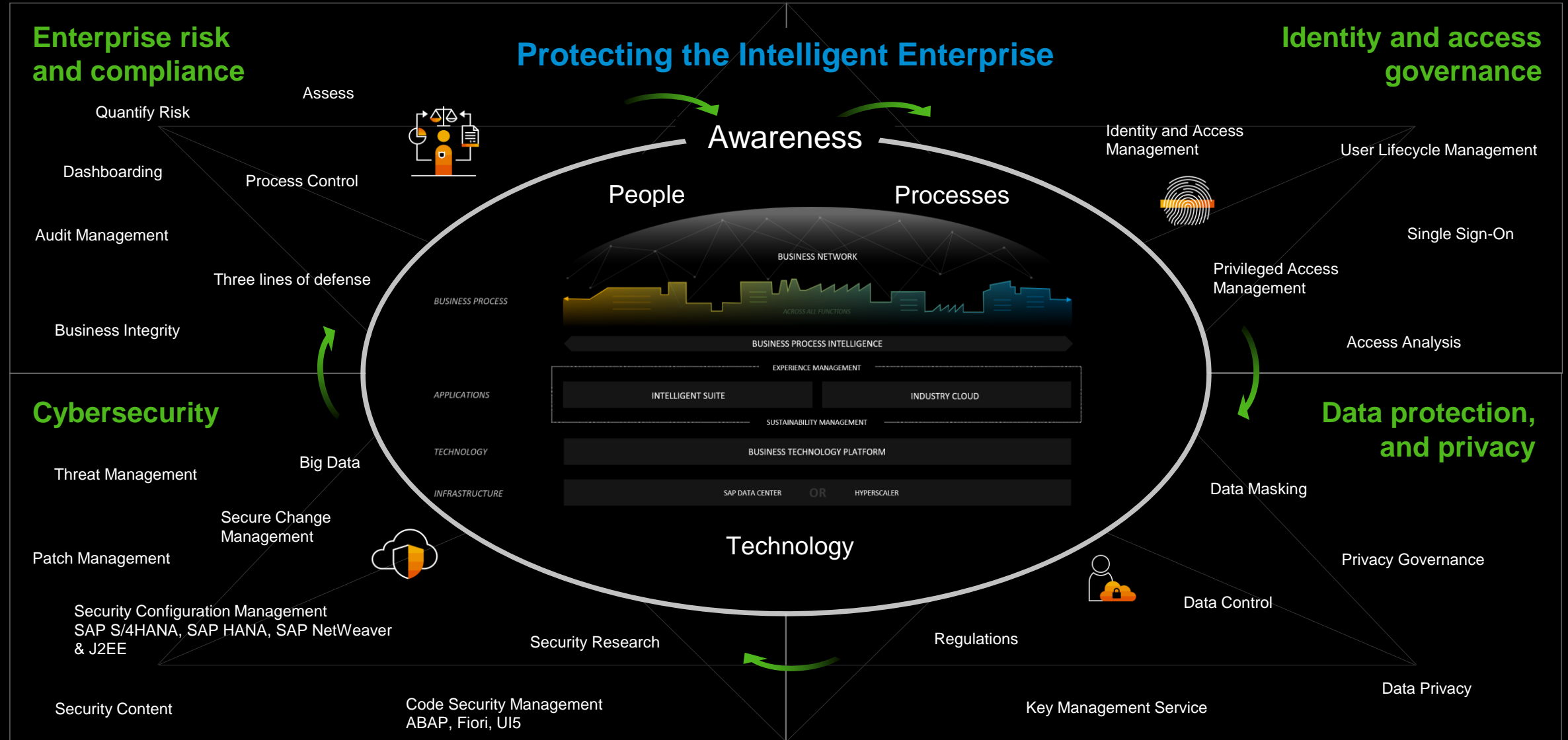
***...and your SAP systems hold mission critical data which can be a blind spot for IT security teams***



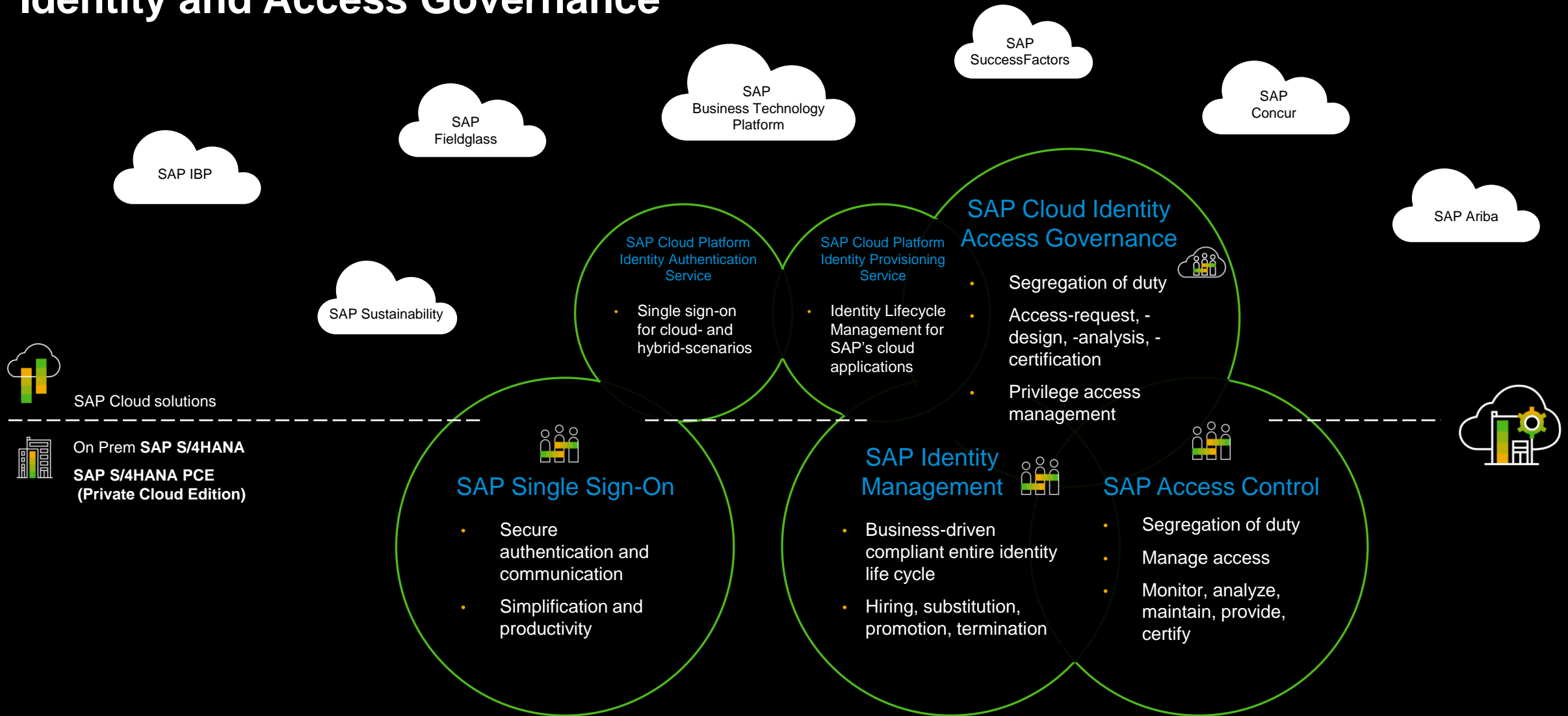
# SAP Secure Operations Map



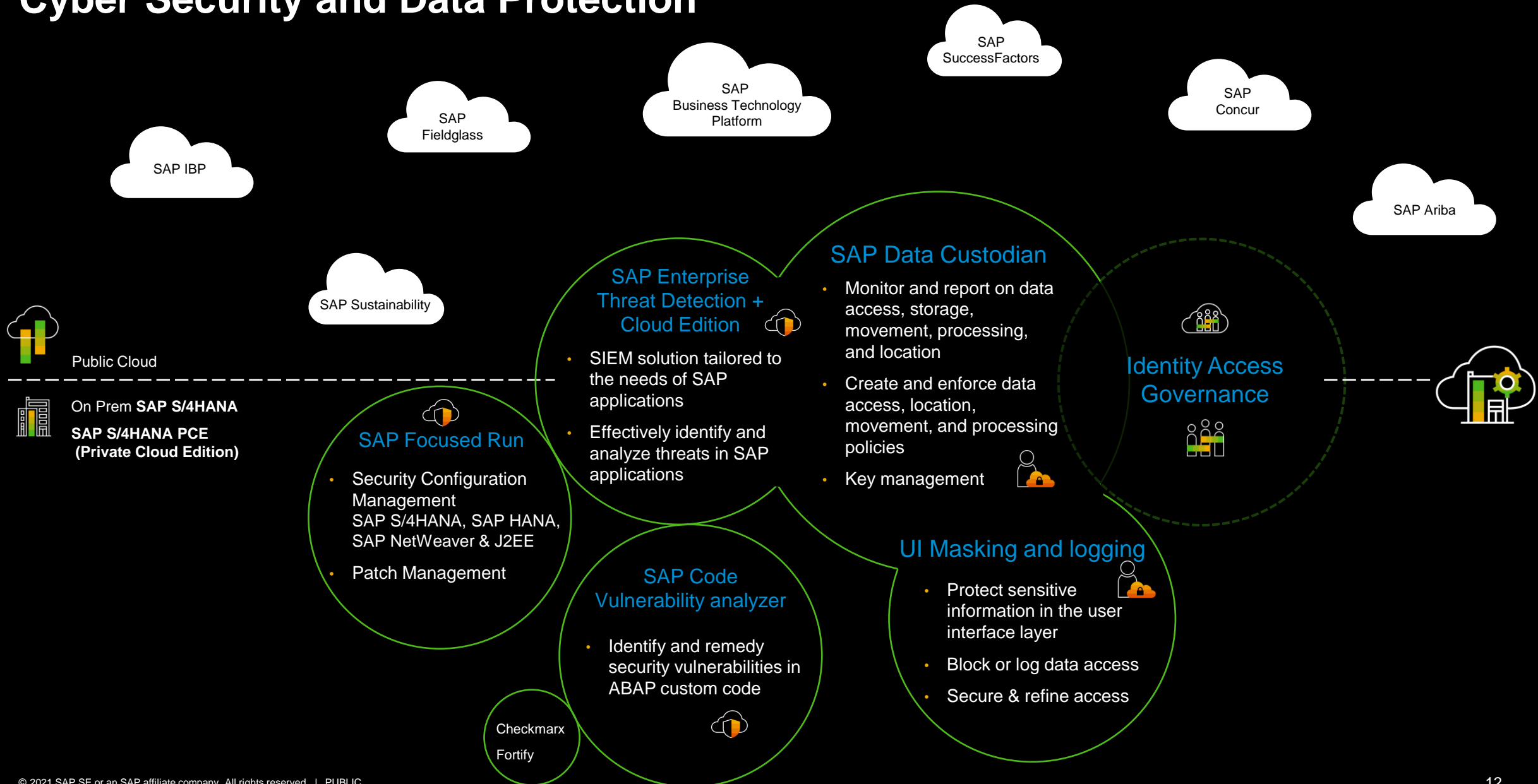
# SAP Depth and Breadth, Supporting the Intelligent Enterprise



# Identity and Access Governance

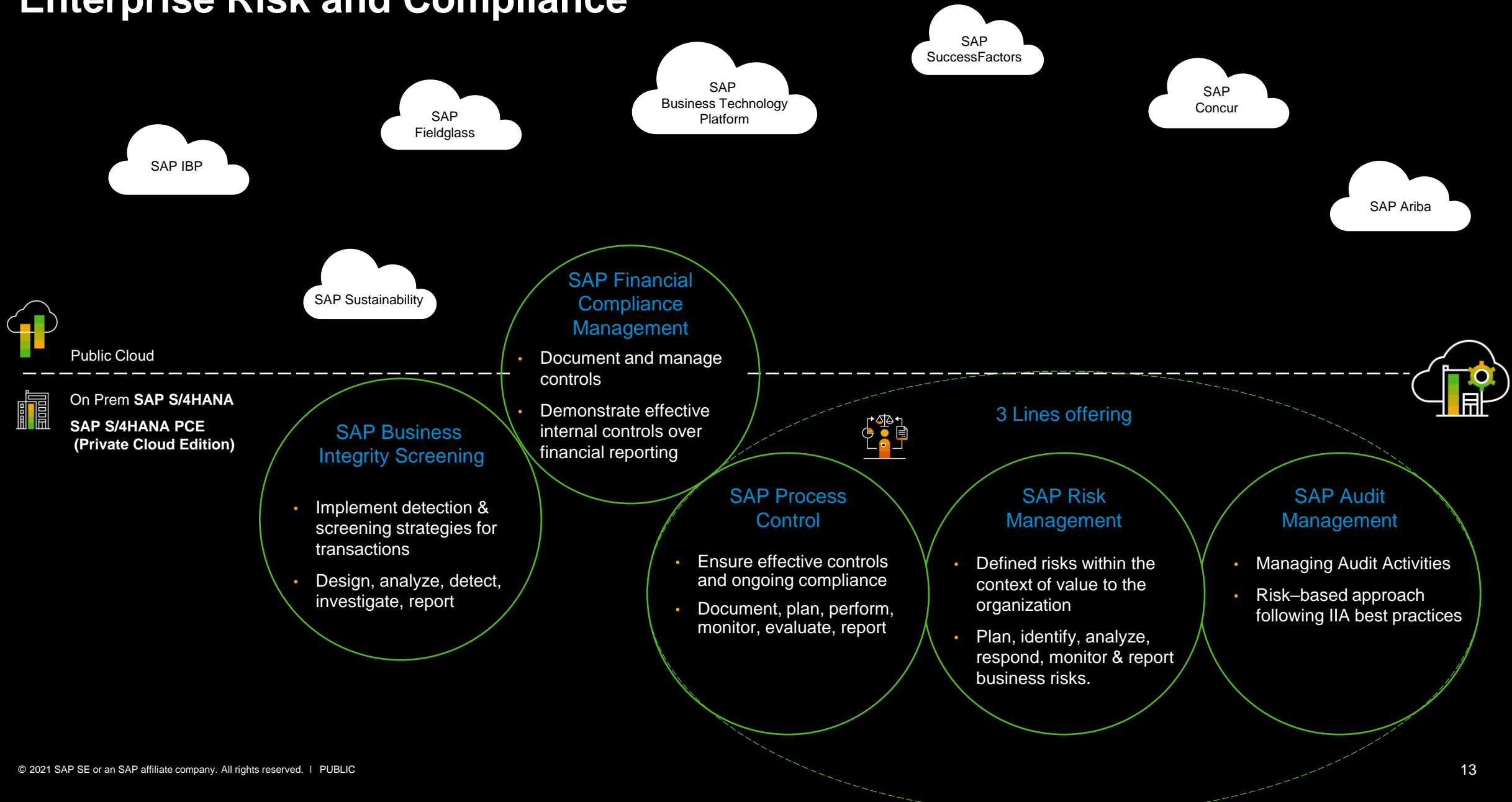


# Cyber Security and Data Protection





# Enterprise Risk and Compliance



# NIST Framework



Identify



Protect



Detect



Respond



Recover

# NIST

**N**ational **I**nstitute of **S**tandards and **T**echnology Cybersecurity Framework

It "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes"

# NIST Framework



## Identify

Asset Management  
Business Environment  
Governance  
Risk Assessment  
Risk Management Strategy  
Supply Chain Risk Management



## Protect

Access Control  
Awareness and Training  
Data Security  
Information  
Maintenance  
Protective Technology



## Detect

Anomalies and Events  
Continuous Security Monitoring  
Detection Processes



## Respond

Response Planning  
Communications  
Analysis  
Mitigation  
Improvements



## Recover

Recovery Planning  
Improvements  
Communications

# Cybersecurity- and Compliance Solutions from SAP based on NIST



## Identify



## Protect



## Detect



## Respond



## Recover

Architecture & Planning services

Empowerment Services

Execution & Implementation Services

Continuous Improvement Services

Security experts

SAP EarlyWatch Alert

SAP Enterprise Threat Detection

Managed Service via ETD

UI data protection masking & logging

SAP Configuration Validation

SAP Business Integrity Screening

SAP System Recommendations

SAP Focused Run

ABAP test cockpit & SAP Code Vulnerability Analyzer

SAP Fortify by Micro Focus

Single Sign-On

User & Identity Management

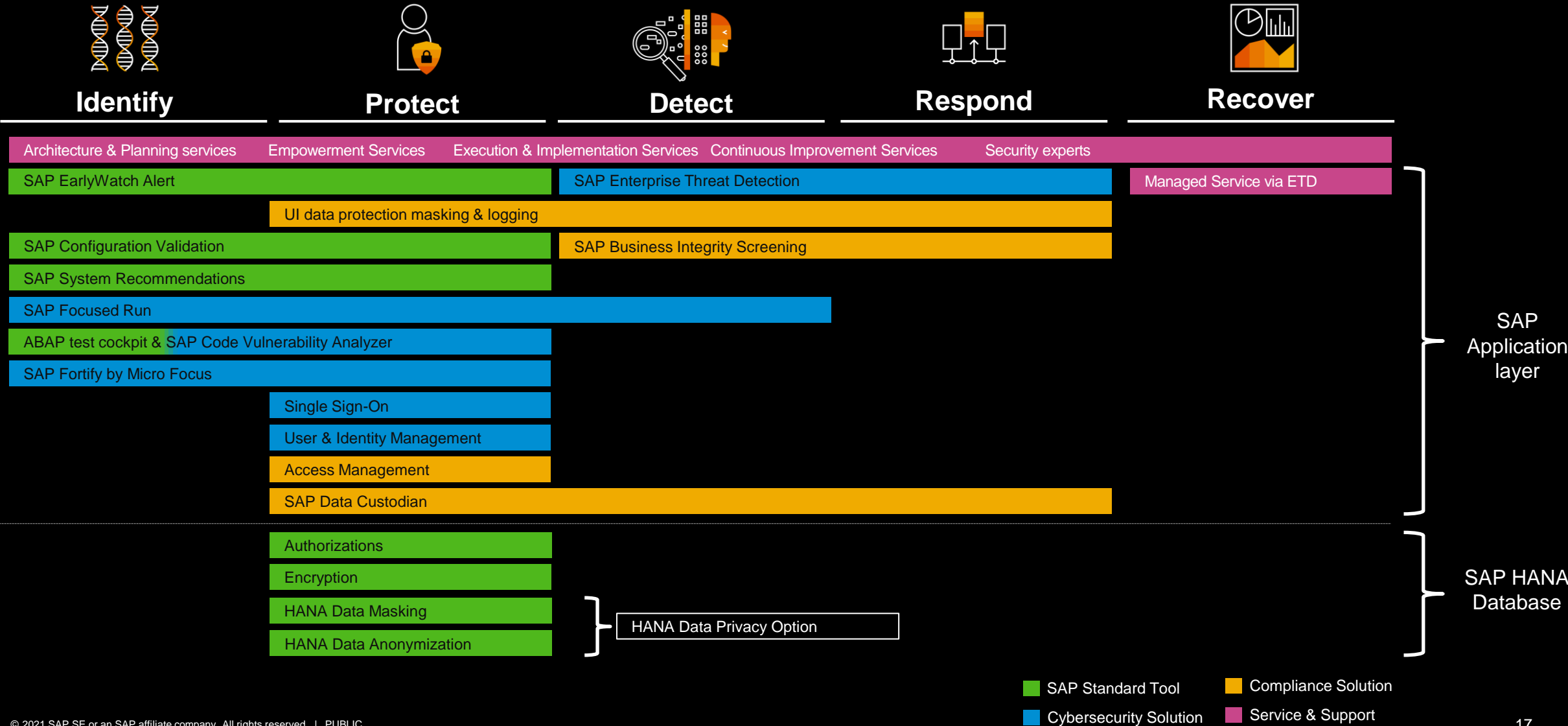
Access Management

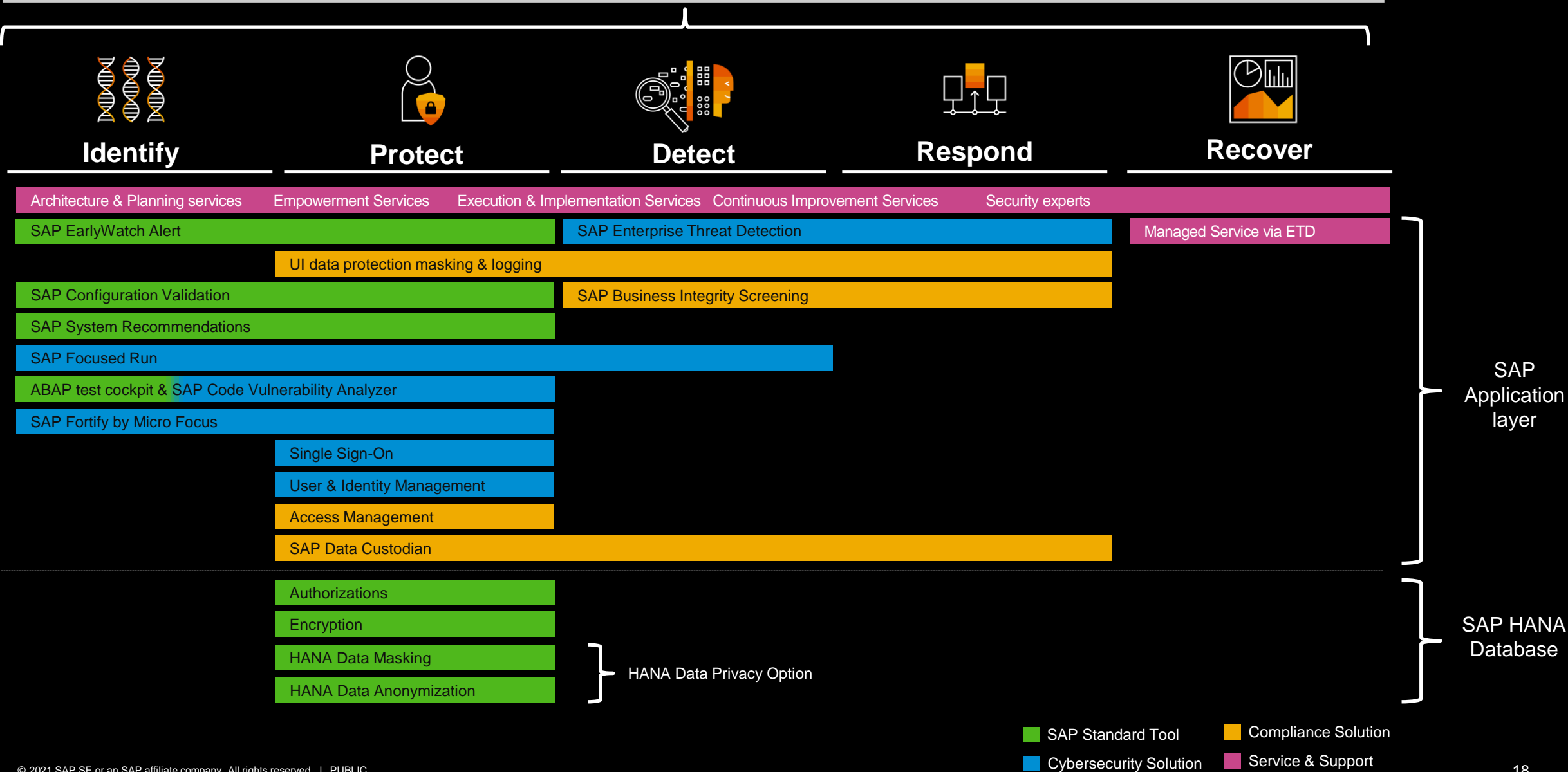
SAP Data Custodian

- SAP Standard Tool
- Cybersecurity Solution
- Compliance Solution
- Service & Support

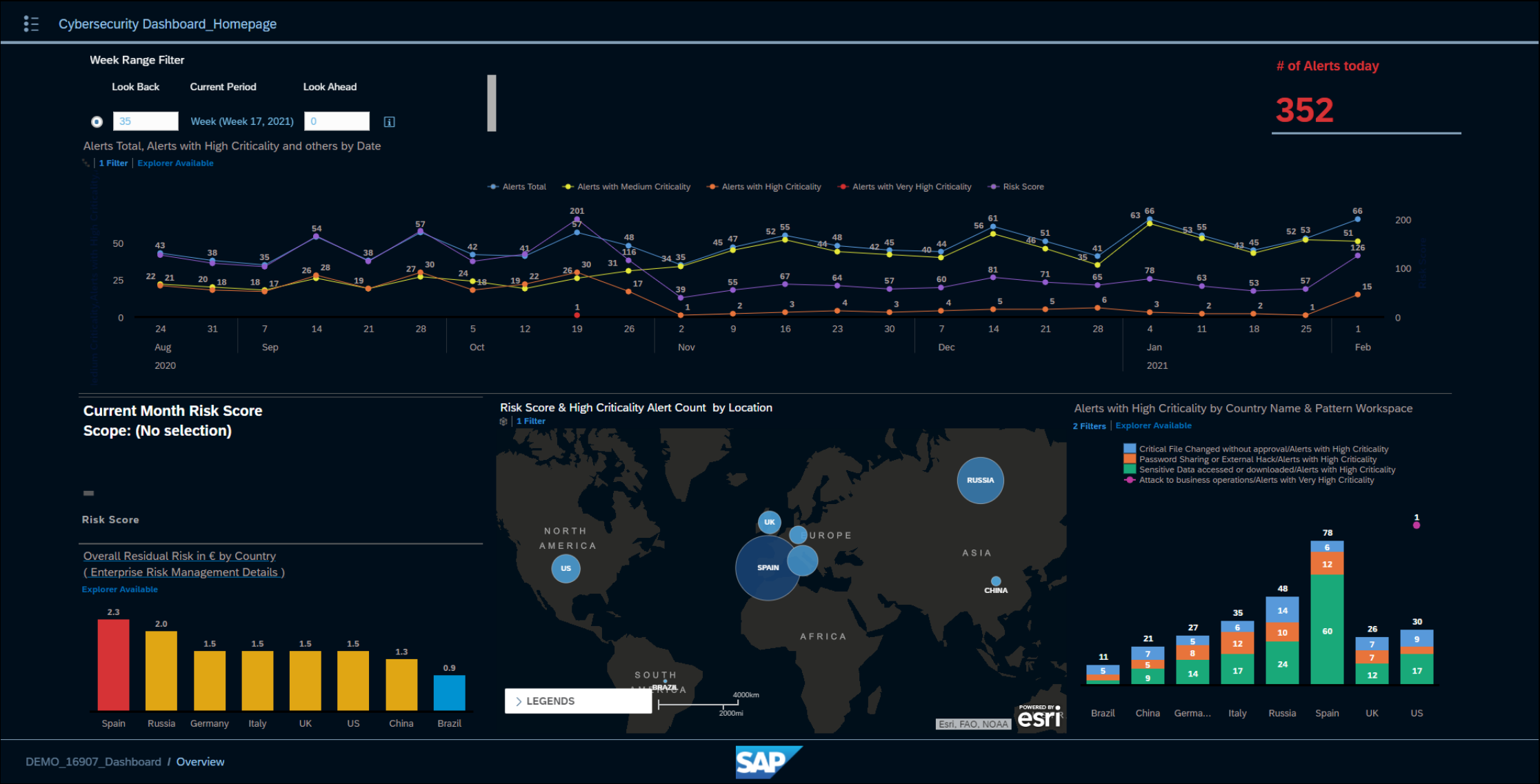


# Cybersecurity- and Compliance Solutions from SAP based on NIST





# SAP Analytics Cloud cyber security dashboard overview



# Cybersecurity- and Compliance Solutions from SAP based on NIST



## Identify



## Protect



## Detect



## Respond



## Recover

Architecture & Planning services

Empowerment Services

Execution & Implementation Services

Continuous Improvement Services

Security experts

**SAP EarlyWatch Alert**

**SAP Enterprise Threat Detection**

**Managed Service via ETD**

UI data protection masking & logging

SAP Configuration Validation

SAP Business Integrity Screening

SAP System Recommendations

SAP Focused Run

ABAP test cockpit & SAP Code Vulnerability Analyzer

SAP Fortify by Micro Focus

Single Sign-On

User & Identity Management

Access Management

SAP Data Custodian

- SAP Standard Tool
- Cybersecurity Solution
- Compliance Solution
- Service & Support

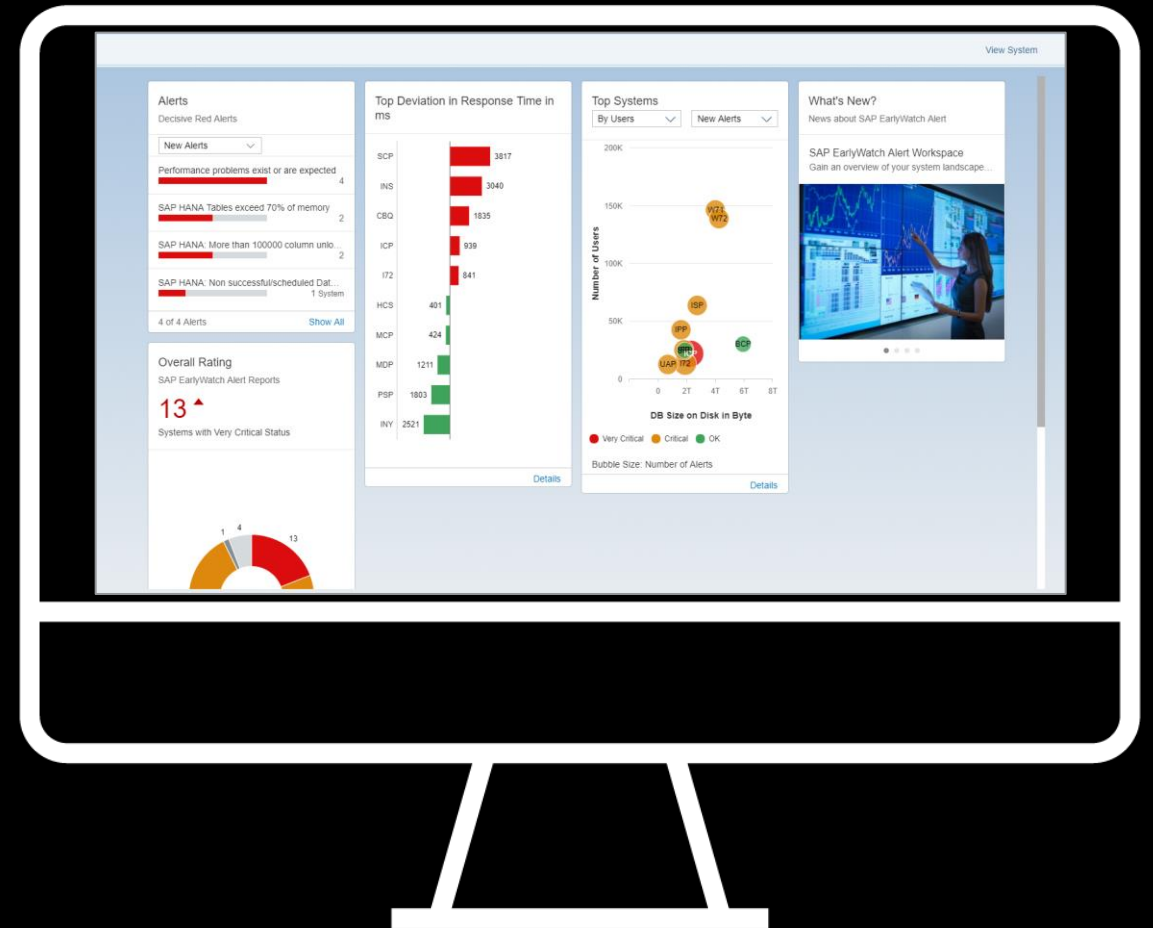


# SAP EarlyWatch Alert Workspace

## Centralized application management

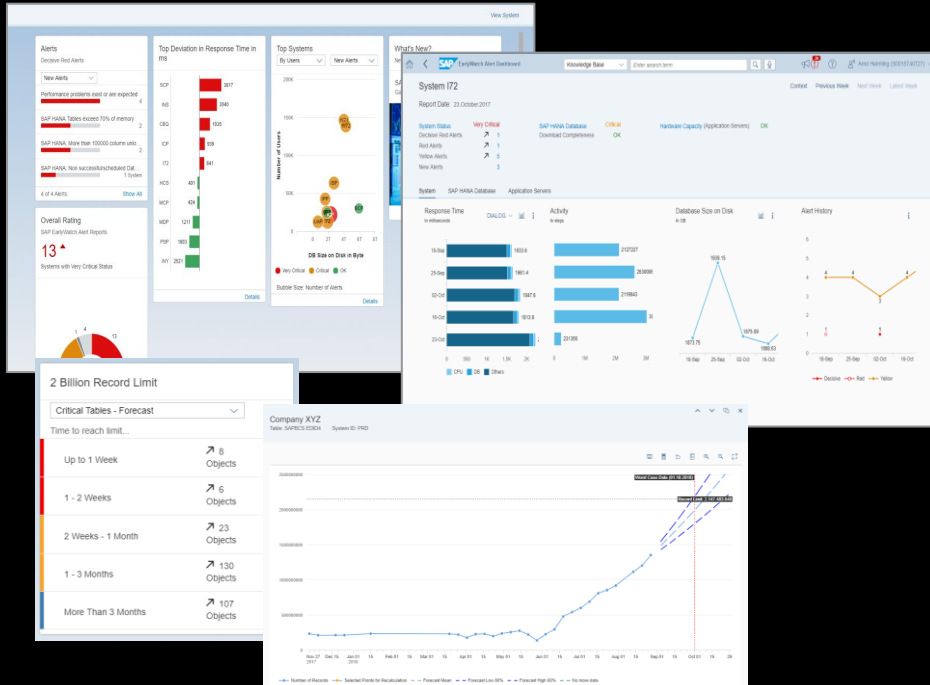
### Gain overview on your system landscape health

- Cost free.
- Shows most critical configuration vulnerability's across prod landscape.
- Prioritized Worklist – share and track progress.
- Accesses the most important systems on a weekly base.
- SAP Governance and Risk Management Team use the Security Card to see what urgently is require.



# SAP EarlyWatch Alert Workspace

SAP Product Excellence Award 2018 – voted by SUGEN customers



- EarlyWatch Alert workspace
- One data lake with 2+ years history of system data
- Designed for Predictive and Preventive service
- Basis for Continuous Quality Checks
- Build for Simplicity with Design Thinking
- Build on SAP Business Technology Platform & SAP HANA
- **Shows critical Security issues across prod landscape**  
(Pre-requisite: S-User Authorization *Display Security Alerts in SAP EarlyWatch Alert Workspace*)
- **Prioritized Worklist – share and track progress. Get Clean!**

**~ 76.400**  
Visits in August 2019

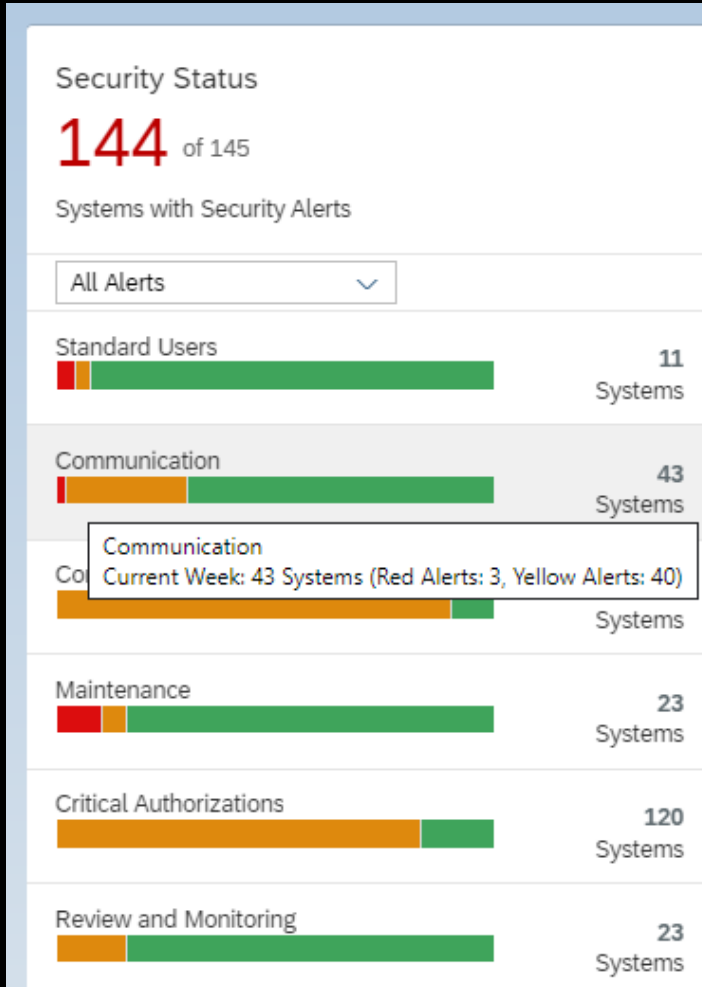
**63,000+**  
Customer systems

**17,000+**  
Systems based on SAP HANA

**~ 1 million**  
SAP HANA objects analyzed  
every week to predicted  
2 billion record limit

# SAP EarlyWatch

## Display Security Alerts in SAP EarlyWatch Alert Workspace



How many systems are vulnerable (“**YELLOW**” or “**RED**”)

- Standard Users including DDIC or SAP\* have default passwords
- **SAP HANA user SYSTEM is active and valid (6 Systems)**
- **RFC Gateway and Message Server Security – Doors wide open (3 Systems)**
- SAP HANA Internal or System Replication Communication is not secured
- Weak Password Policy (ABAP, SAP HANA)
- SAP HANA: SQL Trace configured to display actual data
- **Systems having an old SPS (no longer supported with new SAP Security Notes) (15 Systems)**
- Users having critical basis authorizations like SAP\_ALL, Debug, Display/Change all tables,...
- SAP HANA users having critical authorizations like DATA ADMIN privilege
- Audit Log is not active or written to an unsecure audit trail target

# Cybersecurity- and Compliance Solutions from SAP based on NIST



## Identify



## Protect



## Detect



## Respond



## Recover

Architecture & Planning services

Empowerment Services

Execution & Implementation Services

Continuous Improvement Services

Security experts

SAP EarlyWatch Alert

SAP Enterprise Threat Detection

Managed Service via ETD

UI data protection masking & logging

SAP Configuration Validation

SAP Business Integrity Screening

SAP System Recommendations

**SAP Focused Run**

ABAP test cockpit & SAP Code Vulnerability Analyzer

SAP Fortify by Micro Focus

Single Sign-On

User & Identity Management

Access Management

SAP Data Custodian

- SAP Standard Tool
- Cybersecurity Solution
- Compliance Solution
- Service & Support



# SAP Focused Run

The ultimate solution for Operations

**Addresses advanced customer needs in scalability, data volumes, security, automation, openness, dashboarding & artificial intelligence**

- Manage landscapes with thousands of systems with minimal operations costs
- Monitor real as well as synthetic user requests across systems and technology
- Manage complex landscapes with millions of interface calls and/or message flows
- Efficiently operate thousands of system, user, and integration alerts, including integrated IT infrastructure events
- Enable central governance of software levels and configuration settings
- Deep detailed root cause analysis capabilities tailored to your needs
- Use SAP's out-of-the-box



# Focused Run – Security and Compliance Key Features

**Advanced  
Event & Alert  
Management  
(AEM)**

**Advanced  
System  
Management  
(ASM)**

**Advanced  
User  
Monitoring  
(AUM)**

**Advanced  
Integration  
Monitoring  
(AIM)**

**Advanced  
Configuration  
Monitoring  
(ACM)**

**Advanced  
Root Cause  
Analysis  
(ARA)**

**Advanced  
Analytics &  
Intelligence  
(AAI)**

- Pre defined & policy based security & compliance validation of configurations
- Monitoring of server side certificates
- Security note deployment validation / transparency about gaps vs. achievement
- Integration into operational processes
- Insights into actual usage / system communication & document flow & user behaviour
- Great graphical charts and build in dashboarding incl. Management overview

**Technology Foundation: SAP HANA / SAP NetWeaver ABAP + SAPUI5**

# Cybersecurity- and Compliance Solutions from SAP based on NIST



## Identify



## Protect



## Detect



## Respond



## Recover

Architecture & Planning services

Empowerment Services

Execution & Implementation Services

Continuous Improvement Services

Security experts

SAP EarlyWatch Alert

SAP Enterprise Threat Detection

Managed Service via ETD

UI data protection masking & logging

SAP Configuration Validation

SAP Business Integrity Screening

SAP System Recommendations

SAP Focused Run

ABAP test cockpit & SAP Code Vulnerability Analyzer

SAP Fortify by Micro Focus

Single Sign-On

User & Identity Management

Access Management

SAP Data Custodian

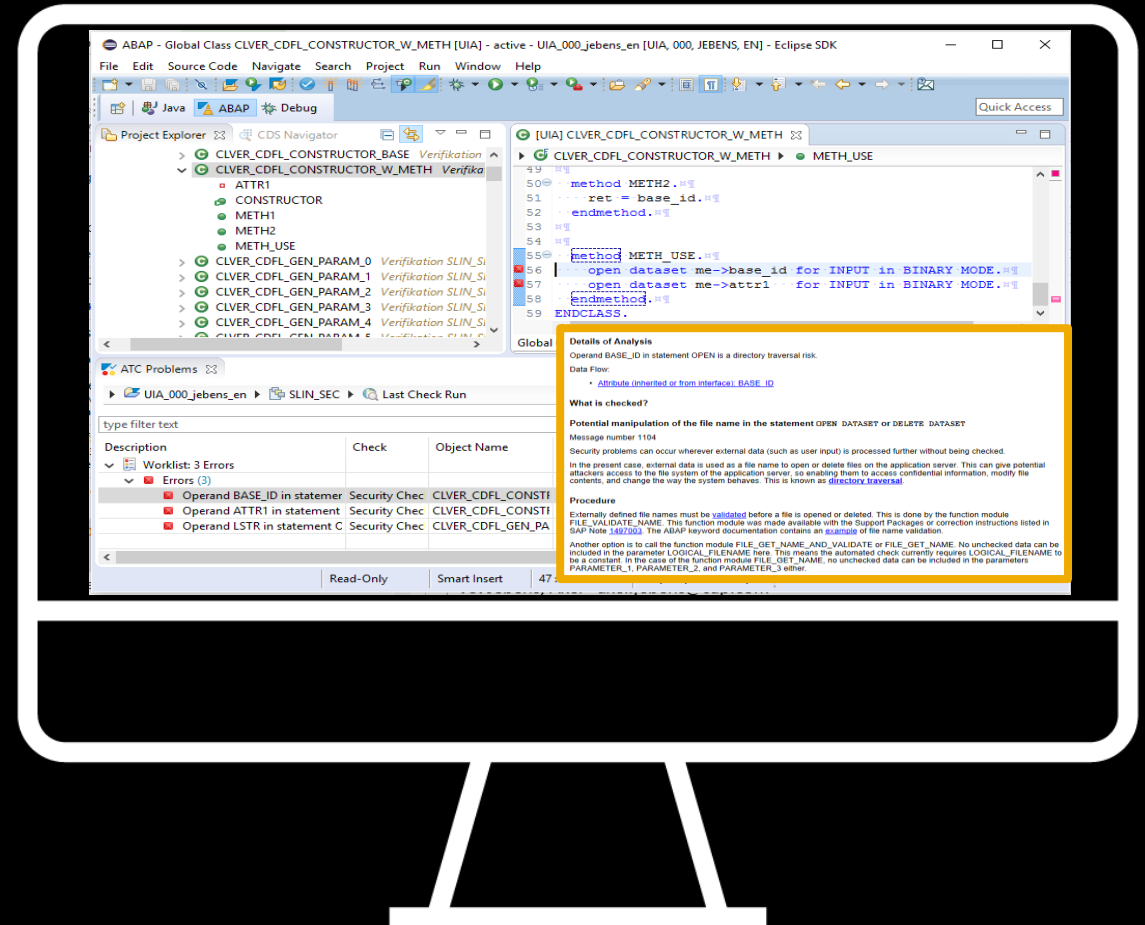
- SAP Standard Tool
- Cybersecurity Solution
- Compliance Solution
- Service & Support

# SAP NetWeaver Application Server, add-on for Code Vulnerability Analysis

## Develop highly secure SAP ABAP applications

### Identify and remedy security vulnerabilities in ABAP custom code

- Tighten application security by scanning custom ABAP code
- Protect against malicious code attacks and data breaches
- Rely on a solution that has been rigorously tested on a massive



# Cybersecurity- and Compliance Solutions from SAP based on NIST



## Identify



## Protect



## Detect



## Respond



## Recover

Architecture & Planning services

Empowerment Services

Execution & Implementation Services

Continuous Improvement Services

Security experts

SAP EarlyWatch Alert

SAP Enterprise Threat Detection

Managed Service via ETD

UI data protection masking & logging

SAP Configuration Validation

SAP Business Integrity Screening

SAP System Recommendations

SAP Focused Run

ABAP test cockpit & SAP Code Vulnerability Analyzer

SAP Fortify by Micro Focus

Single Sign-On

User & Identity Management

Access Management

SAP Data Custodian

- SAP Standard Tool
- Cybersecurity Solution
- Compliance Solution
- Service & Support

# UI Data Security: **Two Step Approach** to Protect Data from Insiders



## UI Masking

**conceal specific data –  
unless required for tasks**

→ make sensitive data  
unavailable for data abuse



“Lock it”...



## UI Logging

**keep data accessible – and create a  
broad + deep log of data access**

- induce compliant behavior
- identify & prove irregular data usage
- baseline for decision on actions



...”or log it!



# Cybersecurity- and Compliance Solutions from SAP based on NIST



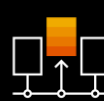
## Identify



## Protect



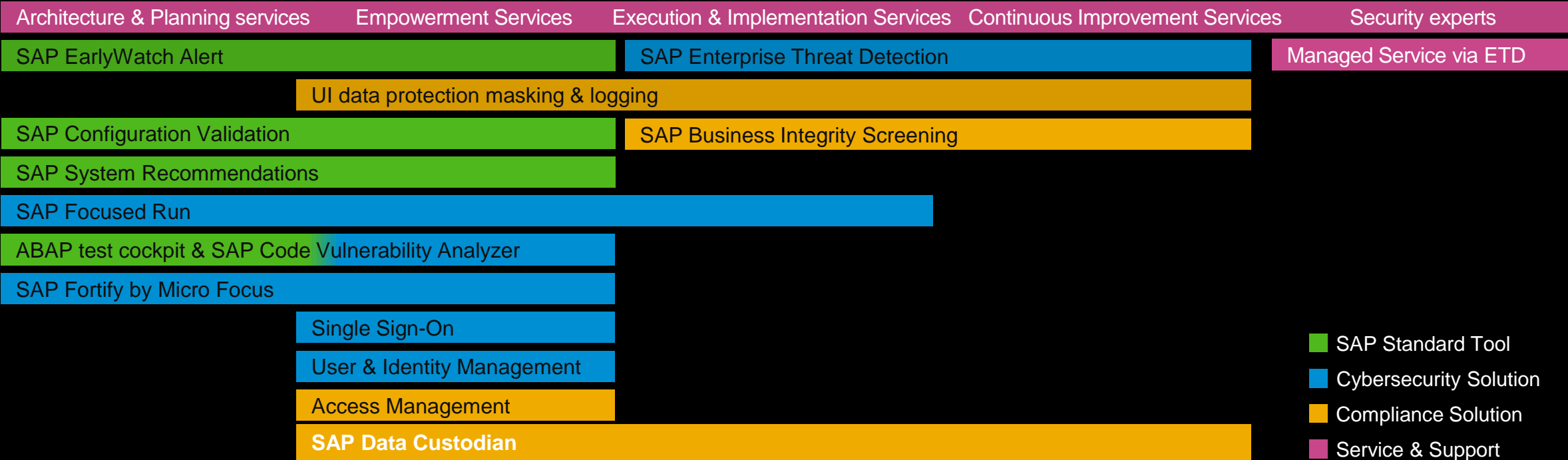
## Detect



## Respond



## Recover



- SAP Standard Tool
- Cybersecurity Solution
- Compliance Solution
- Service & Support

# Challenges In the Multi-Cloud Era

## Data is Everywhere

IaaS | PaaS | SaaS  
Multi-Cloud

Public cloud deployments  
are on the rise

## New Governance Standards

Compliance | Security  
Localization | Audits

Regulatory compliance  
driving data protection

## New Demands

Access | Control  
Geo-Location | Encryption

Shared Responsibility

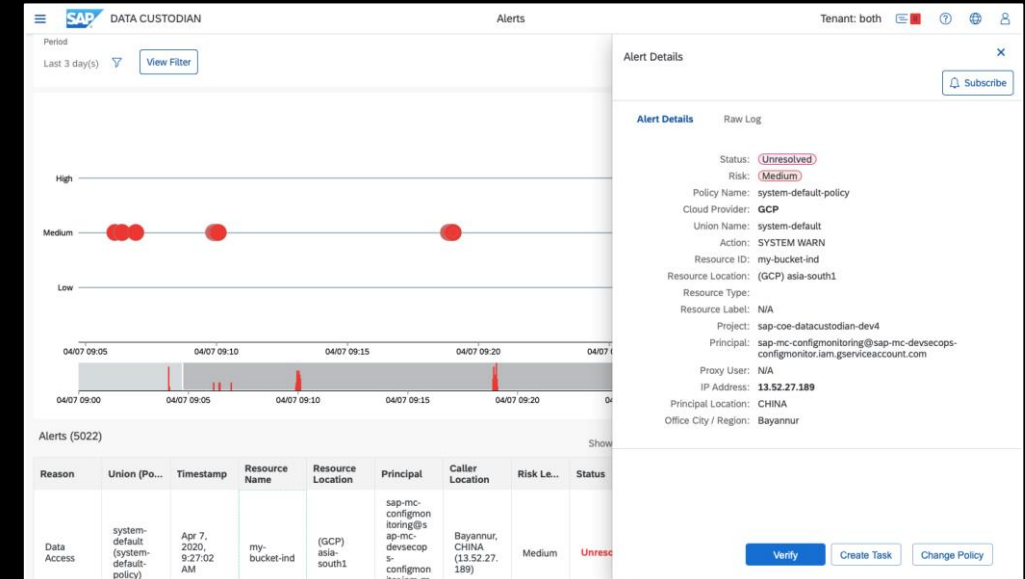
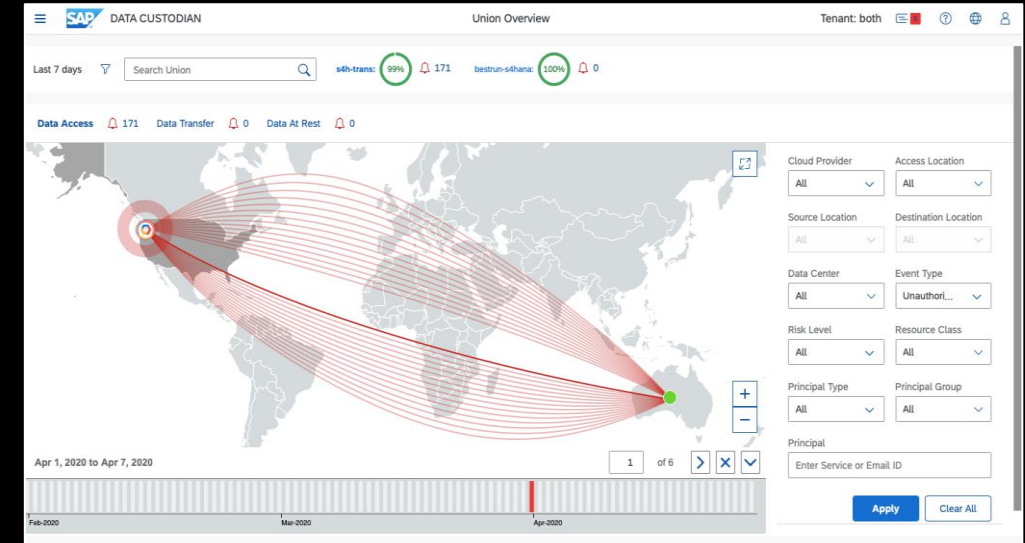


# SAP Data Custodian

## Multi-Cloud Data Insight and Protection

The SAP Data Custodian solution is a Multi-Cloud SaaS application designed to achieve the following business objectives:

- Multi-Cloud and multi-application data insight and protection (Azure, AWS, GCP, AliCloud, S/4H, ECC)
- Data governance, compliance and audit reporting
- Rapid identification and notification of data protection breaches



# Cybersecurity- and Compliance Solutions from SAP based on NIST



## Identify



## Protect



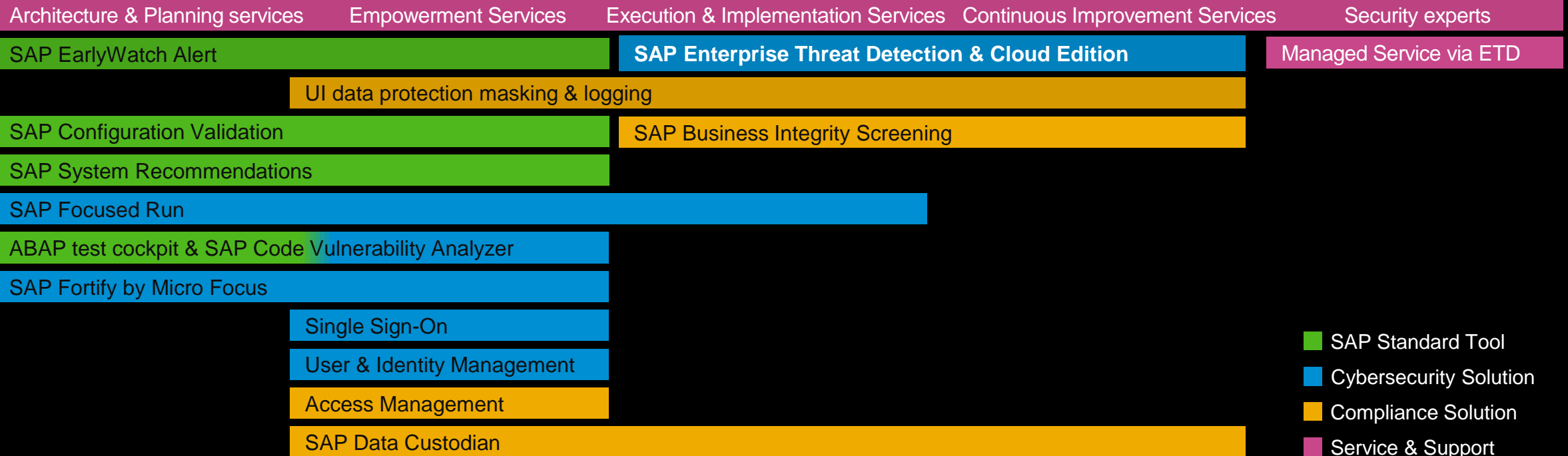
## Detect



## Respond



## Recover



- SAP Standard Tool
- Cybersecurity Solution
- Compliance Solution
- Service & Support



# SAP Enterprise Threat Detection, Cloud Edition



Stop security breaches in today's SAP S/4HANA business applications.

Enterprise Threat Detection gives transparency in to suspicious (user) behavior and anomalies in SAP business applications to identify and stop security breaches in real-time.

Enterprise Threat Detection uses highly efficient and automated processes based on HANA technology and Machine learning to track hacker activity using SAP's predefined and easy customizable attack paths.

## Challenge



- Increasing number of hacker attacks
- Regulatory requirements for security and compliance controls.
- Roles and Authorizations only will not protect an SAP S/4HANA environment.
- Perimeter and IT infrastructure security is not sufficient to protect the SAP S/4HANA business core.
- Analyzing the huge amount of events coming from the SAP S/4HANA Business Applications.

## Solution



- Stop security breaches in today's SAP S/4HANA business applications.
- SAP system Transparency with respect to Security- and Compliance-Events.
- Correlate the complete picture of an hacker attack, not only a few small puzzle pieces.
- Perform forensic investigations, search for threats and detect anomalies in SAP S/4HANA applications.
- All audit logs available in a central instance (manipulation save, unfiltered, normalized, readable).

## Benefits



- **Detect** threats in your SAP S/4HANA applications to avoid financial loss, legal and reputational damage.
- **Safeguard** the operation of your SAP S/4HANA.
- **Reduce** effort for conducting audits.
- **Gain transparency and simplify** the analysis of suspicious activities,
- **Identify security gaps**, and **understand the impact on your business**.
- **Analyze** huge amounts of information quickly and to take the right decision in time.

# Cybersecurity- and Compliance Solutions from SAP based on NIST



## Identify



## Protect



## Detect



## Respond



## Recover

Architecture & Planning services   Empowerment Services   Execution & Implementation Services   Continuous Improvement Services   Security experts

SAP EarlyWatch Alert

SAP Enterprise Threat Detection

Managed Service via ETD

UI data protection masking & logging

SAP Configuration Validation

SAP Business Integrity Screening

SAP System Recommendations

SAP Focused Run

ABAP test cockpit & SAP Code Vulnerability Analyzer

SAP Fortify by Micro Focus

Single Sign-On

User & Identity Management

Access Management

SAP Data Custodian

- SAP Standard Tool
- Cybersecurity Solution
- Compliance Solution
- Service & Support



# SAP Cyber Security MaxAttention Services

## Cybersecurity and compliance engagement

Service portfolio making the design, build and operation of hybrid landscapes work properly



### Strategy and architecture

Develop a strategic road map with respect to security and compliance products from SAP including how to run the hybrid solution in a secure and compliant manner



### Continual improvement

Develop a security and compliance improvement road map, safeguard the security aspect of project implementation, and develop a customer-specific security baseline



### Transparency and mitigation

Ensure regular updates and customer-specific content to enable and improve the core competence in how to design, build, and run a hybrid SAP landscape in a secure and compliant manner

# Key Takeaways

1. SAP systems or applications can be affected by hacker attacks
2. SAP can provide a structured approach to customers and partners covering the SAP related disciplines
3. SAP provides solutions and services to support organizations protection their SAP environment
4. Useful links:
  - a. <https://www.sap.com/about/trust-center.html>
  - b. <https://support.sap.com/en/offerings-programs/support-services/security-optimization-services-portfolio.html>

# Thank you.

Contact information:

**Arndt Lingscheid**

Solution owner GRC & Cyber Security

E-Mail: [a.Lingscheid@sap.com](mailto:a.Lingscheid@sap.com)

Mobile: +49 160 90 84 11 88

SAP SE Dietmar-Hopp-Allee 16, 69190 Walldorf, Germany

Follow us



[www.sap.com/contactsap](http://www.sap.com/contactsap)

© 2021 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/copyright](http://www.sap.com/copyright) for additional trademark information and notices.



# SAP Premium Engagement Session - Cybersecurity

Natascha Lalor, SAP  
September, 2021

PUBLIC

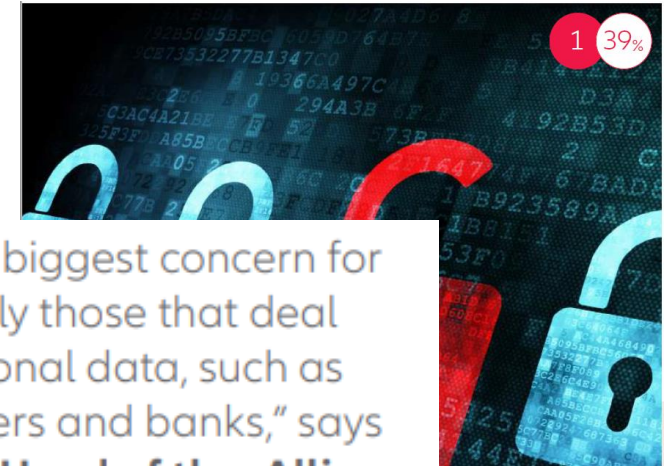


# Allianz Risk Barometer 2021 – published January 2021

## DATA BREACHES AND RANSOMWARE BIGGEST THREATS

According to **Allianz Risk Barometer** respondents, data breaches rank as the cyber exposure companies are most concerned about over the next year, followed by IT vulnerability due to increased remote working and ransomware attacks, which have been increasing in both number and severity. Data breaches already rank as the top cause of cyber incidents for businesses, followed by external events such as ransomware attacks, while employee errors ranks third, reflecting the fact that mistakes and technical problems are the most frequent generator of cyber insurance claims by number, according to AGCS analysis.

“Data breaches remain the biggest concern for most companies, particularly those that deal with large amounts of personal data, such as retailers, healthcare providers and banks,” says **Catharina Richter, Global Head of the Allianz Cyber Center of Competence**, which is embedded into AGCS. “However, ransomware attacks are an ongoing threat for an increasing number of industries, such as manufacturing and service sectors, and can be a cause of significant business interruption. Ransomware incidents and privacy cases will remain prevalent issues for companies in 2021. Attackers continue to innovate while regulatory enforcement and fines for data breaches continue their upwards trend. New cyber loss scenarios are constantly emerging.”

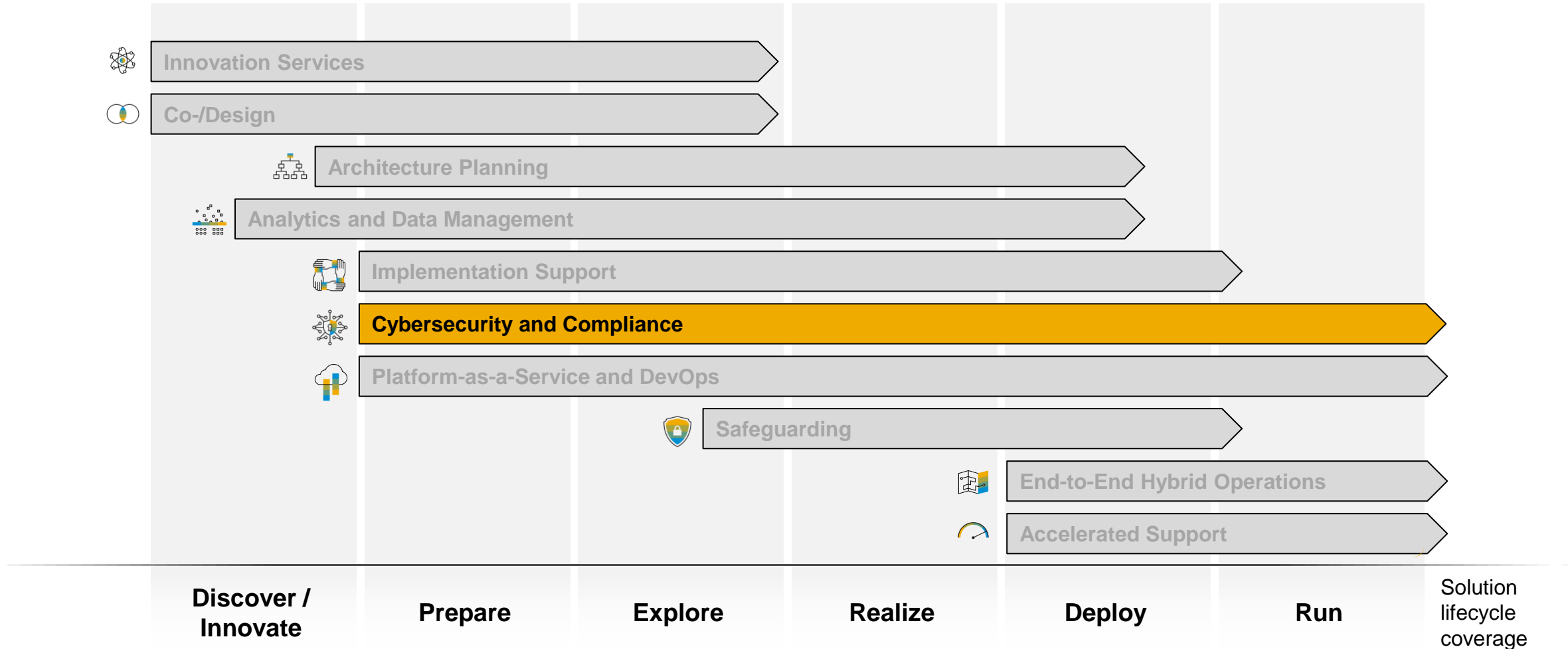


<https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html>



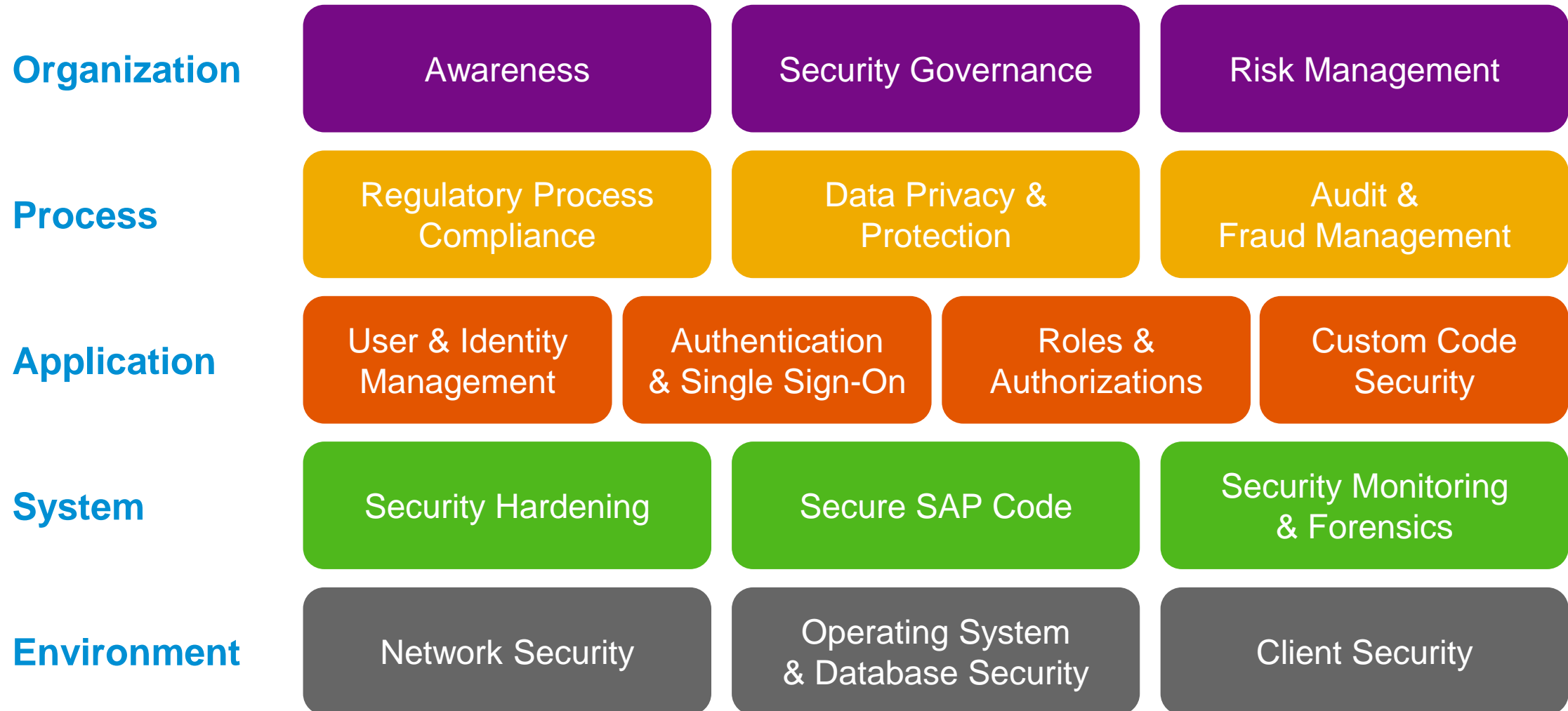
# New focus on innovative edge technologies, design, and architecture

Extended portfolio of the new SAP MaxAttention



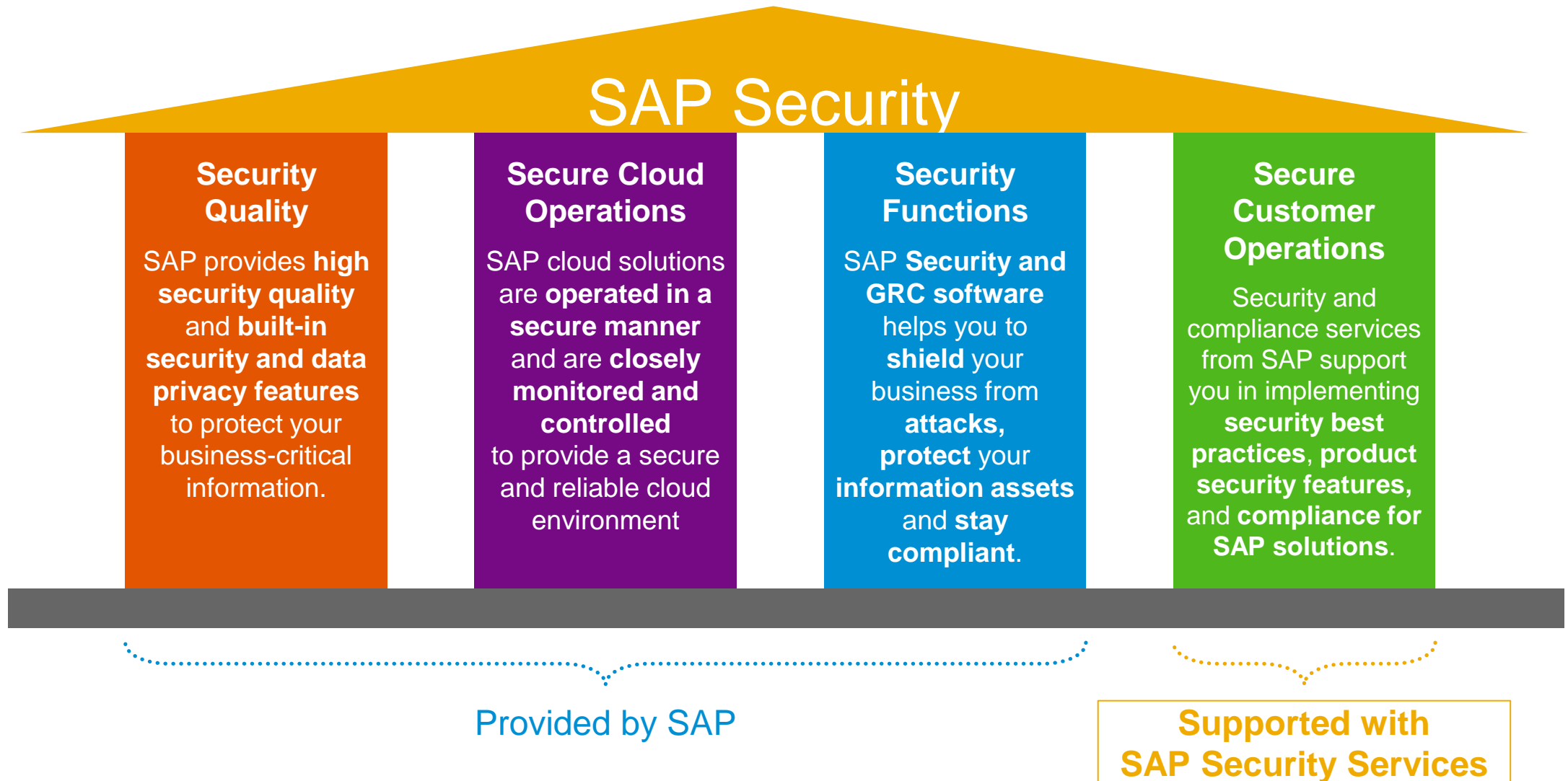
# Cybersecurity und Compliance Topic Areas

## The **Secure Operations Map**



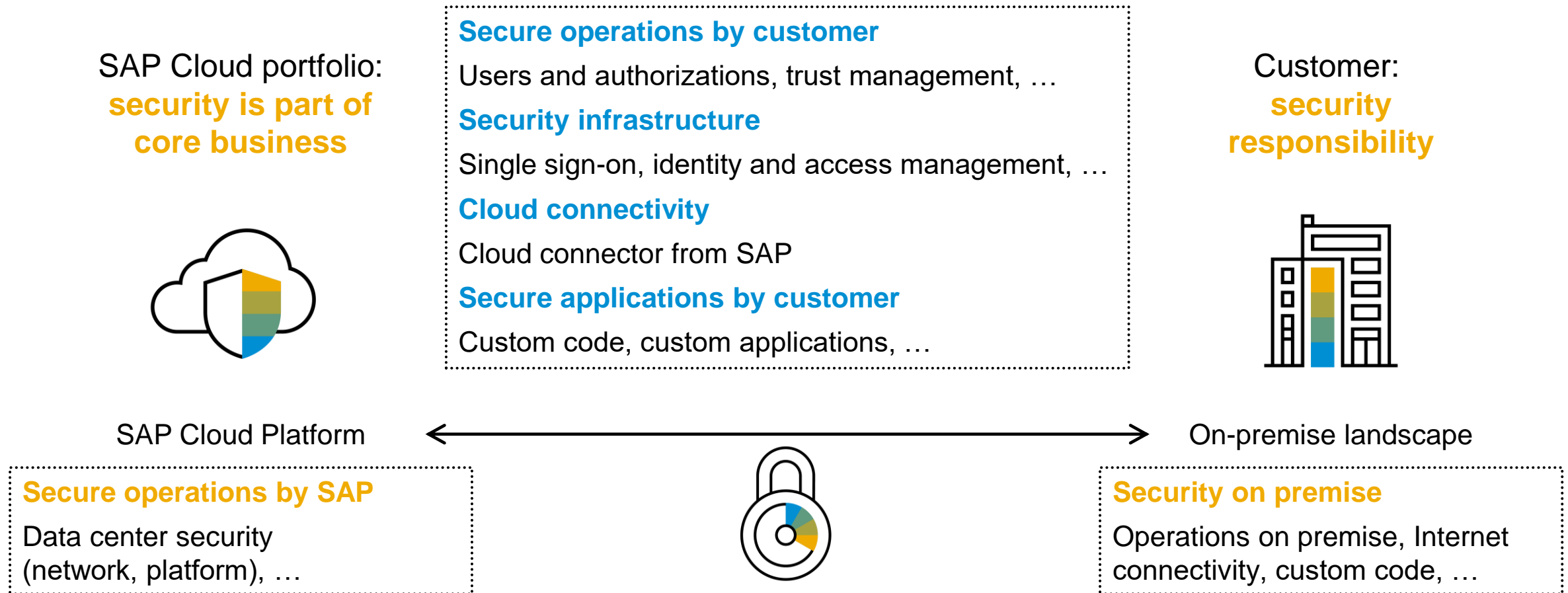
# Why Security Services?

## The Pillars of SAP System Landscape Security



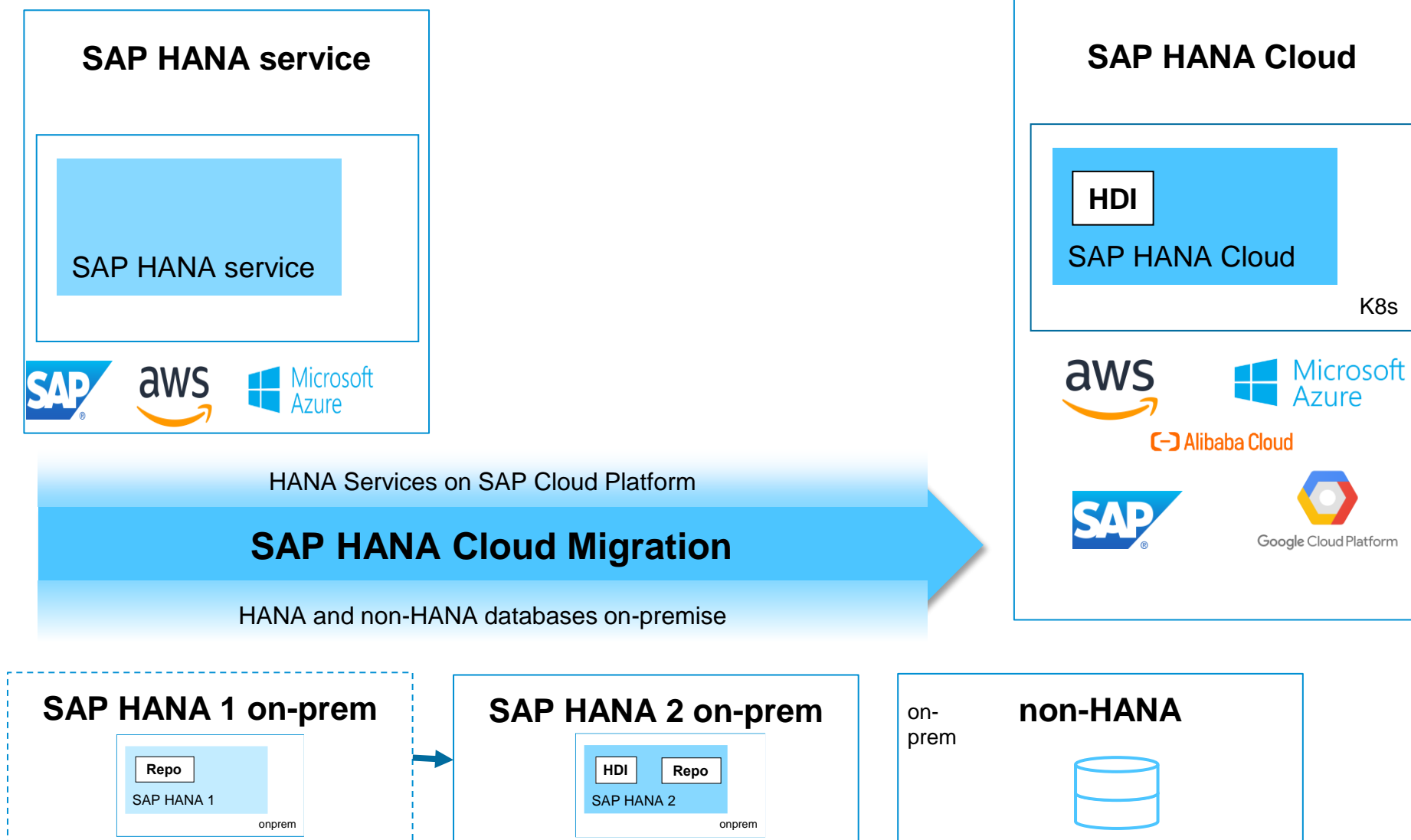
# What to consider for **cybersecurity in hybrid SAP landscapes**

Example: SAP Cloud Platform



# SAP HANA Cloud | Migration scenarios to SAP HANA Cloud

## Overview

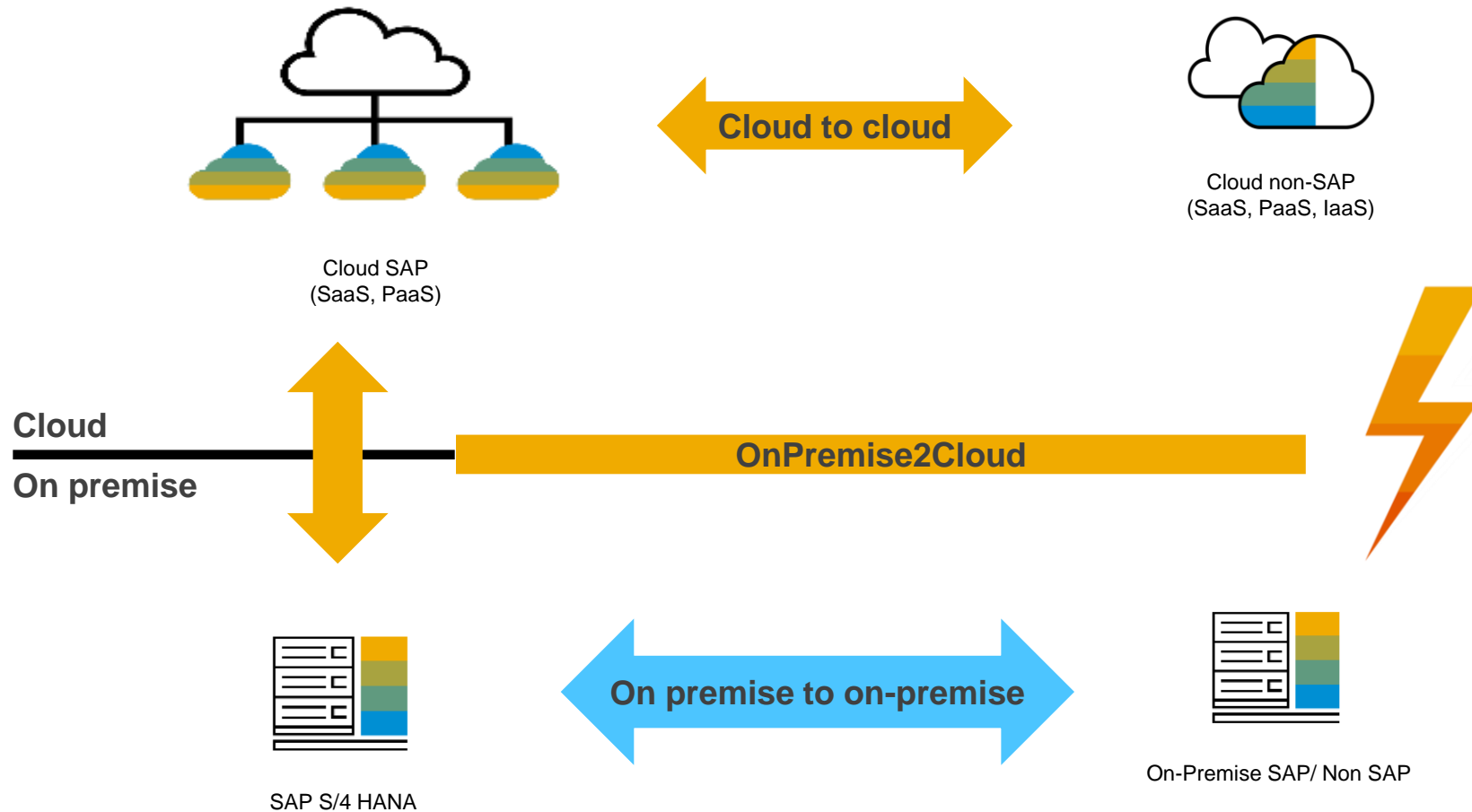


## Security relevant topics

- Identity Access Management Architecture Design
- Authentication and SSO Architecture Design
- SIEM and Monitoring Strategy
- Secure Web Access
- User Authorization
- ...

# Architecture for security and compliance

## Example 2: Move from on-premise to a hybrid landscape



### Security relevant topics

- Consistent user authorization
- Single sign-on, identity and access management
- Custom code and applications (both Cloud and On-Premise)
- Secure system communication
- Secure interfaces between Cloud and On-Premise
- Configuration and security monitoring
- ...

# Global data protection regulations are expanding

Data protection regulations vary globally and are extending their reach

Country	Regulations
USA	USA Patriot Act, Stored Communications Act, EU-US Privacy Shield, California Consumer Privacy Act
European Union	EU Data Protection Directive replaced in 2018 by the EU General Data Protection Regulation (GDPR) – privacy laws in 28 countries
Germany	Federal Data Protection Act (FDPA)
Brazil	General Data Protection Law (LGPD) – 2020
Australia	Privacy Act 1988, Australian state and territory legislation
Singapore	The Personal Data Protection Act (PDPA)
Canada	Personal Information Protection Act (PIPA), Personal Information Protection and Electronic Documents Act (PIPEDA), Freedom of Information and Protection of Privacy Act (FIPPA)
Russia	Federal Law No. 152-FZ on Personal Data





# Global data protection

## DPP requirements at a glance



### Audit & Documentation

#### Blocking & deletion



#### Processing purpose



#### Access restrictions



#### Data Subject Request



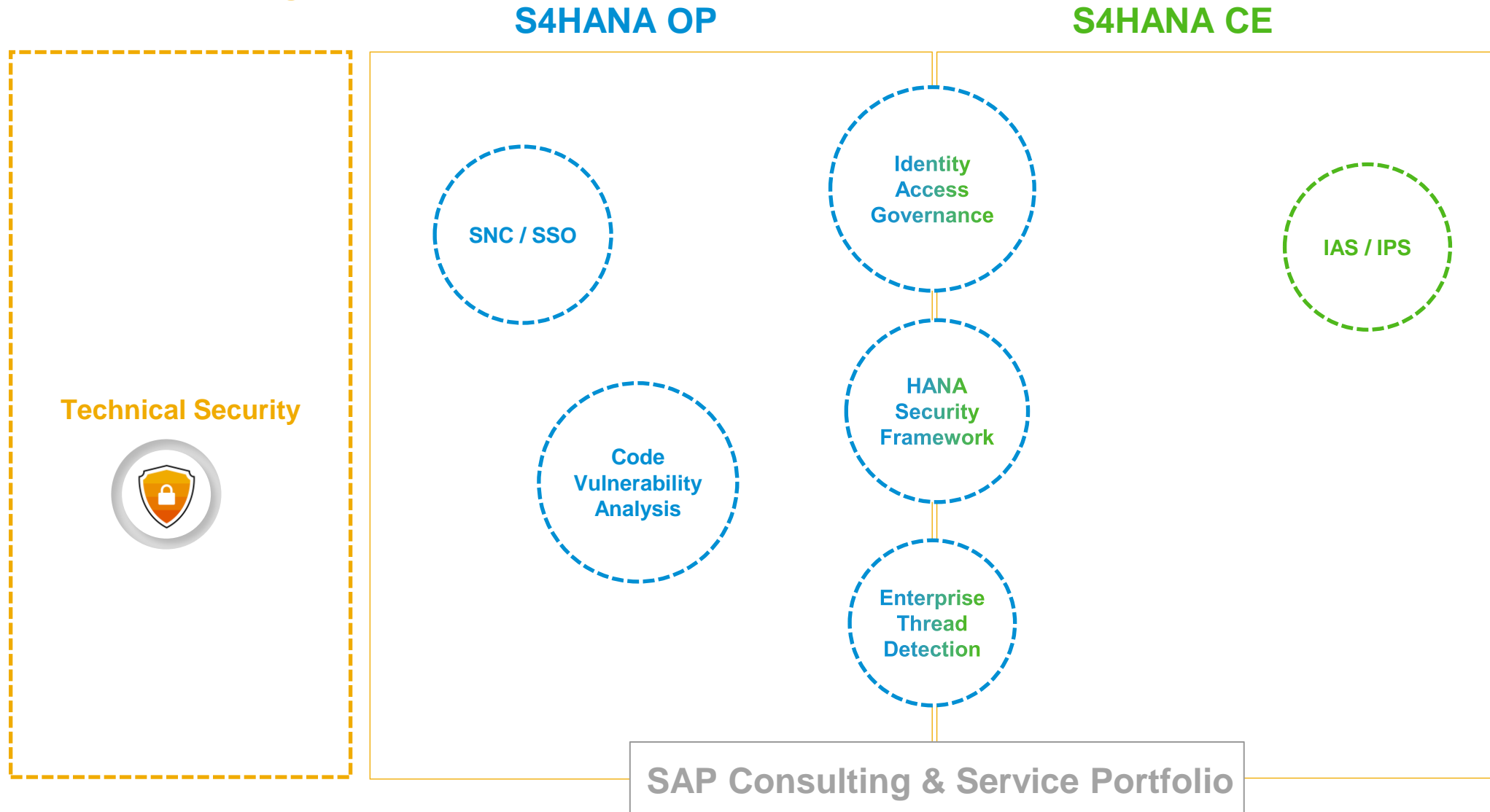
#### Transparency & Correctness



### Technical Security

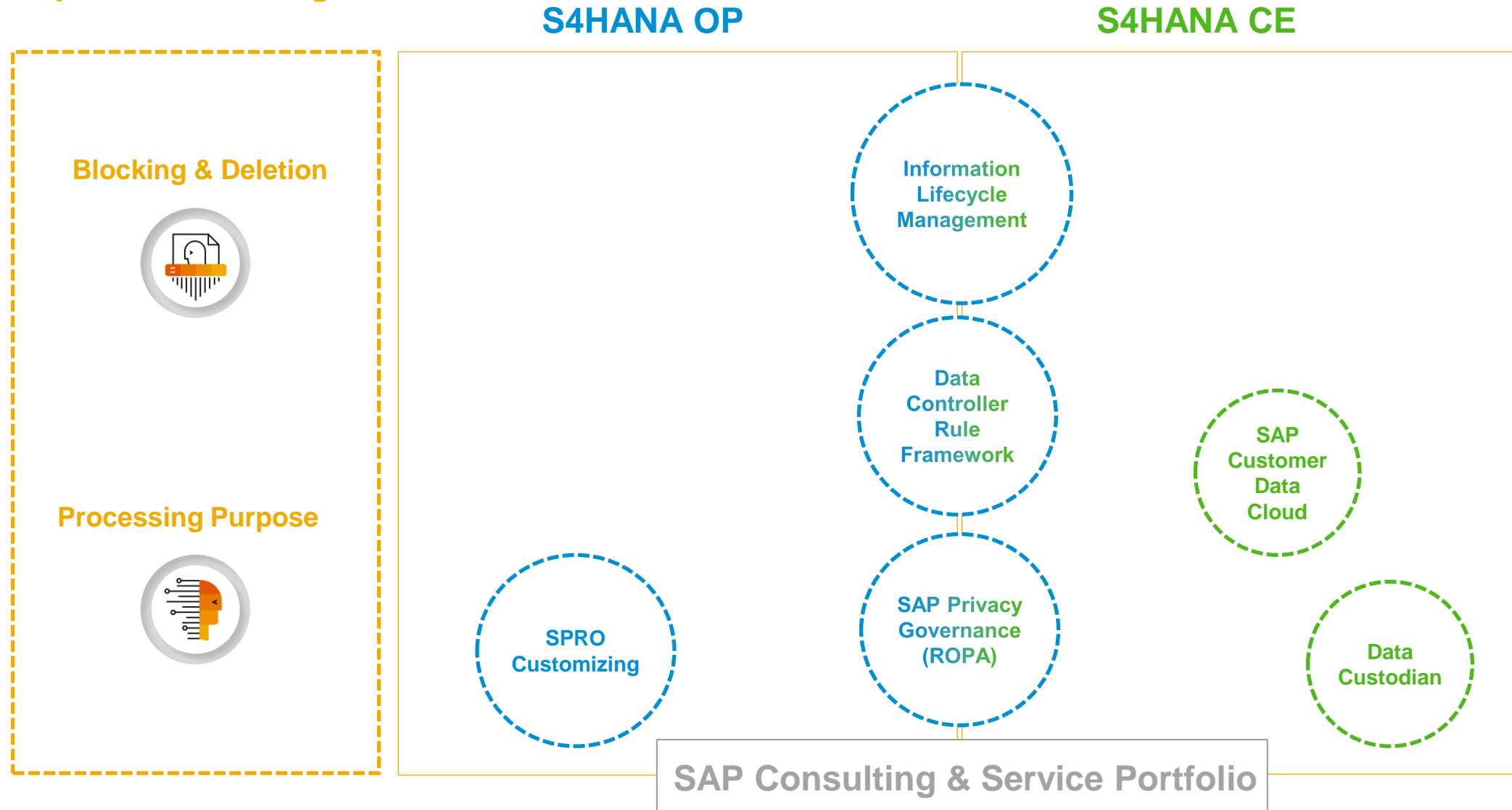
# Global data protection

## DPP requirements at a glance



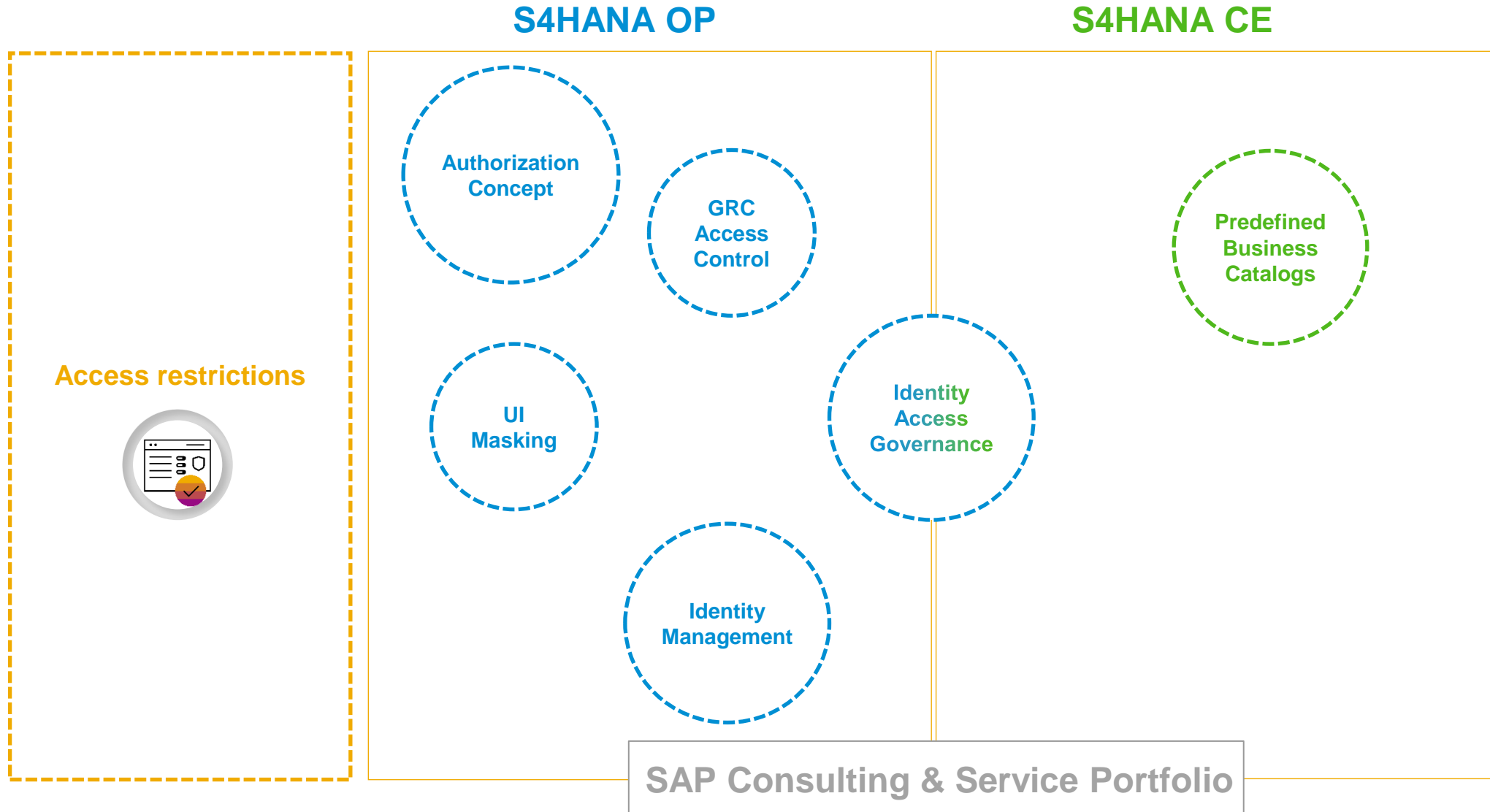
# Global data protection

## DPP requirements at a glance



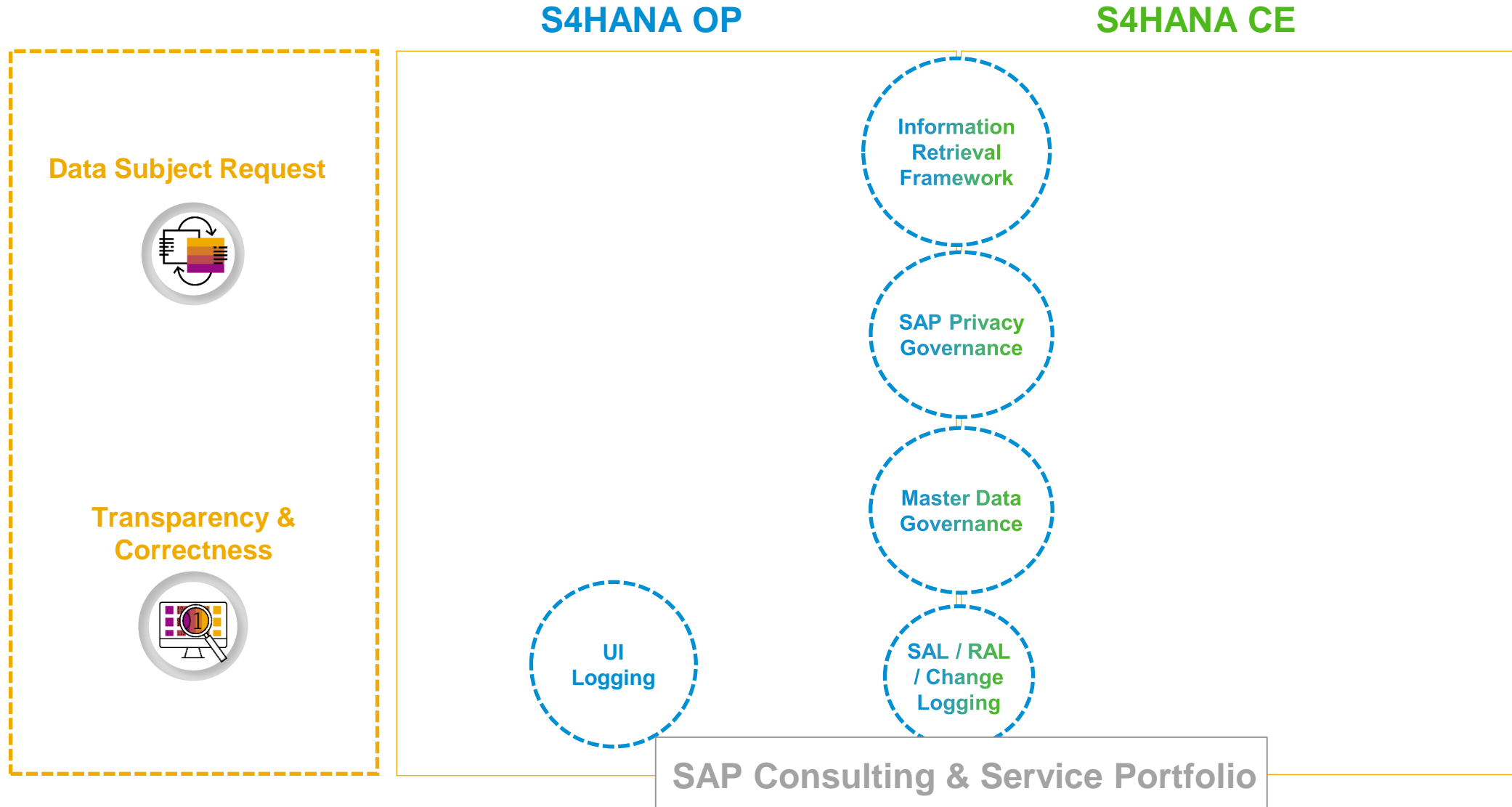
# Global data protection

## DPP requirements at a glance



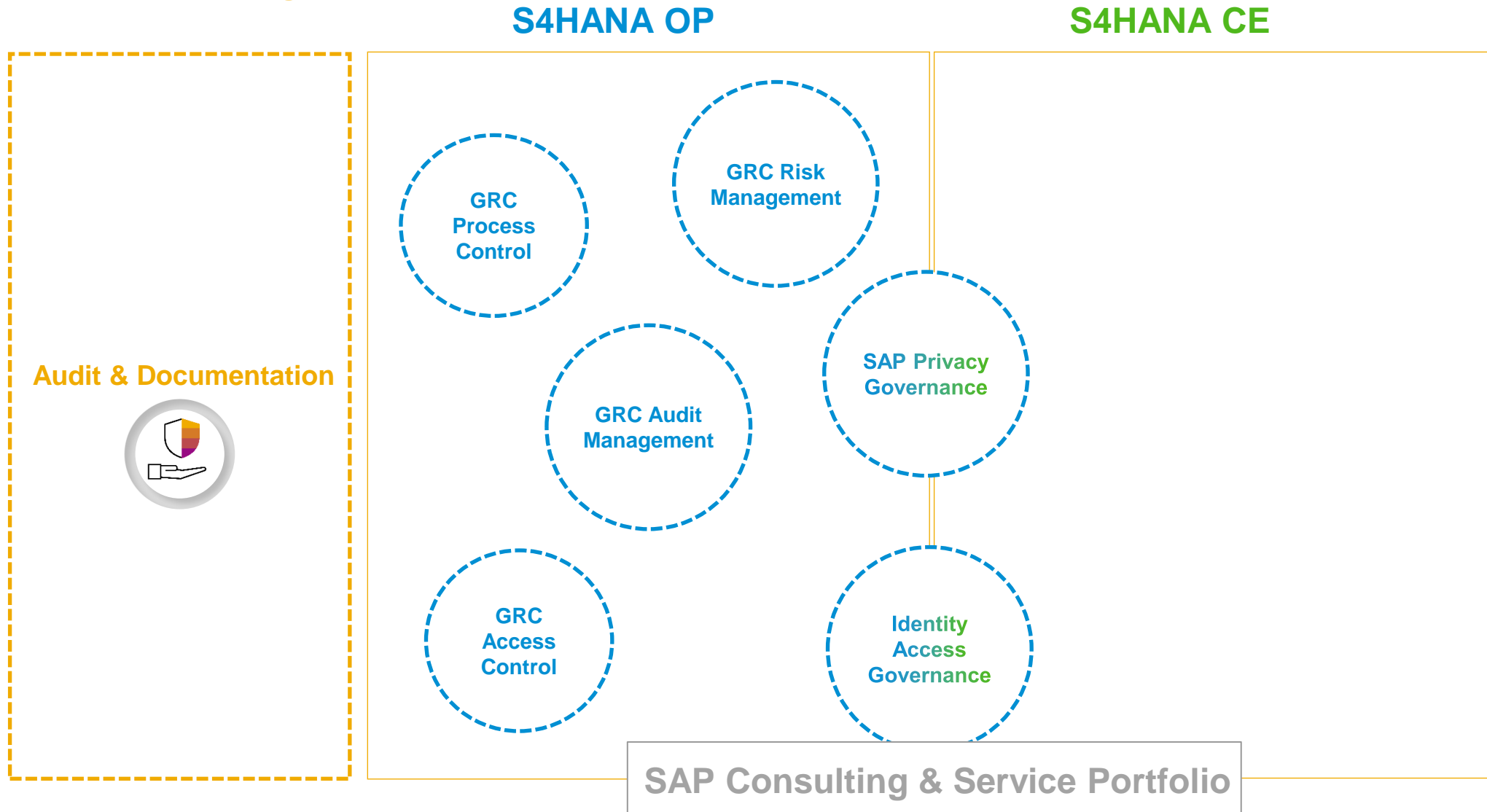
# Global data protection

## DPP requirements at a glance



# Global data protection

## DPP requirements at a glance



# Cybersecurity and Compliance

Engagement level	Level 3		
	Level 2		
Focus topic	Level 1		
Cybersecurity and Compliance	Transparency for security and compliance	Engineering for security and compliance	Architecture for security and compliance
<b>Mission</b>	<ul style="list-style-type: none"> <li>Identify critical gaps and areas for optimization enabling improvements in key competencies</li> </ul>	<ul style="list-style-type: none"> <li>Provide detailed technical analysis of SAP security and compliance requirements</li> </ul>	<ul style="list-style-type: none"> <li>Provide technical architecture review and support development of a strategic road map with respect to SAP security and compliance solutions.</li> </ul>
<b>Outcome and benefits</b>	<ul style="list-style-type: none"> <li>Improved core competence of the customer in how to design, build, and run a hybrid SAP landscape in a secure and compliant manner</li> <li>Discovery of critical gaps</li> <li>Transparency of optimization potential for important security and compliance requirements</li> </ul>	<ul style="list-style-type: none"> <li>Security and compliance improvement road map based on the results of the transparency and mitigation service</li> <li>Customer-specific security standards and procedures</li> </ul>	<ul style="list-style-type: none"> <li>Designed and reviewed technical architecture related to SAP security products and SAP solutions.</li> <li>Nonproductive prototyping utilizing an agile approach to accelerate implementation and deployment of the road map</li> </ul>
<b>Services</b>	<ul style="list-style-type: none"> <li>Transparency and mitigation</li> </ul>	<ul style="list-style-type: none"> <li>+ Continual improvement</li> </ul>	<ul style="list-style-type: none"> <li>+ Strategy and architecture</li> </ul>



# Service Flow Cybersecurity & Compliance

Improvement Analysis and Roadmap Services (IAR)

Technical Security Check

Security Discovery

## Security Engagement

Level 3: Architecture – Architecting for security and compliance

Level 2: Engineering – Improvement for security and compliance

Level 1: Transparency – Empowerment for security and compliance

Security & Compliance Workshop

Contact & Touch Points

Impact Verification

Module FA08  
“Cybersecurity & Compliance”

Architecture Point of View  
Architecture Spotlight

## Deep Dive Packages

Patch Mgmt

Platform Security

DPP (GDPR)

Secure Custom Code

Security Package Catalog

from Catalog



Immediate Action

Level 1: Transparency – Support for security and compliance

Level 2: Engineering – Optimization for security and compliance

Level 3: Architecture – Advisory for security and compliance

# Service Flow Cybersecurity & Compliance

Improvement Analysis and Roadmap Services (IAR)

Technical Security Check

Security Discovery

## Security Engagement

Level 3: Architecture – Architecting for security and compliance

Level 2: Engineering – Improvement for security and compliance

Level 1: Transparency – Empowerment for security and compliance

Security & Compliance Workshop

Contact & Touch Points

Impact Verification

Updated content for BTP Neo  
Added coverage for BTP CF

Module FA08  
“Cybersecurity & Compliance”

Architecture Point of View  
Architecture Spotlight

## Deep Dive Packages

Patch Mgmt

Platform Security

DPP (GDPR)

Secure Custom Code

Added deep dive packages for BTP topics and services of main interest

from Catalog



Immediate Action

Level 1: Transparency – Support for security and compliance

Level 2: Engineering – Optimization for security and compliance

Level 3: Architecture – Advisory for security and compliance

# Service Flow Cybersecurity & Compliance – Content Developed for BTP

Improvement Analysis and Roadmap Services (IAR)

Technical Security Check

Security Discovery

## Security Engagement

Level 3: Architecture – Architecting for security and compliance

Level 2: Engineering – Improvement for security and compliance

Level 1: Transparency – Empowerment for security and compliance

Security & Compliance W

BTP Neo Security  
BTP CF Security  
BTP Feature Set B

Contact &  
Touch Points

Impact  
Verification

Module FA08  
“Cybersecurity &  
Compliance”

Architecture Point of View  
Architecture Spotlight

Immediate Action

## Deep Dive Packages

Identity  
Authentication  
Service

Identity  
Provisioning  
Service

BTP  
Administration  
& Operation

Cloud  
Connector  
Security

BTP  
Authentication  
& SSO

from  
Catalog

Security Package  
Catalog



Level 1: Transparency – Support for security and compliance

Level 2: Engineering – Optimization for security and compliance

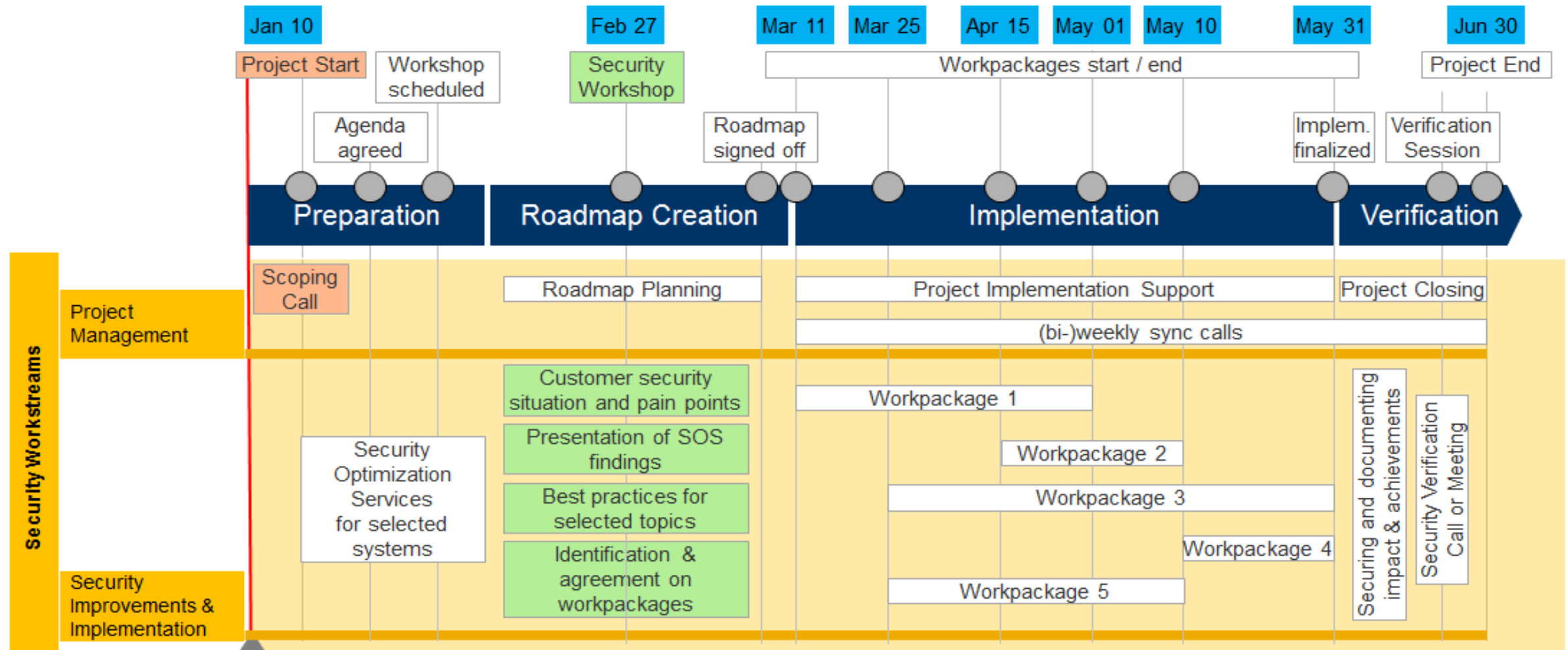
Level 3: Architecture – Advisory for security and compliance

# Identity Provisioning Service – Content

- SAP Identity Management and Access Governance Solutions, SAP Cloud Identity Services
- Identity Provisioning
- Employee lifecycle management in the cloud
- Identity Directory
- Identity Provisioning Connectors & SCIM API Access
- Integration with SAP Identity Management, Hybrid scenarios, integration of 3<sup>rd</sup> party Identity Management

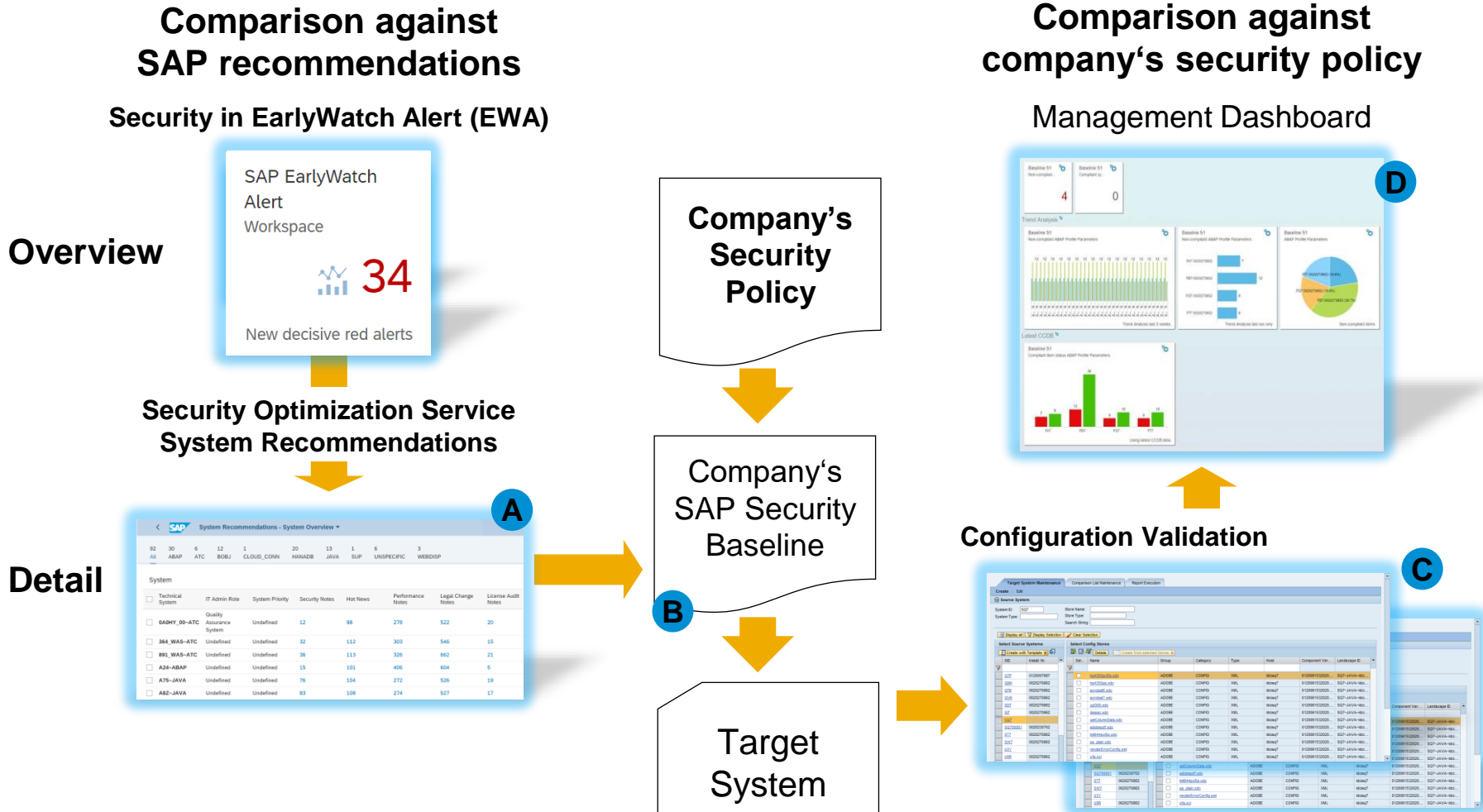
# Transparency for security and compliance

## Security road map creation as part of SAP MaxAttention engagements



# Transparency for security and compliance

## Empowering on available tools and content



### Service delivery example:

**A** Automated services indicate security gaps

**Recommendation: Detailed look into gaps through experts**

**B** Service – Part 1:

- Root cause analysis for security gaps
- SAP Security Baseline maintenance

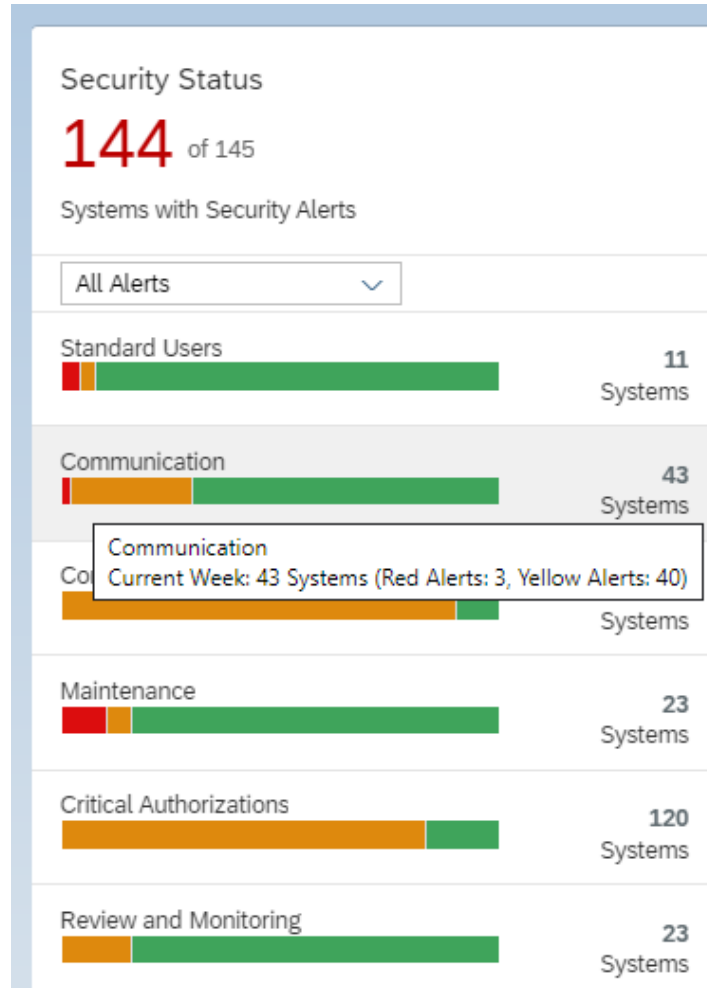
**C** Service – Part 2:

- Security patch deployment cycle
- Configuration setup
- Proactive threat identification

**D** Service – Part 3:

- Security control via dashboard

# EWA Workspace Security Card – Sample Content



## How many systems are vulnerable or even “RED”

- Standard users including SAP\* or DDIC have default passwords
- HANA user SYSTEM is active and valid
- RFC Gateway and Message Server security – Doors wide open
- HANA Internal or System Replication Communication is not secured
- Weak Password Policy
- HANA: SQL Trace configured to display actual data
- Systems having outdated Software no longer supported with SAP Security Notes
- Users having critical basis authorizations like SAP\_ALL, Debug/Replace, Change all tables,...
- HANA users having critical authorizations like DATA ADMIN privilege
- Audit Log is not active or written to an unsecure audit trail target

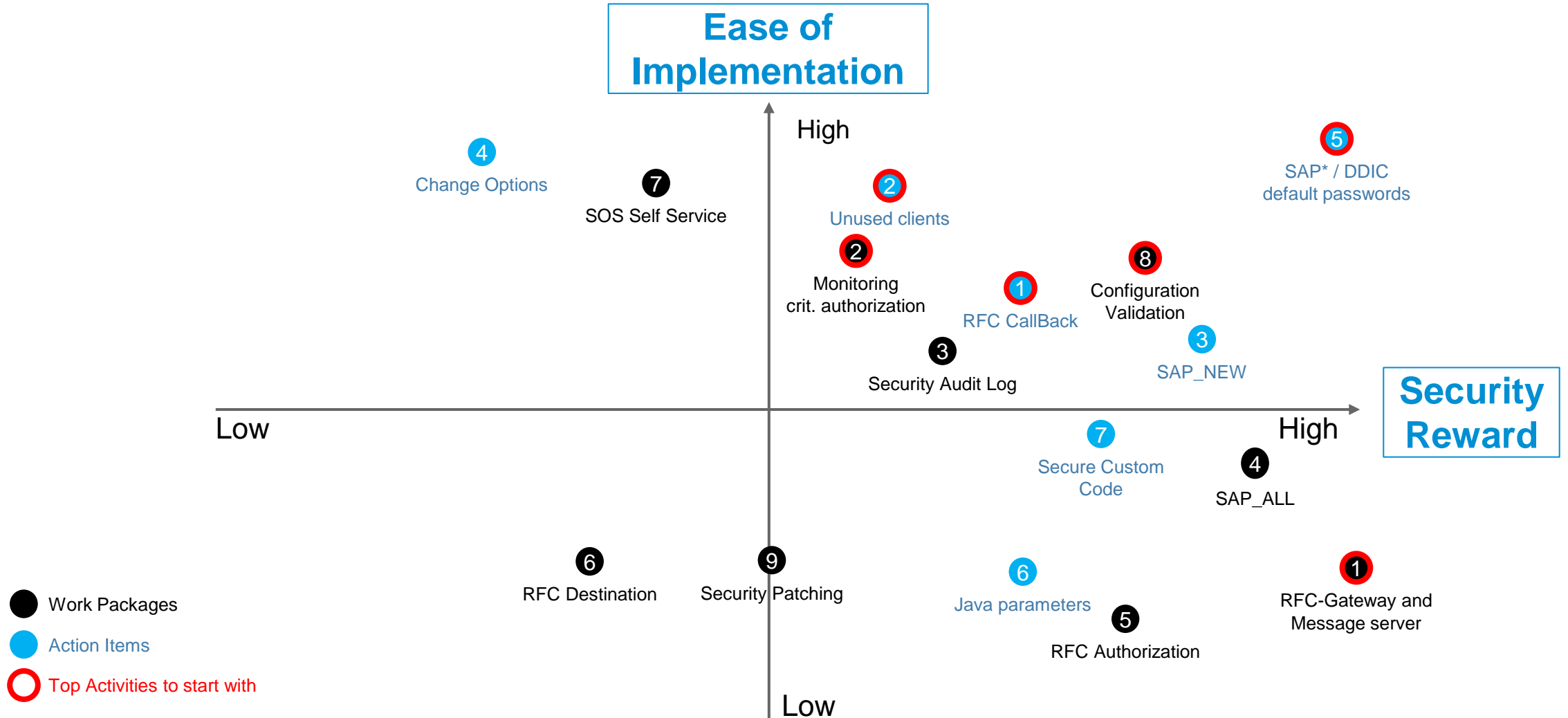
Available at <https://launchpad.support.sap.com/#ewaworkspace>

S-User Authorization required: “Display Security Alerts in SAP EarlyWatch Alert Workspace”



## Sample Result

### Work Packages and Action Items – Risk Heatmap



# Thank you.

Contact information:

**Natascha Lalor**