



# **SAP BTP Security and Compliance** **Overview**

May 2023

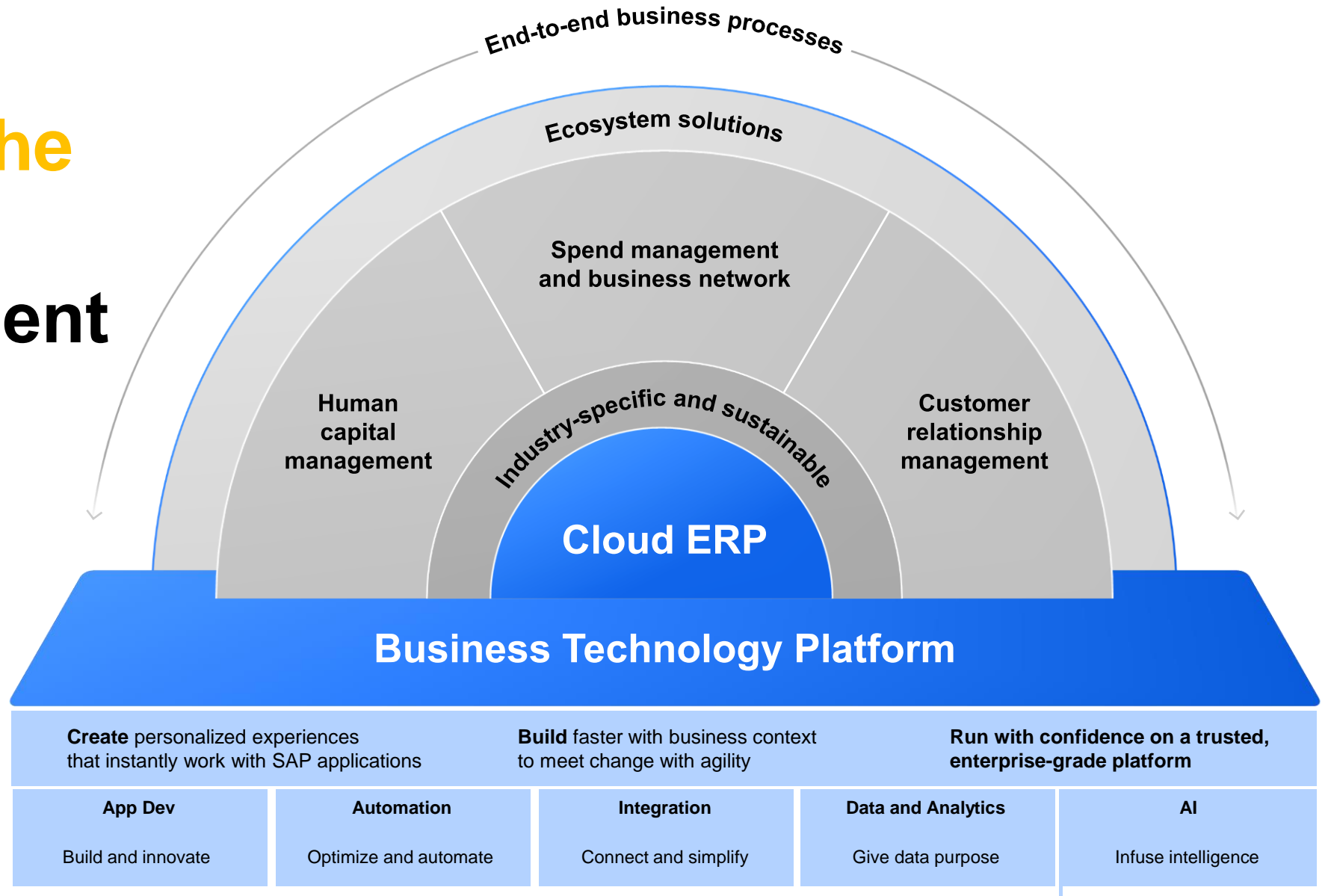
# Disclaimer

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 BTP is the foundation of the Intelligent Sustainable Enterprise



# Agenda

**01**

**Security and Compliance**

**02**

**Access Control and Authentication**

**03**

**Data Protection and Encryption**

**04**

**Compliance with Industry Standards and Regulations**

**05**

**Incident Response and Disaster Recovery**

**06**

**Best Practices for Secure Application Development**

**07**

**Security Monitoring and Threat Detection**

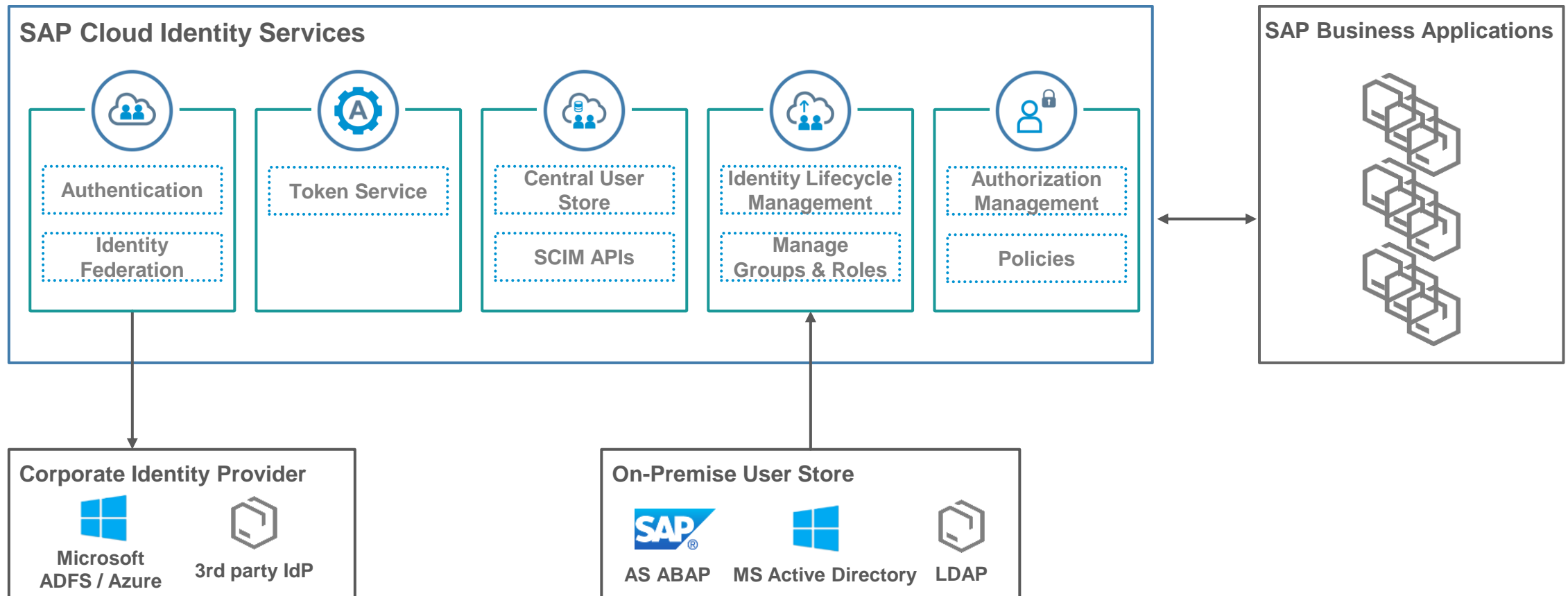


# Security and Compliance Overview

- Access Control
- Encryption
- Identity Management
- Vulnerability Scanning and Penetration Testing
- Logging and Monitoring
- Compliance Management
- Disaster Recovery and Business Continuity
- Incident Response



# Access Control and Authentication



You can find more information about Identity Authentication here:

[SAP Community](#) | [SAP Discovery Center IAS](#) | [SAP Discovery Center IPS](#) | [SAP Discovery Center AMS](#) |

# Data Protection and Encryption

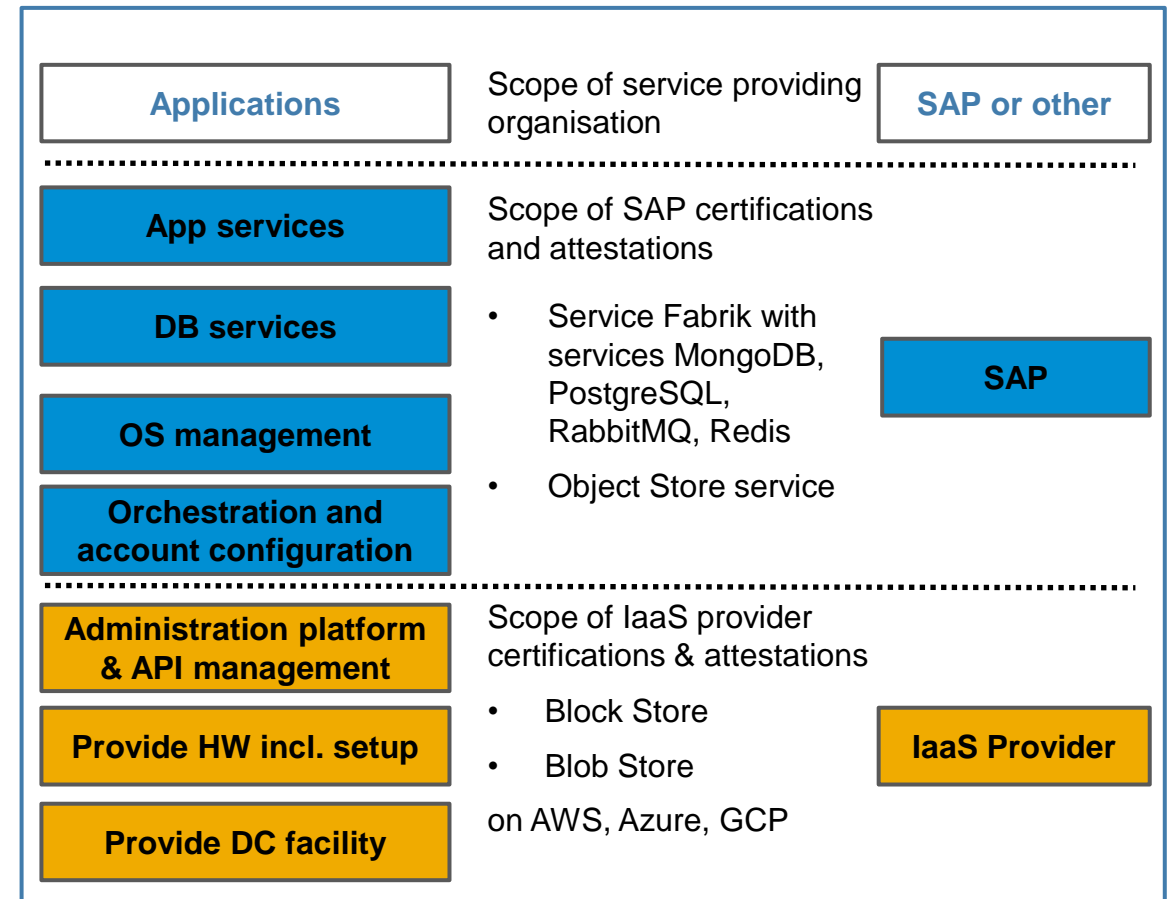
SAP BTP uses encrypted communication channels based on HTTPS/TLS, supporting TLS version 1.2 or higher. It is possible to opt-in for the use of TLS 1.3 in the Custom Domain Manager. This allows the use of TLS1.3 with Applications running on SAP BTP.

[Blog: SAP BTP Transport Layer Security \(TLS\) Connectivity Support](#)

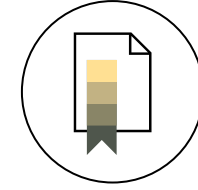
SAP BTP Services use the storage encryption of persistence services. They often use the IaaS layer underlying the SAP BTP. This is configured in the respective IaaS accounts used by SAP BTP. Encrypted backups are stored in a persistence using a strong encryption algorithm. All these keys are stored in a key management service provided by the underlying IaaS layer.

[Data Encryption Strategy \(SAP Help Portal\)](#)

## SAP BTP Service Stack



# Compliance with Industry Standards and Regulations



SAP BTP services and the underlying infrastructure hold various certifications and attestations. The BTP services attestations and certifications can be found under the naming of "SAP Business Technologie Platform" in the SAP Trust Center

SAP BTP runs in secure and certified environments

- World-class data centers
- Advanced network security
- Reliable data backup
- Built-in compliance, integrity, and confidentiality

[Cloud Services with 99.7% availability](#)

For more details, see

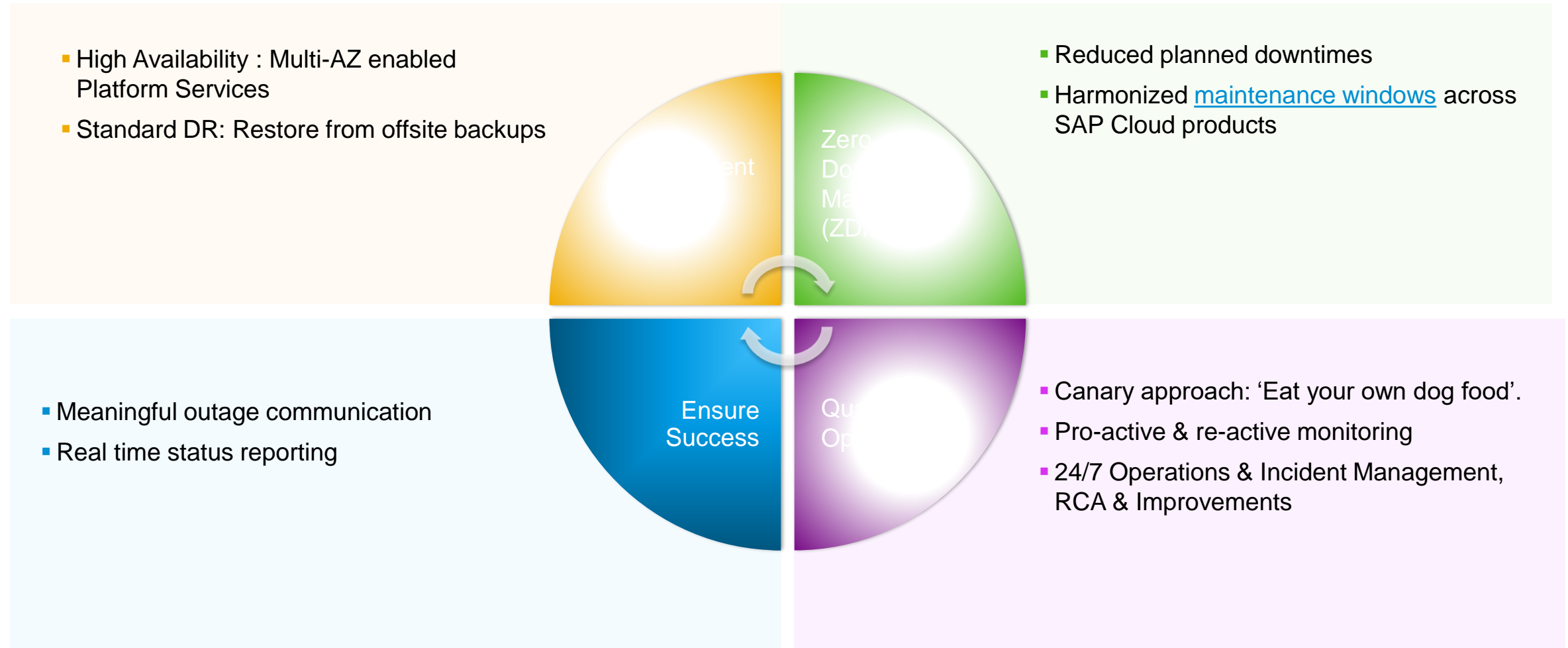
- [SAP Data Center](#)
- [SAP Trust Center](#)
- [Cloud Availability section in SAP for Me](#)

## Certifications & Attestations

- ISO 27001, ISO 27017, ISO 27018 - Information Security Management System
- ISO 22301 - Business Continuity Management System
- SOC 1 Type 2, SOC 2 Type 2
- C5 Type 2 (BSI Germany)
- EU Cloud Code of Conduct
- CSA STAR
- TISAX (Trusted Information Security Assessment Exchange)



# Incident Response and Disaster Recovery



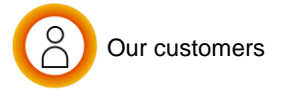
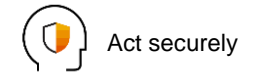
# Best Practices for Secure Application Development

- [SAP Cloud Application Programming Model \(CAP\)](#) which includes build-in security functionalities
- SAP BTP offers various services and APIs to develop secure software applications. See [SAP BTP on SAP API Business Hub](#)
- [SAP BTP Security Recommendations](#) for a securely configured platform



# Security recommendations

## Setting up SAP S/4HANA cloud securely



SAP Help Portal (Documentation) | Browse by Product | Learning Journeys | What's New | Explore SAP | Search | User

Home > SAP S/4HANA Cloud > Protect Your SAP S/4HANA Cloud > Security Recommendations

### Protect Your SAP S/4HANA Cloud 2302.1 English

This document | Search in this document | Advanced Search

← Previous | Favorite | Download PDF | Share | Next →

- Protect Your SAP S/4HANA Cloud
  - Security Recommendations**
    - Explanation of Table Headings
    - Technical System Landscape
    - Security of Data Centers and External Auditing
    - Secure Communication
    - Secure Authentication
    - Identity and Access Management
    - Secure Storage
      - Virus Scanning
    - Security Logging
    - Access Control and Data Protection

## Security Recommendations

SAP S/4HANA Cloud is delivered with secure default configurations wherever this is possible. However, you might want to review some settings and adjust them to your particular use case and corporate policies.

To find out more about the table headings used below, see [Explanation of Table Headings](#).

Hide/Show Columns | Search entire table

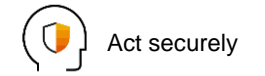
Priority	Secure Operations Map	Topic	Default Setting or Behavior	Reco
Filter: [No Selection]	Filter: [No Selection]	Filter: [No Selection]		
Advanced	Security governance	Communication Systems: Responsibles	Communication must be set up by the customer. No communication systems are configured by default.	Mail info... respo... com... syste...
Recommended	User & Identity Management	Communication Users	Communication must be set up by the customer. No communication users are configured by	Com... users... reuse... con...

Was this page helpful?

[https://help.sap.com/docs/SAP\\_S4HANA\\_CLOUD/55a7cb346519450cb9e6d21c1ecd6ec1/fafa6639cf7b4265b68da63efbc8fb96.html?locale=en-US](https://help.sap.com/docs/SAP_S4HANA_CLOUD/55a7cb346519450cb9e6d21c1ecd6ec1/fafa6639cf7b4265b68da63efbc8fb96.html?locale=en-US)

# Protect your SAP S/4HANA Cloud

## Setting up SAP S/4HANA Cloud securely



Act securely



Our customers

SAP Help Portal (Documentation)

Home > SAP S/4HANA Cloud > Protect Your SAP S/4HANA Cloud

### Protect Your SAP S/4HANA Cloud

2302.1 English

This document Search in this document

Was this page helpful?

Security has always been an important element for the complete product life cycle of all SAP products, including product development, planning, and quality assurance.

As a Software-as-a-Service (SaaS) product, SAP S/4HANA Cloud takes care of infrastructure-level security like networks, operating systems and patch management. Security aspects that might require business decisions are managed by the customer. A typical example is user and authorization management. In some areas, SAP delivers secure default settings which can be modified to meet specific business needs (e.g., for system integrations).

SAP takes care of some of the security focus areas, while others have to be handled by you. Below, you can find an overview of these areas and responsibilities.

The section [Security Recommendations](#) provides a more detailed overview of security configurations with their defaults and recommended values.

Security Focus Area	Customer Responsibility	SAP Responsibility	Related Information
Data storage	n/a	Data encryption, backup	<a href="#">Secure Storage</a>
Network security	Define communication to external systems	Network infrastructure: firewalls, network segmentation etc.	<a href="#">Server Communication Security</a>
Web security	Define additional trusted sites if needed (relax delivered settings).	Deliver secure default settings for protecting the end user UI	<a href="#">Frontend Communication Security</a>
Secure authentication	<ul style="list-style-type: none"> <li>Define password policies and MFA requirements</li> <li>Configure corporate identity provider if required</li> </ul>	Provide a default identity provider	<a href="#">Secure Authentication</a>
User administration and authorizations	Implement authorization concept for business users	n/a	<a href="#">Authorization and User Concept in SAP S/4HANA Cloud</a>
Application-specific virus scans	n/a	Run virus scans	<a href="#">Virus Scanning</a>
Security patching	Adjust authorization concept after functional upgrades	<ul style="list-style-type: none"> <li>Continuous vulnerability scans</li> <li>Security patches</li> <li>Security enhancements of business functionality</li> </ul>	<a href="#">Manage Business Role Changes After Upgrade</a>

[https://help.sap.com/docs/SAP\\_S4HANA\\_CLOUD/55a7cb346519450cb9e6d21c1ecd6ec1/484053beaaa3455590cbf90ca99d541f.html?locale=en-US](https://help.sap.com/docs/SAP_S4HANA_CLOUD/55a7cb346519450cb9e6d21c1ecd6ec1/484053beaaa3455590cbf90ca99d541f.html?locale=en-US)

# Security Monitoring and Threat Detection

- Threat Intelligence Program
- Continuous monitoring of system and application logs
- Network traffic analysis
- Intrusion detection systems
- Proactive monitoring and response to potential threats
- Event, incident, threat, and vulnerability management
- Security information and event management (SIEM)
- 24/7 general security monitoring, including escalation procedures
- Security incident tracking and resolution by security specialists

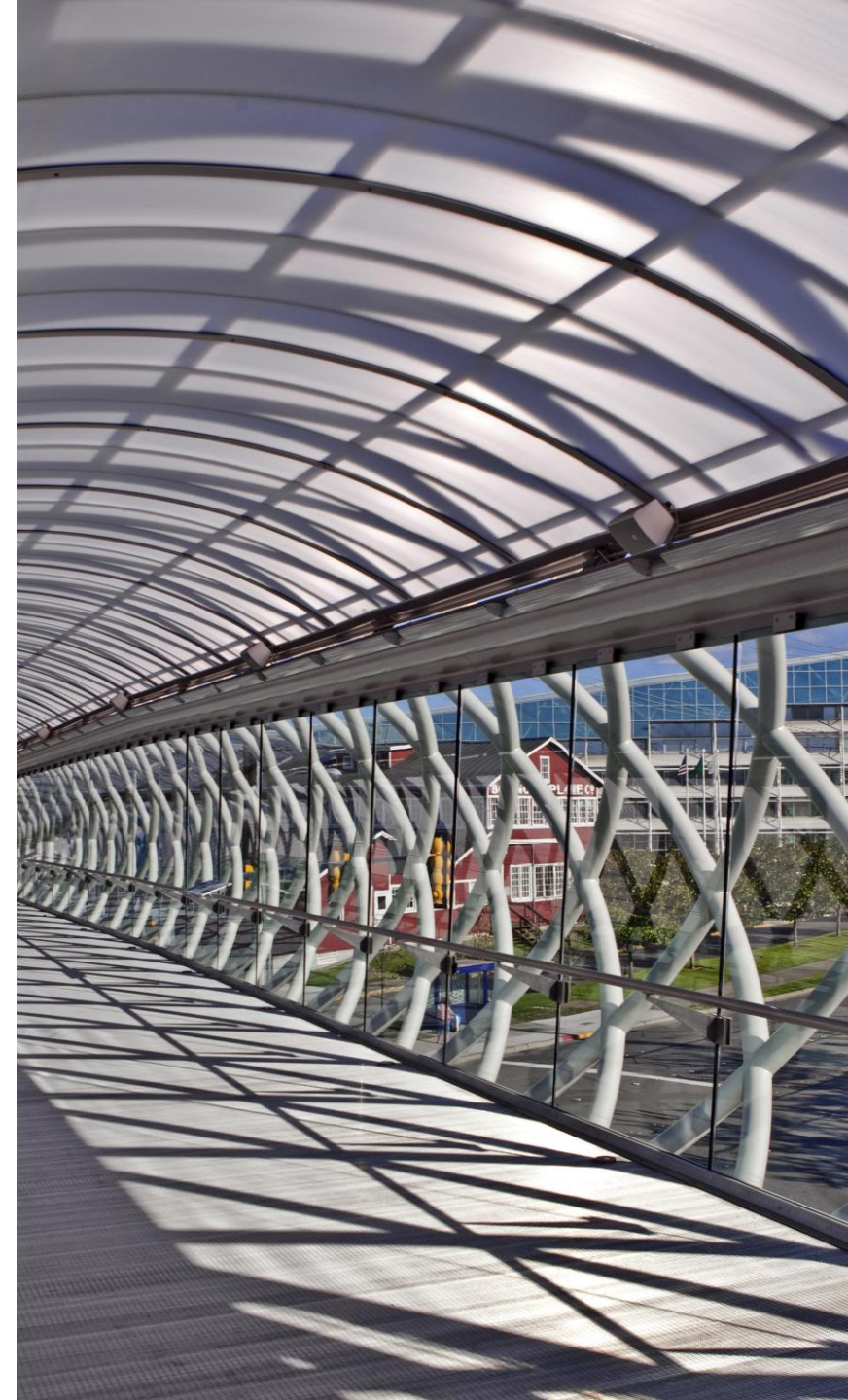
See: [Cloud Services: Reference Guide](#)



# Conclusion

- I. The SAP Business Technology Platform provides a comprehensive set of security and compliance features to ensure the security of customer applications and data.
- II. Secure application development on the platform is supported through best practices for securing application user accounts and data.
- III. Customers can review the platform's security features and controls and use the recommended best practices in configuring their applications for optimal security.

More Information on: [My Trust Center](#) & [SAP for Me](#)



# Thank you.

Contact information:

Jürgen Adolf  
juergen.adolf@sap.com



Follow us



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

© 2023 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.