The Universe of SAP BTP in a Nutshell – Platform Security

SAP BTP Security Team
2023

SAP’s vision is to enable networked intelligent, sustainable, and secure enterprises that deliver business and societal outcomes . . .

1. Build securely

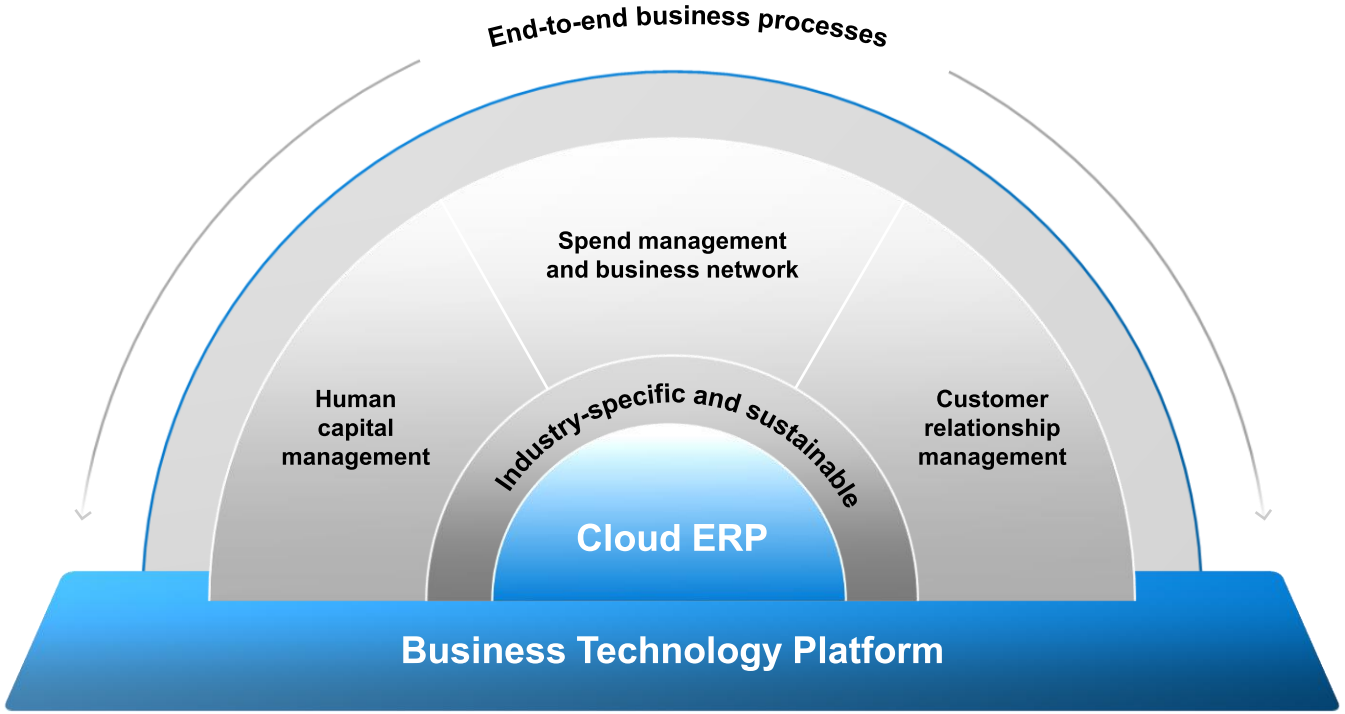
We build secure-by-design solutions.

2. Run securely

We run cloud operations securely.

3. Act securely

We foster a security-first culture in everything we do.



Pillars of security for SAP BTP

1. Build securely

We build secure-by-design solutions.

Secure cloud software development

Leading security, data protection, and privacy features

We Build Secure-by-Design Solutions

Software development

We employ a security-first approach at every stage of the software development and operations lifecycle.

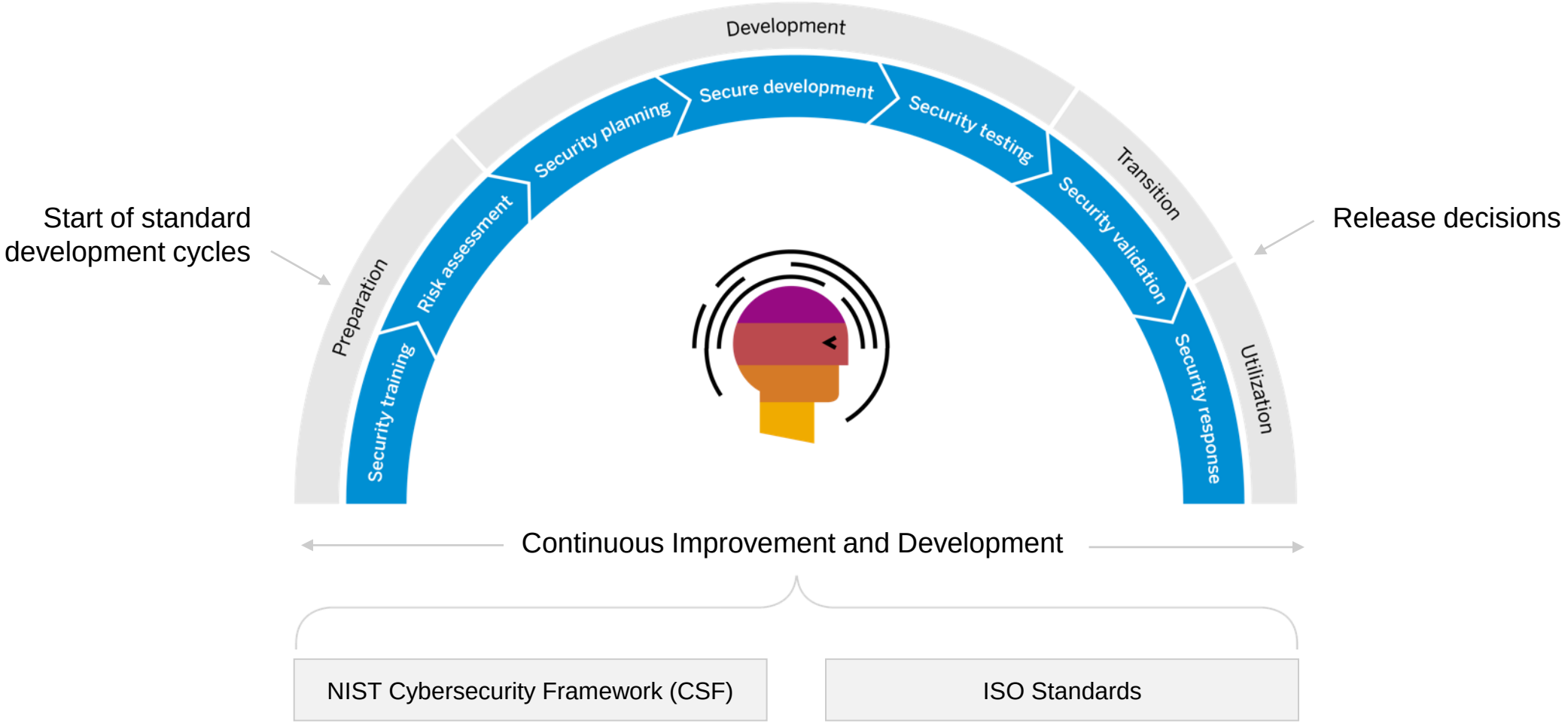
Cloud environments

We partner with leading providers to build secure-by-design cloud environments.

Security solutions

We offer solutions with specialized security and process-oriented controls that elevate customers' security posture.

Phases in the
Secure Software Development and Operations Lifecycle (SecSDOL)



SAP BTP Services to Build Secure Applications

SAP Cloud Identity services

SAP Authorization and Trust Management Services

SAP Connectivity and Destination Service

SAP Audit Log Service

SAP Custom Domain service

SAP Credential Store

SAP Malware Scanning Service

1. BUILD

Software development

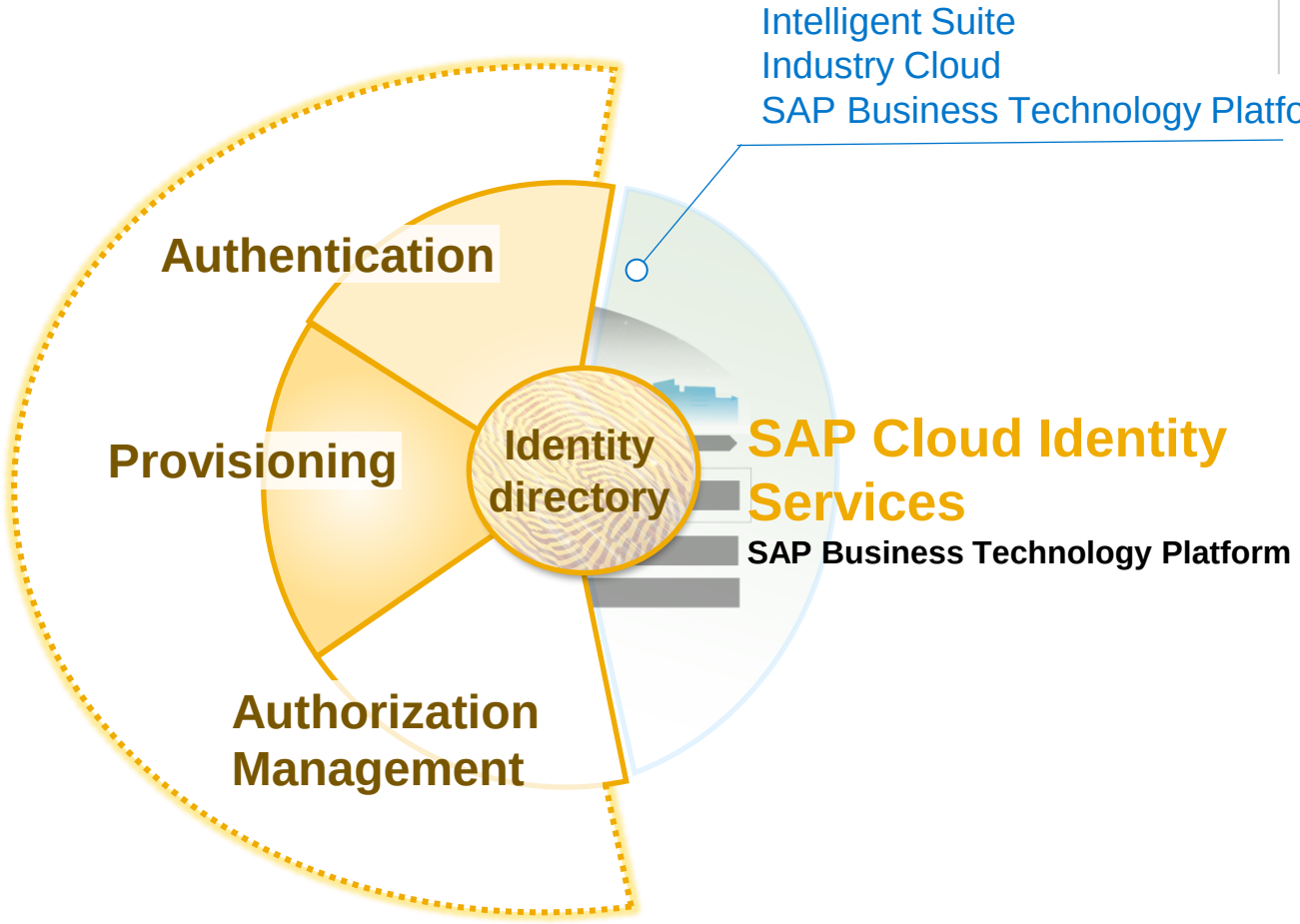
SAP Cloud Identity Services

SAP Cloud Identity Services are the **default** to authenticate and provision users in cloud solutions from SAP.

- Identity authentication
- Identity provisioning
- Authorization management
- Integrated through the common identity directory

The number of **pre-integrated SAP solutions** that require **SAP Cloud Identity Services** will increase**.**

One cloud service from SAP is used to integrate any 3rd party identity management (IDM) system.



SAP Cloud Identity Services - Identity Authentication

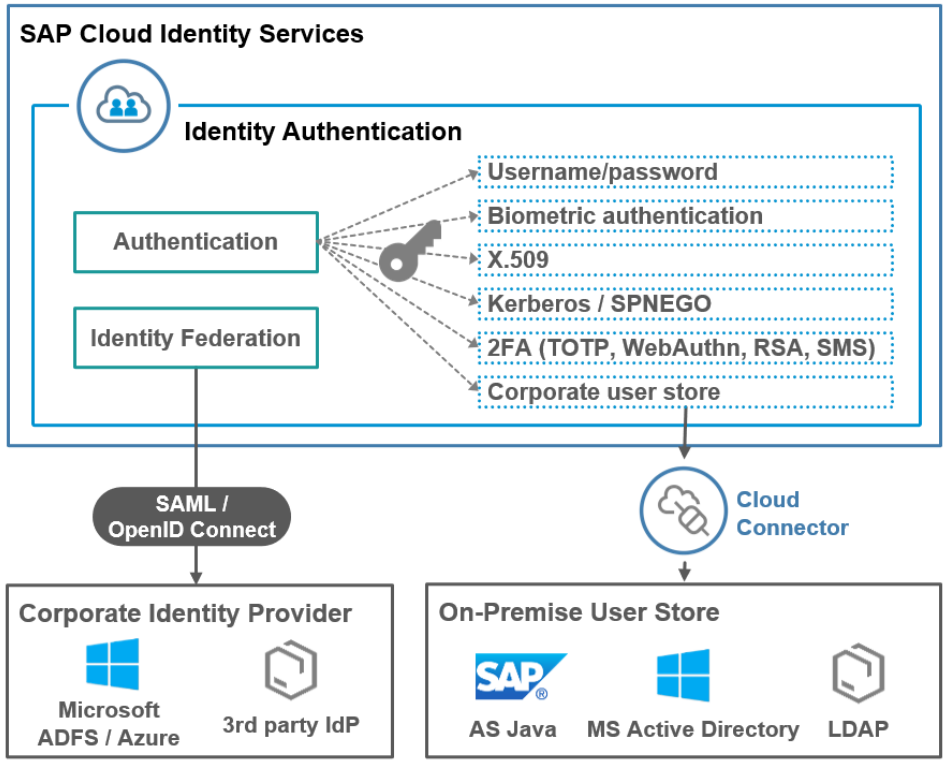
Identity Authentication is a cloud service for authentication, single sign-on (SSO) and user management for SAP cloud applications. It can act as an identity provider itself or be used as a proxy to integrate with an existing single sign-on infrastructure.
Identity Authentication is a component of SAP Cloud Identity Services.

Benefits

- Central SSO endpoint for SAP cloud applications
- Harmonize the authentication mechanisms and user management across SAP cloud applications
- Flexible enforcement of stronger means of authentication (multi-factor authentication)
- Identity Authentication can act as authentication broker to enable SSO for all types of users
- Security token service for protection of system-to-system communication with principal propagation

Key capabilities

- Public cloud service offered in more than 12 regions worldwide
- Cloud Service Providers: SAP, Amazon Web Services, Microsoft Azure
- Support for open standards:
  - Single sign-on: SAML & OpenID Connect
  - Authentication: X.509, Kerberos/SPNEGO, FIDO
  - Multi-factor authentication: time-based one-time password tokens (TOTP), FIDO/WebAuthentication, Email, RSA
  - User provisioning: SCIM
- Conditional authentication to determine where to validate user's credentials
- Risk-based authentication for flexible enforcement of multi-factor authentication
- Configurable password policies
- Branding style options for UI elements, e-mails, and error pages to comply with corporate branding requirements
- Troubleshooting and Audit Logs
- High Availability (HA) / Disaster Recovery (DR): 99,95% standard availability (multi-Availability Zones (AZ) offered in most regions) 'multi-region setup' operated with two data centers in HA and DR mode among the respective data centers
- Zero Downtime Maintenance (ZDM)



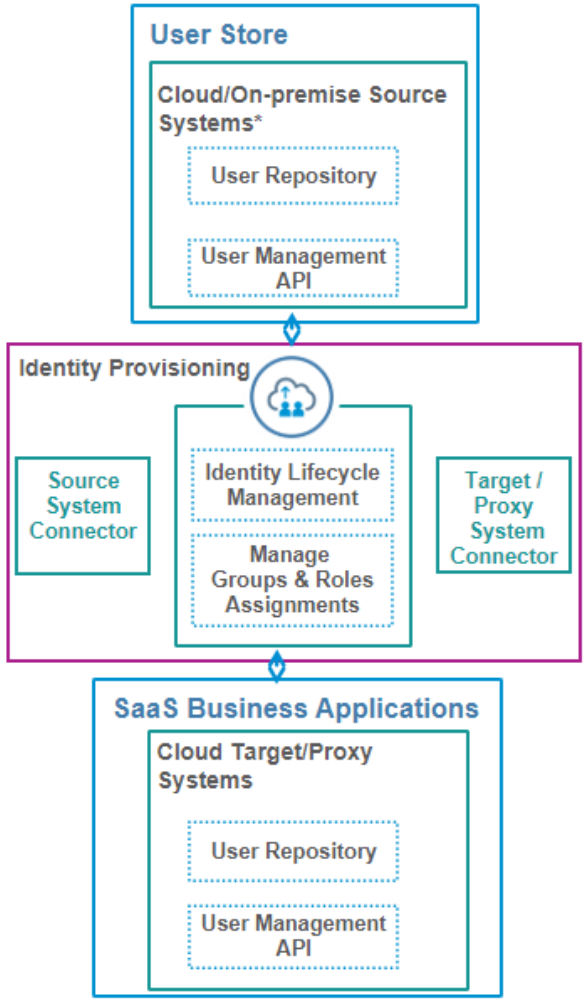
You can find more information about Identity Authentication here:

SAP Discovery Center | SAP Community | Help Portal | API Hub

SAP Cloud Identity Services - Identity Provisioning

Solution Overview

Identity Provisioning is a cloud service for managing identity lifecycle processes in the cloud. The service automates identity lifecycle processes and helps you provision identities and their authorizations to various cloud and on-premise business applications.



Benefits

- Fast adoption of SAP solutions through out-of-the-box integration (bundles)
- Rapid scenario extensions with optimized SAP connectors
- SCIM compliant integration with Identity Management solutions

Key capabilities

- Public cloud service offered in more than 12 regions worldwide
- Identity Provisioning tenants run on the infrastructure of SAP Cloud Identity Services and the SAP BTP, Neo environment (existing tenants only)
- Cloud Service Providers: SAP, Amazon Web Services, Microsoft Azure
- The Identity Provisioning service offers connectors for provisioning of users and groups between multiple supported cloud and on-premise systems, both SAP and non-SAP. The connectors can be customized via the Transformation Editor
- Automatic delivery of pre-configured provisioning systems for specific SAP cloud solutions
- (connectors) relevant to one or more bundled SAP cloud solutions
- The Identity Provisioning service can be consumed either directly through its APIs, or by the user interface (UI)
- Support for open standards:
  - User provisioning: SCIM
  - Transformation editor: JSON
  - Authentication for secure communication with the provisioning systems: X.509
- High Availability (HA) / Disaster Recovery (DR): 99,95% standard availability (multi-Availability Zones (AZ) offered in most regions) ‘multi-region setup’ operated with two data centers in HA and DR mode among the respective data centers for the tenants running on the SAP Cloud Identity Services infrastructure
- Zero Downtime Maintenance (ZDM)

You can find more information about Identity Provisioning here:

SAP Discovery Center | SAP Community | Help Portal | API Hub

SAP Authorization and Trust Management Service

1. BUILD

Software development

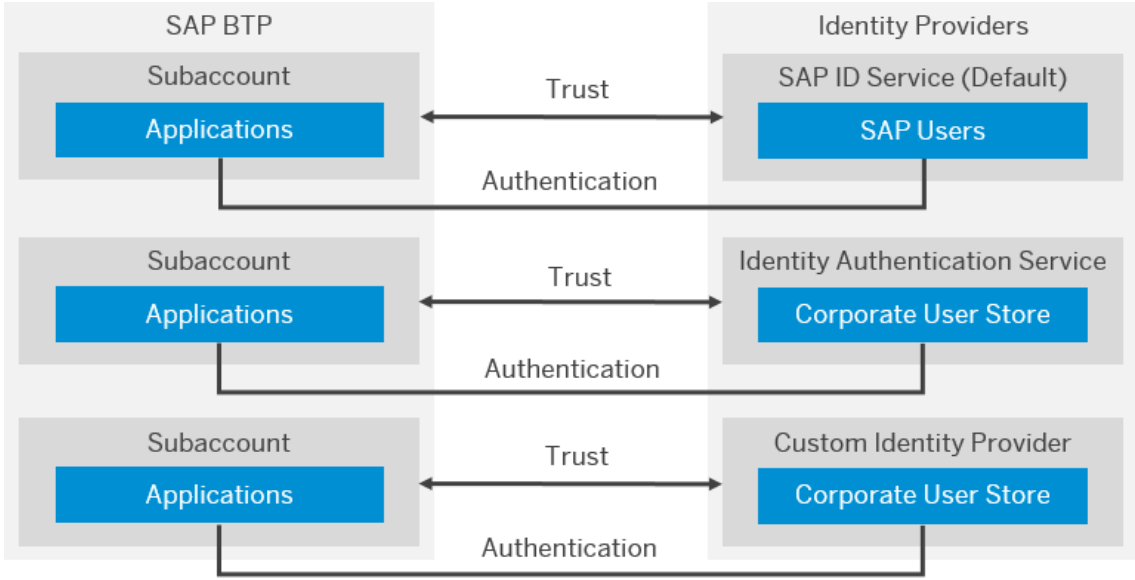
The SAP Authorization and Trust Management service provides security functions such as business user authentication and authentication of applications. It lets you manage user authorizations and trust to identity providers per subaccount. Identity providers are the user base for applications. We recommend that you use an SAP Cloud Identity - Identity Authentication tenant, which can be easily enabled. Alternatively, you can directly use custom corporate identity provider. User authorizations are managed using technical roles at the application level, which can be aggregated into business-level role collections for large-scale cloud scenarios.

Benefits

- Enables administrators to make sure that users only have access to functions for which they are authorized
- Enables developers to request authentication and implement authorization checks in their applications
- Enables administrators to manage user authorizations and trust to identity providers
- Support federated authorization assignment using group attributes from identity providers

Key capabilities

- Default identity provider with pre-configured trust
- One-click trust setup with SAP Cloud Identity Authentication Service
- Use of external identity providers
- Enables developers to define application-specific roles
- Enables administrators to manage authorizations for users
- Enables developers to manage authorizations for applications



You can find more information about Identity Authentication here:

SAP Discovery Center | SAP Community | Help Portal | API Hub

SAP Audit Log Service

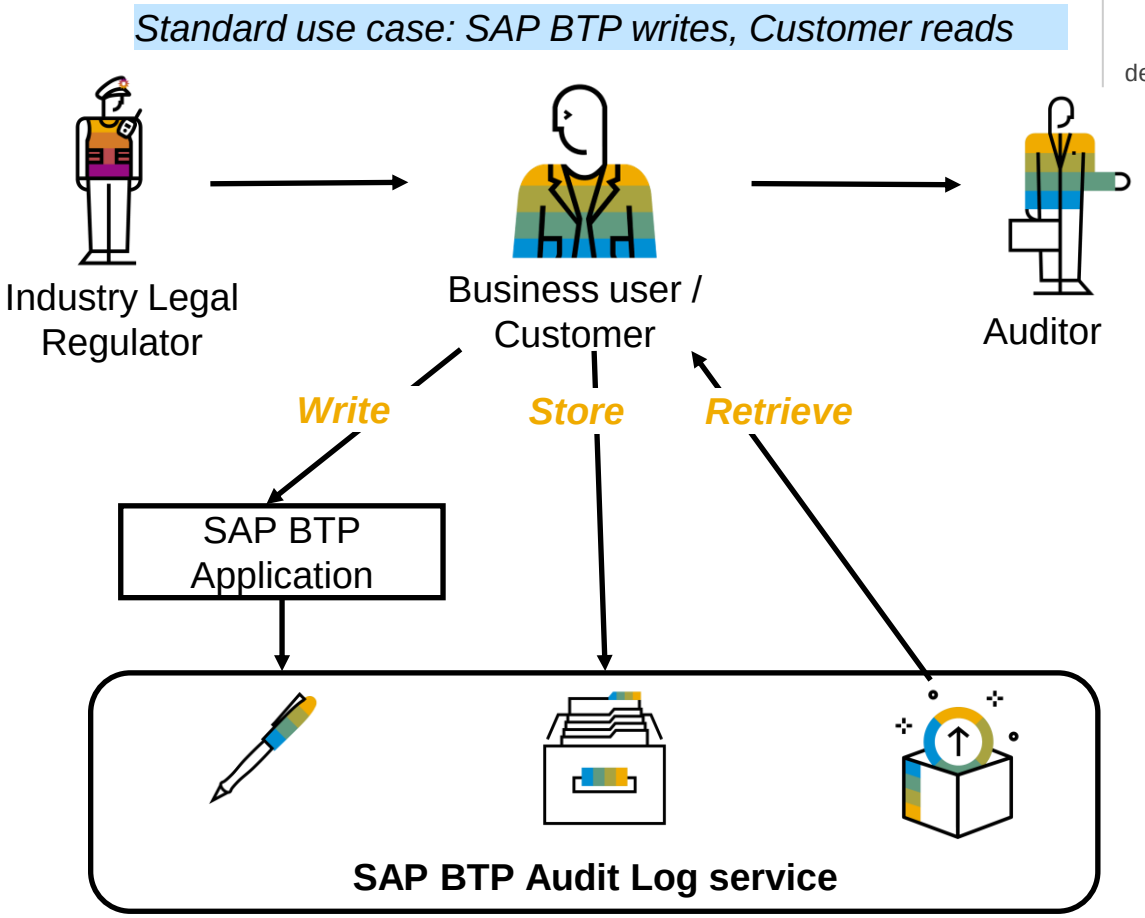
The SAP Audit Log service is a platform service which stores all the audit logs written on your behalf by other platform services that you use. It allows you to retrieve the audit logs for your subaccount via the audit log retrieval API or view them using the Audit Log Viewer.

Benefits

- Allow Auditors to perform Audit related activities in efficient, reliable and complete manner
- Enablement of the cloud provider and/or customer to identify malicious activities
- Provisioning of Forensic evidence that can be used at court
- Make sure your business is compliant with the most recent business and product security standards

Key Capabilities

- Dependency Service for successful operations and commands
- Unified log messages
- 90 days default retention period
- Forward data to existing companywide security log system



You can find more information about the SAP Credential Store here:

Discovery Center: SAP Audit Log Service | Help Portal | API Hub

SAP Credential Store

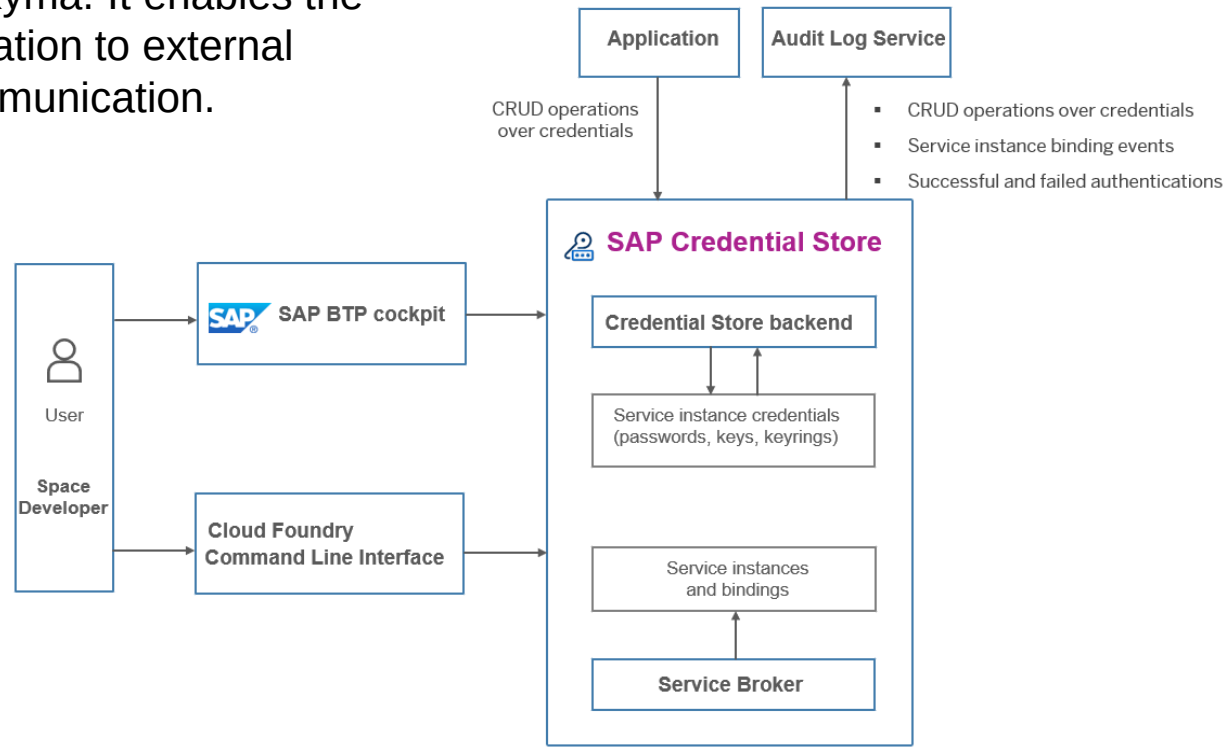
SAP Credential Store provides a repository for passwords, keys and keyrings for applications that are running on SAP BTP, Cloud Foundry or Kyma. It enables the applications to retrieve credentials and use them for authentication to external services, or to perform cryptographic operations and TLS communication.

Benefits

- Create, store and manage cryptographic credentials, which your SAP BTP applications can use to access external services
- Provide higher level of security by using multi-version cryptographic keys to encrypt or decrypt other cryptographic keys
- Share service instances between spaces or subaccounts

Key capabilities

- Encryption of data by using customer's own key
- Retrieval of passwords, cryptographic keys and keyrings for authentication to external services
- Access to service instances from external applications or from applications deployed in another space - by using service keys



You can find more information about the SAP Credential Store here:

[Discovery Center: SAP Credential store](#) | [Help Portal](#) | [API Hub](#)

SAP Custom Domain Service

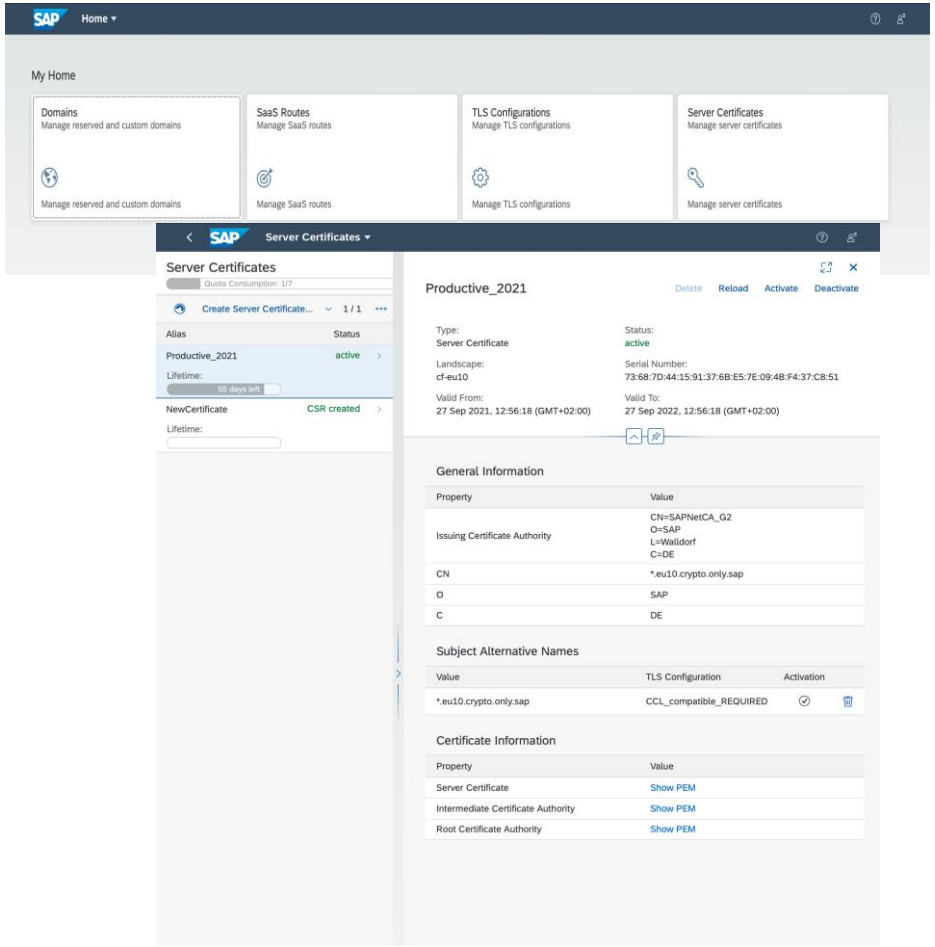
SAP Custom Domain enables subaccount owners to make their SAP BTP applications accessible via a custom domain that is different from the default one (hana.ondemand.com) - for example, www.myshop.com.

Key capabilities

- Manage custom domains and configurations in Manager UI or via CLI
- Bring your own certificates for CSRs generated by the service
- Activate single or multiple custom domains per certificate
- Configure TLS properties like protocol version and cipher suites, mutual client authentication mode and trusted CAs, or HTTP/1.1 and HTTP/2
- Set up custom domain routes to SaaS subscriptions

Benefit

- Access to your domain: Configure your application with a name that is easily recognizable by your customers
- Application identity protection: Upload a TLS/SSL certificate to help secure your application identity and the data transmitted between the browser and your application



You can find more information about the SAP Custom Domain Service here:

Discovery Center: SAP Custom Domain Service | Help Portal

SAP Connectivity and Destination Service

SAP Connectivity Service allows cloud applications running on the SAP BTP to access remote services securely that run on the Internet or on-premise.

Key capabilities

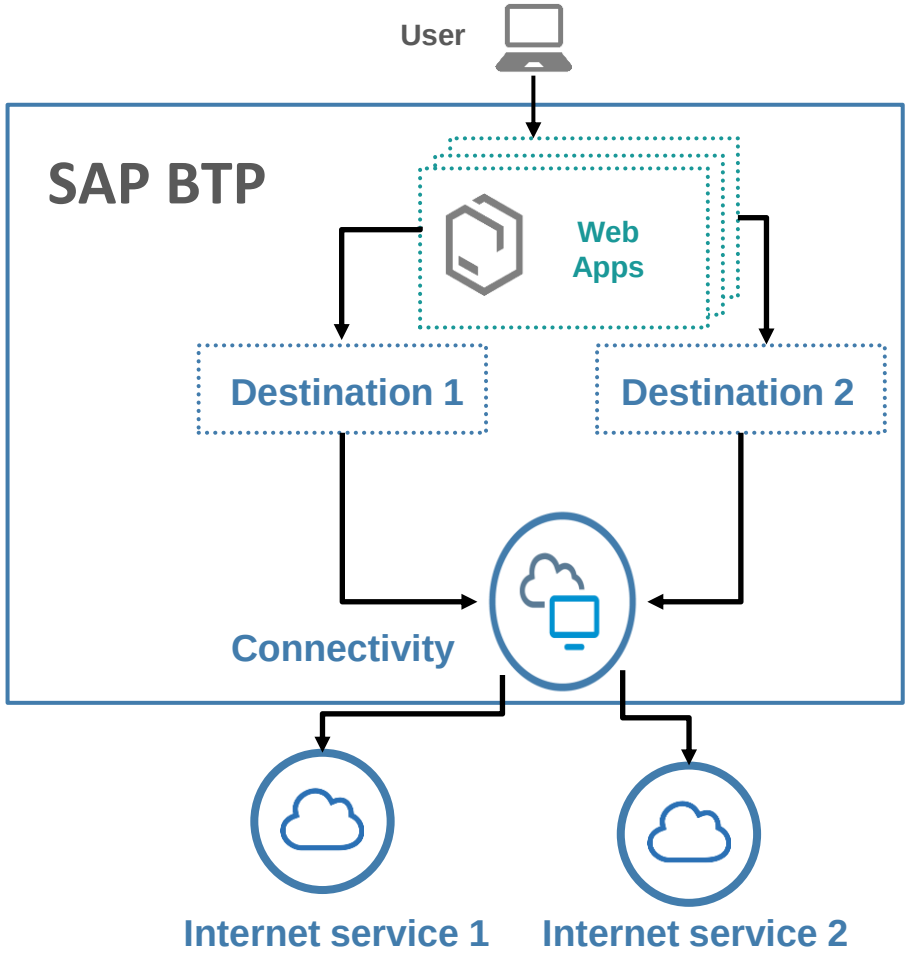
- Consume APIs and data from APIs and data provided by any Internet service via HTTP(s) using destinations
- Consume APIs, data and users provided by on-premise systems via HTTP, RFC, or even with TCP using destinations and the Cloud Connector

Benefits

- Separation of concerns
- Security
- Re-useability
- Access via Tools

You can find more information about the Connectivity service here:

Discovery Center: Connectivity Service | Discovery Center: Destination Service | Help Portal | API Hub



SAP Cloud Connector

1. BUILD

Software development

The SAP Cloud Connector establishes a secure VPN connection between SAP BTP and on-premise systems.

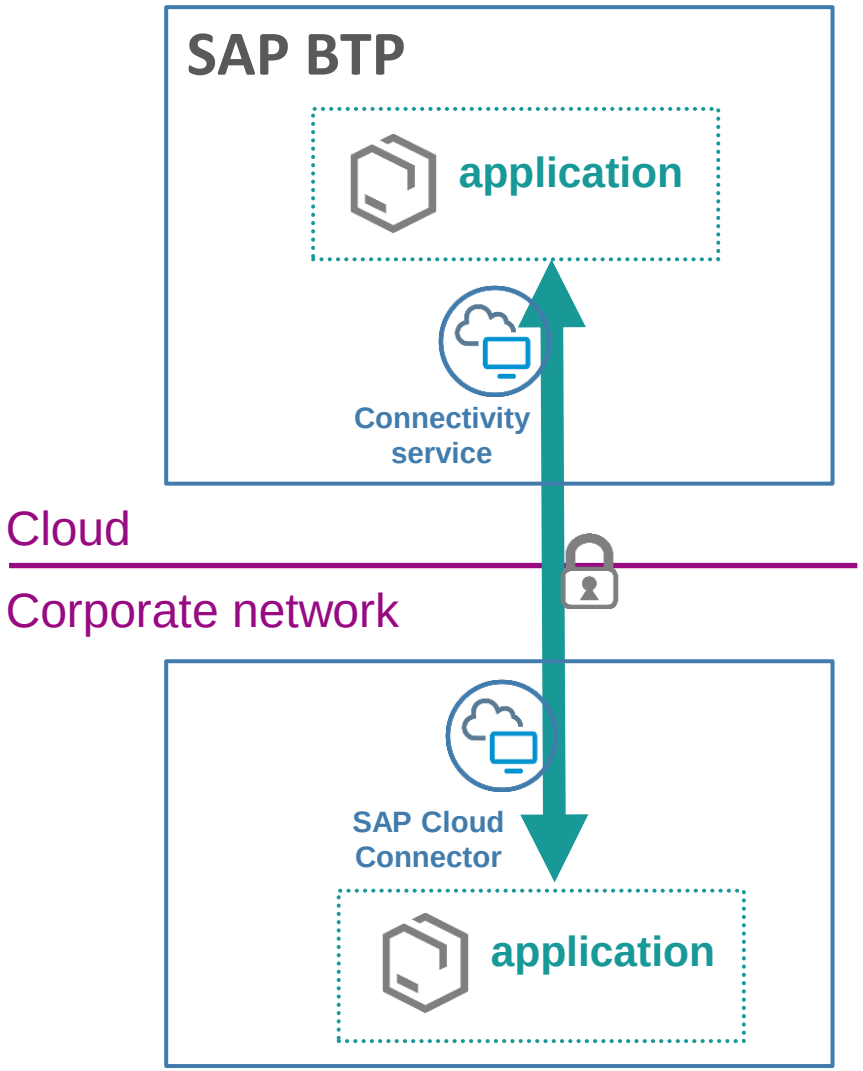
Key capabilities

- Fine grained access control lists of allowed cloud and on-premise resources
- Fine grained audit logging for traceability
- Principal propagation from cloud to on-premise
- Trust relation with on-premise system based on X.509 certificates

Benefits

- No change in the existing corporate firewall configuration is needed
- He initiates encrypted connections to cloud application from inside the on-premise network to the cloud
- Firewall and DMZ remain unchanged

[Blog: Cloud Connector Setup]



SAP Malware Scanning Service

1. BUILD

Software development

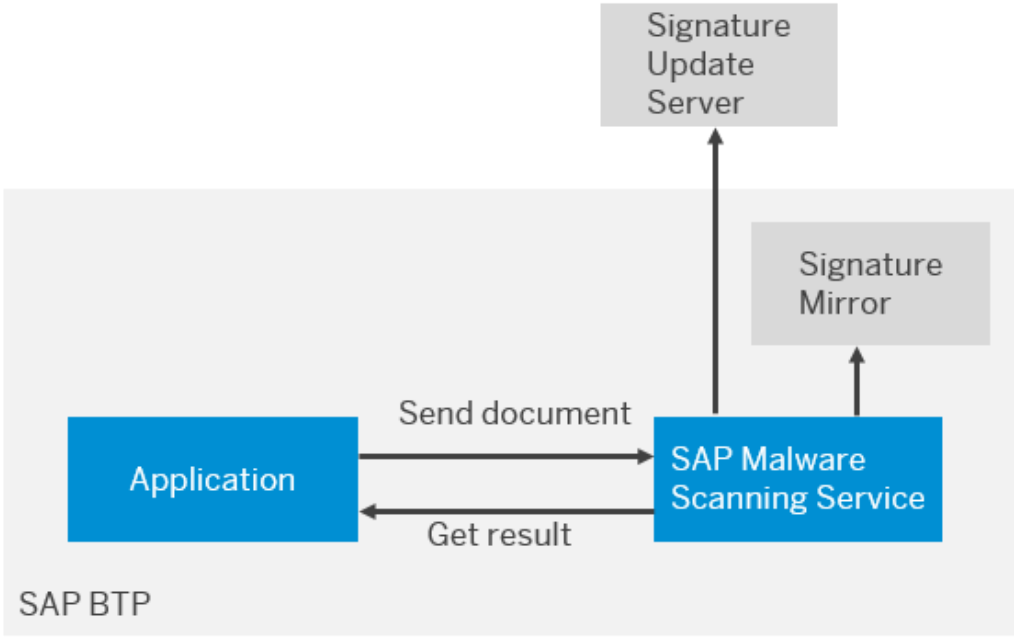
SAP Malware Scanning Service provides the possibility to scan business documents for malware. Integrate this service with your custom-developed apps running on Cloud Foundry. When your apps upload business documents, they can call the SAP Malware Scanning service to check for viruses or other malware.

Key capabilities

- Scanning of documents
- Limit of about 20 concurrent scan requests depending in the overall load
- Service API is available on SAP API Business Hub

Benefits

- Secure SAP and non-SAP Applications, on SAP BTP, cloud foundry environment
- Reduce malware in your environment
- Help meet compliance requirements



You can find more information about the Malware Scanning Service here:

SAP Discovery Center | **SAP Community** | **Help Portal** | **API Hub**

SAP BTP

APIs to develop secure software

1. BUILD

Software development

SAP BTP offers various APIs to develop secure software applications.

A suite of services for user authentication and lifecycle management: SAP Cloud Identity Services

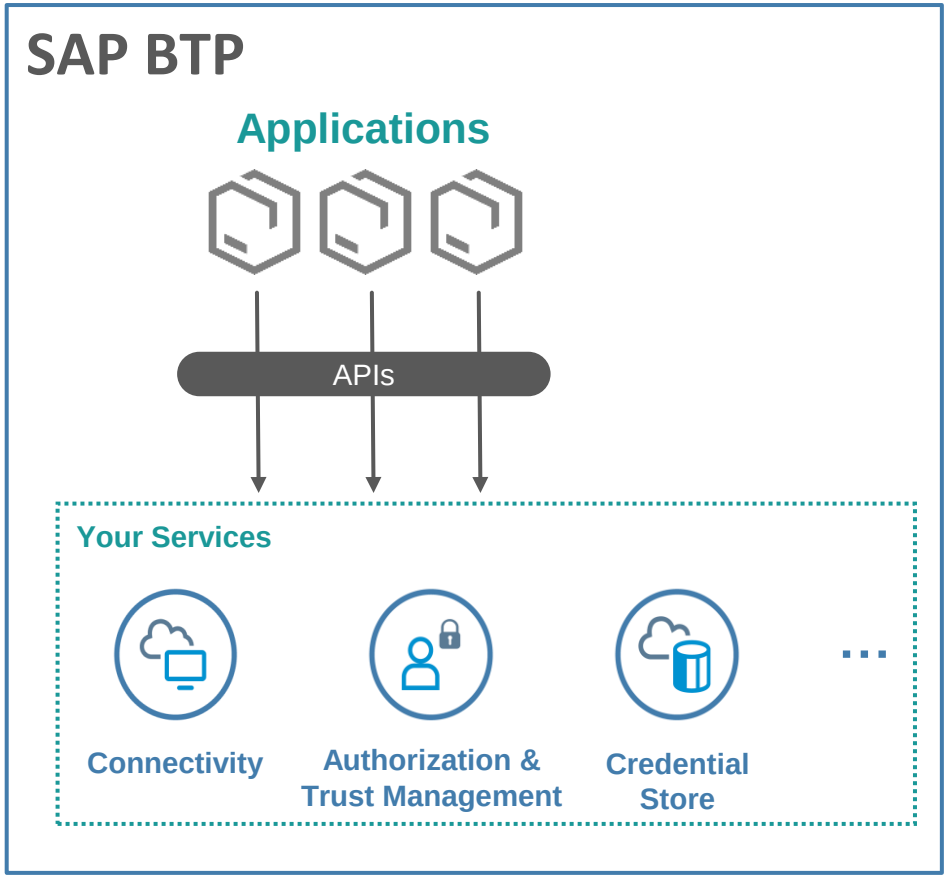
Manage application authorizations and trust for SAP BTP: SAP Authorization and Trust Management Service

Functionality for subaccount members managing: Platform Authorizations Management API

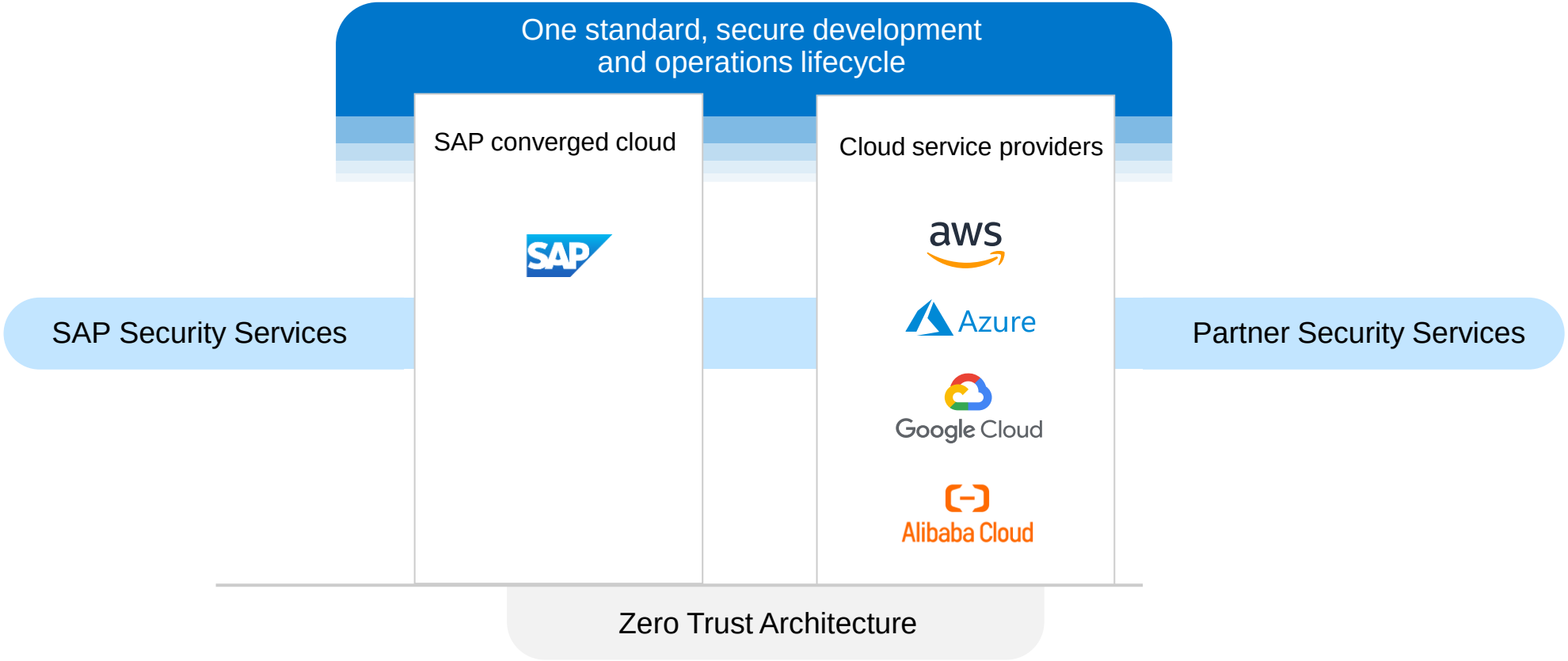
Manage destinations and securely connect to on-premise systems: SAP Connectivity Service

Managing passwords and keys: SAP Credential Store Service

Functionality for retrieving audit logs: Audit Log Retrieval API



We partner to build secure-by-design cloud environments



Additional solutions from SAP for Securing Applications and Data

Visit **sap.com/grc** for more information

Identity and access management

Privacy governance solutions

A data custodian and encryption key management system

Focus on risk management across the portfolio of SAP solutions

Threat detection for SAP applications

Areas of secure software development for SAP BTP

Build securely

Secure cloud software development

SAP’s secure development and operations lifecycle

Threat modeling

Security assessment and testing

Secure coding training for all developers

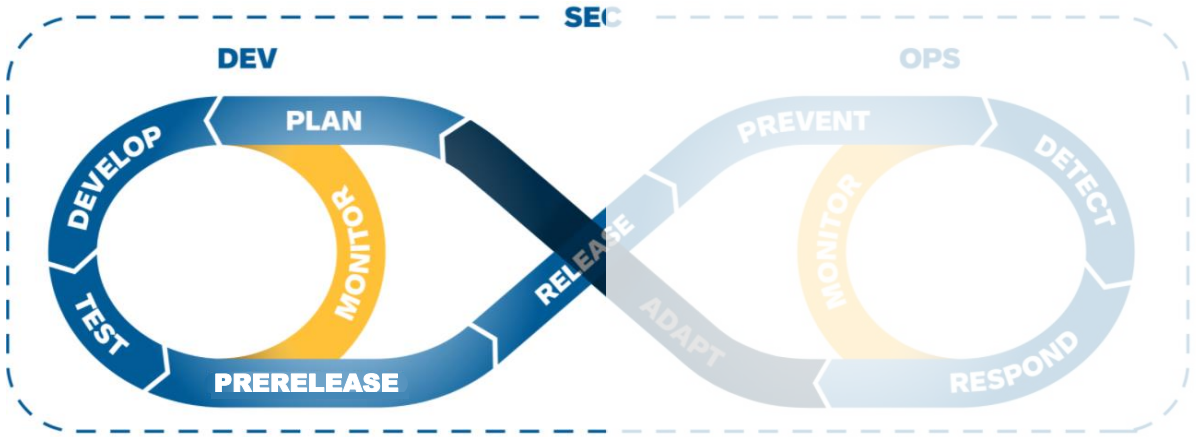
Full application security testing

SAP's secure development and operations lifecycle

Continuous improvement and development

Build securely

Secure cloud software development



Plan	Develop	Test	Prerelease	Release	Prevent	Detect	Respond	Adapt	Monitor
Training plan Release and backlog Design and requirement analysis Technical and security debt Threat modeling Data privacy impact Operations planning	Backlog development Secure coding	Testing and verification Static application security testing Dynamic application security testing Os3 Executing test strategy	Security validation development Staging activities End-to-end integration testing Stress testing	Release decision Code signing Packaging Deployment	Integrity checks Signature verification Configuration management Defense in depth measures (application, network, data centers)	Pentesting Security information and event management (SIEM) alerts and threat intelligence	Security incident management and breach notification	Adopting technical debt from the backlog Sla-driven vulnerability management	Technical logging and monitoring Backlog, process, and compliance verification
	Continuous integration and delivery (CI/CD) pipeline security	*CI/CD pipeline security*	*CI/CD pipeline security*	*CI/CD pipeline security*					

Threat modeling

Evaluating threats in the early stages

Build securely

Secure cloud software development

- Mandatory since 2018
- Required for each line of business
- Part of SAP’s secure software development and operations lifecycle
- Mitigation steps required depending on risk

Full application security testing

Dynamic and static code scanning for SAP Business Technology Platform

SAST:

- Provides white box security testing
- Scans source code
- Prevents vulnerabilities early in the security development lifecycle (SDLC)
- Is fully integrated into development process, hence highly effective vulnerability prevention.
- Can’t discover runtime and environment-related issues
- Typically supports all kinds of software

Full scan of SAP BTP source code, all programming languages used

DAST:

- Provides black box security testing
- Scans a running application
- Finds vulnerabilities in the final solution (prior to delivery)
- Ensures high-quality security validation before delivery
- Can discover runtime and environment-related issues
- Typically scans Web applications and Web services

Runtime testing of SAP BTP Web applications

Security assessment and testing

Internal and external security assessments including penetration tests

Penetration tests

- Internal and external
- Web applications (SAP BTP, SAPUI5, Web Dynpro, other)

Code scans

- Static application security testing (SAST)
- Dynamic application security testing (DAST)

Other application security testing

- Code scan
- Authorization tests end to end
- Virus scans for documents
- Other test methods

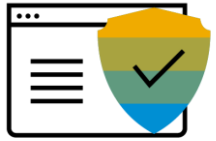
Pillars of security for SAP BTP

Security features

Build securely

Leading security, data protect, and privacy features

Secure user access and permissions



Security audit logs

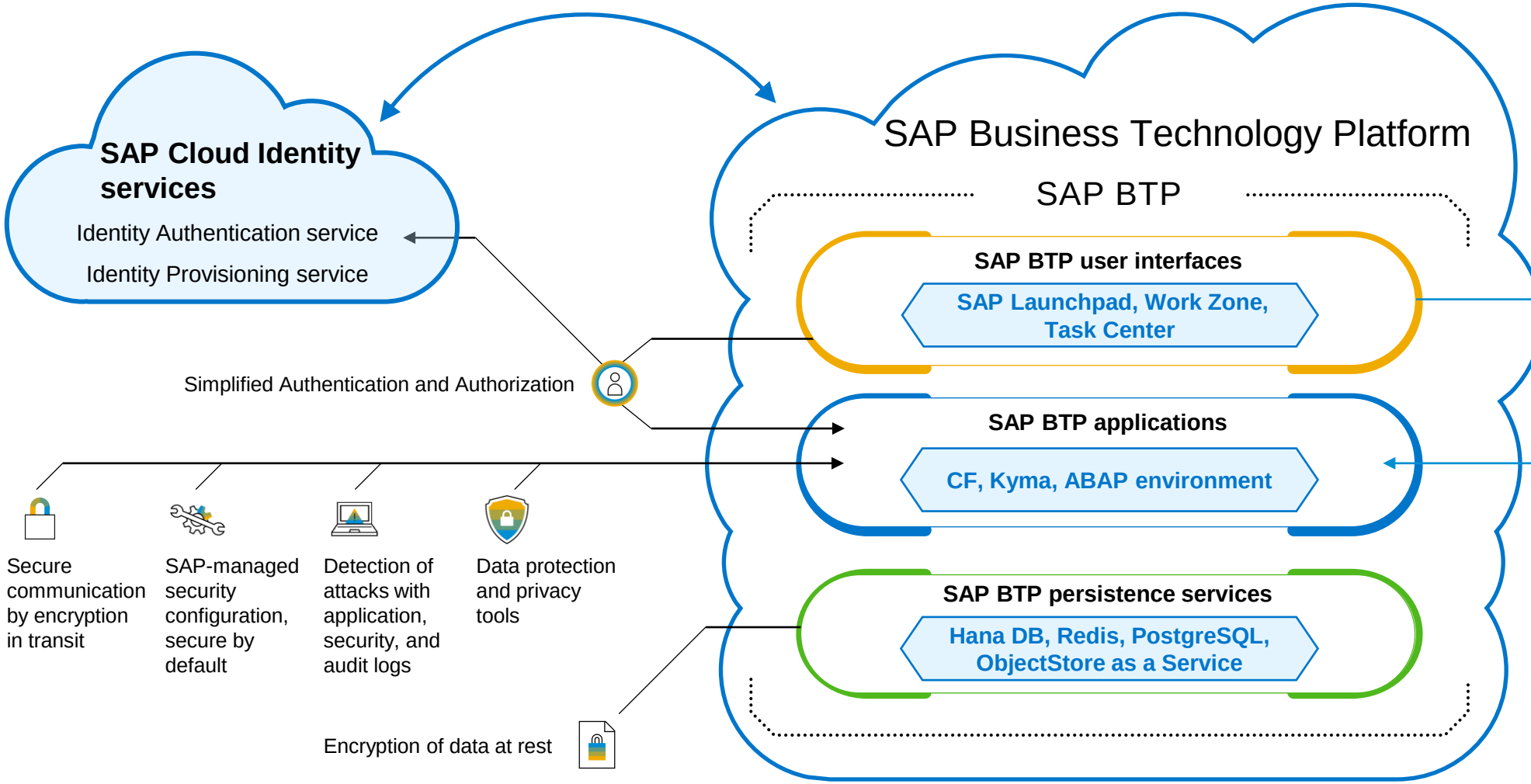
Secure communication and encryption

Security, data protection, and privacy safeguards

SAP BTP – Application layer security

Build securely

Leading security, data protect, and privacy features



Top secure SDL measures:

- Threat modeling
- Static and dynamic code scans
- Internal penetration tests
- External security assessments
- OSS vulnerability scans

Secure user access and permissions

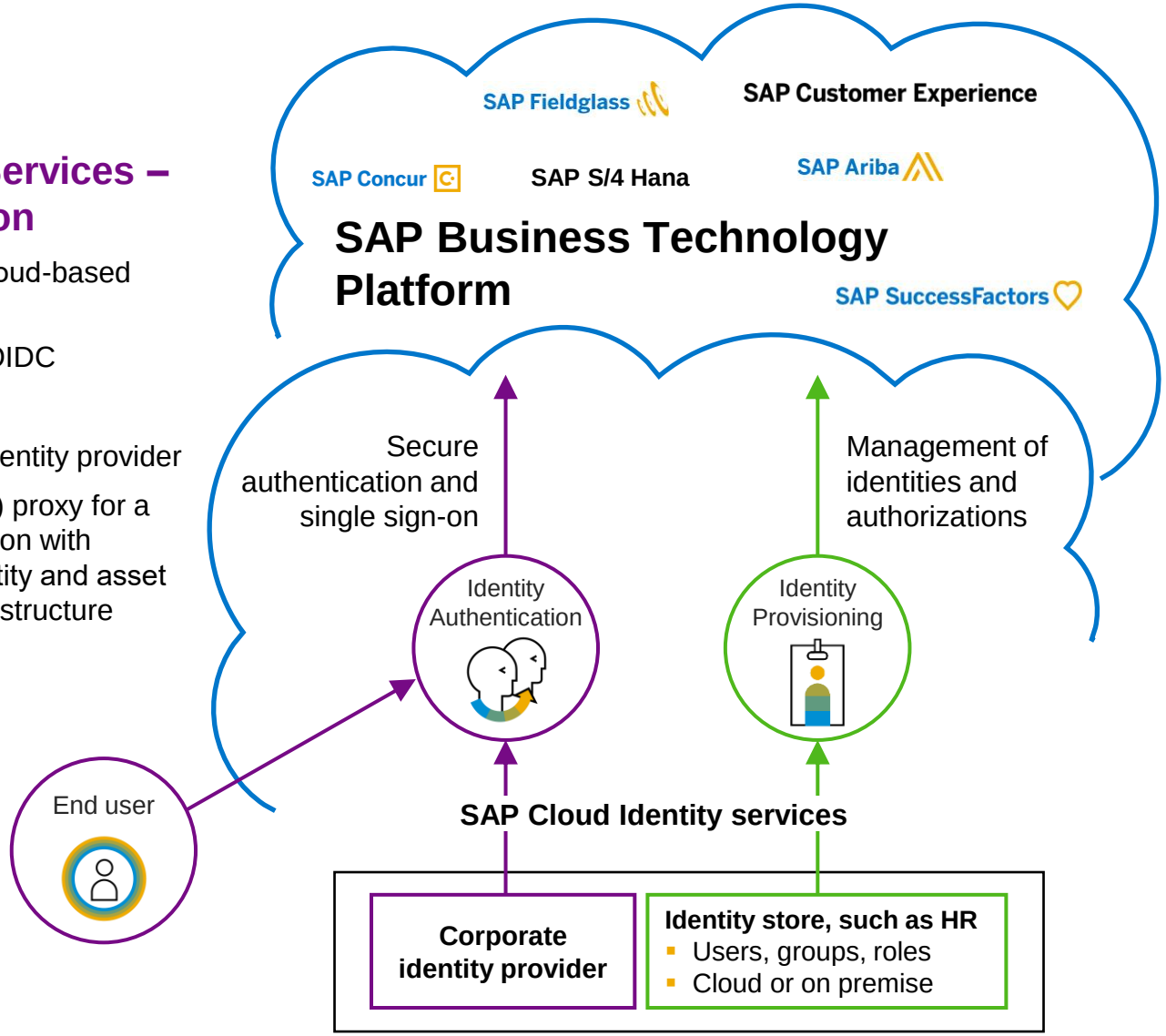
Build securely

Leading security, data protect, and privacy features

Secure access:

SAP Cloud Identity Services – Identity Authentication

- Single sign-on for SAP's cloud-based applications
- Support for X509, SAML, OIDC
- Two usage options:
  - As the landscapewide identity provider
  - As identity provider (IdP) proxy for a smooth, flexible integration with customers' existing identity and asset management (IAM) infrastructure



Managing users and permissions:

SAP Cloud Identity Services – Identity Provisioning

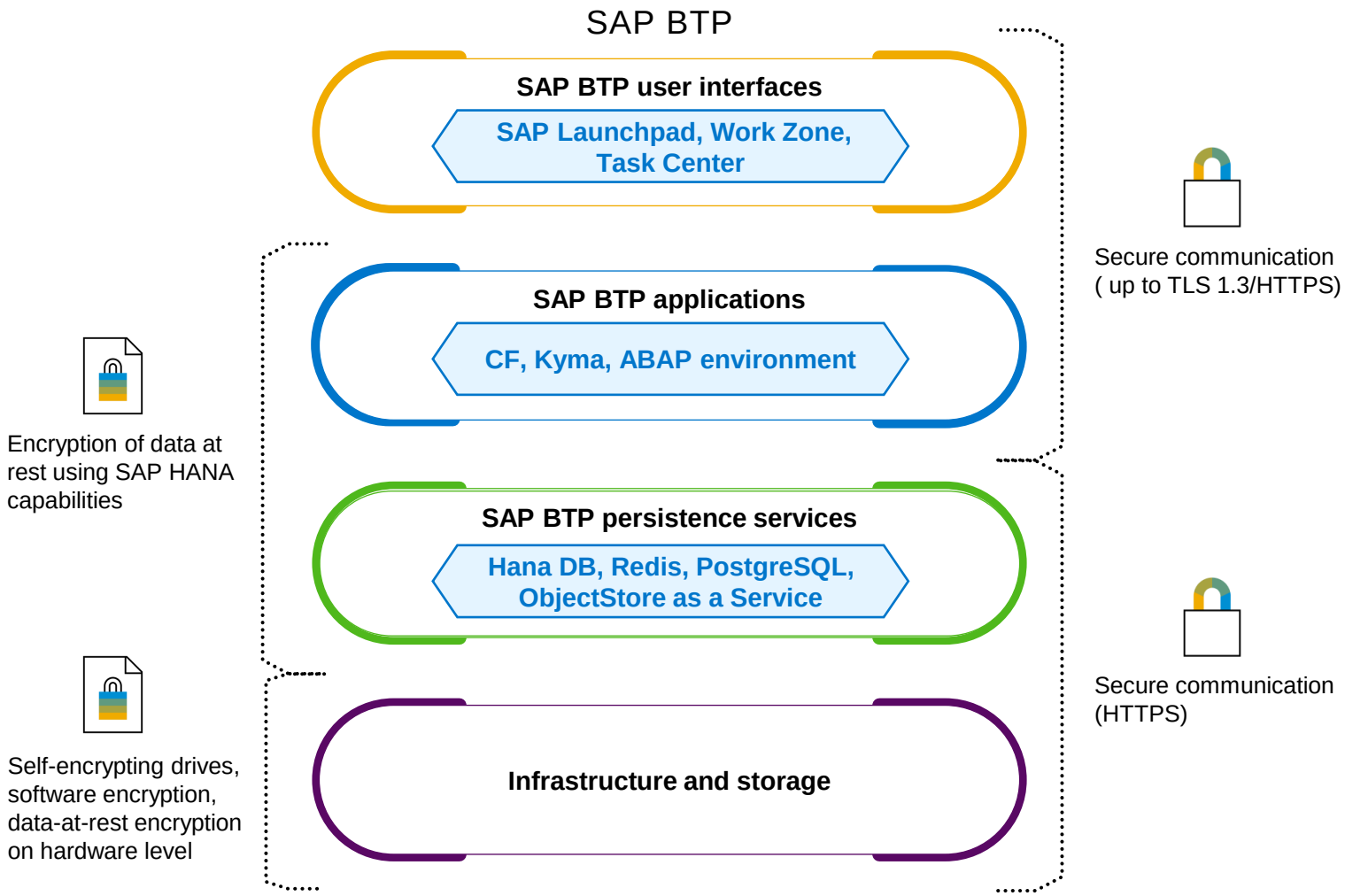
- Identity lifecycle management for cloud-based business applications
- Integrated with SAP Identity Management for hybrid landscapes and other IDM solutions
- Simple and agile onboarding of users and applications
- Dedicated connectors for third-party cloud platforms

Secure communication and encryption

Build securely

Leading security, data protect, and privacy features

- Communication protocols of SAP BTP support encryption, such as HTTPS with up to TLS1.3 and AES-256
- Data at rest encryption is provided by the storage encryption of the persistence services
- They use SAP HANA or the IaaS layer underlying the SAP BTP. This is configured in the respective IaaS accounts used by SAP BTP.
- Storage-level encryption is supported on hardware level by SAP BTP and SAP HANA



Security audit logs via the SAP Audit Log service

Build securely

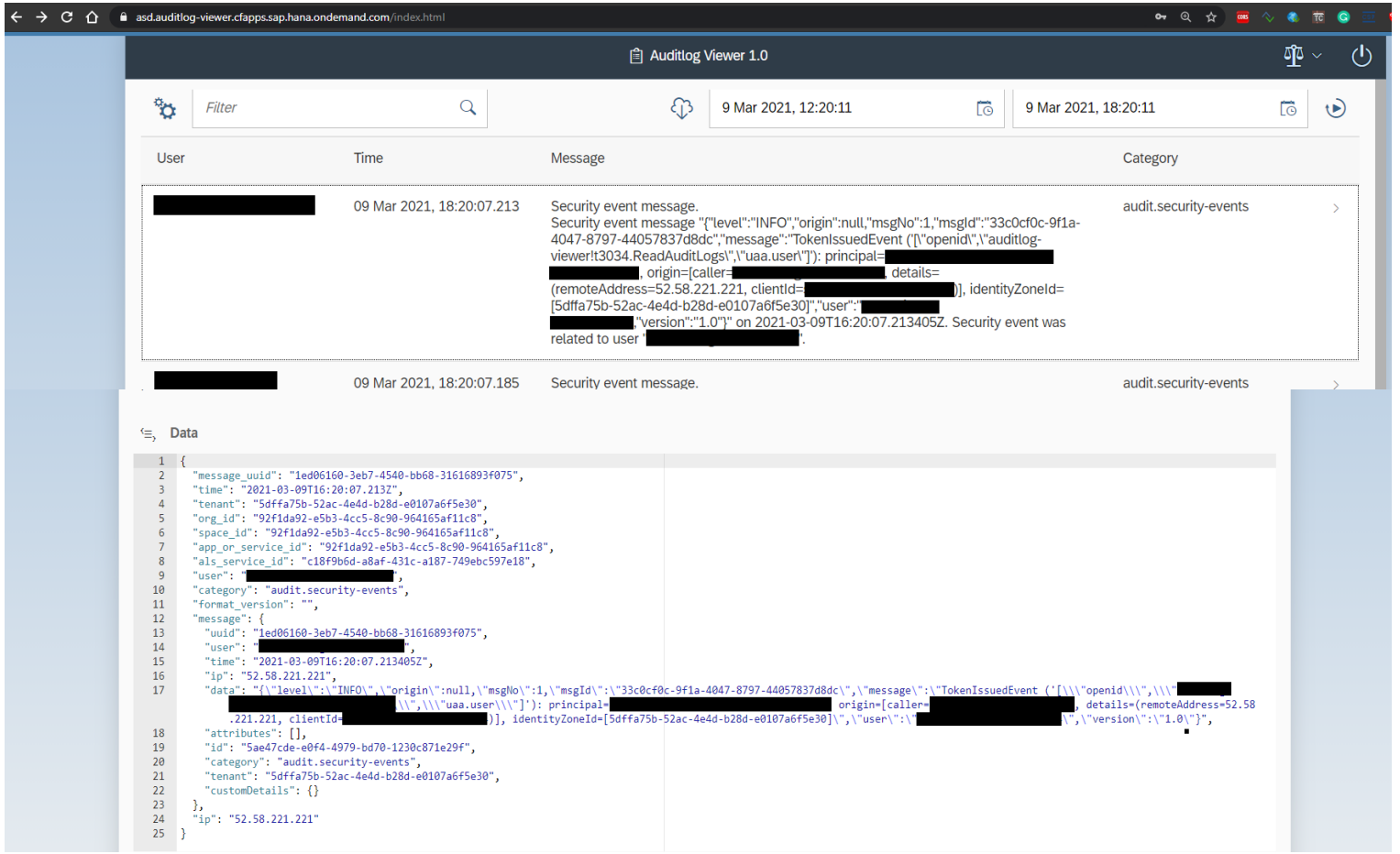
Leading security, data protect, and privacy features

Customer can review security relevant activities of customer users and SAP staff in the security audit log with

- Timestamp
- Terminal ID
- Audit log event

Security-relevant activities include, such as

- User logins
- Permission assignments or removals
- Change of Trust setups
- Subscription updates
- Change of monitoring checks



Pillars of security for SAP BTP

2. Run securely

We run cloud operations securely.

Secure operations and landscape architecture

Comprehensive contracts and audit

Areas of secure operations and landscape architecture

Secure operations

- Robust technical security architecture helping ensure
  - Network segregation
  - Data segregation
- Secure design of cloud services
- Hacking simulation (white box)
- Infrastructure vulnerability scans (monthly)
- Secure identity and access management
- Transparency of SAP access
- Backup and restore
- Disaster recovery options

Detection of attacks

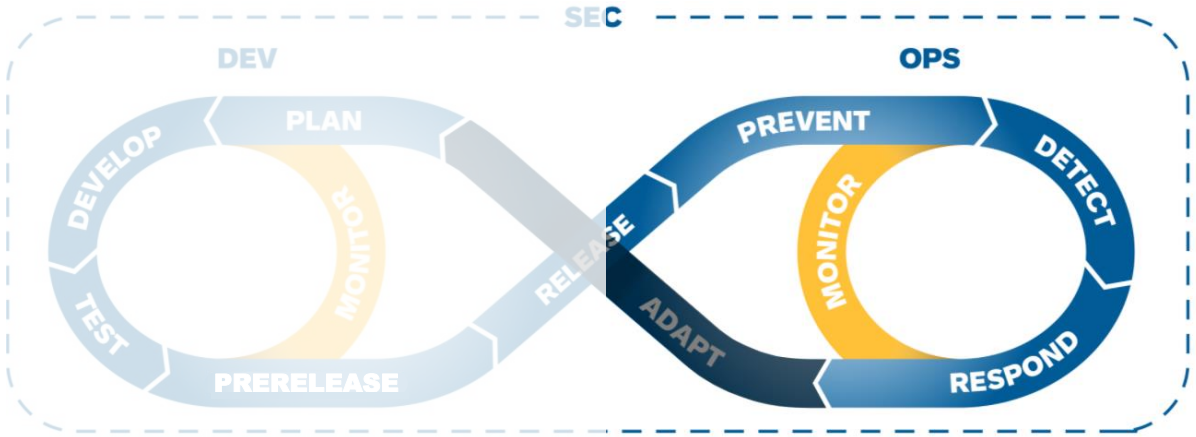
- SAP's Cyber Fusion Center
- Logging and monitoring of security events
- Automated use cases initiate alerts
- Manual extended analysis to identify sophisticated attacks
- Customer security incident process

Data center security

- Benefit from local regulations (select region of data storage)
- Physical security and network security
- Compliance, confidentiality, and integrity
- Data center on tier-level III or IV
- Low latency speeds-up access

SAP’s secure development and operations lifecycle

Continuous security monitoring and operations



Plan	Develop	Test	Prerelease	Release	Prevent	Detect	Respond	Adapt	Monitor
Training plan Release and backlog Design and requirement analysis Technical and security debt Threat modeling Data privacy impact Operations planning	Backlog development Secure coding	Testing and verification Static application security testing Dynamic application security testing Os3 Executing test strategy	Security validation development Staging activities End-to-end integration testing Stress testing	Release decision Code signing Packaging Deployment	Integrity checks Signature verification Configuration management Defense in depth measures (application, network, data centers)	Pentesting Security information and event management (SIEM) alerts and threat intelligence	Security incident management and breach notification	Adopting technical debt from the backlog Sla-driven vulnerability management	Technical logging and monitoring Backlog, process, and compliance verification
	Continuous integration and delivery (CI/CD) pipeline security	*CI/CD pipeline security*	*CI/CD pipeline security*	*CI/CD pipeline security*					

Incident Response and Disaster Recovery

- High Availability : Multi-AZ enabled Platform Services
- Standard DR: Restore from offsite backups

- Reduced planned downtimes
- Harmonized maintenance windows across SAP Cloud products

- Meaningful outage communication
- Real time status reporting

- Canary approach: ‘Eat your own dog food’.
- Pro-active & re-active monitoring
- 24/7 Operations & Incident Management, RCA & Improvements

Comprehensive contracts and independent audits

Service-level agreements

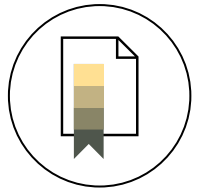
Technical and organizational measures

Independent audits, certifications, and attestations

Security framework description

Applicable local regulations globally

Compliance with Industry Standards and Regulations



Run securely

Secure operations and Landscape architecture

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 Cloud 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

Infrastructure with 99.9% availability

For more details, see

- SAP Data Center
- SAP Trust Center
- Cloud Availability section in SAP for Me
- Service level agreement for SAP Cloud Services

Certifications & Attestations

- ISO 27001 Cert. for Information Security Management Systems
- ISO 22301 Business Continuity Management
- SOC 1 SSAE 18, SOC 2 Type 2
- TISAX Trusted Information Security Assessment Exchange
- FSTEC Federal Service for Technical and Export Control
- C5 (BSI Germany)
- PCI-DSS

Pillars of security for SAP BTP

3. Act securely

We foster a security-first culture in everything we do.

Our employees

Security is foundational to how we organize and run our business, train our employees, and protect people and assets.

Our customers

We partner with customers for continuous feedback and improvement to address evolving security needs.

Our partners

We partner with members of our extensive ecosystem to improve security.

Security is part of our DNA

Act securely

Our employees

Employee preparation:

- Global awareness
- Role-based training

Protection of people and assets:

- Threat-modeling training
- Interconnected physical and cybersecurity

Partnership with customers for continuous feedback and improvement

Customer advisory board

SAP Customer Connection program

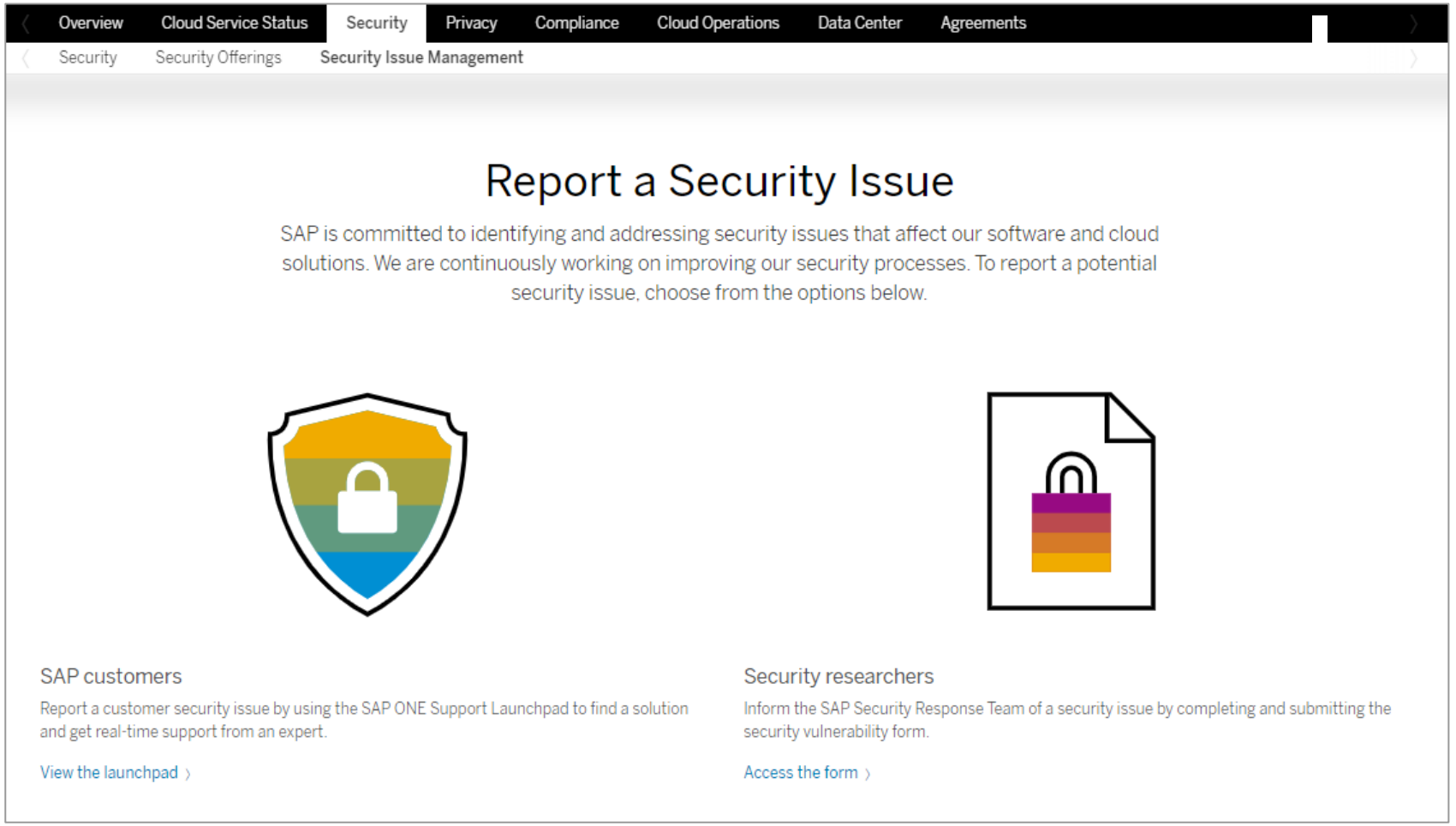
SAP Continuous Influence program

Reporting of security incidents

Proven way for SAP customers and SAP researchers

Act securely

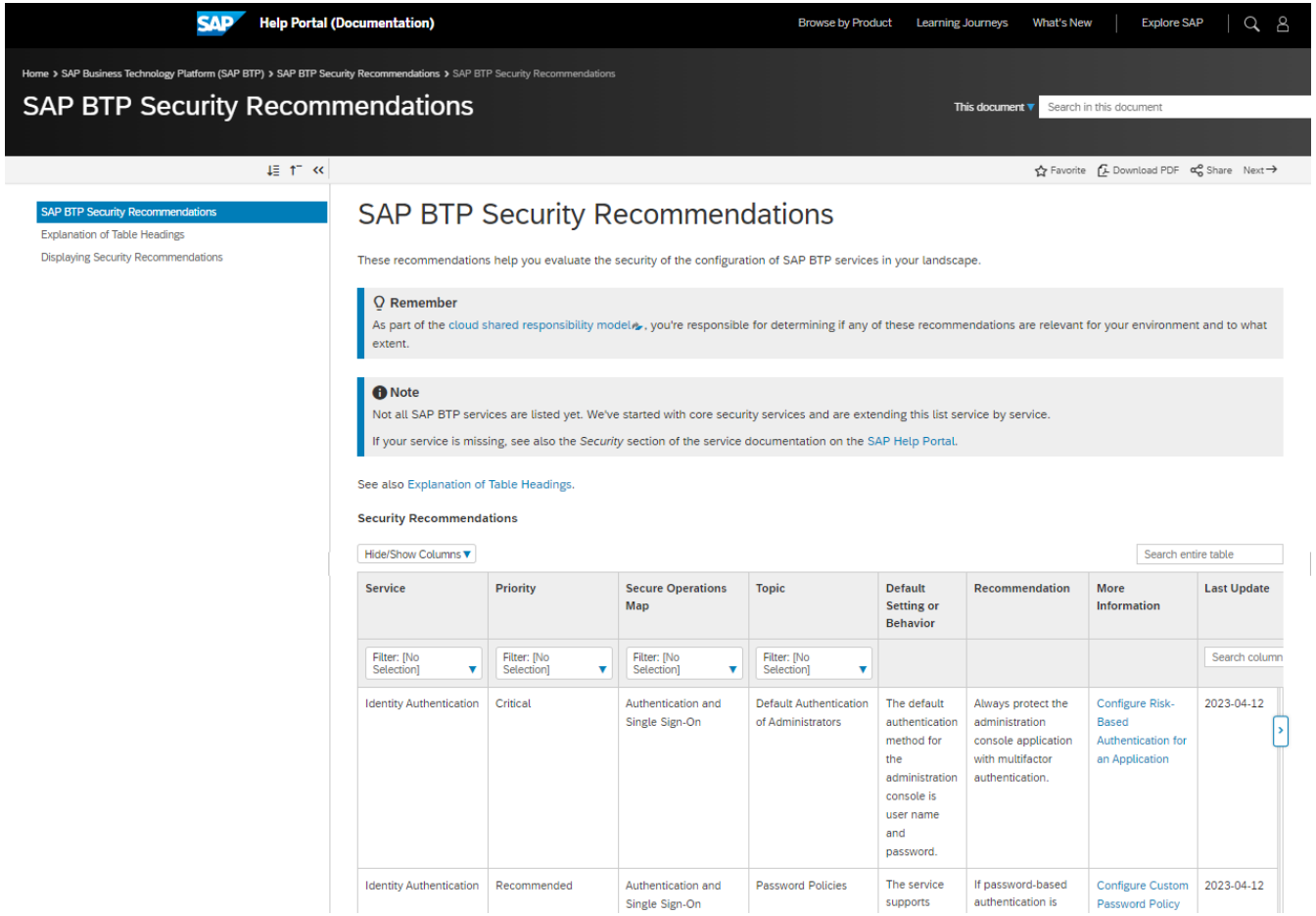
Our customers



www.sap.com/about/trust-center/security/incident-management.html

Security Recommendations

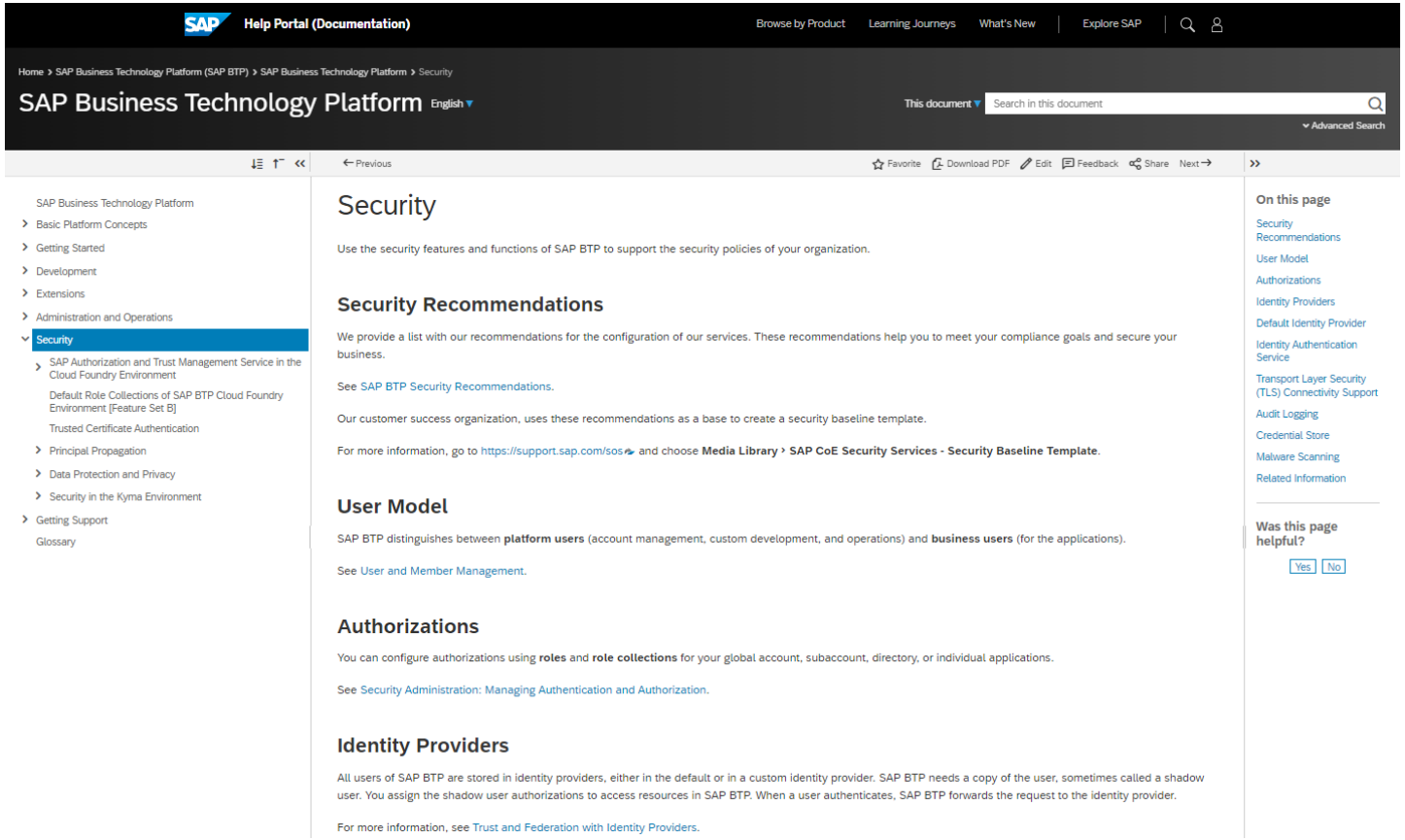
Setting up SAP BTP in the cloud securely



[Help Portal: SAP BTP Security Recommendations]

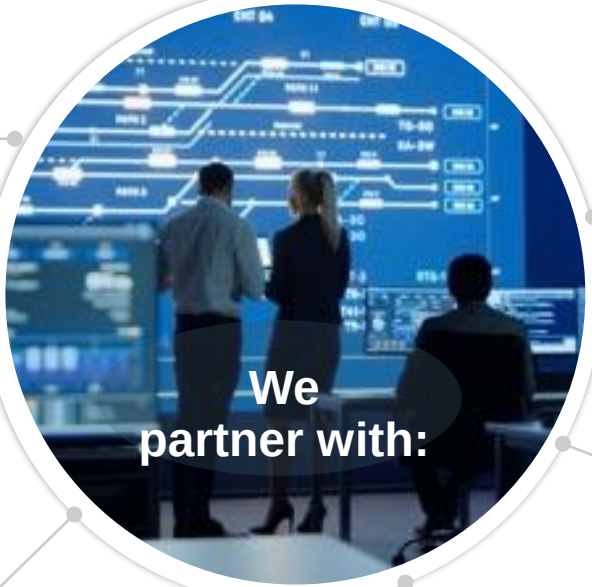
Protect Your SAP BTP environment

Learn about SAP BTP security



[Help Portal: SAP BTP Security]

Ecosystem Partnerships for Enhanced Security



Cloud service providers
Optimized environments with multiple deployment options

Security researchers
Collaborate to improve security posture and readiness

Private / Public partnerships
Bridging the cyber skills gap

System integrators
Vast network of security advisors

Technology partners
Leverage leading technologies to enhance security

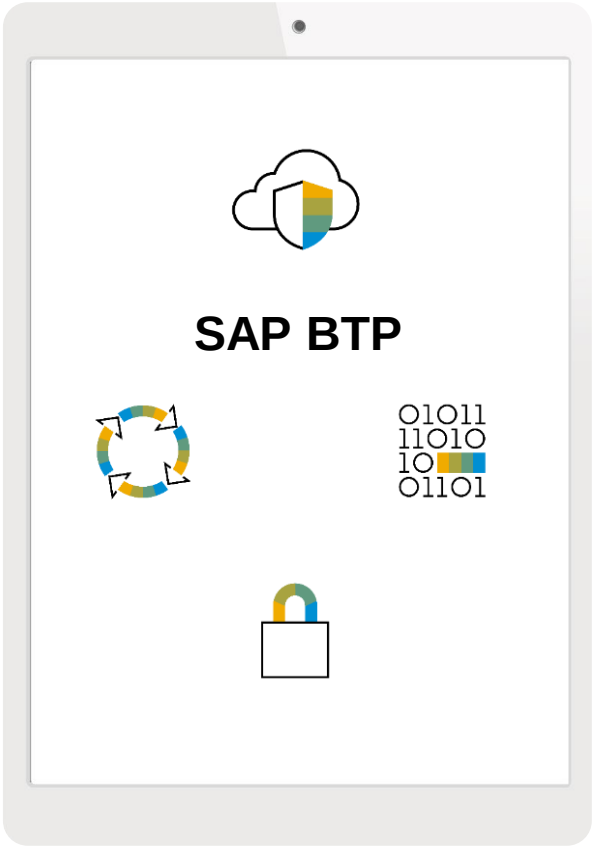
Software vendors
+ 500 Partner solutions available on SAP store

Three key messages to take away

Security and compliance are key capabilities of SAP BTP, approached holistically and from end to end.

SAP BTP is developed securely with built-in state-of-the-art security features and privacy capabilities.

SAP BTP Cloud operations adhere to and go beyond leading industry standards in technology, operative, and legal measures.



Further information

SAP Help Portal
SAP BTP – Documentation including security

Secure software development
White paper: The Secure Software Development Lifecycle at SAP

SAP Trust Center
Certifications and attestations
www.sap.com/about/trust-center/certification-compliance.html

Related SAP TechEd presentations
SEC205 – A Holistic Approach to GDPR and CCPA Helps Purpose-Driven Data Protection
https://events.sap.com/teched/en/session/48835

SEC200 – How to Run Identity and Access Management for the Intelligent Enterprise
https://events.sap.com/teched/en/session/51531

Security related customer content
Cloud Services: Reference Guide
Guide to Customer Content

Thank you.

Contact information:

Jürgen Adolf
juergen.adolf@sap.com

© 2023 SAP SE or an SAP affiliate company. All rights reserved. See Legal Notice on www.sap.com/legal-notice for use terms, disclaimers, disclosures, or restrictions related to SAP Materials for general audiences.