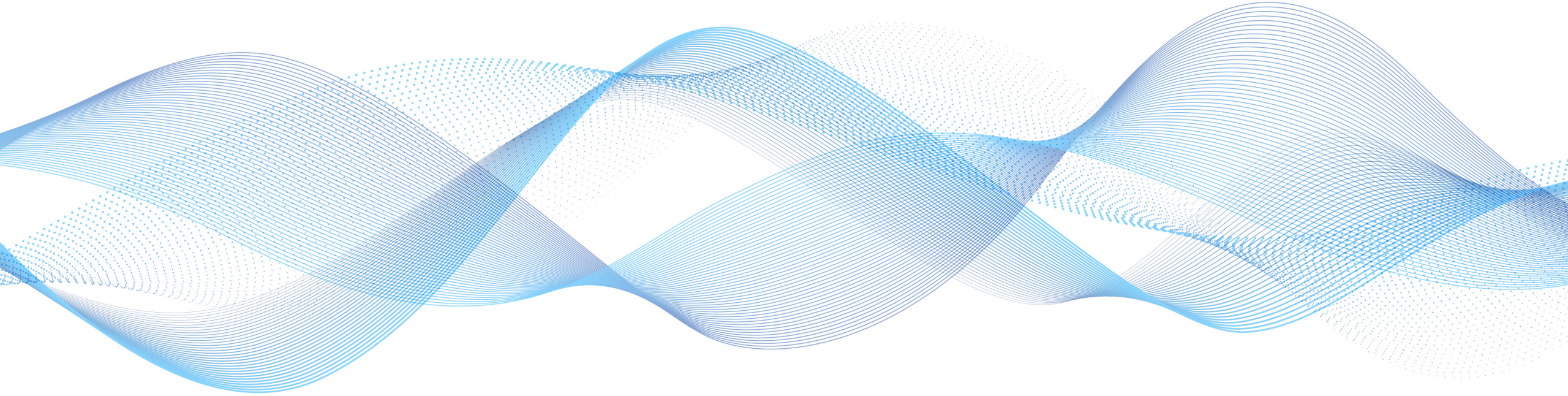


SAP HANA Cloud | Deep Dive
Security

SAP HANA Product Management

Public

Last updated: 12.06.2023

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.

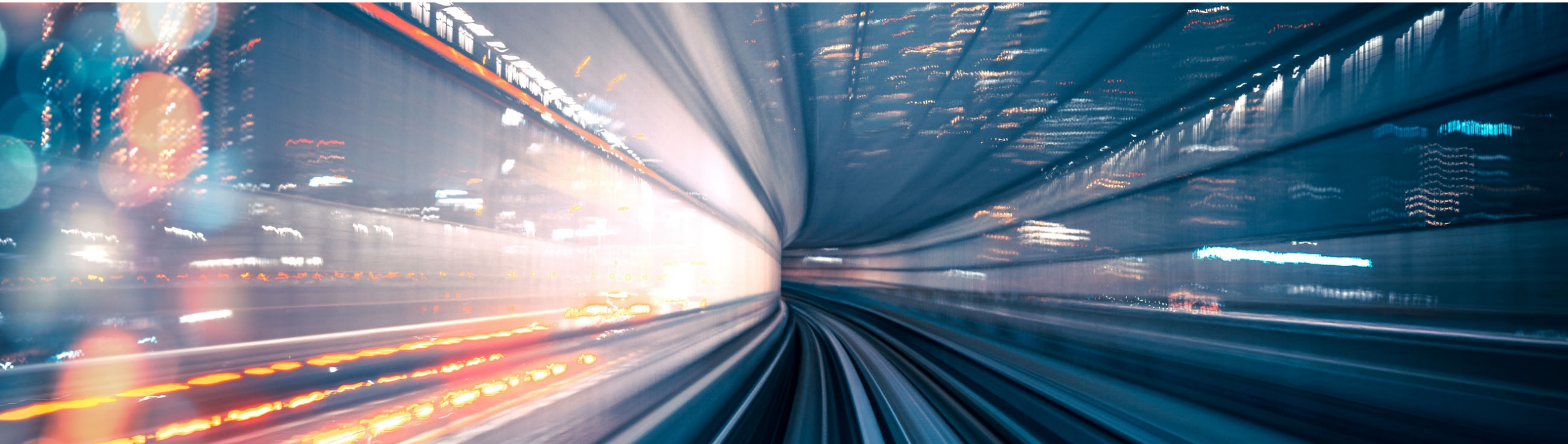
This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, 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 HANA Cloud | Deep Dive Security

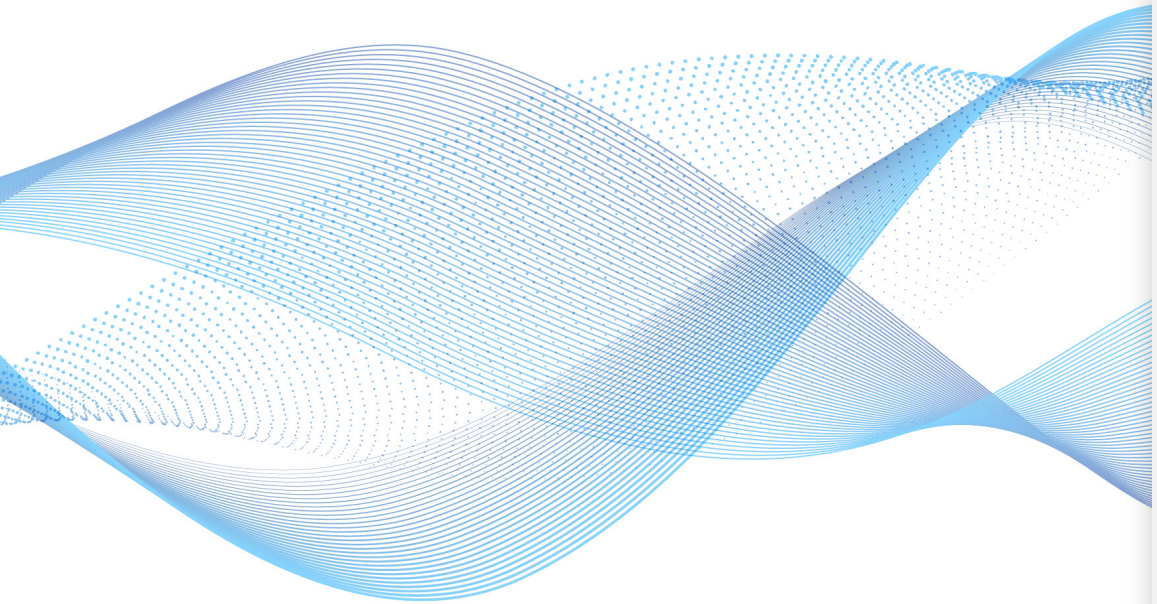
- SAP HANA Cloud Security Approach
- Secure Data and Applications
- Auditing
- Data Privacy
- Secure Development, Operations & Compliance
- Key takeaways
- Take The Next Step

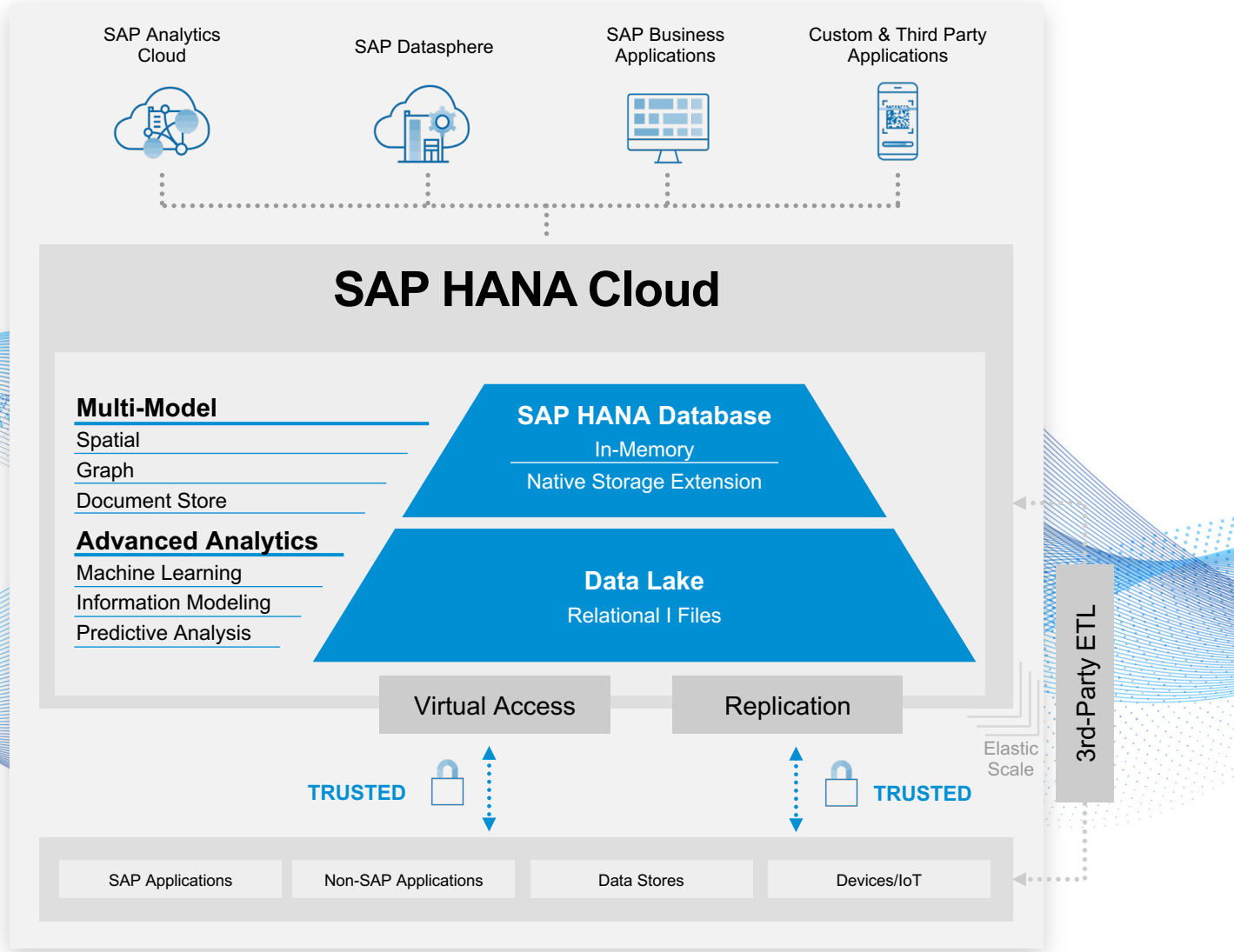
SAP HANA Cloud Security Approach



SAP HANA Cloud

Power **Intelligent Data Applications** with SAP HANA Cloud

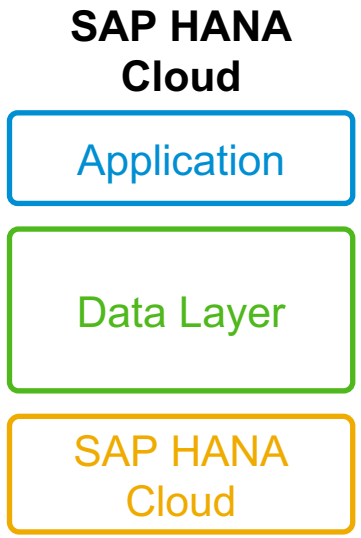




SAP HANA Cloud Security | Shared Responsibility Framework

Customer

controls data access security

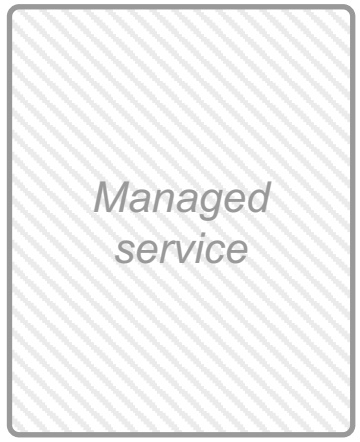


User management & authentication
Authorization
Encryption key management
Masking
Anonymization
Auditing

SAP

manages system and infrastructure security – hardening and secure operations

Certified to most common security standardization (e.g. ISO/SOC)



Secure operations
Encryption
System auditing

SAP HANA Cloud | Holistic security framework

Authentication and user management

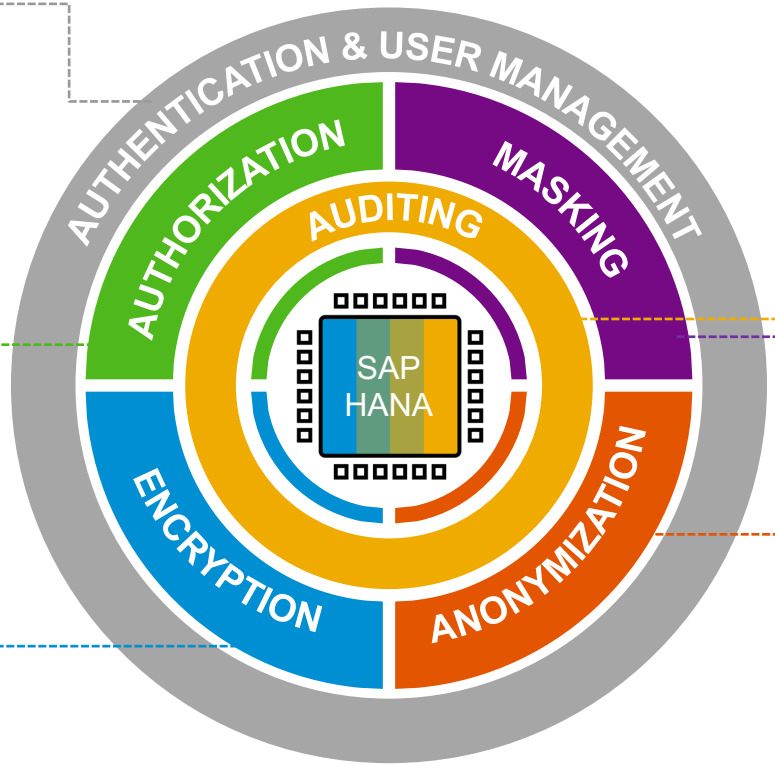
- User and identity management
- Single sign-on (SAML, JWT, X509)
- Identity Access Governance (IAG) and Identity Management (IDM) integration
- LDAP integration
- Password policies per user group

Authorization

- Role management framework
- Privileges for all user types
- Row-level access control
- Integrated application authorizations
- Authorization troubleshooting

Encryption

- At rest and in motion
- Backup encryption
- Key management



Auditing

- Security logging and analysis for all system events, with customizable policies
- Log read and write access to critical data
- Firefighter logging
- Audit retention policies, audit policy wizard
- Comprehensive logging for cloud operator actions

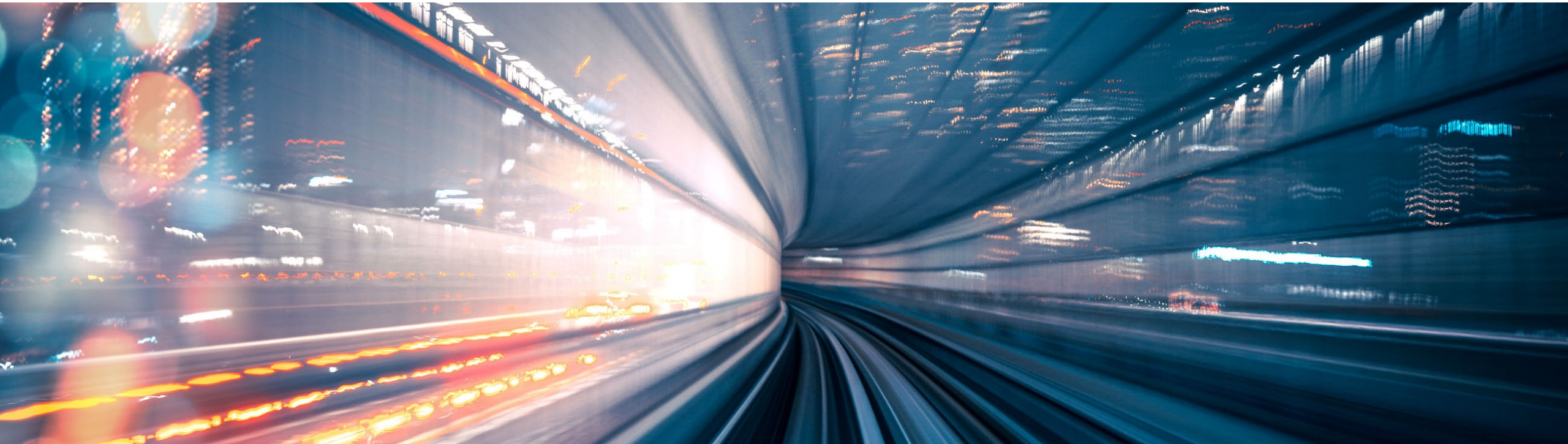
Masking

- Dynamic data masking
- for tables and views
- Custom mask expressions

Anonymization

- Real-time data anonymization
- k-anonymity (including l diversity), differential privacy
- Custom definition of anonymization views (calculation and SQL views)
- Full integration with authorization framework
- Reporting
- Data anonymization KPIs

Secure Data and Applications



Authentication | A closer look at users and how they are authenticated

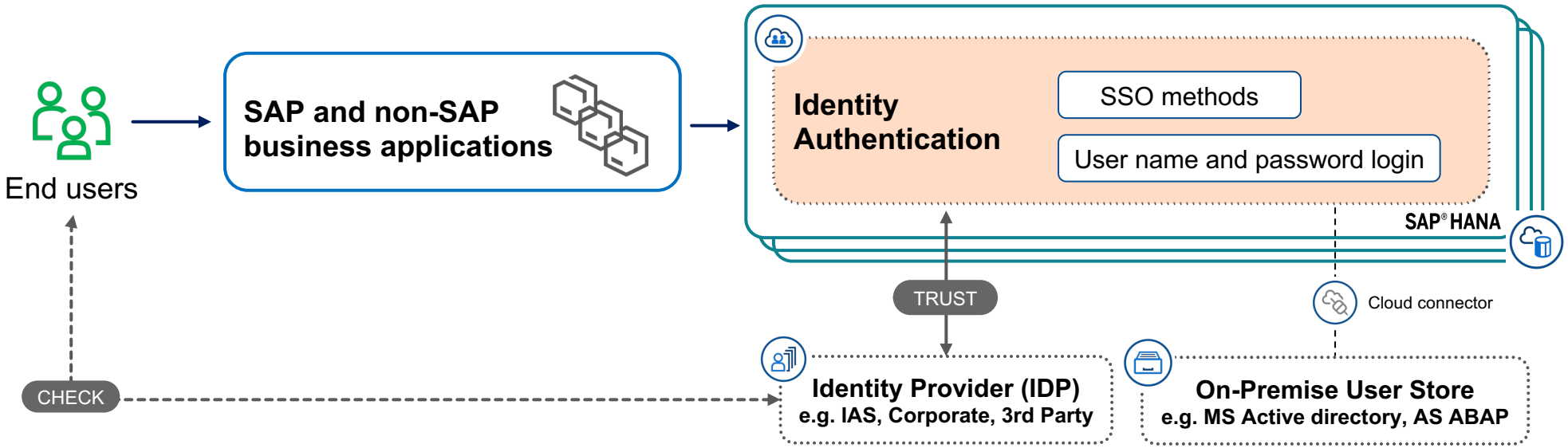
- All access to data and functions requires **authentication**
- Authentication options are **configurable per user**

User name and password login

- No default passwords!
- Customizable password policy (per user group)
- Through LDAP directory server (HANA Database, HANA Data Lake)

Single sign-on (SSO)

- JWT (SAP HANA Cloud, SAP HANA database & data lake)
- SAML (SAP HANA Cloud, SAP HANA database)
- X.509 Certificate-based (SAP HANA Cloud, SAP HANA database)



Authentication | JWT SSO in HANA Cloud Data Lake

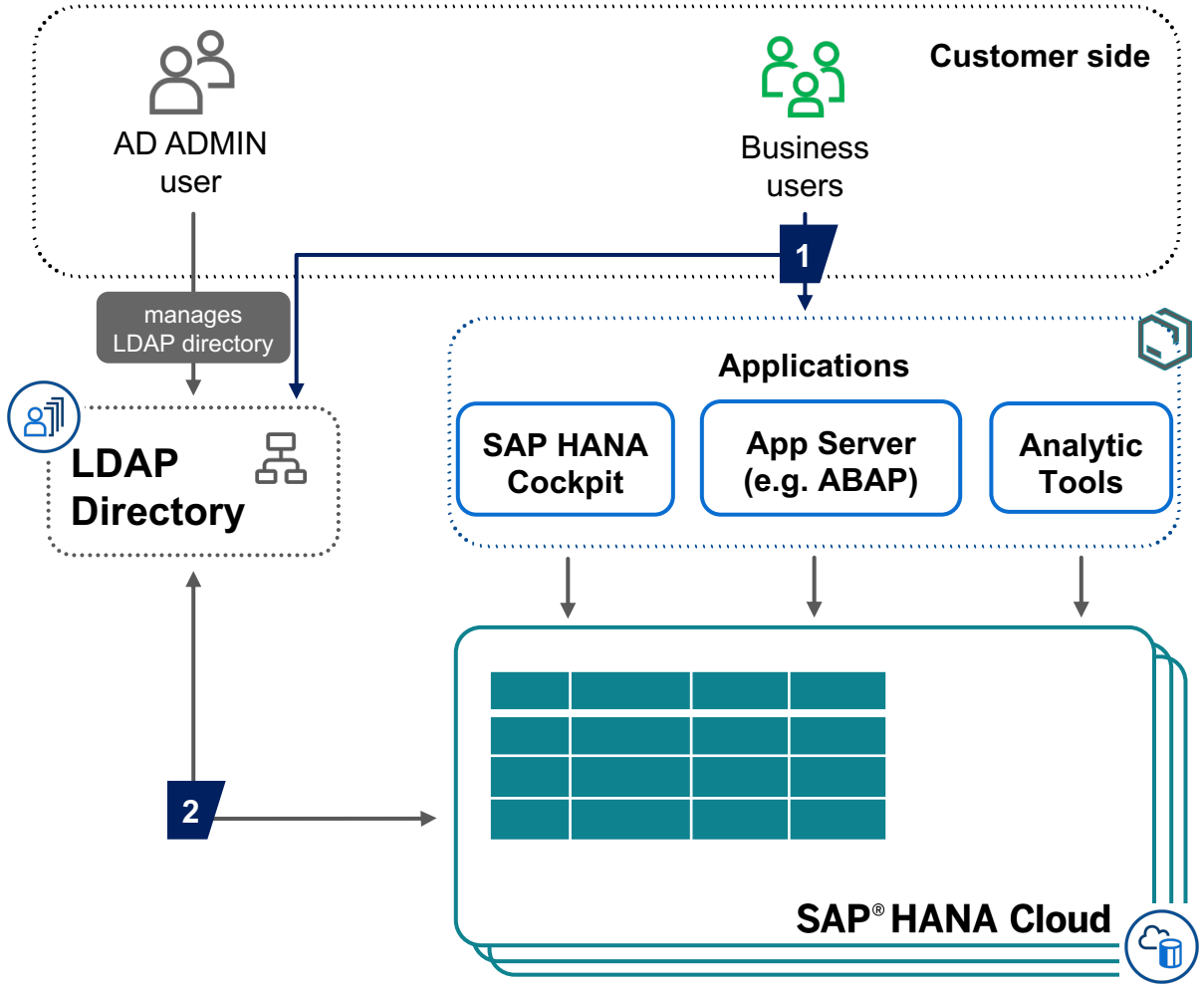
JWT Authentication Workflow

1. Users who have the JWT authentication enabled already can directly login to the application
2. Customer Admin must configure JWT authentication by executing provided *DDL commands in SQL console

- DDLs are provided to create/alter/drop a trust relationship with an external identity provider (IdP) via certificates.
- DDLs provide a mapping of external users and database users.
- Options and login-policies are extended to support JWT similarly to how Kerberos, etc. are done.
- Allows for mapping the IdP-users to database-users

*DDL – Data Definition Language

Authentication & Authorization | Central LDAP User Management



1. Authenticate the user against an LDAP directory server using the user name and password provided by the client

2. Synchronization of users and roles between external LDAP user directory and the SAP HANA user base

Secure Data and Applications | User Management & Authorization

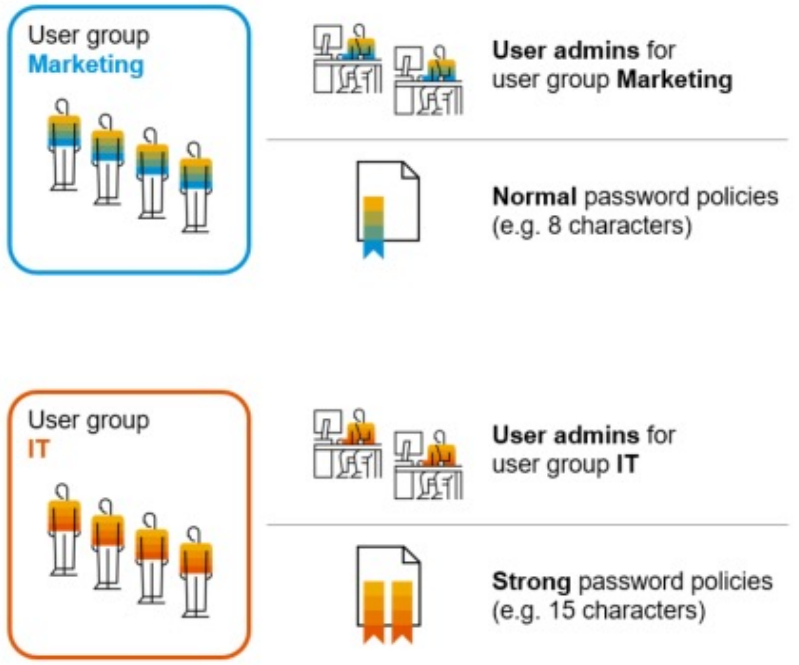
User groups and password policies

For HANA database:

- Manage related users together and assign user group-specific policies
- Manage attached SAP HANA Cloud, data lake schema and data access authorizations
- Configure group-specific values for the individual parameters of the password policy in the definition of the user groups
- The user **DBADMIN** is the user administrator of the user group ‘DEFAULT’

For standalone Data Lake Relational Engine:

- The user **HDLADMIN** is the user administrator

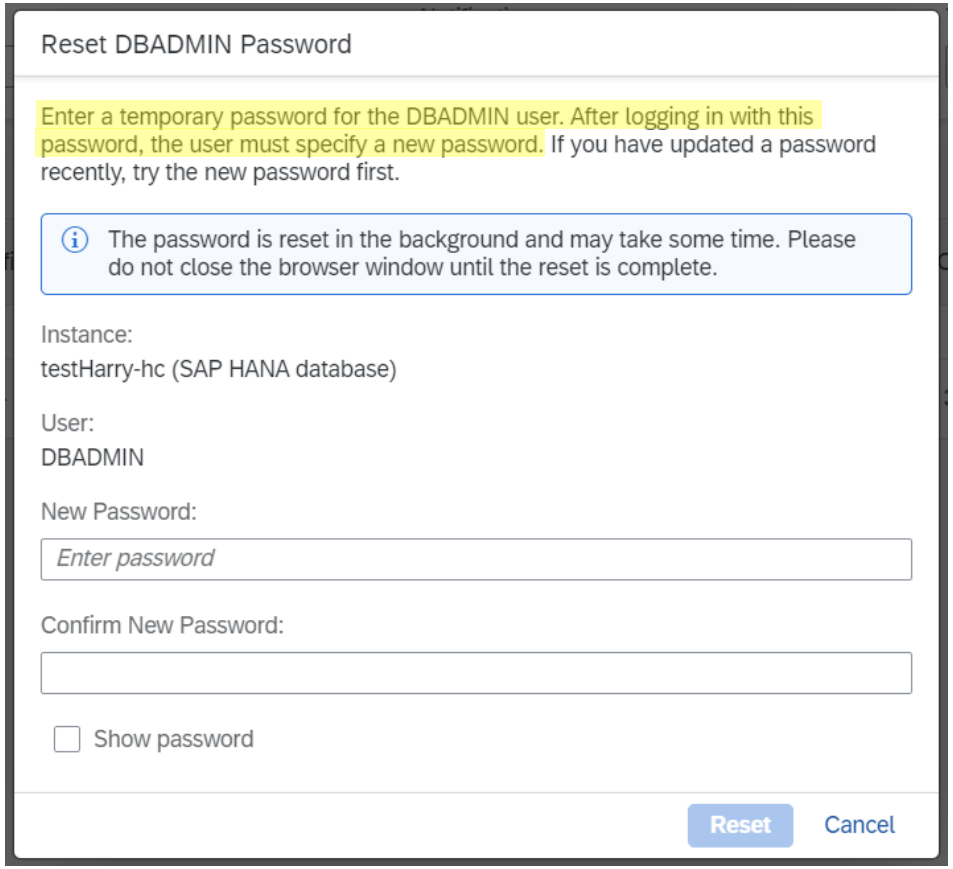


By default the DBADMIN/HDLADMIN passwords expire **after 180 days**

DBADMIN/HDLADMIN is an initial superuser for administrative tasks and **should be deactivated** once customer own admin users are created

Secure Data and Applications | User Management & Authorization
Self-Service: Reset the Administrator User's Password

- Reset the SAP HANA Cloud, SAP HANA database (DBADMIN) or SAP HANA Cloud, data lake (HDLADMIN) administrator user password via new Actions menu item in SAP HANA Cloud Central
  - No longer need to open ticket to reset the password
  - Improves user experience and availability
  - Database user needs the role 'SAP HANA Cloud Security Administrator'
  - When resetting the password:
    - For SAP HANA database, you must *first provide a temporary password that you change the next time you login*
    - For data lake, no need for a temporary password



Secure Data and Applications | Authorization & Roles

Use roles to assign authorizations to users

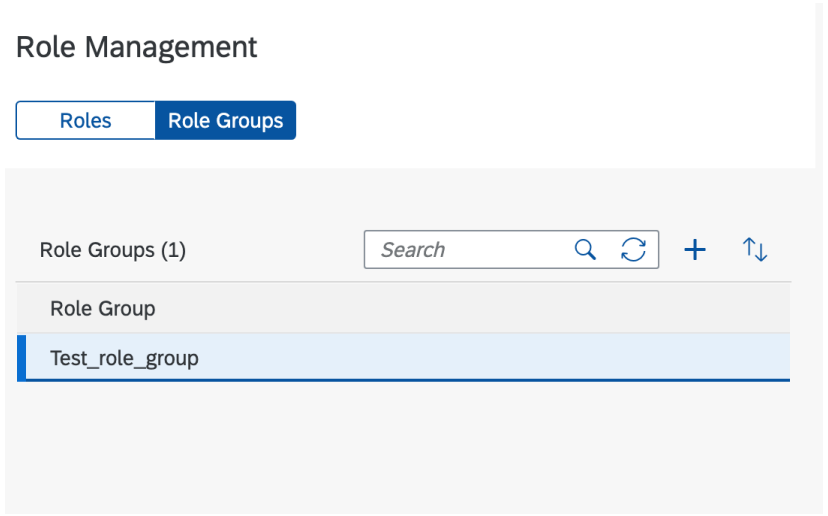
- Roles bundle and structure privileges
- HDI roles and catalog roles available
- Cloud Foundry roles (Space Manager, Space Developer, Space Auditor)

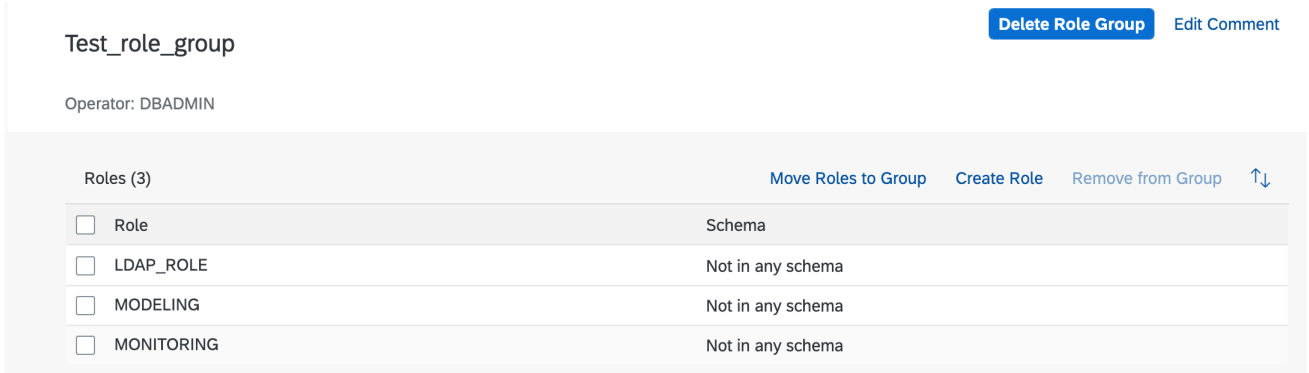
Roles in the SAP HANA database can exist as:

- **Catalog roles** are runtime objects. They are created with the CREATE ROLE statement or in the SAP HANA cockpit and can be managed using role groups.
- **Design-time roles** are design-time objects that become catalog objects on deployment database artifact with file suffix .hdbrole). They can can be created using the SAP Business Application Studio (BAS) and deployed using SAP HANA deployment infrastructure (SAP HANA DI, or HDI).

Secure Data and Applications | Authorization based on Role Groups

- Role groups support a separation of role management tasks.
- This is useful if you want different aspects of your authorization setup managed by different administrators.
- In an SAP HANA Cloud environment, SAP uses role groups to separate the management of **customer-owned roles** and **SAP-owned roles** and therefore the authorization on underlying objects.
- Roles can be assigned to a role group on creation or at a later time using the **SET ROLEGROUP** option of the **CREATE ROLE or ALTER ROLE** statements.





Secure Data and Applications | Authorization & Access control

A role can contain any number of the following privileges:

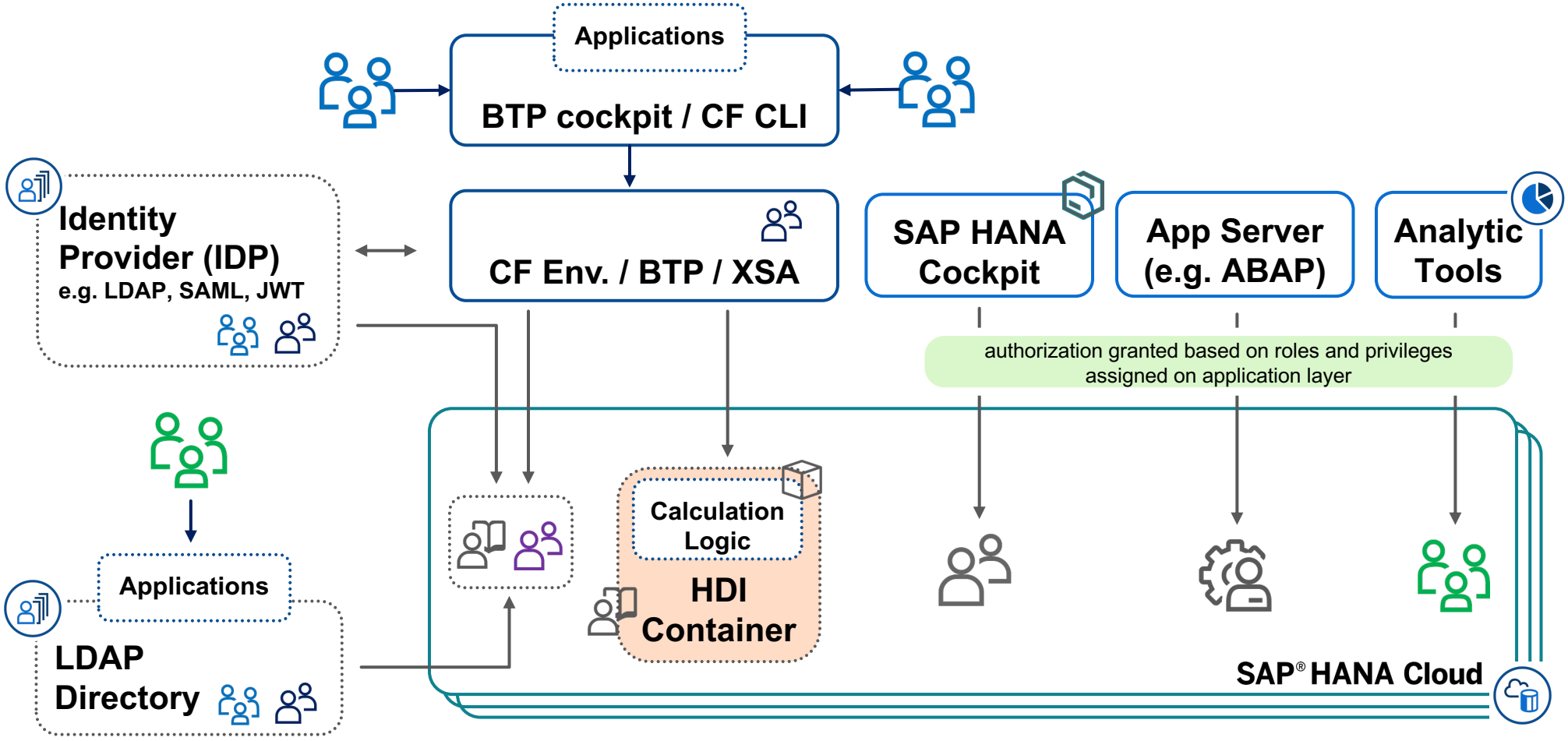
- System privileges for general system authorization, in particular administration activities
- Object privileges (for example, SELECT, INSERT, UPDATE) on database objects (for example, schemas, tables, views, procedures, and sequences)
- Analytic privileges on SAP HANA information models

A role can also contain other roles.

Use row-level access control for:

- Automatic data filtering based on group, role and application
- Added flexibility with predicated privileges to enforce row level privileges
- Combining Predicates From Multiple Grants for
  - same table access
  - different sets of column
  - different access
- Analytic privileges extend standard SQL privileges
- **Example** – Only show accounts belonging to a certain Sales region to respective Sales Managers

Authorization | A closer look at users and how they are authorized



Business Users
Administrators

have

XSA
Scopes, attributes
Roles, role collections

End users
HANA administrators
Tech users
HANA internal users
Infrastructure users

have

HANA
Privileges
Roles

Secure Data and Applications | Comprehensive Encryption

Managed by SAP

Communication encryption

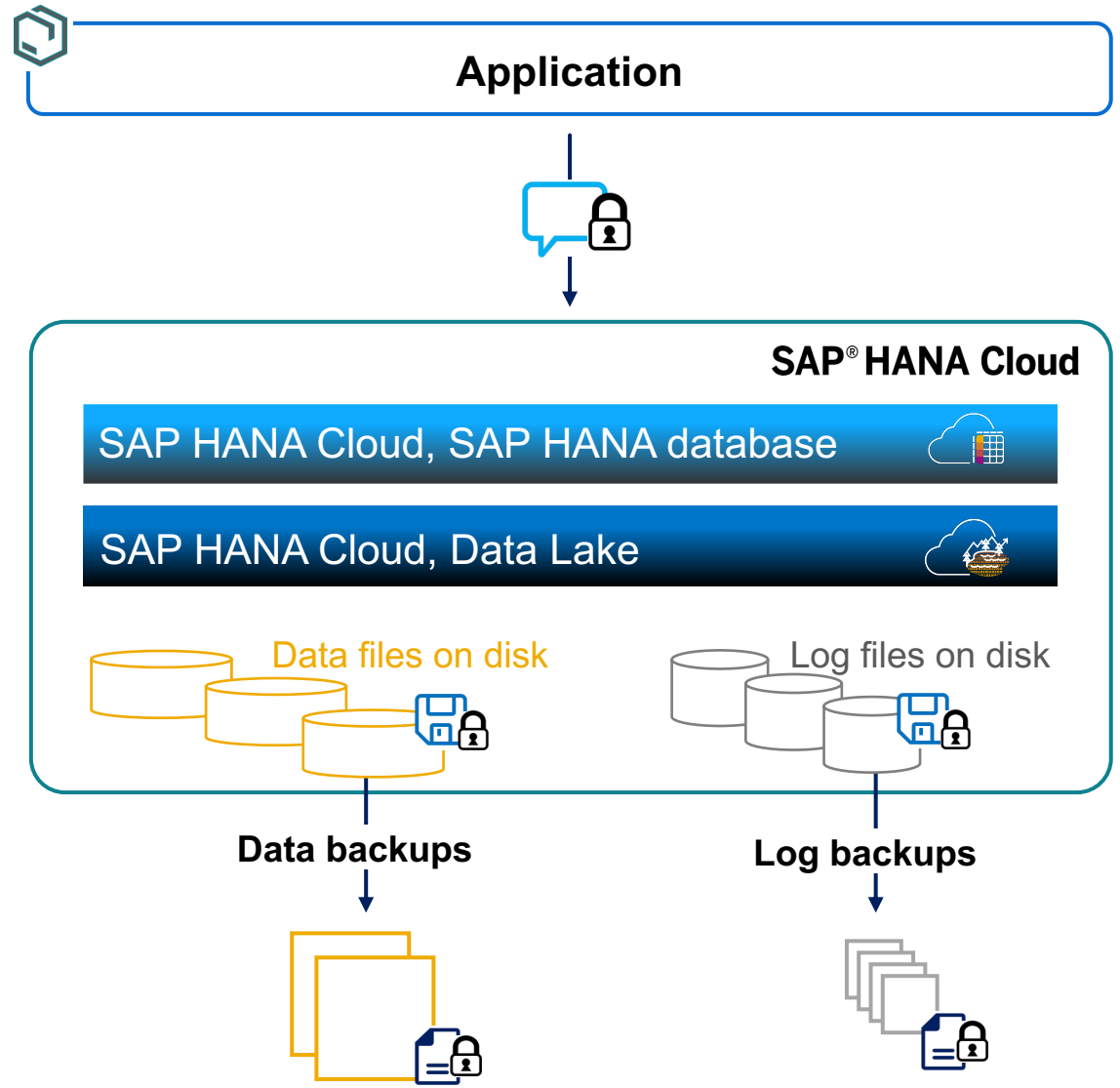
Encrypt data in transit using TLS

Data at rest encryption

Encrypt data stored on disk using data volume encryption and log encryption

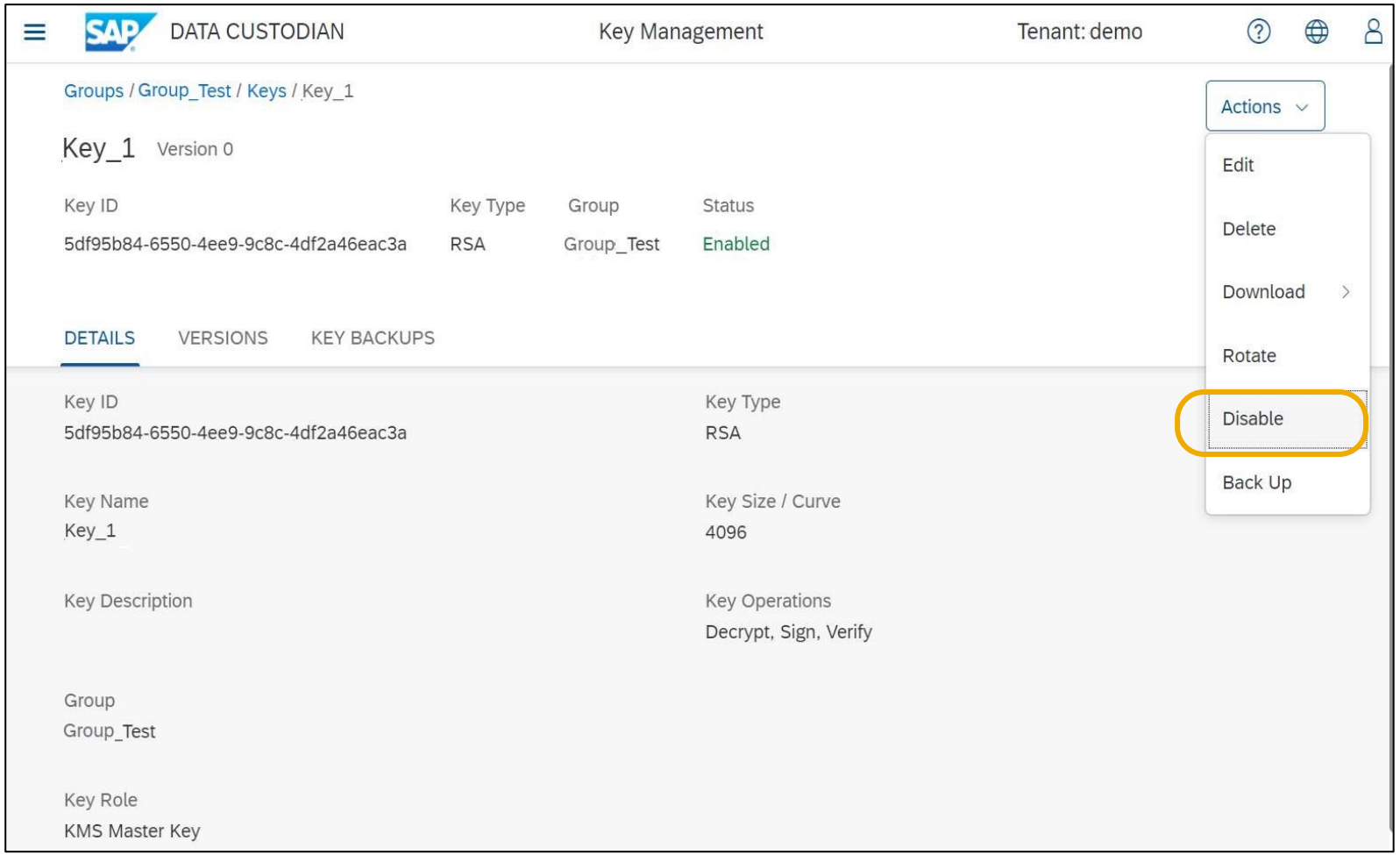
Backup encryption

Encrypt backups with SAP HANA native functionality



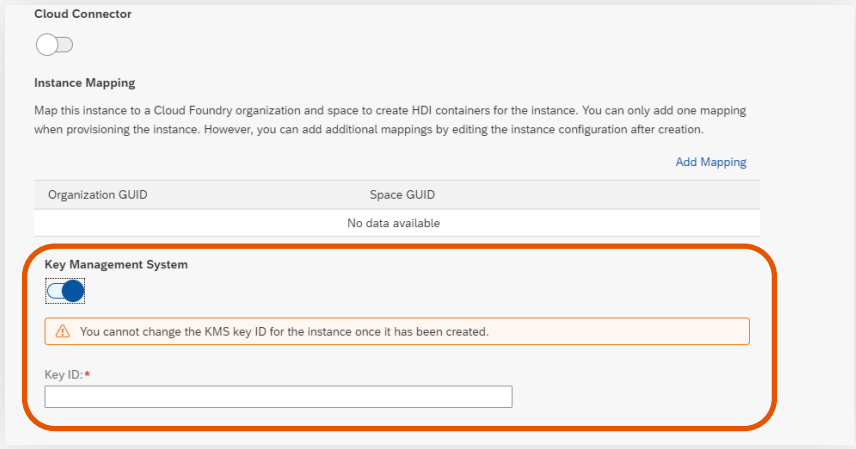
CMK | Key Management in SAP Data Custodian

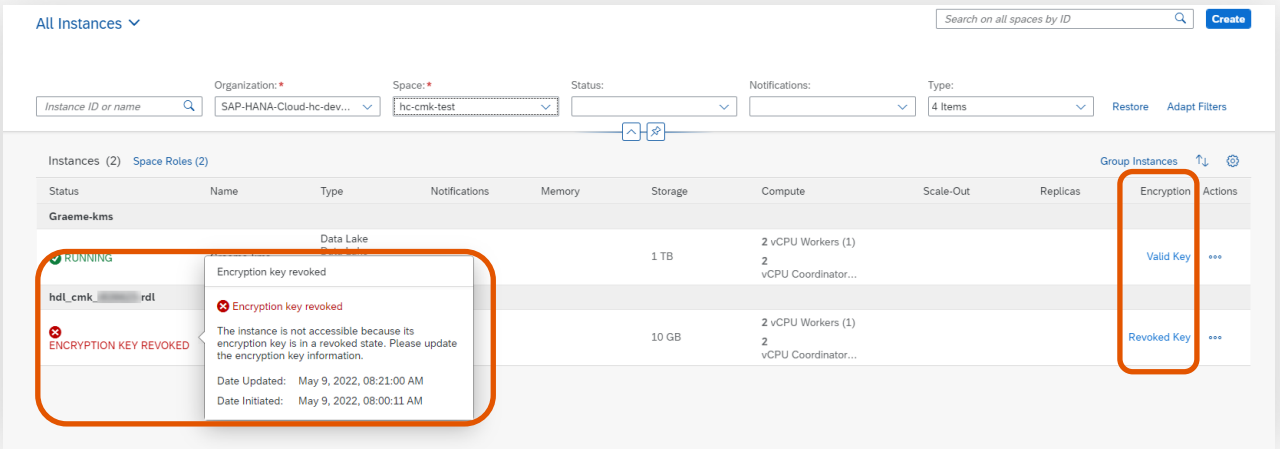
- Ability to control access to the encryption root keys of SAP HANA Cloud, SAP HANA database through SAP Data Custodian key management service
- This supports
  - customer-controlled encryption keys (CCEK),
  - bring your own key (BYOK), and
  - hold your own key (HYOK) functionality,
  - including the possibility to revoke the encryption key



SAP HANA Cloud | Customer-Controlled Encryption keys on instance level

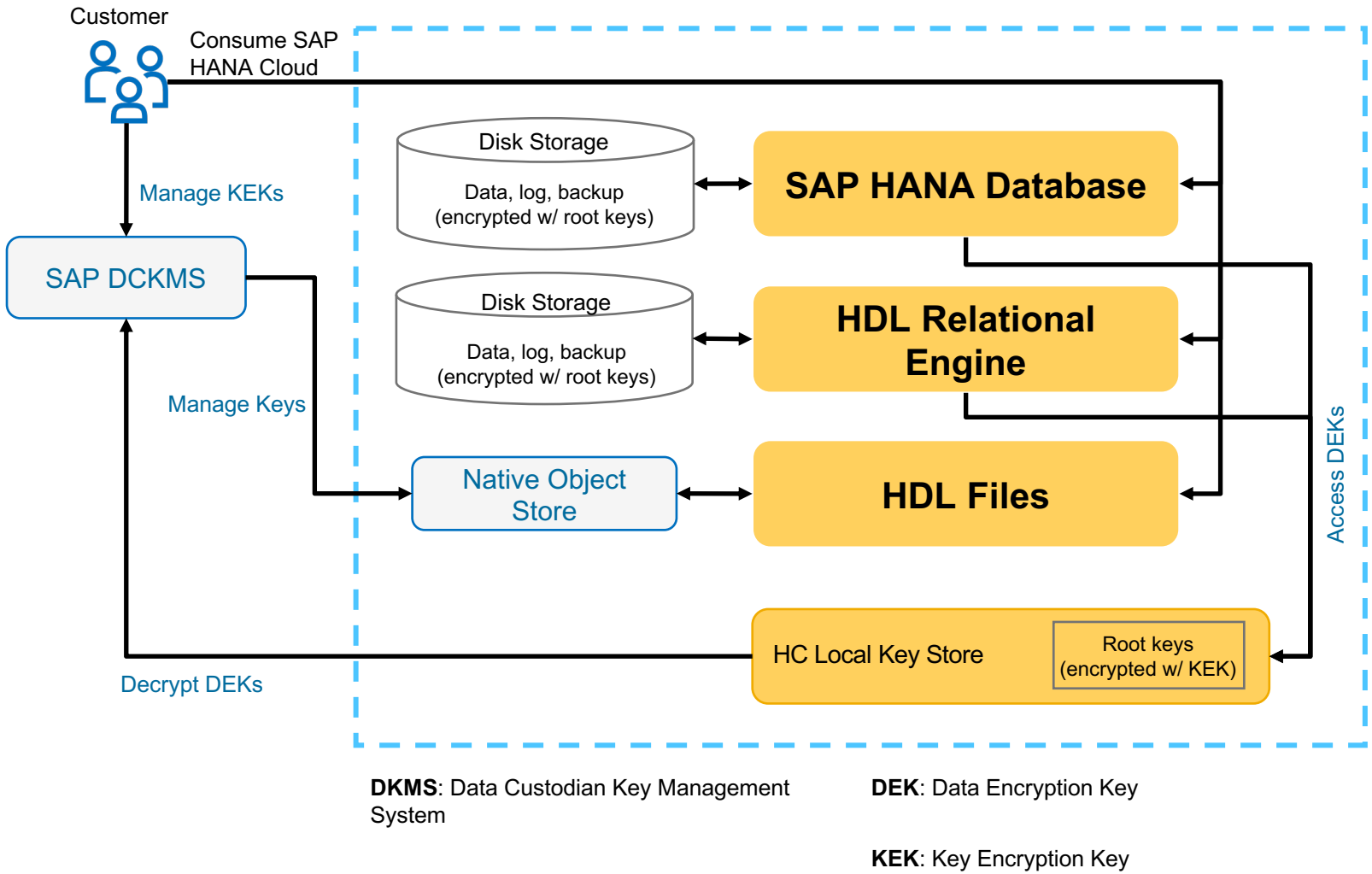
- Fully automatic configuration + tight integration with DC KMS
- HANA Cloud CMK is available in all regions where DC KMS is available
- Integration of SAP Data Custodian Key Management Service with SAP HANA Cloud give users control over encryption keys used by SAP HANA Cloud to store data
- Customers require DC KMS Licenses + Tenant
- support for products based on SAP HANA Cloud: SAP HANA Cloud, SAP HANA database, the data lake component of SAP HANA Cloud, the data lake relational engine, and data lake files
- Gain the ability to revoke SAP's access to the data
- When provisioning a new instance, you can enter the KMS key ID, but you cannot change it once the instance is created





Consumption | Whole instance

- Fully automatic configuration + tight integration with DC KMS
- KEKs never leave DC KMS
- Unencrypted DEKs never leave HC Local key store
- All HANA Cloud Database persistency is supported (HANA DB, HDL RE, HDL Files)

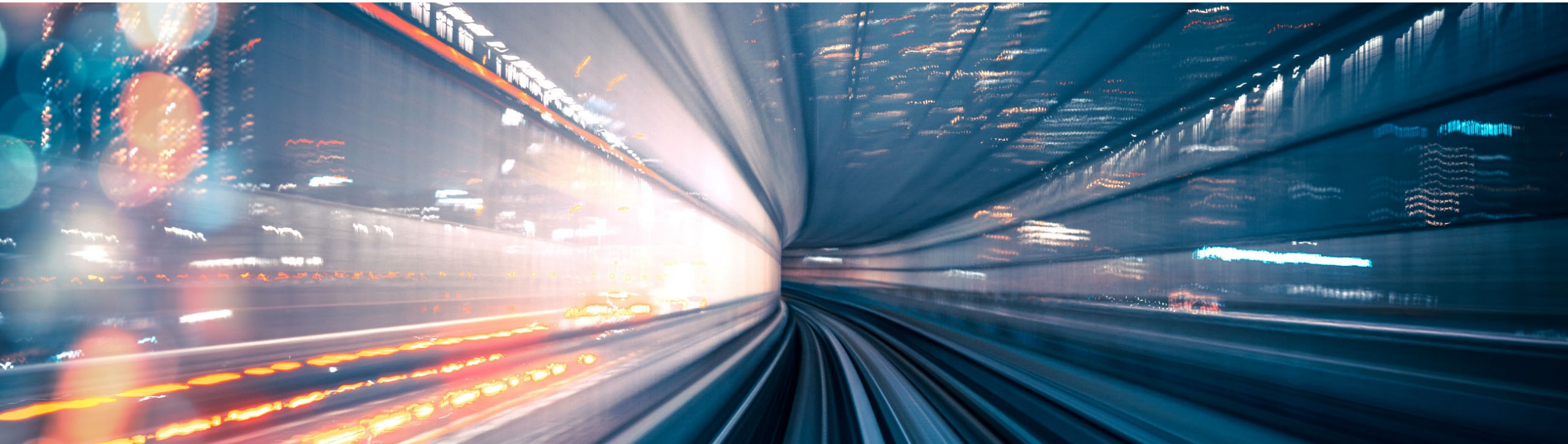


DKMS: Data Custodian Key Management System

DEK: Data Encryption Key

KEK: Key Encryption Key

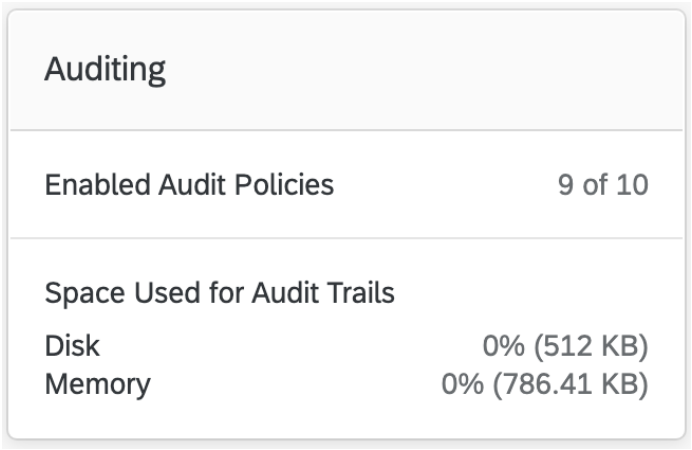
Auditing



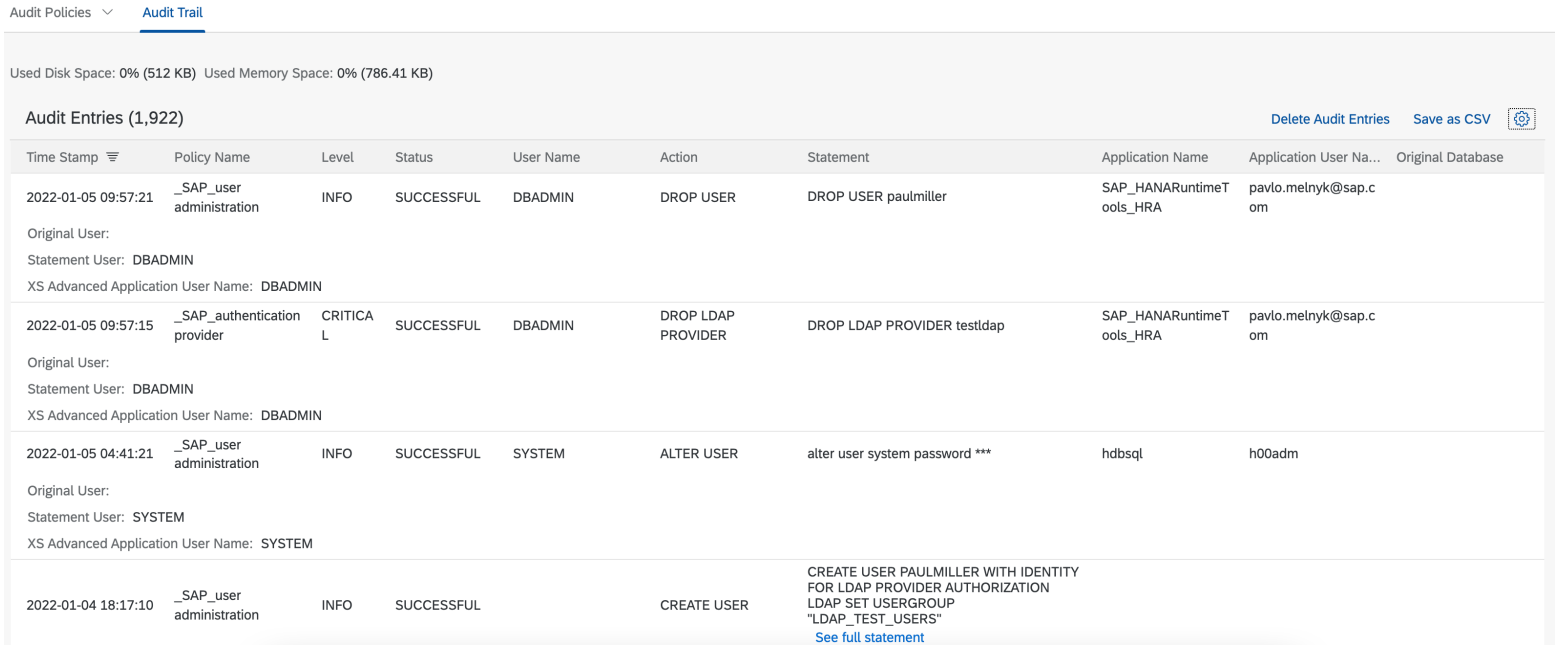
Audit Logging | What does it do?

Records critical system events

- Monitors changes of users, authentication, authorizations, and the system configuration
- Monitors access to the system, its functions, and data (read and write logging)



Screenshots from SAP HANA Cloud Database, HANA Cockpit



Audit Logging | Managed by the customer and SAP

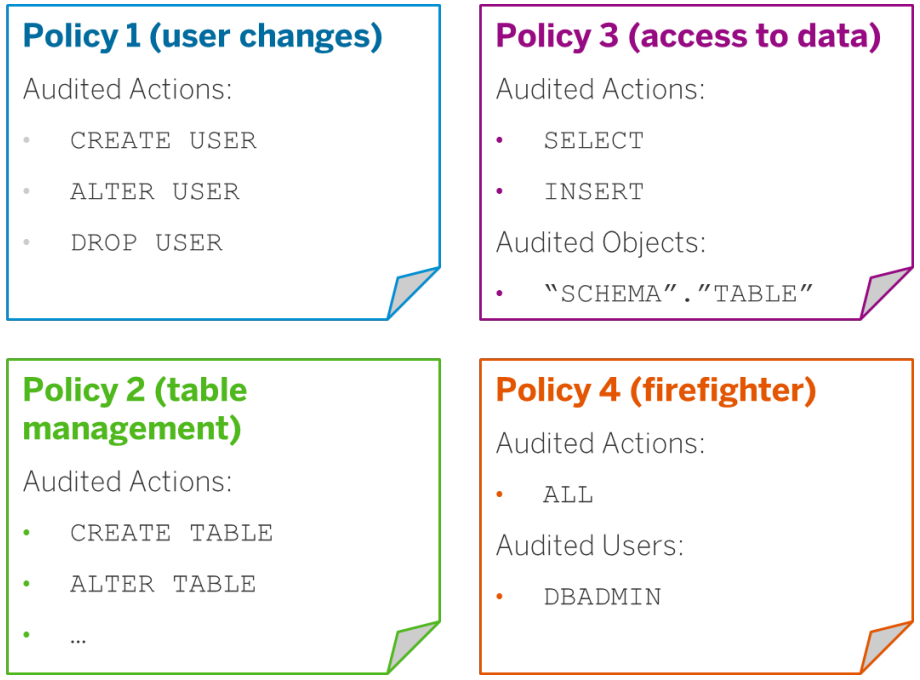
Customer

- Can record critical system events
- Change users, authorizations, and the system configuration
- Access system, its functions, and data (read and write logging)

SAP

- Monitors critical security events in customer systems
- Has no visibility of any business data

Audit events are recorded by audit policies created by SAP to monitor certain critical security events in customer systems.



Audit Logging | In SAP HANA Cloud, SAP HANA database audit events are available in a specially protected table

"PUBLIC"."AUDIT_LOG"

```
38 select TIMESTAMP, SERVICE_NAME, CONNECTION_ID, APPLICATION_NAME, AUDIT_POLICY_NAME, EVENT_STATUS, STATEMENT_STRING from "PUBLIC"."AUDIT_LOG"
39
```

Result × Messages × History

First 1000 rows SQL

	TIMESTAMP	SERVICE_NAME	CONNECTION_ID	APPLICATION_NAME	AUDIT_POLICY_NAME	EVENT_STATUS	
1	2021-05-18 09:57:43.699358000	indexserver	212056	HANACockpit	MandatoryAuditPolicy	SUCCESSFUL	CREATE AUDIT POLICY "ALERT
2	2021-05-18 09:57:43.715069000	indexserver	212056	HANACockpit	MandatoryAuditPolicy	SUCCESSFUL	ALTER AUDIT POLICY "ALERT"
3	2021-05-18 09:58:27.709997000	indexserver	212089	HANACockpit	MandatoryAuditPolicy	SUCCESSFUL	ALTER AUDIT POLICY "ALERT"
4	2021-06-16 12:40:32.433492000	indexserver	213080	sap_xsac_hrtt	MandatoryAuditPolicy	SUCCESSFUL	CREATE AUDIT POLICY "_SAP_
5	2021-06-16 12:40:32.450753000	indexserver	213080	sap_xsac_hrtt	MandatoryAuditPolicy	SUCCESSFUL	ALTER AUDIT POLICY "_SAP_s
6	2021-06-16 12:40:55.734658000	indexserver	213080	sap_xsac_hrtt	MandatoryAuditPolicy	SUCCESSFUL	CREATE AUDIT POLICY "_SAP_
7	2021-06-16 12:40:55.746266000	indexserver	213080	sap_xsac_hrtt	MandatoryAuditPolicy	SUCCESSFUL	ALTER AUDIT POLICY "_SAP_s
8	2021-06-16 12:41:34.613006000	indexserver	213080	sap_xsac_hrtt	MandatoryAuditPolicy	SUCCESSFUL	CREATE AUDIT POLICY "_SAP_
9	2021-06-16 12:41:34.623839000	indexserver	213080	sap_xsac_hrtt	MandatoryAuditPolicy	SUCCESSFUL	ALTER AUDIT POLICY "_SAP_a
10	2021-06-16 12:41:58.795757000	indexserver	213080	sap_xsac_hrtt	MandatoryAuditPolicy	SUCCESSFUL	CREATE AUDIT POLICY "_SAP_
11	2021-06-16 12:41:58.806622000	indexserver	213080	sap_xsac_hrtt	MandatoryAuditPolicy	SUCCESSFUL	ALTER AUDIT POLICY "_SAP_u
12	2021-06-16 12:42:34.133665000	indexserver	213080	sap_xsac_hrtt	MandatoryAuditPolicy	SUCCESSFUL	CREATE AUDIT POLICY "_SAP_

Screenshots from SAP HANA Cloud Database, HANA Database Explorer

- Secure
- Requires specific system privileges
- Data can be accessed and analyzed directly in SAP HANA database
- Recommended basic setup is available in SAP HANA Cockpit

- All audit entries are written to an internal SAP HANA database table
- Audit entries are only accessible through the public system view AUDIT_LOG
- The choice between NSE and in-memory storage for the audit table (also in SPS07 release)

Audit Logging | Auditing Database Events in SAP HANA Cloud, Data Lake Relational Engine

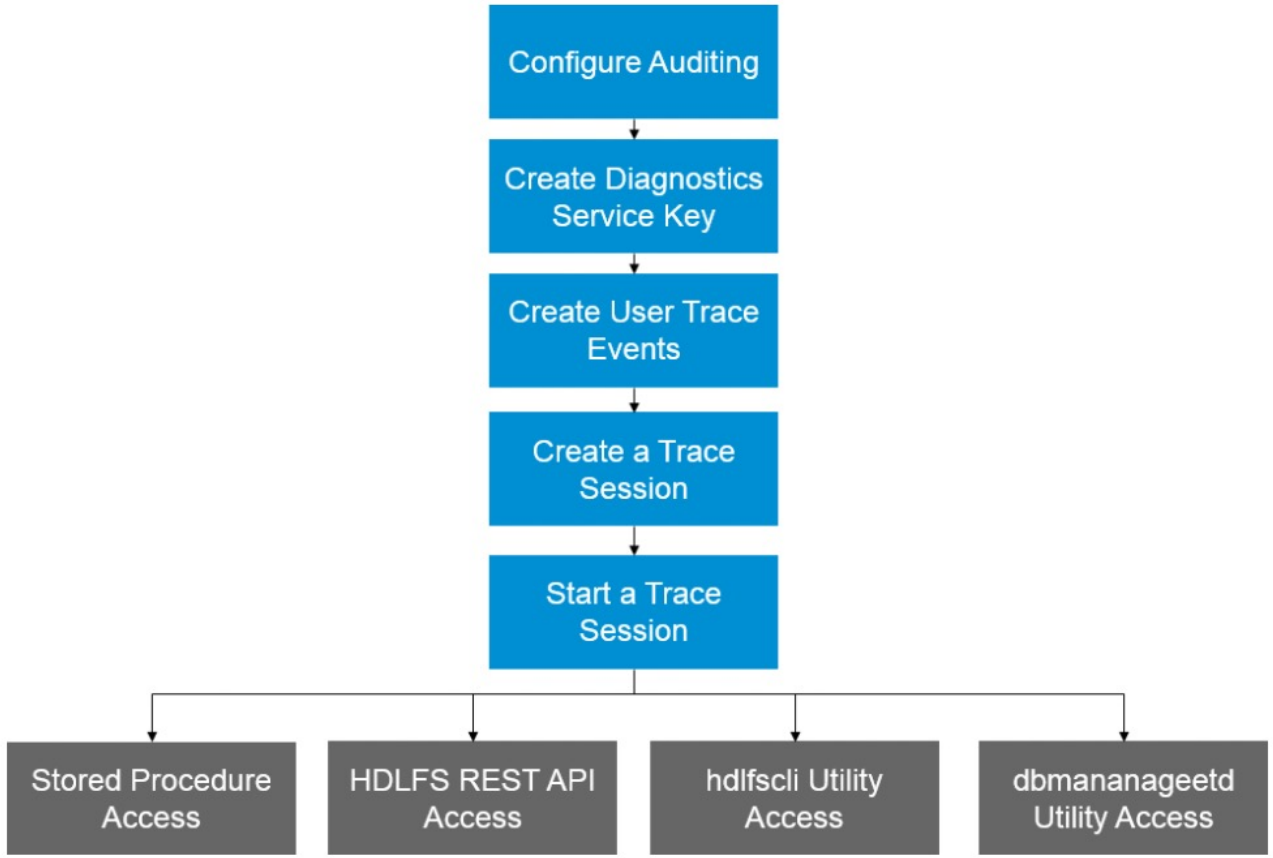
When enabled, auditing tracks all of the activity performed on a data lake Relational Engine database.

Optionally can limit auditing to:

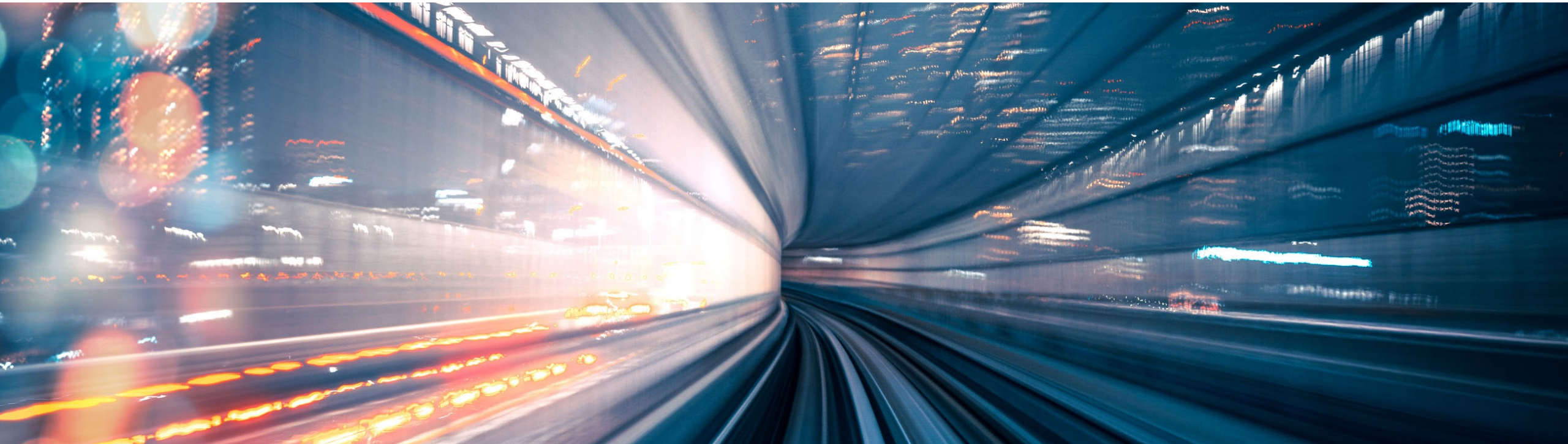
- Connections
- DDL
- Permissions
- Triggers

Audit files are retained for 30 days and can be accessed via:

- HDL Files Rest API
- hdlfscli utility
- dbmanageetd utility



Data Privacy



Why is data privacy important to your business?

Changing legal requirements

GDPR is a regulation in EU law on data protection and privacy in the EU and EEA.

Many **other countries** are implementing or have implemented similar **data privacy laws**, including USA, Brazil, Colombia, and China.

Evolving customer interest on data protection

*"The ability to protect data and create insights will add not only value, but draw customers looking to **embrace privacy by design.”***

Hudson Harris, Chief Engagement Officer at Healthcare company

Increased governmental investigation

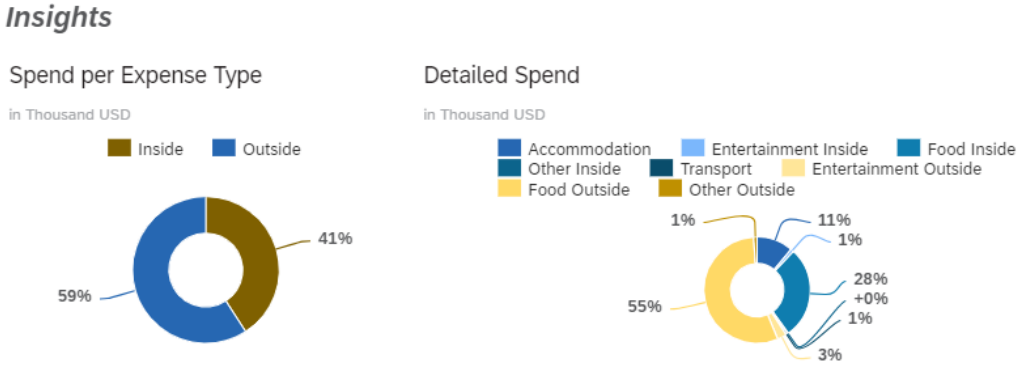
Overall sum of fines increasing, for example, in the GDPR space.

(see https://www.enforcementtracker.com/)

Fines under GDPR amount to 4% of a company’s annual worldwide revenue.

Leveraging competitive advantages

Through analytics, benchmarking, telemetry, and more on sensitive data sets.



Data Privacy | Two possibilities

Data Masking (of attributes)

- Selectively hide sensitive information from DBAs and power users with broad access
- Display / hide sensitive information depending on the user role, for example, for call center employees

Anonymization (of data sets)

- Structured approach to protect the privacy of individuals in complex data sets
- Real-time analytics on anonymized data
- Enables insights from data that could not be leveraged before due to regulations

Data Privacy | Data Masking

Selectively or completely hide sensitive information in tables and views

Use cases

- Display/hide sensitive information depending on the user role, e.g. call center employees and even power users

CREDIT_CARD_NO	NAME	BALANCE
3782-8224-6310-005	Julie Armstrong	453.98
3714-4963-5398-431	Michael Adams	-20.01
3787-3449-3671-000	Richard Wilson	1256.87
4012-8888-8888-188	Nathalie Perrin	-23.67

UNMASKED privilege

CREDIT_CARD_NO	NAME	BALANCE
XXXX-XXXX-XXXX-005	Julie Armstrong	***
XXXX-XXXX-XXXX-431	Michael Adams	***
XXXX-XXXX-XXXX-000	Richard Wilson	***
XXXX-XXXX-XXXX-188	Nathalie Perrin	***

No UNMASKED privilege

- Full integration into the security framework
- Dynamically applied during access → original data stays unchanged
- SQL-based mask expressions on tables and views
- Different masking modes to support different user scenarios

Data Privacy | Data Anonymization Methods

k-anonymity

- Hiding individuals in groups
- Intuitive but informal guarantees

Name	Birth	City	Weight	Illness
Paul	07-1975	Walldorf	82 kg	*AIDS*
Martin	10-1975	Hamburg	110 kg	*Lung Cancer*
Nils	01-1975	Munich	70 kg	*Flu*
Annika	09-1987	Berlin	58 kg	*Multiple Sclerosis*

Medical researcher: correlation between weight and illness?

Name	Birth	Location	Weight	Illness
0c4a67	1975	Germany	~ 96 kg	*AIDS*
df89aa	1975	Germany	~ 96 kg	*Lung Cancer*
305be2	19**	Germany	~ 64 kg	*Flu*
7422c2	19**	Germany	~ 64 kg	*Multiple Sclerosis*
Identifiers		*Quasi-Identifiers*		*Sensitive*

Differential privacy

- Applying noise to hide sensitive information
- Formal statistical privacy guarantees

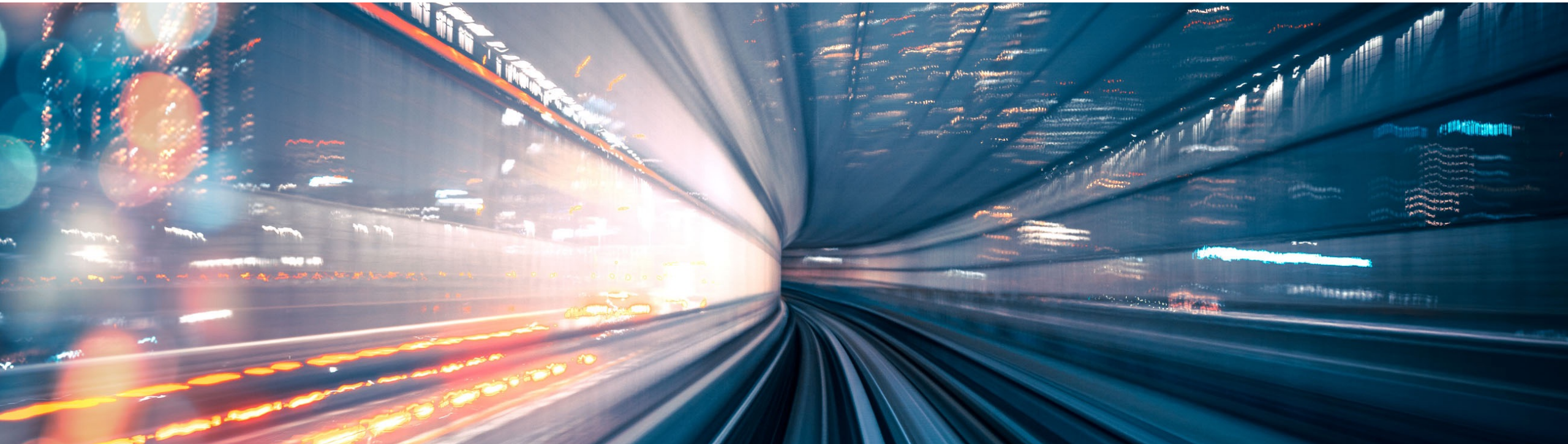
Name	Birth	City	Weight	Salary
0c4a67	07-1975	Walldorf	82 kg	$65k$
df89aa	10-1975	Hamburg	110 kg	$34k$
305be2	01-1975	Munich	70 kg	$75k$
7422c2	09-1987	Berlin	58 kg	$105k$

HR representative: Salary distribution in Germany?

Name	Birth	City	Weight	Salary
0c4a67	07-1975	Walldorf	82 kg	$65k + x_1 = 12k$
df89aa	10-1975	Hamburg	110 kg	$34k + x_2 = -30k$
305be2	01-1975	Munich	70 kg	$75k + x_3 = 140k$
7422c2	09-1987	Berlin	58 kg	$105k + x_4 = 80k$

➔ EU Opinion 05/2014 on Anonymization Techniques proposes k-anonymity (and derivates) and differential privacy (http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)

Secure Development, Operations & Compliance



Secure development and operations in SAP | General setup

SAP HANA Cloud is developed according to SAP's secure development lifecycle, which is a comprehensive framework of processes, guidelines, tools and staff training to safeguard the architecture, design and implementation of all SAP solutions.

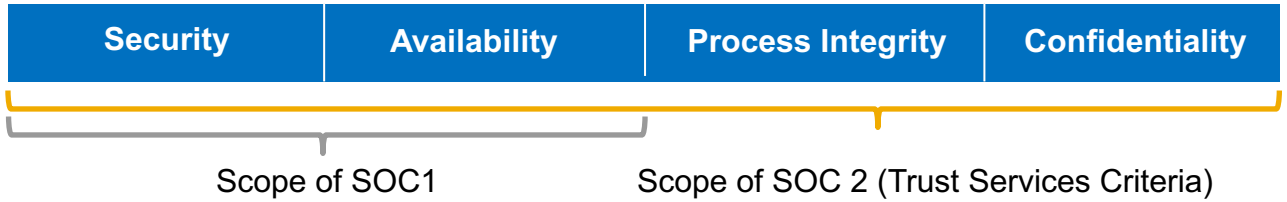
The secure development lifecycle is a threat-based approach, which includes risk and data protection assessments, comprehensive security testing including automated and manual tests as well as penetration testing, and a separate security validation phase.

- Learn about how SAP's secure software development lifecycle ensure highest level of security of our products
- Learn about Secure Software Development and Operations Lifecycle Overview

Security Compliance | Overview

SAP operates its solutions to the highest and most important standards.

Independent SOC1/2 (System and Organization Controls) reports attesting the adequacy and effectiveness of internal controls, and provide assurance that services are operated in a compliant manner



SAP's Management system for Information Security (ISO 27000 family) ensures a risk-based approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving our organizations ability to meet needs and expectations of interested parties.

ISO/IEC 27001: Information Security management system standards

- Provides a holistic approach to security and a comprehensive and measurable set of information security management practices.

ISO/IEC 27017: Code of practice for Cloud service information security

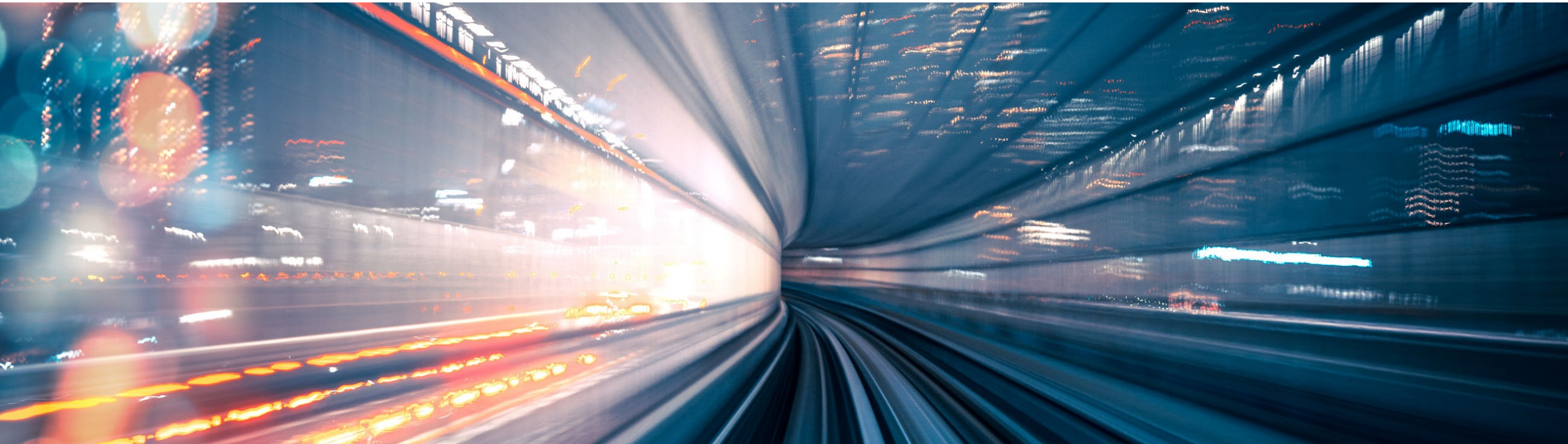
- Supports ISO/IEC 27001 by providing guidance on cloud-specific information security controls.

ISO/IEC 27018: Code of Practice for Personally Identifiable Information

- Supports ISO/IEC 27001 by recommending information security controls for protecting personal data in the public cloud.

For more information, visit SAP Trust Center
Select "Compliance" category and filter by Business Technology Platform for certifications and attestations.

Key takeaways



Key Takeaways | SAP HANA Security and Data Privacy

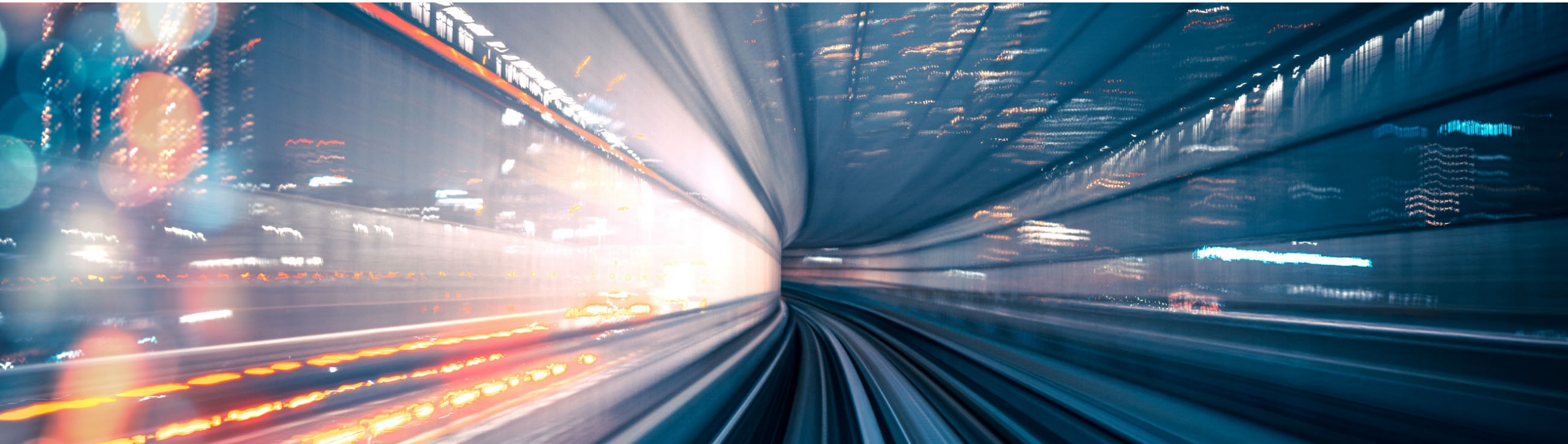
KEY CAPABILITIES

- Comprehensive framework for roles and privileges
- Granular authorization controls and data-masking options
- Certified encryption technologies
- Real-time data anonymization
- Integration with SAP security tools and services
- ISO/SOC certification (SAP HANA Cloud)

BENEFITS

- Provide state-of-the-art security mechanisms for any size company
- Capitalize on the value of all enterprise data, while respecting data privacy
- Enable new data-centric use cases
- Anonymize sensitive and confidential data in real time to protect the privacy of individuals
- Demonstrate digital responsibility

Take The Next Step



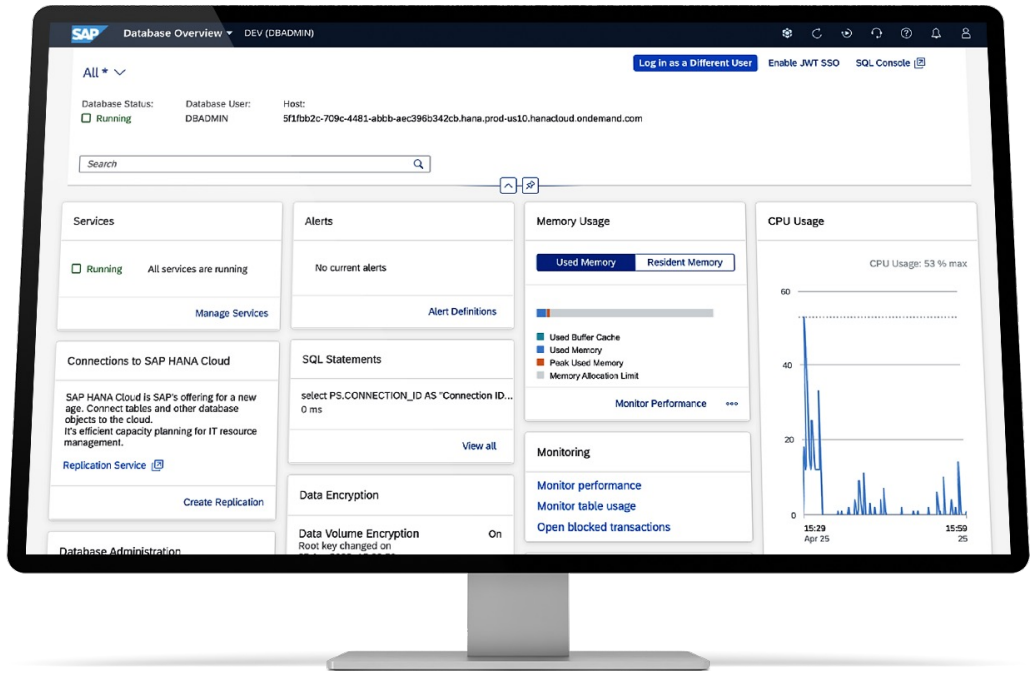
Start now with a free tier or trial!

SAP HANA Cloud is available for free tier or trial.

1. Get a first impression via our free 30-day Guided Experience

2. Jump start into SAP HANA Cloud via our tutorial mission

3. Stay up-to-date with our SAP HANA Cloud Events



Find out more about SAP HANA Cloud

Learn about SAP HANA Cloud

Check out the **sap.com/hanacloud** website, which has valuable resources for fast-tracking your knowledge of SAP HANA and a rich support section designed to help you get the highest quality answers quickly and easily from SAP experts

Read our blogs
community.sap.com

Get started for Free
sap.com/hanacloud

Customer stories
sap.com/hanacloud

Roadmap
roadmaps.sap.com

Get involved in the discussion

Engage with community experts on the SAP Community program to accelerate the development of SAP HANA Cloud powered solutions

Influence the future
influence.sap.com

Stay current
youtube.com/SAPTechnology/SAPHANACloud
#whatsnewinsaphanacloud

Spread the word
https://twitter.com/sapBTP

SAP is here to help.

Contact your local SAP representative

sap.com/corporate/en/company/office-locations.html

Thank you.

Contact information:

Pavlo Melnyk
SAP HANA Product Management
pavlo.melnyk@sap.com

Hui Li
SAP HANA Product Management
hui.li06@sap.com

Tanuja Jadhav
SAP HANA Product Management
tanuja.jadhav@sap.com

Jinhee Jeong
SAP HANA Product Management
jinhee.jeong@sap.com