

Security with SAP Cloud Platform

June 2017

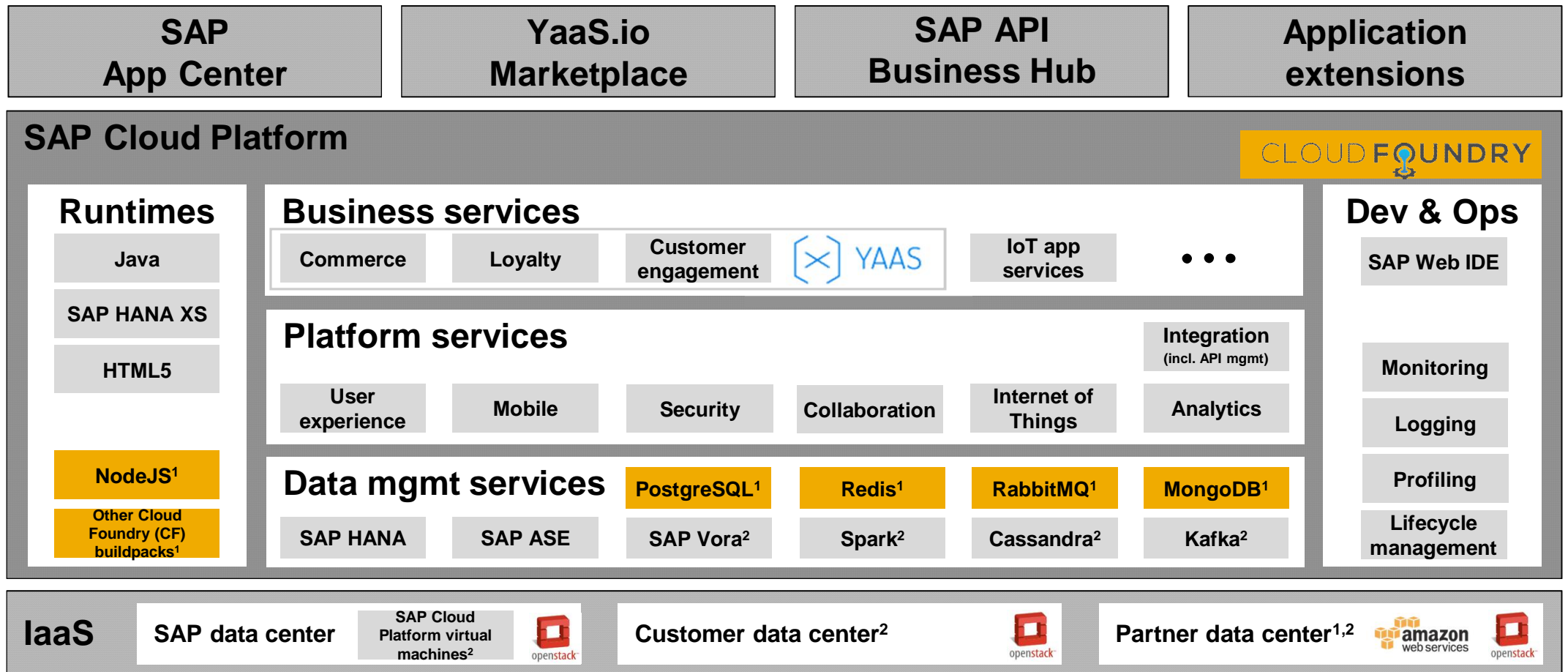
Public



Legal disclaimer

This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document 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. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.

Target state – platform to enable digital transformation



1) CF services available as beta 2) planned innovations or future direction

© 2017 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC

Use cases



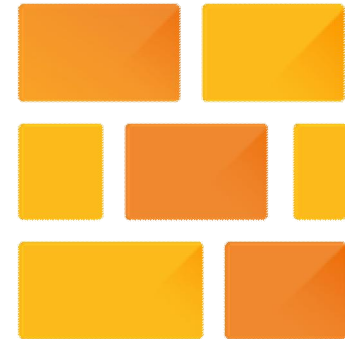
Extend cloud and on-premise applications

Add new functionality to your existing cloud and on-premise applications quickly to optimize your existing investments



Integrate your applications and data

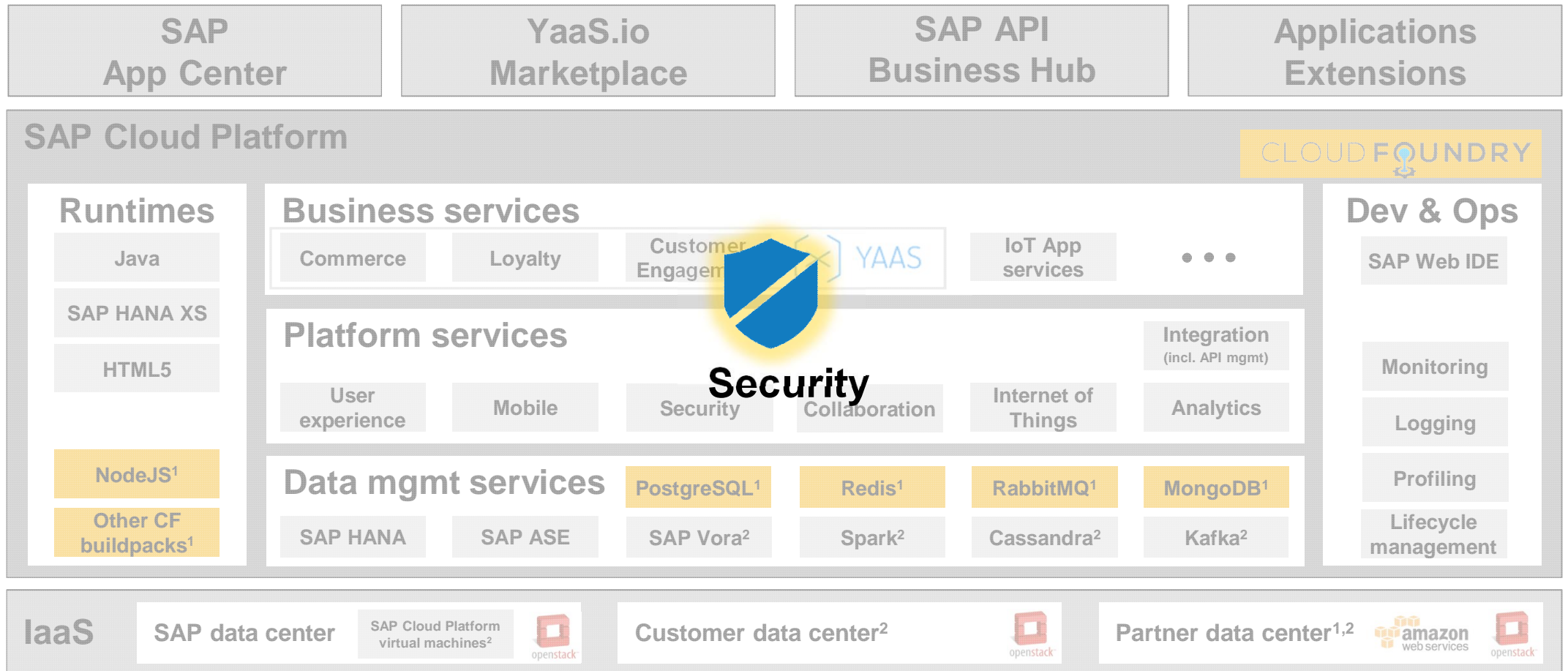
Connect your cloud and on-premise applications to eliminate data silos and make digital access simple, secure, and scalable



Build new cloud applications

Build and run new cloud applications rapidly to solve new problems, engage new customers, and drive new revenue

Security with SAP Cloud Platform



1) CF services available as beta 2) planned innovations or future direction

© 2017 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC

Security overview

Develop secure

- Leverage single sign-on
- Protect your data
- Secure your mobile and IoT scenarios
- Integrate securely with your corporate user directory
- Propagate the logged-on user
- Secure storage of confidential data

Run secure

SAP Cloud Platform

- Secure data center
- Protection of data privacy
- Transparency
- Compliance
- Secure access

Run secure



SAP regions

- SAP regions on SAP tier-level 3 or 4
- SAP regions around the world: 14 countries, 30 locations, and 40 data centers
- Benefit from local regulations (such as strong Germany and EU regulations)
- Low latency that speeds up access
- Customer can choose
 - Region of data storage
 - EU-only operations
 - Preferred region partner
- Backups are always located in the same jurisdiction as the data that is used in day-to-day operations, but for security reasons, the two are physically separated.



*) Not all cloud solutions are available in all regions; for the availability of cloud solutions please compare the official [availability matrix](#)

Secure SAP region

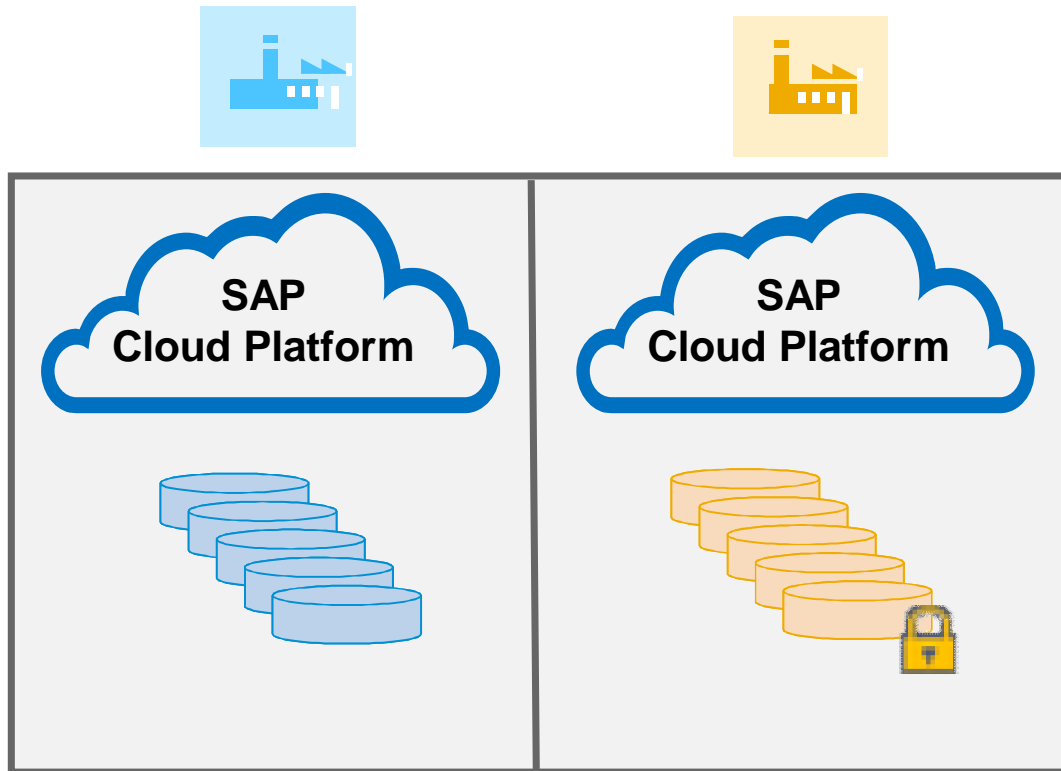
- Video and sensor surveillance
- Access logging
- Security guards
- Fire detection and extinguishing system
- Uninterruptible power supply
- Biometric access control

SAP region availability

SAP tier-3 and tier-4 regions

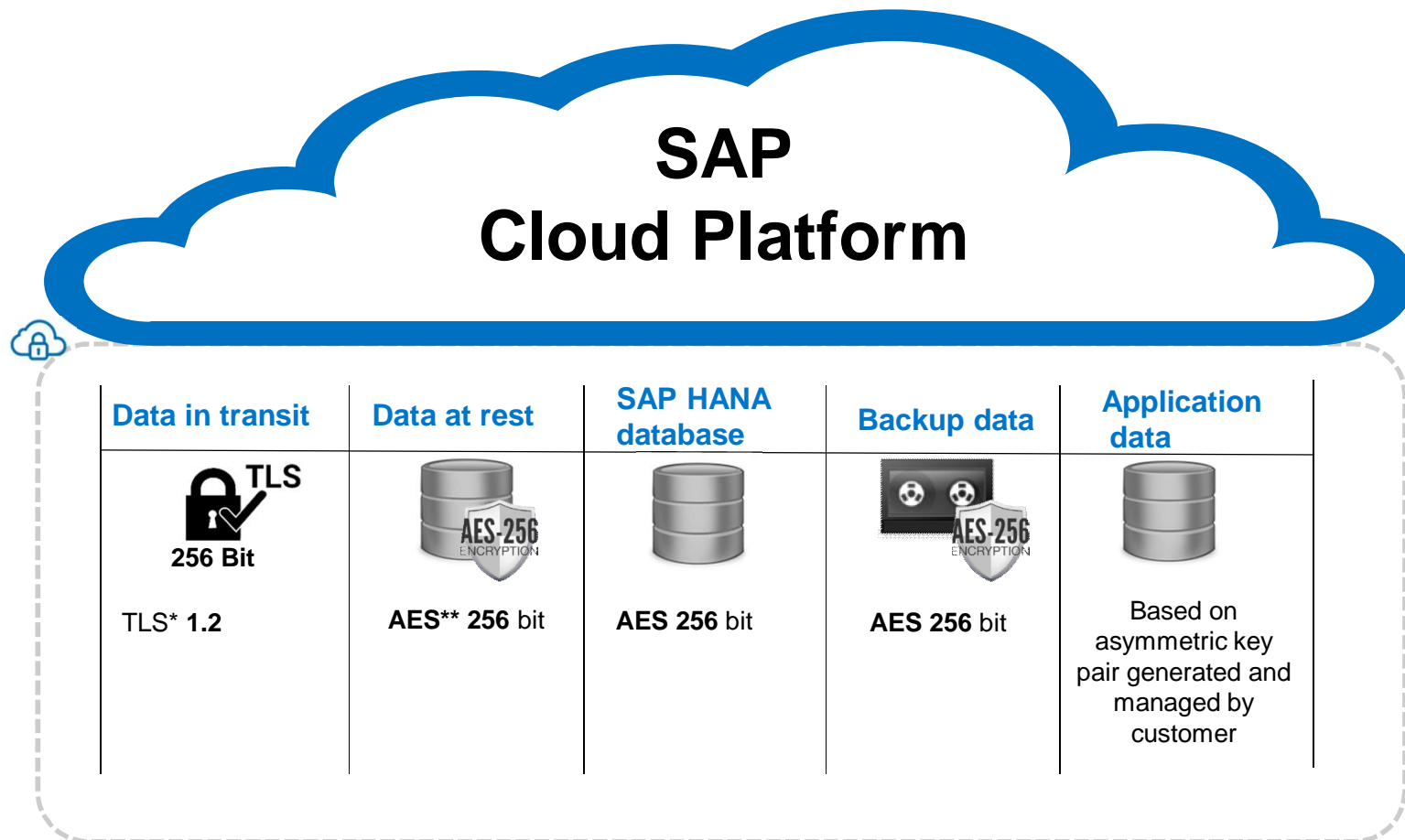
Minimum availability requirements	Tier I	Tier II	Tier III	Tier III+	Tier IV
Stand-alone Data Center building necessary	no	no	no	yes	yes
Amount of external electrical power suppliers	1	1	1	1	2
Amount of transformers to power the Data Center	n	n	n+1	n+1	2n
UPS Battery System necessary	no	yes	yes	yes	yes
Minutes UPS must provide power	0	5	>10	>10	>10
Amount of UPS Systems necessary	n	n	n+1	n+1	2n
(Diesel-) Generators needed	no	no	yes	yes	yes
Amount of cooling systems needed	n	n	n+1	n+1	2n
Server cooling is independent from an office AC	no	no	yes	yes	yes
Fire detection system needs to be installed	yes	yes	yes	yes	yes
Fire extinguishing system must be installed	no	yes	yes	yes	yes
On-site response time of Data Center personnel	<48h	<8h	<1h	<1h	<1h
Available WAN network connection lines	1	n+1	n+1	n+1	2n
Available LAN network connection lines	n	n+1	n+1	2n	2n

Data privacy



- Customer data is strictly separated in its own SAP HANA database
- Data encryption is on the database level

Encryption



Transparency

Only SAP employees who are located in EEA member countries (EU, Iceland, Liechtenstein, and Norway) or Switzerland can operate and support customer data. This European Data Protection (EU-DP) service is available to customers both inside and outside the EU running in SAP regions.

European Union (EU) Access Mode

This SAP Cloud Platform landscape is operated and supported in European Union (EU) Access mode.

As an SAP employee, you must confirm either that you are physically located within the EU or that you have positively verified that EU Access restrictions do not apply in your situation. Your confirmation will be logged.

For details, see:
[European Data Protection at a Glance](#)

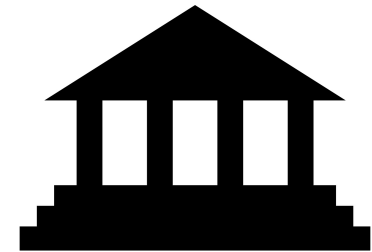
Confirm

Leave

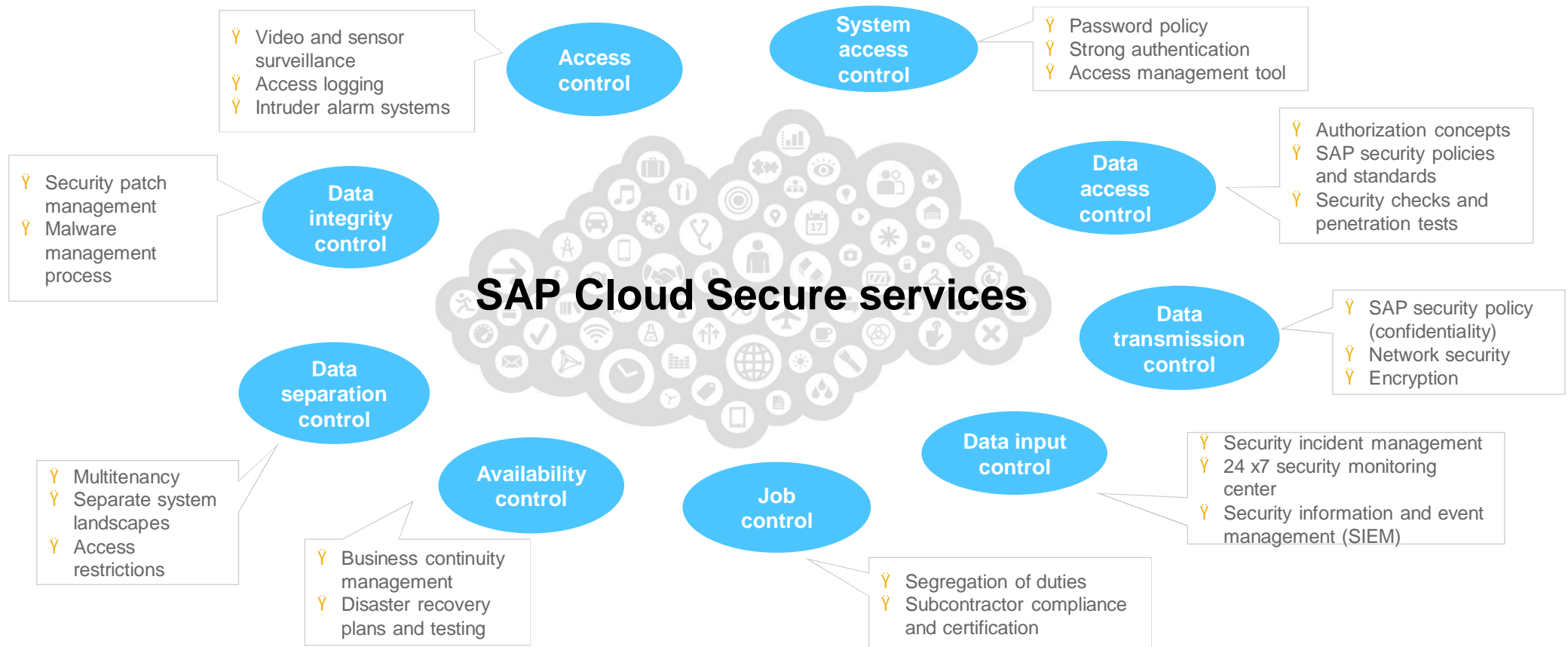
Compliance

Legal compliance

We have clear and company-wide guidelines in place that define how we respond to requests for customer data coming from law enforcement authorities and regarding national security concerns. We take our commitment to our customers and legal compliance very seriously. Customer data is only shared if the request is legally valid. Our legal department evaluates every inquiry in detail. In addition, we will question a request if there are grounds for assuming that they are not in conformity with the law.



Technical and organizational measures at a glance



Security measures

Network

- Copy network filtering
- Intrusion prevention systems
- Multiple firewalls
- Two-factor authentication
- Network admission controls
- Proxies with content filtering
- Advanced threat management

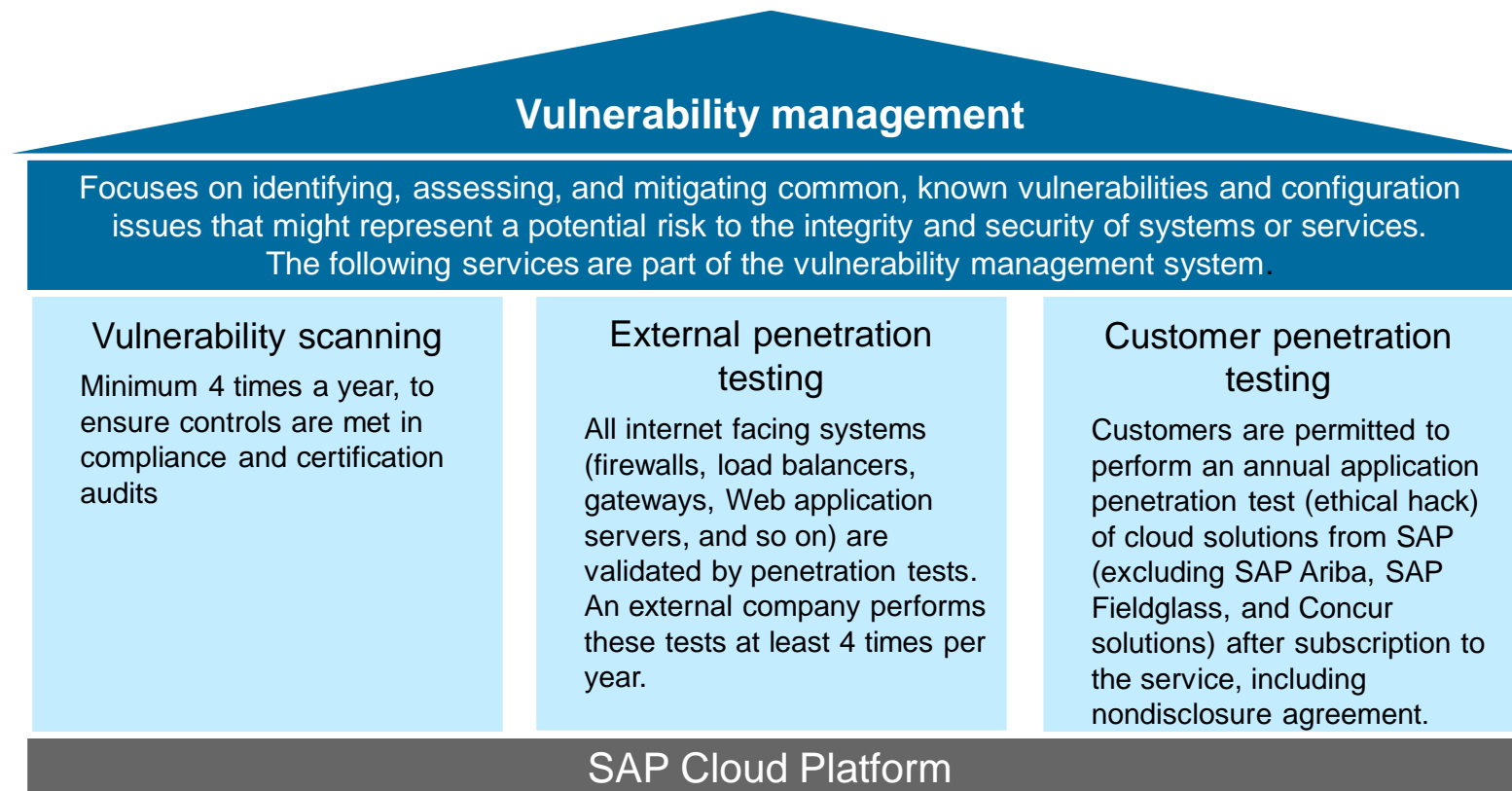
Operating system/application

- Security-hardened systems
- Penetration testing
- Vulnerability scanning
- 24x7 security monitoring center
- Antivirus and malware scanning
- Security patch management
- Backup and restore management

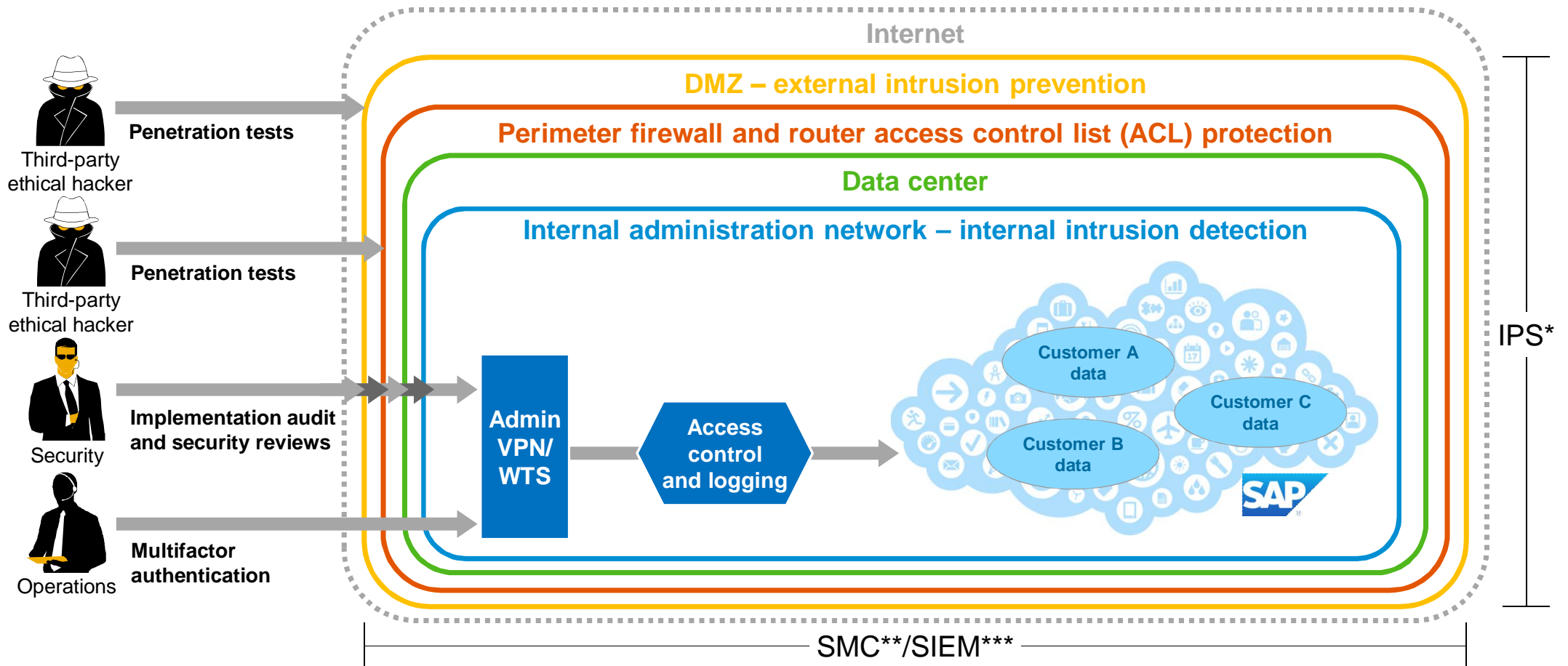
Employee

- Security awareness training

Security measures: vulnerability management



SAP Cloud Secure: segregation and intrusion prevention

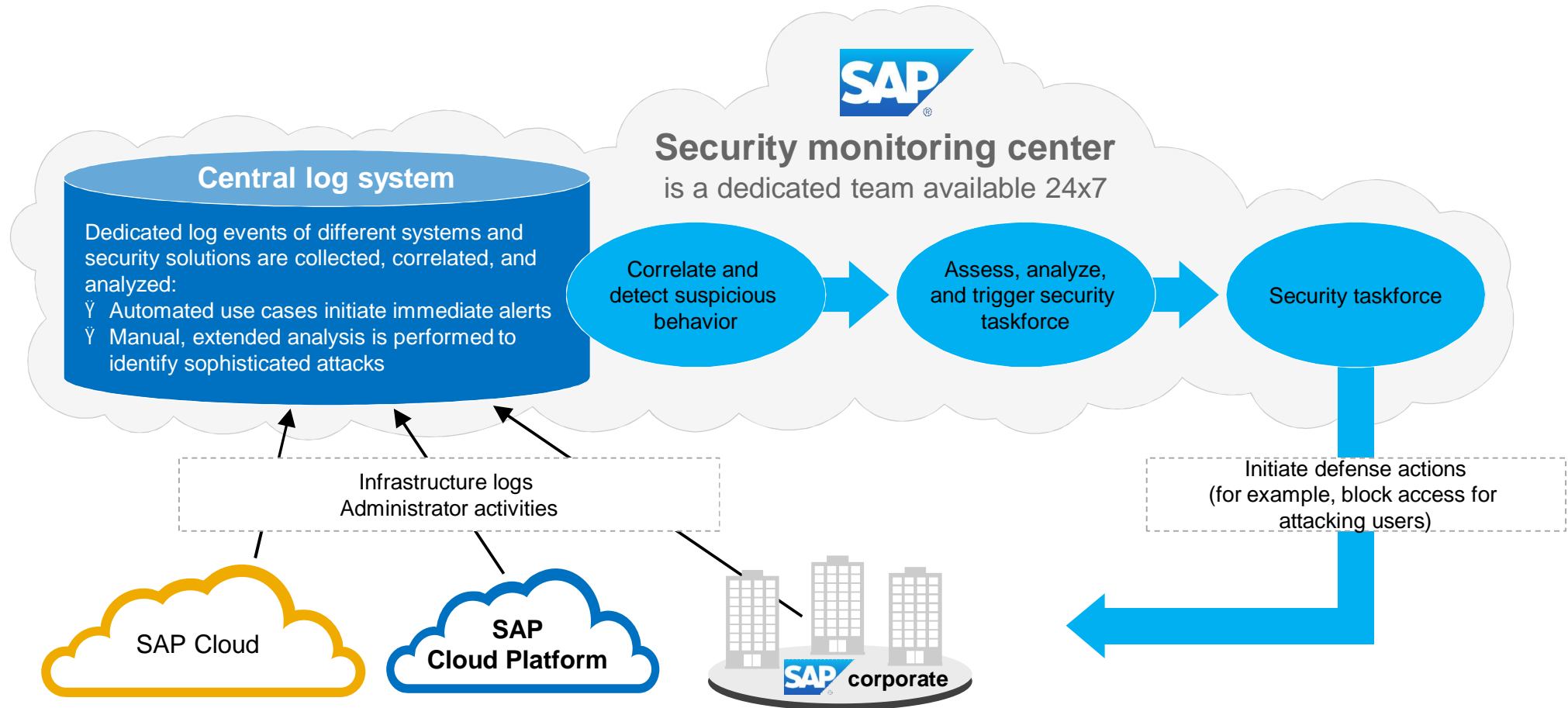


*IPS = network intrusion prevention system

**SMC = security monitoring center (24x7)

***SIEM = security information and event management

Security monitoring



Run secure with SAP Enterprise Threat Detection

Protect the integrity of business processes and prevent theft or manipulation of business data



Customer security incident process

Customer initiated

Customer reports security incident using SAP Cloud Platform Portal

SAP assesses the problem

- Y “Normal security incident” → standard process
- Y “Customer breach” → breach process

SAP provides and implements solution

- Y SAP updates customer about resolution steps

SAP informs customer about closing the security incident

- Y Provides breach report for customer breaches
- Y Informs customer about the implemented solution

Report
security incident

Assess problem

Provide solution

Inform customer

SAP initiated

SAP identifies a security incident

- Y Tracks incidents using internal ticket system

SAP assesses the problem

- Y “Normal security incident” → standard process
- Y “Customer breach” → breach process
 - SAP Informs customer about security incident

SAP provides and implements solution

- Y SAP updates customer about resolution steps for breach

SAP informs customer about closing the security incident

- Y Provides breach report for customer breach

SAP supports law enforcement (optional)

Security incident management

Classification:

Security event

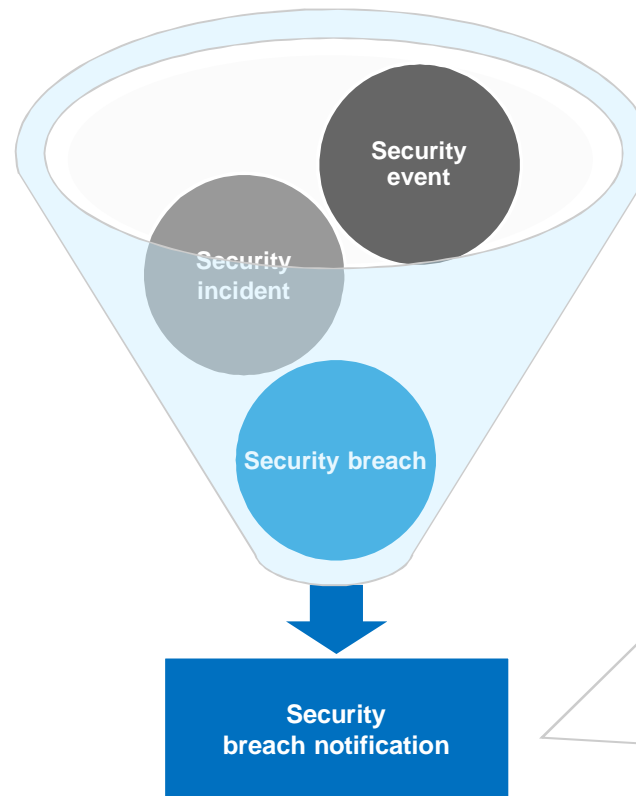
is the **identified occurrence** of system, service, or network condition. It indicates a possible breach on information security policies, standards, or internal controls or previously unknown situation that **may be** security relevant.

Security incident

is a single or a series of unwanted or unexpected information security events that **have a significant probability** of compromising business operations and threatening information security.

Security breach

is a **confirmed security incident** in which sensitive, protected, or confidential data is exposed, transmitted, changed, deleted, stolen, or used by an individual or a group unauthorized to do so.



Notification:

- Y SAP reports **security breaches** to customers **promptly**, maximum within **24 hours** after confirmation
- Y The notification provides:
 - Time and date of the occurrence
 - Territorial information where the data was hosted
 - Affected landscape (solution)
 - Affected systems (applications)
 - Scope of damage (spread of data harmed)
 - Performed activities that lead to the confirmation
 - Performed activities to isolate or deter the damages
 - Elaboration if available (how occurred)
 - Single point of contact for customer (case owner)

Compliance



ISO 27001^{1) 2)}
Certification for Information
Security Management Systems



SOC 1/SSAE 16^{1) 2)}
Statement on Standards for Attestation
Engagements No. 16



SOC 2^{1) 2)}
Service Organization Controls
Report (attestation report)



ISO 22301²⁾
Certification for Business Continuity Management
Systems

**Security measures are audited and confirmed
through
various certifications and attestations**

1) Certification for SAP Cloud Platform

2) The same or equivalent certificates are valid at every data center where cloud solutions are run.

Certificate

Certificate No.: e0339126

The Information Security Management System of:

SAP SE

Complies with the requirements of:

ISO/IEC 27001:2013

The certificate is valid for:

*The ISMS of SAP SE governing development, maintenance and operations
of the SAP HANA Cloud Platform solution.*

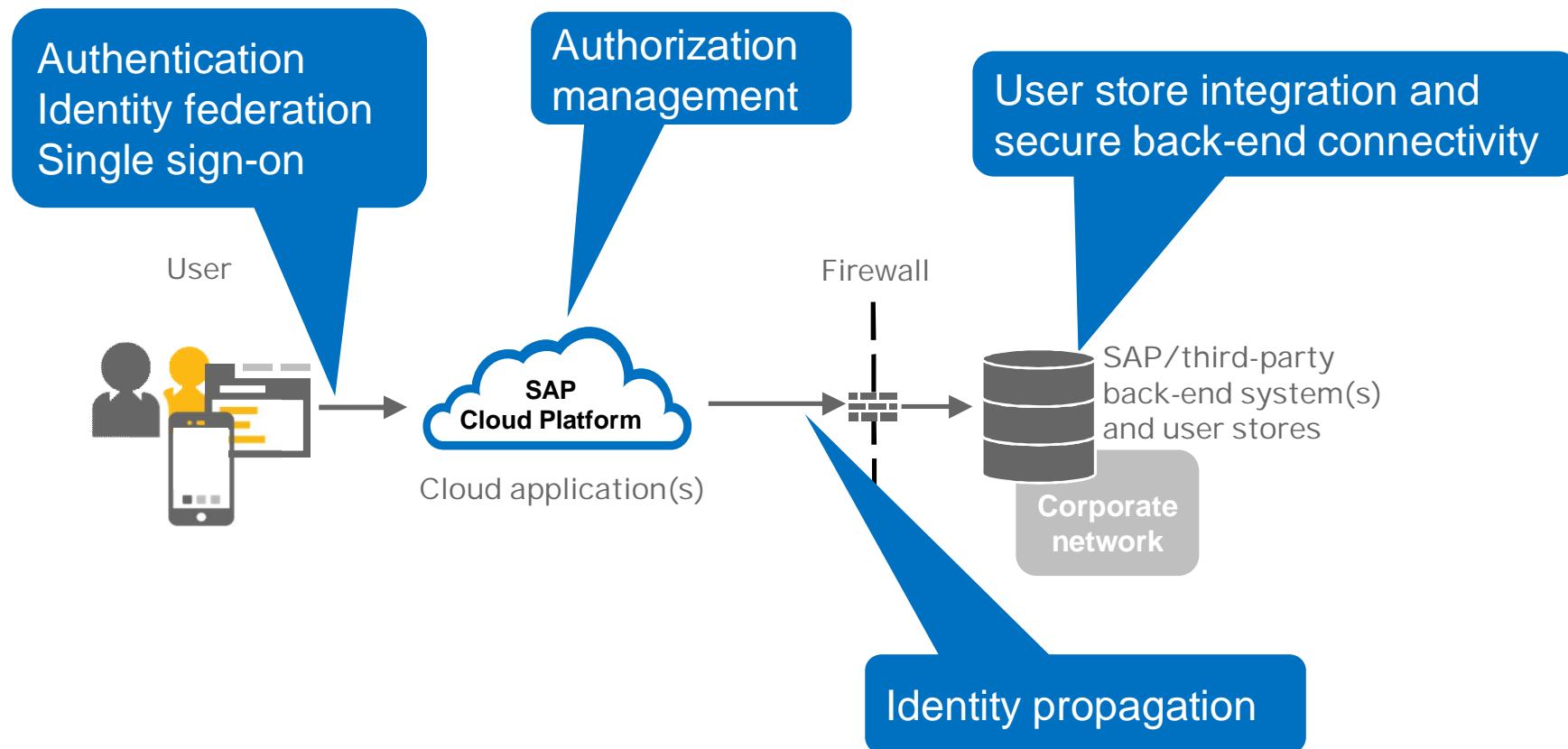
The scope has been further described in document
'HCP ISMS Scope 1.2.pdf' version 1.2, dated 5 November 2014.

The selection of controls has been described in the Statement of
Applicability with reference 'Statement of Applicability_V1.0.xls' dated 21
November 2014.

Develop secure

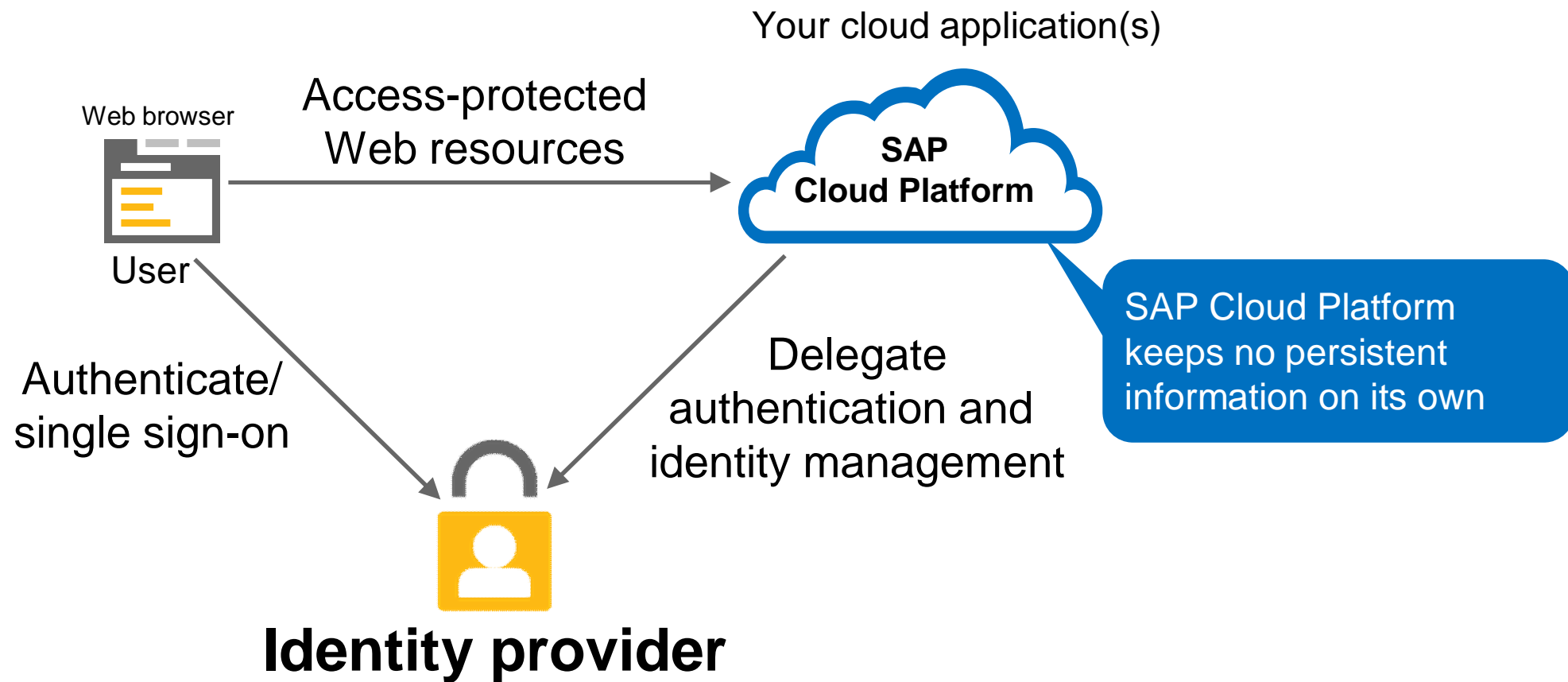


Overview



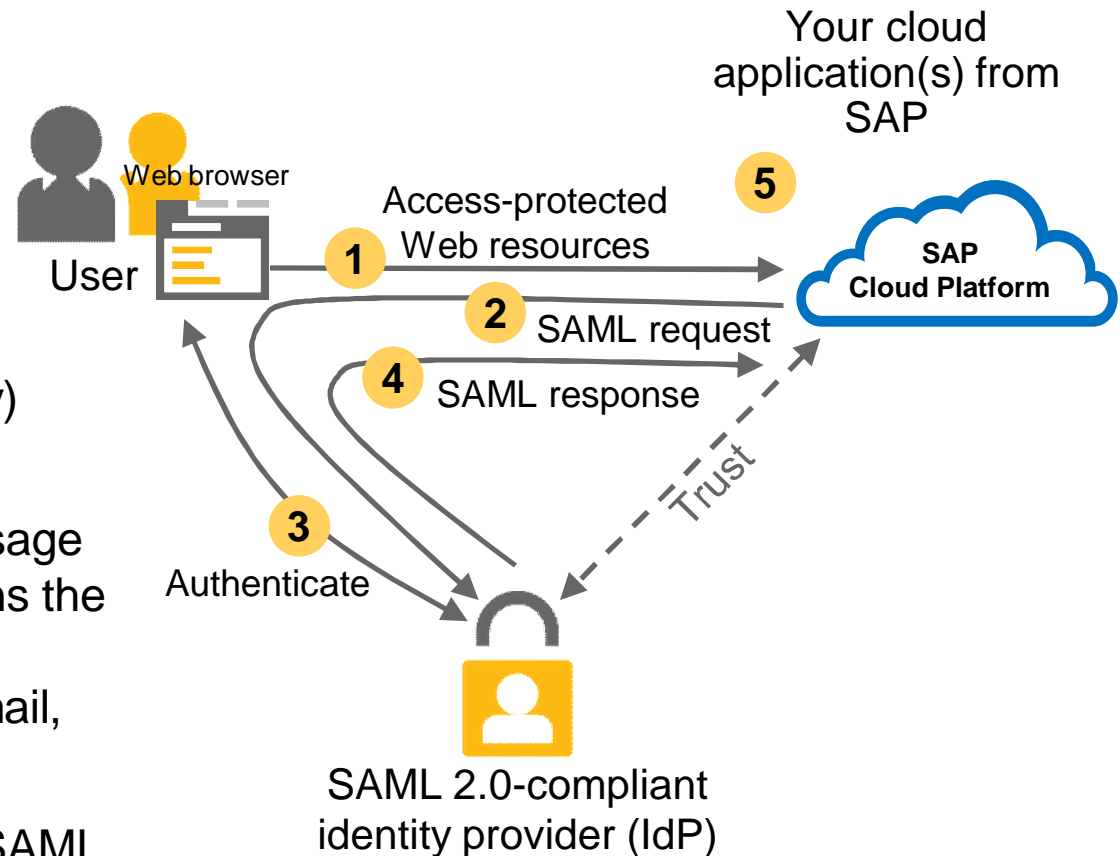
Authentication
Identity federation
Single sign-on

Authentication and single sign-on based on SAML

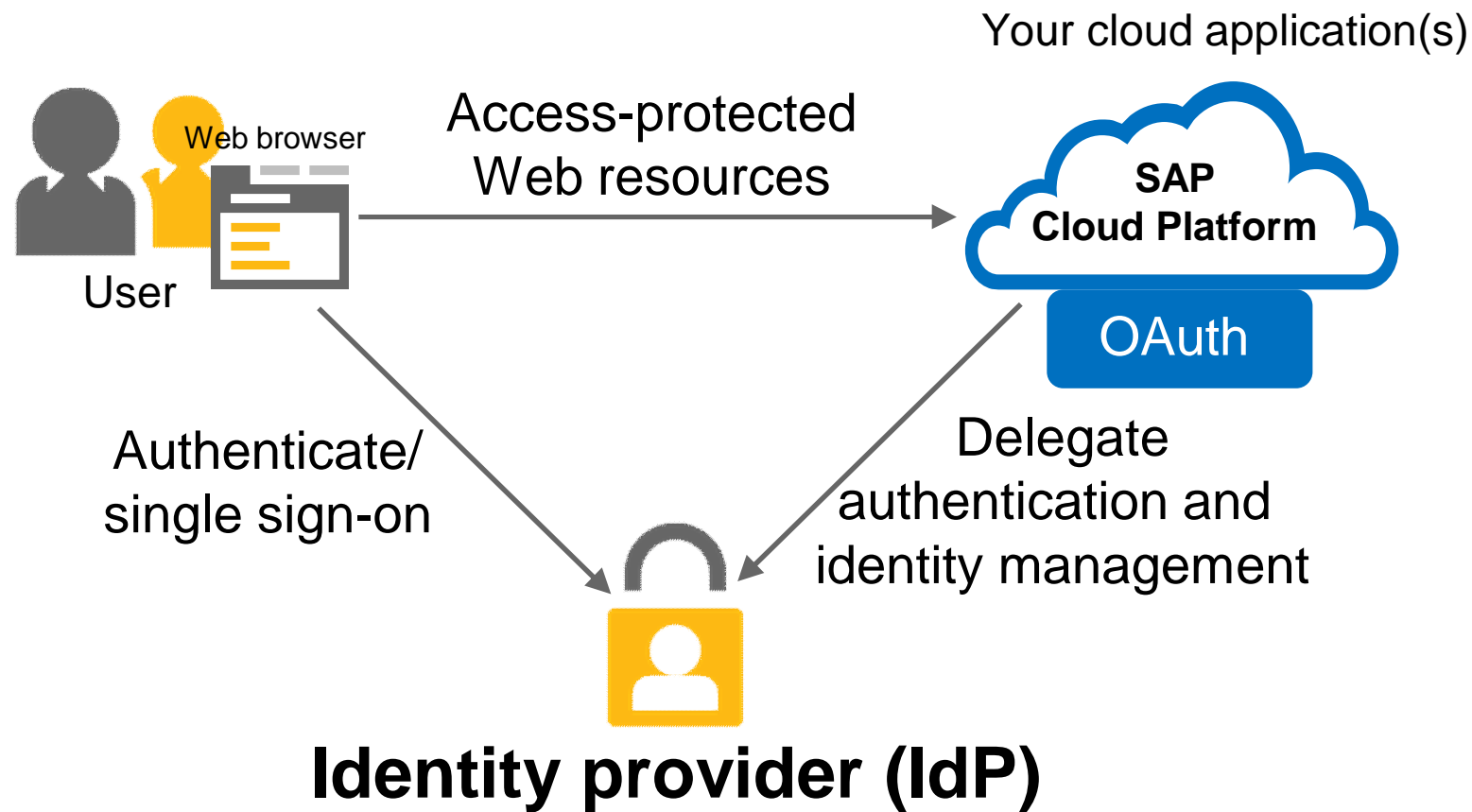


SAML flow

- 1 User accesses protected Web resource on SAP Cloud Platform
- 2 Cloud application sends SAML authentication request via **HTTP redirect** to trusted IdP
- 3 IdP authenticates the user (if not done already)
- 4 Upon successful authentication, IdP sends an **HTML form** with the SAML response message in a hidden field to the Web browser. It contains the **user's ID** and (optionally) additional **user attributes** (such as first name, last name, e-mail, group memberships, and so on)
- 5 **User is created** based on information in the SAML response



Authentication and single sign-on based on OAuth

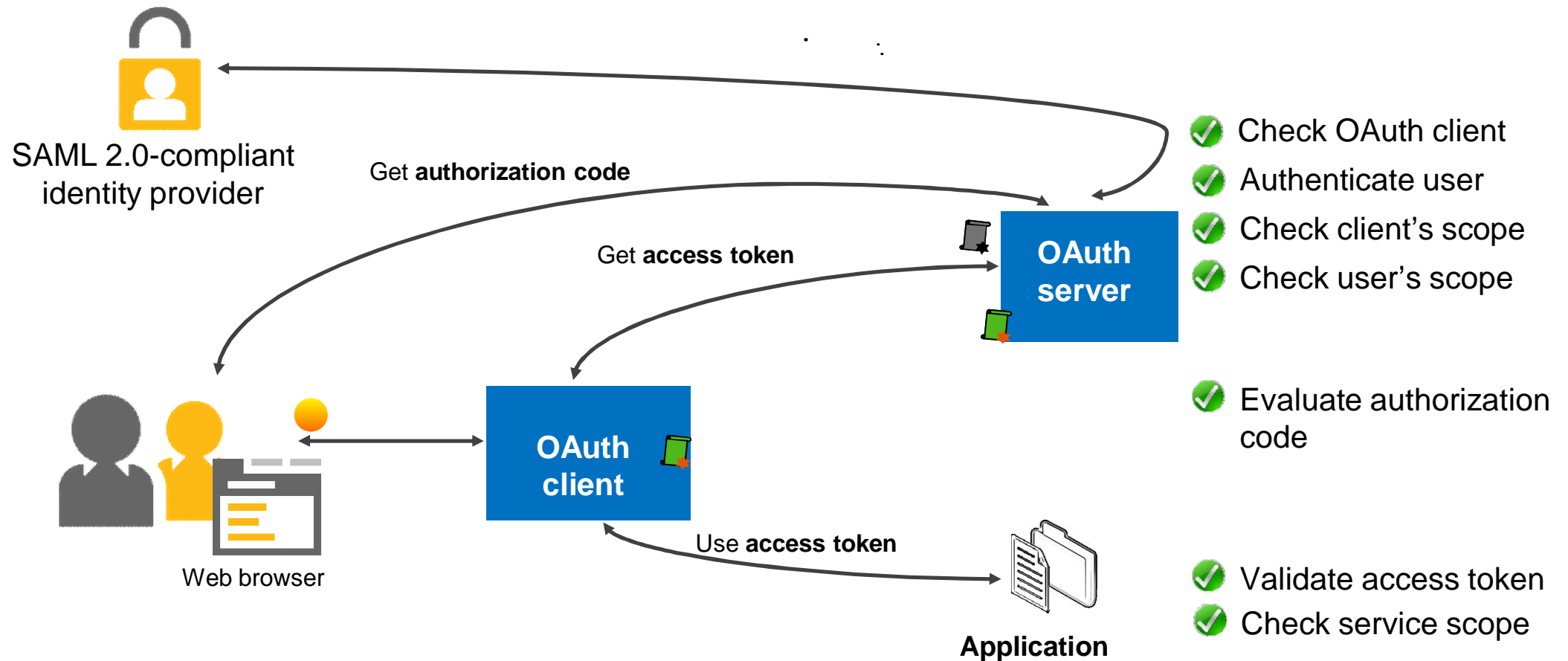


OAuth 2.0




- § OAuth can grant a client access to protected resources without sharing the credentials of the resource owner
- § OAuth 2.0 is specified in IETF RFC 6749
- § OAuth replaces the user's username and password with a token
- § Although the token is still vulnerable to theft, it has a very narrow scope compared to the user's password
- § It allows a specific client to access a specific resource
- § The user is in full control at any time to revoke the granted access to the client



OAuth flow



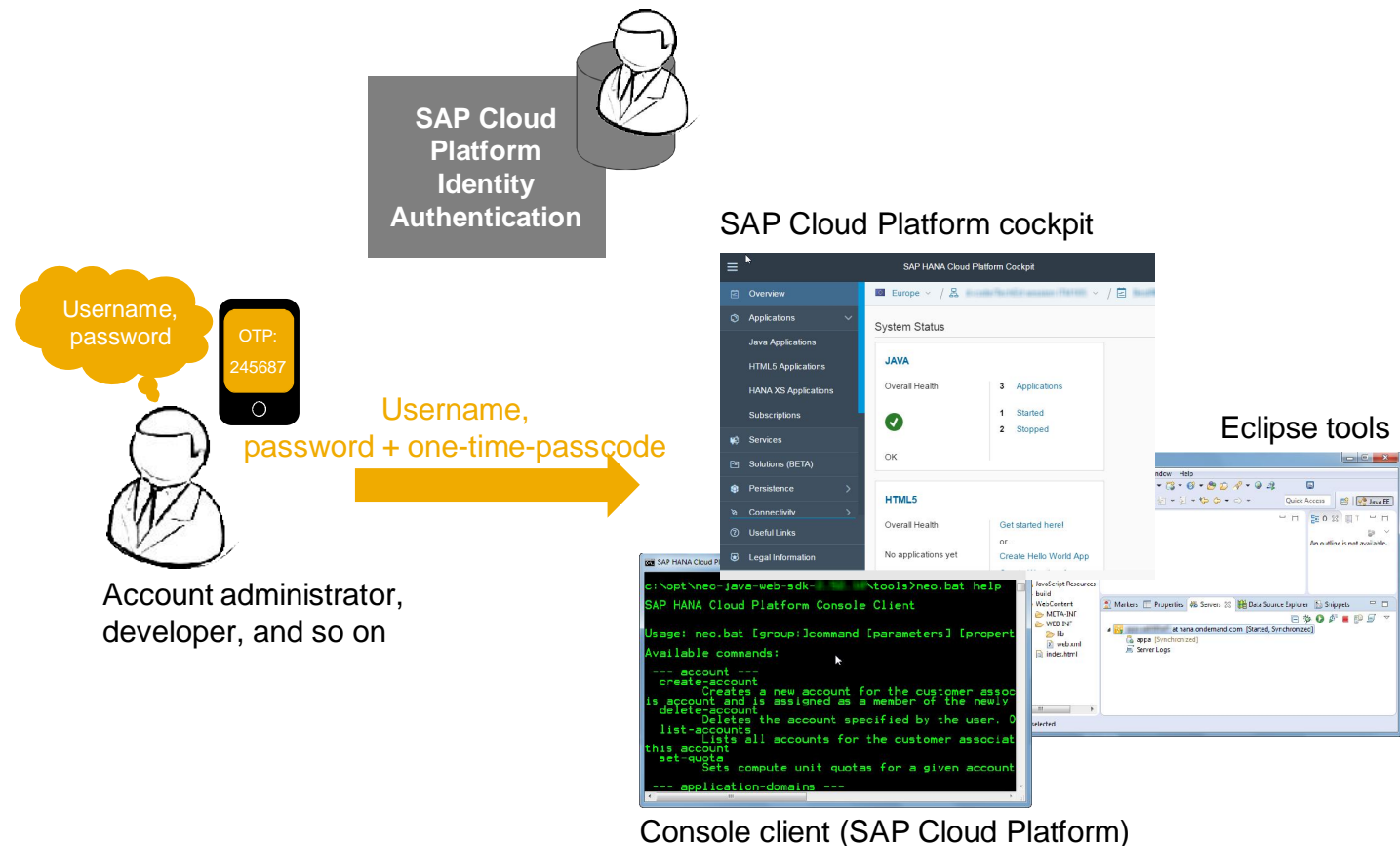
Different user types in relation to supported identity provider (IdP)

 Operators	Employees of platform or infrastructure provider	Corporate directory, VPN, two-factor authentication No IdP support
 Platform users	Customer: administrators, developers, and support	SAP ID service SAP Cloud Platform Identity Authentication (two-factor authentication)
 Business users	End-users of applications	Any SAML 2.0–compliant IdP

This is the current state of planning and may be changed by SAP at any time.

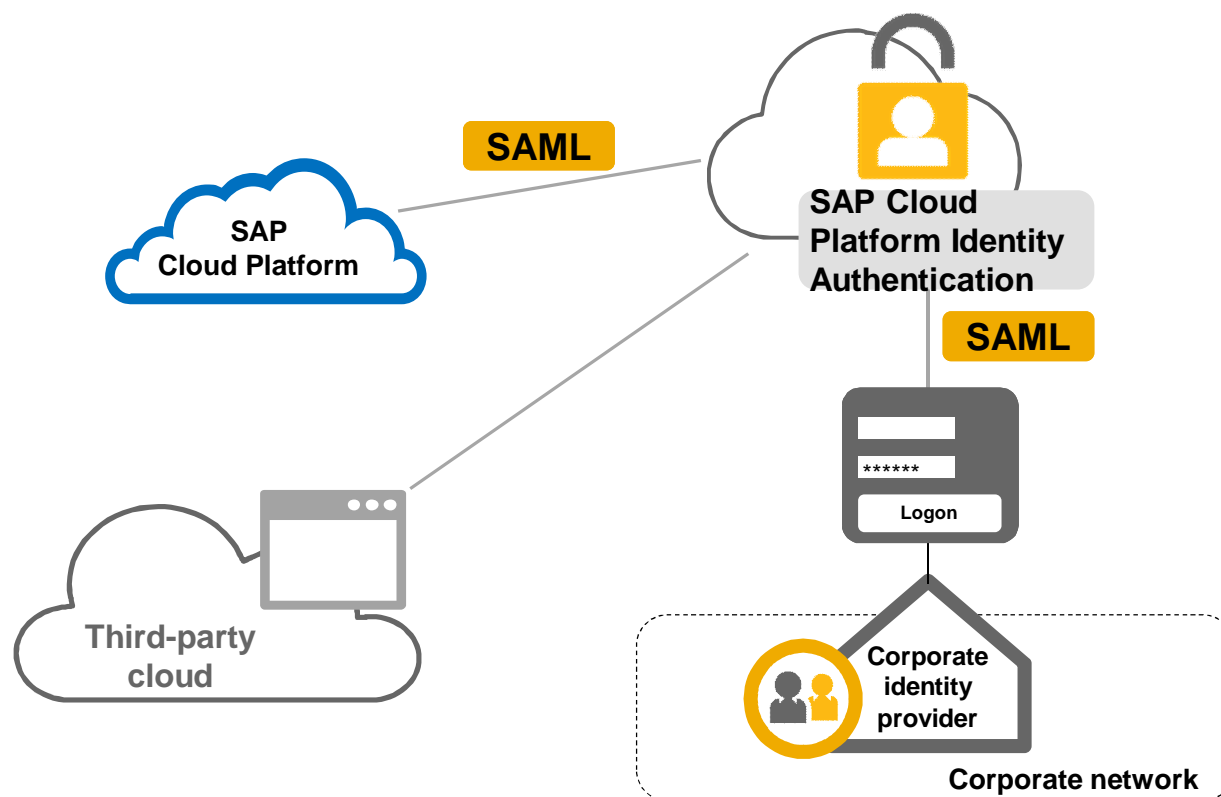
Configurable identity provider for administration of SAP Cloud Platform

- Customers can use their own SAP Cloud Platform Identity Authentication tenant for managing administrators and developers of SAP Cloud Platform instead of using SAP ID service
- This enables customers to use advanced security features, such as:
 - Configurable password policy
 - Strong, two-factor authentication
 - User provisioning to SAP Cloud Platform Identity Authentication is possible



This is the current state of planning and may be changed by SAP at any time.

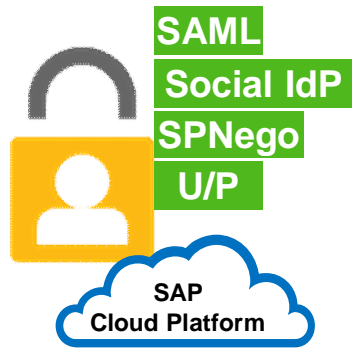
SAP Cloud Platform Identity Authentication as a proxy to a corporate IdP



Identity provider (IdP) proxy

- Y Delegation of authentication to corporate identity provider login
- Y Reuse of existing single sign-on infrastructure
- Y Easy and secure authentication for business-to-employee (B2E) scenarios
- Y Federation based on the SAML 2.0 standard

Identity provider options on SAP Cloud Platform



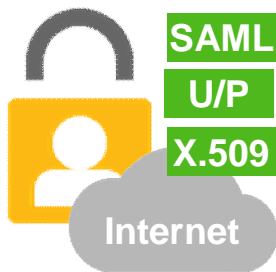
SAP Cloud Platform Identity Authentication

- § Cloud solution for identity lifecycle management
- § Pay per logon requests (counted once per day and user)
- § Isolated user base per tenant
- § Full Web-based user lifecycle management
- § Rich customization and branding features
- § Main scenarios: B2C and B2B
- § Preconfigured, trusted IdP for productive accounts on SAP Cloud Platform



Bring your own Identity provider

- § Prerequisite: SAML 2.0 compliance
- § Main scenario: B2E
- § * Product-specific support for authentication mechanisms, such as Kerberos, X.509, and so on



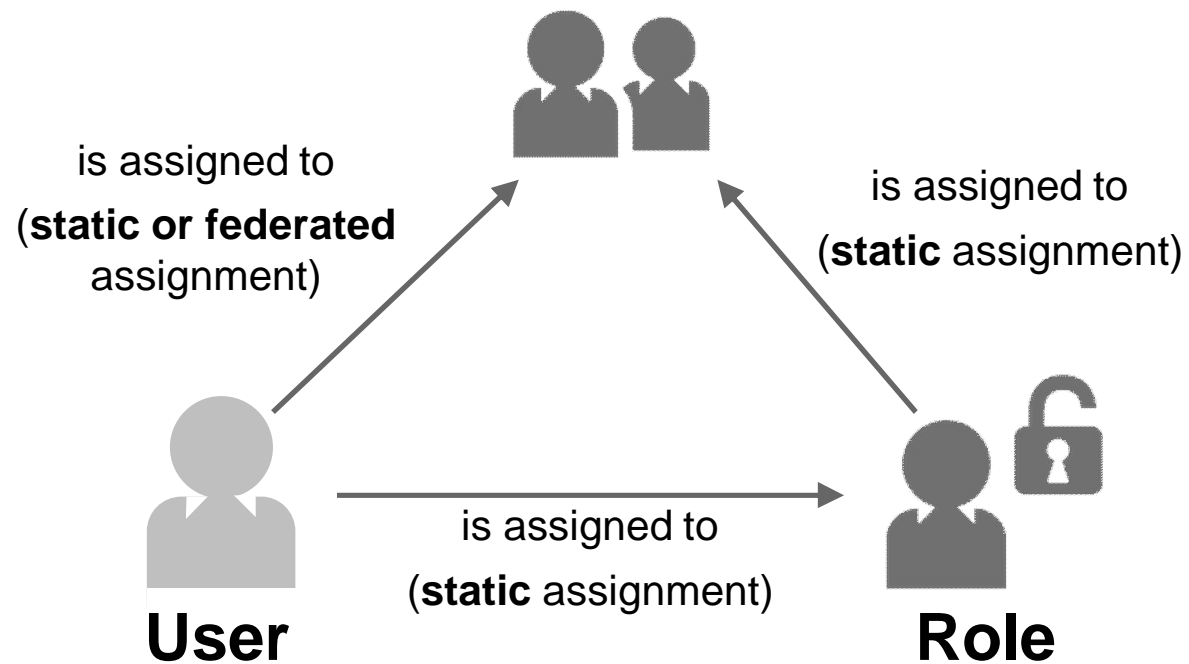
SAP ID service

- § Public SAP identity provider (IdP) on the Internet
- § Free service, similar to social IdPs
- § Shared user base with SAP Community and other SAP Web sites
- § Authentication only - no user lifecycle management
- § Default IdP for trial accounts for SAP Cloud Platform

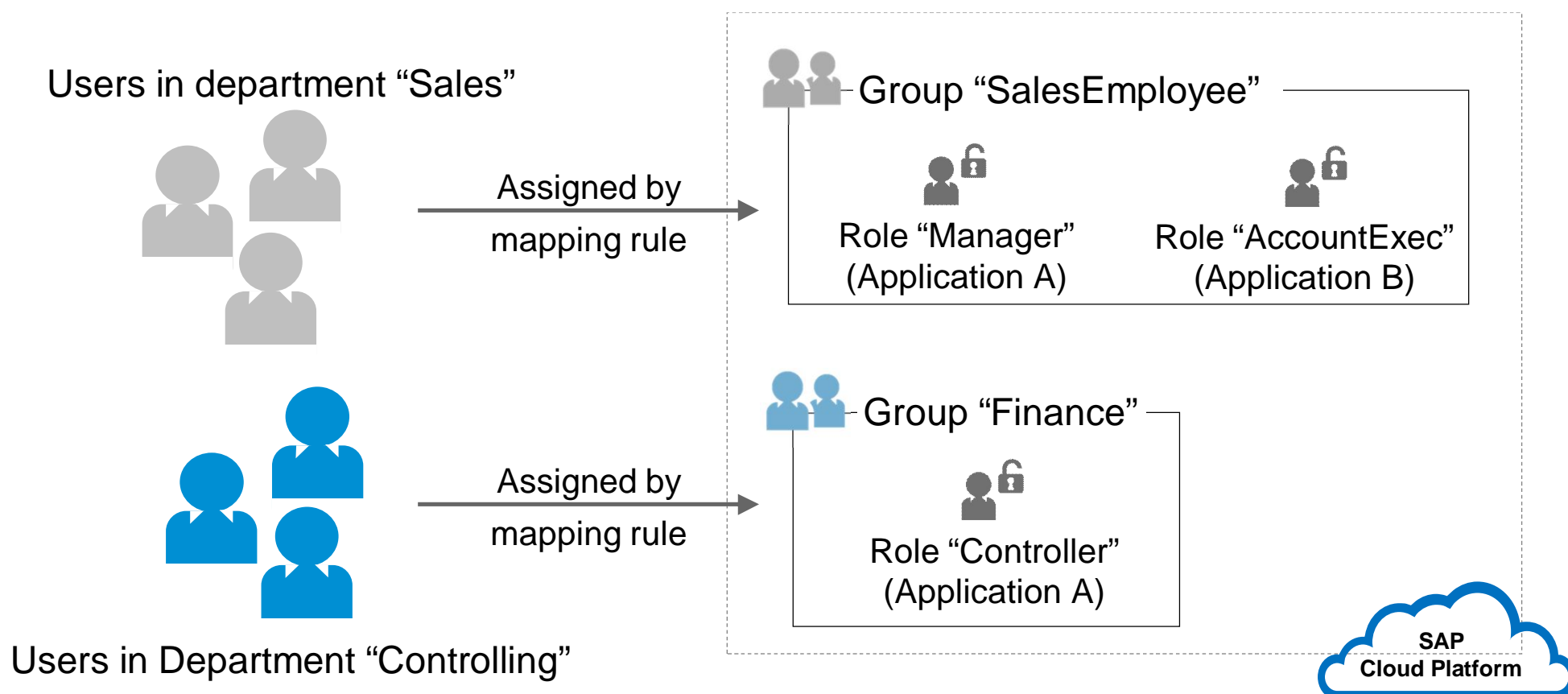
Authorization management

User, role, and group

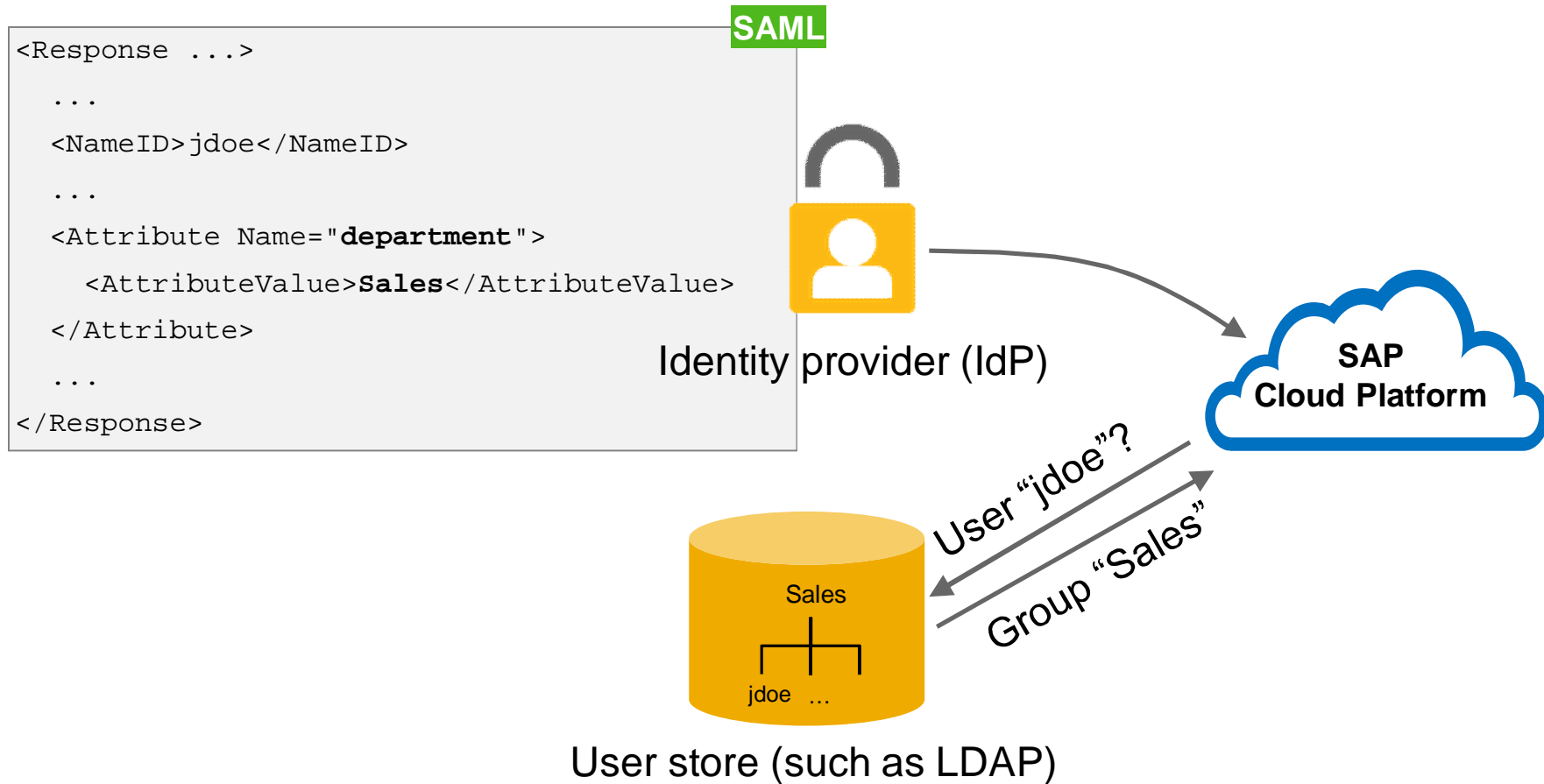
Group or role collection







Federated role assignment



Sources for federated role authorizations



Authorization management in runtimes of SAP Cloud Platform

Runtime				
Authorization objects	<ul style="list-style-type: none"> Java EE roles (web.xml) Custom roles (SAP Cloud Platform cockpit) 	<ul style="list-style-type: none"> Role templates Role collections Custom roles (attributes) 	<ul style="list-style-type: none"> Permissions (neo-app.json) Custom roles (SAP Cloud Platform cockpit) 	<ul style="list-style-type: none"> Privileges (.xsprivileges) Roles (.hdbrole)
Authorization management	<ul style="list-style-type: none"> Static Dynamic (federated authorizations) 	<ul style="list-style-type: none"> Dynamic 	<ul style="list-style-type: none"> Static Dynamic (federated authorizations) 	<ul style="list-style-type: none"> Static

Platform APIs for authorization, trust, and OAuth client management

- § **Authorization management API**
Management of users, roles, groups, and their assignments within the account
- § **Trust management API***
Management of SAML 2.0 trust settings such as local service provider and trusted providers within the account
- § **OAuth client management API ***
Management of OAuth clients, scopes, and access tokens for an account

➔ **APIs are protected with OAuth 2.0**

* Planned innovations or future direction

© 2017 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC

<https://api.hana.ondemand.com/authorization/v1/documentation>

Authorization Management API documentation
version v1

<https://api.hana.ondemand.com/authorization/v1>

The authorization management REST API provides functionality to manage roles and their assignments to users. Roles can be provided within the web.xml or web-fragment.xml and will be extracted during the deployment of the application. Roles deployed with the application are visible for all subscriber accounts unless their shared flag is marked to false. Roles can also be created on subscription level. Assignments for those roles can be established only in the same subscription.

Protection

The API is protected with [OAuth 2.0](#).
Token Endpoint: <https://api.hana.ondemand.com/authorization/v1/apitoken/v1>
Supported grant types: Client Credentials Grant

To use this REST API, you need to get OAuth client credentials (client ID and secret) from SAP HANA Cloud Platform using the [cockpit](#). After that, you need to pass the obtained client credentials to the SAP HANA Cloud Platform token endpoint to obtain an [access token](#). In the requests to this API, include the access token as a header with name Authorization and value Bearer <token value>. The issued token is valid 25 minutes.

Users

Manage role assignments to the specified user.

</accounts/{accountName}/users/roles> GET PUT DELETE

Roles

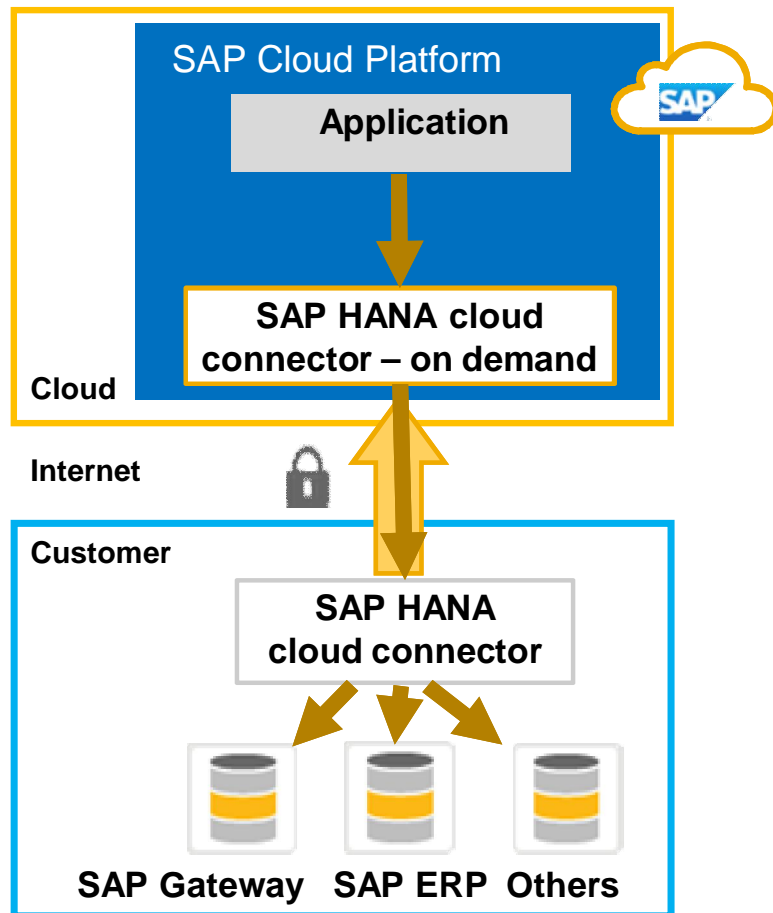
Manage roles and their assignments to users in the specified account and application. Roles can either be deployed with the application or created via the API. Roles deployed with the application are visible for all subscriber accounts unless their shared flag is marked to false. Roles created via the API are visible only within the account for which they are created.

</accounts/{accountName}/apps/{appName}/roles> GET POST PUT DELETE

</accounts/{accountName}/apps/{appName}/roles/users> GET PUT DELETE

Secure back-end connectivity

SAP Cloud Platform Connectivity service

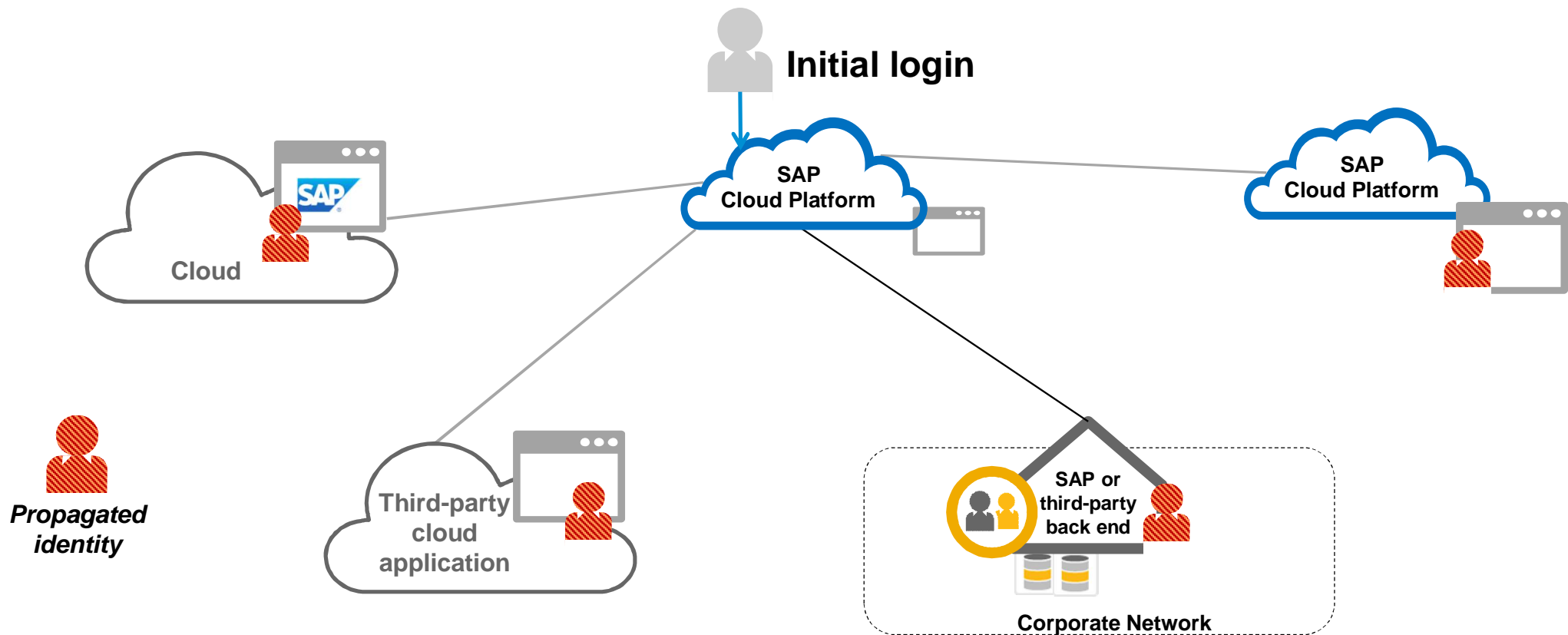


- § Establishes **secure VPN connection** between the SAP Cloud Platform and on-premise systems
- § **Requires no changes** in the existing **corporate firewall** configuration
- § **Initiates encrypted connections** to cloud application from inside the **on-premise network** to the cloud
- § **Provides capabilities to secure access** to on-premise systems
 - Fine-grained access control lists of allowed cloud and on-premise resources
 - Fine-grade audit logging for traceability
 - Trust relation with on-premise system based on X.509 certificates

Identity propagation

Different scenarios for identity propagation

SAP Cloud Platform offers services based on configuration level



Thank you

Contact information:

Jürgen Adolf

Product Manager

Dietmar-Hopp-Allee 16,

Walldorf 69190,

Germany

