SAP Cloud Platform

Security in SAP® Cloud Platform: Trust Matters

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

Run Simple

Table of Contents

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

SAP® Cloud Platform is an essential part of SAP's digital strategy. It is the platform for our customers' and partners' transformation journey toward digital business models. This open platform as a service (PaaS) provides unique in-memory database and application services. It is the proven cloud platform that enables you to rapidly develop new applications or extend existing ones, all in the cloud. Our customers' **trust in the security of SAP Cloud Platform** remains the ultimate currency.

This document provides you with an understanding of our comprehensive approach to security in SAP Cloud Platform. Beyond this, the document gives an overview of the available security services in SAP Cloud Platform and of their functional capabilities. They are an integral part of our offering, and they support you when you entrust your processes and data to SAP Cloud Platform.

Out there in the marketplace, one can find an ever-increasing number of cloud offerings. Security has become a competitive differentiator. We at SAP rely on more than 40 years of experience to provide thorough security for our cloud platform. This security is the result of a multitude of diligently designed, planned, and implemented measures. They span all the different aspects necessary to provide our customers with a cloud solution that has one of the highest levels of security in the industry. In this document, we touch on many of these measures to be as transparent as possible and to give you confidence when you choose SAP Cloud Platform.

DATA CENTERS AND PHYSICAL SECURITY

In a cloud world, data no longer remains locked inside the safe walls of a customer's own data center. Instead, it moves into the cloud, which consequently means building a strong partnership with your cloud provider. To support your digitalization strategy, we at SAP use SAP-owned data centers in combination with private space (collocation facilities) that we rent from external data center providers (collocation providers) as well as from infrastructure-as-a-service (IaaS) cloud providers around the world. This ensures a global reach and fast growth in various countries.

All SAP data centers fulfill at least Level 3 of SAP's data-center-level rating system. First and foremost, this means that we apply the "n+1 principle," meaning that if n items of equipment are required for something to work, there is always one additional item. That is, if any one item of equipment breaks down, everything can still work as intended. We follow this principle for various data center capabilities, including the number

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

of transformers to power the data center; the number of uninterruptible power supply systems and cooling systems; and the number of available wide-area-network and local-area-network connection lines. The availability of power generators, fire detection equipment, and fire extinguishing systems adds to these data center capabilities. Meanwhile, data center personnel ensure that on-site response times are less than 60 minutes. Additionally, SAP demands industry-standard attestations and certifications so that we can show our customers the secure and reliable operations and control framework of our collocation and IaaS providers.

Regardless of whether data is stored in an SAP-owned data center or in a collocation data center, the same procedures and standards apply:

- SAP does not transfer customer data outside the predefined region (unless the customer has been notified or such transfer is a feature of the solution), nor does SAP share it with unauthorized third parties.
- The collocation provider has no administrative access to the SAP cloud servers.
- The collocation provider's services focus only on the provision of power, cooling, and data center space.

Data center security goes beyond securing the facilities; it also encompasses the human factor. All SAP data centers and the areas surrounding them are monitored by security guards on a 24x7 basis using closed-circuit-television surveillance cameras. Perimeter intrusion detection systems such as motion sensors are also in place to detect unexpected access. All movements generate an alarm that is monitored by security staff. To ensure proper functionality, the sensors and surveillance cameras are maintained on a regular basis. As a minimum requirement for access, security badges must be shown. In some data centers, SAP has implemented stronger access controls, including biometrics.

All SAP data center providers keep a log of the names of people entering the server areas used for services for SAP Cloud Platform within the SAP data centers, and of the times they entered. A request workflow for access to the SAP data center facilities is implemented and aligned with SAP. Requests are approved by authorized managers. If the access request is not renewed after a specified period, access is terminated automatically after a certain amount of time.

The security architecture of SAP Cloud Platform aims to establish security measures that are among the highest in the industry. This security is the result of multiple diligently designed, planned, and implemented measures.

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

SECURITY ARCHITECTURE

The security architecture of SAP Cloud Platform aims to establish security measures that are among the highest in the industry. As a public PaaS offering, SAP Cloud Platform is a multitenant environment, which allows the execution of custom code. Therefore, an important security objective is the isolation of customer systems and data flows between them and services for SAP Cloud Platform. This is achieved by two lines of defense:

- **Application sandboxing:** Restricting and managing the capabilities of an application within the container in which it runs
- **Network sandboxing:** Restricting and managing the capabilities of an application to access other systems in the landscape

The following overview concretizes this:

- **Customer and network segregation:** SAP Cloud Platform is set up in a fenced network, separated from the SAP internal network. Customer applications run in sandboxed environments, isolated from each other and isolated from the systems that provide the services and manage the infrastructure for SAP Cloud Platform. The internal traffic is controlled by firewalls. Administrative access for SAP is managed through a terminal service that requires strong authentication.
- **Secure communication:** SAP Cloud Platform is configured to use secure communication in accordance with the protection requirement of the transmitted information. Suitable measures for securing the exchange of information are used. For strong encryption methods and keys, SAP uses at least a 128-bit symmetric key or a 2,048-bit asymmetric key, as well as strong and internationally recognized cryptographic algorithms.
- **Secure application containers:** SAP Cloud Platform supports multiple programming models (for example, Java and Java EE, SAP HANA®, and HTML5). The application containers offered as a service are secured by default, according to the latest Web application security best practices. Additionally, the containers provide state-of-the-art capabilities to application providers to implement secure applications.
- **System hardening:** All systems in the stack for SAP Cloud Platform are hardened. This means that all nonessential services are deactivated in the system. In addition, user accounts that are not required are deleted.
- **Client media encryption:** Device encryption is established for storage of data at rest on laptops, desktops, and mobile devices if used for the data classified as "confidential," including customer data. By default, all SAP-controlled laptops and PCs are supplied with an encrypted hard drive.
- **Deletion of data:** Backup data is retained for a period of 14 days. Logs from customer applications are retained as follows:
  - Maximum of 14 days for development logs
  - Maximum of 18 months for audit logs, unless an extended retention period is required by the customer

  The following conditions apply, as long as permitted by the applicable local laws and industry-specific regulations:
  - All paper materials are shredded after termination of the customer contract.
  - Customer data on SAP Cloud Platform is deleted upon customer request and according to the conditions agreed to between SAP and the customer.

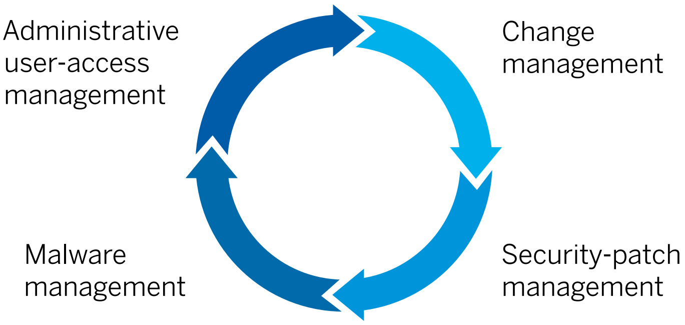
© 2017 SAP SE or an SAP affiliate company. All rights reserved.

OPERATIONAL SECURITY MANAGEMENT

To assure the reliability, integrity, availability, and authenticity of your data, it is essential that we at SAP operate SAP Cloud Platform securely. Our operational security management operations are described below and summarized in Figure 1:

- Change management follows a formal process that is reviewed and approved regularly. Starting with an impact analysis of the change prior to implementation, change requests are consequently planned, tested, tracked, and maintained.
- SAP's security-patch management process mitigates threats and vulnerabilities. SAP's security team rates security patches based on the Common Vulnerability Scoring System standard for operating systems, databases, and virtualization in cloud services. Critical security vulnerabilities that might endanger SAP's service delivery capabilities in SAP Cloud Platform are patched on a priority basis.
- Securing SAP Cloud Platform requires sophisticated malware protection. Therefore, SAP has defined and implemented a malware management process with which we consistently and continuously ensure secure service delivery free of viruses, spam, spyware, and other malicious software. It comprises antimalware agent deployment, regular scans, and malware reporting processes.
- SAP's comprehensive administrative user access management follows the principles of minimal authorization (the need-to-know principle) and segregation of duties. Administrative access to data processing systems in SAP Cloud Platform is subject to strict requirements for personnel and is managed by an access management tool for cloud services. Each access request is assessed by authorized approvers who define the validity of the access. Only a limited number of authorized persons have administrative access rights to this access management tool.

Figure 1: Four Aspects of Operational Security Management


Administrative user-access management
Change management
Malware management
Security-patch management

To react swiftly when employees leave SAP, the aforementioned access management tool is synchronized with the corporate human resources and enterprise resource planning system on a daily basis. Thus, user accounts of employees who leave SAP are automatically deactivated with immediate effect in the access management tool.

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

INCIDENT, THREAT, AND VULNERABILITY MANAGEMENT

The increasing interconnectivity of companies and businesses across the globe has led to an unprecedented exposure of IT systems to the Internet, making it highly attractive to hackers. As companies continue to build new applications and deploy them in their on-premise and cloud environments using SAP Cloud Platform, there is an even stronger need for security across such a hybrid infrastructure. Consequently, SAP has implemented a security incident management process that is aligned with the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27035:2011 information security principles. Security incidents are monitored and tracked by security specialists in cooperation with defined communication channels until resolved. A security breach involves the accidental or unlawful destruction, loss, alteration, or disclosure of customer personal data or confidential data. Or it may refer to a similar incident involving personal data for which a data processor is required under applicable law to provide notice to the data controller.

Transparency is one foundation for trust: once we become aware of any security breach, we promptly inform our customers. The notification is communicated through the defined communication channel and contains the following information:

- Details relating to the security incident that has occurred, known at the time of notification
- The IT infrastructure or application affected by the security incident
- An overview of the mitigation actions performed to restore security
- All further applicable notifications required by country-specific regulations "on obligation to notify"

To prepare for the unknown, SAP has established security information and event management systems for analysis, reporting, and alerting. All critical systems and infrastructure components within SAP Cloud Platform log relevant data, which is stored for a minimum of six months. Data security is ensured through security configuration compliance checks and event monitoring. On top of this, general security monitoring is performed 24x7 for all activities. Once a warning or an alert comes up, it is processed through our ticketing system, and critical events are handled according to the incident management process.

An important security objective is the isolation of customer systems and data flows between them and services in SAP Cloud Platform. This is achieved by application sandboxing and network sandboxing.

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

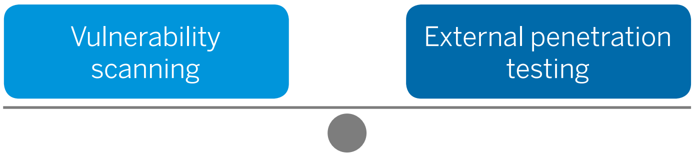
To identify vulnerabilities before others do, our vulnerability management focuses on early identification, assessment, and mitigation of common known vulnerabilities and configuration issues that might pose a potential risk to the integrity and security of systems and services. It covers, but is not limited to, vulnerability scanning and external penetration testing (see Figure 2):

- **Vulnerability scanning:** Vulnerability scans are performed at least four times a year to ensure the highest possible level of security while at the same time adhering to relevant controls in compliance and certification audits. SAP prioritizes vulnerability remediation to reduce risk and impact to customer data and business processes. The assessed and prioritized vulnerabilities are followed up within the security-patch and change management processes.
- **External penetration testing:** All Internet-facing systems (for example, firewalls, load balancers, gateways, and Web application servers) are scanned on a weekly basis. In addition, manual verification and penetration testing is performed to validate risk and priority. Biannual assessment and penetration tests are performed by independent security researchers to verify the security posture of the external and Internet-facing cloud infrastructure. Findings from the penetration testing are followed up according to criticality.

In order to proactively manage new security threats and vulnerabilities that might affect SAP Cloud Platform, SAP has established its own computer emergency response team (CERT). Additionally, SAP's CERT is continually in contact with other external CERTs to exchange relevant information. The response team has established suitable controls and measures for analyzing relevant security threats and vulnerabilities. It assesses risks and develops and deploys countermeasures when appropriate.

Security in the age of digitalization will remain a neck-and-neck race between cybercriminals and cloud solution providers. We at SAP are continually preparing ourselves to safeguard your business.

Figure 2: Managing Threats and Vulnerabilities



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

DATA GOVERNANCE AND LEGAL COMPLIANCE

The confidentiality of your data is paramount to SAP. All customer data processed in SAP Cloud Platform belongs to the customer and is classified as "Confidential" according to SAP's data classification standard, unless the customer chooses to make it visible to the public by means of tools and services within SAP Cloud Platform.

The handling of data classified as "Confidential" includes, but is not limited to, the following protections:

- Access authorization is provided only for specific groups whose members are determined by their role (for example, cloud operations), following the need-to-know principle.
- Disclosure to third parties happens only after these parties become subcontractors by signing agreements that contain sufficient confidentiality language.
- Encryption is required for transfer outside the SAP network.
- Device encryption is required for storage on SAP-controlled laptops, desktops (in case the desktop is operated outside of secured rooms or buildings), and mobile devices.
- Storage infrastructure is provided only by SAP or subcontractors.

Legal requirements are of utmost importance for us, so secure handling of personal data is paramount. At SAP, corresponding intercompany agreements exist to help ensure that legal requirements for handling of personal data are met in all SAP companies and branch offices throughout the world. Similar data protection agreements are executed with all subprocessors. In addition, SAP has established and implemented a certified data protection management system (DPMS), which is based on the British Standard "BS 10012:2009 Data Protection." The implementation and the overall process of the DPMS are internally and externally audited as part of an annual audit cycle.

Our employees' awareness of the sensitivity of data handling is one key pillar for data protection. Every SAP employee who could have access to data stored within SAP Cloud Platform must successfully complete human resource security measures in accordance with applicable law. Employees are bound by SAP's employment documents package, which comprises a code of business conduct that explains policies and a confidentiality agreement that must be acknowledged and either digitally signed or signed in writing by the selected candidates.

SAP has defined and implemented a malware management process with which we consistently and continuously ensure secure service delivery free of viruses, spam, spyware, and other malicious software.

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

A confidentiality and privacy statement (CPS) and other contractual confidentiality provisions are mandatory for all of SAP's vendors and third-party service providers that perform services on behalf of SAP and that have access to confidential information. They must sign the CPS, either digitally or in writing, before they are granted access to SAP software systems and protected areas.

Furthermore, mandatory security awareness training sessions are conducted on a regular basis. The training is designed not only for vendors and third-party providers but also for SAP employees.

Unlike most PaaS offerings, SAP Cloud Platform can – by customer request – optionally be operated and supported in European Union (EU) access mode. Only SAP employees who are located in European Economic Area member countries (EU, Iceland, Liechtenstein, and Norway) or Switzerland can operate and support customer data. This European data protection service is available to customers both inside and outside the EU.

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

SAP Cloud Platform is certified according to ISO 27001:2013, SSAE 16-SOC 1/ISAE 3402* Type 2, and SOC 2 Type 2 security standards and SAP regularly prepares the relevant audit reports.

Our vulnerability management focuses on early identification, assessment, and mitigation of common known vulnerabilities and configuration issues that might pose a potential risk to the integrity and security of systems and services.

*SSAE = Statement on Standards for Attestation Engagements; SOC = Service Organization Control;
ISAE = International Standard on Assurance Engagements

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

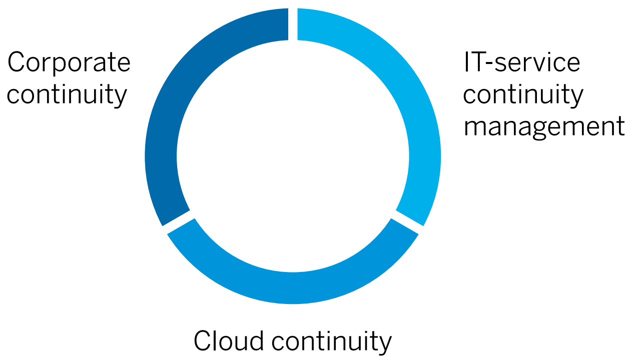
SERVICE RESILIENCE

At the core of SAP's service resilience for SAP Cloud Platform is our business continuity management. SAP has implemented business continuity management aligned to ISO 22301 as part of our management framework for business continuity and operational resilience. The key pillars of this framework are outlined below and summarized in Figure 3:

- The corporate continuity framework enables SAP to respond and adapt rapidly to threats posed against the company. In doing so, SAP follows an all-hazard approach that incorporates handling of all types of disruptive incidents or situations and prepares for specific scenarios that are most likely to happen and recur. This allows SAP to prepare and protect its workforce and enables continuity in critical decision making.
- The IT service continuity framework addresses all risks that could cause a sudden and serious impact on IT infrastructure, threatening the continuity of supported business processes at SAP. In doing so, it helps to prevent and prepare for any major disruptive event and to secure ongoing IT operations during emergencies in order to continue with the provision of services to internal as well as external customers.
- Cloud continuity covers disaster recovery for specific scenarios, such as the total loss of a data center, which could seriously impact the availability of the cloud infrastructure, as bundled in service models and delivered as a service. SAP aims to ensure that it meets customer demands for higher operational resilience of on-demand products and services with respective offerings.

SAP's data center location strategy and data backup processes contribute significantly to our service resilience. SAP maintains backup data centers to enable the off-site storage of customer backup data. SAP uses a backup data center site within the same region as the primary SAP data center whenever possible. In addition, SAP has a formal system backup process and schedule for SAP Cloud Platform, which includes hardware-independent restore and recovery capabilities. All backups are run automatically; their frequency depends on system availability requirements. Appropriate processes and automated tools are in place to validate backup integrity, and backup logs are reviewed daily to detect and correct backup failures. Backups are stored in data center locations on redundant media in the designated region.

Figure 3: Pillars of Business Continuity Management



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

The standard subscription fee for SAP Cloud Platform includes a standard disaster recovery option. It is based on data restore from a backup site. The recovery point objective has no strict service-level agreement, but the objective is 24 hours. The recovery time objective is “best commercially reasonable effort” to restore service as soon as possible at the time of disaster. “Disaster” means an event of substantial extent causing significant disruption to the delivery of services from SAP Cloud Platform and may include physical damage to or destruction of the SAP data center or computing environment. It can be a natural disaster, such as a flood, hurricane, tornado, or earthquake, or a human-induced disaster, such as a hazardous material spill, infrastructure failure, or bioterrorism attack. A disaster is typically not limited to one individual system or landscape but usually involves larger parts of an infrastructure.

SECURITY SERVICES IN SAP CLOUD PLATFORM

SAP offers different mechanisms for ensuring that only approved users have access to SAP Cloud Platform.

SAP Cloud Platform Identity Authentication

With the SAP Cloud Platform Identity Authentication service, you can provide your employees, customers, and partners with simple and secure cloud-based access to the business processes, applications, and data they need. Featuring state-of-the-art authentication mechanisms, secure single-sign-on functionality, on-premise integration, and convenient self-service options, SAP Cloud Platform Identity Authentication simplifies the user experience in the cloud.

SAP Cloud Platform Identity Authentication is based on trusted security standards. You can establish authentication and single-sign-on mechanisms with proven technologies such as the Security Assertion Markup Language. You can also connect several identity providers to set up a comprehensive network of identity checks tailored to your specific requirements.

> Our employees’ awareness of the sensitivity of data handling is a key pillar for data protection. Every SAP employee who could have access to data stored within SAP Cloud Platform must complete security measures in accordance with applicable law.

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

SAP Cloud Platform Identity Authentication supports the security needs of your application with two-factor authentication. If an application requires a higher level of security, a two-factor authentication service is just a click away. After providing correct credentials, users are immediately asked to enter a one-time passcode that expires in 30 seconds to invoke the application.

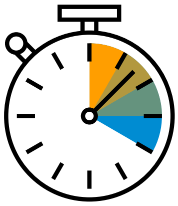
Administrators gain one central entry point for configuring user management processes for all cloud-based applications. The service also centralizes account management tasks and supports identity federation. With all internal and external identities in one place, administration is more efficient, less prone to error, and more secure.

SAP Cloud Platform Identity Provisioning
The SAP Cloud Platform Identity Provisioning service offers a comprehensive approach to identity lifecycle management in the cloud, enabling a high level of security. This cloud service allows customers to centrally manage identities and optimize access and compliance processes across the enterprise, reducing risks in accordance with compliance policies. It can be used independently or integrated with the SAP Cloud Platform Identity Authentication service.

This service helps to speed up the onboarding of users for cloud-based business applications while at the same time increasing security and compliance by extending existing identity lifecycle management toward business applications in the cloud. In addition, SAP Cloud Platform Identity Provisioning reduces the complexity of managing identities in a hybrid system landscape. Finally, it provides fast time to value, based on a lean consumption model with simple yet flexible configuration options.

SAP Cloud Platform Identity Provisioning allows you to rely on an existing user store such as Microsoft Active Directory, the SAP NetWeaver® Application Server component for ABAP®, SAP SuccessFactors® solutions, and SAP Cloud Platform Identity Authentication as the single source of truth for identity data.

Identities and privileges can then be provisioned to cloud solutions such as the SAP Hybris® Cloud for Customer solution or the SAP Jam™ collaboration platform. The complete and up-to-date list of supported applications can be found in the service documentation. As the SAP Cloud Platform Identity Provisioning service supports the system for cross-domain identity management (SCIM) industry standard, you can also integrate other SCIM-compatible applications.



Security in the age of digitalization will remain a neck-and-neck race between cybercriminals and cloud solution providers. We at SAP are continually preparing ourselves to safeguard your business.

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

www.sap.com/contactsap

Run Simple

Studio SAP | 50863enUS (17/05)

© 2017 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 platform 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 http://www.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information and notices.