SAP Products and Solutions

SAP Product and Cloud Security Strategy

Table of Contents

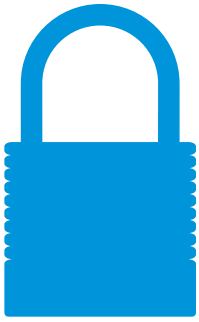
SAP's Commitment to Security

As the dependency on IT systems continues to grow in both the private and public sectors, the threat landscape is constantly changing. In particular, emerging advance persistent threats (APTs) such as "Stuxnet," the "Duque" worm, and "Red October" present an unprecedented quality of attacks on the IT community. In the era of APTs, many traditional security-protection techniques are frequently bypassed, and malicious exploits can reside undetected in critical systems for years. Recent debate over government data-access programs has created more mistrust within this changing threat landscape and reinforces the need for security of critical information systems.

Developing products and providing cloud services, SAP is fully committed to security and privacy. The company has a long tradition of clearly understanding our customers' expectations regarding confidentiality, integrity, and availability when they entrust their businesses to SAP® software systems and services. Our customers can rely on the fact that SAP constantly monitors the evolution of the threat landscape, adjusting countermeasures to mitigate evolving threats before they impact their businesses.

Thanks to cloud computing, core business applications are now available to everyone, from the largest enterprises to small and midsize companies. Customers need to be comfortable with putting mission-critical information on third-party servers. Security concerns in a cloud model are similar to those for the application service–provider model; that is, concerns about whether people will steal information, or that leaks will compromise confidential data, span models. The SAP Cloud portfolio provides robust security controls based on best practices to mitigate these issues. These controls also apply to cloud-delivered software created by SAP partners.

Active collaboration between SAP's product security and cloud security teams helps ensure that we implement proper security and compliance in cloud solutions from SAP. Identified issues are communicated directly to the product development team to expedite fixes. Through strong team cooperation, we can define proper security requirements for our cloud products, and we can implement those requirements consistently throughout the product lifecycle. This is a key advantage for our customers. Whether SAP offerings are developed to be run on premise or in the cloud, our strong commitment to security and data protection helps ensure that SAP products can be operated securely.



Whether SAP offerings are developed to be run on premise or in the cloud, our strong commitment to security and data protection helps ensure that SAP products can be operated securely.

Secure Product Development at SAP

Product development at SAP encompasses a wide variety of well-established practices and internal procedures that position security as an integral part of the software development process. Our security development lifecycle (SDL) is closely aligned with ISO 27034 requirements and incorporates the experiences that embody a 40-year track record of providing security and reliability to customers. The SDL covers all relevant areas, from modern training formats such as e-learning and gamification to our threat-modeling methodology, mandatory static analysis (source-code scanning), a comprehensive security testing strategy, and a solid security response process.

On the technical side, SAP products and solutions are developed and deployed with a leading-edge set of security features.

For example, in the field of encryption in the cloud, search over encrypted data (SEEED) is SAP's most recent security research project. SEEED is a prototype integrated with the SAP HANA® platform. It demonstrates how sensitive data and its processing can be outsourced to the cloud without any trust assumptions on the cloud provider or service consumers, while maintaining the advantages of cloud-based data processing and storage.

As a founding and current board member of the Software Assurance Forum for Excellence in Code (SAFECode), SAP clearly demonstrates the importance of industry-wide cooperation to partner, learn, and jointly contribute to the further evolution of software security in all industries.

The entire set of measures provides the foundation for product security at SAP.

While building secure products is an important prerequisite for achieving the desired level of security, securing systems against APT vulnerabilities, exploits, and attacks is critical as well.

Most SAP customers develop large amounts of their own code on top of SAP standard code. While SAP code runs through the SDL before shipment, custom code often does not. Therefore, custom code often fails to receive adequate attention from security development experts or does not have the right security scan tools applied to it. However, if code delivered and serviced by SAP is secure while custom code still has issues, the overall security level of the SAP software system landscape at customers will most likely not meet their expected level of security.

To meet this security challenge, SAP is currently focusing not only on detecting security-relevant anomalies in SAP landscapes as early as possible, but also on securing the complete stack – not SAP standard code only – enabling customers and partners to secure their coding projects as well.

Based on research done by our security research group, SAP has started to develop an enterprise threat detection solution based on SAP HANA. This will help customers to identify potential attacks and to reveal other security issues (for example, data losses or severe misconfigurations) by analyzing large amounts of data (for example, log file entries) in real time. This innovative Big Data analysis approach can achieve a higher level of security in SAP software system landscapes and beyond.

To detect known classes of vulnerabilities in the code during the development lifecycle as early and as effectively as possible, SAP has built a static analysis tool, the SAP NetWeaver® Application Server component, add-on for code vulnerability analysis, to scan large amounts of ABAP® programming language source code for vulnerabilities – and subsequently eliminate them before shipment. (For other languages, SAP uses commercial or third-party static analysis tools.) To enable customers to develop their ABAP code securely as well, we are offering customers our static analysis tool for their own use.

To enable customers to protect their huge investments in a secure end-to-end system landscape, SAP has set up a multitude of security measures. These include:

- Services and configuration guides to support a customer in configuring and hardening the existing SAP solution landscape
- A security response organization that helps ensure a timely response to security vulnerabilities detected in an SAP product after shipment by providing adequate security patches on SAP's monthly security patch day
- Continuous investment in the optimization of patch management processes for customers and tools to enable a fast and nondisruptive consumption of these patches

To complete the SAP product security strategy, we maintain a close collaboration with best-in-class security researchers. Not for external penetration testing only, the most-merited security researchers are invited to the annual SAP product security expert summit – a two-day event for SAP's internal product security expert community.

As a founding and current board member of SAFECode, SAP clearly demonstrates the importance of industry-wide cooperation to partner, learn, and jointly contribute to the further evolution of software security in all industries.

SAP's Approach to Secure Cloud Offerings

The SAP Cloud portfolio provides robust security controls based on best practices to protect confidentiality, integrity, and availability of a company's information. These controls also apply to cloud-delivered software created by SAP partners.

DATA SECURITY AND PRIVACY

SAP Cloud provides comprehensive support for data protection and privacy rights to safeguard information. This support, based on definitions of the European General Data Protection Regulation, applies to all SAP companies. If country-specific laws or other regulations require stricter standards, SAP Cloud handles personal data in accordance with those stricter laws. The software also carefully limits data access to help protect intellectual property.

SECURITY AND COMPLIANCE ENFORCEMENT

SAP Cloud incorporates strict security and compliance policies from the time a product is developed until it is operational. Regular monitoring procedures help companies immediately identify deviations from their requirements and trigger response measures to help ensure compliance. A technical validation or implementation audit further enforces and verifies proper implementation of these requirements.

PHYSICAL SECURITY AT SAP DATA CENTERS

At SAP we operate our own data centers and partner with local leaders in colocation hosting centers to provide secure, environmentally controlled facilities that offer an integrated security management system. On-site security measures include electronic photo-ID badging, cardholder access control, biometrics, recorded digital video surveillance, and alarm monitoring. All SAP data centers comply with the latest telecommunications industry standards, such as ANSI/TIA/EIA-942 Tier III or higher. Further details on SAP data centers are available at www.sapdatacenter.com.

DATA STORAGE AND LOCATION

In a cloud-computing environment, heterogeneous data from different customers may reside within a single database. Because segregation of heterogeneous data in the cloud environment is key to keeping information private, cloud vendors must demonstrate that they can meet related regulatory and privacy requirements when identifying data for a company's individual customers. SAP Cloud supports logical isolation of data within a solution that extends to the virtual server layer. In certain environments, such as the SAP HANA Enterprise Cloud service, it is possible to get physical isolation through dedicated servers for the SAP HANA database residing in virtual local area networks and other dedicated customer network segments.

The SAP Cloud portfolio provides **robust security controls** based on best practices to protect confidentiality, integrity, and availability of a company's information.

Because the physical storage location of customer data is critical for many organizations, SAP Cloud provides multiple location choices – covering Europe, the Middle East, and Africa (EMEA); the Americas; and the Asia-Pacific-Japan (APJ) regions. All locations comply with the same high standards and are interchangeable from a technical perspective.

CLOUD SYSTEM OPERATIONS

SAP sets strict business and security rules to control access to information-processing facilities and business processes. In all cases, the concept of "least privilege" determines access – meaning that users are limited to the minimum set of privileges required to perform a required function.

To help ensure secure and stable IT operations that comply with industry standards and technology best practices, SAP Cloud applies key security measures across all layers and assets and provides process-integrated internal controls. The effectiveness of those security measures and internal controls is documented by international and country-specific certifications and attestations such as ISO 27001, ISAE 3402, and SSAE 16.

SAP Cloud also includes tools to reduce potential exploitation of technical vulnerabilities. Companies can use operator and fault logs to help identify system problems. System-monitoring tools help them check the effectiveness of controls and verify conformity to information-security policies and standards embedded within SAP Cloud. In addition, SAP uses industry-leading security partners to conduct regular penetration tests on cloud-based and on-premise production environments multiple times each year.

REGULATORY COMPLIANCE AND CERTIFICATION

In 2011 SAP became one of the first vendors of cloud-based software to complete the newest SSAE 16 and SOC 2 audit successfully. Organizations interested in more details can ask their SAP representatives to provide information on all of the procedures used to secure their data in cloud solutions from SAP, along with the auditors' findings. SAP Cloud also meets the requirements of ISO 27001.

The multitiered approach implemented in SAP Cloud – which separates operating system, database, and application – helps organizations balance control and ease of use. Changes made to the cloud environment are logged, along with the users who made them, and are approved and verified through a centralized online application. This multitiered approach makes it possible for us to make modular updates and enhancements to our cloud solutions several times a year. A database can be upgraded without changing a related application, for example, and the application can be upgraded without changing the database. SAP constantly reviews, updates, and publishes our cloud-certification road map. Our customers' requirements influence the road map, and the internal attestation and certification team add certifications and attestations based on actual business cases.

LEARN MORE

To learn more about how SAP can help your organization improve system security, call your SAP representative today or visit us on the Web at www.sap.com.

The Best-Run Businesses Run SAP®