SAPinsider
This article appeared in the Oct ▪ Nov ▪ Dec 2017 issue of *SAPinsider* (www.SAPinsiderOnline.com) and appears here with permission from the publisher, WIS Publishing.
WIS pubs

**Gerold Hübner**
(gerold.huebner@sap.com) is Chief Security and Compliance Officer for SAP Cloud Platform, where he manages the team that handles data protection, security and secure development, certifications, and security-enabling functions such as authentication and single sign-on for SAP Cloud Platform. Prior to this role, Gerold led SAP's central product security team and for 11 years worked in security-related positions at Microsoft.

# Securing the Cloud with SAP Cloud Platform

## How SAP's Security Strategy Builds Trust and Enables a Secure Digital Transition

SAP Cloud Platform is an essential ingredient of SAP's digital strategy. Built using Cloud Foundry technology and principles, SAP Cloud Platform is SAP's open source platform-as-a-service for running, building, extending, and integrating business applications. It enables SAP customers and partners to make the move to the digital business model required to succeed in the new economy.

Security is a major concern for anyone considering this transition, however — along with the benefits of digitizing come increased risks due to code vulnerabilities, missing implementation of security patches, and misconfigurations, to name a few. These risks, combined with the volume and value of data that could be extracted or altered, can lead to significant security threats. SAP minimizes these risks for customers and partners with a comprehensive strategy that ensures the highest levels of security for SAP Cloud Platform.

This article provides insight into the multitude of diligently designed, planned, and implemented measures within SAP Cloud Platform that enable organizations to take advantage of innovations such as the Internet of Things (IoT), big data, and analytics while protecting enterprise data. It first looks at SAP's overarching security strategy, and then walks through how this strategy is realized with SAP Cloud Platform, so that you can move forward in your own digital journey with confidence and trust.

So how does SAP go about ensuring a high level of security for SAP Cloud Platform? With a security strategy built on three foundational pillars.

### The Three Pillars of SAP's Security Strategy

In SAP's experience, securing a technology platform is an orchestration of a wide range of different tasks. It is also an ongoing journey, not a state that one finally reaches. Security is dynamic — it requires a "plan-do-check-act" cycle that involves constantly adjusting to customers' needs and a rapidly changing threat landscape.

SAP's overarching security strategy is built upon three pillars that provide the foundation for executing this "plan-do-check-act" cycle:

- **Secure products**, which means focusing on incorporating security into applications and delivering the highest possible level of protection for content and transactions
- **Secure operations**, which means providing a comprehensive, end-to-end cloud and IT operations security framework — from system and data access secured by system hardening to security patch management, security monitoring, and end-to-end incident handling
- **Secure company**, which means a well-established security culture, secure environments with end-to-end physical security of SAP's assets, business continuity for operational

resilience, and the use of various governance mechanisms

Here, we look at some of the key ways this security strategy is realized with SAP Cloud Platform.

## Secure Products

Secure products are the foundation of any security strategy, so in 2014, SAP established the secure software development lifecycle (secure SDL) framework for use by its internal development team, which integrates risk-based secure software development principles in accordance with ISO 27034.[1] This framework comprises training, tools, and methodologies, as well as processes that are used to perform specified sets of security activities across four key phases: Preparation, Development, Transition, and Utilization. **Figure 1** provides an overview of these phases, along with the security activities performed during these phases — including training, risk identification, planning, development, testing, validation, and response — and some of the key measures involved.

Even with the use of source code scanning and other measures specified by the secure SDL framework, however, many vulnerabilities will remain in the coding, such as cross-site scripting, directory traversal, SQL injection, and buffer overflow vulnerabilities, because some of these require dynamic and extensive penetration testing as well as code scans. In addition, despite the most exhaustive preventive efforts, malicious coding and attempts to attack systems will always occur — and with increasing sophistication. To fill these gaps and meet the security needs of modern environments, SAP decided to extend the secure SDL framework for SAP Cloud Platform by going beyond traditional security measures.

One way SAP achieves this additional level of security within SAP Cloud Platform is via the self-defending applications concept. Self-defending applications are systems that are resilient to attacks such as code injections. To help enable SAP Cloud Platform to reliably prevent such attacks, SAP is currently piloting an approach called "tainting" that it intends to add to SAP Cloud Platform in the future. With this approach, also known as runtime application security protection (RASP), SAP Cloud Platform would be able to identify pieces of information that are fed as input and compare this information to accepted structures — a process known as dynamic information flow tracking. Taint-aware parsers implemented within this process refuse code execution once they encounter tainted code tokens. Application developers building applications on SAP Cloud Platform would also benefit from tainting during design time, since it enables them to focus on application logic while increasing the security level of the application.

SAP also adds security to SAP Cloud Platform with open source software security measures. While the use of open source software is an essential part of SAP Cloud Platform — it enables access to a wide range of components that are enriched for enterprise-readiness, simplifying and speeding the development of sophisticated applications — attacks such as Heartbleed and Shellshock are alarming examples of vulnerabilities that can often be found in open source software components. To bring the numerous benefits of open source software to SAP customers without the risks, SAP Cloud Platform ensures open source software security in two ways:

- While SAP Cloud Platform benefits from access to widely used open source software components, SAP also actively contributes to the open source software community by sharing detected

[1] Learn more about the ISO 27034 standard for application security at www.iso27001security.com/html/27034.html.

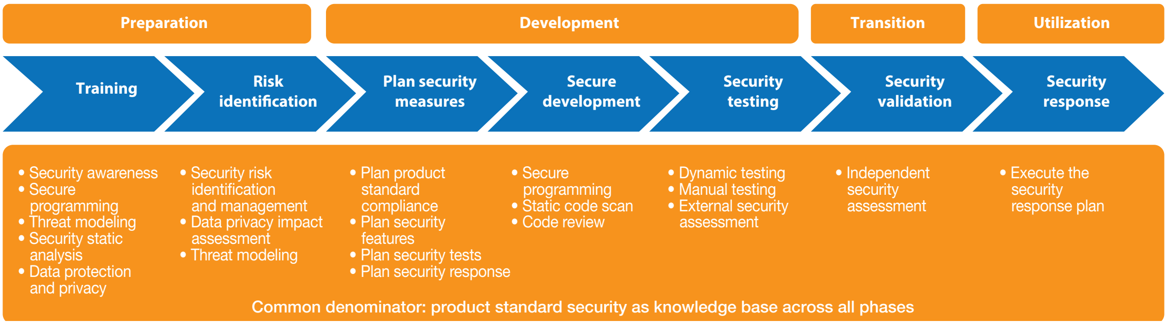

**Figure 1** SAP's secure software development lifecycle (secure SDL) framework

vulnerabilities, patches, and source code scanning results to increase the security level of these components for all other users.

- SAP maintains an internal open source software vulnerability management process, which consists of a company-wide inventory of all open source software components that are in use and tracking of publicly known vulnerabilities. SAP combines these elements with tooling, monitoring, and corresponding processes that help to ensure timely patching or replacement of potentially vulnerable open source software components within SAP software coding.

By using a well-established, secure development framework that incorporates the measures required for protecting modern software, SAP ensures a secure foundation for SAP Cloud Platform.

### Secure Operations

A secure infrastructure and operations framework is essential to an effective security plan. With customers entrusting their data and processes to SAP solutions, data center security is a central focus area for SAP. Secure operations in this sense encompass all measures necessary to ensure secure end-to-end cloud operations as well as the defense of customer data and business operations, including:

- Effective protection of the infrastructure from advanced threats
- Data defense and assurance in a mobile workforce landscape
- Business protection on internal and third-party networks

With SAP Cloud Platform poised to play a central role in many SAP customer transitions into the digital economy, SAP has added measures to ensure the security of its data centers. One is the establishment of SAP's Global Security Operations Center (GSOC), a team of IT security experts at SAP that ensures the secure operation of SAP's own productive implementation and entire cloud infrastructure by connecting all data centers, cloud solutions, network IT, and SAP productive systems to a central monitoring infrastructure run by SAP Cloud Platform.

At the heart of this central monitoring infrastructure is the cloud-based SAP Cloud Platform Cyber Security Analytics, a planned offering currently in use at SAP that combines the computing power of SAP HANA with the advanced threat detection mechanisms provided by SAP Enterprise Threat Detection.[2] SAP Cloud Platform Cyber Security Analytics analyzes 5-15 TB of raw log data per day for real-time detection of security events, such as unusual logon attempts at odd hours or massive data downloads, and to ensure secure cloud and IT operations.

SAP has also added operational security measures to secure the new types of landscapes common to modern infrastructures. SAP Cloud Platform integrates and extends organizations' business processes as they transition into the cloud, including enabling entirely new business scenarios that connect existing processes to IoT. This expansion into the world of devices and sensors comes with a significant risk, however: It increases both the potential attack surface for accessing enterprise data and the endpoints through which this data can be accessed. To address these vulnerabilities, SAP takes security from the core of SAP Cloud Platform to the level of the devices connected to it by establishing trust and security with IoT devices that are equipped with a trusted digital identity, based on X.509 certificates deployed by SAP. This approach allows seamless onboarding of new devices while preserving a high level of security.

By securing cloud and IT infrastructures with centralized monitoring and secure device connections, SAP Cloud Platform establishes a data center security strategy that ensures secure operations.

### Secure Company

A secure company is the final piece of a successful security strategy. SAP is fully aware of its responsibility to its customers and its customers' expectations relating to security, and has a long tradition of building reliable and secure software. As part of its commitment to delivering this security, SAP relies on industry standards, certifications, and attestations that are globally accepted. This reliance goes back to SAP's ISO 9001 certifications as well as the Common Criteria for Information Technology Security Evaluation certification ISO/IEC 15408 for the SAP NetWeaver technology platform.

As SAP customers move into the cloud, SAP continues to extend these trust-building measures by complying with various standards and achieving

[2] For more on SAP Enterprise Threat Detection, see the article "An Integrated Approach to Identifying Security Risks" in the April-June 2016 issues of *SAPinsider* (SAPinsiderOnline.com).

| | |
|---|---|
| ISO 27001 | International Organization for Standardization (ISO) Certification for Information Security Management Systems<br>www.iso.org/isoiec-27001-information-security.html |
| SOC 1<br>SSAE 16 | Service Organization Control 1 (SOC 1) Report<br>Statement on Standards for Attestation Engagements No. 16 (SSAE 16), Reporting on Controls at a Service Organization<br>www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-00801.pdf |
| SOC 1<br>Type 1 & 2 | Service Organization Control 1 (SOC 1) Report<br>(Attestation Report)<br>www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/aicpasoc1report.aspx |
| SOC 2<br>Type 1 & 2 | Service Organization Control 2 (SOC 2) Report<br>(Attestation Report)<br>www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/aicpasoc2report.aspx |

**Figure 2** SAP Cloud Platform complies with a host of standards and certifications

certifications, including the Business Continuity Management (BCM) standard ISO 22301 and the Federal Information Processing Standard (FIPS) 140-2 certification for our CommonCryptoLib crypto kernel,[3] and also committing to programs such as the Information Security Registered Assessors Program (IRAP) for Australian government customers. When it comes to SAP Cloud Platform, organizations can be assured that it runs only in secure, certified environments and data centers that adhere to the highest standards of security and availability (see **Figure 2**).

The easiest way to determine which cloud solutions have which security certifications is to visit SAP Cloud Trust Center,[4] which holds security and data privacy information, service availability details, and compliance search capabilities that allow customers to find, display, and download cloud security certifications, such as SOC 1 and SOC 2, for each product.

A solid security philosophy, adherence to industry standards, and trusted security certifications ensures a secure company that customers can trust.

## Summary

Securing enterprises as they digitize their business is critical — a successful transition to the digital economy depends on it. SAP Cloud Platform is a proven platform that enables a secure transition by addressing security needs in several key ways:

- Measures that go beyond SAP's risk-based secure development framework by using innovations such as "tainting" to enable self-defending systems
- Tracking open source software components and their vulnerabilities, and sharing findings with the open source software community
- Data center security via a central monitoring infrastructure that enables real-time detection of security events
- Extending security from SAP Cloud Platform to IoT-connected devices through trusted digital identities
- Adherence to industry standards, regulations, and attestations

With a cloud platform based on these principles, SAP customers can complete their digital journey with confidence and trust. Learn more about SAP Cloud Platform security at **https://cloudplatform.sap.com/capabilities/security.html**. ■

[3] Learn more about SAP's FIPS 140-2 certification in the article "Is Your Data Properly Protected?" in the January-March 2013 issue of *SAPinsider* (SAPinsiderOnline.com).

[4] SAP Cloud Trust Center is located at www.sap.com/about/cloud-trust-center.html and specific compliance information can be found at www.sap.com/about/cloud-trust-center/cloud-certification-compliance.html.