SAPinsider

This article appeared in the Apr ▪ May ▪ Jun 2016 issue of *SAPinsider* (www.SAPinsiderOnline.com) and appears here with permission from the publisher, WIS Publishing.

WIS pubs

Security in the Digital Era: How SAP Runs Secure

by Ralph Salomon, SAP

Organizations that embrace digital technologies and take steps toward adopting a digital framework have to consider what that means from a security perspective. With cloud, mobile, and Internet of Things (IoT) technologies gaining steam, how will security be affected? SAP asked itself the same questions in undergoing its own digital transformation — and took a detailed look at its own security platform. While SAP is a leader in providing governance, risk, and compliance (GRC) and security solutions for the enterprise, those solutions and platforms are not created in a vacuum; SAP itself is also a large multinational company moving to a digital core, with significant investments in cloud and security technologies. As such, SAP's security platform is evolving to meet the changing demands brought on by a transition to a digital framework.

Pillars of a Security Strategy

In a digital enterprise, attacks and threats can pop up at any time and from anywhere. Long-held business processes are changing with real-time data communicated between any number of points, from enterprise systems to employees' smartphones to IoT-connected devices, flooding organizations with increasing amounts of structured and unstructured data. In this environment, stringent authentication and GRC tools as well as a continuous monitoring framework are critical for ensuring that GRC requirements are fulfilled, and for preventing and reacting to security incidents in a timely fashion.

At SAP, we align our security tools and measures along three pillars of an end-to-end security strategy:

- **Prevention:** Defend against threats via traditional measures, such as security requirements (policies and standards based on international industry practices and compliance demands) antivirus solutions, server configuration requirements, and employee awareness and training.
- **Detection:** Identify deviations from preset requirements and anomalies within our environment and communication, and detect infrastructure vulnerabilities and advanced malware.
- **Reaction:** Ensure security incident management readiness, open lines of communication, facilitate alerts, and minimize detection response time.

At SAP, we use SAP solutions for GRC. In particular, SAP Risk Management and SAP Process Control are foundational services for security that enable a holistic, end-to-end security strategy. SAP Risk Management, for example, is essential for outlining, mitigating, and continuously monitoring risks associated with our infrastructure and any new IT project. This ensures the risk level is both identified and maintained in a manner consistent with the organization's approach and comfort level. In concert with SAP Risk Management, SAP Process Control helps close the loop on an end-to-end security strategy by establishing a robust controls network around the identified risks. SAP Process Control enables a framework of testing and documentation so that the three-pronged strategy of prevention, detection, and reaction is always in sync and in line with overall corporate objectives.

For prevention, SAP leverages SAP Identity Management as a cornerstone solution for managing user accounts and authorizations. SAP Access Control enables workflow-driven assignment of authorizations, providing access to critical functions. With SAP Single Sign-On, end users are assured of seamless authentication and access to solutions and data support, and with thumb-based authentication, users of cloud solutions — such as those delivered by SAP SuccessFactors, SAP Ariba, and partners — have an extra layer of security and usability through SAP Cloud Identity.

For detection, SAP Solution Manager is an important tool that SAP uses to monitor the compliance and security

level of its extensive system landscape. SAP Solution Manager can report on how a system configuration deviates from a preset requirements checklist defined in detailed security standards and procedures. As a monitoring tool, SAP Solution Manager can build up a reference system configuration repository, checking and comparing that master reference against any maintained or new system deployment.

To expand this monitoring framework, SAP leverages a partner solution that focuses specifically on technical security settings and SAP HANA configurations. Leveraging it in conjunction with SAP Solution Manager enables automated mitigation of deviations throughout the system stack. This custom-built solution recently received a CSO50 award[1] that recognized it as an innovative security measure because it both provides continuous security transparency and pushes deviations directly to an administrator who can reset configurations to the right setting.

Expanding Security for the Modern Enterprise

In practice, this homogeneous controls framework and tightly integrated security strategy has served SAP well, especially as it has built out cloud technologies and acquired cloud companies. Putting in place well-documented control frameworks for cloud solutions leads to cloud process templates, enabling new cloud solutions to establish their required control system in a matter of hours rather than the usual weeks-long process of defining and approving the respective control system.

Similar to the requirements for securing the cloud, the increasing need to access enterprise data on mobile devices requires its own set of stringent controls, and this is certainly the case for SAP. To mitigate potential mobile threats, SAP uses SAP Mobile Secure to ensure password protection, disk encryption, and enforcement of several security safeguards on any mobile device, as well as the protection of data stored or accessed through a mobile device.

Another push for a tighter enterprise security framework comes from the IoT phenomenon. Devices, consumer products, and machinery with sensors will all likely require connection to back-end systems, expanding the need for authentication and monitoring mechanisms to validate that a communication network isn't compromised.

Securing SAP's own cloud, mobile, and IoT landscape is a primary driver for the development of SAP Enterprise Threat Detection,[2] which enables organizations to identify security breaches as they occur and react in real time to mitigate danger and prevent damage to the business. Perhaps more than any other security tool in the SAP security portfolio, SAP Enterprise Threat Detection leverages SAP's own implementation of the application to expand the product's functionalities and deliver these improvements to our customers and the market.

SAP Enterprise Threat Detection was created because of an internal drive to develop a security, information, and event management (SIEM) application specific to SAP applications. We had been using a partner-built SIEM solution but wanted to expand the monitoring coverage to the application layer. As there was nothing on the market, SAP's security organization worked with SAP developers to build their own solution: SAP Enterprise Threat Detection. This necessitated a collection of application log data from the SAP systems as well as a connector to these systems. Now we have a real-time view of threats from both inside and outside the organization with a simplified view of log data combined with contextual data.

Stitching Together a Security Blanket

SAP Enterprise Threat Detection is an ideal example of how important the partner ecosystem is to the development and deployment of organization-specific security solutions. Security threats are different for every company, and SAP works continuously with partners to integrate our solutions with third-party tools to develop the most effective capabilities for customers based on their unique threat environments. It also means the integration of SAP solutions, such as SAP Risk Management, with customers' non-SAP systems in a central security monitoring tool so that targeted threats can be dealt with across customers' entire system landscapes.

SAP customers have likely heard the "SAP runs SAP" expression, and we certainly live it with security. In a digital economy where the enterprise must plan for and adapt to more data, more devices, more users, more cloud solutions, and more and different threats, security is too important to be trusted to manual processes or an unintegrated set of solutions that notify you after attacks take place. This is why SAP's security strategy for the real-time, digital enterprise is continuously evolving to stay ahead of emerging threats with solutions that have proven their mettle in a time-tested, digital environment: our own. ■

Ralph Salomon (ralph.salomon@sap.com) is Vice President, Secure Operations in SAP Global Security.

[1] See www.csoconfab.com/cso50-awards.

[2] For more about SAP Enterprise Threat Detection, see "An Integrated Approach to Identifying Security Risks" on page 82 in this issue of *SAPinsider*.