Misuse Detection in SAP Systems

How to Ensure the Integrity and Confidentiality of Your Data

by **Guido Schneider**, *Senior SAP Product Management Advisor, Aspera*

A company's data is a crucially valuable asset in the digital world, and the security of that data is paramount. This is especially true in SAP landscapes, which often feature highly integrated systems combining functionality across multiple areas of the business, giving data access to users across all functions. Companies must focus on protecting data and information in their SAP systems so that the data's availability, integrity, and confidentiality are maintained.

Traditional enterprise solutions play an important role in safeguarding data, but what about data misuse by a company's employees? Can it be detected, and if so, how? In this article, we will explore IT landscapes that can work toward separating tasks and functions, and show how complementary software can provide automated license tracking that allows you to govern system usage automatically, identify what authorizations a given user needs, and ensure that each user only sees the data they require to perform their jobs.

Security Capabilities in SAP Landscapes

SAP offers a variety of solutions that you can use in combination to meet legal requirements for task and function separations, including:

- SAP ERP Human Capital Management for master data management
- SAP Identity Management for workflow-driven application, approval, and management of permissions
- The authorization scheme within SAP systems, as well as the control and management of segregation of duties (SoD) with SAP Access Control
- SAP Risk Management and SAP Enterprise Threat Detection for company-wide risk management and IT threat detection
- SAP Business Integrity Screening (formerly known as SAP Fraud Management) and SAP Process Control for monitoring and detecting potential business process fraud

SAP Business Integrity Screening and SAP Enterprise Threat Detection in particular provide capabilities that can help to thwart data misuse. SAP Business Integrity Screening enables the early detection of suspicious data use and attempted fraud in SAP systems through mass screening. Existing fraud patterns and new detection rules can be defined in the application. SAP Enterprise Threat Detection analyzes security-relevant events across the entire system landscape to detect suspicious user behavior, while only evaluating system log files. This set of rules is supplied by SAP and can be extended. SAP Business Integrity Screening focuses on business process fraud, while SAP Enterprise Threat Detection focuses on IT threats that pose a risk to companies.

If you are using all these products, then you already have a high level of system security. The SAP landscape with

SAP Business Integrity Screening and SAP Enterprise Threat Detection offer good approaches. However, two security issues remain uncovered: employees' user authorizations and their subsequent actions.

Focusing on User Authorizations and Actions

Even with a lot of security features and procedures in place, a company's ability to achieve true data integrity and confidentiality is based on the actions of users. But how can you be sure that users aren't misusing your company's data? First, you need to set up a user's authorizations correctly, and then you need to monitor the user's behavior.

A clear starting point for tracking and maintaining appropriate user access is determining what actions a user should be able to take by mapping your user structure. Employees generally have more authorizations than they need for their daily work, which can add to licensing costs and put the privacy of your data at risk, an important consideration given increasing global data regulations, such as the General Data Protection Regulation (GDPR) in Europe. Every user action should have an underlying business reason that serves the interest of the company.

The same rule applies to data integrity. When a user changes data, there must be a reason for it — for example, a user accepts a delivery and posts it as delivered in the SAP system after the goods have arrived in the warehouse. What if a user's behavior suddenly changes? Perhaps a boss assigned a new task or a user attended SAP training and learned about new transactions to streamline daily work. However, if there is no such reason for the changed user behavior, then misuse could be occurring, which is why it is important to identify the changed behavior and determine the reason for it.

Or consider this scenario for a financial institution: A bank teller's duties include paying out money at the counter to customers, so the teller must have access to customer data. What if the teller looks at the bank account details when a customer is not in the bank? This could be a sign that the teller is misusing the data — even though a wide variety of security products is in use.

Figure 1 illustrates two functionalities that can supplement your SAP controls and thwart these types of data misuse. Aspera's LicenseControl for SAP software recognizes whether the revocation of an authorization leads to a license optimization. The software can also automatically determine which authorizations are not required for your employees' daily work. The Xiting Authorization Management Suite (XAMS) can then remove the authorization from the SAP role. After a fixed period of time, you can view the authorizations you removed and evaluate whether to reinstitute them.

By installing a simple add-on to the server that houses SAP Business Integrity Screening and SAP Enterprise Threat Detection, you can compare two events and note, to use the previous example, if a bank teller views a customer's account details but does not follow up with another action such as a payout. This could be a potential abuse attempt that necessitates action by the company. The tool can notify you with an alert, which can inform you or a compliance officer via email about a change in a user's behavior. A compliance officer can then determine if there is a reason for the change. If not, then it could be attempted data misuse and the data's integrity and confidentiality would no longer be ensured.

You can also review the list of unexploited authorizations per employee yearly to optimize your authorization concept. The fewer authorizations an employee has, the more they comply with the specification of the minimal principle. At the same time, you reduce SAP license costs, since the fewer authorizations an employee has in the SAP system, the less you pay for their use.

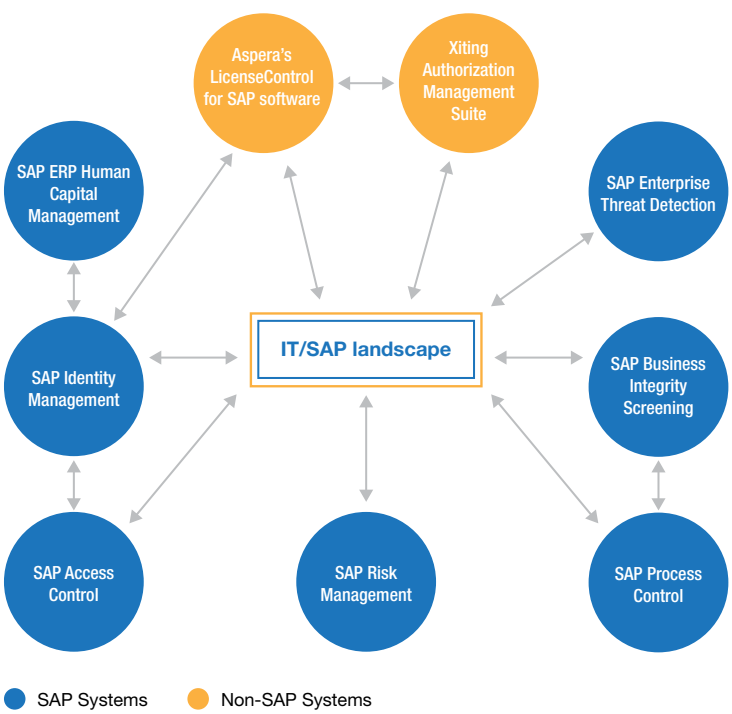

Figure 1 Supplementing the security landscape in an SAP system

Learn More

Strong security starts with a modern IT infrastructure. But it doesn't stop with standard tools; monitoring authorization and user actions is essential. For more information, visit **www.aspera.com**. ■