Securing Sensitive SAP Data Using Attribute Based Access Control (ABAC) and Data Masking

Charles Braswell, CEO, Winterhawk Consulting

SAPinsider
Las Vegas

2023

SAPinsider

In This Session

We will explore various techniques and use cases to provide additional granularity when securing SAP sensitive data by leveraging ABAC and data masking techniques.

What We'll Cover

- How data masking and ABAC can help organizations comply with regulations such as ITAR and GDPR
- Benefits & Challenges of key data masking techniques
- How organizations have successfully implemented data masking solutions
- Wrap-Up

Leveraging Data Masking and ABAC for Compliance

Data Masking & ABAC Defined

Data Masking:

A technique used to protect sensitive or confidential data by replacing it with fictitious or altered data. Static Data Masking is when the data is permanently altered and stored. Dynamic Masking is used to mask sensitive data in transit or while users are interacting with the data, leaving the original copy unaltered.

HR Manager

User	Field	Value
Jane Doe	SSN	123-45-6789
Jane Doe	DOB	05/01/1970

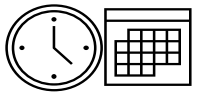
HR Staff

User	Field	Value
Jane Doe	SSN	999-99-9999
Jane Doe	DOB	05/01/XXXX

User Attributes

Job Title
Citizenship
Location
Security

Other Attributes



IP Address
Device Type
Time
Day

ABAC:

Leverages rule-based policies to grant or deny access to users based on attributes such as job title, security clearance, citizenship, device type, IP address, location, time, day, etc.

Offers a flexible and adaptable way to control access, allowing organizations to create more sophisticated security policies that can be adjusted to new regulation requirements.

By combining ABAC with Data Masking, organizations can significantly improve their security posture and decrease the risk of data breaches and unauthorized access to sensitive data as well as help comply with various regulations that require the protection of personal or sensitive data.

Data Type Use Cases

Common Data Types Use Cases where Data Masking is beneficial:

Names: Data masking techniques may involve replacing the original name with a pseudonym or scrambled version of the name.

Email addresses: Data masking techniques may involve replacing the original email address with a fake email address or removing it altogether.

Social Security Numbers (SSNs): Data masking techniques may involve replacing the original SSN with a random number or a scrambled version of the SSN.

Credit card numbers: Data masking techniques for credit card numbers may involve replacing the original number with a fake credit card number or a scrambled version of the number.

Dates: This includes dates of birth, employment, or other important dates. Data masking techniques may involve shifting the original date or replacing it with a random date within a certain range.

Medical data: This includes medical diagnoses, test results, and treatment plans. Data masking techniques may involve removing the original data or replacing it with fictitious data.

Financial Data: Data masking techniques may involve removing the original data or replacing it with fictitious data.

Regulations

Common Regulations where Data Masking is beneficial:

General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA): Requires organizations to protect the personal data of citizens and residents.

Health Insurance Portability and Accountability Act (HIPAA): HIPAA regulates the protection of healthcare information in the United States.

Payment Card Industry Data Security Standard (PCI DSS): PCI DSS requires organizations that process credit card transactions to protect cardholder data.

International Traffic in Arms Regulations (ITAR): ITAR is a US government regulation that controls the export and import of defense-related articles and services, including technical data.

Family Educational Rights and Privacy Act (FERPA): FERPA regulates the privacy of student education records in the United States.

Benefits & Challenges of key data masking techniques

Key Data Masking Techniques

Data masking techniques are used to protect sensitive data by replacing it with a non-sensitive substitute, while preserving the overall functionality of the data. The following are common data masking techniques:

1. Substitution: This technique involves replacing sensitive data with a non-sensitive substitute. For example, a credit card number might be replaced with a string of X's or with a fictitious credit card number.

2. Encryption: Encryption involves transforming sensitive data into an unreadable form that can only be decrypted with a key. This technique is particularly useful for data that must be stored in an accessible format, but which requires protection.

3. Shuffling: Shuffling involves re-ordering the values in a dataset while preserving the relationships between them. This technique is particularly useful for protecting sensitive data in large datasets.

4. Masking: Masking involves concealing part of a data field to protect sensitive information. For example, the last four digits of a social security number or a credit card number might be masked.

5. De-identification: De-identification involves removing or altering information that could be used to identify an individual. This technique is particularly useful for protecting personal information such as names, addresses, and social security numbers.

Benefits & Challenges

Technique	Benefits	Challenges
Substitution	• Easy to implement and understand • Can be applied to a wide variety of data types	• May not provide adequate protection for some types of data • May not be effective against sophisticated attacks
Encryption	• Provides strong protection for sensitive data • Can be applied to a wide variety of data types	• Can be difficult to implement and manage • Can be resource-intensive and impact system performance
Shuffling	• Provides strong protection for large datasets • Can be applied to a wide variety of data types	• May be difficult to implement in some cases • Can impact system performance when used on large datasets
Masking	• Can be easily implemented • Can be applied to a wide variety of data types	• May not provide adequate protection for some types of data • Can be vulnerable to brute-force attacks
De-identification	• Provides strong protection for personal information • Can be applied to a wide variety of data types	• May not be effective against sophisticated attacks

Successfully implementing data masking solutions

Key Implementation Success Factors

1. Identify data owners with knowledge of the relevant regulations and security requirements to confirm exactly what data is sensitive in the organization. Not properly identifying the data with masking requirements, leads to overprotecting the data and complex policies and maintenance.
2. Execute a data mapping initiative to identify where the data is kept and who has access currently.
3. Ensure regular review processes of the data classification scheme are in place to help identify areas for improvement and ensure that the classification remains accurate and up-to-date.
4. Ensure scenarios where data must be masked or filtered will not inappropriately write masked data to the database (Update and Delete transactions).
5. Understand any external sources which may need to be integrated with the policy engine for accurate masking policy determination.
6. Follow the least privilege access principle to ensure only users with a valid purpose can access the unmasked data.
7. Execute a formal system selection initiative to ensure the solution that is the best fit for the organization is deployed.

Wrap Up

Where to Find More Information

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf

"NIST Special Publication 800-162, Guide to Attribute-Based Access Control (ABAC) Definition and Considerations": This guide, provides an overview of ABAC and discusses the key considerations that organizations should take into account when implementing this access control model."

https://pathlock.com/capabilities/data-masking/

"Dynamically mask sensitive data across without hindering end-user productivity, meeting data privacy requirements with ease."

https://blogs.sap.com/2023/02/28/attribute-based-access-control-abac-field-masking-scenario-in-se16-and-mm03-tcodes/

"Learn how to mask "Gross Weight" and "Net Weight" fields in MARA table in transactions SE16 and MM03 for materials of Sensitive Material Group"

Key Points to Take Home

1. Data Masking and ABAC can be deployed independently, but implementing them together provides additional value.
2. Data Masking and ABAC can address security requirements for Privacy, Health Care, Credit Card, and ITAR regulations.
3. Data mapping and classification processes should be initiated to ensure the success of a Data Masking deployment
4. There are a numerous Data Masking techniques when determining the best approach to mask data
5. Data Masking solutions have matured significantly in the past 5 years and can be leveraged to address the most challenging compliance requirements.

Thank you! Any Questions?

Charles Braswell

linkedin.com/in/charlesbraswell

Please remember to complete your session evaluation.

SAPinsider

SAPinsider.org

PO Box 982Hampstead, NH 03841

SAPinsider comprises the largest and fastest growing SAP membership group worldwide, with more than 600,000 members across 205 countries.