Saviynt

SOLUTION GUIDE

Saviynt for SAP HANA

Why should you care about SAP HANA Security?
How can you do it right?

Many companies are making large investments in SAP HANA and adopting it as their strategic "big data" initiative. By integrating with SAP ERP supply chain management tools and incorporating big data analysis, organizations can migrate critical, sensitive information from their standalone database silos to a centralized SAP HANA database.

This adoption and the challenge of protecting critical data on a new platform while also ensuring compliance with security policies and regulations is a high priority for organizations. This brief explores the following aspects:

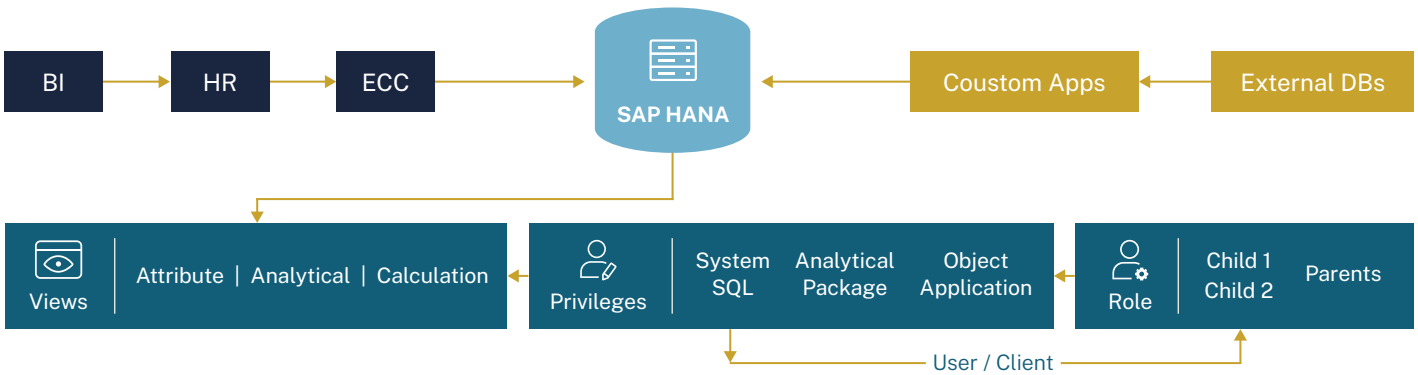
1. Various implementation scenarios of SAP HANA security
2. Thinking about SAP HANA security from the ground-up
3. A look at Saviynt's unique solution for effective fine SAP HANA security management

Simply put, SAP HANA's database behaves like a hybrid application so all the rules of complex user access must be adhered to. Data in SAP HANA is accessed via views; for a business user to run a sales report, access to the sales view, namely an analytical or calculation view, is needed. SAP HANA enforces data restriction on these views through different privileges, as seen in this example.

SAP HANA Security Model is Vastly Different than a Traditional Database

Traditional databases only allow technical users to monitor access to applications that access data via service accounts. Fulfilling SAP HANA's full potential as a big-data platform requires that organizations provide users and clients direct access to execute data-intensive operations within the in-memory database so they can view various reports.

This business requirement exponentially increases the number of user accounts that log into the database. For example, all corporate executives may need to log into SAP HANA through various client connections to execute business critical reports and data.



Lack of Business View

As SAP HANA security is enforced at the data tier, its implementation now lies in the hands of data stewards and database administrators vs. the traditional model where core information security teams or application security teams handled implementation. Unless they have an in-depth knowledge of SAP HANA's database, a business owner's understanding of what business and security rules have been implemented is limited.

Cumbersome Ongoing Management

One of the key benefits of SAP HANA is that companies can integrate their disparate and isolated applications, associated databases and authorization rules into a central SAP HANA-based big data platform. Internal data sources (SAP, Oracle, Content Management etc.) and external data sources (LinkedIn, Twitter, extranet websites etc.) can now potentially reside within the same database.

Security teams can find it extremely difficult to manage user access on an ongoing basis every time a new data source is integrated, meaning another revision of existing SAP HANA security model is created. Security owners face a daunting task in figuring out if the new security requirements have been correctly implemented, or if they weakened/impacted any of the existing security policies/configurations.

A Novel Approach to Implementing & Managing SAP HANA Security

Saviynt has introduced a unique mechanism for SAP HANA's security management that translates the complex security model into a logical view for business owners and security teams. It allows users to define security requirements as logical rules within their security rulebook. It then follows a two-step process to build the security model:

1. Based on the security rules, privileges are then automatically designed and mapped to the users.
2. Derived privilege-user mapping is used to automatically design roles that contain users and privileges.

As a best practice Saviynt does not directly provision privilege-user relationships to SAP HANA, instead role-user and role-privilege relationships are provisioned after requisite approvals are obtained. Saviynt also provides users with the ability to extract user-role information from existing applications and then reuse the clusters to discover SAP HANA roles from privileges.

Audit and Compliance

- Define security / business rules
- Real-time violation checks
- Apply mitigating controls
- Continuous controls monitoring with out-of-box controls library
- Usage analytics
- Risk-based access reviews and certifications
- Evidence reports

Role Design & Management

- Automatic privilege design and creation
- Automated role design and creation
- Privilege discovery from current application roles
- Role-privilege provisioning
- Lifecycle management

Access Provisioning & Management

- Intelligent end user access request portal
- Customizable enterprise-grade workflow designer
- Preventative SOD / security rule violation checks
- Mitigation while request is in-flight
- User access provisioning
- Dashboard & SLA reporting

Cloud Platform Benefits

- Eases over-burdened IT resources
- Deploys rapidly
- Complimentary upgrades
- Controls library mapped to compliance
- IGA focus is on providing business value –not maintaining infrastructure

Next Steps

- **Find out** why Saviynt received the highest product score for Midsize or Large Enterprise & Governance-Focused use cases in Gartner's 2018 Critical Capabilities for IGA.
- **Try a Demo** of the Saviynt IGA Platform
- **Start a Free Trial** of Saviynt's Enterprise Solution

ABOUT SAVIYNT

Saviynt empowers enterprises to secure their digital transformation, safeguard critical assets, and meet regulatory compliance. With a vision to provide a secure and compliant future for all enterprises, Saviynt's cutting-edge solutions have been recognized as industry leaders. For more information, please visit www.saviynt.com.

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com