IBM Security Guardium Data Protection for SAP HANA

Continuously monitor, access and protect sensitive data across your SAP HANA environments

When it comes to protecting sensitive data stored on SAP data repositories, organizations face unique challenges: sensitive data may be dispersed across hundreds of different database columns, precluding column-level monitoring or encryption; vulnerabilities stemming from misconfigured privileges or missing patches could leave SAP data stores at risk; and insiders with privileged access could potentially view, change or exfiltrate data, without their actions being tracked or detected.

IBM® Security Guardium® Data Protection for SAP HANA empowers security teams to safeguard sensitive data through automated discovery, classification, vulnerability assessments, real-time, contextual activity monitoring and advanced threat detection — extending comprehensive data protection across heterogeneous, hybrid multicloud environments, including SAP HANA databases.

The solution continuously monitors all data access operations in real-time to detect unauthorized actions, based on detailed contextual information— the “who, what, where, when and how” of each data access. Guardium Data Protection automates data security governance controls and reacts automatically to help prevent unauthorized or suspicious activities by privileged insiders and potential hackers and helps accelerate compliance to reduce operational risk and total cost of ownership.

Highlights

- Scan entire SAP HANA environment to understand where sensitive data resides
- Automatically take action or report regulatory compliance
- Monitor access to high-value SAP HANA environment, in real-time
- Automate vulnerability scanning and configuration
- Integrate with SecOps and ITOps tools for incident orchestration and response

Risk reduction

Guardium Data Protection for SAP HANA reduces the risk of a data breach by providing real-time data security intelligence.

Database discovery, data classification and entitlement reports can be scheduled or run on-demand to scan the entire SAP HANA environment to further understand where sensitive data resides, based on pre-built templates for regulations such as CCPA, SOX, PCI, GDPR, PII, HIPAA and more.

Vulnerability assessments can proactively scan SAP HANA deployments to detect potential vulnerabilities and generate reports with suggested remedial actions. With more than more than 92 out-of-the-box SAP HANA vulnerability assessments based on Common Vulnerabilities and Exposures (CVEs), industry best practices and SAP recommended security practices, the results can be distributed, integrated into IT Service Management tools such as ServiceNow or imported into a broader vulnerability management platform for remediation and closed-loop feedback.

Pre-built policies, real-time data activity monitoring, security alerts, and blocking allow organizations to take action on specific activities, such as failed login attempts, unauthorized access to sensitive tables, off-work activities, data exfiltration and more. Guardium Data Protection creates real-time alerts when a policy is violated and enables integration with SIEM tools such as QRadar and Splunk or proactive actions such as blocking or quarantining users to prevent suspicious access. It also supports Application User Translation (AUT) and Pseudo tracking to help keep users responsible for their actions.

Advanced threat detection uses machine-leaning (M/L) algorithms, and a combination of rules-based policies and symptom analysis to detect patterns of behaviors that map to known industry attack vectors, to identify insider and external threats. Identified cases are categorized by severity for investigative analysis and response.

Centralized control and automation

Through an automated deployment, Guardium Data Protection provides key capabilities to help streamline data security management without impacting data sources, networks, or applications, such as:

- Customizable workflows, with preset accelerators for common compliance requirements, create custom processes while ensuring certain team members see only data and tasks related to their roles
- Secure and self-sustained platform through the Guardium user interface allows for audits of all operations to maintain compliance controls, segregation of duties and compliance with latest security mandates and Federal Information Processing Standards (FIPS) 140-2.

Performance and Scalability

Guardium Data Protection can be implemented with negligible performance impact—less than 1% overhead in most cases and does not require modifications to your existing SAP environment. The solution is equipped to scale seamlessly from one data source to tens of thousands without disrupting operations. Automation capabilities include:

- Load balancing scalability and performance features help reduce management costs and minimize need to manage detailed configuration information
- Batch operations facilitate integration of any IT process, through a script-based command-line interface (CLI) to Guardium
- Centralized aggregation and management merges and normalizes audits from multiple data sources to provide enterprise-wide reporting and forensics

Integration

Most existing security solutions lack the complete visibility into data access patterns required by regulatory mandates. Guardium Data Protection provides analytics-based, in-depth insight while seamlessly integrating into existing security solutions. In addition, Guardium Data Protection provides a modular integration model with existing IT systems, such as data

management, ticketing and archiving solutions such as IBM Cloud Pak for Data, ServiceNow and Amazon S3. The goal is to streamline IT and security operations by complementing and extending them with data security capabilities.

Why IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

For more information

Discover how IBM Security Guardium solutions can help you take a smarter, integrated approach to safeguarding critical data across your hybrid, multicloud environments. Visit ibm.com/security/data-security/guardium

---

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.