



Highlights:

- Protects SAP data environments from fraud, external or internal attack, privilege abuse and data leakage.
 - Reduces operational costs and simplifies compliance with internal and external audit requirements including SOX, PCI DSS, ISO 27001, NIST 800-53 and SAS70.
 - Reports on SAP user credentials from which unauthorized operations were performed.
 - Meets auditor requirements to monitor access to sensitive information, regardless of origin.
 - Breaks down complex SAP transactions into operations meaningful for audit, security and operational needs.
-

Application Monitoring for SAP

Detect Fraud in Real-Time by Monitoring Application User Activities

Security and Compliance for SAP

SAP is one of the most widely deployed ERP systems globally, with implementations typically containing significant amounts of data which are both mission critical and highly sensitive.

Customer data, financial data and personnel data are all examples of sensitive information managed within SAP. It is therefore not surprising that many compliance requirements and audits involve data managed by SAP, requiring IT security organizations to ensure their SAP data is secure.

Guardium Application Monitoring for SAP provides a packaged solution that addresses both the security and compliance requirements for SAP data — without requiring changes to existing business processes or application source code.

The primary purpose of application-layer monitoring is to detect fraud that occurs via enterprise applications. This level of monitoring is often required for data governance requirements such as SOX, ISO 270001, SAS 70 and NIST 800-53 controls.

Securing Multi-Tier Enterprise Applications

Multi-tier enterprise applications are often the most difficult to secure because they are highly distributed and designed to allow Web-based access from insiders and outsiders such as customers, suppliers, and partners. In addition, multi-tier enterprise applications such as SAP mask the identity of end-users at the database transaction level, using an optimization mechanism known as “connection pooling”.

Connection pooling identifies all transactions with a generic service account name, making it challenging to associate specific database transactions with particular application end-users. This is especially true if you’re relying on traditional database logging tools that can only monitor and identify users based on their database login accounts.



Highlights:

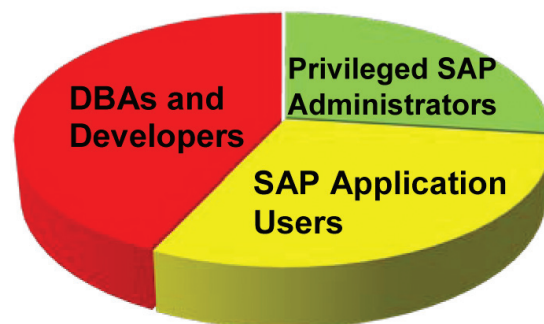
- Covers both direct and indirect data access: through the application, directly to the database by privileged users, and via interfaces that connect directly to the database.
- Supports creation of policies and real-time alerts for specific conditions, such as when particular application users update sensitive tables.
- Uses deterministic methods to positively identify application users, unlike other systems that rely on approximate methods such as statistical sampling and traffic matching, which are not valid for auditing and forensic purposes.
- Automates distribution of exception reports to oversight teams, with electronic sign-offs and escalations.
- Supports SAP ERP (previously R/3) and NetWeaver BW (previously SAP BW) data environments, including SAP specific policies.
- Custom policies easily created via drop-down menus which include sensitive SAP data sets which are hard to identify.
- Can be managed by non-DBAs such as InfoSec teams.
- Supports all common back-end database environments including Oracle, IBM DB2 and Informix Server, Sybase, Microsoft SQL Server and Teradata.
- Provides a single platform for centralized controls — across all major DBMS platforms and enterprise applications.

Application Type	User	Item Name	Operation Type	Transaction Code
SAP	HANSSCHMIDT	HFPT_COEJA_PP_ORDER_RPSCO_V2 Query		Change Order (IW32)
SAP	HANSSCHMIDT	MATERIAL	Update	Create Material (MMZ1)
SAP	VOLKERHESTERMANN BANK		Update	Change Bank (FI02)
SAP	HANSSCHMIDT	ADRESSE3	Update	User Maintenance (SU01)
SAP	GEORGHELD	ADRESSE3	Update	User Maintenance (SU01)
SAP	GEORGHELD	ADRESSE3	Update	User Maintenance (SU01)
SAP	HANSSCHMIDT	MATERIAL	Update	Create Material (MMZ1)
SAP	HANSSCHMIDT	MATERIAL	Update	Change Material (MMZ2)
SAP	HANSSCHMIDT	ORDER	Update	Change Order (IW32)

Figure 1: Guardium Application Monitoring for SAP empowers IT security organizations to rapidly identify fraud and other actions that violate corporate policies, such as unauthorized changes to sensitive data. Guardium monitors and reports on application user credentials associated with specific database transactions, even when applications use a generic database service account to access the database via connection pooling.

Since SAP data resides in relational databases, it can also be accessed through direct database connections (for example, via developer tools such as SQL *Plus) as well as through the SAP application. Guardium provides the only comprehensive solution that addresses both of these access paths. It positively identifies application users associated with specific database transactions, as well as identifying direct access by privileged users to unauthorized SAP objects.

Major Sources of Risk



Scalable Enterprise Security Platform

Guardium Application Monitoring for SAP is architected on Guardium's industry-leading Data Activity Monitoring (DAM) and Vulnerability Assessment technology, augmenting these core modules with SAP-specific policies, audit reports and tracking groups. Guardium's DAM technology monitors all database access in real-time without relying on native database logs, impacting performance or requiring database changes.

Unique in the industry, Guardium’s multi-tier architecture automatically aggregates and normalizes audit information – from multiple systems and locations – into a single centralized repository. This enables enterprise-wide compliance reporting, correlation, forensics, and advanced database-focused analytics.

A graphical Web console provides centralized management of policies, report definitions, compliance workflow processes, and appliance settings (such as archiving schedules). This scalable, multi-tier architecture can easily be scaled up to meet any mix of throughput and auditing policies, simply by adding appliances which work together in a federated model.

Guardium also offers a Vulnerability Assessment module that provides a best practices library of automated tests for identifying vulnerabilities such as missing patches, misconfigured privileges, default accounts, and weak passwords. This module is supported by a subscription service that provides preconfigured compliance policies and groups for major applications such as SAP.

Comprehensive Policy-Based Monitoring and Auditing

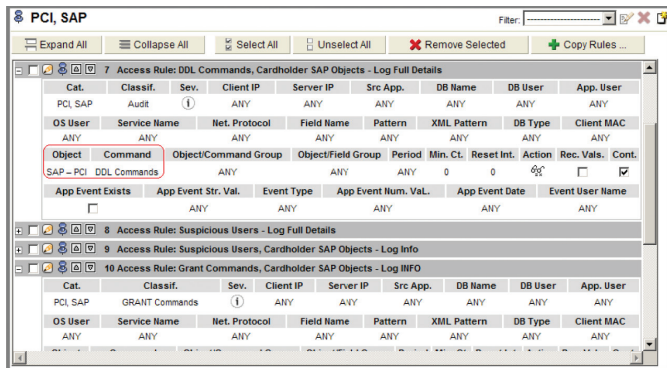


Figure 2: Guardium provides granular, preconfigured policies and reports for SAP applications to rapidly identify suspicious or unauthorized activities such as changes to sensitive objects or multiple failed logins. Sensitive SAP objects, which can require significant research to locate, are also identified to facilitate the development of custom policies. A range of actions, such as real-time SNMP alerts, can be configured to occur when policy rules are violated.

Guardium 7 provides:

- Built-in preconfigured policies developed specifically for SOX and PCI implementations which usually include the SAP application within their scope (see Figure 2).
- Comprehensive assessments of the underlying database engine where the SAP data is stored.
- Full activity and data access audit that shows both direct and indirect activities performed and data accessed.
- Audit trails for activity performed by users, showing access at the database level with user IDs at the application level (see Figure 1).
- Breakdowns of complex SAP transactions (e.g. FI02 – “Change Bank”) into granular operations which support audit, security and operational requirements, while maintaining correlation with the native SAP Identifiers (see Figure 3).

ACHIMOTTO	BILLING_SCHEDULE_SAVE	Query	Daily PO (ME23N)
ACHIMOTTO	MELDUNG	Insert	Create Notifications (IGS21)
ACHIMOTTO	OBJECT_NUMBER_QM	Query	Create Notifications (IGS21)
ACHIMOTTO	ILOA_UPDATE	Query	Create Notifications (IGS21)
ACHIMOTTO	IVOC_POST_NOTIFICATION	Query	Create Notifications (IGS21)
ACHIMOTTO	STATUS_UPDATE	Query	Create Notifications (IGS21)
ACHIMOTTO	ML_DOCUMENT	Query	Maintain Vendor Eval (ME61)
HANSSCHMIDT	BANK_DOCUMENT	Query	Change Bank (FI02)
HANSSCHMIDT	POST_BANK_ADDRESS	Query	Change Bank (FI02)
HANSSCHMIDT	BANK	Update	Change Bank (FI02)
HANSSCHMIDT	BANK	Update	Change Bank (FI02)

Figure 3: To support auditing, compliance and security requirements Guardium provides implementation details for SAP transactions such as FI02 (“Change Bank”), while maintaining correlation with the original transaction codes.

Broad Heterogeneous Application Support

In addition to its support for SAP, Guardium supports application-layer monitoring for all major applications and application servers, without requiring code changes. These applications include:

- Oracle E-Business Suite
- PeopleSoft
- Siebel
- Business Objects Web Intelligence
- Cognos 8 Business Intelligence

Guardium also identifies application user IDs for custom and packaged applications built upon standard application server platforms such as:

- IBM WebSphere
- BEA WebLogic
- Oracle Application Server
- JBoss Enterprise Application Platform

About the Guardium Platform

Guardium's real-time database security and monitoring solution monitors access to sensitive data, across all major DBMS platforms and applications, without impacting performance or requiring changes to databases or applications.

The solution prevents unauthorized or suspicious activities by privileged insiders, potential hackers, and end-users of enterprise applications such as SAP, Oracle EBS, PeopleSoft, Siebel, Business Intelligence and in-house systems. Additional modules are available for performing database vulnerability assessments, change and configuration auditing, data-level access control and blocking, data discovery and classification, and compliance workflow automation.

Forrester Research recently named Guardium "a Leader across the board," with "dominance and momentum on its side." Guardium earned the highest overall scores for Architecture, Current Offering and Corporate Strategy.

About Guardium, an IBM Company

Guardium, an IBM Company, safeguards critical enterprise information by continuously monitoring access and changes to high-value databases. Guardium's scalable platform simplifies governance with unified policies for heterogeneous infrastructures while reducing operational costs by automating compliance processes, enabling organizations to safely use trusted information to drive smarter business outcomes.

Guardium's enterprise platform is now installed in more than 450 data centers worldwide, including 5 of the top 5 global banks; 4 of the top 6 insurers; top government agencies; 2 of the top 3 retailers; 20 of the world's top telcos; 2 of the world's favorite beverage brands; the most recognized name in PCs; a top 3 auto maker; a top 3 aerospace company; and a leading supplier of business intelligence software.

Guardium was the first company to address the core data security gap by delivering a scalable enterprise platform that both protects databases in real-time and automates the entire compliance auditing process.



Copyright © 2010, Guardium, an IBM Company. All rights reserved.
Guardium is a registered trademark and Safeguarding Databases, S-GATE
and S-TAP are trademarks of Guardium.

February 2010
All Rights Reserved.

IBM, and the IBM logo are trademarks of International Business Machines Corporation in the United States, other countries or both. For a complete list of IBM trademarks, see www.ibm.com/legal/copytrade.shtml.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

Any reference in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.



Please Recycle
