**IBM Information Management**
Brochure

# Protect your SAP data environment with IBM InfoSphere Guardium

*A proactive approach to database monitoring helps prevent fraud and ensure compliance*

IBM

## SAP data environments: Is your organization ready to rise to the challenge?

Protecting your SAP data repositories is a matter of extreme importance, particularly when the data in question is sensitive personal information subject to external regulations such as PCI DSS, Sarbannes-Oxley and HIPAA. Basic database security practices are insufficient to truly protect these high-risk data environments. Instead, organizations need a proactive approach to database security, building a platform that includes real-time monitoring, application-level fraud detection, and user-specific rules. With IBM® InfoSphere® Guardium®, you can build a database security platform that meets the challenges of the SAP data environment.

Today, many organizations are starting to realize that building an effective database security platform is not a one-time event, but rather a process that occurs over time. Data security solutions from IBM InfoSphere Guardium can help simplify this process in your organization by providing preconfigured rules and policies that help take the guess work out of securing a database environment. By using Guardium to secure SAP database environments, your organization can monitor user activity to detect and respond to fraud, without causing large-scale disruption of IT operations.

Organizations face unique challenges when it comes to protecting sensitive SAP data, such as:

- **Dispersed data:** Sensitive information may occur in hundreds of different database columns, making it extremely difficult to conduct column-level monitoring or encryption.
- **Performance:** SAP database environments need to maintain maximum responsiveness, even while security measures are being implemented.
- **Data variety:** Both structured data (database files) and unstructured data (log files, extract-transform-load data files, and archive data) need to be protected.
- **Supportability:** Modifying SAP applications or altering database tables jeopardizes support agreements.
- **Expense and total cost of ownership:** Custom encryption development may be extremely expensive, due to the wide breadth of SAP applications.
- **Privileged user access:** Insiders with privileged access to SAP data could potentially harm the data without their actions being tracked.

## Key benefits

IBM InfoSphere Guardium is the world's most widely-deployed database activity monitoring platform, making it a proven solution for securing SAP data to meet rigorous data governance and compliance regulations. By going beyond existing SAP logs, the Guardium solution can provide enhanced SAP fraud monitoring that helps your organization meet even the most stringent regulatory and audit requirements.

The solution can also be deployed in a diverse range of environments, with database support for all major DB vendors on all major operating systems, including UNIX, Linux and Microsoft Windows, Z/OS and iSeries, and file support for files located in physical, virtual and cloud environments. No matter what your SAP software environment looks like, IBM has the experience and best practices you need to ensure that your SAP software environment continues to operate at optimal performance levels.

When users initiate pooled connections or super-user rights, tracking their actions and accounting for your data becomes even more of a challenge. The InfoSphere Guardium solution provides application user translation and sudo tracking to help keep all users responsible for their actions, no matter who they are or how they're accessing the database. The solution also allows you to track SAP_ALL misuse, to ensure that your most powerful users aren't able to threaten your data, or cover up their tracks afterwards.

InfoSphere Guardium can begin protecting your SAP environment with no modification to your existing database environment, allowing for quick and cost-effective implementation with little or no down time. By eliminating dependency on native logging, the Guardium solution can save your organization between $15,000 and $40,000 per year per terabyte of live data on audit data storage costs. Guardium also provides protection for both structured and unstructured data, ensuring that all of your sensitive data and audit requirements are being met. The solution can be scaled effortlessly to meet the needs of all SAP software environments, no matter how large or complex. The Guardium solution offers all of these benefits, all while coming preconfigured with rules and settings designed to make managing data in SAP environments easier.

## Customer references

### Consumer food manufacturer

A Fortune 500 consumer food manufacturer with 15 billion dollars in annual revenue needed to secure its SAP data for Sarbannes-Oxley compliance. By deploying an InfoSphere Guardium database security platform, the company took a proactive approach to securing their data, realizing a 239 percent return on investment and full payback of their initial investment in less than six months. The solution also helped the company pass a series of four separate internal and external audits.

### National retail chain

A national retail chain of over 6400 stores needed a way to drive PCI and Sarbannes-Oxley compliance in their five major data centers. The organization operated an extremely complex data environment, including many different database servers and custom applications. In only four weeks, the company was able to implement the InfoSphere Guardium solution and save themselves millions of dollars in potential penalties for non-compliance. The solution included a number of features that automated specific PCI requirements, such as compensating control for database encryption, maintaining secure systems, and tracking and monitoring all access to cardholder data.

## What analysts are saying

*"Most enterprises are paying too little attention to the very real security risks associated with their databases … Native logging isn't the answer [lack of granularity, separation of duties not supported, high overhead]."*

-Jeff Wheatman, Gartner

*"Basic database security is no longer sufficient to protect private data … Critical databases have hundreds or even thousands of connections per second, so it is humanly impossible to view and detect security anomalies."*

-Noel Yuhanna, Forrester Research

*"Databases house a higher percentage of confidential data than any other type of repository … In most organizations (63 percent), database security depends primarily on manual or ad hoc processes … no match for well-organized cybercriminals, malicious insiders and accidental events."*

-Jon Oltsik, Enterprise Strategy Group

## Why IBM?

IBM InfoSphere Guardium is part of the IBM InfoSphere portfolio, an integrated platform for defining, integrating, protecting and managing trusted information across your systems. The IBM InfoSphere platform provides all the foundational building blocks of trusted information, including data integration, dataware housing, master data management and information governance, all integrated into a core of shared metadata and models. The portfolio is modular, so you can start anywhere and mix and match IBM InfoSphere software building blocks with components from other vendors, or choose to deploy multiple building blocks together for increased acceleration and value. The IBM InfoSphere platform establishes an enterprise-class foundation for information-intensive projects, providing the performance, scalability, reliability and acceleration needed to simplify difficult challenges and deliver trusted information to your business faster.

## For more information

To learn more about IBM InfoSphere, please contact your IBM sales representative or visit: **ibm.com**/software/data/guardium/



IBM Software
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
October 2012



IMB14150-USEN-01