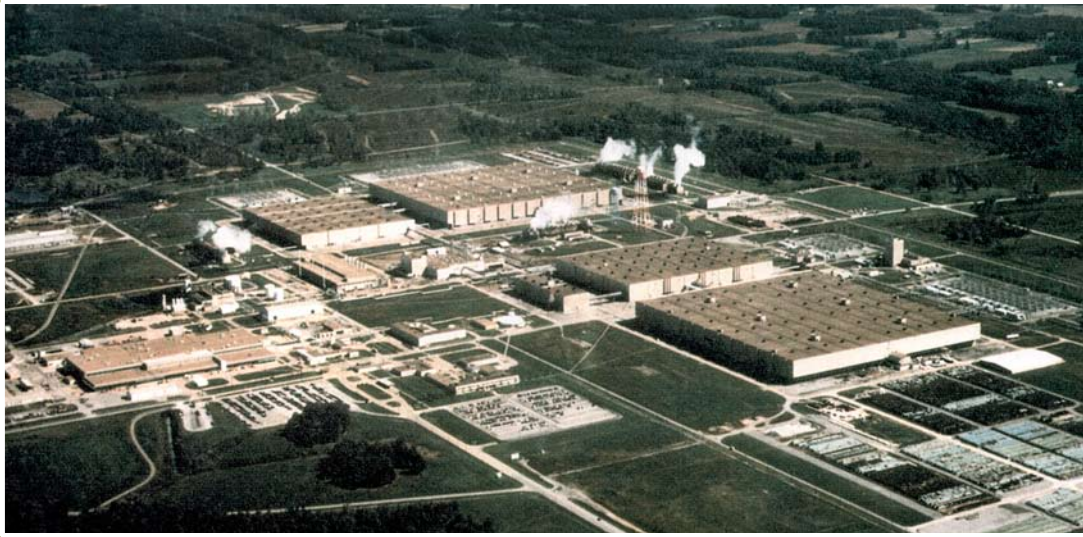
Guardium®

Customer Success Story

USEC Case Study



Industry: Energy

Employees: 2,800

Annual revenue: $1.6 billion

Number of data centers: 3

Applications: Oracle Financials, PeopleSoft, and in-house inventory applications

Database platforms: Oracle and Microsoft SQL Server

url: www.usec.com

Business Results

- Enhances internal controls without impacting performance or business processes
- Eliminates hundreds of staff hours to pass SOX audits
- Prevents privileged insiders from unauthorized access and changes to critical data and database structures
- Immediately uncovers user activity in all databases, revealing policy violations and most vulnerable data

"I had a problem and Guardium solved it," said Gorrie. "Guardium not only reduced our compliance costs as promised, but also enhanced our database security safeguards to continuously protect our most sensitive data."

"No other solution even approached what Guardium can do," said Gorrie. As enterprises confront stringent SOX requirements, solutions must minimize insider threats and unauthorized changes, while fully documenting compliance for efficient audits.

"Guardium's technology was key to helping us pass our SOX audit. The Guardium system gives us both real-time alerting and granular audit reporting, while automating the entire process. This helps us meet our auditors' requirements while saving us several hundred hours a year in staff time."

~ Robert G. Gorrie, Corporate Information Security Manager at USEC

Challenge: Monitoring Privileged Users to Pass SOX Audits – Without Impacting Performance

USEC Inc. (NYSE:USU) is a global energy company and operator of the only uranium enrichment facility in the U.S. As a highly regulated public company, USEC must comply with Sarbanes-Oxley (SOX) mandates requiring real-time, granular controls governing activities of database administrators (DBAs) on critical financial and HR databases.

Specifically, USEC requires controls that proactively identify unauthorized database changes that could affect the integrity of its financial data, such as changes to critical tables and whenever database applications are patched. In addition, the company was looking for a way to easily reconcile all changes with approved work orders from its corporate change tracking system.

"You have to trust your DBA," said Robert G. Gorrie, USEC's Corporate Information Security Manager, "but 'trust' is not something that will keep your auditors at bay."

At the same time, USEC's controls must allow DBAs to do their jobs, fully supporting enterprise databases without hindering their daily responsibilities. New policies that would add overhead, decrease database performance or increase maintenance and support time would be costly and counterproductive.

Incomplete Tools a Burden

Companies can choose outside help, or attempt to capture user data with native database logging solutions. USEC, however, learned that most offerings are insufficient for auditors' requirements, and that native logging was inherently risky and ineffective.

Proposed solutions included intrusion detection systems (IDS), agent-based technology and proxy access scenarios. Those tools, however, lacked granular views into DBA activities and would have consumed hundreds of hours of staff time to manually review logs – equivalent to entire weeks of work for the company's 50-person IT department.

[1] Intelligent Enterprise: *Field Report: Nuclear Fuel Supplier Tightens Database Security*, by Mark Leon, February 23, 2007

Native database logging was also not an option. "The problem with a lot of database products is that the logging that's built into them is fully configurable by the DBAs themselves. So you can turn on logging, but the DBA can turn it right off," added David Vordick, Chief Information Officer (CIO) at USEC.

In addition, native logging significantly diminishes database performance and processing speed, unacceptable side-effects.

A Single, Unified Solution: Detect, Define, Deter

Guardium's appliance-based solution monitors all network traffic at the SQL command level, giving USEC a detailed, irrefutable view of all database access. Guardium protects all three of USEC's data centers in Kentucky, Maryland and Ohio, while maintaining maximum database performance.

USEC's implementation of Guardium gives the energy company a comprehensive offering to meet audit needs and enforce security policies with:

- A single, cross-platform solution for all database platforms and locations
- Granular, real-time controls governing database access and changes
- Instant alerts of unauthorized activities to security staff
- Pre-configured reports tailored for SOX requirements.

"No other solution even approached what Guardium can do," said Gorrie. As enterprises confront stringent SOX requirements, solutions must minimize insider threats and unauthorized changes, while fully documenting compliance for efficient audits.

The implementation only took a few weeks, providing a quick return by allowing USEC to fill security and compliance gaps rapidly after the purchase.

USEC uses Guardium's solution to provide real-time controls that proactively identify any unauthorized database changes that could affect the integrity of its financial data. For example, alerts are immediately generated whenever changes are made to critical tables and whenever database applications are patched. In addition, the Guardium solution tracks all changes down to the SQL statement level and stores this fine-grained audit information in a secure, tamper-proof repository, allowing IT security managers to easily reconcile all changes with approved work orders from its corporate change tracking system.

To map its multi-site network, USEC used Guardium to identify who accessed each database, when it was accessed and what questionable patterns of behavior existed. The findings revealed issues in applications accessing critical data, and changes to data and their underlying structures. "The discoveries helped us define policies for access and change control," said Gorrie.

The result: a new process requiring DBAs to give Gorrie advance notice of scheduled, authorized database changes; Gorrie then cross-references access and changes against these approved actions to ensure only permitted work occurs. Guardium stores all actions, which are captured at the fine-grained SQL statement level, in a secure, tamper-proof repository. If USEC needs to delve into specific user actions or database activity, it can quickly search aggregated information as a forensics tool, eliminating the time-consuming manual process of poring through old log files.

SOX and Security Successes

USEC has passed two SOX audits since implementing Guardium's system. Both audits avoided weeks of manually compiling the required data by leveraging Guardium's pre-configured SOX reports to prove that DBAs and other privileged insiders complied with mandates. Auditors immediately noted essential controls around critical corporate data and the proactive alerting Guardium gives when users violate IT policies.

"Guardium's approach was key," said Gorrie. "The Guardium system gives us both real-time alerting and granular audit reporting, while automating the entire process. This helps us meet our auditors' requirements while saving us several hundred hours a year in staff time."

"When it comes to Sarbanes-Oxley," said Vordick, "it's good to have one less thing to worry about."

USEC tightened database security with Guardium's patent-pending S-TAP™ (software tap) to monitor "back-door" local access over non-network connections, closing a gaping hole that DBAs could otherwise exploit.

Guardium also prohibits use of unauthorized applications, such as developer tools, from accessing critical production databases, which could affect the integrity of its enterprise data.

"I had a problem and Guardium solved it," said Gorrie. "Guardium not only reduced our compliance costs as promised, but also enhanced our database security safeguards to continuously protect our most sensitive data."

[2] SearchDataManagement.com: ***Database Activity Monitoring Helps USEC with SOX Compliance, by Hannah Smalltree***, February 27, 2007

[3] CIO Decisions: (Problem Solved) – ***Answers for Auditors***, by Ellen O'Brien, March 2007

Guardium®
SAFEGUARDING DATABASES™

230 Third Avenue • Waltham, MA 02451 USA • T: +1 781 487 9400 • F: +1 781 487 7900 • www.guardium.com