



Guardium eNews: May 2008

## CONTENTS

- Guardium Unveils First Cross-DBMS Solution to Block Privileged User Access to Sensitive Data and Enforce Separation of Duties
- Guardium Wins *Red Herring* 100 and is Named American Business Awards Finalist
- Complimentary SANS White Paper on DAM
- Guardium Launches New Web Site
- Best Practices Seminar Featuring Gartner: June 10 in Charlotte
- PCI and TJX Discussed in RSA Video Interview
- Survey Indicates Internal Employees Pose Biggest Threat (*Information Security*)
- Military Contractor Raids Government Database (*Computerworld*)
- Coding Error Exposes Personal Data (*SC Magazine*)
- Risk Management Lessons from Société Générale (*CIO*)
- *BankInfoSecurity* Podcast about Database Security for Financial Services

## **Guardium Unveils First Cross-DBMS Solution to Block Privileged Users from Accessing Sensitive Data**

***For the First Time, Organizations Can Fully Enforce Separation of Duties - Without Disrupting Business Processes or How DBAs Do Their Jobs***

Guardium just announced the first cross-DBMS solution that prevents privileged users - such as DBAs, application developers and outsourced personnel - from viewing sensitive data in corporate databases.

Guardium S-GATE™ is the only technology that allows organizations to safeguard enterprise data and meet compliance requirements without the cost and complexity of modifying databases, application code or existing business processes, and without relying on "after-the-fact" mechanisms such as logging and alerting.

S-GATE's ability to enforce granular access control policies that apply only to privileged users means that organizations can now implement robust preventive controls - without the risk of blocking legitimate business access.

S-GATE also strengthens security and enforces separation of duties (SOD) by preventing DBAs from performing security functions such as creating new database accounts and elevating privileges for existing accounts. At the same time, authorized individuals can continue to use

their system privileges to perform day-to-day administrative tasks - including backups, patching and tuning - without interruption.

Since S-GATE leverages Guardium's existing policy engine, it can actually be used to block ANY transaction, not just those from privileged users (although we expect that privileged user enforcement will be its primary use initially). In the Guardium system, policies are flexibly defined based on any combination of session parameters, such as the database user name, OS user name, IP address, source application, SQL command, specific database object they're accessing, etc.

With V7, Guardium now protects against insider threats in several ways. First, it continuously monitors all database transactions and stores the audit trail in a centralized repository for forensic investigations and verifying compliance. Second, Guardium allows you to create policies that automatically generate real-time alerts whenever an access rule has been violated, such as a DBA viewing cardholder data or deleting a critical financial table.

Security experts refer to these types of controls as "detective controls" -- similar to cameras at the entrance to the bank vault -- and they're fairly effective against insider threats because people are more careful about their behavior when they know they're being monitored.

S-GATE goes one step further by allowing you to actually block transactions that violate security policies -- similar to physically locking the door to the vault before any unauthorized access occurs. This is an additional layer of protection called a "preventive control."

Available with Guardium 7, S-GATE is an add-on extension to S-TAP ("software tap"), Guardium's lightweight, host-based agent. Unique in the industry, S-TAPs are non-intrusive software probes that monitor network streams at the OS level of database servers, including both network access and local access by privileged users (via shared memory, named pipes, Oracle Bequeath, etc.). S-TAPs have minimal impact on server performance because they relay all traffic to separate Guardium appliances for policy evaluation, analysis, reporting and secure online storage of audit trails.

[\*Click here to read the full release\*](#)

## **Guardium Wins *Red Herring* 100 and is Named American Business Awards Finalist**

Guardium won two coveted award recognitions in May:

- The *Red Herring* 100 North America, an award given for technology innovation to the top 100 private technology companies. Past winners have included Google, YouTube, Salesforce.com, Netscape, Yahoo! and Skype. *Red Herring's* staff chose Guardium after evaluating more than 1,500 private companies through a careful

analysis of financial data and subjective criteria, including quality of management, execution of strategy, and dedication to R&D.

- A finalist for the American Business Awards in the category of "Best New Product or Service - Computer Software." Other finalists in this category include: Microsoft, Adobe, Citrix Online, salesforce.com, and WebEx. Hailed as "the business world's own Oscars" (*New York Post*, April 27, 2005), The American Business Awards are the only national awards program honoring great performances in business.

[\*Click here to read the full Red Herring 100 release\*](#)

[\*Click here to read the full American Business Awards release\*](#)

## **SANS White Paper: Technical Overview on DAM**

This white paper provides a technical overview of database activity monitoring (DAM) and explains why DAM is "an extremely valuable tool for compliance and security." It describes deployment architectures, key features and evaluation strategies.

Written by Rich Mogull, former Gartner security analyst, the paper describes how DAM is a real-time database security and auditing tool that records all DBMS activity without the overhead of local database logging. For example, DAM monitors all DBA activity and enforces separation of duties for SOX. For PCI, it provides a compensating control for encryption.

The paper also explains how DAM provides real-time security that:

- Prevents data breaches for Web-facing applications
- Protects sensitive databases by detecting unusual activity and unauthorized access by insiders
- Enforces change and configuration policies for databases
- Provides database-focused monitoring and analytics that aren't available with SIEM tools

[\*Download whitepaper here\*](#)

## **Guardium Launches New Web Site**

The new version of Guardium's site taps Web 2.0 functionality such as tabbed entries to make it easier for visitors to access the wide range of educational content available on the site. The new site is filled with data security resources including case studies, white papers, lab reviews, Webcasts and industry analyst reports. A Flash animation on the home page describes several of Guardium's customers and the business problems we've solved for them.

[\*Check out the new home page here\*](#)

[\*Check out the Resources section here\*](#)

## **Best Practices Seminar Featuring Gartner**

Guardium is hosting a three-city seminar series featuring a Gartner analyst and Guardium's CTO. New York and Chicago wrapped in early May, and Charlotte is scheduled for June 10, educating C-level executives and day-to-day IT security and database professionals on the latest technology to safeguard enterprise data and automate compliance controls.

CTOs, CSOs and DB administrators will receive strategic and tactical recommendations on how to effectively protect sensitive data stored in corporate databases, mitigate risk and tighten internal controls while reducing costs to comply with Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI-DSS) and data privacy laws.

[Register here](#)

## **PCI and TJX Discussed in RSA Video Interview**

Guardium's Phil Neray was interviewed from RSA by freelance reporter Ericka Chickowski. Topics include database security, TJX, PCI and retail data breaches.

[Watch here](#)

## **Survey Indicates Internal Employees Pose Biggest Threat**

Marcia Savage, *Information Security*

The 2008 Global Information Security Workforce Study, conducted by analyst firm Frost and Sullivan for certification organization (ISC)2, surveyed 7,548 information security pros worldwide.

Fifty-one percent of the respondents said internal employees pose the biggest threat to their organizations. The finding represents an ongoing trend in the past two to three years, as the numbers of remote workers and portable storage devices have jumped in the enterprise, said Rob Ayoub, Frost & Sullivan network security industry manager.

[Read story here](#)

## **Military Contractor Raids Government Database**

Grant Gross, *Computerworld*

A former U.S. military contractor has pleaded guilty to exceeding authorized access to a computer and aggravated identity theft after he was accused of selling names and Social Security numbers of 17,000 military employees, the U.S. Department of Justice said.

Randall Craig, 41, of Houston, pleaded guilty today to both counts of an indictment returned in April by a grand jury in U.S. District Court for the Southern District of Texas. Craig acknowledged selling information contained in a military database to a person he believed to

represent a foreign government, according to the U.S. Attorney's Office for the Southern District of Texas and the FBI.

[Read story here](#)

## **Coding Error Exposes Personal Data**

Jim Carr, *SC Magazine*

A software security researcher has exploited a flaw in the sex offender registry webpage operated by the Oklahoma Department of Corrections.

The vulnerability, caused by a SQL query in the page's URL, allowed the researcher to download the Social Security numbers of more than 10,000 individuals.

The people who wrote the web application made some basic mistakes in how they wrote it, specifically in the case of SQL injections, said Phil Neray of Guardium. "You need to verify the input from web application before forwarding the query to the database, and obviously they were not doing that."

[Read story here](#)

## **Risk Management Lessons from Société Générale**

Peter Sayer, Thomas Wailgum, *CIO*

An investigation into rogue trader Jérôme Kerviel's allegedly fraudulent actions at Société Générale bank uncovered an apparent breakdown in financial and internal IT controls subverted by an employee with IT know-how and authorized systems access.

The tale of Kerviel's exploits, which led to \$7.2 billion in losses for one of France's largest banks, continues to unfold as French police probe the 31-year-old trader's transactions.

Meanwhile, IT experts say, the case should serve as a warning that businesses can do better to manage IT-related risk.

[Read story here](#)

## **BankInfoSecurity.com Podcast about Database Security for Financial Services**

Guardium's Phil Neray is interviewed on trends in database security for the financial sector, as part of BankInfoSecurity.com's RSA coverage.

[Listen to or download the podcast here](#)

## **UPCOMING EVENTS**

*Please visit us at the following upcoming events:*

**Gartner IT Security Summit**

June 2 - 4, 2008

Gaylord National Resort  
Landover, MD

**Best Practices for Database Security & Compliance -- Featuring Gartner**

June 10, 2008  
Westin Charlotte  
Charlotte, NC

**New England DB2 Users Group**

June 17, 2008  
Host Hotel  
Sturbridge, MA

Guardium's CTO, Ron Bennatan, Ph.D., will be presenting "Best Practices for Database Security and Data Governance" from 10:45 to noon. Eric Offenbergl from IBM will be presenting on "Understanding Data Governance" from 13:00 to 14:15.

**Gartner Identity and Access Management Summit for EMEA**

June 23 - 24, 2008  
Royal Lancaster Hotel  
London, UK

**Sybase TechWave**

August 4 - 8, 2008  
Mandalay Bay Convention Center  
Las Vegas, NV

**STAY ON THE MAILING LIST**

**[Please click here.](#)**

And please let us know what you like (and don't like) about our newsletter - just send an email to [phil\\_neray@guardium.com](mailto:phil_neray@guardium.com).

***Quick Links***

[Auditing & Compliance](#)  
[Database Activity Monitoring](#)  
[Change Control](#)  
[Database Leak Prevention](#)  
[Lab Reviews, Case Studies & White Papers](#)  
[Media Coverage & Upcoming Events](#)

***✓ Secure enterprise data ✓ Pass the audit***

Copyright © Guardium 2008. All rights reserved.  
Guardium is a trademark of Guardium. All other trademarks and service marks are the property of their respective owners.