



Guardium eNews: March 2008

CONTENTS

- **Guardium Now Installed in More Than 350 Data Centers Worldwide Including 3 of Top 4 Global Banks**
- **Guardium Integrates with SIEM and Log Management Leaders to Deliver Comprehensive Information-Centric Security**
- **Gartner Analyst & CIO of NYSE-Traded Company Discuss DAM (Videocast)**
- **Podcast: Rich Mogull Discusses SocGen Breach: Highlights Need for Monitoring and Auditing**
- **Reminder: Forrester Webcast Archived**
- **Breach of MTV Computer Files**
- **Should You Hire a Convicted Hacker?**
- **2 minutes on....Data breach law expands**
- **Is the Risk Manager to Blame for the Subprime Crisis and the Société Générale Scandal?**
- **Partner News**
- **Upcoming Events**

Guardium Now Installed in More Than 350 Data Centers Worldwide, Including 3 of Top 4 Banks, One of World's Largest PC Manufacturers and a Global Soft Drink Brand

Guardium recently announced that it doubled its customer base in 2007 and is now installed in more than 350 data centers worldwide, including more than 60 Global 500 and Fortune 1000 companies in all major industries.

Blue-chip customers include:

*** Financial Services:** 3 of the top 4 global banks, one of the top cardholder brands worldwide and one of the largest mutual fund companies in the U.S.

*** Manufacturing:** Many global leaders including a global soft drink brand, one of the world's largest PC suppliers and one of the world's largest automotive companies.

*** Retail & Hospitality:** Well-known brands including Wyndham International, one of the top 3 global retailers, a well-known coffee retailer, one of the top 3 U.S. food & drug retailers and a major office supply brand.

* **Software & Services:** More than a dozen companies including ChoicePoint, one of the market leaders in business intelligence software and Premiere Global Services.

* **Insurance:** 3 of the top 5 global insurance companies plus 2 of the top 5 U.S. insurance companies.

* **Energy:** Some of the country's largest energy companies including National Grid, Nevada Power and USEC.

* **Telecommunications:** 12 leading telecommunications companies including 3 of the top 10 worldwide.

* **Transportation:** Major transportation organizations including BNSF Railway Company, Frontier Airlines and Tampa International Airport.

* **Government:** Several well-known government agencies including the Federal Trade Commission (FTC) and the Washington Metropolitan Area Transit Authority.

* **Health Care:** Major organizations including Blue Cross-Blue Shield of Hawaii (HMSA) and Blue Cross-Blue Shield of North Dakota (Noridian Mutual).

* **Media & Entertainment:** Five leading media brands including Discovery Communications (parent company of the Discovery Channel).

The company's financial performance and rapid customer adoption are a result of its innovative enterprise architecture, which enables organizations to safeguard the privacy and integrity of critical data in enterprise applications such as Oracle E-Business Suite, PeopleSoft, SAP, Business Intelligence and in-house systems.

At the same time, Guardium's scalable platform optimizes operational efficiency by automating and centralizing compliance controls across heterogeneous data center environments.

[*Click here to view the full release.*](#)

Guardium Integrates with SIEM and Log Management Leaders to Deliver Comprehensive Information-Centric Security

Integration with ArcSight ESM, CA, Cisco MARS, LogLogic, RSA enVision and SenSage Provides 100% Visibility and Database Analytics for SOX, PCI-DSS and Data Privacy

Guardium is integrating its database activity monitoring (DAM) platform with leading security information and event management (SIEM) and log management systems.

Until now, SIEM users were faced with the challenge of importing raw logs generated by internal DBMS utilities. This is typically impractical because internal DBMS utilities impose significant performance overhead on databases and produce massive amounts of unfiltered information -- or don't capture critical activities such as

unauthorized or suspicious queries to sensitive information including cardholder data.

In addition, native utilities are unable to identify end-user fraud and other abuses that occur via multi-tier enterprise applications -- such as Oracle e-Business Suite, PeopleSoft, SAP and Business Intelligence -- rather than via direct access to the database. Finally, native DBMS utilities don't meet auditors' requirements for separation of duties since they are managed by DBAs whose activities also must be audited.

By combining Guardium's contextual knowledge of database activity patterns, structures and protocols, with SIEM and log management products from ArcSight, CA, Cisco, LogLogic, RSA (the Security Division of EMC) and SenSage, organizations can now enhance their ability to:

- * Proactively identify and mitigate risks from external attacks, trusted insiders and compliance breaches.
- * Implement automated controls for Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI DSS) and data privacy regulations.
- * Manage system and network events alongside critical logs and events from the core of their data centers -- enterprise databases and applications -- for enterprise-wide correlation, forensics, incident prioritization and reporting.

Guardium's scalable enterprise platform consolidates and normalizes audit information from multiple DBMS platforms, enterprise applications and data center locations into a single centralized repository. Its real-time monitoring technology uses both policy-based controls and anomaly detection to detect and prevent unauthorized or suspicious activities.

Other information which can be forwarded to SIEM systems include security exceptions related to: suspicious database errors and failed logins; discovery and classification of sensitive data; configuration audits; and changes to database structures and data values that don't match authorized changes in change management systems such as BMC Remedy.

[**Read the full release here**](#)

Gartner Analyst & CIO of NYSE-Traded Company Discuss DAM

You're invited to a Videocast featuring a Gartner analyst, Guardium and David Vordick, CIO for USEC, a \$1.85 billion, NYSE-traded energy company. In this on-demand presentation:

- * Gartner discusses the benefits of database activity monitoring (DAM), including a comparison to complementary technologies including security information and event management (SIEM), data leakage protection (DLP) and database encryption.

* David Vordick describes how Guardium addressed his security and compliance challenges, and why he chose Guardium.

* Phil Neray of Guardium highlights 3 customer case studies and provides an overview of the Guardium architecture.

[Watch Videocast here](#)

Insider Costs Bank \$7 Billion - Password Sharing?

Securosis' blogger and former Gartner analyst Rich Mogull discusses Jerome Kerviel, the former Société Générale trader who managed to lose \$7 billion during the past year, all while using his knowledge of the bank's security system to conceal the financial damage. He also discusses the need for tighter monitoring controls to protect against password-sharing and similar practices that hide individual accountability.

[Listen to podcast here](#)

Webcast with Forrester: Best Practices for Database Security & Compliance

View an archived Webcast of "Best Practices for Database Security and Compliance" with Forrester analyst Noel Yuhanna: Includes discussion of the Forrester Wave -- a comprehensive assessment covering 14 vendors across 116 criteria -- and an overview of the Guardium architecture.

[Click here to view archived Webcast](#)

Breach of MTV Computer Files

By *REUTERS*

Computer files with confidential data on **about 5,000 employees** at MTV Networks were **breached by someone outside the company**, the network told employees.

MTV later said in a statement that the security breach occurred after an Internet connection in an employee's computer was compromised.

Although it was not immediately clear whether the password-protected files were opened, MTV, a division of Viacom, notified law enforcement authorities and a credit monitoring company to safeguard the identities of the affected employees, the statement said.

[Read full article](#)

Should You Hire A Convicted Hacker?

By Mathew Schwartz, *InformationWeek*

What happens when hackers who have served time in prison or home confinement are released? The very skills that can land them behind bars are skills they share with high-achieving, law-abiding IT security

professionals. But convicted hackers looking for legitimate employment are not necessarily finding it in the enterprise.

[Read full story here](#)

2 minutes on....Data breach law expands

By Jim Carr, *SC Magazine*

California's extension of its **data breach notification law to cover health care records** promises to have significant impact on how medical organizations deal with patient information. Most notably, it fills what might be called a loophole in HIPAA.

Prior to passage of AB1298, which took effect in January, organizations that lost medical records weren't required to notify victims if the lost records didn't contain their name and Social Security number and one of several other data elements, including account numbers with a personal identification number or a driver's license or California ID card.

"We've had a similar law in Massachusetts since October 2007," noted John Halamka, CIO of CareGroup Health System as well as the CIO of Harvard Medical School. "Our response was to document all the databases that contain personally identifiable information, ensure they were protected with strong technical security, and that they have audit trails that our privacy officer can review."

[Read full story here](#)

Is the Risk Manager to Blame for the Subprime Crisis and the Société Générale Scandal?

By Melanie Rodier, *Wall Street & Technology*

As is usually the case with rogue traders, Kerviel had too much control, says Rob Hegarty, managing director of TowerGroup's securities and investment practice. "This shows a lack of supervisory procedures, and lax monitoring from the systems' standpoint," he says, adding, "Kerviel also had in-depth knowledge of multiple areas of the company."

Even though he circumvented the bank's risk management systems, Kerviel was no computer genius, Hegarty notes. "He wasn't even close to being one," he says. "He was just knowledgeable in checks and balances. He probably had a little technical knowledge, but it was more a case of operational knowledge."

"Many financial institutions think they have proper security controls in place," adds Phil Neray, VP of database security provider Guardium. "But password controls only allow specific database users from making changes to data. The most they will tell you is that someone with privileged access logged on at a given time, but they won't say what commands were executed -- that level of granular monitoring doesn't exist. So **if someone has access to a privileged account, they can go in and cover their tracks, and no one would know.**"

[Read story here](#)

Partner News

Guardium is pleased to announce that it has executed a Distribution Agreement with COMPUTERLINKS. This Agreement allows COMPUTERLINKS to distribute Guardium technology in the United Kingdom, Ireland, Germany, Austria, Switzerland, Denmark, Norway, Sweden and Finland.

We would like to extend an invitation to our partners and their customers to visit us at the upcoming RSA Conference from April 7-11 in San Francisco, CA. You can find Guardium at Booth # 2450. We look forward to seeing you!

UPCOMING EVENTS

Please visit us at the following upcoming events:

[RSA CONFERENCE 2008](#)

APRIL 7-11, 2008

San Francisco, CA

Booth #2450

Request your free expo pass - a \$100 value - by emailing peg.odonnell@guardium.com. Act now - offer good until April 4th!

[SANS \(SysAdmin, Audit, Network, Security\) 2008](#)

April 21 - 22, 2008 (Exhibits)

Walt Disney World Dolphin

Lake Buena Vista, FL

Booth #206

[Infosecurity Europe](#)

Apr. 22-24, 2008

Grand Hall, Olympia

London, UK

Booth #D122

[2008 IIUG Informix Conference](#)

Apr. 27-30, 2008

Overland Park Marriott

Overland Park, KS

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.

Quick Links

Auditing & Compliance: www.guardium.com/solutions/auditing_compliance

Data Security: www.guardium.com/solutions/data_security

Change Control: www.guardium.com/solutions/change_control

Leak Prevention: www.guardium.com/solutions/db-leak-prevention

Lab Reviews, Case Studies & White Papers:

www.guardium.com/resources/collateral

Media Coverage: www.guardium.com/press/media

Upcoming Events: www.guardium.com/press/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.