



Guardium eNews: April 2008

CONTENTS

- Best Practices Seminar Series Featuring Gartner
- Guardium Announces First Solution to Monitor Encrypted Database Traffic
- Guardium Integrates Vulnerability Management to Better Protect Databases, Assess Risk and Reduce Compliance Costs
- Guardium Ties Activity Monitoring to Major SIEM Products (*eWeek*)
- TJX to Pay \$24M More for Lost Data (*USA Today*)
- Unified Threat Management, Demystified (*CIO Magazine*)
- Employees Snoop on Customer Data (*AP*)
- Hannaford Data Heist Shows Limits of PCI (*ZeroDayThreat.com*)
- Man Charged with ID Theft at NY Hospital (*AP*)
- FAQ: The Passport Breach: What Exactly Is in Those Records? (*Computerworld*)
- Upcoming Events -- including complimentary IDUG exhibits pass

Best Practices Seminar Series Featuring Gartner

Produced by the publisher of SearchSecurity.com and Information Security Magazine

Gain face-to-face access to a top expert from Gartner as he reveals the latest, most effective solutions to safeguard your critical enterprise data and automate your compliance controls. Attendees will:

-- Benefit from Gartner's tactics to mitigate risk and tighten internal controls while simplifying and reducing the cost of compliance (for SOX, PCI, and data privacy laws).

-- Discover how to increase operational efficiency by automating and centralizing database logging and reporting across all your database platforms, data centers and compliance initiatives.

MAY 6, 2008
Marriott Marquis
New York, NY

MAY 8, 2008
InterContinental Chicago
Chicago, IL

JUNE 10, 2008
Westin Charlotte
Charlotte, NC

SEPTEMBER 9, 2008
San Francisco, CA

[Click here for full event information](#)

[Register for a seminar here](#)

Guardium Announces First Solution to Monitor Encrypted Database Traffic, Including Oracle ASO

Guardium announced the **first database activity monitoring (DAM) solution that inspects encrypted database traffic**. Guardium 7 helps organizations prevent anomalous behavior in real time - even in highly secure environments where encryption is mandated - and create a granular audit trail for forensic investigations and regulatory compliance, without impacting application or database performance.

Arup Nanda, long-time Oracle DBA and co-author of *Oracle Privacy Security Auditing* (Rampant TechPress), commented: "Guardium 7 addresses a critical need by supporting Oracle ASO network encryption with non-invasive, fine-grained monitoring and auditing for encrypted database traffic over the wire. Encrypting sensitive information such as credit card numbers is a requirement for most organizations, but it doesn't eliminate the need for an additional layer of defense. DAM solutions protect sensitive information from external threats and abuses by privileged insiders." Mr. Nanda was also named "DBA of the Year" by Oracle Magazine and is a member of the New York Oracle User Group Executive Committee.

Data privacy regulations such as the Payment Card Industry Data Security Standard (PCI-DSS) require companies to encrypt sensitive information moving across public networks, such as the Internet. Until now, DAM solutions were prevented from analyzing encrypted traffic because they could not see the actual content of each session, such as which SQL commands were being executed, by whom, and on which database objects.

The new technology has been incorporated into **an enhanced version of Guardium's S-TAP™** (software tap). Unique in the industry, S-TAPs are lightweight software probes that monitor network streams at the OS level of database servers. They have minimal impact on performance because they relay all traffic to separate Guardium appliances for analysis, reporting and online storage of audit trails in a secure, tamper-proof repository.

In Version 7, Guardium monitors encrypted traffic on all major operating systems including Sun Solaris, IBM AIX, HP-UX, Microsoft Windows, Red Hat Linux, and SUSE Linux. Support is provided for all network encryption methods used in Oracle environments including:

- **Oracle Advanced Security Option (ASO)**, which supports native Oracle Net encryption as well as SSL encryption via a range of algorithms including RSA's RC4, DES, Triple-DES and AES.
- **IPSEC**, an industry standard for encrypting IP communications.

- **SSH and SSL tunnels**, using services running on the host to terminate the encryption.
- **Hardware-based network encryption**, where the encryption is offloaded to specialized processors on a network interface card (NIC) so that there is no impact to the database server's CPU.

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

Guardium Integrates Vulnerability Management to Better Protect Databases, Assess Risk and Reduce Compliance Costs

Guardium announced that it has tightly integrated vulnerability management with its enterprise database security and compliance platform.

Guardium 7 is the first solution in the industry to address the entire database security and compliance lifecycle with a unified Web console, back-end data store and workflow automation system. With this unified approach, organizations now have a single scalable platform to deliver critical security and compliance functions across all of their data centers, DBMS platforms and enterprise applications, including:

- Comprehensive protection of critical enterprise data
- Risk assessment with business context, and
- Security and compliance at lower cost and with less effort -- freeing IT resources to focus on other strategic initiatives.

Guardium 7 allows organizations to rapidly:

- **Pinpoint database vulnerabilities.**
- **Prioritize remediation activities-based on business risk.**
- **Protect unpatched systems with real-time controls.**
- **Harden databases.**
- **Document and streamline compliance.**

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

"This integration is definitely beneficial - after all, it's all about data security, whether it's scanning, discovering, assessing the environment, auditing or monitoring," said Noel Yuhanna, an analyst with Forrester Research, to *eWeek*.

[*Read eWeek article on Guardium's vulnerability management integration*](#)

Guardium Ties Activity Monitoring to Major Data Security Products

By Brian Prince, *eWeek*

Guardium has integrated its technology with products from CA, Cisco Systems, ArcSight, LogLogic and EMC's RSA security division to improve visibility and analysis into security events.

The integration allows organizations to send information obtained from Guardium's DAM product to security information and event management

(SIEM) systems, **combining information about database activities with data regarding network and IT infrastructure events from firewalls and other sources.**

Forrester Research analyst Noel Yuhanna said integration between DAM and SIEM makes sense as organizations struggle with information security.

"Having information in one place for security is definitely very important, because you can relate audit and monitoring activities, and also implement policies, controls and procedures more easily and effectively," he said.

"The goal is definitely to deal with information security more centrally [and] monitor and audit activities across your organization, across any type of data, application and system, and also implement control, policies and procedures as well."

[Read full article](#)

TJX to Pay \$24M More for Lost Data

By Byron Achohido, *USA TODAY*

Discount retailer TJX has set what could be an expensive precedent for anybody who loses sensitive data to hackers or insider thieves.

The company agreed to pay MasterCard **\$24 million for losing records of 29 million MasterCard transactions.** That deal comes after TJX last November agreed to pay Visa \$41 million for losing 65 million Visa records. It has also paid an \$880,000 fine for violating the payment card industry's self-imposed rules for securing digital files.

Meanwhile, TJX has also set a benchmark for how costly it can be to lose sensitive data, a phenomenon that continues to accelerate at a record pace. **More than 300 companies, universities, government agencies and hospitals reported losing more than 162 million records in 2007, triple the amount from 2006,** according to USA TODAY's analysis of data loss news reports compiled by watchdog group Attrition.org.

The pace continues, with 66 data loss incidents reported so far this year. Last month, the Hannaford Bros. grocery store chain reported losing 4.2 million credit and debit card numbers, despite complying with the payment card industry's security rules.

"Digital assets aren't any different than physical assets," says Phil Neray, vice president of security firm Guardium. "If I entrust my jewelry to a repair store and it gets stolen, they're liable for the loss."

[Read full article](#)

Unified Threat Management, Demystified

By Bill Snyder, *CIO*

Protecting the secrets of a uranium enrichment plant should be enough to keep any CIO very busy. But when Sarbanes Oxley mandated even

tougher controls on databases containing key financial information, David Vordick, CIO of USEC, a \$1.9 billion public company that operates a gaseous diffusion plant in Paducah, Kentucky, knew he was going to get even busier.

His security defenses are complex and multi-layered; and while simplicity is generally a good thing, it's not Vordick's priority. "Our philosophy is defense in depth. That means looking at multiple (security) products from multiple vendors. We can not be dependent on any one layer," he says.

As USEC designed its security architecture, Vordick and his team had a wealth of options. They could have chosen to install one or more UTM (unified threat management) appliances, devices that handle multiple threats from a single chassis, or opted for a series of single function, best of breed appliances.

USEC chose a best-of-breed database security appliance by Guardium, plus point products from other vendors, largely because the defense in depth strategy meant that the convenience of deploying and managing a single device was outweighed by the fear of creating a single point of failure, Vordick says. Moreover, USEC sought a security appliance that would serve as a check on IT employees with privileged database access who might seek to view or change data without proper authorization, an atypical function for a UTM.

[*Read full article*](#)

Employees Snoop on Customer Data

Associated Press

A landlord snooped on tenants to find out information about their finances. A woman repeatedly accessed her ex-boyfriend's account after a difficult breakup. Another obtained her child's father's address so she could serve him court papers.

All worked for Wisconsin's largest utility, where **employees routinely accessed confidential information** about acquaintances, local celebrities and others from its massive customer database.

Vast computer databases give curious employees the ability to look up sensitive information on people with the click of a mouse. The WE Energies database includes credit and banking information, payment histories, Social Security numbers, addresses, phone numbers, and energy usage. In some cases, it even includes income and medical information.

Experts say **some companies do little** to stop such abuses even though they could lead to identity theft, stalking and other privacy invasions.

[*Read full article*](#)

Hannaford Data Heist Shows Limits of PCI

By Byron Achohido, ZeroDayThreat.com

Placing the burden on merchants to protect our sensitive data clearly is not a panacea. The hack/heist of 4.2 million customer transaction records from the Hannaford Brothers' supermarket chain emphatically makes that point.

As we've previously reported, TJX similarly lost 94 million customer records—partly because it failed to comply with the Payment Card Industry-Data Security Standards, mainly enforced by Visa and MasterCard.

But the Hannaford Brothers were PCI compliant—and still got ripped off.

Given that risk, implementing database monitoring and encryption are relatively simple and inexpensive, says Ron Ben-Natan, CTO of Guardium. And yet many organizations continue to believe "it won't happen to us," he says.

[Read full blog post](#)

Man Charged with ID Theft at NY Hospital

By Verena Dobnik, Associated Press

A man who worked in the admissions department at a prestigious Manhattan hospital has been charged with stealing and selling information on nearly 50,000 patients.

Prosecutors said Dwight McPherson, 38, a former worker at New York-Presbyterian Hospital/Weill Cornell Medical Center, exploited his access to the hospital's computer registration system to acquire lists of patient names, phone numbers and Social Security numbers over a two-year period.

McPherson told agents that in 2006 he was approached by someone offering money in exchange for the names, addresses and other identifying information of male patients born between 1950 and 1970. The complaint said McPherson sold a batch of 1,000 records in December or January for \$750, and another batch for \$600 a short time later.

[Read full article](#)

FAQ: The Passport Breach: What Exactly Is in Those Records?

By Jaikumar Vijayan, *Computerworld*

The U.S. Department of State admitted that the passport records of Sens. Barack Obama (D-Ill.), Hillary Clinton, (D-N.Y.), and John McCain, (R-Ariz.), were **improperly accessed by contract workers** this year. Just what sort of information did those contractors have access to? What records on the presidential candidates might they have seen? The State Department's own description of its passport record system offers some clues, as well as an indication of just how much data the government compiles on passport applicants.

- What exactly is a passport record?
- Where are passport records stored?
- What individuals and records are covered by the system?

- What else is in the system?
- How is the information collected?
- How is all this information used?
- Who uses the system?
- How is the information protected?

[Read full article](#)

UPCOMING EVENTS

Please visit us at the following upcoming events:

[IIUG - Informix User Group Conference 2008](#)

April 27 - 30
Overland Park
Kansas, KS

[IDUG - International DB2 User's Group](#)

May 18 - 22, 2008
Hyatt Regency, Booth # 508
Dallas, TX
Interested in receiving a **complimentary IDUG exhibits pass** from
Guardium? Contact Peg O'Donnell at peg.odonnell@guardium.com.

[IANS - New York Metro Information Security Forum](#)

May 20 - 21, 2008
Roosevelt Hotel
NY, NY

[Gartner IT Security Summit](#)

June 2 - 4, 2008
Gaylord National Resort
Landover, MD

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

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.