



Guardium eNews: September 2008

CONTENTS

- Learn How Dell Simplified Database Security for SOX, PCI, SAS 70
- Guardium Integrates with CEF and Achieves ArcSight Certification
- 5 Steps for Stopping the Insider Threat (*Wall Street & Technology*)
- Prevent Privileged Users from Accessing Sensitive Data (*SQL Server Magazine*)
- Princeton Review Data Exposed Due to Configuration Flaw (*InformationWeek*)
- Guardium CTO Interviewed on Data Security Trends (*Business News Americas*)
- Two Enterprise Security Platforms to Protect Corporate Data (*Network World*)
- Upcoming Events

Learn How Dell IT Simplified Database Security for SOX, PCI, SAS 70

[Download](#) a published case study to learn how Dell's IT group replaced its homegrown scripts and native database auditing with Guardium's automated, cross-DBMS, appliance-based platform - resulting in streamlined compliance and a significant reduction in auditing overhead.

Dell rapidly deployed Guardium to 300+ DBMS servers - in 10 datacenters worldwide - with plans to expand to 700+ additional servers in the next phase.

[Download here](#)

[Register for Webcast: October 22, 2008 at 2:00pm EDT](#)

Guardium Integrates with CEF and Achieves ArcSight Certification

Integration with the ArcSight SIEM Platform Provides Enterprises with Clear Visibility into Internal and External Database Threats

Guardium and ArcSight, Inc. (NASDAQ: ARST) announced that Guardium has been certified for integration under the ArcSight EnterpriseView Partner Program, delivering the next generation of business risk monitoring solutions.

Guardium's built-in support for CEF (Common Event Format) enables customers to seamlessly integrate with the award-winning ArcSight SIEM Platform to provide a business-level dashboard view of who is accessing their critical enterprise data and how that data is being used. The combination of Guardium and ArcSight technology allows enterprises to better understand their users, data and applications at a deep level to minimize risk, promote proper governance and reduce compliance costs.

[Click here to read news release](#)

5 Steps for Stopping the Insider Threat

Melanie Rodier, *Wall Street & Technology*

Guardium's Phil Neray offers guidance on preventing insider data theft.

The threat of insider fraud appears to be increasing. Insider data theft accounted for nearly 16 percent of all data breaches in 2008, up from 6 percent a year earlier, according to a study by the Identity Theft Resource Center. And perhaps more alarming, customer data stolen by an employee is misused more frequently than data obtained through an external breach, a recent study by ID Analytics reveals.

Phil Neray, VP of database security company [Guardium](#), says there are two main reasons for the rise in the insider threat: Demand for sensitive corporate data has increased, and there is now a thriving black market where fraudsters can buy and sell this type of data.

"Also, most corporations have spent the last 10 years focusing on tighter controls around the perimeter of networks," Neray adds. "It's getting harder to break into firms from the outside in traditional hacking attacks, so the bad guys are focusing on how to use insiders to get to the data."

[Click here to read article](#)

Prevent Privileged Users from Accessing Sensitive Data

Megan Bearly, *SQL Server Magazine*

With SQL injection attacks and data thefts happening more and more frequently, many companies are looking for a solution that not only provides database activity monitoring and alerting functionality, but also preventative control over who can access data. Recently, I spoke with Phil Neray, Guardium's vice president of strategy, about [Guardium 7.0](#) and [S-GATE](#), which provide granular control over data access.

According to Neray, this product provides a practical way to enforce data access policies. Guardium 7.0 also includes vulnerability assessment functionality that monitors for various vulnerabilities and threats. Guardium 7.0 even monitors encrypted data. In addition, this product ships with more than 100 preconfigured best practice reports for SOX and PCI compliance.

S-GATE lets you block privileged users, such as DBAs, from accessing sensitive data, without having to worry about whether you're blocking legitimate access as well. This product includes real-time preventative controls, continuous access policy enforcement, and fine-grained auditing.

[Click here to read article](#)

Princeton Review Data Exposed Due to Configuration Flaw

Thomas Claburn, *InformationWeek*

One file reportedly contained information about 34,000 students and another contained names and birth dates of 74,000 students.

The Princeton Review, an educational testing company, inadvertently exposed the personal data and test scores of tens of thousands of Florida students on its Web site, according to [a report](#) in The New York Times.

According to The New York Times, a Web site configuration flaw made hundreds of files on the Princeton Review's Web site accessible over the Internet. One file reportedly contained information about 34,000 students and another contained names and birth dates of 74,000 students.

Such breaches are not uncommon: There were [446 publicly reported breaches in the U.S. in 2007](#) and some experts suggest that as few as 5% of breaches get publicly reported.

According to Phil Neray, vice-president of marketing at Guardium, the problem lies in management. "Boards of directors and management teams have not made [data protection] a priority in many, many companies," he said. "The reason why this has to come from the top is that in many cases you're asking business units to change bad business practices. And you need budgets [to invest in database protection]."

[Click here to read article](#)

Guardium CTO Interviewed on Data Security Trends

Cristina Molina, *Business News Americas*

Companies are showing increased interest in having several layers of security to protect information.

And as the information is mainly located in databases, the opportunities in for companies such as Guardium are constantly increasing.

High ranking executives from Guardium were recently invited to a security seminar that took place in Santiago, Chile, organized by Chilean IT security solutions provider Neosecure. BNamericas spoke with Guardium's CTO and VP Ron Bennatan:

"There are a lot of places where you can invest in security, and one thing that people try to solve is leakage of data. There are many more issues regarding direct access to the repository, direct access to the database. So we are saying "the data sits inside the database, how do we guarantee there is no unauthorized access?" And even when it leaves the database on a pen drive or in an email it started inside the database, so the question is how did they get into somebody's desktop so that they could put it on an email? Today the hardest problem is direct access to the database and new regulations are looking at how to control the data inside the database itself... It is all about making it easier, more practical, and making it cost less."

[Click here to read article](#)

Two Enterprise Security Platforms to Protect Corporate Data

Linda Musthaler, *Network World*

"It's the data, stupid." OK, the phrase is not quite catchy enough to become a must-have bumper sticker, but it's a mantra for every organization with sensitive information. Today's article looks at two enterprise security platforms designed to protect corporate data. Guardium focuses on securing the data and actions involving databases, and Symantec's Vontu platform provides data loss prevention (Compare Data Leak Protection products) on the network, at the endpoint, and in storage devices.

[Guardium's](#) technology platform (also called Guardium) safeguards databases and enterprise applications. It uses policy-based controls and anomaly detection to prevent unauthorized activities by potential hackers, privileged insiders, and end users of enterprise databases and applications such as Oracle EBS, PeopleSoft and SAP. All user activities are monitored, including those by privileged users, application users, DBAs accessing databases directly, remote developers, and even batch processes.

[Click here to read article](#)

UPCOMING EVENTS

Please visit us at the following upcoming events:

Accenture Technology Consulting Workshops

Business Partner Fair

September 23 - 24, 2008 - London, UK

September 30 - October 1, 2008 - Rome, Italy

Presentations will be given by Ron Bennatan, CTO

Topic: Protecting Your Most Critical Assets - Data

September 24th - Infrastructure Security Track (London, UK)

September 30th - Infrastructure Security Track (Rome, Italy)

IDUG Europe

October 13 - 16, 2008

Hilton Warsaw

Warsaw, Poland

See Guardium in the NEON Enterprise Software stand.

ComputerLinks University

October 14, 2008

Oslo, Norway

McAfee FOCUS 2008

October 20-23, 2008

MGM Grand Las Vegas

Las Vegas, NV

Guardium is a [founding member of the McAfee Security Innovation Alliance.](#)

Guardium Webcast cosponsored by BMC

Learn How Dell IT Simplified Database Security for SOX, PCI, SAS 70
October 22, 2008
2:00pm EDT
45-minute online presentation

IBM Information on Demand

October 26 - 31, 2008
Mandalay Bay Resort & Convention Center (Booth #11)
Las Vegas, NV

*Guardium is a member of IBM's Data Governance Council and has achieved **Advanced Industry-Optimized status for the Financial Markets industry**, within IBM's PartnerWorld Industry Networks.*

2008 ISSA SoCal Security Symposium

October 30, 2008
Renaissance Long Beach Hotel
Long Beach, CA

InfoSecurity Netherlands

November 12-13, 2008
Jaarbeurs Utrecht - Halls 8 & 9 (Stand #A048)
The Netherlands

CSI - Computer Security Institute 2008

November 15-21, 2008
Gaylord National Resort Hotel (Booth #623)
Washington, D.C.

Infosecurity et Storage Expo 2008

November 19 - 20, 2008
Le Salon de la Sécurité Informatique (Booth #B30)
Porte de Versailles
Paris, France

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](#)
[Database Leak Prevention](#)
[Lab Reviews, Case Studies & White Papers](#)
[Mainframe Visibility](#)
[Media Coverage & Upcoming Events](#)

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

Guardium is a trademark of Guardium. All other trademarks and service marks are the property of their respective owners.