Guardium
SAFEGUARDING DATABASES™

Guardium Protects Corporate Databases Against Identity Theft

Network Appliance Prevents Unauthorized Access
From Both Inside and Outside the Firewall

WALTHAM, MA , February 7, 2006 – Guardium, Inc., the database security company, today introduced its Data Privacy Accelerator, the first database-centric solution for preventing identity theft, including unauthorized access by 'trusted' insiders.

The solution will debut at RSA 2006, Booth 2206 next week in San Jose, CA.

The Guardium Data Privacy Accelerator™ builds upon the Guardium SQL Guard™ platform, the most widely used network solution for database security and auditing. Leading companies in a broad range of industries - including financial services, telecommunications, retail, media, energy, manufacturing and pharmaceuticals - rely on Guardium to monitor and prevent unauthorized access to their most valuable information, which can include credit card and Social Security numbers as well as corporate financial information. Guardium's family of network appliances supports all leading enterprise databases, anywhere on the network.

"Massive identify theft is most companies' biggest nightmare, even if they're too afraid to say these words out loud," said Ram Metser, president and chief executive officer, Guardium. "Databases are rich and under-protected targets. They hold all the confidential customer and employee information you absolutely can't afford to have breached."

The Guardium Data Privacy Accelerator delivers a portfolio of pre-configured policies, real-time alerts, and audit reports that are specifically tailored to the challenges of identify theft, based on industry best practices. For example, the system automatically generates real-time alerts whenever anomalous database activity is detected, such as a high volume of requests for first and last names in combination with credit card or bank account numbers. Requests can also be blocked when sensitive information is accessed in unexpected ways, such as after-hours queries or access from unapproved applications.

An interactive visual access map provides high-level network views of all database users, applications and servers, with zoom-in detail showing exactly which information is being accessed and which database commands are being executed. In almost every company, this initial insight prompts immediate security changes. In many cases, employees are unwittingly violating corporate policies or creating security loopholes.

$5 Million Mistake?
A typical data theft can easily cost companies millions or tens of millions of dollars. An even bigger potential cost is the subsequent brand erosion, and loss of shareholder value.

"Protecting customer data is much less expensive than dealing with a security breach in which records are exposed and potentially misused," writes Avivah Litan, research vice president, Gartner, Inc.

According to Gartner's September 2005 report entitled, "Management Update: Data Protection is Less Costly Than Data Breaches," companies spend "an expenditure of at least $90 per account when data is compromised or exposed during a breach." This translates to a bottom-line hit of almost $5 million for a company with only 50,000 exposed accounts.

Because most corporate databases are linked to multiple critical business applications - such as Oracle Financials, SAP, or Siebel - any compromise can also undermine performance and security across the network, potentially affecting the core business.

Compliance Accelerates Best Practices
Many IT professionals are now discovering that regulatory requirements are accelerating implementation of best practices for information security and change management. This delivers a major additional benefit: driving new efficiency in IT operations.
The Guardium Data Privacy Accelerator provides several capabilities that simplify labor-intensive compliance and change control processes, making it easier to meet auditors' requirements:

- Creating detailed audit trails whenever suspicious events are detected, documenting the complete "who, what, when, and how" of database access. This critical documentation is stored in a tamper-proof data vault for future investigation and "digital forensics."

- Automating audit workflows for ensuring that appropriate personnel automatically regularly receive audit reports and approve them before forwarding to the next level of approval. This approach clearly documents that a management oversight process has been implemented and is being followed.

- Customizable compliance reporting and alerting, including a powerful set of query tools for "mining" all of the information about SQL traffic captured by the SQL Guard system.

Add-on modules are also available for implementing specific regulations such as Sarbanes-Oxley (SOX), the Payment Card Industry (PCI) Data Security Standard, and Basel II. The SQL Guard family supports Oracle, Microsoft, IBM, and Sybase database environments.

About Guardium
Guardium, Inc., the database security company, develops the most widely-used network solution for database security and auditing. By securing sensitive information - such as credit card data, personal identity information, and corporate financial data - Guardium protects the world's best-known brands while minimizing the cost and complexity of IT governance and compliance.

Named "Hot Pick" by Information Security magazine, Guardium's family of network appliances monitor and prevent unauthorized access in real-time - without the performance loss or insider security risk of traditional logging solutions. A centralized multi-tier architecture provides scalability for large and distributed enterprises.

Guardium's partners include IBM, EMC, HP, Microsoft, Oracle and Sybase, and the company is a member of IBM's prestigious Data Governance Council. For more information, please visit www.guardium.com or call 781-487-9400.

Press Contacts:
Corinne Sheen or Adam Parken
Corporate Ink
617-969-9192
csheehan@corporateink.com or aparken@corporateink.com