Bring Database Activity into Compliance

Guardium's Non-Invasive Approach to Real-Time Database Monitoring and Security

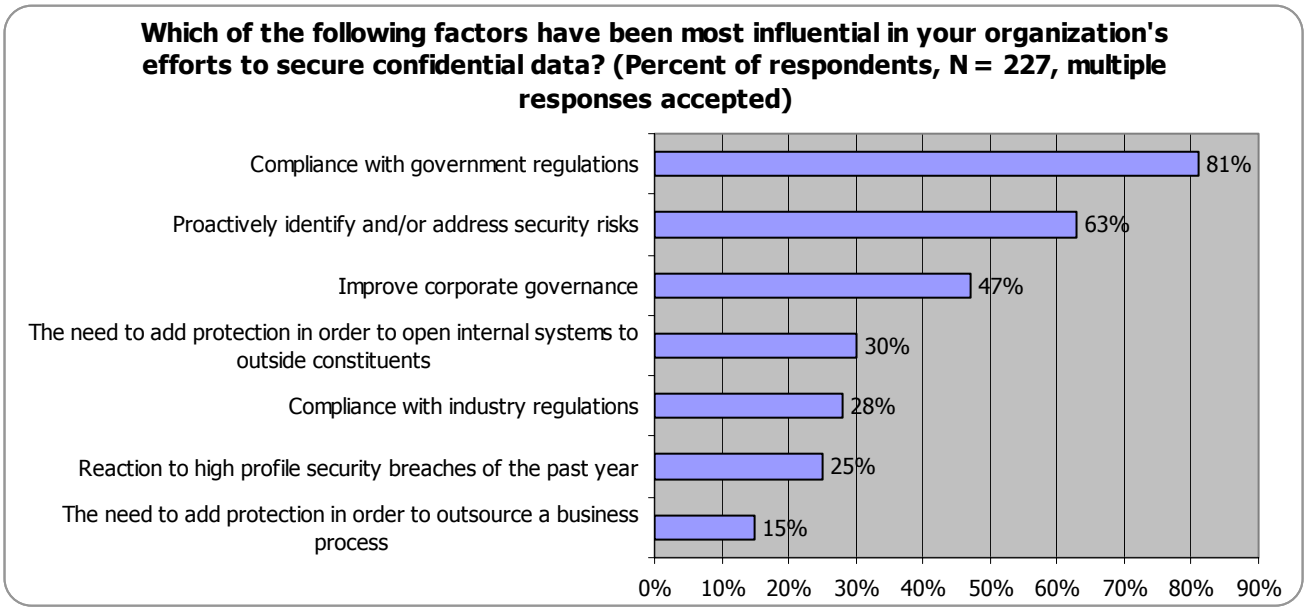
By Eric Ogren
Security Analyst, Enterprise Strategy Group

July 2006

Executive Summary

Compliance with government regulations dominates the priorities of enterprise security managers to secure confidential data. It is no longer enough to keep evil intrusions from outside the firewall away from the business, database security teams also have the mandate to protect the enterprise against inadvertent leakage of critical data, and to audit all database activity in order to assure that critical business applications such as Oracle Financials, SAP, and PeopleSoft are effectively secured. This prioritization on protecting against data theft, shown in Figure 1, is reflected by the influence on IT security plans of compliance with government regulations including Sarbanes-Oxley, Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard, and CA 1386.

Figure 1
Compliance dominates enterprise security agendas
Source: Enterprise Strategy Group, 2006



Guardium's technology inspects SQL transactions to audit database activity and protect against intrusions for the organization's most sensitive applications. The network appliance approach allows corporations to quickly meet compliance requirements for handling confidential information in databases without impacting deployed applications. In particular, Guardium's customers use the solution to control access to sensitive databases, detect patterns of abuse by privileged users, enforce corporate change control policies, and completely audit activity affecting sensitive information in database systems.

This special report, commissioned by Guardium, examines a comprehensive approach to securing confidential data and auditing database activity for compliance with government regulations and corporate security policies. The purpose is to provide information and make recommendations for database security to assure true compliance and business continuity. Information in this report derives from Enterprise Strategy Group research and interviews with security executives of global operations.

Auditing Confidential Database Activity

Security teams are deploying solutions to meet the requirements of government regulations for activity audit and assessment of database security policies. The specialized expertise of intelligent inspection of SQL queries and responses is a central element of an effective enterprise security program for sensitive information retained in databases. While there are many features to drive product comparisons, business requirements include:

- **Do not place business application delivery at risk.** Security issues are irrelevant if the database security product cannot satisfy corporate business requirements. Auditing of database activity for confidential data must not adversely impact application performance, integrity or reliability. A security solution that impedes the company's ability to conduct business, or is prohibitively labor-intensive to administer, will not be successfully deployed.

- **Continuously audit and assess database activity**. Government regulations, such as Sarbanes-Oxley, HIPAA, and PCI require constant vigilance to assure the integrity of confidential information. Database security teams are mandated to continuously audit database activity, and assess database security performance on a regular basis. The audited activity extends beyond simple update and delete operations that affect the integrity of the database, to also include read operations for possible data theft and tracking of schema changes for possible unauthorized changes by privileged users.

- **Segregate system management duties between security and operations teams.** Best practices require that oversight functions of audit and assessment of database transactions for compliance be managed by corporate security, while operations teams focus on delivering business services through applications. This establishes the checks and balances of independent auditing into the datacenter. Audit information should always be stored and managed in secure processes that are separate from operational procedures.

- **Efficiently manage large amounts of audit data.** Collection of transactions, especially database READ operations, can generate a large volume of data in each of the distributed datacenters. Government regulations specify retention of audited activity log files which is as long as five years for Sarbanes-Oxley and can be as long as two years more than the life of a patient for HIPAA. The database security solution must support IT data management practices, such as query tools for data mining and forensics, compression, and archiving to near-line and off-line storage devices.

- **Make database security intrinsic to application delivery.** Database monitoring and security solutions should also deliver value to application teams. Database security is uniquely positioned to inspect every transaction that goes into or out of the database. Look for ways to use this insight to improve the quality of service delivered to application end-users. For example, a high rate of logon or SQL errors may indicate a programming error in an application server that saps performance, or direct SQL calls from a new IP address may indicate that a new application is being used before the corporate help desk is ready to provide support. In addition, application users may be performing unauthorized transactions from within business applications, which can be detected by monitoring database activity and then correlating unusual or unauthorized activity to application user IDs.

- **Implement proactive security controls**: Implement policies and technologies that support immediate discovery and proactive response to security incidents and unauthorized changes, rather than "after-the-fact" responses that occur long after the incidents have occurred.

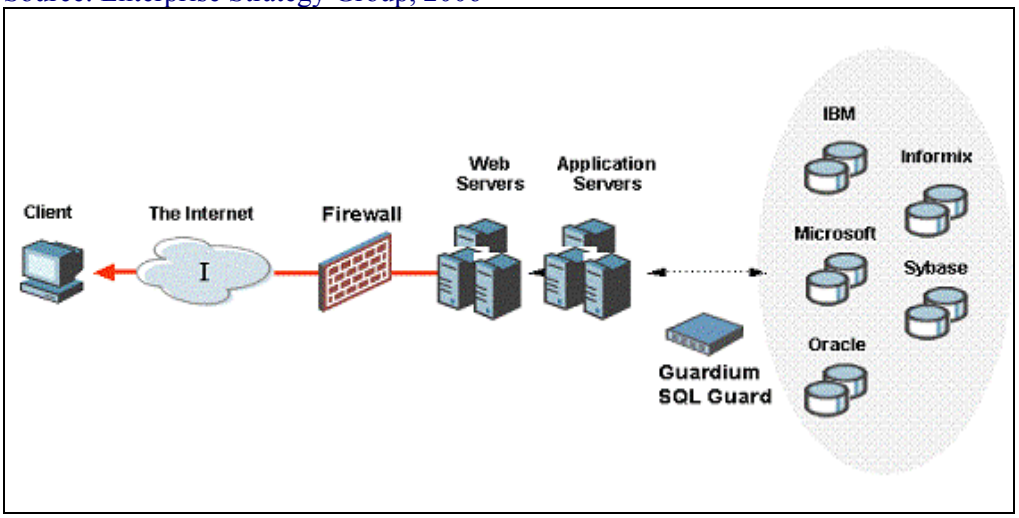
Guardium's Approach

Guardium's approach is to deploy a passive or inline network sniffing appliance in the datacenter where inbound and outbound SQL activity can be inspected and audited, as shown in Figure 2, for IBM, Microsoft, Oracle, Informix and Sybase databases. Software agents can optionally be installed on database servers in order to monitor local access such as from directly connected consoles or shared memory access.

The Guardium product line provides non-invasive database auditing of internal and external users as well as segregation of security duties from privileged users. Software modules plug into the administrative console to provide workflow automation for auditing and compliance reporting (AuditGuard), policy-based control such as real-time alerts and blocking (PolicyGuard), and graphical mapping of database access patterns and dashboard tracking of security metrics (HealthGuard).

Additional software modules help IT efficiently meet compliance requirements with pre-configured reports and policies for SOX, PCI, data privacy laws, and Basel II, based on industry best practices and COSA/COBIT guidelines. The company also supports auditing and security at the application level for Oracle EBS, and PeopleSoft. An API permits customers to extend coverage to other enterprise applications, which allows organizations to correlate end-user application IDs with database activities.

Figure 2
Guardium's Auditing and Protection
Source: Enterprise Strategy Group, 2006



Database security products that specialize in interpreting SQL commands and application behavior can be deployed as either appliances on network segments in front of the data center or as host software installed on corporate database servers. Database security appliances are deployed inline to filter malicious SQL traffic before it can reach the database, or are passively deployed on the network, operating on real-time copies of traffic to avoid placement on the SQL data path. There is no risk of increased transaction latency or interruption of traffic flow to the database. Consider database appliances for these characteristics:

- **Discover databases and traffic patterns.** Application teams are continually adding new instances of database servers, or adding new applications that access existing databases, according to business

requirements. Guardium's ability to simply detect when the application delivery profile has changed allows security and governance teams to proactively validate that configurations, schemas, access paths, and auditing capabilities all comply with corporate operating policies.

- **Audit and assess.** All SQL traffic touching sensitive data must be audited and assessed for compliance with security and data privacy policies. For example, the Payment Card Industry mandates in requirement number 10 that the compliant enterprise "implement automated audit trails to reconstruct the following events, for all system components: all individual user accesses to cardholder data". Guardium includes modules, such as for PCI and SOX, that assess audited traffic for compliance with government regulations and internal security policies. Automatically generated reports supply audit teams with up to date compliance profiles.

- **Prevent inappropriate access and SQL attacks in real-time.** The mainstay of any database security product is to protect the database against unauthorized or unusual access in real-time. The Guardium product line inspects SQL commands for unauthorized or malicious policy violations, notifying IT when instructions jeopardize database integrity and optionally blocking command execution when required. In addition, Guardium audits changes to the database schemas to ensure that privileged users follow critical change request procedures.

- **Scale to enterprise levels.** Protecting corporate database assets is an enterprise-wide job. Guardium's cross-platform, multi-tier architecture integrates with enterprise standards to support centralized, policy-based control and aggregation of audit data across:

    - Multiple database platforms from vendors including IBM (DB2 and Informix), Microsoft, Oracle, and Sybase (ASE and IQ).
    - Multiple physical locations such as distributed data centers, remote branch locations, and different business units.
    - Multiple requirements for complying with government regulations, primarily SOX, PCI, GLBA, Basel II, and state disclosure laws modeled after CA SB 1386.

The corporation's most critical assets reside in its databases. The database security challenge is to protect the database against attacks on its integrity, as well as to guard against suspicious behavior and faulty business processes that may lead to disclosure of sensitive information. Guardium's approach is to meet these requirements with a network appliance that provides leading-edge database monitoring and security in order to strengthen the security and compliance processes of enterprise applications.

Recommendations and Conclusions

Complying with government regulations to protect sensitive enterprise information starts with strong audit and protection processes in the data center. It is imperative that security officers apply database security best practices to their organization, and rely on detailed audit trails when investigating any breach of security policy. Other controls in a defense-in-depth strategy, such as encryption and identity management, are undermined if the security of the data center itself is weak.

- **Form a cross-functional Database Security Council with expert representatives from applications, databases, storage, security, and corporate audit.** Use trend and baseline activity data from database audit and assessment processes to communicate to executive management the corporation's ability to effectively protect sensitive data and to continuously meet regulatory requirements.

- **Gain awareness about your existing environment.** The first task of the Database Security Council is to use intelligence gained from a network inspection of SQL traffic to identify all existing access paths to sensitive data and database structures. Unauthorized or malicious activities are often discovered in the first hours of operation, typically leading to formal reminders to administrators, developers, outsourcers, and partners about corporate security policies, as well as changes to access and change control procedures. This awareness of the application environment can often be used to gain executive approval for additional capital expenditures for new database monitoring technology, especially when effectively presented in a business context and combined with justification related to requirements from both internal and external auditors.

- **Create automated and optimized processes to ensure continuous compliance and protection:** Practical, cost-effective technology now exists to implement automated controls and compliance monitoring for sensitive data – without massive increases in IT headcount or the need for external consultants or outsourcers. Implement compliance requirements for protecting sensitive data before embarking on other security deployments.

Enterprises have placed a clear priority on compliance with government regulations to assure the privacy of customer and employee information as well as the integrity of their corporate financial data. ESG believes that network-based, cross-platform appliances with rich software functionality, such as that offered by Guardium, have substantial advantages over manual or database-resident approaches in delivering enterprise-wide database monitoring and security that is non-invasive to previously deployed applications. ESG recommends that enterprises place Guardium on the shortlist when evaluating products for database monitoring, security and compliance.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. and was sponsored by Guardium. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. Copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482.0188.