HOW THE GUARDIUM PLATFORM HELPED DELL IT SIMPLIFY ENTERPRISE SECURITY

By Phil Neray
Addison Lawrence
David McMaster
Venugopal Nonavinakere

Safeguarding data is critical for many organizations, but auditing data access activity to comply with regulatory standards can be a complex undertaking. As part of its initiative to simplify IT, the Dell IT group implemented the Guardium platform and database activity monitoring technology to help protect its globally distributed database servers and streamline compliance processes.

Related Categories:

Best practices
Guardium
Microsoft SQL Server
Oracle
Regulatory compliance
SAP
Security

Visit DELL.COM/PowerSolutions for the complete category index.

Securely maintaining sensitive financial and customer information in enterprise data centers can be complex and challenging, and the heterogeneous global environment that stores enterprise data for Dell is no exception. The Dell IT infrastructure includes thousands of servers worldwide that run a diverse mix of enterprise applications such as Oracle® E-Business Suite, Oracle JD Edwards®, and Oracle Hyperion software as well as the Oracle Database and Microsoft® SQL Server® database platforms on both Microsoft Windows® and Linux® operating systems.

To add to this complexity, organizations typically must report and audit data access activity to comply with regulatory standards such as the Sarbanes-Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI-DSS), and Statement on Auditing Standards Number 70 (SAS 70). These detailed reports usually involve documenting the activities of everyone accessing these systems, including help-desk personnel, outsourcers, and privileged users such as database administrators (DBAs) and system administrators. In addition, an oversight team to review and approve these reports on a regular basis—instead of simply generating and stacking them on someone's desk—helps to ensure that a formal process is in place for tracking and addressing exceptions such as failed logins and unauthorized changes to database structures (schema modifications) through Data Definition Language (DDL) operations.[1]

Dell IT administrators are continually looking for new and innovative ways to safeguard critical data in these systems from both external and internal threats, including inadvertent or accidental changes that can affect the integrity of financial data governed by standards. The Dell IT group wanted to replace its manual, internally developed approaches—one for Oracle Database and one for Microsoft SQL Server—with an automated, cross-platform, appliance-based solution that could not only secure the privacy and integrity of critical data, but also streamline the process of reporting and auditing data access activity to comply with regulatory standards.

To help accomplish these goals, the Dell IT group implemented the Guardium platform and its database activity monitoring (DAM) solution, a real-time monitoring technology for safeguarding database data and automating compliance reporting and oversight processes. Dell deployed this automated, cross-platform solution for securing its enterprise

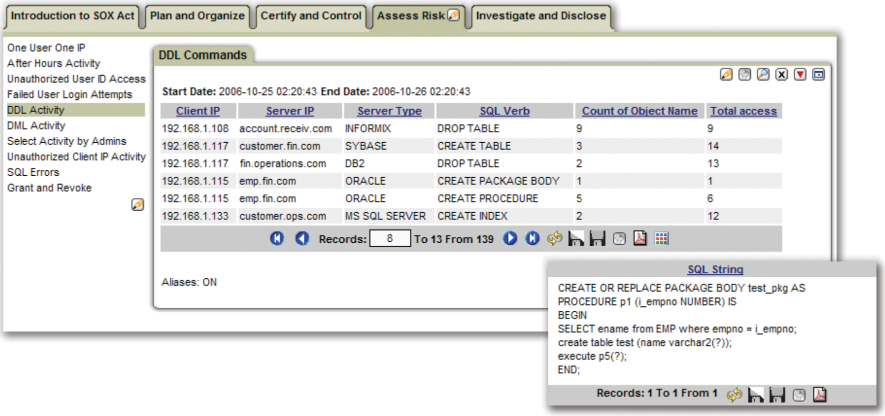
[1] These materials reflect Dell's view of compliance with the statutes and standards as of July 11, 2008, and may be superceded by changes in the statutes/standards. This information is not intended as legal advice and may not be used as such, nor does this information reflect a full and exhaustive explanation of all relevant statutes and standards. You should seek the advice of your own legal counsel on any legal compliance questions.

data centers to help establish a structured monitoring process for tracking changes and documenting database activity; monitoring all database activity—including privileged user activities—independently from native database logging and auditing features; and simplifying reporting for compliance with regulatory standards in its globally distributed systems.

UNDERSTANDING DATABASE SECURITY TECHNOLOGIES

Although traditional security technologies such as firewalls can be essential building blocks for a layered defense against security threats to enterprise data, they lack embedded knowledge about database protocols and structures and are therefore limited in key ways:

- **Perimeter defenses, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs):** Lack specific awareness of database protocols and activity patterns
- **Database encryption:** Does not protect against access to back-end databases by privileged users with access to keys or against hackers who hijack application servers; it can also require significant architectural changes to existing applications and databases
- **Data leak prevention:** Catches sensitive data leaving endpoints through e-mail or instant messages, but does not protect sensitive data at the source, in the data center
- **Native database management system (DBMS) logging utilities:** Do not provide real-time protection such as alerting or blocking, can create performance overhead, and do not support the separation of duties required by auditors because they are controlled by the same teams that need to be monitored
- **Security Information and Event Management (SIEM) systems:** Rely on imported DBMS log data, cannot detect unauthorized activities in real time, and lack database-focused analytics



Start Date: 2006-10-25 02:20:43 **End Date:** 2006-10-26 02:20:43

Client IP	Server IP	Server Type	SQL Verb	Count of Object Name	Total access
192.168.1.108	account.receiv.com	INFORMIX	DROP TABLE	9	9
192.168.1.117	customer.fin.com	SYBASE	CREATE TABLE	3	14
192.168.1.117	fin.operations.com	DB2	DROP TABLE	2	13
192.168.1.115	emp.fin.com	ORACLE	CREATE PACKAGE BODY	1	1
192.168.1.115	emp.fin.com	ORACLE	CREATE PROCEDURE	5	6
192.168.1.133	customer.ops.com	MS SQL SERVER	CREATE INDEX	2	12

Records: 8 To 13 From 139

Aliases: ON

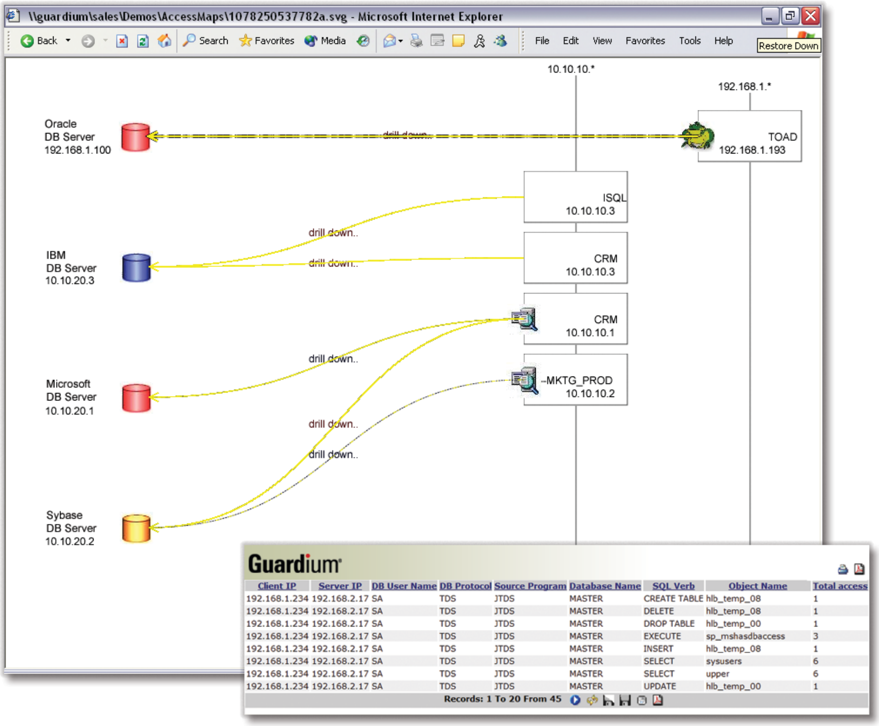
SQL String

```
CREATE OR REPLACE PACKAGE BODY test_pkg AS
PROCEDURE p1 (i_empno NUMBER) IS
BEGIN
SELECT ename from EMP where empno = i_empno;
create table test (name varchar2(?));
execute p5(?);
END;
```

Records: 1 To 1 From 1

Figure 1. *The Guardium platform provides over 100 preconfigured reports for regulatory standards compliance*

DAM technology—designed to monitor, analyze, and log transactions to a DBMS—provides an alternative to these traditional approaches to help provide increased security for databases. To help minimize performance overhead on production systems—which may process millions of transactions per day—DAM systems typically operate independently of native DBMS logging and auditing functions. Using an independent system for DAM is also important because of the formidable challenge of storing, analyzing, and archiving large volumes of captured audit information. DAM systems typically capture highly granular information about each transaction, including SQL command, database and OS account, date and time, originating IP address and server, source application, database name, network protocol, application account, and bind variable data (see Figures 1 and 2).



Client IP	Server IP	DB User Name	DB Protocol	Source Program	Database Name	SQL Verb	Object Name	Total access
192.168.1.234	192.168.2.17	SA	TDS	JTDS	MASTER	CREATE TABLE	hlb_temp_08	1
192.168.1.234	192.168.2.17	SA	TDS	JTDS	MASTER	DELETE	hlb_temp_08	1
192.168.1.234	192.168.2.17	SA	TDS	JTDS	MASTER	DROP TABLE	hlb_temp_00	1
192.168.1.234	192.168.2.17	SA	TDS	JTDS	MASTER	EXECUTE	sp_mshasdbaccess	3
192.168.1.234	192.168.2.17	SA	TDS	JTDS	MASTER	INSERT	hlb_temp_08	1
192.168.1.234	192.168.2.17	SA	TDS	JTDS	MASTER	SELECT	sysusers	6
192.168.1.234	192.168.2.17	SA	TDS	JTDS	MASTER	SELECT	upper	6
192.168.1.234	192.168.2.17	SA	TDS	JTDS	MASTER	UPDATE	hlb_temp_00	1

Records: 1 To 20 From 45

Figure 2. *The Guardium platform monitors all database transactions at a granular level and provides a visual access map showing databases, clients and applications*

In addition, keeping DAM separate from native DBMS logging functions helps demonstrate *separation of duties*—sometimes called segregation of duties—which can be crucial for internal control. In this context, separation of duties means that the DAM system creates and stores an audit trail without relying on components in the DBMS infrastructure, which could be subject to tampering by privileged users. To help ensure independent accountability, DAM administrators should be security professionals or auditors rather than members of the privileged user group being monitored.

EVALUATING THE GUARDIUM ARCHITECTURE

The Guardium architecture offers a noninvasive, network-based, database-independent platform for continuously monitoring and analyzing database traffic in real time to help immediately identify unauthorized or suspicious activities, both at the network level and on database servers. Built on 2U Dell™ PowerEdge™ 2950 servers, each system runs a suite of real-time monitoring, security, and compliance applications on a hardened Linux kernel. Multiple appliances can be combined in a multi-tier topology to handle high-transaction volumes and/or distributed environments.

Transactions are stored securely in the appliance in an embedded high-performance database for regulatory standards compliance reporting, auditing, correlation analysis, and forensics. To support separation of duties and provide a verifiable audit trail, audit information cannot be modified by anyone—even privileged users. The Guardium platform provides additional security measures, including real-time security alerts through Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP), custom actions such as automated account lockouts, and blocking. IT organizations can monitor database traffic by using one or a combination of noninvasive methods:

> **“The Guardium architecture offers a noninvasive, network-based, database-independent platform for continuously monitoring and analyzing database traffic in real time to help immediately identify unauthorized or suspicious activities.”**

- **Software taps (S-TAPs):** S-TAPs are lightweight software probes installed on each database server to monitor database traffic at the OS level. Because S-TAPs do not rely on the database to collect or process the log data, impact on database performance is generally minimal (typically 2–4 percent). Instead, they simply relay database traffic to separate Guardium appliances in the network for analysis and storage. S-TAPs can also collect traffic from database servers in remote locations to help eliminate the need for dedicated appliances in isolated locations. S-TAPs are important because they also monitor local backdoor access to databases by privileged users through non-TCP protocols such as shared memory, named pipes, and Bequeath, an Oracle Net Services protocol. Finally, a specialized version of S-TAP, called S-GATE, can be used to selectively block unauthorized transactions by privileged users, such as viewing of sensitive data—thereby helping enforce separation of duties and adding a new layer of preventive controls without the risk of blocking legitimate access from authorized users and applications.
- **Switched Port Analyzer (SPAN) port or hardware tap:** In this configuration, the Guardium appliance is deployed as a non-in-line, passive network monitor that captures a mirrored copy of the network stream by connecting to a standard SPAN port in a network switch, or to an in-line network tap, with zero performance impact on database servers.

To help maximize flexibility, organizations can use a combination of host-based and network-based collection, depending on their network topology and relative ease of access to database servers and/or network switches.

DEFINING DELL REQUIREMENTS FOR DATABASE ACTIVITY MONITORING

In early 2007, a cross-organizational team from Dell Global Data Services and Dell Global Information Security Services defined its requirements for a DAM solution. The Dell team needed a scalable, secure, and reliable way to audit sensitive, highly restricted data such as credit card and social security numbers. At the time, Dell was using internally developed scripts with native database auditing for Oracle databases, and a combination of scripts and a third-party tool for Microsoft SQL Server databases.

Although the existing approaches met immediate auditing needs, keeping the scripts properly deployed and the jobs running resulted in supportability issues and added complexity to the environment. Databases that were reporting correctly one day would stop reporting audit data on another day, causing frustration for project teams because the DBAs were in strong demand for delivering business projects—and were instead required to perform repeated maintenance to correct auditing problems. In one case, the Oracle SYSTEM tablespace filled with log files,

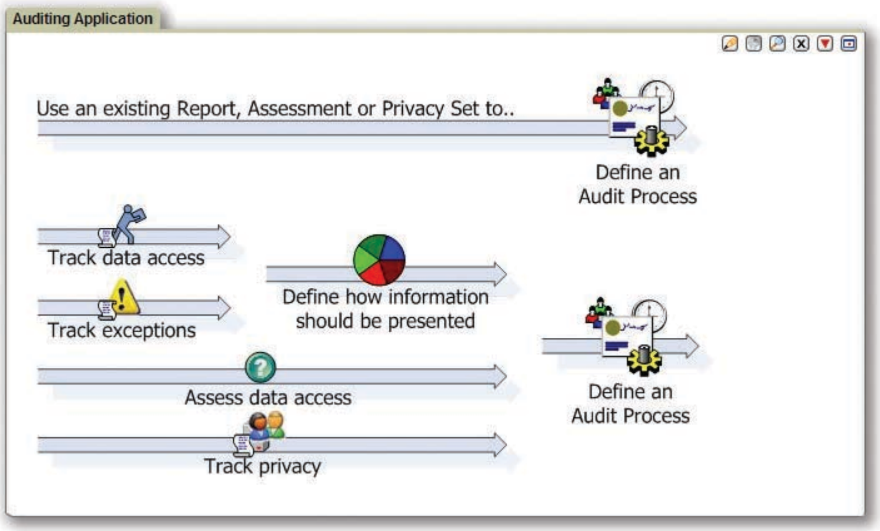


Figure 3. *The Guardium platform helps security professionals and auditors automate regulatory standards compliance, including sign-offs and escalations*

causing a database outage and increasing frustration even further.

Administrators reviewing audit logs also struggled to keep up with the volume of data generated because no data filtering was available, and they labored to document closure to every action item they found when reviewing the audit log. Additional problems were found in the controls for the audit logs because the DBAs were responsible for both installing and maintaining the audit processes.

To help meet its growing business needs, the Dell project team looked for a solution that could provide out-of-the-box auditing for multiple database platforms, including Oracle Database and Microsoft SQL Server. The solution needed to make minimal overhead demands on the database server, provide automated evidence for passing audit requirements (see Figure 3), and be deployable without DBA expertise and without changes to the databases. The audit data reporting needed to be able to compare the audit data to change tickets that were approved in the Dell change-management system and to provide filtering to suppress logging of database changes that were made through authorized applications. Showing that DDL commands such as `DROP TABLE` are logged and checked to ensure appropriate management approval is important for SOX regulations, and reviewing inquiries on credit card and social security numbers—for example, through ad hoc `SELECT` commands—is critical to the requirements of PCI-DSS and privacy standards.

Dell also required real-time alerting for critical security events, such as brute-force password attacks (flagged by repeated failed logins) and SQL injection (flagged by repeated references to nonexistent table names). Finally, the data in the audit log needed to be protected from manipulation by privileged users such as the DBAs.

The team needed to meet all of these requirements within three months on some of the critical databases in the Dell IT environment, including databases supporting 24/7 manufacturing and the DELL.COM Web site. These databases include complex configurations for high availability using Oracle Real Application Clusters (RAC) and Microsoft SQL Server clusters, and complex configurations for disaster recovery using Oracle Data Guard and Microsoft SQL Server database mirroring.

IMPLEMENTING GUARDIUM IN THE GLOBAL DELL ENVIRONMENT

In late 2007, Dell deployed the Guardium platform to approximately 300 database servers in 10 data centers around the world during a 12-week period. In enterprise environments like the Dell implementation, multiple appliances can be deployed in a federated system with a scalable, multi-tier topology consisting of the following components (see Figure 4):

- **Centralized management server:** Automatically aggregates and normalizes audit information from multiple systems and locations into a single

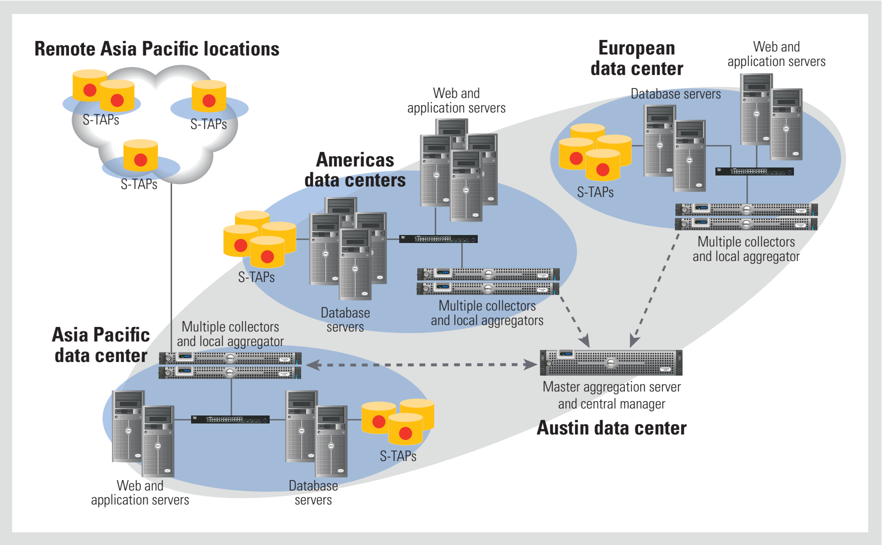

Remote Asia Pacific locations
S-TAPs
S-TAPs
S-TAPs
European data center
Web and application servers
Database servers
S-TAPs
Multiple collectors and local aggregator
Web and application servers
Americas data centers
S-TAPs
Database servers
Multiple collectors and local aggregators
Asia Pacific data center
Multiple collectors and local aggregator
Master aggregation server and central manager
Austin data center
Web and application servers
Database servers
S-TAPs

Figure 4. *The scalable Guardium architecture supports a multi-tier topology for centralized aggregation of audit data and management of security policies*

repository for enterprise-wide regulatory standards compliance reporting, correlation, and forensics

- **Graphical Web console:** Provides centralized management of policies, report definitions, compliance workflow processes, and server settings
- **Role-based administration:** Restricts access to specific appliances, modules, policies, and audit data based on organizational roles
- **Efficient architecture for storing audit data:** Uses patent-pending, intelligent storage algorithms that provide significantly better storage efficiency than traditional flat file–based approaches
- **Lightweight Directory Access Protocol (LDAP) integration:** Supports auto-population and maintenance of groups based on existing enterprise-wide directory services

Because of its highly distributed environment, Dell implemented the Guardium architecture using a four-tier topology in which S-TAPs gather database traffic from each database server, collector appliances receive audit data from multiple S-TAPs, central aggregators in the major geographical areas receive data from multiple collectors, and a Web-based central management console in Austin provides enterprise-wide, centralized policy and appliance management.

The deployment of the Guardium platform successfully met the requirements established by Dell without causing an outage to any of its databases, and produced a significant reduction in auditing overhead in databases. The project team configured Guardium to automatically retrieve a list of table names containing highly restricted data from the Dell Data Classification tool. The Guardium architecture allows DBAs to identify and analyze previously unknown activity on the databases, such as application errors, database time-outs, and legacy scripts causing login failures. The team also implemented closed-loop change control by integrating the Guardium platform with Dell's BMC Remedy change-management system; this integration enables Dell personnel to review reports and alerts comparing all observed database changes from the Guardium system with approved change requests from the change-management system.

In the next phase of the implementation, Dell plans to deploy the Guardium platform to 725 additional database servers. Dell anticipates that this expansion will enable auditing on all databases classified as critical to essential business functions. Dell also plans functionality expansion, including the deployment of additional Guardium modules such as the Change Auditing System (CAS) module, which monitors changes to external database configuration files and environment variables that can impact security posture. Dell also plans to deploy Guardium's Vulnerability Assessment module, which provides security vulnerability and configuration assessment reporting for databases. Finally, Dell plans to deploy specialized Guardium modules for monitoring end users that interact with the database through enterprise applications such as the Oracle e-Business Suite, which use shared "service accounts" to access the database.

SECURING SENSITIVE ENTERPRISE DATA

For many enterprises, practical solutions that address the complexity and challenges of securing databases and complying with regulatory standards are critical to success. Like other organizations with globally distributed IT infrastructures, Dell needed a more scalable, secure, and reliable system than traditional security technologies and manual approaches could provide to help secure and audit access to sensitive, highly restricted data. The Guardium platform provides a comprehensive DAM system that enabled Dell to rapidly deploy and integrate it with its existing infrastructure to help enforce change controls, restrict access to sensitive data, provide automated and centralized controls for regulatory standards compliance, mitigate the risk of Web-based attacks, detect fraud, and automatically locate and classify sensitive data.

Phil Neray is vice president of marketing for Guardium and has more than 20 years of technology experience. He was previously senior director of worldwide strategic marketing for the Symantec Application and Infrastructure Management business unit, and started his career as a field operations engineer with Schlumberger working on remote oil rigs in South America. He has a Bachelor of Electrical Engineering (Honors) degree from McGill University, where he graduated with distinction.

Addison Lawrence is a security consultant for Dell Global Information Security Services, and has worked at Dell for 8 years. He has a B.S. in Computer Science from Texas A&M University–Corpus Christi and an M.B.A. from Texas A&M University.

David McMaster is a database administrator in the Dell IT Global Data Management Services organization. He has a bachelor's degree from the University of Kansas.

Venugopal Nonavinakere is a program manager handling database security projects for the Global Database Management Services organization. He has a bachelor's degree in Mechanical Engineering from Bangalore University.

MORE ONLINE
DELL.COM/PowerSolutions

QUICK LINK

Guardium:
www.guardium.com