

NIST 800-53 Accelerator

Automated Real-Time Controls to Protect Against Cyberattacks & Insider Threats

Highlights

Full suite of database security applications:

- Automate & simplify NIST 800-53 controls with preconfigured policies, reports & assessments
- Address FISMA, FISCAM, OMB, NIST, DIACAP & HIPAA policy requirements
- Real-time database monitoring and alerting to immediately identify unauthorized activities
- Continuous fine-grained auditing
- Cross-database audit repository with secure audit trail & separation of duties
- Vulnerability & configuration assessment to identify unpatched and misconfigured systems
- Change Audit System (CAS) to prevent unauthorized changes to database structures, data values, privileges and configurations
- Real-time prevention (blocking)
- Granular access controls
- Data discovery
- Compliance workflow automation (electronic sign-offs, escalations, comments, etc.)
- Data mining for forensics
- Long-term log retention
- Integration with existing infrastructures: LDAP/AD, change management (e.g., BMC Remedy), SIEM (e.g., ArcSight CEF), RSA SecurID, Kerberos, etc.
- Centralized cross-database policy management via Web console
- Monitor all privileged user activities including local access (SSH console, shared memory, BEQ, TLI, etc.)
- Identify fraud via multi-tier, connection-pooled applications (PeopleSoft, SAP, Cognos, etc.), without modifying applications.
- Prevent SQL injection attacks with baselining and policy-based anomaly detection
- Supports all major database platforms including Oracle, SQL Server, DB2, Informix, Sybase, MySQL, Teradata
- Supports all major COTS applications including Oracle EBS, PeopleSoft, Siebel, JDE, Business Objects, Cognos plus custom applications.

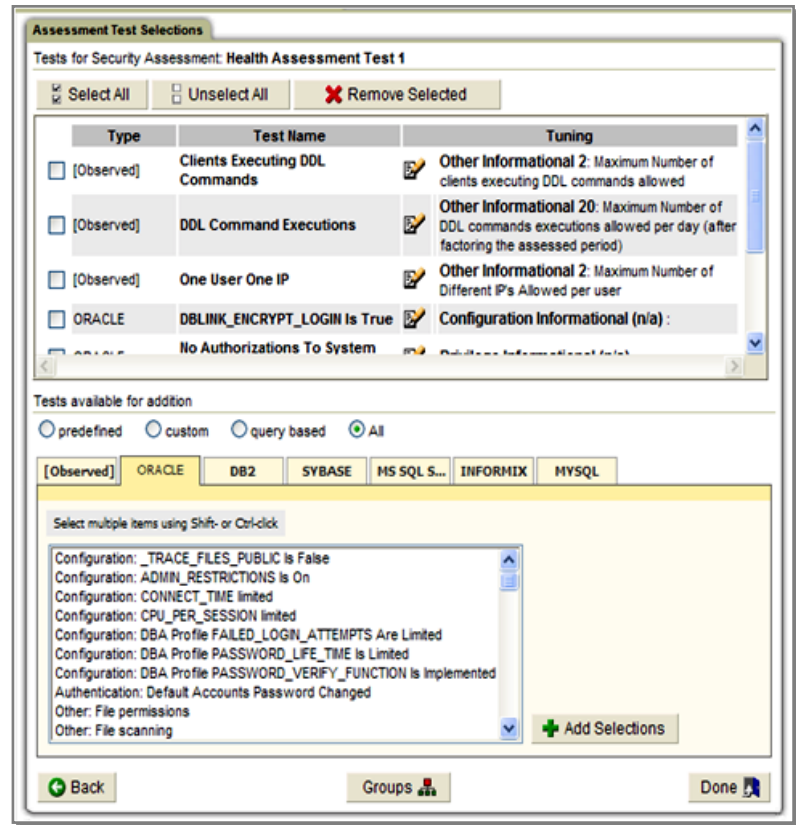


Figure 1: *Guardium provides a full suite of database security applications for automating and simplifying NIST 800-53 compliance across your entire database and application infrastructure. Major functionality components include real-time database monitoring with policy-based alerts and blocking, fine-grained auditing, data discovery and vulnerability management. Guardium provides hundreds of preconfigured reports and policies along with a library of vulnerability tests, based on best practices, developed by DISA.*

Overview

Protecting against cyberattacks such as SQL injection, breaches, fraud and insider threats has heightened the need for federal agencies and contractors to carefully review their security programs against the FISMA-mandated NIST 800-53 standard and comply with OMB M-06-16, in order to secure PII and other sensitive data such as financial data and classified information.

Guardium provides the most widely-used solution for preventing information leaks from the data center and ensuring the integrity of critical data.

Guardium 7 automates security operations and optimizes operational efficiency with a scalable, multi-tier architecture that automates and centralizes compliance controls across your entire application and database infrastructure – without impacting performance or requiring changes to applications or database.

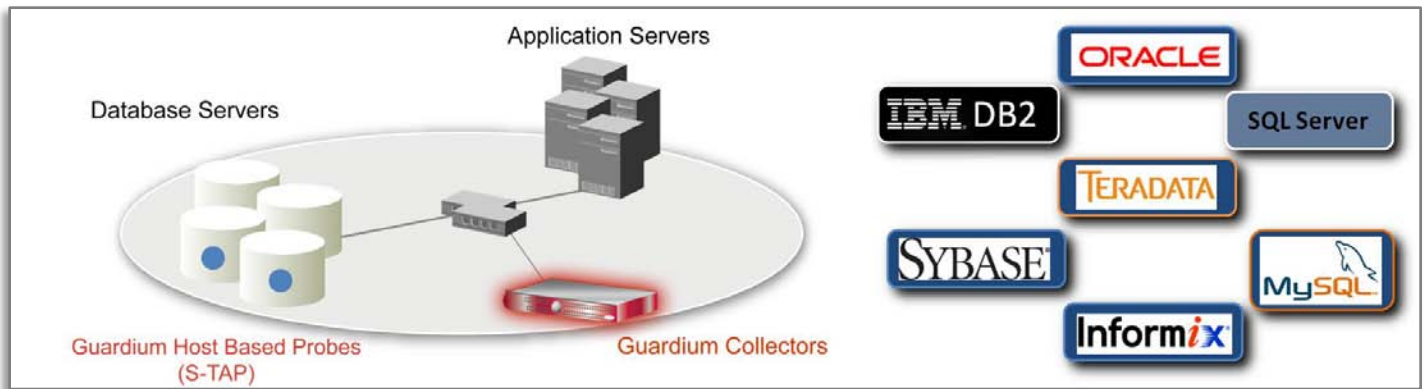


Figure 2: Non-Invasive Monitoring & Auditing: Unlike native log-based approaches, Guardium provides a non-invasive, cross-DBMS architecture that captures 100% of all database activities in real-time – including all privileged user actions, SELECTs and end-user IDs for pooled connections – without impacting performance or requiring changes to database or applications. S-TAPs are lightweight, host-based probes that monitor all database traffic at the OS level, including local access by privileged users, and relay it to Guardium collector appliances for analysis, data mining and reporting. Collector appliances gather monitored data from S-TAPs and Z-TAPs (mainframe-resident probes) and/or by connecting directly to SPAN ports in network switches.

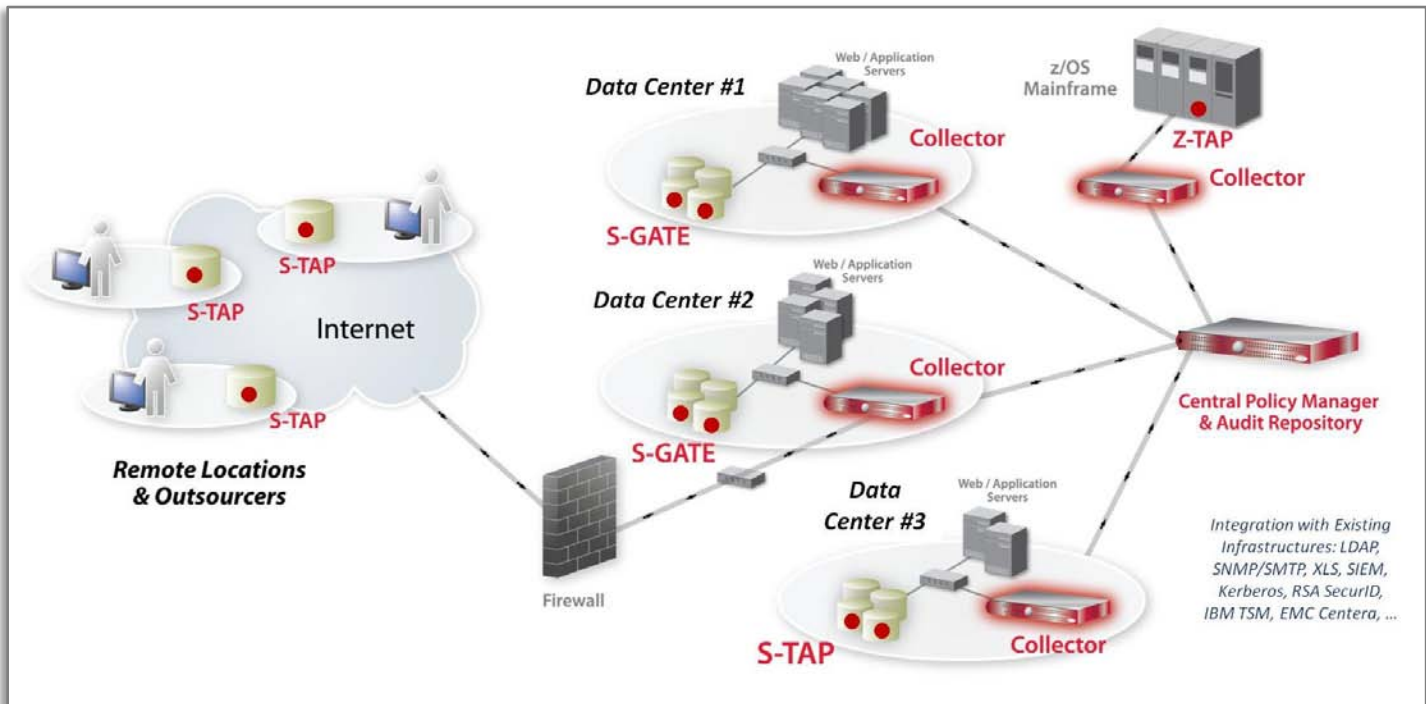


Figure 3: Scalable Multi-Tier Architecture: Guardium's scalable architecture supports both large and small environments, with centralized aggregation and normalization of audit data, and centralized management of security policies and appliance configurations via a Web console – enterprise-wide. Simply add collectors or adjust filtering parameters to support increased transaction volume and/or audit granularity. Aggregators automatically aggregate audit data from multiple collector appliances. For maximum scalability and flexibility, multiple tiers of aggregators can also be configured.

Table 1: Certification and Accreditation – NIST SP 800-53 Security Controls Support

Control ID	Control Name	High Baseline	Feature / Implementation Note
AC-02	ACCOUNT MANAGEMENT	AC-2 (1) (2) (3) (4)	Support for control enhancements #2, #3, and 4.
AC-03	ACCESS ENFORCEMENT	AC-3 (1)	S-GATE or S-TAP
AC-04	INFORMATION FLOW ENFORCEMENT	AC-4	Guardium 7 with S-TAP
AC-05	SEPARATION OF DUTIES	AC-5	Guardium 7 enables organization to efficiently implement separation duties. Also enforces separation of duties through blocking access to records based on policy.
AC-06	LEAST PRIVILEGE	AC-6	Guardium 7 can implement additional security controls over and above the database to meet policy and operational requirements. Guardium 7 can provide entitlement reports showing all user accounts and access privileges
AC-07	UNSUCCESSFUL LOGIN ATTEMPTS	AC-7	Failed login attempts are monitored and policies can be established to lock-out accounts after specified thresholds are reached.
AC-10	CONCURRENT SESSION CONTROL	AC-10	Today: Detect and alert. Future: Limit based on policy.
AC-11	SESSION LOCK	AC-11	For access to Guardium system.
AC-12	SESSION TERMINATION	AC-12 (1)	System can alert and perform custom action to terminate the session.
AC-13	SUPERVISION AND REVIEW - ACCESS CONTROL	AC-13 (1)	Can monitor, report and use workflow to automate review. Integrates with ArcSight, Remedy, RSA Envision, McAfee ePO, others.
AC-17	REMOTE ACCESS	AC-17 (1) (2) (3) (4)	Control Enhancement #4 only for database admin functions.
AU-01	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	AU-1	Organization can facilitate and implement database audit policy and procedures through Guardium suite
AU-02	AUDITABLE EVENTS	AU-2 (1) (2) (3)	Guardium supports the base requirement and all enhancements for database auditing.
AU-03	CONTENT OF AUDIT RECORDS	AU-3 (1) (2)	Extensive granularity with ability to track end-points and end-user accounts when accessing through shared or pooled middleware.
AU-04	AUDIT STORAGE CAPACITY	AU-4	Guardium available in storage capacities to meet operational requirements
AU-05	AUDIT PROCESSING	AU-5 (1) (2)	Server: Monitor system, database capacity, log space. S-TAP: Monitor and alert when down. Guardium system: Monitors itself and alerts. Alert via email, console (SNMP, SMTP). Can be fed to SIEM (e.g., ArcSight). Monitor server space & native audit via scripts.
AU-06	AUDIT MONITORING, ANALYSIS, AND REPORTING	AU-6 (1) (2)	For supported database: Oracle, SQL Server, IBM database2 & Informix, Sybase, MySQL, Teradata.
AU-07	AUDIT REDUCTION AND REPORT GENERATION	AU-7 (1)	System retains audit data, read-only on source, but variety of ways to view and reduce.

Control ID	Control Name	High Baseline	Feature / Implementation Note
AU-08	TIME STAMPS	AU-8 (1)	Synchronize with NTP services. Span all database for central log with single timestamp overcoming devices which are not synchronized.
AU-09	PROTECTION OF AUDIT INFORMATION	AU-9	Hardened Linux platform with no root access.
AU-11	AUDIT RETENTION	AU-11	Enterprise database auditing with interfaces to standard archiving solutions including IBM TSM, EMC Centera, NAS, etc.
CA-02	SECURITY ASSESSMENTS	CA-2	Comprehensive vulnerability assessment module.
CA-03	INFORMATION SYSTEM CONNECTIONS	CA-3	S-GATE can be used to prevent access from unauthorized systems and networks.
CA-07	CONTINUOUS MONITORING	CA-7	Can monitor / assess technical controls within Guardium scope.
CM-02	BASELINE CONFIGURATION	CM-2 (1) (2)	Inventory: Database, configuration, binaries, stored procedures, functions, tables, users, etc.
CM-03	CONFIGURATION CHANGE CONTROL	CM-3 (1)	Integrates with change management systems (e.g., Remedy). Detects changes and can check for authorized changes.
CM-04	MONITORING CONFIGURATION CHANGES	CM-4	Detect database configuration changes, audit, alert and report.
CM-05	ACCESS RESTRICTIONS FOR CHANGE	CM-5 (1)	Audit and enforce at database level
CM-06	CONFIGURATION SETTINGS	CM-6 (1)	Database security configuration assessments and monitoring based on DISA STIGS, NIST and CIS Benchmark.
CP-07	ALTERNATE PROCESSING SITES	CP-7 (1) (2) (3) (4)	Product supports cold, warm and hot site failover configuration and operations with multiple sites, nodes and database.
CP-09	INFORMATION SYSTEM BACKUP	CP-9 (1) (2) (3) (4)	Backup must use FIPS 140-2 validated product/module
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	CP-10 (1)	Guardium can be used to compare known good state to reconstructed system to detect any variances.
IA-05	AUTHENTICATOR MANAGEMENT	IA-5	Can do strong passwords today and associated password requirements.
IR-04	INCIDENT HANDLING	IR-4 (1)	Real-time incident detection at database level which can be used for analysis and response.
IR-05	INCIDENT MONITORING	IR-5 (1)	Real-time detection and monitoring of threats mitigating the risk of Web-based attacks with real-time identification of suspicious behavior and execution of preventative actions.
IR-06	INCIDENT REPORTING	IR-6 (1)	Extensive reporting features which can be used to support incident reporting.
IR-07	INCIDENT RESPONSE ASSISTANCE	IR-7 (1)	Can be configured to send incidents based on type and organizational structure.
RA-05	VULNERABILITY SCANNING	RA-5 (1) (2)	Guardium performs vulnerability and patch scanning on database servers.

Control ID	Control Name	High Baseline	Feature / Implementation Note
SA-11	DEVELOPER SECURITY TESTING	SA-11	Can be used to test and monitor development versions of database.
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	SC-17	Guardium plugs into customer PKI.
SI-04	INTRUSION DETECTION TOOLS AND TECHNIQUES	SI-4 (2) (4) (5)	Provides support for control and all HIGH enhancements as it pertains to database.
SI-06	SECURITY FUNCTIONALITY VERIFICATION	SI-6	Hardened Linux OS with no root access.
SI-07	SOFTWARE AND INFORMATION INTEGRITY	SI-7 (1) (2)	Monitors critical files on database servers.
SI-09	INFORMATION INPUT RESTRICTIONS	SI-9	Supports variety of granular control on input.
SI-10	INFORMATION INPUT ACCURACY, COMPLETENESS, AND VALIDITY	SI-10	Can detect certain input out of range or outside threshold values and then block. (<u>Not</u> a replacement for dynamic application vulnerability testing.)

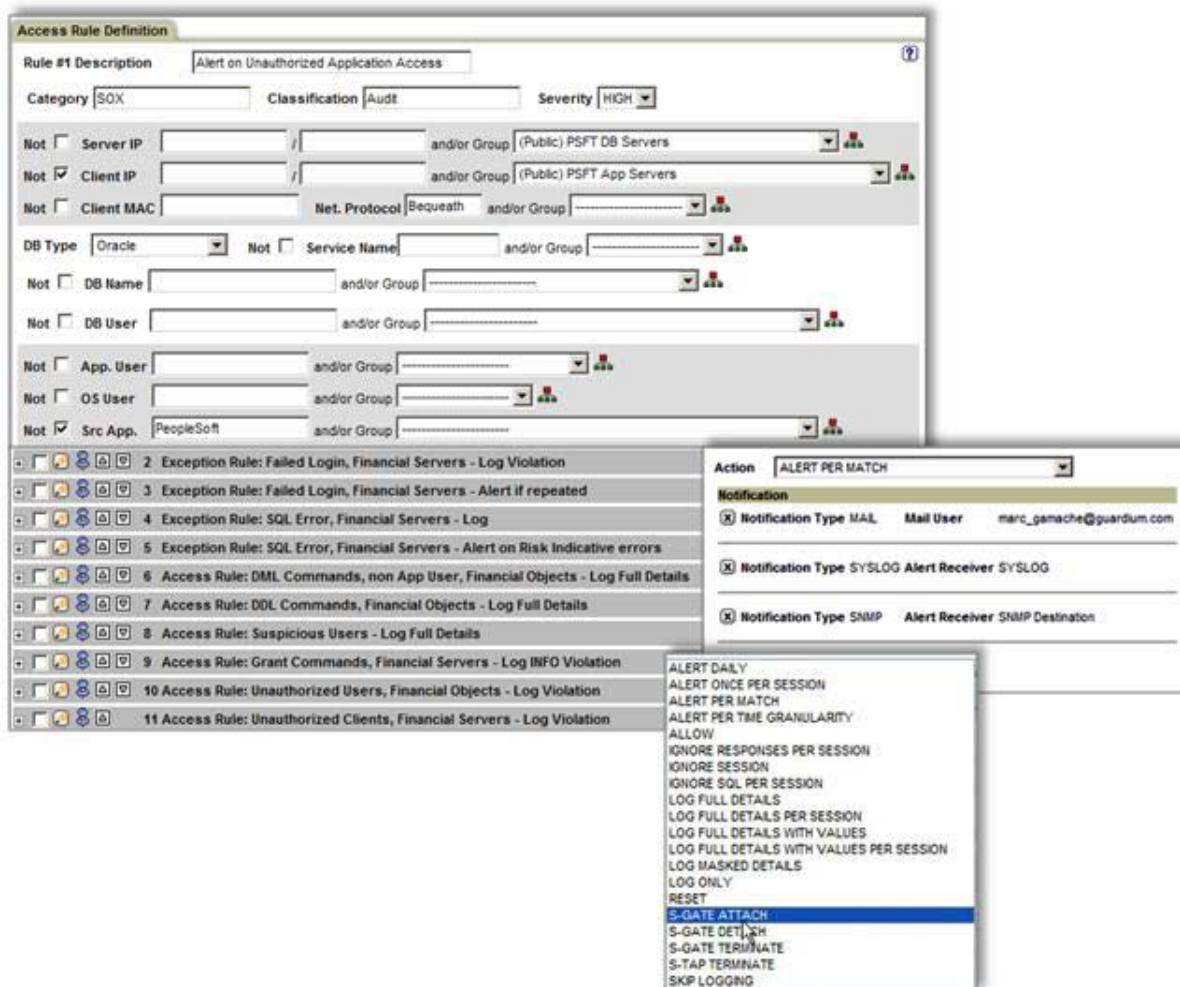
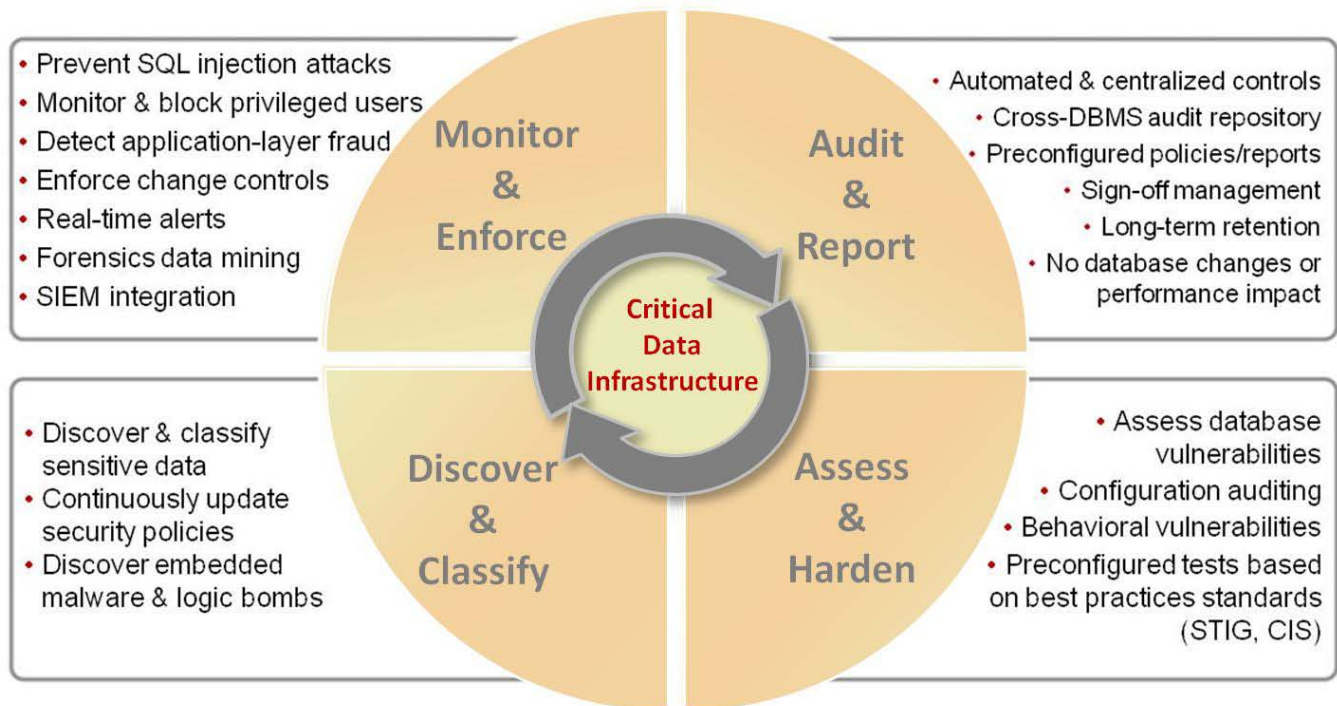


Figure 4: Granular Policies. *Guardium provides granular, preconfigured policies and reports to rapidly identify suspicious or unauthorized activities such as access via unauthorized applications or multiple failed logins. A range of actions, such as real-time SNMP alerts, can be configured to occur when policy rules are violated.*



About the Guardium Platform

Guardium's real-time database security and monitoring solution monitors all access to sensitive data, across all major database platforms and applications, without impacting performance or requiring changes to database or applications.

The solution prevents unauthorized or suspicious activities by privileged insiders, potential hackers, and end-users of enterprise applications such as Oracle EBS, PeopleSoft, Siebel, JD Edwards, SAP, Business Intelligence and in-house systems. Additional modules are available for performing database vulnerability assessments, change and configuration auditing, data-level access control and blocking, data discovery and classification, and compliance workflow automation.

Forrester Research recently named Guardium "a Leader across the board," with "dominance and momentum on its side." Guardium earned the highest overall scores for Architecture, Current Offering and Corporate Strategy ("The Forrester Wave: Enterprise Database Auditing And Real-Time Protection, Q4 2007" by Noel Yuhanna, October 2007).

About Guardium

Guardium, the database security company, delivers the most widely-used solution for ensuring the integrity of enterprise information and preventing information leaks from the data center. Founded in 2002, Guardium was the first company to address the core data security gap by delivering a scalable enterprise platform that both protects database in real-time and automates the entire compliance auditing process.

The company's enterprise security platform is now installed in more than 450 data centers worldwide, including top government agencies; 3 of the top 4 global banks; 3 of the top 5 insurers; 2 of the top 3 global retailers; 15 of the world's top telcos; 2 of the world's favorite beverage brands; the most recognized name in PCs; a top 3 auto maker; a top 3 aerospace company; and a leading supplier of business intelligence software.

For more information, please contact your Guardium partner, Regional Sales Manager or visit www.guardium.com.

Guardium®
SAFEGUARDING DATABASES™