

# PCI Accelerator

## How Guardium Helps Secure Your Data and Meet PCI DSS Requirements

The screenshot shows the Guardium PCI Accelerator interface. At the top, there are tabs for 'Sarbanes-Oxley Accelerator', 'PCI Accelerator', 'Data Privacy Accelerator', and 'Basel II Accelerator'. Below these are sub-tabs for 'Overview', 'Req 3 Protect', 'Req 6 Maintain', 'Req 7 Restrict', 'Req 8 Assign', 'PCI Req 10 Track & Monitor', 'PCI Req 11 Ongoing Validation', and 'PCI Policy Monitoring'. The main content area is titled 'PCI - Access to Cardholder Data' and displays a table of database access logs. The table has columns for Database Name, Server Type, DB User Name, Server IP, OS User, Client IP, SQL Verb, Count of Object Name, and Total access.

Database Name	Server Type	DB User Name	Server IP	OS User	Client IP	SQL Verb	Count of Object Name	Total access
CUSTOMER_DATA	ORACLE	TMOORE	192.168.200.108	ROOT	192.168.20.107	REVOKE	7	30
CUSTOMER_DATA	ORACLE	TMOORE	192.168.200.108	ROOT	192.168.20.107	SELECT	9	118
CUSTOMER_DATA	ORACLE	TMOORE	192.168.200.108	ROOT	192.168.20.178	DATABASE	2	37
CUSTOMER_DATA	ORACLE	TMOORE	192.168.200.108	ROOT	192.168.20.178	GRANT	9	40
CUSTOMER_DATA	ORACLE	TMOORE	192.168.200.108	ROOT	192.168.20.178	SELECT	2	19
CUSTOMER_DATA	ORACLE	BHENRY	192.168.200.108	ROOT	192.168.20.107	DATABASE	2	26
CUSTOMER_DATA	ORACLE	BHENRY	192.168.200.108	ROOT	192.168.20.107	SELECT	5	16
CARD_PROCESSING	ORACLE	BENJI	192.168.200.108	ROOT	192.168.20.178	DATABASE	1	1
CARD_PROCESSING	ORACLE	TMOORE	192.168.200.108	ROOT	192.168.20.107	DATABASE	2	4
CARD_PROCESSING	ORACLE	TMOORE	192.168.200.108	ROOT	192.168.20.107	SELECT	1	2
CARD_PROCESSING	ORACLE	TMOORE	192.168.200.108	ROOT	192.168.20.178	CREATE TABLE	1	1
CARD HOLDER_DATA	MS SQL SERVER	ALAMO	192.168.200.109	LAMO	192.168.20.107	SELECT	2	4
CARD HOLDER_DATA	MS SQL SERVER	ALAMO	192.168.200.109	LAMO	192.168.20.107	USE	2	4
CARD HOLDER_DATA	SYBASE	LMETAXOTOS	192.168.200.108	ROOT	192.168.20.119	EXECUTE	1	41

### Highlights

- Provides customizable PCI DSS specific reports, policies, tools, and workflow automation which accelerate compliance and simplify validation with a broad range of Requirements.
- Automatically discovers and provides categorization of all instances of sensitive data like credit card numbers.
- Monitors returned data for sensitive patterns such as Track 2.
- Implements granular access controls for sensitive data, including restricting access by user, address and application.
- Protects cardholder data against external Web attacks and insider breaches with policy-based alerts and comparisons to normal baseline activity.
- Creates a secure, detailed, verifiable audit trail of all database activities, including those of privileged users.
- Increases operational efficiency through automation of the entire compliance reporting cycle across all systems, applications and DBMSs; including report generation, distribution, issue escalation and sign-offs.
- Provides automated assessment<sup>1</sup> of database vulnerabilities and environmental configuration risks<sup>2</sup>; providing real-time tools, metrics and recommendations for proactive improvement of security lifecycle, for both PCI non-PCI DSS environments.

**Figure 1:** The PCI Accelerator module used in conjunction with core Guardium product capabilities provides a comprehensive solution to comply with a broad range of PCI DSS requirements. Among its capabilities, the module provides a complete audit trail of all data access, part of a simple, powerful solution for meeting Requirement 10. Policy violations, such as access to other users' accounts, or inappropriate cardholder data access can be easily uncovered and remedied.

### Burgeoning PCI DSS Requirements

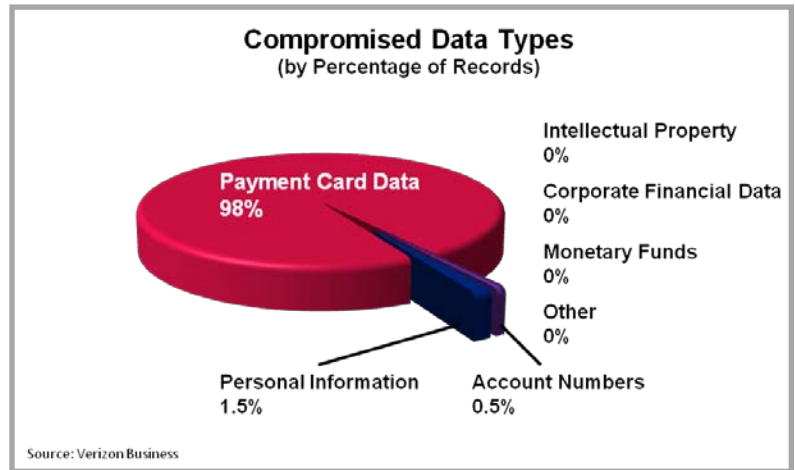
Payment card use is widespread today. Along with growing global use, the industry has experienced a troubling increase in incidents of financial fraud. In response, the leading payment card companies worked together to develop a set of technical and operational requirements designed to protect cardholder data, commonly referred to as PCI DSS (Payment Card Industry Data Security Standard).

Recent high profile data thefts, along with industry statistics, indicate significant work remains to be done in most organizations to implement PCI DSS. As shown in Figure 2, in its 2009 Data Breach Investigation Report of 150 global organizations which experienced breaches, Verizon's Business Risk Team found that 98% of records compromised involved payment card data. "While other types of data are sought by certain groups (i.e. competitors may target IP), the vast majority of cybercriminals are looking for a quick and easy payoff. Payment cards certainly fit the bill." Investigations also showed that 95% of the organizations attacked which were subject to PCI DSS were NOT compliant with Requirement 10.

Given the higher transaction fees and heavy fines levied for PCI DSS violations, combined with the potential costs of breach remediation and brand damage, many organizations are now seeking means of implementing PCI DSS faster, more effectively and more efficiently.

## Database Security and Auditing Provides a Simple, Cost Effective Means of Securing Cardholder Data

Most organizations subject to PCI DSS are currently relying on various forms of log management to try to achieve compliance with the monitoring and auditing aspects of the Standard. Logging at the detailed level required to achieve compliance imposes a severe performance penalty on systems, while requiring substantial technical resources on an on-going basis to collect and analyze the logs. Security Information and Event Management (SIEM) or centralized logging systems can help with aggregation, but lack the detailed data views or analytical tools to address the needs of the payment card industry. Additional deficiencies in the logging approach include the fact that it does not deal with the substantial issue of insider threats, or provide the separation of duties (SOD) required by auditors. These issues, combined with the results cited above clearly indicate the logging approach is inadequate.



**Figure 2:** Verizon's 2009 Data Breach study found that the vast majority of records compromised in 150 breached organizations involved Payment Card Data and that on average the breached organizations were only roughly 5% compliant with PCI DSS Requirement 10.

Guardium is the only solution available that can:

- Automatically locate (see Figure 4) and classify sensitive information, such as cardholder data.
- Assess database vulnerabilities and configuration flaws.
- Provide 100% visibility at a granular level into all database transactions involving sensitive data.
- Monitor and enforce a wide range of policies such as restricting sensitive data access, privileged user actions and database change control.
- Create a single secure centralized audit repository across large numbers of heterogeneous systems and databases.
- Automate the entire compliance auditing process, including creating and distributing reports as well as capturing comments and signatures.

## The PCI Accelerator Provides a Rapid Path to Compliance

Guardium provides a comprehensive solution that addresses database security and auditing needs across the enterprise; securing all kinds of sensitive data such as financial statements, personnel records and intellectual property. The PCI Accelerator is an optional software module designed to harness the capabilities of the core Guardium product in order to address the specific requirements of PCI DSS. Out-of-the-box reports and policies (see Figure 3) accelerate your ability to comply with PCI by providing a base upon which you can build, either by customizing the Accelerator, or complementing it with custom reports and policies. The PCI Accelerator's capabilities, along with interfaces to a variety of tools in the underlying system are organized in a tabular fashion (see Figure 4) by Requirement, making the product fast to implement and easy to use.

PCI Accelerator Overview		
Reports		Tools
Cardholder Server Report	One User One IP Report	Workflow Review Group Tool
Cardholder Database Report	Admin User Login Graph	Audit Process Tool for Exception, Data Access and Vulnerability Reviews
Cardholder Sensitive Objects Report	Open Sessions By IP Report	Data Access Map
Database Clients to Servers Map	Unauthorized Application Access Report	Change Auditing Targets and Results <sup>2</sup>
PCI Active Database Users Report	Cardholder Data Root/Admin Activity Report	Vulnerability Assessment Targets, Results and Audit Process <sup>1</sup>
PCI Database Administrators Report	Audit Trail Access Report	Data Access Baseline Policy Builder
PCI Authorized Source Programs Activity Report	Audit Trail Invalid Access Report	
Cardholder Data User Activity Report	Audit Trail Archive Log	
Failed Login Users Report	Policy Description Report	
Policy Violation Chart	Policy Violation Report	
Terminated Users Report	Large Data Extrusion Report	

**Figure 3:** The PCI Accelerator helps companies accelerate DSS compliance by organizing targeted reports and interfaces to relevant tools by Requirement.

## Automatic Discovery and Real-Time Monitoring: Protecting Data Begins With Knowing Where It Is

The key goal of PCI DSS is to ensure protection of cardholder data, as called out in Requirement 3. One of the first challenges in meeting this objective is to ensure all such data is identified and categorized. This is difficult in large distributed organizations with numerous distinct systems. Verizon has found that overlooked or forgotten assets are involved in a high percentage of breaches, as indicated in Figure 5. Guardium provides an easy way to meet this challenge. The core product includes an engine that crawls all databases looking for specified patterns such as 16 digit credit card numbers and 9 digit social security numbers. An alarm may optionally be generated the first time sensitive data is discovered, enabling investigation of the need for storage of that particular item, as called out in Requirement 3.

Once sensitive objects have been located, they are automatically tagged with meta-data classifications such as "Privacy-Restricted" or "Payment Card Data" and added to groups of items with similar properties. This ensures that appropriate policies are automatically applied to groups of objects with similar properties. In addition, executing the classifier process on a scheduled basis ensures that your policies are always up-to-date, even as developers change locations of sensitive objects.

Cardholder data protection mechanisms extend well beyond discovery. All movement of sensitive data such as CVV or PIN data can be identified, recorded, and flagged if it violates established policies, ensuring inappropriate duplication or access are immediately visible. Requirement 10 stipulates very granular data requirements for this type of monitoring, including identifying all users accessing the data (privileged and regular), invalid logical access events and so forth. Many companies find Requirement 10 particularly daunting, but with the PCI Accelerator, this level of monitoring is provided as a packaged solution (see Figure 1).

The PCI Accelerator provides a wealth of insight into sensitive data access by both regular and privileged users. This includes specific objects accessed, SQL verbs used, total accesses, date/time of access, user ID, client address, invalid logical access attempts, and more. All this data is stored in a single secure repository. Workflow automation tools are provided to ensure required actions are taken promptly, and a verifiable audit trail is maintained as required by Section 10.

### Strong Access Control Measures Are Easily Implemented

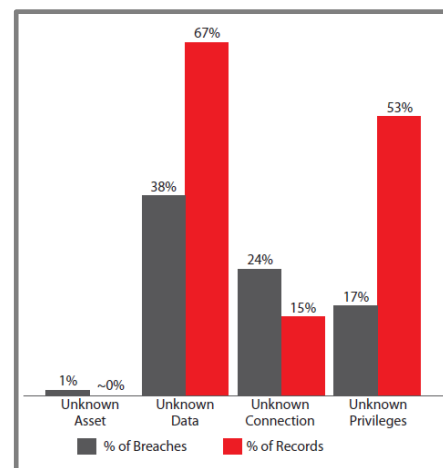
One of the best forms of sensitive data protection is, of course, to restrict access to those with a business need-to-know. This is precisely what PCI DSS Requirement 7 calls for. Guardium enables a variety of granular access controls to be placed on sensitive data; for instance specifying who can access it, from which applications, at which locations, at what times, using which commands. Guardium's ability to block unauthorized actions through the real-time prevention capabilities in its software agents and appliances maximizes protection of cardholder data, supporting the key goal of Requirement 7.

To ensure access policies based on User IDs are efficacious, ID use must be monitored for abuse, as spelled out in Requirement 8. Guardium supports this goal, by:

- Identifying who is sharing database IDs (see Figure 6), and when this is being done
- Monitoring the creation of new IDs and privilege escalation
- Restricting the use of special IDs such as privileged vendor IDs
- Alerting and restricting action based on failed login attempts
- Verifying that your password policies are being enforced

Object Name	Database Name	Server IP	Server Type	Total access
ssn	CUSTOMER_DATA	192.168.200.108	SYBASE	1
account_number	DEBIT_CARDS	192.168.200.108	DB2	1
address_1	DEBIT_CARDS	192.168.200.108	DB2	1
ssn	DEBIT_CARDS	192.168.200.108	DB2	1
creditcarddata	CREDIT_CARDS	192.168.200.108	ORACLE	1
address_1	CUSTOMERDB	192.168.200.110	MS SQL SERVER	1
full_names	CREDIT_CARDS	10.10.9.250	ORACLE	2
ssntable	SYSMASTER	192.168.200.108	INFORMIX	2
ssntable	CUSTOMER_DATA	192.168.200.109	MS SQL SERVER	2
address_1	CREDIT_CARDS	192.168.200.108	DB2	2
ssn	TEMPDB	192.168.200.108	SYBASE	2
address_1	DEBIT_CARDS	192.168.200.108	DB2	2
cc	CREDIT_CARDS	192.168.200.108	ORACLE	2
credit	CREDIT_CARDS	192.168.200.108	ORACLE	2
address_1	CREDIT_CARDS	192.168.200.108	ORACLE	3
address_1	CUSTOMER_DATA	192.168.200.110	MS SQL SERVER	4
track1	CREDIT_CARDS	10.10.9.250	ORACLE	5
track2	CREDIT_CARDS	10.10.9.250	ORACLE	6
ssn	CREDIT_CARDS	10.10.9.250	ORACLE	7
full_name	CREDIT_CARDS	10.10.9.250	ORACLE	8

**Figure 4:** PCI Accelerator tabs make the functions supporting each Requirement easily accessible. The Guardium solution automatically locates the systems and databases containing sensitive cardholder data, in support of Requirement 3.



**Figure 5:** For several years Verizon has found that overlooked or unknown assets were a factor in a significantly portion of data breaches (Source: 2009 Data Breach Report).

## Automate the Identification and Remediation of Security Risks

PCI DSS Requirement 2 (Do not use vendor-supplied passwords and security parameters), and 11 (Regularly test security systems and processes) are designed to ensure discovery of software vulnerabilities in your cardholder environment before hackers can exploit them. Guardium's Vulnerability Assessment (VA) option provides a low-touch means of meeting those requirements.

The VA module incorporates an extensive library of assessment tests, based on industry best practices, to flag missing patches, misconfigured privileges, default accounts, weak passwords and other static vulnerabilities. It also identifies dynamic or behavioral vulnerabilities—such as sharing of administration accounts and excessive administrator logins—by monitoring actual user activity over time. Finally, it includes embedded knowledge about enterprise applications such as Oracle EBS and SAP, to protect critical tables reserved for these applications. A quarterly subscription service ensures that assessment tests are always up to date.

DB User Name	Count of Client IP	Count of Sessions
39BMB1MGAMACHE	1	1
ASANDLER	1	1
ADMIN	1	1
APPLSYSUB	1	53
APPS	1	86
BENJI	2	9
BFEDER	1	1
BFEDERMAN	1	1
BFEDERMANN	2	67
CUSTOMAPP_POOLEDUSER	1	14
DB2ADMIN	1	2
DB2INST1	5	295
DBPOOLEDUSER	1	16
DSMTTH	6	83
JJAMES	2	9
GDEMODB2BFEDERMANN	1	1
GDEMODB2VLMETAXOTOS	1	3
GDEMODB2MGAMACHE	1	13
GDEMODB2WNSHAPIRA	1	6
GDEMODB2WNSHAPIRA	1	4

**Figure 6:** Guardium monitors the activities of all database users, including privileged users. Policies can be created to detect and block suspicious behavior. The PCI Accelerator reports inappropriate activity specifically called out by PCI DSS, including identifying the use of shared accounts (Requirement 8).

## Maintain Secure Systems by Automating Change Control Processes

Given the large number of databases in most enterprises, and the rates of changes in each, another significant challenge to be addressed according to PCI DSS is managing change control (Requirement 6: Maintain secure systems). Without change control, malware or harmful changes may be introduced into the data environment by outsiders or insiders, by accident or purposefully, causing leakage, corruption or the introduction of vulnerabilities.

The Guardium solution provides visibility into all changes to the database such as schema or value changes. The Change Auditing module provides similar capabilities for the database environment, tracking changes such as registry values, environmental variables and file ownership, as well as modifications to key files such as executables and scripts.

While such information is highly useful, Guardium simplifies the practical application of the data by correlating actual changes with authorized changes in existing change management systems such as Remedy®, using the Enterprise Data Connector module. The Guardium solution can flag which changes do not have tickets, or have invalid tickets, as well as presenting summaries of the actual commands performed compared to summary descriptions from the change order. These capabilities help secure your cardholder data by ensuring only authorized changes are made to the database environment.

**Audit Process Definition**

Description: Weekly PCI Review

Active:  There's a schedule associated with this process

Archive Results:  Keep for a minimum of 365 days or 0 runs

CSV/CEF File Label: Weekly\_PCI\_Review

**Receivers**

Receiver	Action Req.	To-Do List	Email Notif.	Cont.
<input checked="" type="checkbox"/> pci (pci pci)	<input type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> role: infosec	<input type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> role: dba	<input type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> audit (audit audit)	<input type="radio"/> Review <input type="radio"/> Sign	<input checked="" type="checkbox"/>	<input type="radio"/> No <input type="radio"/> Link <input type="radio"/> Full Results	<input checked="" type="checkbox"/>

**Audit Tasks**

- Report: Review Access To Cardholder Data [PCI Access to cardholder data] (NOW -1 week to NOW)
- Classification Process: Discover Cardholder Data [Weekly data classification process]
- Security Assessment: Weekly PCI Security Assessment [Detect xp\_cmdshell]
- Report: Failed Login Report [Failed Login Attempts] (now -1 week to now)

**Roles**

No roles have been assigned to this Process

Buttons: Back, Remove, Clone, Comment, Refresh, Save, Done

**Figure 7:** Guardium's incident management and workflow automation capabilities enable users to cost effectively identify, resolve and track incidents to comply with Requirement 12.

## Automated Reports and Workflow Improve Security and Streamline Audit Preparation

To secure your environment, and validate compliance with Requirement 12 (Maintain an Information Security Policy), it is necessary to ensure that processes are in place to identify, resolve and track incidents in a timely manner. With Guardium's incident management and Compliance Workflow Automation (see Figure 7), you can easily automate report generation, distribution, electronic sign-offs, commenting and escalation. These tools are key to efficiently securing and auditing the distributed heterogeneous environments typical of most payment card information systems.

Timestamp Date	Category Name	Access Rule Description	Client IP	Server IP	OS User	DB User Name	Full SQL String	Severity Description
2009-04-10	pqi	Alert on Failed Login	10.10.9.240	192.168.20.195	SYSTEM	Oracle		MED
2009-04-10	pqi	Alert on Failed Login	10.10.9.240	192.168.20.195	SYSTEM	DBSNMP		MED
2009-04-10	pqi	Unauthorized CreditCard Access	10.10.9.240	127.0.0.1	SNIKTIN	FINANCE	select * from creditcard Extrusion Values: *****-3451	HIGH

**Figure 8:** Policy violations and supporting detail can be automatically detected and dispatched for remediation through workflow automation.

## Guardium as a Compensating Control

For many organizations, one of the more difficult sections of the Standard can be 3.4, which calls for a mechanism to render sensitive data unreadable through encryption, hashes or other means. Implementation of this requirement can be difficult because of the significant impact on system performance, application software and processing throughput. PCI DSS allows for the use of alternate compensating controls if the primary requirement cannot be met due to technical constraints or business limitations. Depending upon your environment, Guardium may be appropriate to consider for this purpose due to its strong monitoring and access controls. These same capabilities can also play a role in segmenting your network to isolate the cardholder environment when reconfiguration with technologies like firewalls is impractical.

## Single Solution Addressing a Wide Range of PCI DSS Requirements

Although PCI DSS places a heavy focus on assessment, monitoring and control of the cardholder data environment, it also details requirements for things like firewalls (Requirement 1), virus protection (Requirement 5) and physical access control, which are the domains of other providers. However, unlike other products which focus on satisfying a narrow set of PCI DSS requirements, Guardium provides users with a single solution which addresses a broad range of Requirements, including 2, 3, 6, 7, 8, 10, 11 and 12.

Req.	Summary Description	Guardium PCI DSS Capabilities
<b>2</b>	<b>Do not use vendor defaults for system passwords</b> <ul style="list-style-type: none"> <li>Configure system parameters to prevent misuse</li> <li>Encrypt non-console admin access</li> </ul>	<b>Comprehensive suite of DBMS-specific tests based on industry standards (CIS, STIG)</b> <ul style="list-style-type: none"> <li>Checks for default passwords, misconfigured accounts, privileges, etc.</li> <li>Tracks and audits usage and alerts on misuse</li> <li>Locks configurations after vulnerabilities remediated</li> <li>Monitors encrypted traffic (Oracle ASO, SSL, etc.)</li> </ul>
<b>3</b>	<b>Protect stored cardholder data</b>	<b>Real-time database leak prevention</b> <ul style="list-style-type: none"> <li>Auto-discovers and classifies stored data; identifies sensitive data in query result stream</li> <li>Continuous, real-time policy-based monitoring with proactive security (alerts, blocking)</li> <li>Compensating control for column-level encryption</li> </ul>
<b>6</b>	<b>Maintain secure systems</b> <ul style="list-style-type: none"> <li>Establish a process to identify security vulnerabilities</li> <li>Follow change control procedures for all configuration changes</li> <li>Separation of duties (development, test and production)</li> </ul>	<b>Centralized vulnerability and configuration assessment</b> <ul style="list-style-type: none"> <li>Ensures all current patches are applied and vulnerabilities identified; provides "virtual patching"</li> <li>Alerts on all configuration changes</li> <li>Enforces separation of duties (SOD) with real-time alerting and granular access controls</li> </ul>
<b>7</b>	<b>Restrict access to cardholder data</b>	<b>Proactive, real-time access control (independent of native DBMS controls)</b> <ul style="list-style-type: none"> <li>Blocks any unauthorized user, including DBAs and system administrators, from accessing cardholder data</li> <li>Policies defined by source IP or application, OS or DB user, time, SQL command, object, etc.</li> <li>Compensating control for unsegmented networks</li> </ul>
<b>8</b>	<b>Assign a unique ID to each person with computer access</b> <ul style="list-style-type: none"> <li>Enforce password policies</li> <li>Limit repeated access attempts</li> </ul>	<b>Complements native DBMS controls with external, cross-DBMS controls</b> <ul style="list-style-type: none"> <li>Alerts on credential sharing, failed logins, account creation, privilege escalation</li> <li>Verifies password policies are enforced; locks accounts or terminates sessions</li> </ul>
<b>10</b>	<b>Track and monitor access to cardholder data</b>	<b>Continuous, granular auditing with scalable architecture to handle high transaction volumes</b> <ul style="list-style-type: none"> <li>Fine-grained audit trail of all database activities (SELECTs, DDL, DML, DCL, logins, etc.)</li> <li>Does not rely on native trace or audit logs: has minimal performance impact; enforces separation of duties</li> <li>Tracks all network and local connections, including direct access by DBAs (shared memory, etc.)</li> <li>Audit information stored securely in separate appliance to prevent anti-forensics/tampering</li> <li>Identifies fraud by resolving end-user IDs in multi-tier, connection-pooling applications such as SAP, PeopleSoft, etc.</li> <li>Integrates with LDAP, IAM, SIEM, change management, CMDBs, McAfee ePO, etc.</li> <li>Compliance workflow automation (electronic sign-offs, escalations) demonstrates proactive oversight process</li> <li>PCI Accelerator provides pre-configured reports based on best practices</li> </ul>
<b>11</b>	<b>Regularly test security systems and processes</b> <ul style="list-style-type: none"> <li>Run internal and external vulnerability scans</li> <li>Deploy integrity monitoring to detect modification of critical system files</li> </ul>	<b>Integrated vulnerability scanning, file integrity monitoring and behavioral vulnerability testing</b> <ul style="list-style-type: none"> <li>Includes hundreds of pre-configured vulnerability tests for all major DBMS/OS combinations</li> <li>Tracks changes to database configuration files and other external objects such as environment/registry variables, executables, scripts and OS files</li> </ul>
<b>12</b>	<b>Maintain an Information Security Policy</b> <ul style="list-style-type: none"> <li>Monitor and analyze security alerts and distribute to appropriate personnel</li> <li>Monitor and control all access to data</li> </ul>	<b>Robust automated controls for enforcing information security policies</b> <ul style="list-style-type: none"> <li>Real-time alerts, correlation alerts, centralized aggregation of all audit data, SIEM integration</li> <li>Automated sign-offs demonstrate formal oversight process</li> <li>100% visibility and control over all database transactions (with optional blocking)</li> </ul>

**Figure 9:** Guardium helps users rapidly secure cardholder data and comply with PCI DSS by satisfying a broad range of Requirements.

The Guardium solution with the PCI Accelerator will save hours of skilled labor digging through logs, constructing reports and documenting processes for auditors, while providing real-time protection of the flow of cardholder data across your entire enterprise.

## About the Guardium Platform

Guardium's real-time database security and monitoring solution monitors all access to sensitive data, across all major DBMS platforms and applications, without impacting performance or requiring changes to databases 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, 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 preventing information leaks from the data center and ensuring the integrity of enterprise data.

The company's enterprise security platform is now installed in more than 450 data centers worldwide, including 5 of the top 5 banks; 3 of the top 5 insurers; top government agencies; 2 of the top 3 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.

Guardium has partnerships with Accenture, ArcSight, BMC, EMC/RSA, IBM, McAfee, Microsoft, Oracle, Sybase and Teradata, with [Cisco as a strategic investor](#), and is a member of IBM's prestigious [Data Governance Council](#) and the [PCI Security Standards Council](#).

Founded in 2002, Guardium was the first company to address the core data security gap by delivering a scalable, cross-DBMS enterprise platform that both protects databases in real-time and automates the entire compliance auditing process.

Copyright © 2009 Guardium. All rights reserved. Information in this document is subject to change without notice. Guardium, Safeguarding Databases, and S-TAP are trademarks of Guardium. All other trademarks and service marks are the property of their respective owners. PCI-AC1109

---

<sup>1</sup> Working in conjunction with Guardium Vulnerability Assessment module

<sup>2</sup> Working in conjunction with Guardium Changes Auditing System module

**Guardium**<sup>®</sup>  
**SAFEGUARDING DATABASES™**

230 Third Avenue  
Waltham, MA 02451 USA  
T: +1 781 487 9400  
F: +1 781 487 7900  
[www.guardium.com](http://www.guardium.com)