PCI Accelerator
for Database Compliance

The Payment Card Industry (PCI) Data Security Standard offers a single approach to safeguarding sensitive data for all credit card brands. It consists of twelve requirements. Following this standard results in a single validation process to protect cardholder information.

Guardium's Solutions

Working in conjunction with Guardium's other solutions, the PCI Accelerator speeds compliance by providing:

- **Cardholder Database Access Map**
  A graphical map of access between cardholder database clients and servers. This map provides an at-a-glance view of activities by access type, content, and frequency.
- **PCI Compliance Report Card**
  A detailed view of security health for cardholder databases access, used to automate the compliance process with continuous real-time snapshots customized for user defined tests, weights, and assessments.
- **Comprehensive Audit Trail**
  The non-intrusive generation of a comprehensive audit trail for data usage and modifications required for regulatory compliance.
- **Automated Scheduling**
  Automated scheduling of PCI workflows, audit tasks, and dissemination of reports to responsible parties across the company; increases organizational accountability.
- **Dynamic Policy Baseline Builder and SQL-Level Database Firewall**
  Simplified and automated development of access rules for cardholder information; explicit enforcement of policies with continuous refinement capability, as well as SQL-level database firewall access control.

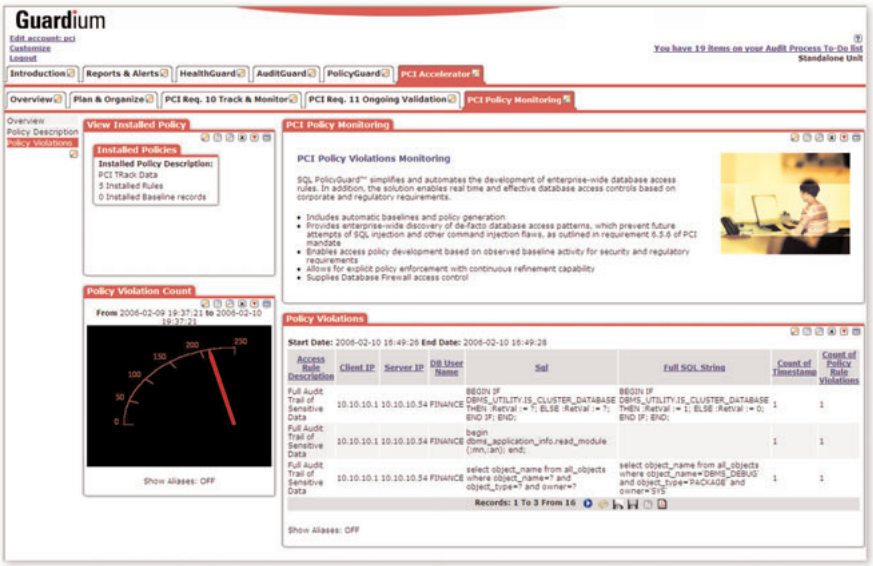
Accelerating the process

As part of Guardium's growing array of database compliance accelerators, the PCI Accelerator for Database Compliance streamlines and automates the procedures needed to support these directives and allow for cardholder information security.

Numerous PCI Data Security Standard requirements emphasize the importance of real-time monitoring and tracking of access to cardholder data and continuous assessment of database security health, including:

- Requirement 3: Protect stored data by keeping only the minimum information necessary
- Requirement 6: Secure systems by following a change control process
- Requirement 7: Limit access to need-to-know
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security vulnerabilities
- Requirement 12: Maintain and enforce information security policies

The PCI Accelerator assists organizations in establishing controls around the usage and storage of cardholder track data. The system can automatically scan all SQL data traffic in real-time, looking for recognizable patterns that are contained in the magnetic strip. Policy rules can be set to perform pattern tests. Suspicious events receive an immediate, automated response: blocking the storage or retrieval of track data, sending instant notifications, or logging violations for further research and correction.



Providing the tools to speed compliance

Tailored to address the process of monitoring and controlling cardholder information storage and access, the PCI Accelerator provides pre-configured report templates and other tools that can be customized to reflect specific organizational requirements.

Predefined report templates and automated workflows increase visibility into database activities while simplifying discovery of issues that need a closer investigation. The report templates can be customized to directly reflect specific organizational requirements. The solution also audits and helps document cardholder information access activities and establish an environment of increased accountability and visibility. The PCI Accelerator's functionality includes:

TAB	BENEFIT
Plan and Organize	Provides reports that enable users to plan PCI database compliance. The reports allow users to view information about who and what touches cardholder information; easily map cardholder servers, clients, databases, and users; verify that generic IDs and accounts are disabled or removed; assure that shared user IDs are not used for system administration activities and other critical functions, and more.
PCI Requirement 3: Safeguard Track Data	Assists organizations in establishing controls around the usage and storage of cardholder track data. The system can automatically scan all SQL data traffic in real-time, looking for recognizable patterns that are contained in the magnetic strip. Policy rules can be set to perform pattern tests. Suspicious events receive an immediate, automated response: blocking the storage of track data, sending instant notifications, or logging violations for further research and correction.
PCI Requirement 6: Change Management Control	Supplies an innovative and powerful solution to the problem of reconciling database schema changes. SQL Guard allows the DBAs to associate change request numbers with changes made to the database and then compare them with standard change management solutions (Peregrine, Remedy, etc.) to identify unapproved changes.
PCI Requirement 10: Track and Monitor	Enables users to certify that database access activities are above-board and that those that fall outside of the PCI Data Security Standard's parameters can either be rectified or explored further. Functionality provided includes a variety of reports on such topics as system exceptions and failed user logins, user activity audit trails, and cardholder data access by unauthorized applications. In addition, the solution automates workflows and disseminates database access information across the organization.
PCI Requirement 11: Continuous Vulnerability Assessments	Includes a Security Health Assessment that delivers the metrics and visual tools required for continuous assessment and proactive improvement of database security systems and processes. A dashboard view lets users map real-time and historical security measurements against preconfigured metrics like Shared Accounts, After Hours Login, Unauthorized User Access, and more.

Guardium®
SAFEGUARDING DATABASES™

230 Third Avenue • Waltham, MA 02451 USA • T: 781 487 9400 • F: 781 487 7900 • www.guardium.com