PCI Requirement	Guardium PCI Capabilities
2: Do not use vendor-supplied defaults for system passwords and other security parameters	• Vulnerability management module tests for existence of default passwords for common DBMS platforms. • Defines access rules to monitor and alert on usage of default IDs
3: Protect stored cardholder data	• Establishes granular access controls around cardholder and sensitive authentication data • Protects Web-facing applications from external attacks (such as SQL injection) via anomaly detection • Identifies movement of CVV/PIN data • Automatically locates & classifies sensitive data
6: Develop and maintain secure systems and applications	• Monitors and alerts on all changes to databases including changes to internal structures, data values, and external DBMS configuration files • Automates reconciliation of database changes to authorized work orders (Remedy, Peregrine, etc.)
7: Restrict access to cardholder data by business need-to-know	• Restricts access by user, application, subnet, etc., including privileged users
8: Assign a unique ID to each person with computer access	• Identifies use of shared database IDs • Identifies creation of new IDs • Restricts use of privileged vendor IDs • Alerts on failed logins & restricts repeated attempts
10: Track and monitor all access to network resources and cardholder data	• Creates secure, verifiable audit trail with granular information about *who, what, when, where, how* of all database activities • Identifies end-user IDs in connection pooling environments where database only sees generic ID (Oracle EBS, PeopleSoft, SAP, Siebel and custom applications) • Automates report distribution and documents oversight to guarantee timely response • Provides 100+ preconfigured audit templates and reports for PCI, SOX, and data privacy laws
11: Regularly test security systems and processes	• Assesses vulnerability and configuration risks. • Monitors integrity of all database files including configuration files, OS files, shell scripts, etc. • Delivers the metrics and real-time visual tools required for continuous assessment and proactive improvement of database security.
12: Maintain a policy that addresses information security for employees and contractors	• Provides practical, appliance-based technology to monitor and enforce corporate policies—without impacting performance or business processes.