IDERA® | SQL Security Solution Brief

SECURITY AND COMPLIANCE SOLUTIONS FOR PCI DSS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

The Payment Card Industry Data Security Standard (PCI DSS), currently at version 3.2, is a set of comprehensive requirements developed by the PCI Security Standards Council which includes American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. to help standardize the broad adoption of consistent data security measures on a global basis. In addition, it also includes requirements for security management, policies, procedures, network architecture, software design and other safeguards. PCI DSS is intended to help organizations to proactively secure customer credit card-related (cardholder) data.

Cardholder data that resides in Microsoft SQL Server database systems must adhere to the PCI DSS requirements. These requirements, in essence, mandate that IT and security professionals define and oversee the proper business disciplines and best practices for SQL Server access in order to prevent internal and external intrusions and enhance SQL Server confidentiality, data integrity and availability.

In order to define the proper PCI DSS baselines, audit database object/data changes, and report the appropriate data security-related findings to auditors and regulators, you must be able answer the following questions:

1. **Who has access to my “Payment Card” data?**
2. **What has changed with SQL Server permissions, logins & access?**
3. **How do I define a secure baseline and maintain it across my SQL Server enterprise?**
4. **How can I implement repeatable processes to help maintain my standards?**
5. **How do I audit permission, object and data changes on my SQL Server?**
6. **What is the best way for me to comply with Federal regulations with regards to my SQL Server databases?**
7. **How do I ensure that my PCI data can be rendered unreadable wherever it is backed up?**

HOW DOES **SQL SECURE** ADDRESS THESE REQUIREMENTS?

SQL Secure is a security analysis solution that helps IT organizations to identify SQL Server security violations and ensures security policies are enforced. You can find out who has access to what and identify each user's effective rights across all SQL Server objects. Furthermore, you can also alert on violations of your corporate policies, and secure your environment (internally and externally) from the most common methods of intrusion.

SQL Secure helps IT organizations address the requirements of PCE DSS with a built-in policy template that captures the relevant configurations and recommended settings as they relate to Microsoft SQL Server.

HOW DOES **SQL COMPLIANCE MANAGER** ADDRESS THESE REQUIREMENTS?

SQL Compliance Manager is a comprehensive SQL Server auditing, alerting and reporting solution that uses policy-based algorithms to track changes to your SQL Server objects and data. SQL Compliance Manager provides continuous auditing of all SQL Server activity by identifying who did what, when and how, whether the event is initiated by privileged users or hackers.

SQL Compliance Manager specifically goes beyond traditional auditing approaches by providing custom real-time monitoring and auditing of all data access, updates, schema modifications and permission changes.

HOW DOES **SQL SAFE BACKUP** ADDRESS ADDRESS THESE REQUIREMENTS?

SQL Safe Backup provides customizable policies to help you to facilitate backing up your PCI data and additionally delivers state-of-the-art encryption to ensure your backup files are protected anywhere they are stored.

PCI DSS	Requirement	IDERA SOLUTION
Section 2	Do not use vendor supplied defaults for system passwords and other security parameters. Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack.	SQL Secure provides 3 IDERA defined templates that exceed the guidelines from CIS, SRR & MSBPA. Vendor supplied defaults are identified as key items to change in order to reduce areas where a hacker can infiltrate payment card data.
Section 2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to all default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	SQL Secure provides security checks that ensure that vendor supplied defaults are not used in the SQL Server environment. If they are used, an assessment can be run to quickly identify and report any exceptions.
Section 2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards, which may include, but are not limited to: *- Center for Internet Security (CIS)* *- International Organization for Standardization (ISO)* *- SysAdmin Audit Network Security (SANS) institute* *- National Institute of Standards Technology (NIST)*	SQL Secure provides built-in policies that check your database server settings against best practice guidelines established by CIS, NIST (SRR) and MSBPA. The IDERA defined templates provide a more realistic baseline for hardening your security and also exceed the requirements set forth by the industry standards.
Section 3.4	Render primary account number (PAN) unreadable anywhere it is stored (including on portable digital media, backup media, and in logs.	SQL Safe Backup provides customizable policies to help you to facilitate backing up your PCI data and additionally delivers AES 128- and 256-bit encryption that would render the backup files unreadable anywhere they are stored.
Section 7.1	Limit access to system components and cardholder data only to those individuals whose job requires such access.	SQL Secure analyzes granted and inherited rights on tables containing cardholder data so you can instantly verify that access is limited to only those who should have it.
Section 7.1.1	Define access needs for each role, including: - System components and data resources that each role needs to access for their job function - Level of privilege required (for example, user, administrator, etc.) for accessing resources.	SQL Secure extracts access rights for privileged users to identify and validate established baselines.

PCI DSS	Requirement	IDERA SOLUTION
Section 7.2.2	Assign privileges to individuals based on job classification and function.	SQL Secure confirms assigned privileges according to their roles that are assigned. Changes are flagged for investigation.
Section 8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	SQL Secure shows all users, including de-nesting groups both locally and within Active Directory, to help identify users that should not have certain accesses, but in fact do.
Section 8.5.8	Identify all users with a unique user name before allowing them to access system components or card holder data. Do not use group, shared, or generic accounts and passwords. 8.5.8.a - For a sample of system components, examine user ID lists to verify the following: *- Generic user IDs and accounts are disabled or removed* *- Shared user IDs for system administration activities and other critical functions do not exist* *- Shared and generic user IDs are not used to administer any system components*	All users of SQL Server (internal, external and temporary) can be uniquely identifiable with SQL Secure. Should their access/permissions change, an assessment can be run to identify those changes.
Section 9.3	Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	SQL Secure provides “snapshot” capabilities for a given point in time for all user accesses and permissions. Once a user is terminated an assessment report can be run to confirm and document that the user’s access has been revoked.
Section 10	Track and monitor all access to network resources and cardholder data. It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.	SQL Compliance Manager audits all user activity to PCI data. If there is an exception, you can easily track, alert and report on the events that caused it and determine the cause.
Section 10.1	Implement audit trails to link all access to system components to each individual user.	SQL Compliance Manager provides continuous auditing of all SQL Server activity, identifying who did what, when and how.

PCI DSS	Requirement	IDERA SOLUTION
Section 10.2	Implement automated audit trails for all system components to reconstruct the following events: ***10.2.1*** *- All individual user accesses to cardholder data* ***10.2.2*** *- All actions taken by any individual with root or administrative privileges* ***10.2.3*** *- Access to all audit trails* ***10.2.4*** *- Invalid logical access attempts* ***10.2.5*** *- Use of identification and authentication mechanisms* ***10.2.6*** *- Initialization of audit logs* ***10.2.7*** *- Creation and deletions of system-level objects*	SQL Compliance Manager audits all of the events required by section 10.2 and also provides detailed reports for internal and external auditors.
Section 10.3	Record at least the following audit trail entries for all system components for each event: ***10.3.1*** *- User identification* ***10.3.2*** *- Type of event* ***10.3.3*** *- Date and time* ***10.3.4*** *- Success or failure indication* ***10.3.5*** *- Origination of event* ***10.3.6*** *- Identity or name of affected data, system component or resource*	SQL Compliance Manager audits all of the events required by section 10.3 and also provides detailed reports for internal and external auditors.
Section 10.5	Secure audit trails so they cannot be altered.	SQL Compliance Manager provides an immutable audit trail of all SQL Server activity, including administrator activities. Any changes to the audit logs can be detected, and alerts can be configured to notify the appropriate personnel.
Section 10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	SQL Safe Backup provides policy based management for backing up PCI data and additionally provides AES 128- and 256-bit encryption which makes your backups tamperproof and secure.
Section 10.7	Retain audit trail history for at least one year, with a minimum of three months online availability.	SQL Secure and SQL Compliance Manager store all audit data in a central repository which makes it easy to archive data for any length of time.
Section 12.2	Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	SQL Secure and SQL Compliance Manager are used to standardize daily security procedures for auditing changes to SQL Server data and objects and also helping to define user permissions, accesses and maintaining them.

IDERA understands that IT doesn't run on the network – it runs on the data and databases that power your business. That's why we design our products with the database as the nucleus of your IT universe.

Our database lifecycle management solutions allow database and IT professionals to design, monitor and manage data systems with complete confidence, whether in the cloud or on-premises.

We offer a diverse portfolio of free tools and educational resources to help you do more with less while giving you the knowledge to deliver even more than you did yesterday.

Whatever your need, IDERA has a solution.

IDERA