IDERA WHITEPAPER

PCI DSS:
WHAT EVERY DBA NEEDS TO KNOW

THIS WHITEPAPER GIVES AN OVERVIEW OF THE KEY PCI DSS REQUIREMENTS THAT APPLY TO DATABASE SECURITY AND THE IDERA PRODUCTS THAT CAN HELP ENSURE COMPLIANCE WITH THIS CRUCIAL DATA SECURITY STANDARD.

WWW.IDERA.COM

idera™
TOOLS FOR SQL SERVER™

INTRODUCTION

The PCI DSS (Payment Card Industry Data Security Standard) defines security standards for organizations that handle payment card account data. This standard was created in 2005 by the PCI Security Standards Council, an organization founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc. The Council's mission is to enhance payment account data security by encouraging broad adoption of the PCI Security Standards.

DBAs responsible for SQL Servers that store and manage payment account data need to comply with PCI DSS requirements in order to ensure that account data is properly secured. This whitepaper gives an overview of the key PCI DSS requirements that apply to database security and the Idera products that can help ensure compliance with this crucial data security standard.

PCI DSS Section 2.2 Requirement:

Section 2.2 requires that organizations develop configuration standards for all system components and ensure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

WHAT THIS MEANS FOR DBAs:

There are known weaknesses with all databases, and known ways to configure them to address and minimize security risks and vulnerabilities. Fortunately, those methods are documented in the standards provided by organizations such as those listed above. DBAs should ensure that their system configurations are consistent with these security best practices.

HOW IDERA CAN HELP:

SQLsecure provides built-in policies that will check your database server settings against security best practices established by CIS and NIST SRR (Security Readiness Review for SQL Server), or your own internal security standards. SQLsecure will highlight variances from the security policies, and continuously recheck your settings against these policies to notify you if any settings are changed in the future.

PCI DSS Section 7.1 and 7.2 Requirements:

Sections 7.1 and 7.2 require that organizations limit access to computing resources and cardholder information to those individuals whose job requires such access. Additionally, companies must establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.

WHAT THIS MEANS FOR DBAs:

The more people who have access to databases housing cardholder data, the more risk there is that a user's account will be mishandled through inexperience or malice. Your organization should create a clear policy for data access control to define how, and to whom, access is granted. DBAs should then be diligent in limiting access to those identified by the policy.

HOW IDERA CAN HELP:

SQLsecure gives you the ability to look at 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. Additionally, SQLsecure analyzes user and role assignments so you can see users' effective permissions. Conducting a similar assessment manually is difficult and time-consuming, if not impossible, to do.

PCI DSS Section 8.1 and 8.5.8 Requirement:

Sections 8.1 and 8.5.8 require that organizations identify all users with a unique user name before allowing them to access system components or cardholder data. Organizations should not use group, shared, or generic accounts and passwords.

WHAT THIS MEANS FOR DBAs:

DBAs need to account for all the users that have access to a database. This requires full enumeration of login accounts and verification of owner uniqueness as well as proper assignment. By ensuring each user is uniquely identified—instead of using one ID for several employees—a DBA can ensure that individual responsibility for actions is being maintained and effective audit trails can be recorded for each employee. This will help speed issue resolution and containment if misuse occurs.

HOW IDERA CAN HELP:

SQLsecure provides a complete list of users by de-nesting groups both locally and within Active Directory. This often exposes users that should not have database access, but in fact do. Additionally, **SQL compliance manager** audits all database activity for all users, making it easy to keep a detailed audit trail of exactly who did what, how, when, and where.

PCI DSS Section 10.1 Requirement:

Section 10.1 requires that organizations establish a process for linking all access to system components (especially access with administrative privileges such as root) to each individual user.

WHAT THIS MEANS FOR DBAs:

It is critical for organizations to have the ability to link access to database components back to a specific user, in particular, for those users with administrative privileges. This system should generate audit logs and provide the ability to trace back suspicious activity to a specific user. Post-incident forensic teams heavily depend on these logs for investigations.

HOW IDERA CAN HELP:

Idera's SQL compliance manager provides continuous auditing of all SQL Server activity, telling you who did what, when and how. SQL compliance manager collects data efficiently, stores it securely, and provides analysis tools and reports to support forensic analysis. It also includes multiple tamper-proofing and data security features, as well as methods for watching events without exposing account information.

PCI DSS Section 10.2 and 10.3 Requirements:

Section 10.2 requires automated audit trails for all system components to reconstruct a number of crucial cardholder data access events including:

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 assessment trails
10.2.4 Invalid logical access attempts
10.2 5 Use of identification and authentication mechanisms
10.2.6 Initialization of the assessment logs
10.2.7 Creation and deletion of system-level objects

PCI DSS Section 10.2 and 10.3 Requirements, cont'd:

Additionally, section 10.3 requires the following specific information to be recorded in the audit trail 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

WHAT THIS MEANS FOR DBAs:

Hackers on the network will often perform multiple access attempts on targeted systems. Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up. By recording these entries for the auditable events, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when, and how.

HOW IDERA CAN HELP:

Idera's SQL compliance manager audits all of the events required by section 10.2, and collects all details required by section 10.3, and more. Additionally, SQL compliance manager has an alerting engine as well as counters and trend graphs to identify activity level anomalies often associated with suspect activities.

PCI DSS Section 10.5 Requirement:

Section 10.5 requires organizations to secure audit trails so they cannot be altered.

WHAT THIS MEANS FOR DBAs:

Often a hacker who has entered the network will attempt to edit the audit logs in order to hide their activity. Without adequate protection of audit logs, their completeness, accuracy, and integrity cannot be guaranteed, and the audit logs can be rendered useless as an investigation tool after a compromise.

HOW IDERA CAN HELP:

Idera's 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.

PCI DSS Section 10.7 Requirement:

Section 10.7 requires organizations to retain audit trail history for at least one year, with a minimum of three months online availability.

WHAT THIS MEANS FOR DBAs:

DBAs must have a way to archive audit logs for at least a year to allow for the fact that it often takes a while to notice that a compromise has occurred or is occurring, and to allow sufficient log history to determine the length of time that the breach occurred and to assess the impact.

HOW IDERA CAN HELP:

Idera's SQLsecure and SQL compliance manager store all audit data in a central repository which makes it easy to archive data for any length of time to meet regulatory requirements.

SUMMARY

PCI DSS Section	Overview	Recommended Idera Product
Section 2.2	Develop configuration standards for all system components and assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	**SQLsecure** provides built-in policies that will check your database server settings against security best practices established by CIS and NIST (SRR) and highlight any variances.
Section 7.1 & 7.2	Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	**SQLsecure** 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 8.1 & 8.5.8	Identify all users with a unique user name before allowing them to access system components or cardholder data. Organizations should not use group, shared, or generic accounts and passwords.	**SQLsecure** shows all users, including de-nesting groups both locally and within Active Directory, to help identify users that should not have database access, but in fact do.
Section 10.1	Establish a process for linking all access to system components (especially access with administrative privileges such as root) to each individual user.	**SQL compliance manager** provides continuous auditing of all SQL Server activity, telling you who did what, when and how.
Section 10.2 & 10.3	Automated audit trails are required for all system components to reconstruct crucial cardholder data access events. Specific information must be collected for each audit event.	**SQL compliance manager** audits all of the events required by section 10.2, and collects all details required by section 10.3, and more.
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 10.7	Retain audit trail history for at least one year, with a minimum of three months online availability.	**SQLsecure** and **SQL compliance manager** store all audit data in a central repository which makes it easy to archive data for any length of time.

For additional information or to download a 14-day evaluation of any Idera product, please visit: www.idera.com.

ABOUT IDERA

Idera delivers a new generation of award-winning tools for managing and securing the world's fastest growing database management system: Microsoft SQL Server. Battle-proven and engineered for the enterprise, Idera's solutions include: Auditing and Compliance, Performance & Availability, Backup and Recovery, Change & Configuration Management. Headquartered in Houston, Texas, Idera's products are sold and supported worldwide directly and via authorized resellers and distributors around the globe. For more information, or to download a free 14-day full-functional evaluation copy of any of Idera's tools for SQL Server, please visit www.idera.com.

Idera | BBS Technologies
802 Lovett Blvd Houston, Texas 77006
PHONE 713.523.4433 | TOLL FREE 877.GO.IDERA (464.3372)
FAX 713.862.521O | WEB www.idera.com

idera™
TOOLS FOR SQL SERVER™