Suggested URL for this landing page:
http://www.likewise.com/solutions/compliance/pci-dss.php

Pls link to this page from
http://www.likewise.com/solutions/compliance/index.php

============================
METADATA

Title: PCI Compliance

Description: Likewise Data Analytics and Governance delivers PCI DSS compliance by securing, auditing, and monitoring information on file servers and storage NAS.

Keywords: PCI DSS, data storage compliance, information security, access control, IT compliance, compliance security, unstructured data, storage NAS, file server

============================
H1:
PCI Compliance

H2 Subtitle:
Managing File Servers and NAS Systems for PCI DSS Compliance

The Payment Card Industry Data Security Standard is a set of requirements for businesses that process payment card information. Developed by Visa, American Express, and other members of the PCI Security Standards Council, the standard sets forth policies, procedures, and practices to protect customer account data.

The standard includes IT compliance requirements for controlling access to customer data, authenticating business users, monitoring access, maintaining a secure storage network, and auditing system resources. Likewise helps you fulfill these requirements by securing, monitoring, and auditing customer account information stored on file servers and NAS systems.

The business value of using Likewise for PCI compliance spans the categories of security, risk mitigation, and cost reduction:

*Comply with a number of PCI DSS requirements.

*Protect the confidentiality, integrity, and availability of unstructured account information.

*Reduce the risk of noncompliance, security breeches, and PCI DSS violations.

*Cut the costs of compliance, storage, and security.

============================
<h2>Regulatory Compliance Solutions for PCI DSS
</h2>
The PCI DSS requirements apply to all system components that are connected to the part of

the network that contains cardholder data or sensitive authentication data, including file servers and network attached storage (NAS) systems.

When unstructured customer account data is stored on file servers and NAS systems, the Likewise solution brings you into compliance with many of the standard's requirements. Likewise authenticates business users, controls access to customer data, monitors access and file changes, maintains a secure NAS storage network, and audits system resources.

<!-- these are h3s:: -->

User Authentication for File Servers and NAS Systems

Authenticating business users who are attempting to access credit card account information is a requirement of section 8 of PCI DSS. Likewise Storage Services authenticates a user by using the user's unique, single ID from either Microsoft Active Directory or another identity management systems, such as LDAP. Likewise's authentication is cross platform and multiprotocol -- it authenticates users from Linux, Unix, Windows, and Mac clients.

For more information about Likewise authentication, see Likewise Storage Services.

Access Control for Unstructured Data

Section 7 of PCI standard requires the implementation of an automated access control system. Likewise Storage Services features automated access control that authorizes access to unstructured customer account data on file servers and network attached storage (NAS) systems. For access control, Likewise performs authorization based on the user's unique ID in your identity management system, enabling you to enforce one-user, one-ID policies and to limit access to only those with a business need-to-know. See Storage Access Control: Securing Access to Files Servers and NAS Storage.

Access Monitoring

Section of 10 of PCI DSS requires that you track and monitor all access to cardholder data. After capturing and recording all access attempts and system activity, Likewise stores the data in a high-performance NoSQL database. As a result, analytics, forensics and historic reports can be executed with speed and ease.

In addition, the Likewise dashboard monitors exceptions so you can track invalid logical access attempts, which is one of the sub-requirements of PCI DSS section 10. See Exception Monitoring and Reporting: Identity-Aware Exception Monitoring for Security and PCI Compliance.

File Integrity Monitoring for PCI DSS Compliance

PCI DSS requirement 11.5 mandates file integrity monitoring that raises an alert for unauthorized changes to content files. With Likewise, you can track changes made to files that contain data governed by the PCI data security standard. See File Activity Monitoring: Tracking Unstructured Data for Security and PCI Compliance.

Locating and Securing Account Information

Likewise Data Analytics and Governance will search unstructured data for cardholder account information, such as credit card numbers, mark the data as sensitive, and then secure it. See Securing Unstructured Data: Protecting Sensitive Files by Uniting Identity, Security, and Storage.

Auditing Unstructured Information for IT Compliance

<!-- pls add link to the auditing white paper; we'll add more links and content to this later after, but I want to get us going without too many dependencies -->

To satisfy the requirements of section 10 of the PCI standard, Likewise records the following entries for each event that takes place on a storage system or file server: user identification; type of event; date and time; success or failure; indication origination of event; and the identity or name of affected data, system component, or resource.

In addition, Likewise's centralized NoSQL database backs up these audit trails and then protects them with its build-in security system, thereby showing the required chain of custody. Moreover, the NoSQL database cost-effectively scales to retain huge amounts of audit-trail data. See Auditing Unstructured Data: Identity-Aware Storage, File Activity Monitoring, and Compliance Reporting Across Platforms.

Dashboard with Compliance Reports

Another PCI DSS requirement, set forth in section 10.6, is that you review logs for all system components at least daily. The Likewise dashboard lets you monitor storage servers and their logs in near real-time for authentication, authorization, and other security events. The dashboard ties each event to a user's identity. To help demonstrate compliance to an auditor, the dashboard also generates PCI compliance reports. See Likewise Data Analytics and Governance.

===================================
<!-- list of features is tailored for each page:: -->

Features

*Compliance reports for PCI DSS
*Access control and access reports
*File modification reports
*Templates for custom reports
*Historical reports for auditing and forensics
*Chain of custody for event data
*Dashboard with custom views
*Alerts for policy violations
*User authentication
*Privileged user monitoring
*Exception monitoring
*NoSQL database for analytics
*Event aggregation from NetApp, EMC NAS systems, etc.
*File integrity monitoring