Lepide

Datasheet

PCI DSS

PCI DSS

Organizations must make sure they have records available to prove that they are compliant. These records can only be generated through in-depth auditing of these servers and putting together detailed reports. Native auditing has numerous drawbacks when it comes to this. In many cases, it is either too time consuming or too complex a process to be viable. Lepide simplifies IT auditing tasks and provides a single platform with which to audit multiple instances of different servers. It also contains many pre-defined reports within a PCI compliance section that have been specifically tailored to help you meet these requirements.

Secure Cardholder Data

Ensure users aren’t accessing cardholder data unless they require that access to perform their job role.

Monitor Access to PCI Data

Monitor and alert on all user behavior relating to data that falls under PCI DSS compliance.

Pre-Set PCI Reports

Numerous pre-defined reports tailored to meet some of the more stringent auditing aspects of PCI DSS compliance.

How Lepide Helps

Audit Access to Payment Data

Any access to payment data needs to be recorded in order to ensure that no unauthorized activities are taking place and that the sensitive data is safely stored. Lepide contains in-depth auditing reports that enable you to monitor and report on every access made to files, folders and mailboxes. You can get real-time alerts on any access made to critical data or mailboxes delivered as emails to selected recipients or as push notifications to the Lepide Mobile App.

Audit Users of Payment Data

Any Active Directory user that has the ability to create, delete or modify payment data must have their actions closely monitored and audited. Any changes in their permissions should be made clear to the administrators and other concerned persons in order to ensure a policy of least privilege is upheld. Lepide displays real-time reports on the activities of Active Directory users. Each change is audited in real-time, and an alert is sent to the intended recipients via email or push notifications on the Lepide Mobile App.

Audit Computers Storing Payment Data

Computers that store payment data are required to be audited as per PCI standards. This is to ensure that accesses and changes taking place on that particular computer are authorized and the payment data is secure. Lepide provides dedicated reports to keep track of changes made to computer objects. Real-time information helps administrators maintain awareness on critical issues that may arise due to any unwanted change.

Keep a Check on User Groups

Access permissions are often assigned to users through groups. This means that any changes in group memberships may result in excessive permissions being awarded to junior members of staff. When this occurs in relation to payment data, PCI compliance comes into play. Lepide helps you keeps track of all changes made to Active Directory and Exchange Server groups. It notifies administrators in real-time about any critical change taking place in these servers.

Keep Track of Permissions

In accordance with PCI compliance regulations, it is advisable to maintain a policy of least privilege to ensure that users have only the levels of privilege that they require in order to fulfill their job requirements. Lepide keeps track of all changes in the permissions of Active Directory objects and offers dedicated reports on them. You can set real-time alerts that will be delivered by email or push notification to the Lepide Mobile App.