Lepide

Datasheet

Gramm–Leach–Bliley Act (GLBA)

GLBA Compliance with Lepide

Complying with GLBA is not an easy task, as it involves multiple frameworks being put in place simultaneously. One important task GLBA requires you to undertake is regular and pro-active auditing of critical IT systems and data. However, maintaining a stringent auditing strategy of server components through native methodologies is not easy, as the process can be both time consuming and complex. Lepide provides you with an extra weapon when it comes to IT auditing; with continuous monitoring, predefined reports and real-time alerts on for detecting critical changes.

Secure GLBA Data
Ensure users aren't accessing data related to GLBA unless they require that access to perform their job role.
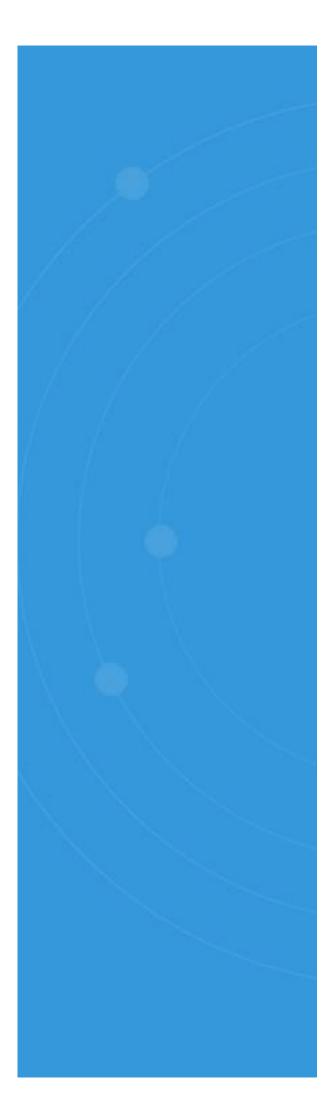
Monitor Access to GLBA Data
Monitor and alert on all user behavior relating to data that falls under GLBA compliance regulations.

Pre-Set GLBA Reports
Numerous pre-defined reports tailored to meet some of the more stringent auditing aspects of GLBA compliance.

How Lepide Helps

Audit Changes in Data Permissions

Permissions protect files and folders from unauthorized user access. Any changes taking place to permissions that go unnoticed, could result in inappropriate or unauthorized levels of access being awarded to members of staff. Excessive permissions can be a threat to data integrity. Lepide monitors all changes in permissions of files and folders. Every change is notified in real-time through email and push notifications to the Lepide Mobile App.

Audit Changes in Group Memberships

A typical user can receive administrative privileges by becoming a member of an administrative group. Sudden changes in group memberships should therefore be dealt with quickly before it they turn into insider threats. Lepide monitors all changes in group memberships and notifies administrators in real-time through emails to selected recipients or notifications to the Lepide Mobile App.

Audit Changes in Shared Folders

Shared Folders store sensitive data that has to be shared with all users in a network. They are great for encouraging a collaborative work environment, but strict and pro-active auditing needs to take place in order to ensure that no unauthorized changes are taking place. Changes made to shared folders, such as who deleted or modified a file need to be recorded and corrected where necessary. Lepide audits all changes made in Shared Folders; including content and permissions.

Audit Changes in Group Policies

Most IT security features are applied through domain-wide Group Policy Objects. Any sudden change to these policies can create a loophole in the IT security settings that allows for insider misuse/abuse. Lepide enables you to keep track of all changes in Group Policy Objects and notifies you in real-time via email or push-notifications to the Lepide Mobile App. Lepide also works in conjunction with Lepide Object Restore Wizard to allow you to restore whole Group Policy Objects in a matter of clicks.