ManageEngine
DataSecurity Plus

GLBA Compliance

Automate and simplify GLBA compliance using DataSecurity Plus

Automate and simplify GLBA compliance using DataSecurity Plus

The Gramm-Leach-Bliley Act (GLBA)—also known as the Financial Services Modernization Act—mandates the standards that financial institutions, such as commercial banks, security firms, insurance companies, and credit unions, need to follow to ensure the confidentiality and security of their customers' financial records and personal information. Failure to comply can result in dire consequence for businesses, including imprisonment of directors and officers for up to five years, penalties up to $100,000 per violation, or both.

Become GLBA compliant using DataSecurity Plus

DataSecurity Plus' audit tools help protect your organization's critical information against loss, misuse, unauthorized access, or modification by proactively identifying and addressing potential threats using preconfigured alerts. In addition, DataSecurity Plus' robust auditing and reporting capabilities help ensure data integrity, prove regulatory compliance, and verify role-based access, ensuring business continuity.

Below is a list of reports you can use to prove that your organization is GLBA compliant.

GLBA standards	DataSecurity Plus report or alert
Track all modifications to files in order to assess risks to data integrity and resolve violations, if any.	All file/folder changes report
	Deleted/overwritten files report
	Security permission changes report
	Most modified file report
	File modified after N days report
	Create events report
	Renamed/moved events report
Periodically review all attempts to access critical data, including both successful and failed attempts.	All failed attempts report
	Read events report
	Most accessed file report
	Most accesses by processes/user report
	File accessed after N days report
Review access rights and file permissions periodically to ensure that no excessive permissions are assigned beyond what is needed.	NTFS permissions report
	Share permissions report
Utilize customizable alerts to enable timely detection of any user actions that violate your data protection policies.	File/folder moved or renamed alert
	File/folder security changes alert
	File/folder removed alert
	Media files alert
Use preconfigured alerts to detect and respond quickly to potential data breaches.	Ransomware file alert
	Threshold-based alert

* You can also generate customized reports based on file path, users, business hours, etc..

The DataSecurity Plus advantage

Audit file and folder access
Obtain detailed information on the quintessential four W's—who accessed what, when, and from where—for all file and folder accesses.

Maintain compliance
Meet many of the critical compliance requirements mandated by regulations such as PCI DSS, HIPAA, FISMA, GDPR, SOX, and GLBA.

Monitor file permissions
Examine share and security permissions of files and folders to prevent access exploitation.

View a snapshot of your environment
Through continuous, real-time monitoring, get a bird's-eye view of your entire file server environment.

Set up real-time monitoring and alerts
Become proactive with real-time file and folder access and change auditing. Continuously monitor your file server environment with email notifications about critical activities.

Create reports and schedules
Generate exhaustive reports in multiple formats like PDF, XLS, CSV, and HTML. Flexible scheduling allows you to deliver reports periodically via email.

Archive audit data
Preserve large amounts of audit data for future review without affecting software performance. Archiving can also be automated.

Other features
In terms of features, we've barely scratched the surface. To learn more about the many, many more features available in DataSecurity Plus, schedule an online demo with one of our experts.

About DataSecurity Plus

ManageEngine DataSecurity Plus is a data visibility and security solution. It tracks and alerts on critical file modifications and movement across file servers, failover clusters, workstations, and USBs. Users can locate and analyze files containing PII/ePHI stored in Windows file servers, failover clusters, and OneDrive environments using built-in data discovery rules. Its data leak prevention (DLP) capability helps detect and respond to the exfiltration of sensitive data via USBs, email, printers, and more. It also provides detailed audit reports that help organizations streamline compliance with multiple IT regulations.

Download free trial $ Get a quote