

SOX Compliance

# Automate and simplify SOX compliance using DataSecurity Plus



## **Automate and simplify SOX compliance using DataSecurity Plus**

Enacted in response to multiple corporate accounting scandals, the Sarbanes Oxley Act (SOX) (also known as the Public Company Accounting Reform and Investor Protection Act) safeguards investors from fraudulent activities involving internal employees. Heavy penalties and stringent regulatory standards are imposed to ensure all the financial information processed by an organization is genuine and reliable.

## Become SOX compliant using DataSecurity Plus

DataSecurity Plus is an audit tool that delivers the visibility required to monitor and track the validity of all financial information in an organization. DataSecurity Plus' various reports can help you manage the difficult task of proving compliance while ensuring the security of your financial data.

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

SOX 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
	Create events report
	Renamed/moved events report
	Files modified after N days 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
	Files 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

DataSecurity Plus is real-time Windows file server auditing and analysis software that tracks, monitors, and reports all accesses and modifications made on your file server environment. It provides a detailed analysis of file storage, helps meet multiple compliance requirements, and generates instant, user-defined email alerts while carrying out automatic responses in the event of unauthorized or malicious file changes. Additionally, generate detailed, preconfigured reports with DataSecurity Plus and export the results to XLS, HTML, PDF, and CSV formats to assist in interpretation and computer forensics.