ManageEngine
DataSecurity Plus

HIPAA Compliance

Automate and simplify HIPAA compliance using DataSecurity Plus

Automate and simplify HIPAA compliance using DataSecurity Plus

The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) mandate the standards companies need to follow to protect and maintain the confidentiality of personally identifiable health care information. An added benefit of compliance with HIPAA and HITECH, which is mandatory for all entities that transmit healthcare information, is that it allows you to proactively dodge both external threats and insider privilege abuse.

Become HIPAA/HITECH compliant using DataSecurity Plus

DataSecurity Plus has extensive reports to help you meet HIPAA and HITECH's data security standards. With these reports, you can draw meaningful insights on accesses, modifications, and permissions of critical files to help mitigate insider threats.

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

HIPAA/HITECH standards	DataSecurity Plus report or alert
Monitor all modifications to protected health information (PHI) across file servers to detect 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
	File modified after N days report
Audit and report all data accesses to PHI to ensure that no unauthorized changes are taking place.	All failed attempts report
	Read events report
	Most accessed file report
	Most accesses by processes/user report
	File accessed after N days report
Track and monitor all changes to access rights and file server permissions to identify anomalies.	NTFS permissions report
	Share permissions report
Utilize customizable, built-in capabilities for alerts to regularly audit file/folder-related activities.	File/folder moved or renamed alert
	File/folder security changes alert
	File/folder removed alert
	Media files alert
Detect and respond to mass access with customizable, automated responses.	Ransomware file alert
	Threshold-based alert

* Using this HIPAA compliance tool 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