

FISMA Compliance

# Automate and simplify FISMA compliance using DataSecurity Plus



## Automate and simplify FISMA compliance using DataSecurity Plus

The Federal Information Security Management Act (FISMA) of 2002 and the Federal Information Security Modernization Act (FISMA) of 2014 enforce stringent standards to ensure the security, confidentiality, and integrity of United States federal property and information. These acts mandate that all federal agencies, along with their contractors, service providers, and any organizations that operate government IT systems, follow certain policies, procedures, and processes to mitigate ever-growing data threats.

## Become FISMA compliant using DataSecurity Plus

DataSecurity Plus' audit tool helps you streamline your organization's network security, and detect and respond to potential threats, through continuous monitoring and reporting of all activities on your file server. You can use DataSecurity Plus' automated, actionable audit reports to achieve and maintain compliance with federal standards.

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

FISMA 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
	Files accessed after N days report
Review access rights and file permissions periodically to ensure that no excessive permissions are assigned.	NTFS permissions report
	Share permissions report
Utilize customizable alerts to quickly detect 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

Periodically examine file storage to verify that data stored is relevant, required, and does not exceed the requirements defined in your data retention policy.	Old files report
	Stale files report
	Unmodified files report
	Large files report
	Hidden files report
	Non-business files report
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.

**Disclaimer:** Fully complying with the FISMA requires a variety of solutions, processes, people, and technologies. This page is provided for informational purpose only and should not be considered as legal advice for FISMA compliance. ManageEngine makes no warranties, express, implied, or statutory, about the information in this material.

## DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It analyzes file storage and security permissions, deletes junk files, and detects security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing personally identifiable information (PII), payment card information (PCI), and electronic protected health information (ePHI). It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage. Together, these capabilities ensure the all-round protection of data at rest, data in use, and data in motion.

To explore these features and see DataSecurity Plus in action, [check out the online demo](#).

To learn more about DataSecurity Plus, visit [www.datasecurityplus.com](http://www.datasecurityplus.com).

↓ Download free trial

\$ Get a quote

### Explore **DataSecurity Plus**' capabilities



#### File server auditing

Audit and report on file accesses and modifications, with real-time alerts and automated responses for critical file activities.

[LEARN MORE](#)



#### File analysis

Analyze file security and storage, manage junk files, optimize disk space usage, and identify permission vulnerabilities.

[LEARN MORE](#)



#### Data risk assessment

Discover and classify files containing sensitive data, such as PII, PCI, and ePHI, by combining content inspection and contextual analysis.

[LEARN MORE](#)



#### Data leak prevention

Monitor endpoint file activities, and detect and disrupt data leaks via USBs, email, web applications, and printers.

[LEARN MORE](#)



#### Cloud protection

Track enterprise web traffic and enforce policies to block the use of inappropriate, risky, or malicious web applications.

[LEARN MORE](#)