



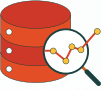



Use cases

DataSecurity Plus



DSP Use cases

	File server auditing	1
	File integrity monitoring	1
	Ransomware quarantining	2
	Data discovery	2
	Storage analysis	3
	Compliance reporting	3

File server auditing

Gain visibility and insight into all file activities on your critical file server.

- Get a snapshot of your recent user or file activities and trends.
- Discover who has what permissions (NTFS and share permissions) over your critical files.
- Examine files and folders that have the same level of permission (e.g. full control), and assess their necessity.
- Monitor and report on specific objects, access types, or user activities.

File integrity monitoring

Strengthen security and streamline compliance.

- Trigger instant alerts on sudden spikes in file or folder access or modification events.
- Selectively monitor critical files, folders, shares, or user activities.
- Receive real-time notifications on multiple denied access attempts to critical files.
- Track source and host details and more as a part of forensic analysis.
- Monitor changes made to your sensitive files that occur after business-hours.

Ransomware quarantining

Detect and respond to ransomware attacks instantaneously.

- Spot indicators of ransomware attacks using threshold-based, real-time alert profiles.
- Detect ransomware attacks faster with the auto-updated ransomware file types library.
- Shut down ransomware-infected systems using preconfigured, custom scripts.
- Track the client IP or host details for post incident root cause analysis.

Data discovery

Locate and analyze high-risk content.

- Find files, folders, or shares that store personal data or PII/ePHI.
- Gain visibility into personal data including its type (e.g. name, SSNs, banking details, and more), volume, and location.
- Spot your organization-specific critical data by creating custom policies and rules.
- Monitor who accesses personal data, including when, where, and how it's used.

Storage analysis

Discard redundant data and free up disk space.

- Identify and isolate old, stale, unmodified, large, non-business, and hidden files present in your file server.
- Analyze and compare disk space usage and trends at any point in time.
- Monitor the last modified, accessed, and created critical files.
- Gain visibility into critical file or folder meta properties including size, owner, object type, and more.
- Uncover which users or what file are eating up your storage space.

Compliance reporting

Meet external regulatory mandates including HIPAA, PCI DSS, the GDPR, SOX, and more.

- Address critical requirements of PCI DSS and HIPAA regulations using the change detection capability.
- Become GDPR-compliant by locating personal data (PII/ePHI) stored in unintended locations using data discovery.
- Identify the root cause of security incidents using accurate forensic data, and generate clear and concise audit records.
- Audit and archive audit trails to ensure accountability for each file activity.

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.

± 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

Detect and disrupt data leaks via USBs, email, web applications, and printers; monitor endpoint file activity; and more.

[Learn more](#)



Cloud protection

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

[Learn more](#)

Our Products

AD360 | Log360 | ADAudit Plus | EventLog Analyzer

Exchange Reporter Plus | SharePoint Manager Plus