

A background network diagram consisting of interconnected nodes and lines. Some nodes are highlighted with blue circles or dots. The nodes are arranged in a complex, non-linear pattern, suggesting a data network or system architecture.

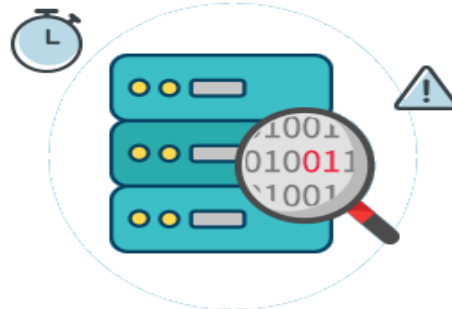
# DataSecurity Plus

Data visibility and security solution

# Solutions offered by DataSecurity Plus



Data discovery



Real-time Windows  
file server auditing



Storage analysis

# Other highlights of DataSecurity Plus

- Helps streamline multiple compliance requirements including GDPR, HIPAA, PCI, and more.
- Generate instant, user defined email alerts while carrying out automatic predefined responses when potential security threats such as ransomware occurs.
- Selectively monitor critical files, folders, or even users to effectively pinpoint any unauthorized changes made to files.
- Identify root cause of security incidents faster using actionable, accurate forensic data, and generate clear concise audit records as legal evidence.

# File server auditing capabilities

A decorative network diagram in the top right corner, consisting of various sized circles (nodes) connected by thin lines (edges). Some nodes are solid grey, while others are hollow white with a grey border. The connections form a complex, interconnected web.

- Audits, reports, and sends alerts, in real-time on all accesses and modifications to every file and folder in your Windows file server.
- Monitors file integrity and detects unauthorized changes made to your files.
- Offers visibility into file share permissions; sends real-time notifications on changes to sensitive files.
- Detects, alerts, and shuts down ransomware attacks in real time.

# Why you need File server auditing component?

- To audit, monitor, and track changes made to your sensitive files at any point in time including non business hours.
- For file integrity monitoring.
- To detect, inform, and respond to sudden spike in file access or modification using real-time alert, and automated response.
- To identify who has, what permission to all files and folders.
- To quarantine possible ransomware attacks on your organization.

# Data discovery capabilities



- Finds personal data (also known as PII) stored in files, folders, or shares.
- Offers visibility into types of personal data (e.g. names, ages, credit card details, SSNs, and more).
- Track who accesses personal data, including when, where, and how the personal data is used.
- Keep personal data inventory updated using automated file discovery policies to scan at regular intervals.
- Streamlines compliance and personal data privacy requirements mandated by regulations such as GDPR, HIPAA, PCI, and more.



# Why you need Risk assessment (data discovery) component?

- To look for sensitive personal data (also known as PII) stored unbeknownst.
- To red flag presence of PII/PHI in unintended locations.
- To run a data vulnerability check
- To assess the risk of the data stored.

# Storage analysis capabilities

A decorative network diagram in the top right corner, consisting of various sized circles (nodes) connected by thin lines (edges). Some nodes are solid grey, while others are hollow white with a grey border. The connections form a complex, interconnected web.

- Identifies old, large, unmodified, non-business, stale, hidden, and other files to de-clutter your storage space.
- Offers insights on disk space utilization trend by analyzing storage space usage.
- Identifies who or what is eating up your storage space.
- Determines total file count based on user, file category, and file type.



A decorative network diagram in the top right corner, consisting of various sized circles (nodes) connected by thin lines (edges). Some nodes are solid grey, while others are hollow white with a grey border. The connections form a complex, interconnected web.

# To help you explore DataSecurity Plus we offer

- A fully functional 30-day trial period.
- An extended evaluation license, if needed.
- 24\*5 Technical support.
- An extensive knowledge base.



# DataSecurity Plus licensing details

- DataSecurity Plus has two components: file server auditing and data discovery.
- File server auditing includes storage analysis.
- One can purchase file server auditing and/or data discovery components as needed.
- Example: A customer can purchase the license to audit 5 file servers, and assess risks (data discovery) for 2 servers.

# DataSecurity Plus pricing

- Licensing for DataSecurity Plus is based on the number of file servers
- File server auditing component starts at \$745 per annum
- Risk assessment (data discovery) component starts at \$395 per annum



## What our customers are saying

“Information is a significant component of most organization's competitive strategy. Hence it needs to be preserved as securely as possible in our systems. Data Security Plus is a high valued solution to ensure the file system integrity, data loss prevention and it helps us to comply with regulatory standards.”

**- Phurich Leemekanont**  
**Acting Manager, IT**  
**Mubadala Petroleum**

# Supported Platforms

ManageEngine DataSecurity Plus supports Windows File Server 2003, and later versions.

Cluster Auditing supports Failover Clusters in Windows Server 2008 R2 and later versions.

Official Distributor:



[www.channel-it.com](http://www.channel-it.com)