

# Take charge of your sensitive data with **DataSecurity Plus**

Safeguard data at rest, in use, and in motion from theft, exposure, and leaks.



# Solutions offered by **DataSecurity Plus**



## File Server Auditing

Audit and report on all file accesses and modifications with real-time alerts and automated threat responses for high-risk file activities.



## File Analysis

Analyze disk space usage, manage junk data, identify at-risk data, analyze file permissions, and more by analyzing file security and storage.



## Data Risk Assessment

Discover and classify files containing sensitive personal data —such as PII or ePHI— based on their vulnerability using content and contextual information.



## Data Leak Prevention

Detect and prevent sensitive data leaks via USB devices, emails, web applications, printers, and more through real-time endpoint security monitoring.



## Cloud Protection

Track your organization's web traffic, scrutinize the use of shadow web apps, and enforce policies to block inappropriate or malicious web content.

Get **DataSecurity Plus** easily installed, configured and running within minutes.

[Download now](#)

Free, 30-day trial



# File Server Auditing with DataSecurity Plus

Annual plan starts at  
**\$745 for Windows file servers**  
**\$595 for NetApp CIFS servers**

[Download now](#)

Free, 30-day trial

[Learn more about File Server Auditing](#)

#### Supported environments:

Windows file servers, failover clusters, workgroups,  
and NetApp CIFS server environments



**Audit all file activities**, including create, delete, rename, and permission changes, along with details on who modified which file, when, and from where.



**Report on file copy-and-paste activities** when files have been copied by directly or remotely logging on to the file server.



**Ensure file integrity** by keeping track of unwanted file modifications and suspicious data transfers with real-time notification and response capabilities.



**Detect and stop ransomware attacks** in their tracks by quickly identifying their source and isolating malware-infected machines from the network.



**Track high-risk file activities**, such as repeated failed attempts to access critical files or sudden spikes in file permission changes.



**Expedite forensic analysis** using our extensive collection of accurate, audit-ready reports.



# File Analysis with DataSecurity Plus

Annual plan starts at \$95

[Download now](#)

Free, 30-day trial

[Learn more about File Analysis](#)

### Supported environments:

Windows file servers, failover clusters, and workgroup environments.



**Analyze disk space usage** and trigger alerts when free space falls below preconfigured values.



**Identify data hoarders** by scrutinizing the storage consumption rates of your employees over time.



**Manage ROT data**, i.e., find and purge duplicate, stale, non-business, and other unneeded junk data from your storage repositories.



**Delete duplicate files** and reclaim disk space. Compare file name, last modification time, and size to identify identical copies accurately.



**Find orphaned files** such as those owned by disabled, deleted, and expired users to reduce the risk of data theft.



**Analyze file security permissions** and understand who has what levels of access over your business-critical files.



**Identify at-risk data** such as files with broken or improperly inherited permissions, files corrupted by known ransomware variants, and more.



**Locate overexposed data**, i.e., files with open access to everyone and those with full control levels of permission.



**Gain insights into file storage** with details on file ownership, type, and location. Selectively track files that are currently open, hidden, and more.



# Data Risk Assessment with DataSecurity Plus

Annual plan starts at \$395

[Download now](#)

Free, 30-day trial

[Learn more about Data Risk Assessment](#)

**Supported environments:**

SMB-based shares and Microsoft  
SQL Server environments



**Discover sensitive personal data**—such as PII, ePHI, and PCI—using regular expressions and by matching keywords.



**Enable content-aware protection** by profiling business-critical data based on its calculated risk score.



**Use automated or manual classification** to tag sensitive files with predefined labels, i.e., Public, Internal, Restricted, and Sensitive.



**Identify and secure critical data** using predefined data discovery and classification rules, and comply with mandates like the GDPR, the CCPA, HIPAA, and the PCI DSS



**Enable proximity scanning** to reduce instances of false positives and increase accuracy in detecting business-critical information.



**Facilitate on-the-fly classification** by scrutinizing and cataloging files when they're created, modified, and more.



**Expedite your incident response** with options to move, delete, or quarantine sensitive data using custom scripts.



**Use incremental scans** to reduce the load on the CPU by scanning only new and modified files.



**Audit sensitive file activities** along with details on who accessed what file, which policies it violates, when, and from where.



# Data Leak Prevention with DataSecurity Plus

Annual plan starts at \$345

[Download now](#)

Free, 30-day trial

[Learn more about Data Leak Prevention](#)

#### Supported environments:

**Endpoints:** Windows client OS    **Applications:** Outlook

**Browsers:** Chrome, Firefox, Internet Explorer, and more

**Removable storage auditing and blocking:** USBs

**Virtual desktops:** Citrix and VMware (provided the OS installed is Windows 7 or above)

**Distributed machines:** Laptops and desktops

**Others:** Internal drives, printers, clipboards, network shares, Wi-Fi, and Bluetooth adapters



**Prevent data leaks** by detecting and disrupting the unauthorized flow of critical files via USB devices, email, printers, Wi-Fi, and more.



**Audit removable storage devices** and gain insight into who transferred what file to the device, when, and from where.



**Enforce external device control** by limiting the functions of USB devices such as denying read, write, or execute access.



**Enable file copy protection** to detect and disable high-risk file copy activities across local and network shares.



**Use application control** to obstruct employees from running malicious or non-vetted executables with block lists.



**Employ safe email practices** by scanning email attachments for confidential files and preventing users from sharing them.



**Trigger instant messages** using on-screen pop-ups to warn employees regarding possible data leak prevention policy violations (Outlook).



**Automate your incident response** by executing tailored scripts that can disconnect rogue users' sessions, shut down corrupted machines, and more.



**Use endpoint security monitoring** to detect sudden anomalies in data transfers and file access patterns.



# Cloud Protection with DataSecurity Plus

**\*Free add-on of the Data Leak Prevention module**

[Learn more about Cloud Protection](#)

#### Supported environments:

Cloud applications: Box, Dropbox, Microsoft 365 (OneDrive, Sharepoint, and Exchange Online), and more.

Network protocols: HTTP and HTTPS

Browsers: Chrome, Firefox, Internet Explorer, and more



**Audit web traffic** across your organization along with details on which website was accessed, when, and from where.



**Leverage the deep packet inspection** capability to examine web requests that contain encrypted parameters.



**Use cloud app discovery** to gain app, domain, and user-based insights on the accesses made by users in your network.



**Filter URLs** by sanctioning or banning apps directly from the report interface or by using custom parameters, thereby mitigating overall risk.



**Audit file uploads** made to various storage applications, including Microsoft 365, Google Workspace, Zoho Suite, and DropBox.



**Deploy Cloud DLP** policies to granularly block risky file uploads based on domains, URLs, application suites, and other parameters.



**Scrutinize shadow IT** cloud services based on the category of apps accessed and risk score, and correlate these insights with the top actors who use them.



**Block inappropriate domains**, such as social networking, e-commerce, and other low-reputed or productivity-draining sites deemed unsafe for your organization.



**Assess the reputation scores** of domains based on real-time data from integrated threat analytics, and ensure that only business-critical applications are sanctioned for use.



# ManageEngine DataSecurity Plus

A unified data visibility and security platform  
A two-pronged solution to fighting insider threats, preventing data loss,  
and meeting compliance requirements

**Download now**

Free, 30-day trial

## Contact information



### Website

[www.manageengine.com/data-security/index.html](http://www.manageengine.com/data-security/index.html)



### Personalized demo

[www.manageengine.com/data-security/demo-form.html](http://www.manageengine.com/data-security/demo-form.html)



### Pricing details

[www.manageengine.com/data-security/pricing-details.html](http://www.manageengine.com/data-security/pricing-details.html)



### Live demo

[demo.datasecurityplus.com](http://demo.datasecurityplus.com)



### Sales inquiries

[sales@manageengine.com](mailto:sales@manageengine.com)



### Tech support

[support@datasecurityplus.com](mailto:support@datasecurityplus.com)



### Toll-free

+1.408.916.9891

## Additional resources

Presentation

Architecture

Help center

Quick start guide

Resource center