ManageEngine
DataSecurity Plus

Compare
DataSecurity Plus editions

DataSecurity Plus is a unified data visibility and security platform that provides file auditing, file analysis, data risk assessment, data leak prevention, and cloud protection capabilities. Explore the differences between DataSecurity Plus' Free and Professional editions using the table below.

S.No	DataSecurity Plus capabilities	**Free edition** The edition with limited capabilities. Once the trial period for the Professional edition is over, without a valid license your instance will default to the Free edition.	**Professional edition** The fully-functional edition of DataSecurity Plus.
1.	**File server auditing** Audit and report on file accesses and modifications, with real-time alerts and automated responses for critical file activities.	Not supported. Only retains audit data from the evaluation period.	Pricing starts at $745 for 2 file servers. Get quote
1.1	**File access auditing** Report on all file accesses and modifications with detailed information on who did what, when, and from where.	NA	✓
1.2	**File copy auditing** Track file copy-and-paste activities across both local and shared files and folders.	NA	✓
1.3	**File integrity monitoring** Detect and respond to high-risk and suspicious file changes that could be ndicative of security threats.	NA	✓
1.4	**File change notifier** Trigger instant notifications upon sudden spikes in critical file activities like SACL, owner, or permission changes, file deletions, etc.	NA	✓
1.5	**Privileged user monitoring** Use custom reports to track file activities by administrators, privileged user accounts, and AD groups.	NA	✓

1.6	**Ransomware detection and response** Detect and disrupt potential ransomware attacks instantly with our automated threat response mechanism.	NA	✓
1.7	**Access pattern analysis** Gain insights into the most accessed files, most active users, most used processes, etc., by analyzing access patterns over time.	NA	✓
1.8	**Compliance-ready reporting** Use the multiple audit-ready reports to satisfy requirements mandated by regulatory standards like GDPR, PCI-DSS, HIPAA, etc.	NA	✓
1.9	**Forensic analysis** Use actionable, accurate audit data to track and identify the root cause of security incidents involving file misuse.	✓ using audit data from evaluation period	✓
2.	**File analysis** Analyze disk space usage, manage junk data, identify at-risk data, and analyze file permissions by analyzing file security and storage parameters.	Supported scanned data size: 500GB	Pricing starts at $95 for 1TB of scanned data. Get quote
2.1	**Disk space usage analysis** Track data growth trends and employees' disk usage patterns to find users who consume most of your storage space.	✓	✓
2.2	**File status reporting** Generate reports on files open currently, empty folders, active junction points, hidden files, active sessions, etc.	✓	✓
2.3	**File ownership analysis** Cross-analyze the riskiness of the files containing sensitive data with their owner details to identify high risk users, alarming data trends, and much more.	✓	✓
2.4	**Critically low storage space notifier** Trigger email alerts when free space within the storage drives falls below preconfigured values.	✓	✓
2.5	**Security permission reporting** Generate on-the-fly reports and find high-privileged users, effective permissions, and NTFS permissions over files and folders.	✓	✓

2.6	**ROT or junk data analysis** Find and manage redundant, obsolete, and trivial data in your data stores to reclaim wasted storage space.	✓	✓
2.7	**Duplicate file management** Find duplicate files by comparing their meta data, preview all copies, and deleted unnecessary instances from the UI.	✓	✓
2.8	**Orphaned file discovery** Find the list of all files and folders owned by inactive, disabled, or deleted users.	✓	✓
2.9	**Inactive file detection** Identify and analyze files that are old, stale, unmodified, hidden, etc.	✓	✓
2.10	**File permission hygiene diagnosis** List files and folders with broken permission inheritances and excessive access rights (such as Full Control).	✓	✓
2.11	**Ransomware-corrupted file management** Locate and delete files infected by ransomware using the pre-built library of known ransomware file types.	✓	✓
3.	**Data risk assessment** Discover and classify files containing sensitive data such as PII, PCI, and ePHI by combining content inspection and contextual analysis.	Supported scanned data size: 100GB	Pricing starts at $395 for 2TB of scanned data. Get quote
3.1	**Sensitive data discovery** Find all instances of sensitive data in your data repositories by matching with key phrases or regular expression patterns.	✓	✓
3.2	**Automated data classification** Classify files based on their sensitivity and vulnerability into custom parent and child abels created per your organization's requirements.	✓	✓
3.3	**Sensitive data analysis** Categorize and analyze files containing sensitive data by their owners, file type, source type, policies, and rules.	✓	✓

3.4	**User risk score calculation** Assign a risk score to all users by analyzing the sensitivity and vulnerability of the content owned by them.	✓	✓
3.5	**Built-in data discovery policies and rules** Use built-in, compliance-specific rules and policies to find data governed by regulatory standards like the GDPR, PCI-DSS, HIPAA, etc.	✓	✓
3.6	**Data ownership analysis and notifier** Use instant email notifications to alert data owners of the presence of vulnerable, sensitive data owned by them.	✓	✓
3.7	**Sensitive data confidence level estimator** Use the confidence level filters—i.e. high, medium, and low—to indicate the reliability of the sensitive data instances.	✓	✓
3.8	**File type recognition** Scan sensitive content from over 50 file types, including email, text, compressed, and more.	✓	✓
4.	**Data leak prevention** Detect and disrupt data leaks via USBs, email, web applications, and printers through real-time endpoint file activity monitoring.	Supported number of workstations: 50	Pricing starts at $345 for 100 workstations. Get quote
4.1	**Content-aware protection** Use file classification labels to secure files containing sensitive data across: **Distributed machines:** laptops and desktops **Applications:** Outlook **Removable storage:** USB, SD cards, etc. **Virtual desktops:** Citrix, VMWare (provided the OS installed is Windows 2003 or above). **Browsers:** Chrome, Firefox, Internet Explorer, etc. **Others:** Printer, clipboard, fax, network shares, Wi-Fi, and Bluetooth adapters.	✓	✓
4.2	**Endpoint security monitoring** Detect file access and data transfer anomalies in endpoints to ensure file integrity.	✓	✓
4.3	**File copy protection** Stop data theft attempts by restricting the use of clipboards, which blocks file copy actions across network shares, local files, and USBs.	✓	✓

4.4	**Application control** Track the use of applications and restrict the use of suspicious and high-risk executables by adding them to blocklists.	✓	✓
4.5	**External device control** Limit various functionalities within USB devices by denying read, write, and execute access.	✓	✓
4.6	**USB blocking** Regulate the use of removable storage media by adding high-risk and unvetted USB devices to the blocklist.	✓	✓
4.7	**Email attachment data leak protection** Instantly detect and block emails (Outlook) containing classified files as attachments from being sent.	✓	✓
4.8	**Printer auditing** Monitor local print server usage and generate reports with details on who printed what and when.	✓	✓
4.9	**Web browser auditing** Analyze potential file uploads and downloads by tracking all file activities initiated by web browser processes.	✓	✓
4.10	**Removable storage auditing** Generate detailed reports on all USB file actions and track file transfers with details on who did what, from where, via which device, etc.	✓	✓
4.11	**Manual data classification** Admins and data owners can tag sensitive files with predefined labels such as Public, Private, Confidential, or Restricted.	✓	✓
4.12	**Incident response policies** Respond to security events detected by quarantining infected devices, disabling rogue user accounts, moving vulnerable files to secure locations, etc.	✓	✓
4.13	**End-user education and awareness** Use on-screen pop-up messages to inform or warn employees regarding unsafe file transfer actions that could result in data leakage.	✓	✓

5.	**Cloud protection (Free Data Leak Prevention module add-on)** Track your organization's web traffic, scrutinize the use of shadow apps, and enforce policies to block inappropriate and malicious cloud applications.	Not supported. Only retains audit data from the evaluation period.	Unlimited
5.1	**Cloud application discovery** Audit your organization's web traffic and gain insights into the cloud apps in use, their reputation, app category, etc.	NA	✓
5.2	**Content and URL filtering** Block your employees from accessing malware-infested and productivity-draining cloud applications.	NA	✓
5.3	**Shadow web app discovery** Closely track the use of shadow web apps—i.e. un-vetted web services—to find the top actors who access them and analyze the risk posed by these services.	NA	✓
5.4	**Low-reputed cloud app analysis** Find and scrutinize the use of unreliable and high-risk cloud applications by analyzing their history, age, underlying URLs, etc.	NA	✓
5.5	**Deep packet inspection** Inspect your network traffic by reading through the contents of your encrypted data packets.	NA	✓
5.6	**File upload monitoring** Report on upload requests made across SharePoint, OneDrive, Exchange, Box, and DropBox, as well as Zoho applications like Cliq, WorkDrive, Sheet, Writer, Projects, and more.	NA	✓
5.7	**Web request tracking** List both successful and failed plain HTTP requests made.	NA	✓

*The features and capabilities available to Free edition users are subject to change and may be revised without notice by DataSecurity Plus.