ManageEngine
DataSecurity Plus

Take charge of your sensitive data with DataSecurity Plus.

Discover, monitor, and protect sensitive data from being exposed or stolen.

www.datasecurityplus.com

Solutions offered by DataSecurity Plus

File server auditing

Audit, report, and alert on all file accesses and modifications made in your file servers, failover clusters, and workgroup environments in real time.

Data leak prevention

Detect, disrupt, and respond to sensitive data leaks via endpoints, i.e., USBs, email, and more through security monitoring.

Data risk assessment

Leverage in-depth content inspection and manual tagging capabilities to discover sensitive data and classify files based on their vulnerability.

File analysis

Gain in-depth visibility into data stores to locate at-risk data, and manage inactive data to reduce data storage costs with detailed reports on file metadata, junk files, and server storage.

File server auditing with DataSecurity Plus

Audit file and folder access and obtain detailed information on the four W's—who accessed what, when, and from where—for all file accesses and modifications.

Detect and shut down potential ransomware attacks at their inception with an automated threat response mechanism.

Trigger instant alerts on sudden spikes in file or folder access, modification, or permission change event.

Report and alert on file copy-and-paste to events in real time using predefined policies.monitoring.

Track and analyze failed access attempts made by suspicious users before they snowball into critical security issues.

Perform forensic analysis using actionable, accurate audit data for all anomalous file events.

Supported environments: Windows file servers,failover clusters, and workgroups.

ManageEngine
DataSecurity Plus

Data leak prevention

with DataSecurity Plus

Monitor, track, and analyze when sensitive data (PII/ePHI) is modified by users, copied to or from workstations, and more.

Send instant alerts to data owners, sysadmins, or your IT security team in the event of policy violations.

Create user awareness with custom pop-up messages for policy violations that include unwarranted file movements via email.

Real-time security monitoring for a wide range of file events to ensure the integrity of local files.

Block, delete, and quarantine files, or choose any other predefined active remediation available to prevent data leaks.

Applications: Outlook.

Removable storage: USBs, SD cards, cameras, mobile phones etc.

Virtual desktops: Citrix, VMware (provided the OS installed is Windows 2003 and above).

Distributed machines: Laptops, desktops.

Others: Print, clipboard, fax, network shares.

ManageEngine
DataSecurity Plus

Data risk assessment

with DataSecurity Plus

Find, analyze, and track sensitive personal data—also known as PII/ePHI—stored in file server and failover cluster environments.

Detect high-risk data using specific keywords and regular expressions, or use a predefined combination of the two to reduce false positives.

Automate incident response with predefined remediation options including block, delete, and quarantine.

Single web-based console to create and define your own policies and rules, respond to critical incidents, report file events, and more.

Simplify data classification with both automated and manual file tagging capabilities to reduce the burden on the admin.

Use incremental scans to reduce the runtime by scanning only new or modified files.

Scan sensitive content from more than 50 file types including email, text, compressed, and more.

Streamline compliance using predefined policies for various external mandates including GDPR, PCI DSS, HIPAA, and SOX with more than 50 rule templates.

ManageEngine
DataSecurity Plus

File Analysis with DataSecurity Plus

File analysis helps analyze, identify, and discard junk data to declutter storage space.

Manage ROT data by finding and purging redundant, obsolete, and trivial (ROT) data, duplicate files, and more.

Optimize disk space usage by analyzing growth trends and disk usage patterns, and generate alerts when free space falls below a pre-configured limit.

Examine security permissions to identify overexposed files, analyze who has access to your sensitive files, and more.

Review file permissions to capture files with inconsistent permissions and files accessible by everyone to help reinforce role-based user privileges.

Locate and manage non-business files like videos, images, and other personal files belonging to employees along with hidden files that need to be filtered out of your file servers.

Drill down and analyze data volume, disk space status, and junk files at the domain, server, or drive level all in one central dashboard.

Track harmful ransomware-infected files using our predefined library of over 50 ransomware file types to help eliminate them from your file servers.

Track all the shares from your file server with share size details and share paths locations to help optimize file sharing resources.

DataSecurity Plus system requirements
Supported browsers: Firefox, Google Chrome, Microsoft Edge
Supported server OS: 2003 R2, 2008, 2008R2, 2012, 2012 R2, 2016
Supported client OS: Windows XP, Vista, 7, 8, 8.1, 10
Processor: 2.0GHz
RAM: 8GB
Disk space: 20GB
For complete system requirements of DataSecurity Plus, visit our support page.