ManageEngine
DataSecurity Plus

A unified data security posture management platform

- File Audit
- File Analysis
- Data Risk Assessment
- Data Leak Prevention
- Cloud Protection

ManageEngine
DataSecurity Plus

AGENDA

Data security: Need of the hour

Exponential data growth: Control over data usage and proactive data management is essential to reduce expenses and optimize storage efficiency

Advanced threats to sensitive data: Increasing data breach incidents necessitate a content-aware data loss prevention measure that can locate and protect vulnerable, sensitive files

Complying with regulations: An automated data-centric audit and protection approach can help organizations meet compliance requirements

About DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data security posture management platform. It provides a host of capabilities, including:

- File server auditing and file integrity management
- Ransomware detection and response
- Security incident response
- File and security permission analysis
- Data discovery and classification
- File copy protection
- Endpoint and cloud data leak prevention
- Cloud application protection

Solutions offered

DataSecurity Plus comprises of the below modules:

File Audit

Report, analyze, and alert on file accesses and modifications in real time

File Analysis

Analyze file storage, monitor disk space usage, and examine security permissions to locate junk data and security vulnerabilities

Data Risk Assessment

Discover and classify files containing sensitive data (PII, PCI, and ePHI)

Solutions offered

Data Leak Prevention

Detect and disrupt sensitive data leaks via endpoints (USBs, email, etc.)

Cloud Protection

Audit your organization's web traffic to track and control the use of high-risk web applications

Highlights of

File Audit

Highlights of File Audit

Audit file and folder access: Track file read, create, modify, move, delete, copy, paste, etc. to learn who did what, when, and from where

Monitor file integrity: Detect critical events like file changes after business hours, user activity in sensitive files, and multiple failed access attempts

Receive real-time change alerts: Alert admins to unauthorized or unusual file changes, and automatically execute custom scripts to shut down attacks

Shut down ransomware attacks: Detect and respond to ransomware attacks with an automated threat response mechanism

Comply with regulatory mandates: Meet the requirements of multiple IT regulations like PCI DSS, HIPAA, GDPR, FISMA, GLBA, and more

Highlights of

File Analysis

Highlights of File Analysis

Manage ROT data: Find and delete redundant, obsolete, and trivial files to reduce expenditure on storage

Delete duplicate files: Locate duplicate files by comparing file names, sizes, and last modification times, and delete the unnecessary copies to free up primary storage

Analyze disk space usage: Track disk space consumption, and receive alerts on critically low disk space to ensure business continuity

Examine file permissions: Analyze NTFS permissions and detect security vulnerabilities like broken inheritances and files owned by dormant users

Detect overexposed files: Detect files with excessive permissions such as those accessible by every user or allow unrestricted access

Highlights of

Data Risk Assessment

Highlights of Data Risk Assessment

Discover sensitive data: Scan enterprise storage for passport numbers, email addresses, credit card numbers, and over fifty other types of personal data

Analyze trends in PII storage: Receive reports on the volume, type, and trends in the storage of sensitive data

Detect storage policy violations: Instantly detect data that violates enterprise storage policies and respond by executing custom script

Analyze file sensitivity and vulnerability: Analyze the risk associated with files by viewing details on the amount and type of personal data they contain and who can access them

Classify sensitive files: Classify files containing PII, PCI, or ePHI to better understand which files need elevated data security measures

Highlights of Data Risk Assessment

- **Avoid non-compliance:** Avoid the risk of non-compliance penalties by generating periodic reports on the location and amount of sensitive data stored in your environment
- **Leverage incremental scanning:** Scan only new and recently modified files to reduce data discovery scan times
- **Examine file security:** Identify employees who can access files containing personal information
- **Analyze risk scores:** Assess the vulnerability of personal data with an evolving risk score, assigned based on its content, ownership, and more

Highlights of

Data Leak Prevention

Highlights of Data Leak Prevention

- **Audit file activity in endpoints:** Audit file accesses across your Windows workstations in real time
- **Classify endpoint data:** Classify files based on their sensitivity as Public, Internal, Confidential, or Restricted
- **Enable content-aware protection:** Closely monitor who owns and accesses sensitive data. Execute instant responses when threats to this data are detected
- **Monitor removable devices:** Audit and control the use of removable storage media and all sensitive data transfer activities to them
- **Prevent data leaks via USBs:** Lock down peripheral ports in response to malicious user behavior to prevent potential data leaks

Highlights of Data Leak Prevention

- **Block data exfiltration via email:** Block files with highly sensitive data—such as PII or ePHI—from being moved via email (Outlook)
- **Automate incident response:** Delete or quarantine files, block USB ports, or choose from other predefined remediation options to prevent data leaks
- **Audit printer usage:** Track and analyze who printed what files and when
- **Control the use of applications:** Create allow and block lists to exercise granular control over which applications can be used by employees.
- **Prevent file copy actions:** Track attempts to copy critical files across local and network shares and block unwarranted file transfers.

Highlights of

Cloud Protection

Highlights of Cloud Protection

- **Track cloud application usage:** Monitor your organization's web traffic to analyze which websites were accessed, when, from where, and by whom

- **URL filtering:** Prevent your employees from accessing unproductive, risky, or unnecessary cloud applications

- **Assess the threat of shadow IT:** Spot employees who are putting your organization at risk with their use of shadow cloud applications

- **Audit file uploads:** Monitor file uploads made to various storage applications, including Microsoft 365, Google Workspace, and DropBox

Highlights of Cloud Protection

Deploy Cloud DLP policies: Granularly block risky file uploads based on domains, URLs, application suites, and other parameters.

Assess domain reputation scores: Use real-time data from integrated threat analytics to ensure that only business-critical applications are sanctioned for use.

How DataSecurity Plus stands out

One-stop solution: It is an integrated, all-in-one software for sensitive data visibility and security for data at rest, in use, and in motion.

Enhanced data protection: It includes a vast array of user activity monitoring and data loss prevention capabilities to protect your data from insider threats, ransomware, theft, exfiltration via endpoints, and more

Compliance reporting: It can generate comprehensive reports using predefined templates to demonstrate compliance with the GDPR, HIPAA, the PCI DSS, and more

Meet organizational needs: It offers an intuitive dashboard and quick deployment, and it is scalable and customizable

Licensing details

File Audit

Licensed based on the number of file servers. Users also get 1TB free File Analysis capabilities for every licensed server.

File Analysis

Licensed based on data size in Terabytes.

Data Risk Assessment

Licensed based on data size in Terabytes.

Licensing details

Data Leak Prevention

Licensed based on the number of endpoints.

Cloud Protection

Free add-on of the Data Leak Prevention module.

Supported environments

File Audit

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

File Analysis

Windows file servers, failover clusters, and workgroups

Data Risk Assessment

SMB-based shares and Microsoft SQL servers

Supported environments

Data Leak Prevention

Endpoints: Windows client OS

Application: Outlook

Browsers: Chrome, Firefox, and Microsoft Edge

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

Supported environments

Cloud Protection

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

Network protocols: HTTP and HTTPS

Browsers: Chrome, Firefox, and Microsoft Edge

How we aid your evaluation

- A fully functional 30-day, free trial
- Extension of evaluation license, if needed
- 24x5 technical support
- An online demo hosted at demo.datasecurityplus.com
- An extensive knowledge base

Our customers

"DataSecurity Plus provides insight into the types of data being stored on our servers so we can better protect it"

Rosemarie Deronne,

Systems engineer, Eastern Virginia Medical School

"DataSecurity Plus is a high-valued solution that ensures file system integrity and data loss prevention, and it helps us comply with regulatory standards"

Phurich Leemakanot,

Mubadala Petroleum

Contact us

Telephone:

+1.925.924.9500

Live chat:

For instant responses

Email the support team:

support@datasecurityplus.com

Visit our website:

www.datasecurityplus.com

Email the support team:

ZOHO Corporation,
4141 Hacienda Drive,
Pleasanton, CA 94588, USA

Download now