ManageEngine
DataSecurity Plus

Perfecting your DLP strategy

A guide to developing an effective data loss prevention plan

www.datasecurityplus.com

Table of contents

1. Introduction

A 2018 study by Igneous found that, for a typical organization, unstructured data grows 23 percent annually, which means that every 40 months, it will double in size. In the same research, around one-fourth of the companies studied cited data growth rates of over 40 percent, meaning their total unstructured data doubled every two years.

Considering this exponential growth of data, enterprises need an easy way to continuously categorize, evaluate, and secure their ever-growing data stores. This need is compounded by the fact that most of this data is likely to be confidential, personally identifiable information, or some other form of sensitive data that has to be protected at all costs.

However, are enterprises capable of ensuring data protection on a large scale?

In this new era of integrated cybersecurity software, the need of the hour is to take a close look at all available solutions to identify the best way to protect data. After all, one size does not fit all, and clinging to antiquated approaches to data protection is never advisable.

As data proliferates, traditional data protection software has taken a step back to allow comprehensive data loss prevention solutions to take their rightful place: Spearheading every CISO's objective of ensuring complete visibility and security of data at rest, in use, and in motion.

1.1 The "risk acceptance" approach to data security

68 percent of business leaders feel their cybersecurity risks are increasing. - Accenture

The average time to identify a breach in **2019 was 206 days** - IBM

IT security today is no longer just about preventing attacks, nor about totally blocking threats from popping up. The best way to describe the mindset of CISOs today is **risk acceptance.**

After all, with evolving trends in cyber theft, avoiding breaches is virtually impossible. Once enterprises accept that they are either already under attack, or could be attacked by cybercriminals at any time, they can focus on what should be done next to safeguard their critical data.

By anticipating an attack around every corner and preparing for different types of scenarios, enterprises won't be caught off guard when an attack does get through their defenses. Instead, they'll be prepared to face and mitigate the damage that a breach can cause to their data stores.

1.2 What is data loss prevention?

Data loss prevention (DLP) is the process of identifying, classifying, cataloging, monitoring access to, and controlling the use of business-critical data, with the aim of ensuring that it does not leave the network without due authorization. The rise of sophisticated cyberattacks and data security threats, combined with the establishment of stringent data security norms and regulations, has heightened the importance of adopting DLP practices and tools.

Traditional data protection methods have a narrow approach with siloed data visibility and security software that impedes the correlation between the context of data and access details. A necessary component of effective data loss prevention strategies, this correlation is integrated within DLP software and given due importance by data loss prevention strategies.

1.3 Capabilities of data loss prevention software

Implementing DLP software can provide insight into how stakeholders use enterprise data. To protect sensitive information, organizations must first know that it exists, discover where it exists, and ascertain who uses it and for what purposes. Furthermore, the software should be capable of controlling the use of sensitive data, and protecting it from external attackers and insiders alike.

A comprehensive DLP solution can:

Discover sensitive personal data
such as personally identifiable information and electronically protected health information (PII and ePHI) stored across enterprise storage repositories.

Assess the risks
associated with the data by analyzing permissions, storage location, data type, and more.

Classify and catalog files
containing PII and ePHI to enable admins to control the movement of data across file servers and endpoints.

Monitor user activity
in files containing sensitive and classified information, and alert administrators to suspicious activities.

Detect the movement of restricted files
to external storage devices and web applications.

Prevent data leaks
by utilizing tailored DLP policies to detect and block harmful file transfer attempts.

Apart from these, best-in-class DLP tools can also provide detailed reports for proving compliance with current and evolving regulatory mandates, such as the GDPR, PCI DSS, HIPAA, ISO 27001, SOX, CCPA, and more.

2. Choosing the right DLP tool

On average, only five percent of companies' folders are properly protected. - Varonis

Cybercrime will cost the world **$6 trillion** annually by 2021. - Cybersecurity Ventures

Some DLP software is notoriously complex for the basic use cases faced by small and medium-sized enterprises (SMEs). Gartner's analysts reiterated this, and went on to emphasize the importance of considering certain key factors when choosing DLP software.

Decision makers must account for company size, the volume of data stored, existing software, applicable regulatory requirements, business objectives, and human and financial resources available for operating and maintaining the DLP solution. With careful consideration, enterprises can avoid purchasing and installing software that ultimately ends up being ineffective or a bad fit.

Of all the factors to take into account, here are the three main metrics to consider when choosing a DLP tool.

2.1 Identify the data that needs the most protection

Understanding the type, content, and context of the data stored, and gaining insights into the level of protection required is the first step of evaluation. To protect critical data, security officers need to locate it, monitor who accesses it, and control how and where it is used.

With a comprehensive DLP solution, they can discover and auto-classify sensitive data across enterprise storage. It can also provide deep visibility into data usage and movement, with information on employees' access trends. In turn, this will aid in better understanding the level of protection needed, where safeguards need to be applied, as well as identify any deficiencies in existing data security processes.

2.2 Flexibility of provided DLP policies

Most DLP solutions have a multitude of built-in data loss prevention policies. However, decision makers must analyze whether these are in fact helpful and capable enough to protect an enterprise's most vulnerable gateways of data theft: endpoints.

The DLP software should be capable of monitoring all file activity in endpoints and external ports, tracking copy-and-paste actions, detecting unwarranted data transfers, and instantly halting attempts to exfiltrate sensitive data via USBs and printers. Employees must be given the confidence to handle sensitive data securely, with a combination of educative on-screen prompts about actions violating data use policies and a list of available active response actions.

Further, these policies must allow CISOs to tailor them based on the enterprise's needs and wants, and the software must allow the creation of additional policies for highly-specific use cases.

2.3 Resources needed for software deployment

DLP tools are much more than just an expensive green tick on a compliance checklist. The price tags of many highly-reviewed DLP vendors are often beyond the means of SMEs, because they also have to factor in the costs associated with the time and manpower required to choose, deploy, and maintain the software.

When choosing the software, decision makers must analyze the ease of implementation, operation, and maintenance; what level of training is provided by the vendor; and whether the tool is easy to tune to the enterprise's needs.

By taking these three key criteria into the decision-making process, CISOs can identify the best data loss prevention software faster, and analyze its effectiveness in meeting their needs.

3. Developing a DLP strategy

Building an effective data loss prevention strategy starts with the best practices listed below.

Deploy your DLP solution in phases

Before deployment, list and prioritize all the files that need to be protected. Create a timeline to ensure that deployment is completed in phases. Trying to implement DLP measures across endpoints, the cloud, and servers all at once leads to an enormous amount of false positives, which can quickly lead to alert fatigue.

Start off with data discovery and classification

Knowing what data needs to be protected and where it lies is the first step of DLP. Data discovery and classification capabilities provide visibility into sensitive data storage and the protection measures associated with it. Once categories are put in place, DLP solutions can operate on the classified content.

Create, fine-tune, and update your risk policies

Perform tests during your initial deployment using a small subset of policies to build a baseline, and then expand from there. Fine-tune risk profiles, policies, and rules regularly to reduce false positives, enhance effectiveness, and realign with changing business needs.

Record all identified incidents

Maintain clear, concise documentation of all violated policies and detected incidents. Use an informative dashboard to analyze top data loss incidents, risk scores, and security incidents, and employ appropriate active or passive remediation.

Run tests with a DLP endpoint agent

Before implementing the solution across the organization, perform in-depth tests with your DLP endpoint agent to ensure that it is properly configured, performs to your satisfaction, runs policies as per your requirements, and is compatible with the existing workstation applications.

Integrate with cloud access security brokers

Identifying and protecting sensitive information on cloud applications is also an essential part of an effective DLP solution. Integrating cloud access security brokers (CASB) with your DLP solution extends data security to cloud platforms as well.

4. Enriching your DLP approach

With the information on hand about the downfalls of using multiple software and with DLP in mind as the endgame, here are the key takeaways.

4.1 The advantages of deploying comprehensive DLP software

The primary lessons learned by CISOs in their journey towards identifying the best data loss prevention tools are:

- Data risk assessment and DLP are not mutually exclusive.
- File auditing and DLP are not mutually exclusive.

Combining the capabilities of data visibility and data security tools within a DLP software gives organizations the upper hand in identifying threats, and reacting to them rapidly with greater precision.

4.2 Get the DataSecurity Plus advantage

As always, ManageEngine aims to cater to all these needs with comprehensive DLP software, DataSecurity Plus. It provides file auditing, file integrity monitoring, ransomware detection and response, security incident response, data discovery, data classification, and DLP capabilities, and is truly a one-stop solution to ensure that your organization's data remains secure within your network.

5. Data loss prevention with DataSecurity Plus

With the combined capabilities of file analysis and data risk assessment, you can identify sensitive data, assess all associated information, and analyze whether it's at risk due to storage location, ownership, or assigned security permissions. Then, implement a data classification process to tag data with contextual information such as the type of data it is, its sensitivity, its level of confidentiality, and how valuable it is to your organization.

With this contextual information in hand, you can implement appropriate security controls to protect the data from accidental changes, deletions, and theft. This will ensure compliance with various privacy and security mandates, and also prove that all of your data is safe within your network, thereby meeting the objectives of the DLP process.

ManageEngine's comprehensive data loss prevention offering, DataSecurity Plus, can:

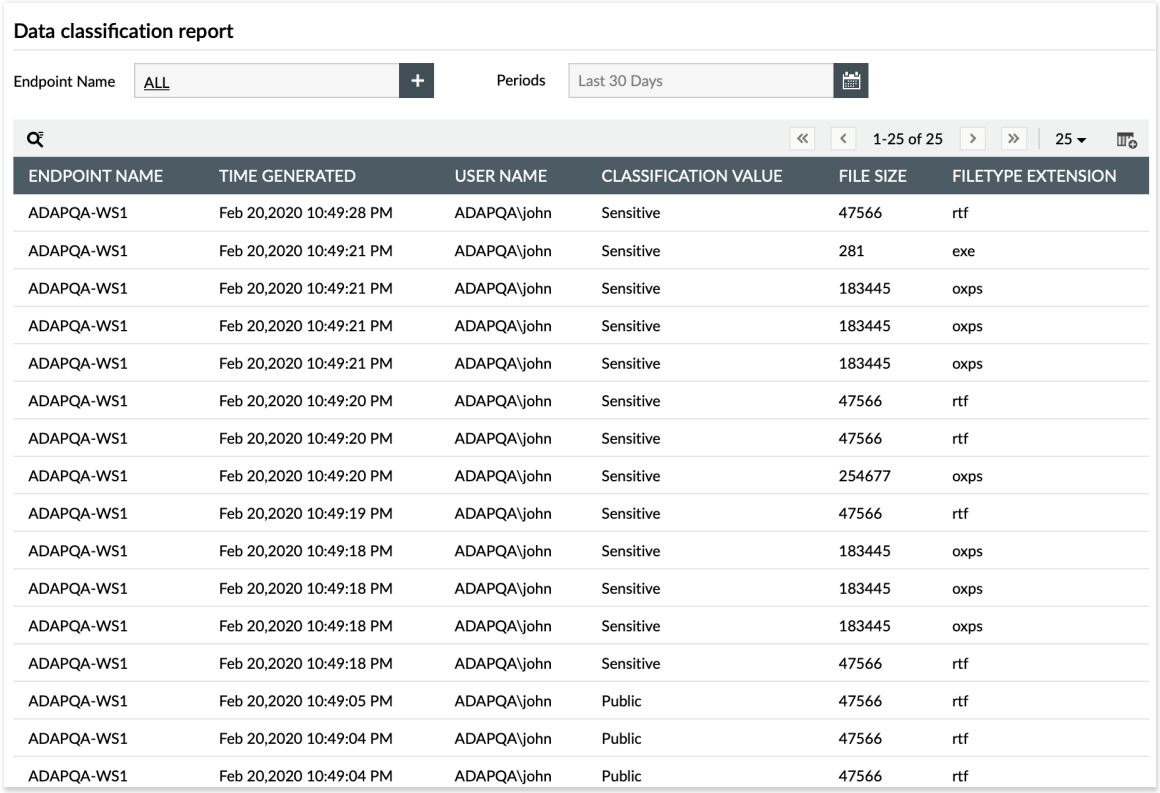
Discover sensitive data

- Scrutinize Windows file server and failover cluster environments for PII, PCI, and ePHI using the data discovery tool.
- Receive reports on the volume, type, and trends observed in the storage of sensitive data.
- Search for passport numbers, email addresses, credit card numbers, and numerous other types of personal data with preconfigured and customizable data discovery policies.
- Scan across multiple file types, including email, text, compressed, and more.
- Create and maintain an inventory of your organizations' most sensitive data by scheduling data discovery scans at regular intervals.

Classify sensitive files

- Analyze the risk associated with files by viewing details on effective permissions, ownership, file location, and more.
- Manually classify files containing personally identifiable information (PII) and electronically protected health information (ePHI) with data classification software.

- Automate the classification of files with high risk scores to better understand which files need elevated data security measures.
- Catalog sensitive files in workstations, and prevent data exfiltration via Outlook emails, web applications and external storage media.



Data classification report

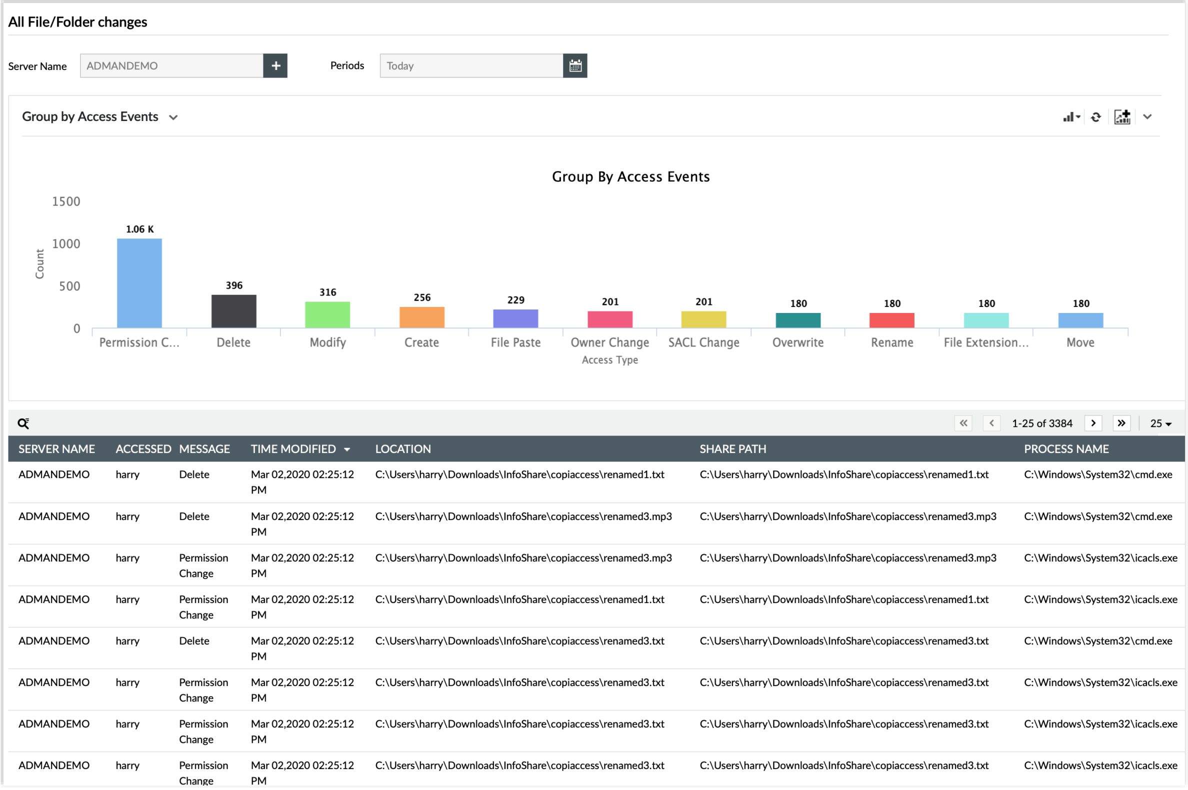
Endpoint Name: ALL | Periods: Last 30 Days

1-25 of 25 | 25

ENDPOINT NAME	TIME GENERATED	USER NAME	CLASSIFICATION VALUE	FILE SIZE	FILETYPE EXTENSION
ADAPQA-WS1	Feb 20,2020 10:49:28 PM	ADAPQA\john	Sensitive	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:21 PM	ADAPQA\john	Sensitive	281	exe
ADAPQA-WS1	Feb 20,2020 10:49:21 PM	ADAPQA\john	Sensitive	183445	oxps
ADAPQA-WS1	Feb 20,2020 10:49:21 PM	ADAPQA\john	Sensitive	183445	oxps
ADAPQA-WS1	Feb 20,2020 10:49:21 PM	ADAPQA\john	Sensitive	183445	oxps
ADAPQA-WS1	Feb 20,2020 10:49:20 PM	ADAPQA\john	Sensitive	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:20 PM	ADAPQA\john	Sensitive	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:20 PM	ADAPQA\john	Sensitive	254677	oxps
ADAPQA-WS1	Feb 20,2020 10:49:19 PM	ADAPQA\john	Sensitive	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:18 PM	ADAPQA\john	Sensitive	183445	oxps
ADAPQA-WS1	Feb 20,2020 10:49:18 PM	ADAPQA\john	Sensitive	183445	oxps
ADAPQA-WS1	Feb 20,2020 10:49:18 PM	ADAPQA\john	Sensitive	183445	oxps
ADAPQA-WS1	Feb 20,2020 10:49:18 PM	ADAPQA\john	Sensitive	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:05 PM	ADAPQA\john	Public	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:04 PM	ADAPQA\john	Public	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:04 PM	ADAPQA\john	Public	47566	rtf

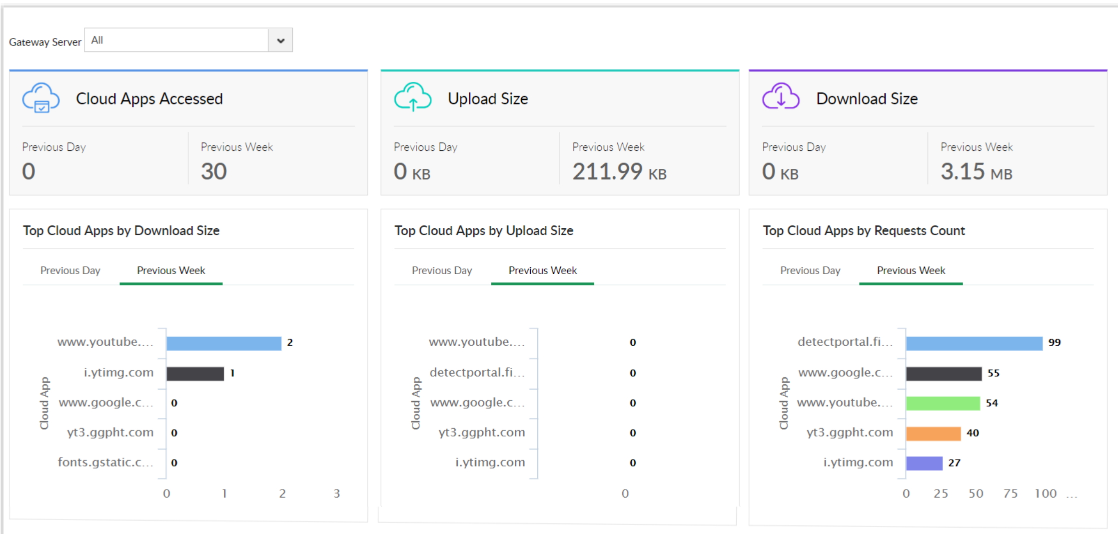
Monitor user activity

- Audit file servers and report on users accessing files to know the who, what, when, and where behind all critical file activity.
- Drill down into events that matter most, such as sudden permission changes, copy-and-paste events, file deletions, and renaming events.
- Verify the integrity of critical files with real-time reports on suspicious file activity.
- Trigger instant alerts whenever there is a sudden spike in file or folder access or modification events, or multiple failed access attempts.
- Detect ransomware attacks using threshold-based alert profiles and an up-to-date library of known ransomware file types. Execute custom scripts to shut down infected machines and halt the progress of the malware, thereby mitigating damage.



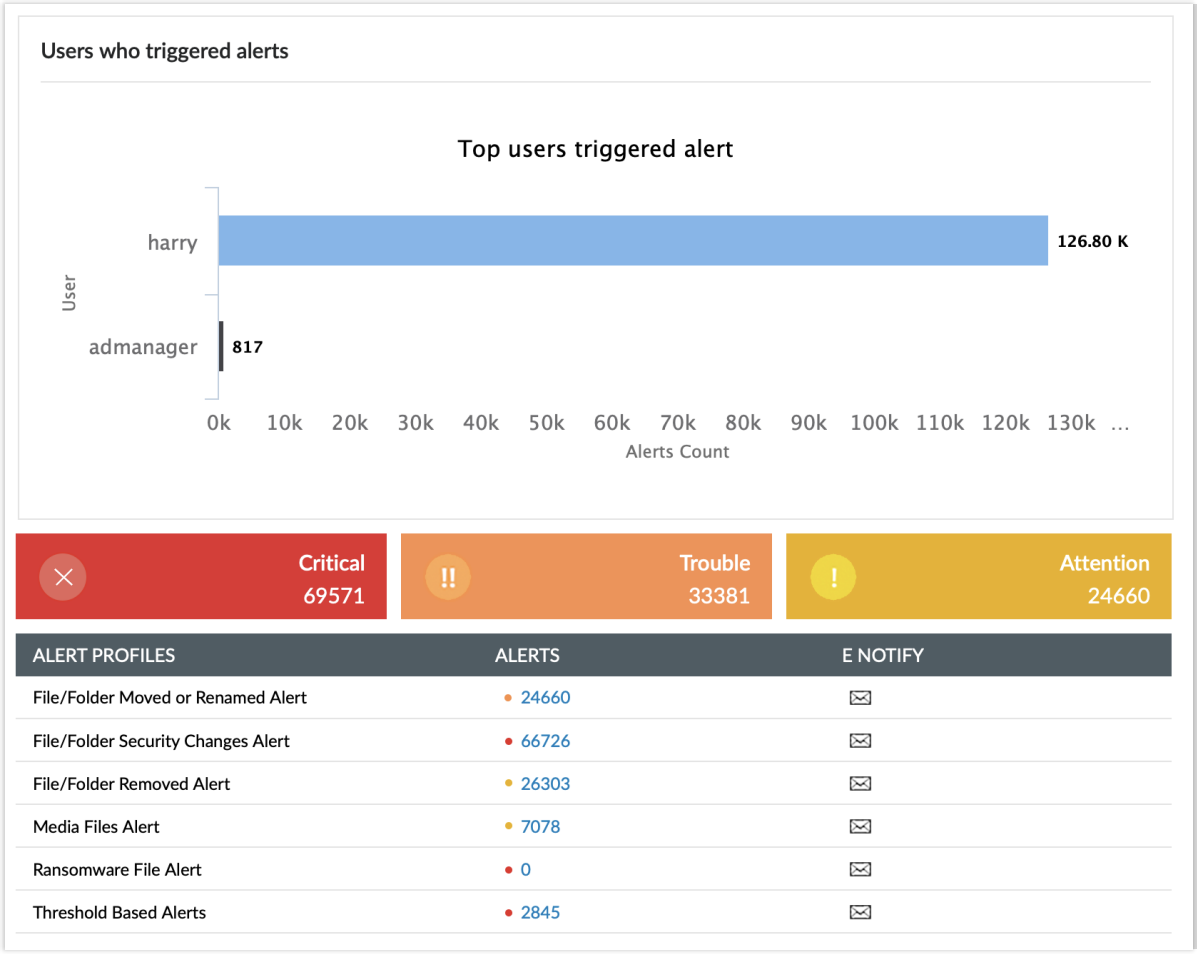
Enable cloud protection

- Audit your organization's web traffic to track the use of high-risk applications.
- Implement centralized control over the use of sanctioned and unsanctioned applications.
- Control user activities across millions of harmful websites, and block them from visiting harmful or dark sections of the web.
- Track and analyze which of your enterprise's sensitive resources are uploaded to the cloud.



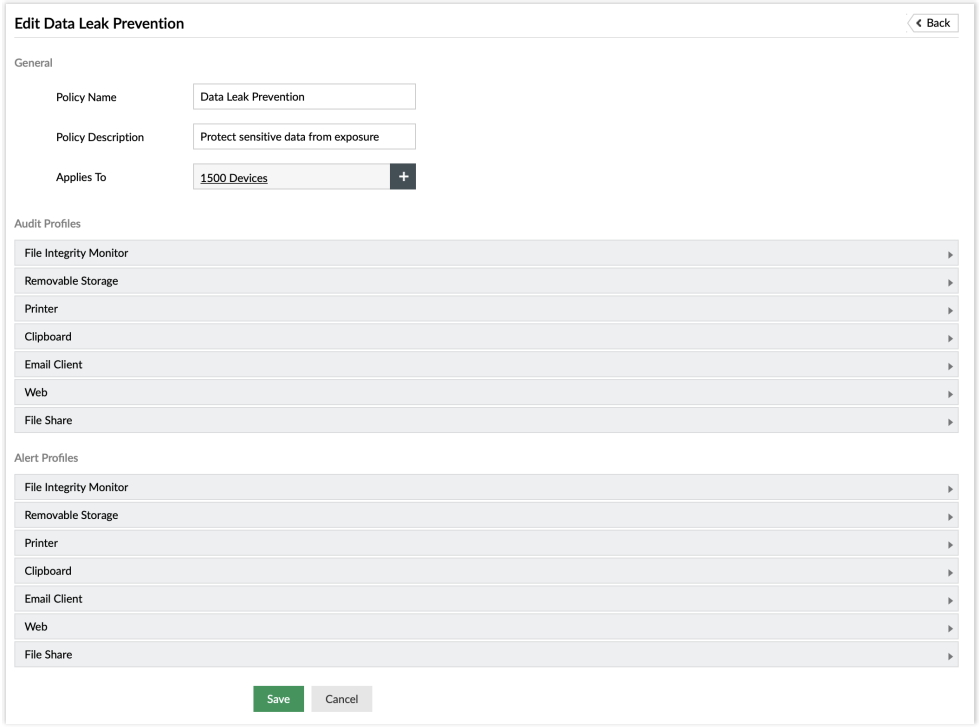
Detect security threats

- Reduce the surface area of attacks by detecting permission vulnerabilities like broken inheritances, files allowing unrestricted access, and more with file analysis.
- Minimize noncompliance risk by correlating storage analysis and data discovery to uncover sensitive data that has been stored beyond its limitation period.
- Get real-time alerts for suspicious file access events and unusual user activity such as files accessed after an extended period of inactivity, or during non-business hours.
- Notify admins about critical file changes, and automate responses to security threats such as ransomware intrusions and file copy actions.
- Monitor suspicious users, important files, and unsecured locations for unauthorized file activity.



Prevent data leaks

- Set up and start securing your data easily with the data loss prevention tool's built-in alerting and response policies.
- Monitor file activity in removable storage media and disrupt sensitive data transfers to USB drives.
- Monitor Outlook attachment activity and block users from attaching critical business data to emails.
- Use on-screen pop-up messages to warn employees about data usage policy violations.
- Handle critical policy violations using custom scripts and a host of available remediation options for deleting or quarantining files and blocking file transfers.



Comply with regulations

- Address the requirements of PCI DSS, HIPAA, GDPR, SOX, CCPA, and other regulations with real-time compliance reporting.
- Set up report subscriptions to receive periodic, audit-ready reports on file activity, sensitive data storage, detected security incidents, and more.
- Identify the root cause of security incidents using forensic data, and generate clear and concise audit trails to ensure accountability for all file activity.

6. Conclusion

Data loss prevention is a continuous process that is enriched when the right tools, procedures, and management are put in place. Reiterating the facts discussed earlier, one size does not fit all, and considerable care, caution, and time should be taken while choosing DLP software. By doing so, CISOs can make an informed decision, and also take full advantage of the chosen software's capabilities to effectively protect their enterprise data against internal and external attacks.

Next steps

- **Free trial**
  Set up and evaluate DataSecurity Plus's capabilities with a free, fully functional 30-day trial.
- **Interactive demo**
  View an online instance of DataSecurity Plus (available without signing up).
- **Guided product tour**
  Schedule a demo to have a product expert walk you through the software and answer your questions.
- **Request a quote**
  View pricing details and request a personalized quote.

DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It analyzes file storage and security permissions, deletes junk files, and detects security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing personally identifiable information (PII), payment card information (PCI), and electronic protected health information (ePHI). It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage. Together, these capabilities ensure the all-round protection of data at rest, data in use, and data in motion.

To explore these features and see DataSecurity Plus in action, check out the online demo.
To learn more about DataSecurity Plus, visit www.datasecurityplus.com.

Download free trial $ Get a quote

Explore **DataSecurity Plus' capabilities**

File server auditing
Audit and report on file accesses and modifications, with real-time alerts and automated responses for critical file activities.

Learn more

File analysis
Analyze file security and storage, manage junk files, optimize disk space usage, and identify permission vulnerabilities.

Learn more

Data risk assessment
Discover and classify files containing sensitive data such as PII, PCI, and ePHI by combining content inspection and contextual analysis.

Learn more

Data leak prevention
Detect and disrupt data leaks via USBs, email, web applications, and printers; monitor endpoint file activity; and more.

Learn more

Cloud protection
Track enterprise web traffic and enforce policies to block the use of inappropriate, risky, or malicious web applications.

Learn more