ManageEngine
DataSecurity Plus

Data loss prevention best practices

Data loss prevention (DLP) is the process of identifying sensitive data; monitoring its flow across the organization; and preventing its theft, loss, or misuse through unintended or unauthorized actions. The sudden rise of information security threats coupled with stringent regulatory mandates has highlighted the importance of adopting DLP practices and tools. A world-class DLP solution can protect sensitive data no matter where it's stored, how it's used, or how it's transmitted.

6 best practices for deploying your DLP solution

1. **Start off with data discovery and classification.**

   Knowing what data needs to be protected and where it lies is the first step for DLP. Data discovery, classification, and manual tagging capabilities provide visibility of sensitive data, including where it's located as well as how it's being protected. Once categorized, DLP solutions can be implemented to operate on the classified content.

2. **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 become overwhelming.

3. **Record all raised incidents.**

   Maintain clear, concise documentation of all violated policies and incidents that have been raised. Use an incident dashboard to analyze top data loss incidents, user risk scores, and security incidents to fine tune your DLP solution and employ appropriate active or passive remediation.

4. **Create, fine tune, and update your risk policies.**

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

5. **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's properly configured, performs satisfactorily, runs policies as per your requirements, and is compatible with the existing workstation applications.

6. **Integrate with Cloud Access Security Brokers**

   Identifying and protecting sensitive information on cloud applications is also an essential and important part of an effective DLP solution. Integrating Cloud Access Security Brokers (CASB) with your DLP solution extends data security to cloud platforms to provide data security across the entire organization.

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

About 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 also analyzes file storage and security permissions, deletes junk files, and detects file security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing PII, PCI, and ePHI. It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage.

$ Get Quote Download free trial