WHITE PAPER

Building a Comprehensive Data Loss Prevention Program

A Step-by-Step Guide

Executive Summary

In an increasingly digital world, protecting sensitive data is paramount. Organizations face growing risks of data loss, theft, and unauthorized access, which can lead to significant financial, legal, and reputational damage. Data loss prevention (DLP) programs are critical for safeguarding sensitive data, particularly for businesses that must adhere to stringent regulatory requirements such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and California Consumer Privacy Act (CCPA). To build a robust DLP program, you need to develop and implement a successful DLP strategy that addresses business and technical requirements.

Forty percent of data is stored across multiple types of environments, punctuating one of the difficulties involved in protecting data—it's everywhere.[1]

The Critical Role of Data Loss Prevention

Data breaches are becoming increasingly common. The volume of sensitive data is growing across a wide range of environments, including endpoints, cloud services, and communication platforms. As organizations move toward more distributed workforces and digital ecosystems, securing data has never been more important.

As organizations face increased cybersecurity and compliance risks, protecting data is crucial. But with a well-designed DLP strategy, businesses are better able to protect sensitive information, ensure compliance with regulatory requirements, and prevent accidental or intentional data leaks.

DLP Program Checklist

1. Identify and understand regulatory obligations

A DLP program should begin with a clear understanding of the regulatory landscape. Different industries and regions are subject to various regulations that dictate how data must be handled and protected. Key regulations include:

□ **GDPR:** Governs the handling and protection of personal data on European Union (EU) residents by organizations in and outside the EU.

□ **HIPAA:** Sets standards for the protection of health information.

□ **PCI DSS:** Enforces security practices for organizations that process payment card information.

□ **CCPA:** Protects the personal data of California residents.

□ **Federal standards** such as Committee on National Security Systems Directive 504 (CNSSD 504), which establishes directives for user activity monitoring in national security systems.

Organizations must assess their regulatory obligations and ensure that their DLP strategy addresses these requirements effectively. Mapping DLP policies to specific regulatory standards helps maintain compliance and avoid penalties.

2. Develop your DLP scope

Defining the scope of a DLP program is crucial for aligning the strategy with business goals and the organization's risk profile. To understand the scope, you must determine what data types and systems will be monitored and protected. Consider the following:

□ **Success metrics:** Establish measurable goals, such as minimizing false positives (FP rates), increasing detection accuracy, and reducing training interventions.

□ **Endpoints and networks:** Ensure that DLP policies cover all devices, servers, and internal networks.

□ **Cloud applications:** These include data stored in or transmitted through cloud services, which addresses the growing use of SaaS and cloud storage platforms.

□ **Chat and messaging platforms:** Secure communication channels where sensitive data could be inadvertently shared.

A well-defined DLP scope provides clear boundaries for policy development and helps focus resources where they are most needed.

3. Identify business requirements

For a DLP solution to succeed, it must meet the organization's specific business requirements without impeding day-to-day operations. Key considerations include:

□ **Business processes:** Understand which processes need to be secured, such as transferring customer payment data to external contractors or partners.

□ **Workflow integration:** Ensure that the DLP system supports secure business activities without introducing significant friction.

□ **Data flows:** Map the flow of sensitive data within the organization to identify high-risk areas that require additional protection.

Balancing security needs with business efficiency is essential to successfully adopt and enforce DLP policies.

4. Identify technical requirements

Technical requirements play a significant role in designing and deploying a DLP program. Organizations must consider several factors to ensure their DLP solution can operate effectively within their IT environment. Key technical requirements include:

□ **Performance on endpoints:** Ensure that the DLP system has minimal impact on user productivity and device performance.

□ **Compatibility with endpoints:** Verify that the solution works across different operating systems and device types (such as Windows, macOS, and Linux).

□ **Minimized overhead for building and maintaining rules:** The system should offer an intuitive interface and easy rule management to reduce administrative burden.

□ **Bandwidth and storage requirements:** Ensure that DLP policies do not strain network resources or require excessive data-log storage.

□ **Off-network performance:** Consider how the DLP system will perform for remote or hybrid workers who may operate outside the corporate network.

Addressing these technical requirements early in the planning process can help organizations avoid performance bottlenecks and ensure smooth deployment.

5. Understand what data you need to protect

Identifying the types of data that requires protection is essential for configuring DLP policies. Common categories of sensitive data include:

□ **Internal data:** Corporate information that could be damaging if exposed.

□ **PII:** Data such as names, Social Security numbers (SSN), and addresses that can identify individuals.

□ **PHI:** Sensitive health-related data protected under HIPAA.

□ **Payment card information:** Credit card numbers, expiration dates, and security codes.

□ **Intellectual property:** Proprietary information such as source code, design documents, and trade secrets.

□ **Financial data:** Budgets, forecasts, and transaction records.

□ **Business partner information:** Contracts, agreements, and confidential communications with third-party vendors or partners.

Understanding which data needs protection allows for more precise policy creation, reducing the risk of data leakage.

6. Develop an identification and classification system

Sensitive data can exist in structured, unstructured, and semi-structured forms, and each form requires different detection methods. A DLP system should incorporate a range of techniques to classify and identify sensitive data, including:

- **Structured data:** Often stored in databases (such as customer records and financial data).
- **Unstructured data:** Text documents, presentations, images, videos, and chat logs.
- **Semi-structured data:** Emails, spreadsheets, and other formats that mix structured and unstructured elements.

Data classification methods include:

- String matching is used to identify credit card numbers, SSNs, and other standardized formats.
- Regular expressions for more flexible detection of patterns like account numbers or financial data.
- Keyword detection is used to identify confidential or sensitive terms.
- User and role-based identification is used to classify data based on who owns or interacts with it.

Implementing a robust classification system is essential for accurately detecting and enforcing DLP policies.

7. Define security requirements and policies

Defining clear security requirements ensures that the DLP program protects data without overwhelming users with unnecessary alerts. Consider the following when defining policies:

- **Controls and escalations:** Establish protocols for escalating incidents and triggering appropriate responses, such as warnings or blocking transmissions.
- **User training:** Incorporate regular training to educate employees on avoiding accidental data leaks.
- **Encryption:** Require encryption for sensitive data both in transit and at rest.
- **Data sanitization and redaction:** Ensure sensitive information is redacted properly from documents and communication channels where necessary.

Comprehensive policies and enforcement mechanisms ensure consistent protection of sensitive data across the organization.

8. Determine roles and responsibilities

A successful DLP program requires clear assignment of roles and responsibilities. Consider the following key roles:

- **Rule creation:** Designated administrators should have the authority to define and update DLP policies.
- **Rule enforcement:** Automated enforcement mechanisms should apply rules consistently across users and systems.
- **Exception handling:** Specific individuals or teams should manage exceptions and handle false positives or unusual cases.

Clearly defined roles help streamline policy management and ensure accountability across the organization.

9. Employee communication

Effective communication is essential to the success of any DLP program. Organizations should:

- **Distribute and require review of policies:** Ensure that employees know the DLP rules and the consequences of noncompliance.
- **Educate employees on cyber hygiene:** Provide training on best practices for handling sensitive data.

□ **Clarify sanctioned vs. unsanctioned apps and devices:** Help employees understand which tools are approved for business use and which pose security risks.

Ongoing communication and training help foster a culture of security awareness and compliance.

Nearly 60% of breaches involved the disclosure of personal information.[2]

10. Identify and correct poor cyber-hygiene practices

Continuous monitoring and adjustment of DLP policies are necessary to identify and correct risky behaviors. Organizations should:

□ **Monitor unsafe activities:** Track patterns of behavior that indicate poor cyber hygiene, such as using unsanctioned apps or improperly sharing sensitive data.

□ **Adjust policies based on effectiveness:** Regularly review DLP policies to ensure they function as intended.

□ **Provide risk-informed user education:** Offer targeted training to employees who engage in risky behavior to reduce future incidents.

By proactively addressing poor cyber hygiene, organizations can reduce the risk of accidental data leaks.

11. Rollout and enforcement

A comprehensive rollout plan is key to successfully enforcing DLP policies. Consider the following steps:

□ **Test incident response plans:** Before full deployment, run simulations to ensure the organization is prepared for data breaches or policy violations.

□ **Enforce policies with appropriate actions:** Enforcement could include blocking uploads, isolating compromised devices from the network, locking user sessions, or terminating risky processes.

□ **Monitor and adjust:** Continuously monitor the system to ensure policies are enforced and remain effective.

A phased rollout, accompanied by thorough testing, ensures smooth implementation and maximizes the effectiveness of the DLP program.

Safeguard Data and Ensure Compliance

A strong DLP program is critical for safeguarding sensitive data and ensuring compliance with regulatory requirements. The first step in a successful DLP program is understanding the regulatory requirements specific to your industry and region. Aligning your DLP policies with these regulations ensures compliance and effective protection of sensitive data.

Organizations can develop a robust strategy that aligns with their business goals and risk profile by creating and following the DLP checklist. From understanding regulatory obligations to defining technical requirements and rolling out policies, a well-planned DLP program ensures that sensitive data is protected, risks are minimized, and compliance is maintained.

By adopting these best practices, organizations can secure their critical information, safeguard their reputation, and build trust with customers and stakeholders.

[1] IBM and Ponemon Institute, Cost of a Data Breach Report 2024, July 30, 2024.

[2] Verizon, 2024 Data Breach Investigations Report, May 5, 2024.

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.