Data Loss Prevention Security Assessment

Create a Plan to Protect Your Critical Information

What Is Data Loss Prevention (DLP)?

Data loss prevention refers to a combination of technology, policy, and process that helps your organization monitor and control critical information, and develop a complete data security strategy. The technology monitors, detects, and blocks sensitive data exfiltration while data is **in-use** (endpoint actions), **in-motion** (network traffic), and **at-rest** (data storage). The policy establishes appropriate guidelines for your organization and users, and the process ensures the security solution delivers the results you want. The objective of a successful DLP strategy is to prevent sensitive data from being disclosed to unauthorized personnel, either by malicious intent or inadvertent mistake.

What Is a Data Loss Prevention Security Assessment?

Our assessment is a discovery of your network and the identification of sensitive data—in motion or at rest—to ensure it is not exposed to unauthorized sources. Conducting a DLP Security Assessment is the first step for DLP planning, design, and implementation. The goal is to identify sensitive data within your environment—including LAN, WAN, VPN sites, and cloud—and to identify potential threats and vulnerabilities to the data. This data includes:

- Non-public data, such as financial, HR, legal, and compliance data
- Personally Identifiable Information (PII), such as Social Security numbers, credit card information, and Protected Health Information (PHI)
- Intellectual property, such as patents, trademarks, and design documents

What Value Proposition Does a DLP Security Assessment Provide?

- **Understand and document your requirements for protecting sensitive information**—An assessment assists with requirements gathering, facilitating a series of discussions to capture organizational expectations, concerns, and requirements. These are distilled, standardized, and organized for the organization to approve.
- **Determine and document security risk and existing gaps**—We conduct a comprehensive security and gap assessment of the organization to identify, locate, and contextualize sensitive data and determine what gaps exist in securing that data.
- **Classify and document sensitive data**—An effective DLP implementation depends on classifying data correctly and effectively. We design a data classification scheme for your organization and help implement it.
- **Determine and execute a risk remediation plan**—Based on the results of the gap assessment and data classification effort, we will develop a comprehensive organizational DLP strategy and recommend controls, procedures, and technologies to implement.

Utilizing a best-of-breed strategy based on industry-leading tools, we can perform the DLP Security Assessment remotely by shipping a pre-configured appliance, virtual machine, or solution to your data center, or by working on site as required. A local portal can provide access for your team to review events in real time and historically.

What Deliverables Will the DLP Security Assessment Provide?

- Report detailing the data identified, its classification, and the system the data resides on or the sender/receiver
- Comprehensive DLP strategy
- Custom DLP solution recommendations
- Estimate to conduct a Proof-of-Concept in a structured environment (if requested)

How Is the DLP Security Assessment Scoped?

The scope is determined using a simple sizing spreadsheet for the approximate number of locations and devices. A 30-minute scoping call may follow if additional clarification is required.

How Long Does a DLP Security Assessment Take?

For a complete baseline, the assessment typically runs over a 4-week period. Using a predefined database of over 300 rules, alerts will be generated if any transfers of sensitive data are detected. Additionally, our enumeration tools will scan data storage locations to report sensitive information locations.

Engage GovConnection to Create an Effective Data Protection Plan

In today's security landscape, IT organizations across all industries must navigate a complex set of regulatory, compliance, and strategic demands. With ever-present security risks, technology evolution, and tightening regulations, security compliance can be difficult to achieve and maintain. Our DLP Security Assessment can provide you with a better understanding of your organization's current risks and help identify opportunities to protect your sensitive data from loss or leakage.

Call an Account Manager to schedule a Security Assessment today, or visit www.govconnection.com/securityassessment

1.800.800.0019
www.govconnection.com

we solve IT™ | GovConnection™
A PC CONNECTION COMPANY