

DATA SHEET

Data loss Prevention (DLP) Services



Introduction

Data Loss Prevention is a set of tools and processes that are used to detect and prevent unwanted destruction, unauthorized access, and exfiltration of sensitive data. A robust DLP solution can help organizations ensure data protection on all devices and in different stages of the data lifecycle. As a DLP advisory service provider, Encryption Consulting will identify the sensitive data within your environment, identify potential threats and vulnerabilities to the data and protect sensitive data from data leaks.

DLP Assessment

Our DLP Assessment service provides you with a better understanding of your organization's current data leak risks and help identify opportunities to protect your sensitive data from loss or leakage. This study will provide our customers with a current state summary and future state vision/strategy recommendations.

Approach:

- Meet with key stakeholders to understand customer's requirements for protecting sensitive data.
- Review the current DLP implementation as per industry standards and best practices.
- Gain an understanding of the current state, including challenges, and use cases.
- Define a strategy and roadmap to deploy DLP solution across the customer's environment.



DLP Strategy

Through this service, experts from Encryption Consulting will provide a robust and effective DLP strategy which will look at what data is considered sensitive, where it is located, how it moves in and out of the organization, and what are the risks of the data being stolen or compromised. We'll also evaluate your current DLP tools and identify the areas of highest risk. This will enable you to prioritize your efforts and budget in order to reduce data leak risk. We will develop a high level DLP strategy to guide future project activities.

Highlights:

- Evaluate current state of DLP tools by conducting workshops with identified stakeholders and analysing supporting documents.
- Provide recommendations and generate enhancement opportunities across people, processes, and technology areas.
- Develop initiative plans for Data loss prevention.
- Preparation of prioritized strategic roadmap for implementing data loss prevention tools and processes.



DLP Implementation

The experts from Encryption Consulting will work with you to design a DLP implementation. Our methodology is modular and iterative in nature and can be customized based upon an organization's current DLP program maturity level and objectives.

Approach:

1. Planning and Analysis:

- Discuss customer's DLP requirements and understand organisation's future model for offering DLP services.
- Review of current process followed across the business units globally
- Understand existing technology infrastructure and all third-party products which the organization intends to integrate with DLP.
- Identify gaps and define future state plan.

1. Design

- Design and document a DLP solution based on customers' requirements.
- Perform vendor analysis.
- Develop a detailed implementation plan including high-level architectural diagram.

1. Implementation of DLP solution:

- Assist organisation in DLP solution deployment
- Build an operations and installation guide
- Test plans to prove solutions functionality
- Perform Policy/Rule testing and tuning



Why Encryption Consulting LLC?



Encryption Advisory Services

Encryption is used for securely protecting data from unauthorized access. Data encrypted can only be seen by those that possess the key to change the data back to plain text. Encryption is now one of the oldest yet still most effective technology solutions able to have data security for organizations.



Public Key Infrastructure

PKI is a security ecosystem that has stood the test of time for achieving secure Internet-based transactions by the use of digital certificates. Digital certificates have provided security to servers and routers from the very early stages of the Internet through Public Key Infrastructure



Hardware Security Module - HSM

Hardware Security Modules provides protection and strong authentication with cryptographic processing by the use of digital keys inside a physical computing device. This device offers an isolated tamperproof environment which can create and secure cryptographic keys, protecting critical cryptographic operations, all while enforcing self-implemented policies over the keys.



Certificate Lifecycle Management

Certificates typically have a 4-phase lifecycle - Discovery, Enrollment, Provisioning, and End-of-life. To make your PKI mature and reliable, you must have more control over all the phases



Enterprise Encryption Platforms

Does your business have the need to encrypt large amounts of data-at-rest found in structured databases or in unstructured files across physical, cloud, or both types of environments? Do you want to protect data without disruptive changes to applications or business practices?



Cloud Data Protection Services

The transition towards uploading data on the public cloud is now becoming the normal standard. With relying on the cloud for data storage, cloud security must now become the number one priority for organizations

See it in action

Encryption Consulting LLC is a customer-focused cyber security consulting firm providing an array of services in all aspects of data protection.

[Contact Us](#)