GlobalLogic®

Why Data Loss Prevention Matters to Your Organization

by Sushil Goyal, Consultant Engineer

Contents

Introduction 1

Defining Data Loss Prevention

Why DLP Matters to Your Organization 2

Protection Against Theft and Accidental Disclosure of Sensitive Information

Protection Against Security Threats

Protection of Confidential Data

Preventing the Leakage of Confidential Information

Preventing the Misuse of Data

Dealing with a Growing Amount of Data

Leading DLP Software 4

Conclusion 5

Introduction

Data loss prevention (DLP) is an approach that helps protect your organization's sensitive data. It restricts end users from moving valuable information outside the business network.

We know that data is very important for any organization. It's challenging for any organization to protect their data from unauthorized access, misuse of personally identifiable information (PII) covered by regulations like GDPR and HIPPA, theft of confidential information, and other outside threats that are increasing daily. DLP implementation restricts end users from accidentally or unknowingly sharing data that could put the organization at risk. DLP software monitors and controls end user activities, filters data streams on networks, and monitors data to protect data at rest, in motion, and in use.

Defining Data Loss Prevention

Data Loss Prevention has been defined in the following ways:

"Data loss prevention is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users."

"Data loss prevention is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network."

"Data loss prevention is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data."

"The DLP term refers to defending organizations against both data loss and data leakage... Data loss refers to an event in which important data is lost to the enterprise, such as in a ransomware attack. Data loss prevention focuses on preventing the illicit transfer of data outside organizational boundaries."

In the 2017 Gartner Magic Quadrant for Enterprise DLP, Gartner estimates the following:

- By 2022, 60% of organizations will involve line-of-business owners when crafting their DLP strategy, up from 15% today
- By 2020, 85% of organizations will implement at least one form of integrated DLP, up from 50% today
- By 2022, a majority of DLP market revenue will be driven by integrated DLP products, as opposed to enterprise DLP systems

Why DLP Matters to Your Organization

Data breaches can result in the loss of sensitive business information that may affect an organization's reputation, resulting in financial loss and the possibility the organization may face lawsuits. Organizations that have faced breaches know the importance of data protection.

Data can be leaked from any computing device, including physical and virtual servers, databases, end-user equipment, storage devices, and mobile devices. There are multiple reasons your organization requires data loss prevention. I will list some of these below.

Protection Against Theft and Accidental Disclosure of Sensitive Information

Not all data loss is the result of external, malicious attacks. The unknowing disclosure or mishandling of confidential data by employees is also a significant factor.

It is difficult to identify if someone is using his or her valid access to data for the wrong purposes. For that reason, insider threats can be difficult to prevent. DLP can detect files containing confidential information and restrict them from leaving via the network.

It can block sensitive data transfers to USB drives and other removable media and offers the ability to apply policies that safeguard data on a case-by-case basis.

Protection Against Security Threats

The mission of cyber thieves is to destroy and disrupt data or information, and they always target sensitive information. Attackers can acquire access to sensitive information by phishing, malware, or code injection. We have discovered Trojan horses, worms, viruses, and more.

Spear phishing is the latest method of getting into a business. Spear phishing is a way of creating emails that appear to be from a familiar sender. The email is personalized in such a convincing way that the receiver does not hesitate to open the message and the contaminated attachment.

Protection of Confidential Data

DLP software and tools provide IT and security teams with a 360-degree view of the location, flow, and usage of data across the organization. They check network actions against your organization's security policies and allow you to protect and control sensitive information, including customer data, personally identifiable information (PII), financial data, and intellectual information.

With a detailed understanding of this data, your organization can set up policies to protect itself and make risk-oriented decisions about the assets that need to be protected and at what cost.

Data breaches can result in the loss of sensitive business information that may affect an organization's reputation, resulting in financial loss and the possibility the organization may face lawsuits. Organizations that have faced breaches know the importance of data protection.

Data can be leaked from any computing device, including physical and virtual servers, databases, end-user equipment, storage devices, and mobile devices. There are multiple reasons your organization requires data loss prevention. I will list some of these below.

Preventing the Leakage of Confidential Information

Many data leaks happen because employees lose sensitive data in public, use the open internet, or fail to restrict access per organizational policies.

Some employees deliberately steal data as a form of revenge for perceived negative treatment, for personal profit, or for no other reason than to simply harm the business.

Employees use company computers, mobile devices, or digital equipment to shop, email, and browse the Web. Users are on social media with business and personal email addresses, and they often work in unsecured environments.

Preventing the Misuse of Data

DLP software and tools monitor all endpoint activity on a corporate network. They can block or restrict emails or attachments that contain confidential data, apply policies on removable media devices such as USB thumb drives, and even restrict common computer activities such as printing, copying, and pasting. DLP provides complete data visibility and control, ensuring that employees, third-party vendors, contractors, and partners are prevented from leaking organization data, whether intentional or not.

Dealing with a Growing Amount of Data

Data has become one of the most valuable and vulnerable assets in an organization. Security needs to shift towards a data-centric approach, involving a switch from securing networks, applications, and endpoints to identifying, controlling, and securing data.

Leading DLP Software

Data loss prevention software detects data breaches and continuously monitors sensitive information to block it from going outside a network. The main feature of DLP solutions is distribution control to ensure employees do not send sensitive information outside business networks. Network admins set up the business rules and procedures that define who can view, change, and share data.

There are many DLP tools available in the market to protect your data. You can choose a tool as per your needs. Gartner ranks the following tools based on customer's choices in 2020:

1. Symantec DLP
2. McAfee DLP
3. Forcepoint DLP
4. Endpoint Protector
5. Digital Guardian DLP
6. Spirion
7. Safetica DLP
8. InfoWatch DLP
9. GTB Technologies DLP
10. Fidelis Network

Conclusion

Data loss prevention solutions aim to prevent sensitive data and confidential information from being stored, used, or transferred insecurely. Organizations can set specific rules at a very low level for data access and movement. The protection of sensitive data at rest, in transit, and at endpoints can reduce data theft or unauthorized access.

DLP solutions require continuous training, education, and monitoring. DLP is an investment in loss protection and risk management, now and into the future. It requires corporate awareness of data loss challenges and understanding of the need for preventive measures.

About the Author

Sushil Goyal received the MCA degree in computer applications from Guru Jambheshwar University of Science and Technology in 2008. He has been working as a consultant engineer at GlobalLogic since 2015. His primary areas of interest are data warehousing, data integration, data analysis, and data security.

References

What is Data Loss Prevention (DLP) | Data Leakage Mitigation

DAG Tech - Business IT Support & IT Services, Cloud Solutions, vCTO

Data Loss Prevention Solutions (DLP) Reviews 2021

Gartner Magic Quadrant for Enterprise Data Loss Prevention 2017