Data Leak Prevention vs Data Loss Prevention: Safeguarding Information in the Digital Age

In this digital age, enterprises in all industries are creating and accumulating an astronomical amount of sensitive data to store and exchange. Given a prevalence of highly sensitive data, preventing it from getting into the wrong hands or avoiding data loss by accident has become a top priority. While on surface data loss vs data leak can look harmless, it can lead to financial losses, reputational damages, and even trigger litigation. To secure an organization's sensitive information, one must understand the difference between data leak prevention vs data loss prevention, and how they can make the security system stronger if used with expertise.

What is Data Leak Prevention?

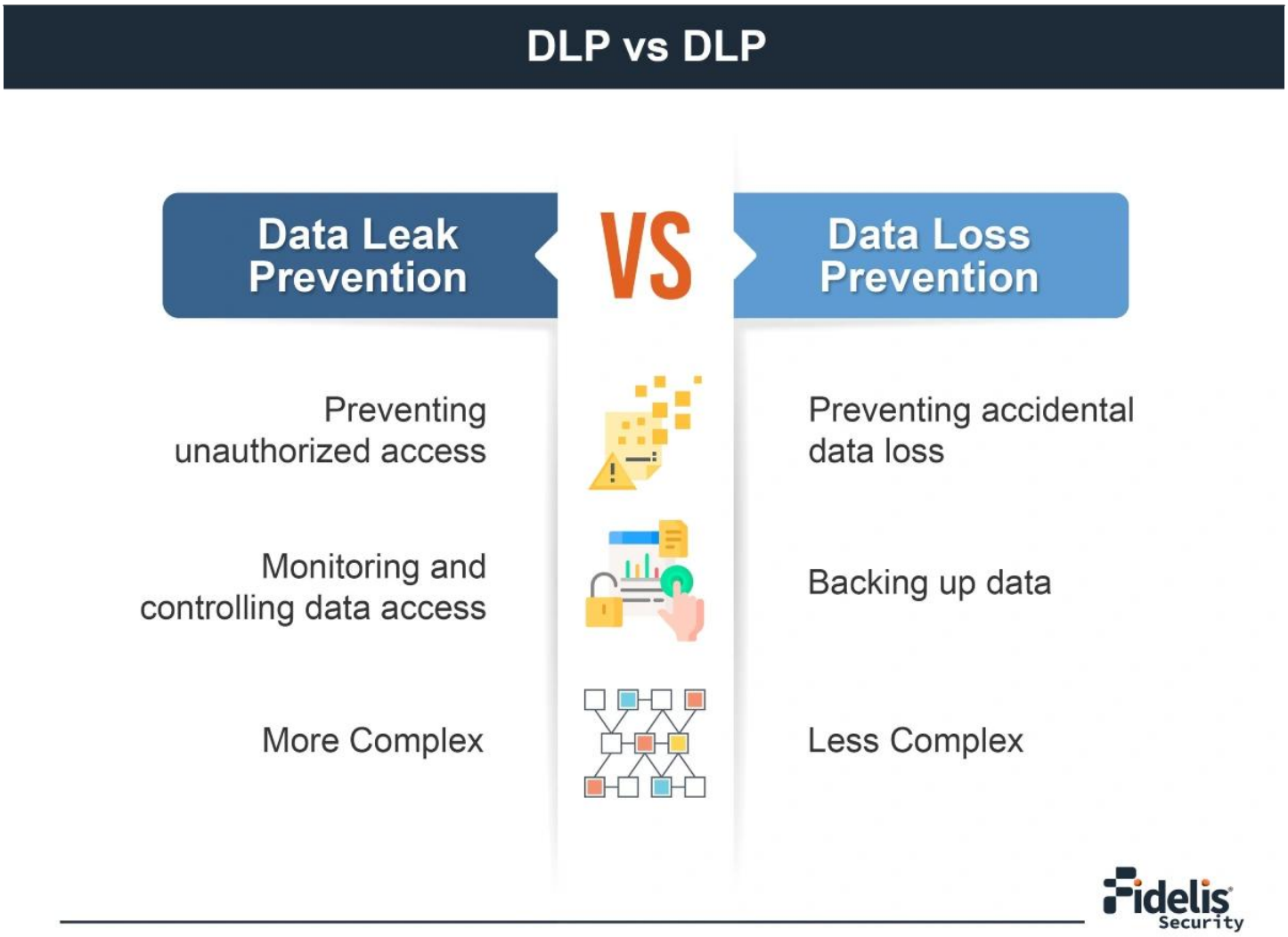
Data Leak Prevention is a set of strategies, tools and processes designed specifically to prevent any sensitive information from being exposed to unauthorized access. Unauthorized access includes people who don't have the right to use the data within an organization or any external entities. The core of Data Leak Prevention technology is focused on protecting sensitive data; be it client information, trade secrets, or financial records from being shared out to an unauthorized source. DLP systems are deployed to prevent the intentional or even unwilling leakage of data by insiders, as well as external threats.

Malicious attacks, insider threats or human error can lead to data breaches. This could be done by a disgruntled employee or a result of simple human error. Which ultimately affects the organization's reputation and can cost the organization millions of dollars.

What is Data Loss Prevention?

Data Loss Prevention (DLP) describes a variety of tools and strategies designed to make sure that data is not lost or stolen, whether it be at rest, in storage, in transit, or during use. Data can be lost for many reasons such as hardware failure, human error, or natural disaster. We must have a Data Loss Prevention plan to keep our business running without losing data and ensure its reliability.

Key Difference Between Data Leak Prevention and Data Loss Prevention?



Even though both the names sound similar, their goals and target areas are quite different to each other. Let’s know more about data leak prevention vs data loss prevention.

Data Leak Prevention is a process of stopping secure data from being exposed to the external environment. The external environment can be malicious hacker or some competitor trying to bring your business down. Data Loss Prevention is to ensure that any confidential data such as client information, trade secrets, or financial information does not end up with some unauthorized person. It helps to counteract any intentional or accidental leaks carried out by insiders or hackers. The goal of Data leak prevention technology is averting data breaches, data sharing over insecure medium or unsolicited stealing away of sensitive files.

While with Data Loss Prevention is making sure that important data remains intact in the company. The key objective should be to ensure data is not lost or destroyed, and unavailable due to corruption or database tabletops in response to hardware failures, human errors, malicious activity such as cyberattacks; etc. Data loss prevention strategies ensure that data can recover quickly and completely, preserving data integrity and availability.

Use Cases

Data Leak Prevention: An example of a data leak is an employee emailing a spreadsheet with customer financial information to an unauthorized third party. The email can be intentional or unintentional. Data leak prevention technology would see that something sensitive was being sent out, as a response to this, it will either prevent it from going out or log a message so that

the security team could stop the exposure.

Data Loss Prevention: Let's say a server crashes in a company and with it, a critical database full of financial records is lost. In that situation, a data loss prevention system would have previously backed up the data so the organization could restore the data from backup. This will safeguard the company from any downtime along with permanent data loss.

Why You Need Both Data Leak and Data Loss Prevention

First things first: you need to understand that your organization's network is far from hackproof. You are one click away from massive monetary losses and lawsuits. At its worst, a cyberattack might just wipe out your business.

Let's think about in case of a data failure, ***what can go wrong?***

A lot, and none of it is good. Imagine that the critical data of your company such as customer information, intellectual property, or financial information suddenly becomes inaccessible or even worse accessed by your competitors. Here's what could happen:

Your company's critical data such as financial records, customer information, intellectual property—suddenly becomes inaccessible or, even worse, is accessed by your competitors. Here's what could happen:

- ## Operational Shutdown

  There’s no way around it: without data, your business is coming to a halt. Operations will stop, projects will be on hold, and employees won’t be able to work effectively. While a couple of hours might seem like something that can be easily sorted out, think of what would happen if those two hours turned into days—possibly weeks.

- ## Financial Downfall

  Regardless of the way your business is operating, every minute you’re down, you’re losing money. From failed sales opportunities to keeping your employees on the clock to gauge their output.

- ## Loss of Trust

  While dealing with the loss of data, the main thing you’re losing along with it is trust. You’re not simply losing files; you’re losing customers, partners and sponsors—they won’t be thrilled to work with a company that lost so much sensitive information and failed to protect it.

- ## Legal Consequences

  Depending on the type of data you lost, the legal consequences of the data breach could vary significantly. If personal identifiable information that belongs to your customers, subscribers, or any website users falls into the wrong hands you can land in court with hefty fines and penalties.

In conclusion, data loss is not just a technical problem, it is a business risk, and that risk can be mitigated by applying data leak and data loss prevention best practices and deploying a powerful DLP solution like Fidelis Network®.

Stay Ahead of Data Loss Threats

Your guide to selecting the best Network DLP for your organization.

- Comprehensive Insights
- In-Depth Analysis
- Expert Recommendations

Download our Free Guide

Best Practices for Implementing Data Leak and Data Loss Prevention

Data Leak Prevention Best Practices

Restricting Access to Sensitive Information: Only limited people should be allowed to

access data based on those who absolutely need it to work efficiently. This will protect valuable data from being exposed to unauthorized people.

Encrypting Data in Transit and at Rest: Add another layer of essential security using strong encryption to secure your data while in transit and at rest.

Implementing Strong Monitoring and Alerting Systems: Advanced monitoring systems such as Fidelis Network® Data Loss Prevention Solution should be used as it can detect abnormal activity and send an alert to SOC team.

Data Loss Prevention Best Practices

Regular Backups and Data Redundancy: Regular backups of the critical information should be conducted and redundancy measures such as creating multiple copies of data in different formats must also be deployed.

Using Robust Data Recovery Tools: Use comprehensive tools such as Fidelis Network® Data Loss Prevention Solution that can recover lost data promptly when a loss has occurred.

Employee Training to Prevent Accidental Deletions: Having employees properly trained in how to handle data to minimize likelihood of a loss of data through accidental deletion.

Choosing the Right DLP Solutions for Your Business

Selecting the right tools can drastically impact the security stance of your organization. So, here are the factors that you must take into consideration when choosing which DLP tool suits your business

- Classify what kind of data your company is handling and then identify the data that is Confidential. Any Data Loss Prevention solution you go with must provide powerful protection that is specifically designed for such data types.
- Then, consider the scalability of these DLP tools. Your data protection requirements will evolve with the growth of your business. Choose a solution that scales easily with your organization.
- It is also crucial that a DLP solution should have integration capabilities. The right Data loss prevention solution will effectively interoperate with your IT infrastructure, including cloud services and on-premises applications with minimal human intervention.
- Another important factor is user experience. If the tool is complex, employees get frustrated, and productivity goes down. You should seek out a solution that has a user-friendly interface and provides straightforward guidance on how to manage data protection policies effectively.

What makes Fidelis Network® the best choice?

Let’s talk now why Fidelis Network® DLP Solution is the best option. Fidelis provides full visibility into data in motion on your network and endpoints, and it detects/responds to advanced threats in real time. With its state-of-the-art machine learning models, it can trace user activity patterns and identify a mischievous data exfiltration operation.

In addition, Fidelis Network® integrates seamlessly with the rest of your security tools, delivering a comprehensive end-to-end solution to protect privacy. The solution also has the ability to accurately inspect all enterprise content. It can scale and keep up with your organization’s growth without any hang ups.

So, in conclusion, if you’re stuck in the process of data leak prevention vs data loss prevention then choosing Fidelis Network® Data Loss Prevention Solution presents the best solution for organizations determined to keep data secure and their work environments conducive to productivity, utilizing a wide range of features and unmatched performance. data leak prevention vs data loss prevention.

Explore how Fidelis Data Loss Prevention can help you!

Talk to an expert

Frequently Ask Questions

What is the difference between data leak vs data loss?

Data leak refers to the unauthorized transmission of data from within an organization to an external destination or recipient. This commonly results from cyberattacks, insider threats, or mistakes in sharing. In contrast, data loss pertains to the unintentional loss of data due to hardware failures, accidental deletion, or corruption. Essentially, a data leak involves exposure of sensitive information to unauthorized third-parties, while data loss involves losing access to information altogether.

Why are both Data Loss Prevention and Data Leak Prevention important for data security?

Data Loss Prevention (DLP) and Data Leak Prevention (DLP) are the need of the hour to create a robust data security strategy. Data Loss Prevention is mainly about preventing information deletion and corruption, which, in essence, boils down minimizing the probability for organizations losing control over their data assets. However, Data Leak Prevention focuses on preventing unauthorized sharing and protection against external threats. Together, they cover the defense of internal mishaps and external breaches to ensure that organizations can stay compliant and keep a good reputation.

Can the same tools be used for both data leak and data loss prevention?

While there is some overlap in the tools used for both Data Loss Prevention and Data Leak Prevention, specific features may differ based on their focus areas. Many modern security solutions such as Fidelis Network® offer integrated functionalities that address both concerns, allowing organizations to implement a unified approach to safeguard their data. However, it’s essential to assess your organization’s specific needs to ensure the chosen tools deliver comprehensive protection.

How often should organizations conduct backups and tests?

Ideally you would want to back up your data once a day or even once a week, but the backup interval can vary depending on how often your data is changing and the impact of losing that information. You need to backup and test these backups at least on quarterly basis.