Infopercept

Data Loss Prevention

Infopercept

Overview

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

DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk.

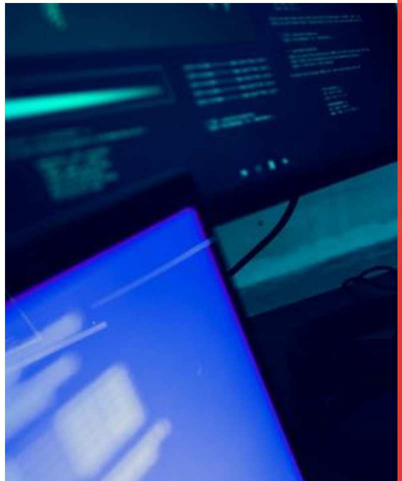
For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Drop-box, the employee would be denied permission.

DLP products may also be referred to as data leak prevention, information loss prevention or extrusion prevention products.

Literature Review

DLP software classifies regulated, confidential and business critical data and identifies violations of policies defined by organizations or within a predefined policy pack, typically driven by regulatory compliance such as HIPAA, PCI-DSS, or GDPR.

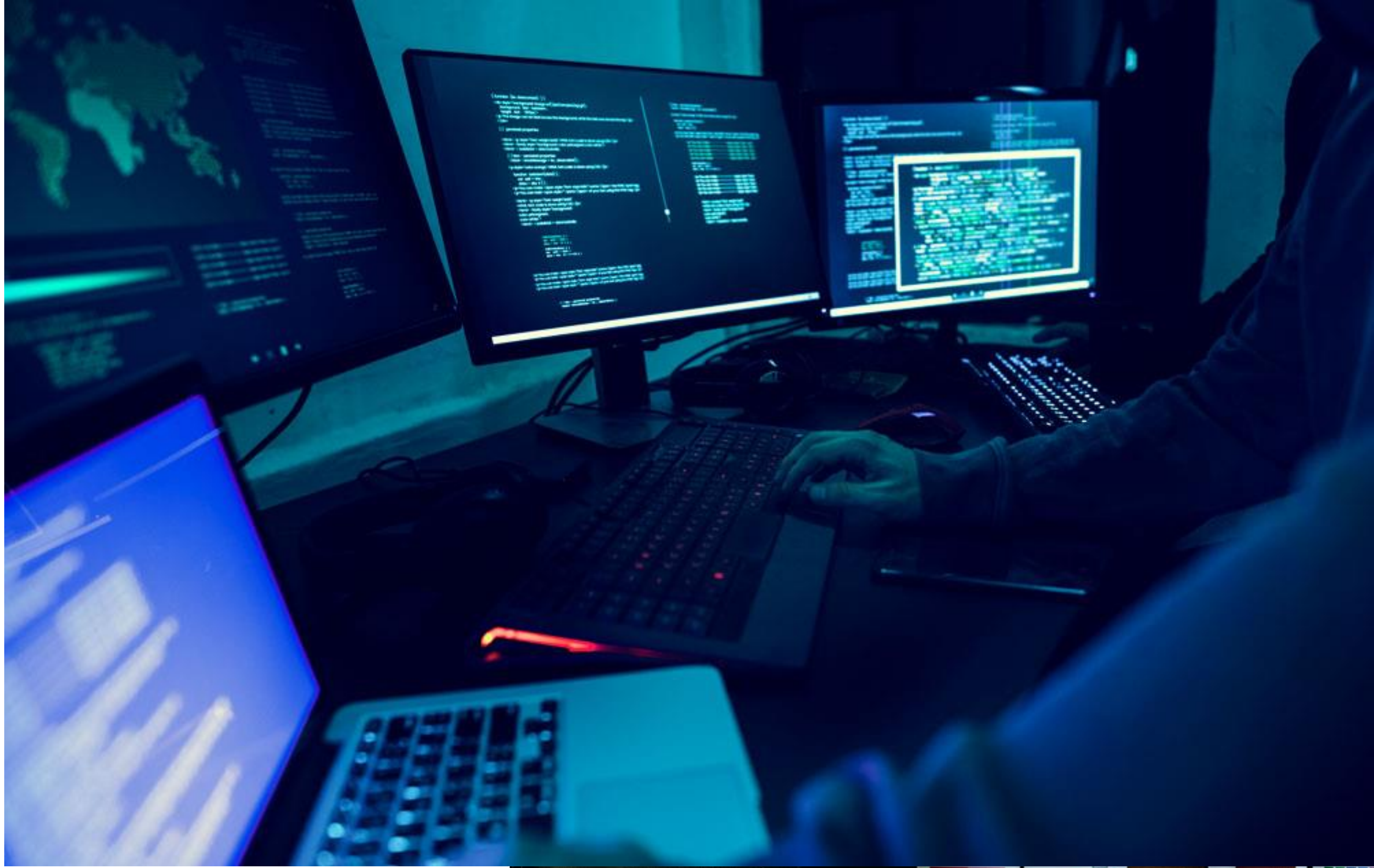
Once those violations are identified, DLP enforces remediation with alerts, encryption, and other protective actions to prevent any kind of data loss

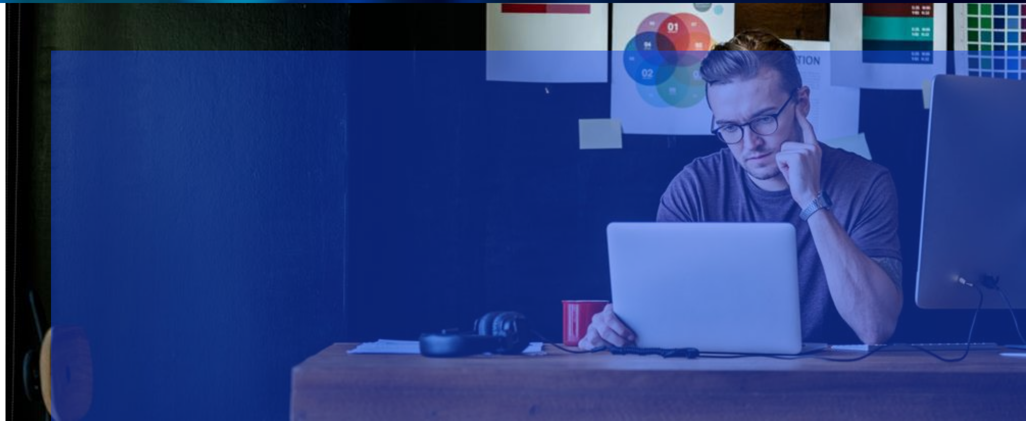


Data loss prevention software and tools monitor and control endpoint activities, filter data streams on corporate networks, and monitor data in the cloud to protect data at rest, in motion, and in use. DLP also provides reporting to meet compliance and auditing requirements and identify areas of weakness and anomalies for forensics and incident response.

Purpose of the study

To study the concept of Data loss prevention technique which is very essential for every organization to comply with.



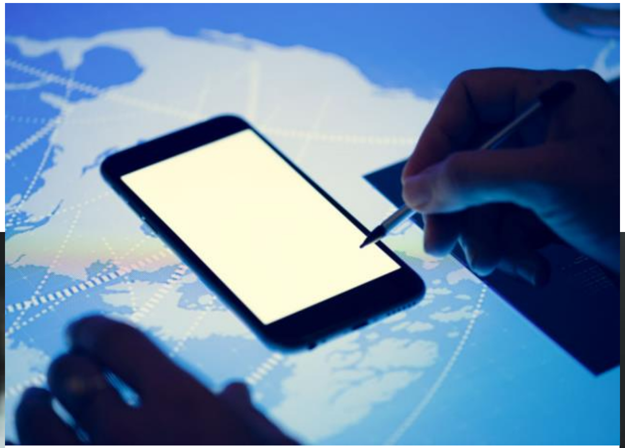


Findings

7 TRENDS DRIVING DLP ADOPTION

The Growth of the CISO ROLE:

DLP provides clear business value in this regard and gives CISOs the necessary reporting capabilities to provide regular updates to the CEO.



Evolving Compliance Mandates:

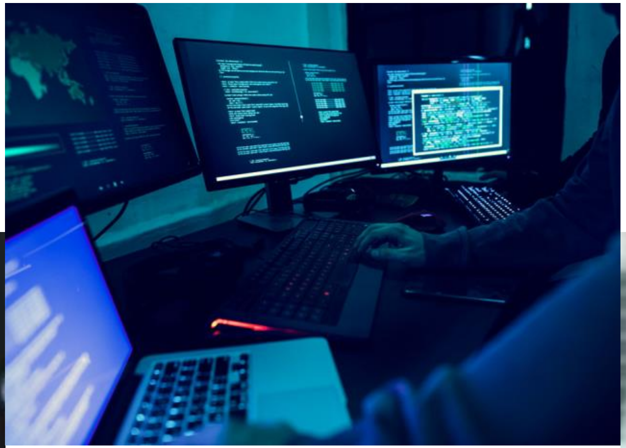
DLP solutions allow organizations the flexibility to evolve with changing global regulations.

Data Breaches are Frequent and Large:

Adversaries from nation states, cyber criminals and malicious insiders are targeting your sensitive data for a variety motives, such as corporate espionage, personal financial gain, and political advantage. DLP can protect against all kinds of adversaries.

There are More Places to Protect Your Data:

Increased use of the cloud, complicated supply chain networks, and other services you no longer have full control over has made protecting your data more complex.



Your Organization’s Stolen Data is Worth More:

Stolen data is often sold on the Dark Web, where individuals and groups can purchase and use it for their own benefit.

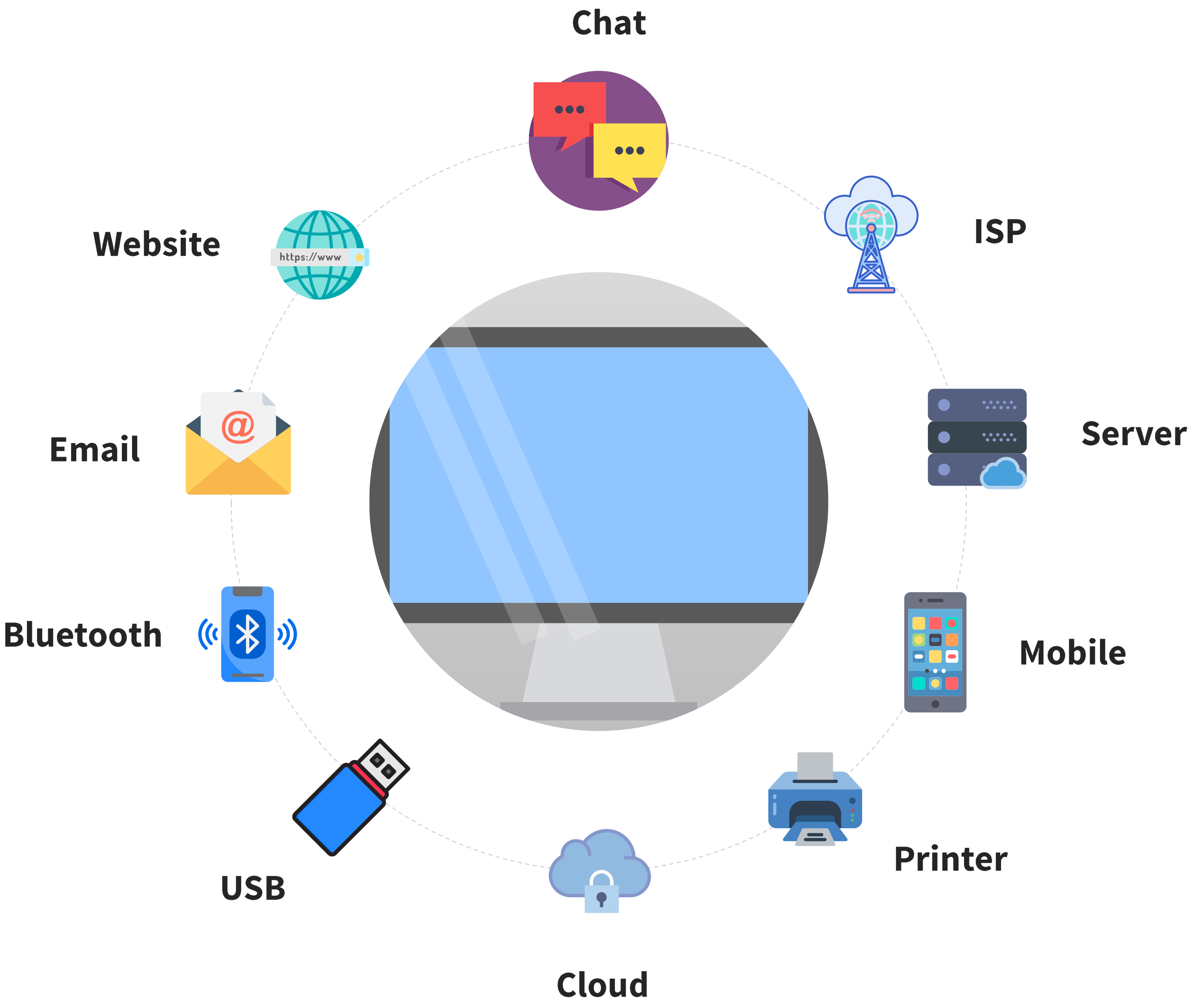
There’s More Data to Steal:

From 1975 to 2015, the amount of intangible assets grew from 17% of the S&P 500 market value to 84%, according to a study. This means your organization has more data to protect.

There’s a Security Talent Shortage:

Managed DLP services act as remote extensions of your team to fill that personnel gap.

Various aspects where DLP is used



Infopercept

USE CASES OF DLP

Personal Information Protection / Compliance:

- Does your organization collect and store Personally Identifiable Information (PII), Protected Health Information (PHI), or payment card information (PCI)?
- If so, you are more than likely subject to compliance regulations, such as HIPAA (for PHI) and GDPR.

IP Protection:

- Does your organization have important intellectual property and trade or state secrets that could put your organization's financial health and brand image at risk if lost or stolen?
- With policies and controls in place, you can protect against unwanted exfiltration of this data.

Data Visibility:

- DLP solution can help you see and track your data on endpoints, networks, and the cloud.

USE CASES OF DLP

Endpoint DLP

- Stops sensitive data from getting out of your organization at the greatest point of risk – the endpoint.
- Focus on monitoring PC-based systems (laptops, tablets, POS, etc.) for all actions such as print or transfer to CD/DVD, webmail, social media, USB and more.

Network DLP

- Helps support compliance and reduce risks of data loss by monitoring and controlling the flow of sensitive data via the network, email or web.
- Network DLP appliances inspect all network traffic then enforce policies to ensure protection. Policy actions include: allow, prompt, block, encrypt, reroute, and quarantine.
- Accelerates compliance efforts securely-Reports provide a detailed picture of sensitive and regulated data movement for audits.

Infopercept

USE CASES OF DLP

Datacenter or storage-based data DLP

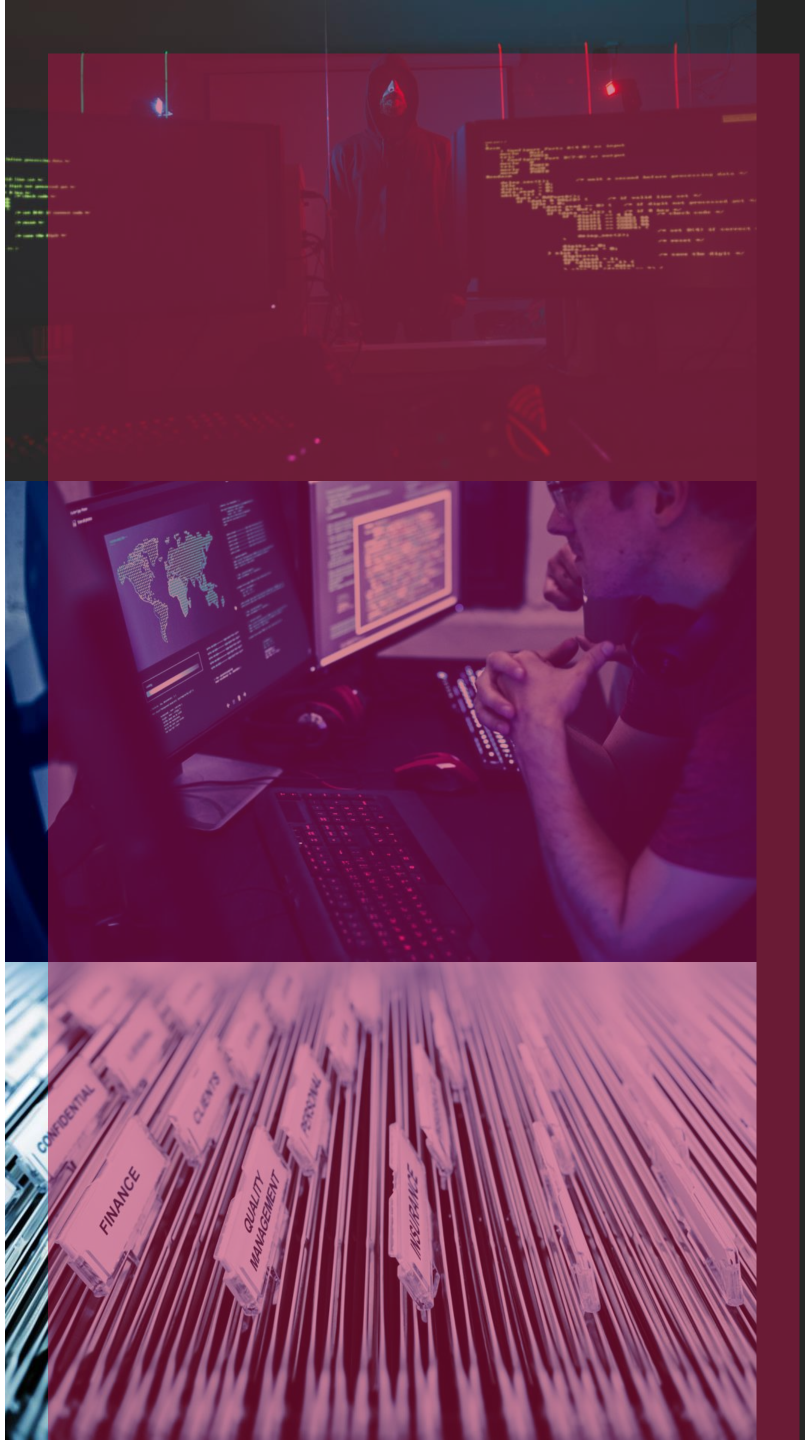
- Focus on protecting data at rest within an organization’s datacenter infrastructure, such as file servers, SharePoint and databases.
- Discover where confidential data resides and enable users to determine if it's being stored securely.

Cloud DLP

- Enables cloud storage security.
- Protects all your sensitive data.
- Delivers comprehensive remediation and logging.

Infopercept

Causes of Data Leaks



Insider threats

- A malicious insider, or an attacker who has compromised a privileged user account, abuses their permissions and attempts to move data outside the organization.

Extrusion by attackers

- Many cyber attacks have sensitive data as their target. Attackers penetrate the security perimeter using techniques like phishing, malware or code injection, and gain access to sensitive data.

Unintentional or negligent data exposure

- Many data leaks occur as a result of employees who lose sensitive data in public, provide open Internet access to data, or fail to restrict access per organizational policies.

Data Leakage Prevention

You can use standard security tools to defend against data loss and leakage. For example, an Intrusion Detection System (IDS) can alert about attacker attempts to access to sensitive data. Antivirus software can prevent attackers from compromising sensitive systems. A firewall can block access from any unauthorized party to systems storing sensitive data.

If you are part of a large organization, you might turn to designated DLP tools or solutions to safeguard your data. You can also use tooling in the Security Operations Center (SOC) to assist with DLP. For example, you can use a Security Information and Event (SIEM) system to detect and correlate events which might constitute a data leak.

Conclusion

Through this study, we concluded that Data Loss Prevention helps in ensuring the fact that the sensitive data does not get sent to the wrong person, either intentionally or unintentionally.

DLP regulatory compliances are essential to protect the cloud storage service with legal standard and rules. This will protect regulated items wherever they live.

It delivers security alarms with lowest false rate and simplifies the data management working on cloud.

Infopercept

THANK YOU FOR YOUR TIME NOW YOU FEELING SAFE ?

For More Information Please Visit our Website

www.infopercept.com