TATA Tele Business Services | PO Big

DATA LOSS PREVENTION: NOW FIND PEACE OF MIND FROM DATA THEFTS

Market Trends

Increase in Cyberattacks

74%

of SMEs suffered cyberattacks in the last one year

Remote Work and BYOD

60%

of employees use personal smartphones for work purposes

DLP* Adoption

28%

is the estimated annual growth rate for cloud DLP industry from 2021 to 2031

*Data Loss Prevention

Source:
1. 74% SMBs suffered a cyber attack in the last one year
2. The Future Of BYOD: Statistics, Predictions And Best Practices To Prep For The Future
3. Cloud data loss prevention market estimated to hit $27.5 billion by 2031 | SC Media (scmagazine.com)

Business Challenges

Monitoring usage of devices in the workplaces

Data leakage/ data loss/ data theft

Increase in sophisticated cyber threats

Regulatory compliance with data

Secure mobile device management

Intellectual property protection

Introducing Data Loss Prevention Solution

Data Loss Prevention (DLP) is an advanced solution designed to protect sensitive data from unauthorised access, use, or disclosure. DLP works by monitoring, identifying, and controlling the flow of sensitive data within an organisation's network and endpoints.

Top Modules of Data Loss Prevention Solution

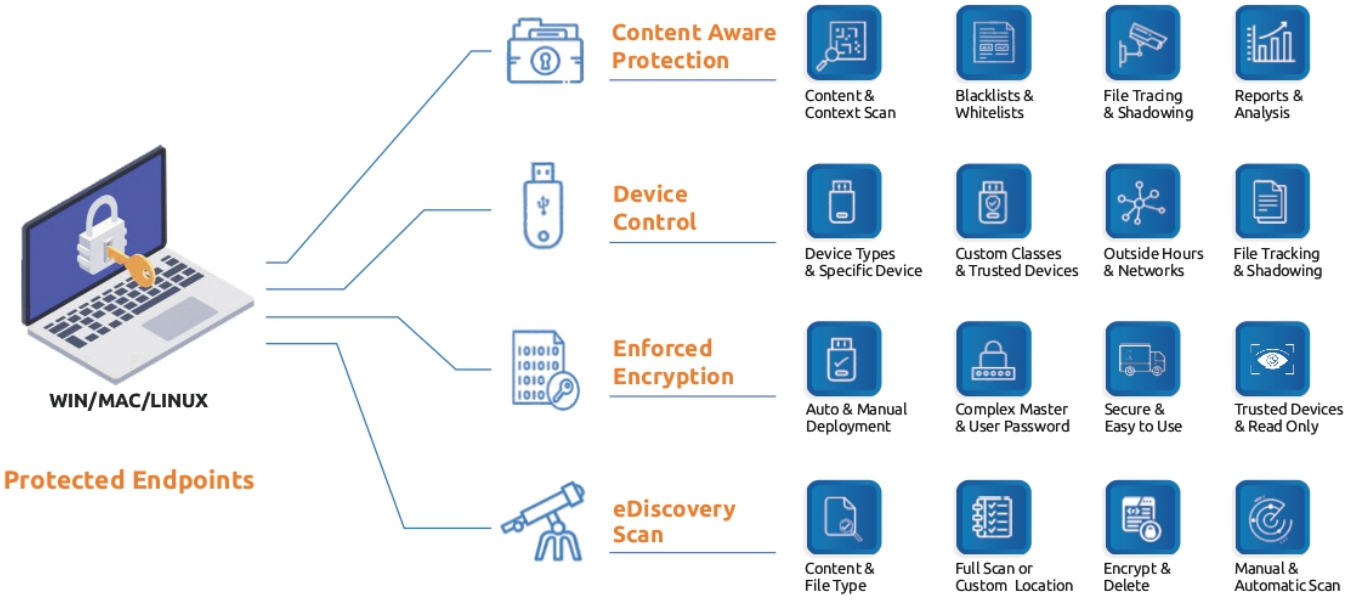
Content Aware Protection
Scanning Data in Motion

Device Control
USB & Peripheral Port Control

Enforced Encryption
Automatic USB Encryption

eDiscovery Scan
Scanning Data at Rest

DLP Solution: Schema



Content Aware Protection

Scanning data in motion

Monitor, control and block file transfers. Detailed control through both content and context inspection.

User Remediation
Empower users to safely override a DLP policy and offer options to justify data transfers.

Blacklists and Whitelists
Created based on custom content, file names, or generate allowlists to avoid redundancy.

File Tracing and Shadowing
Record all file transfers or attempts to various online applications and other exit points.

Reports and Analysis
Monitor activity related to file transfers with a powerful reporting and analysis tool.

Compliance (GDPR, HIPAA etc.)
Become compliant with industry rules and regulations like GDPR, HIPAA, PCI DSS, etc.

Offline Temporary Password
Temporarily allow file transfers to computers disconnected from the network.

Transfer Limit
Set a transfer limit within a specific time interval. It can be either based on the number of files or file size.

Optical Character Recognition
Inspect content from photos and images, detecting confidential information from scanned documents.

DLP for Thin Clients
Protect data on terminal servers and prevent data loss in thin client environments.

DLP for Printers
Policies for local and network printers to block printing of confidential documents.

Print Screen and Clipboard Monitoring
Revoke screen capture capabilities. Eliminate data leaks of sensitive content through copy function.

Threshold for Filters
Define up to which number of violations a file transfer is allowed.

Device Control

USB & peripheral port control

Lockdown, monitor and manage devices. Granular control based on Vendor ID, Product ID, Serial Number and more.

Device Types and Specific Devices

Set rights - deny, allow, etc. for device types or specific devices (using VID, PID and Serial Number).

Custom Classes and Trusted Devices

Rights can be created based on classes of devices making product management easier.

Outside Hours and Outside Networks

Device control policies can be set to apply when outside normal working hours.

File Tracing and Shadowing

Record all file transfers to various USB storage devices, providing a clear view on user actions.

Set Rights Granularly

Device rights can be configured globally, per group, computer, user and device.

Active Directory Sync

Take advantage of active directory to make large deployments simpler.

Users and Computers Information

Gain a better visibility with information such as employee IDs, teams, location etc.

Offline Temporary Password

Temporarily allow device access to computers disconnected from the network.

Create Email Alerts

Predefined and custom email alerts can be set up to provide information.

Dashboard and Graphics

Visual overview of the most important events and statistics, graphics and charts are available.

Reports and Analysis

Monitor all activity related to device use with a powerful reporting and analysis tool.

SIEM Integration

Logs and events can be automatically forwarded to any SIEM solution for a comprehensive overview.

Enforced Encryption

Automatic USB encryption

Encrypt, manage and secure USB storage devices by using 256-bit AES encryption. Password-based, easy to use and very efficient.

Automatic and Manual Deployment
Both automatic and manual deployment is available.

Complex Master and User Passwords
Password complexity can be set as needed.

Secure and Easy to Use
Password-based, easy to use and very efficient.

Trusted Devices or Read Only
Authorize only encrypted USB devices

eDiscovery Scan

Scanning data at rest

Discover, encrypt and delete sensitive data. Detailed content and context inspection through manual or automatic scans.

Content and File Type
Filters can be created based on custom content such as keywords and expressions, or file names.

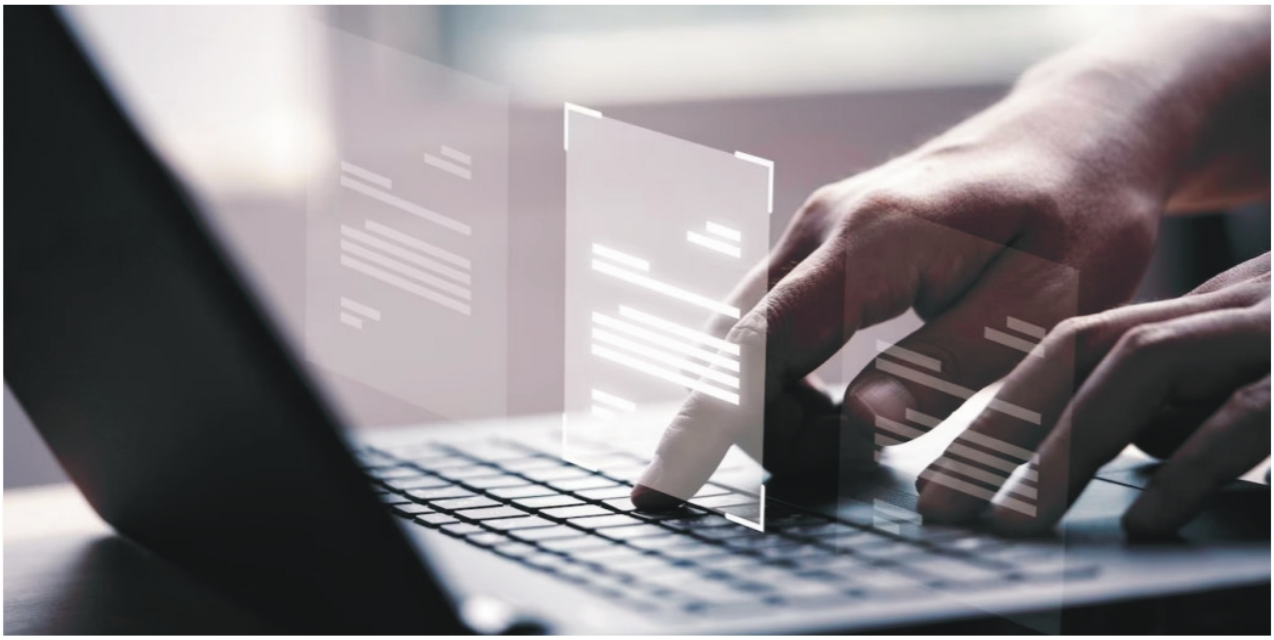
Full Scan or Custom Location
Filters can be created based on predefined locations and avoid redundant scan.

Encrypt and Delete
Data at rest containing confidential information can be encrypted to prevent unauthorized employee access.

Manual and Automatic Scan
In addition to the clean and incremental scans, automatic scans can be scheduled.

Compliance (GDPR, HIPAA etc.)
Become compliant with industry rules and regulations like GDPR, HIPAA, PCI DSS etc.

SIEM Integration
Leverage security information and event management products by externalizing logs.



Multiple Deployment Options

Virtual Appliance

- Formats: .ovf, .ova, .vmx, .vhd, .pvm, .xva
- Compatible with VMware, VirtualBox, Parallels Desktop for Mac, Microsoft Hyper-V and Citrix XenServer

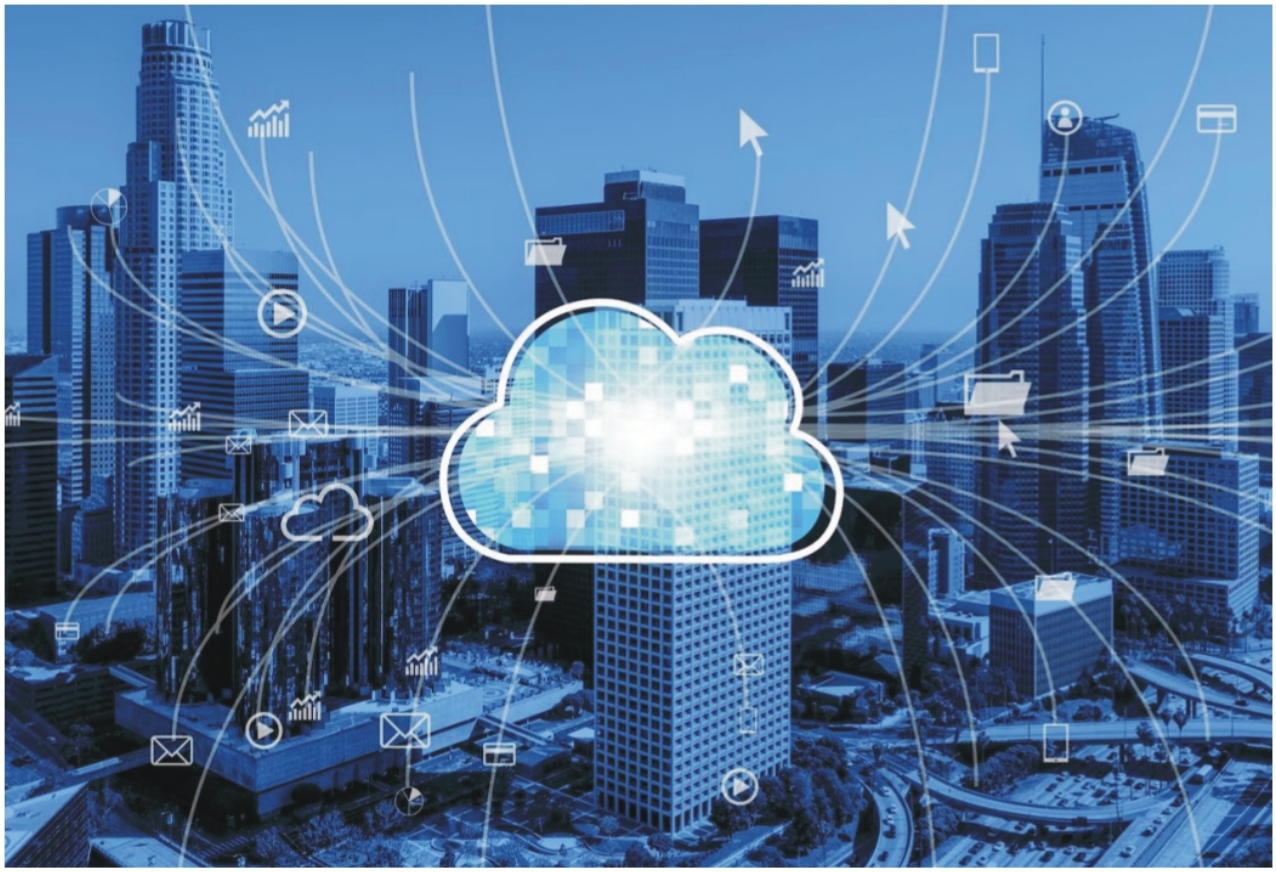
Cloud Services

Available for deployment in the following cloud services:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

Cloud Hosted

- Available as a SaaS, hosted in the cloud
- Deployment region and various other security configuration options available



Why Choose DLP Solution from TTBS?

1. **Multi OS Support**
   Supports Win, Mac, Linux

2. **Zero-day OS Support**
   Supports Win, Mac, Linux

3. **Agent Size & Functionality**
   Non-intrusive, simple and lightweight agent of 46 MB

4. **Content Aware Protection**
   Controls > than 130+ file types, detects source code

5. **False Positives**
   Accurate detection of sensitive information

6. **Device Control**
   Controls more than 40+ devices

DLP Solution: Top Features

Easy and fast deployment

Cross-platform solution

Lightweight agent

Granular policies & settings deployment

Intuitive, user- friendly interface

Modular approach

DLP Solution: Top Benefits

Web-based administration

Multilingual interface

Security across all platforms

Centralized management

All modules in a single management console

Zero-day protection

DLP Solution: Use Cases

Media

- Protects your content from unauthorized distribution
- Reduces the risk of insider threats and data loss from malicious, negligent, and compromised users
- Secures copyrighted content, and confidential client data
- Complies with data protection regulations and standards

BFSI

- Secures sensitive data and eliminates the risk of accidental data loss and data theft
- Prevents operational disruptions, regulatory issues, and penalties.
- Prevents reputational damage due to data breaches at the endpoint

Healthcare

- Helps protect confidential patient data and comply with data privacy regulations, including HIPAA, GDPR, CCPA, and more
- Secures health related data and reduces the risk of insider threats and data loss from malicious, negligent, and compromised users

IT/ITeS

- Secures intellectual property, user credentials, and personal information across macOS, Windows, and Linux machines
- Offers continuous protection, even when employees work offline
- Ensures regulatory compliance

FAQs

Q. What is Data Loss Prevention (DLP), and why is it important for organizations?

A. DLP is designed to protect sensitive data from unauthorized access, use, or disclosure. It is crucial for organizations because it helps prevent data breaches, minimize the risk of sensitive data leaks, comply with data protection regulations, safeguard intellectual property, and maintain customer trust and reputation.

Q. How does DLP work to prevent data breaches and leaks?

A. DLP works by monitoring, identifying, and controlling the flow of sensitive data within an organization's network and endpoints. It uses content inspection, contextual analysis, and predefined policies to detect potential data breaches or unauthorized data transfers.

Q. What types of data does DLP protect, and how can I identify sensitive data in my organization?

A. DLP can protect various types of sensitive data, such as personally identifiable information (PII), financial data, intellectual property, and confidential business information. Sensitive data can be identified by conducting risk assessments and using automated tools to discover and tag sensitive information.

Q. Is DLP suitable for businesses of all sizes?

A. DLP solutions can be tailored to suit the needs of both small businesses and large enterprises.

Q. Does DLP impact employee productivity or hinder legitimate data sharing within the organization?

A. DLP can be configured to balance data security with legitimate data sharing and employee productivity. By creating well-defined policies, organizations can ensure that sensitive data is protected while allowing authorized users to access and share data as needed for their job roles.

Q. Can DLP solutions handle data protection in cloud environments and with remote employees?

A. Yes, many modern DLP solutions support cloud environments and remote work scenarios. They can protect data in cloud applications, monitor data transfers to and from the cloud, and secure data accessed by remote employees through various devices and locations.

Q. What are the key compliance regulations that DLP can help address?

A. DLP solutions can help organizations comply with various data protection regulations, including the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and many industry-specific regulations.

FAQs

Q. How does DLP distinguish between legitimate data use and potential data exfiltration attempts?

A. DLP uses a combination of content analysis, context, and predefined policies to differentiate between legitimate data use and potential data exfiltration. Policies can be customized to identify abnormal data access patterns, high-volume transfers, or unauthorized data recipients, triggering alerts or enforcement actions when necessary.

Q. Can DLP prevent data breaches caused by external threats, such as hackers and cybercriminals?

A. DLP can help prevent data breaches caused by both internal and external threats. While it primarily focuses on insider threats (employees, contractors, etc.), it can also detect and block data exfiltration attempts by external hackers who manage to gain access to the organization's systems.

Q. How do DLP solutions handle encrypted data and protect against insider threats?

A. DLP solutions can inspect and analyze encrypted data through techniques such as SSL decryption. DLP can also implement user behavior analysis to detect suspicious activities and potential insider threats, helping prevent data breaches from within the organization.

M: +91 90290 00574 | **Email Id:** salman.khan1.creative@tatatel.co.in