

Microsoft Azure Data Loss Protection

The definition of what sensitive data is has expanded over the years. This increases the need for organizations to re-evaluate their security and risk management practices

The lack of visibility on the business processes that affect sensitive information and application usage can be detrimental to the organization. The organization could be left vulnerable to data relocation, duplication, and removal from the corporate network without your knowledge. Dimension Data can extend your organization's visibility across your IT landscapes with Microsoft's Data Loss Protection. This visibility provides the basis for deciding what to allow, what to restrict and what to block altogether. You also have flexibility in how you configure your Data Loss Protection policies. This allows you to prevent the unintentional or accidental sharing of sensitive information.

Microsoft 365 Data Loss Protection policies are how you monitor the activities that users take on sensitive items at rest, in transit, or in use and take protective actions.

Benefits of Data Loss Protection:

- MS Office 365 becomes one of today's best data loss prevention software with its comprehensive approach.
- Dependable suite for word processing, presentation and calculated sheets. It offers all you may need in one package, storage and file sharing.
- Great integration with most remarkable tools in the market.

What to Monitor

Predefined or custom policy templates to assist your organization in getting started

Microsoft 365 offers an abundance of predefined policy templates that speak to health and medical data, financial data as well as privacy data all for various countries and regions. Should you choose to create a custom policy, the available sensitive information types, sensitivity labels and retention labels will be used.

Where to Monitor

Select one or more locations that you want DLP to monitor for sensitive information.

Monitor Exchange email, SharePoint sites, OneDrive accounts, Teams chat and channel messages and on-premises repositories to name a few.

Match Policy Conditions

Accept pre-configured conditions or define custom conditions.

Accept pre-configured conditions or define custom conditions. A few examples are:

- Item should contain specified sensitive information used in particular contexts
- Item has a definite sensitivity label

Policy Action

Determine the action to take when the policy conditions are met.

Depending on the location where the activity is occurring, a few examples are:

- Teams Chat and Channel: Block sensitive information from being shared in the chat or channel
- On-premises file shares: move the file from where it is stored to a quarantine folder.

How Data Loss Protection works to achieve business benefits



Dimension Data Solution

- Data-centric protection for sensitive information without the need for an additional agent, enabling you to prevent risky or inappropriate sharing, transfer, or use of sensitive data in accordance with your organization's policies.
- Get insights when sensitive data is accessed and shared directly from the Activity Explorer in the Microsoft 365 compliance center.
- Having the right data protection and governance approach to address regulatory compliance and privacy
- Mitigates data leaks and risks by providing context-based policy enforcement for data at rest, in use, and in motion on-premises and in the cloud.



Joint Solution

- Advanced capabilities to help you make informed risk-management decisions
 - Dedicated tool that assists you in identifying your data, protecting your data and preventing data loss
 - Data Loss Protection capabilities extended to items that are used and shared on Windows 10 computers
-



Tangible Benefits / Desired Outcomes

- Monitor and protect your data at rest, data in use and in motion on-premises and in the cloud.
- Gain visibility into discovered content and where that content is.
- Monitor what's being done with your sensitive data.
- When a user performs an action that meets the criteria of a DLP policy, DLP provides alerts in the DLP alert management dashboard.
- Organization meets compliance requirements and protects sensitive information on endpoints.
- Manage your DLP policies across Microsoft 365 from one location.
- Take maximum advantage of Dimension Data industry benchmarking and NTT's leading security technology providers

Why Dimension Data?



Dimension Data has a proven track record as a Microsoft partner with a large skilled and experienced team of Microsoft-certified specialists. From consulting to managed services, we ensure the right data protection and governance approach to address regulatory compliance. We assess current IT landscape, deliver recommendations and a roadmap for optimization. Along the way, offering guidance through complexities and intricacies of monitoring what has been done with your sensitive data. As Microsoft's Partner of the Year, we offer bespoke business solutions using a SAFe Agile methodology and globally integrated ITIL processes. With our highly skilled application, security teams, we guarantee excellence in delivery. Dimension Data is able to provide a full end-to-end solution to an organisation in every industry vertical. Our capability across the full IT stack enables us to provide supporting services giving you an advantage.