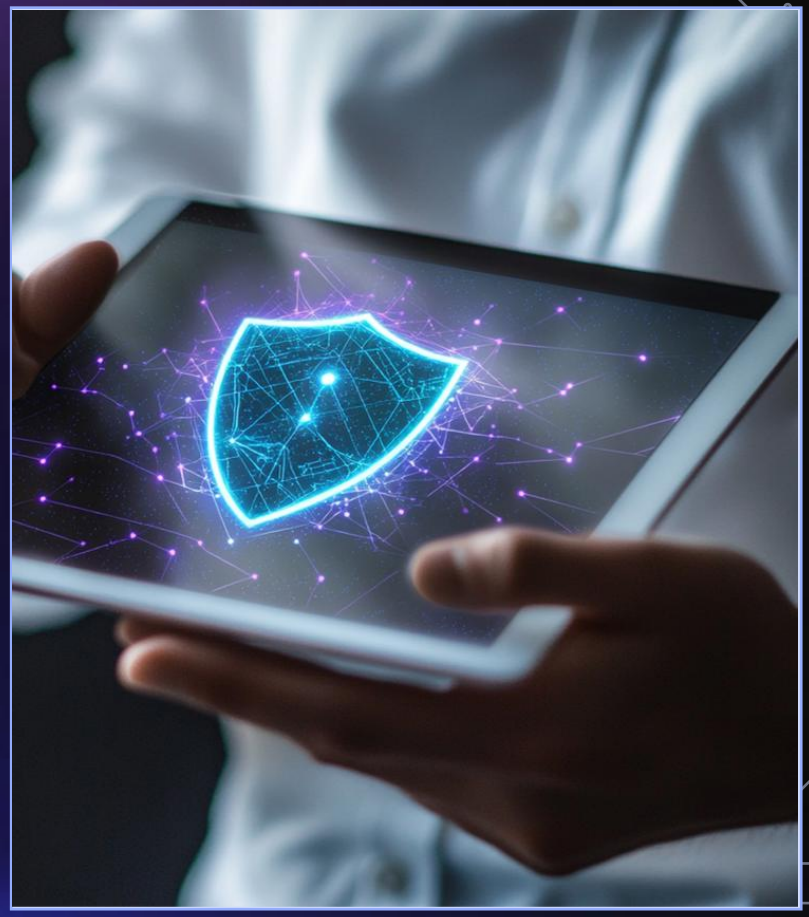
Microsoft Purview

Sensitivity Labels in Microsoft Purview

Contents

01

Creating & Configuring Sensitivity Labels



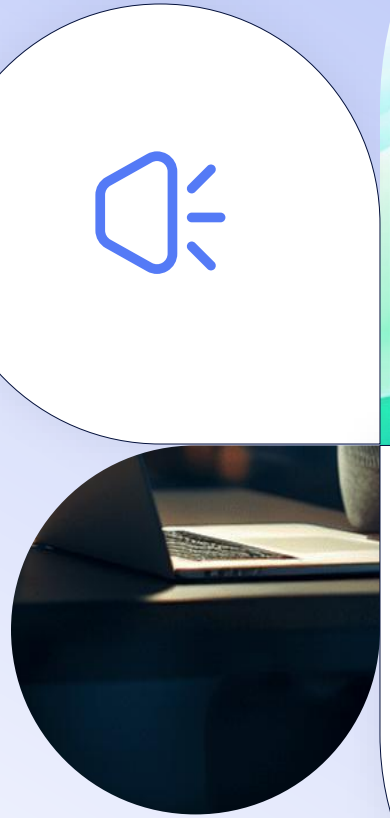
Definition and Importance

Overview

Sensitivity labels classify and protect sensitive data by applying relevant security settings. They can be used to “drive” different compliance activities.

Business Implications

Implementing sensitivity labels can enhance data security and ensure compliance with regulations.



Steps for Creation

Initial Configuration

Begin by defining label names, descriptions, and the protections settings to be applied. Best practices suggests a defined and consistently applied standard at the enterprise level.

Publishing Labels

Labels must be published to be available for users or auto-labeling policies. We'll see some of this in our lab(s).

Advanced Features

Customization Options

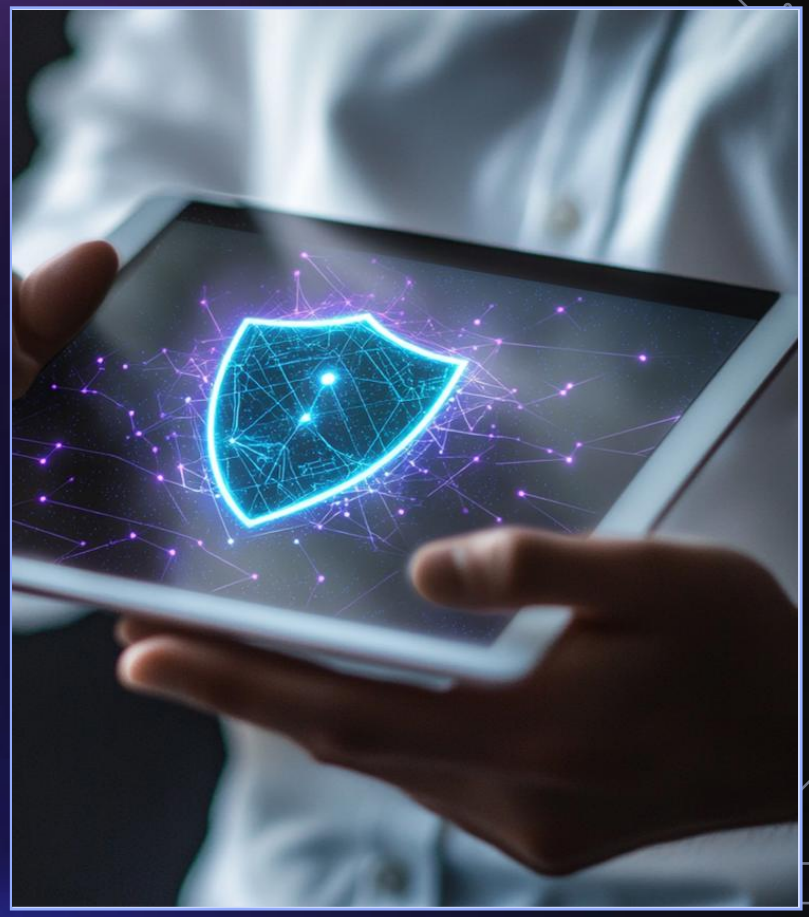
Customize sensitivity labels to meet specific organizational needs, including user permissions.

Handling Protected Data

Sensitivity labels can manage encryption and protection across different environments. This is part of their power.

02

Label Policies and Publishing



Policy Configuration

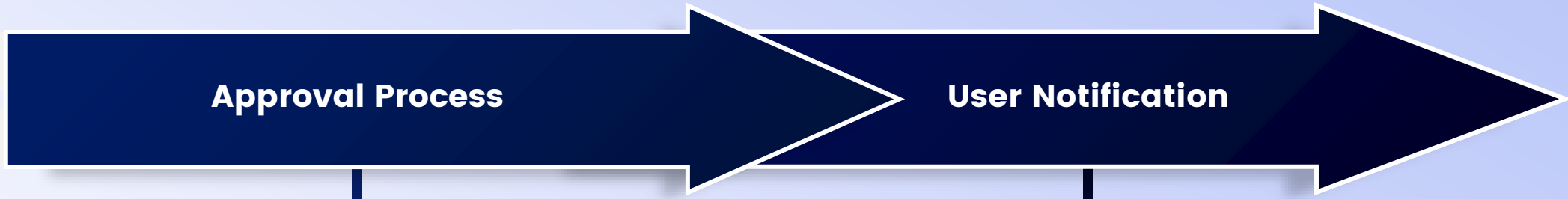
Defining Policies

Organizations must define policies that specify how sensitivity labels are applied and enforced.

User Groups

Labels can be published to specific user groups within the organization to ensure targeted protection.

Publishing Workflow



Establish approval workflows to make sure labels are correctly configured before being published. Use simulation mode (before activating) auto-labeling policies to assess impact.

Notify users about new or updated sensitivity labels and their impact on data handling practices. If users are unfamiliar or unaware, they may not manually label correctly where required or auto-labeling can be disruptive and confusing.

Policy Management

Regular Updates

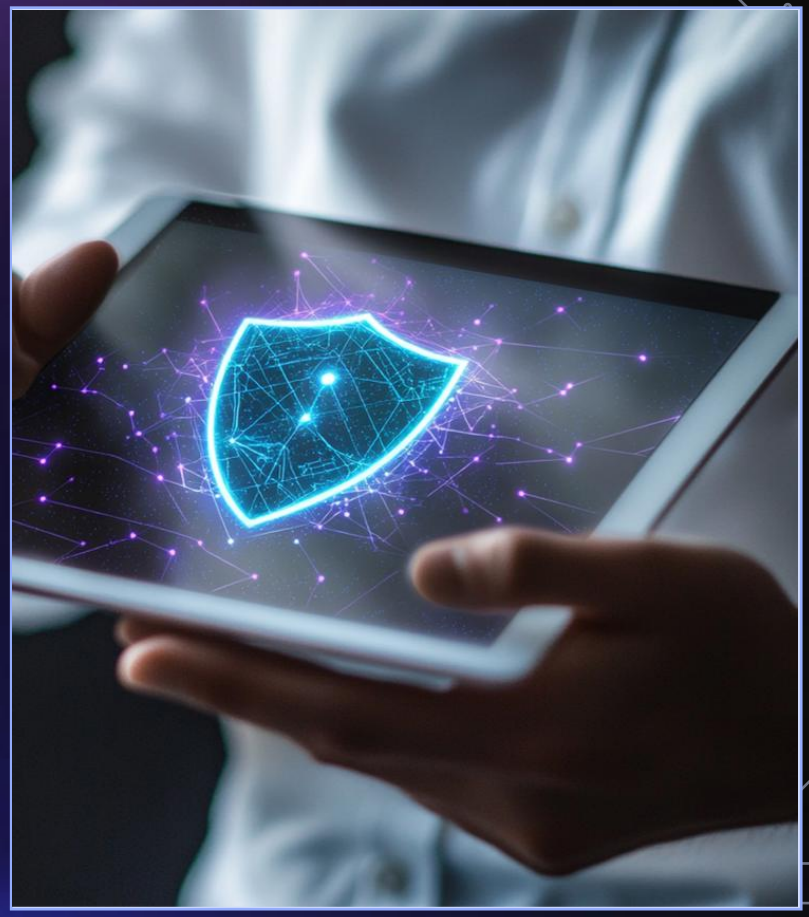
Regularly update policies to adapt to new security threats and compliance requirements.

Monitoring Compliance

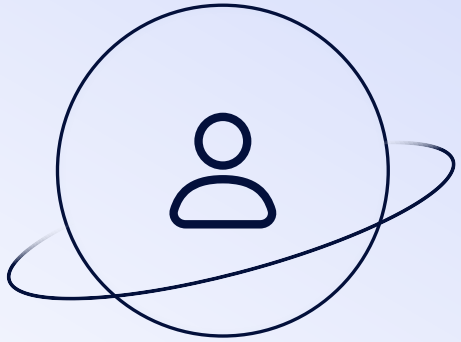
Continuous monitoring ensures labels are being applied correctly and policies are effective.

03

Configuring Encryption through Sensitivity Labels

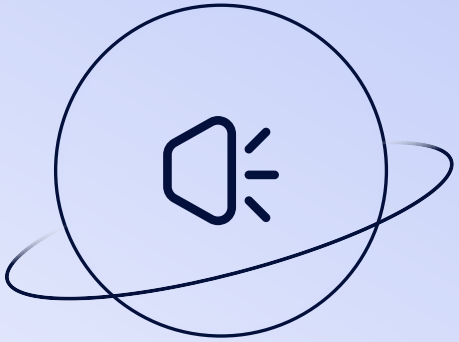


Types of Encryption



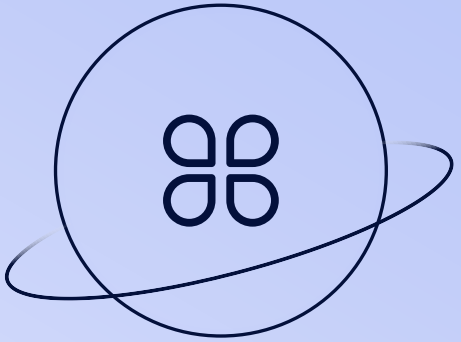
Symmetric Encryption

Symmetric encryption uses the same key for encryption and decryption, providing quick data protection.



Asymmetric Encryption

Asymmetric encryption involves a public key for encryption and a private key for decryption, ensuring high security.



Hybrid Encryption

Hybrid encryption combines the benefits of both symmetric and asymmetric encryption for optimal security.

Implementing Encryption

Policy Settings

Configure sensitivity label policies to enforce encryption standards on sensitive information.

Key Management

Effective key management practices are going to be crucial for maintaining the fidelity of encryption and encryption security.

User Access Controls

01.

Permissions

Set permissions to control who can access and modify encrypted data based on sensitivity labels.

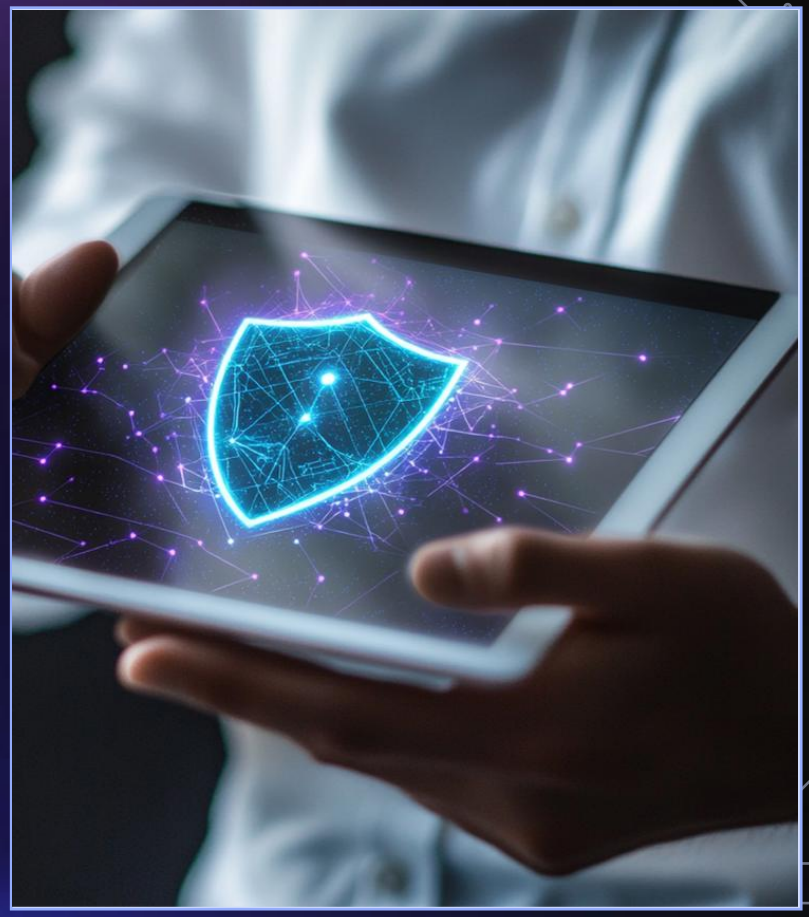
02.

Training

Provide training for employees on how to handle encrypted data within their business processes. This can be a difficult concept to grasp – especially for non-technical resources.

04

Auto-Labeling Policies



Auto-Labeling Introduction

Definition

Auto-labeling policies automatically apply sensitivity labels to data based on pre-defined rules.

Benefits

Automates data protection processes and reduces the administrative burden on IT departments. Also, if configured and applied correctly, it can help alleviate errant or missed labeling.

Configuration Steps

01 Setting Rules

Define rules based on data types, locations, or content that trigger automatic label application.

02 Testing Policies

Test auto-labeling policies in a pilot phase to ensure they work as intended before wider deployment. As previously mentioned, simulation mode can help here. Also, creating a smaller group and associating to just that pilot set of users allows you to explore and understand impact and effect.

Optimization

Review and Adjustments

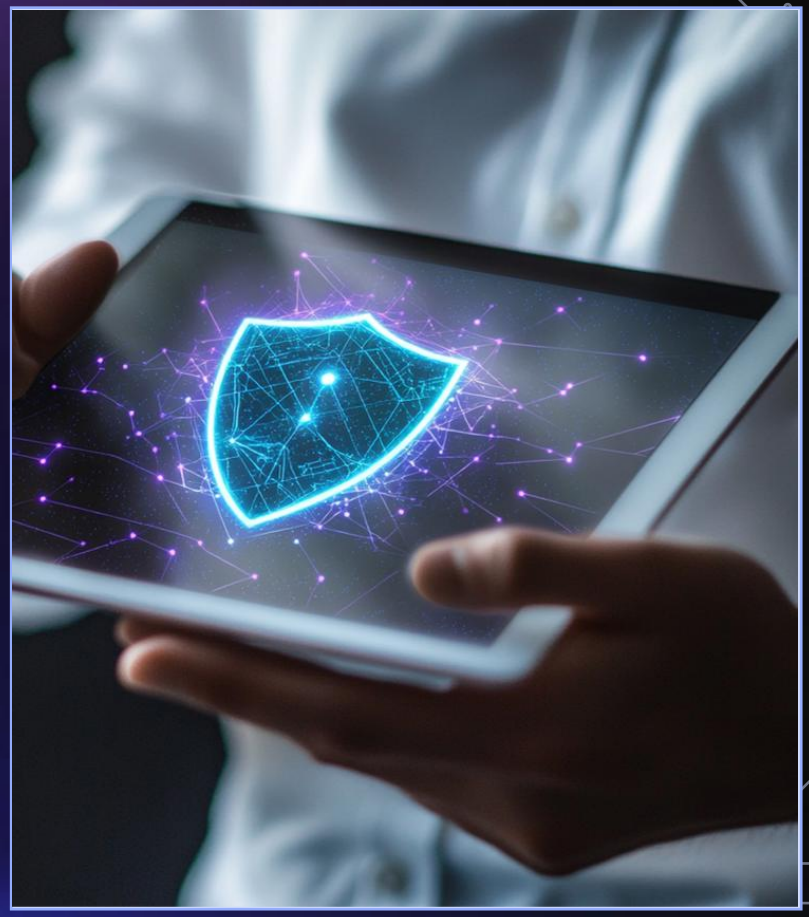
Regularly review the effectiveness of auto-labeling rules and make necessary adjustments.

Feedback Mechanism

Establish a feedback loop to gather user input on auto-labeling accuracy and performance. As with anything, practice continuous improvement via solicited (or unsolicited) feedback.

05

Tracking Sensitivity Label Usage



Monitoring

- **Usage Reports**

  Generate reports to monitor how and where sensitivity labels are being used across the organization.

- **Anomaly Detection**

  Tools to detect anomalies in sensitivity label application can identify potential security threats.

Compliance and Auditing

Data Audits

Conduct regular data audits to ensure that sensitivity labels and associated policies are correctly applied.

Regulatory Compliance

Tracking label usage helps in demonstrating compliance with industry regulations and standards.

Strategy Integration

Zero Trust Architecture

Integrate sensitivity labels with zero trust strategies for comprehensive security.

Defense-in-Depth

Use sensitivity labels as part of a multi-layered defense strategy (defense in depth) to protect data from various threats at various levels.

Thanks