DATA & AI

Data Security

Protect your data with Microsoft Purview

REPLY CLUSTER

PURVIEW FEATURES

Why should organization rely on Microsoft Purview?

User Experience

Microsoft Purview offers an Office-like interface that is both intuitive and familiar, making it easy for users to adopt and integrate into their daily workflow. The user experience is designed to be seamless without a steep learning curve.

Visibility and Control

Provides comprehensive visibility over your data, enabling secure management and going beyond mere compliance.

Comprehensive Protection

It safeguards sensitive data across different platforms, apps, and clouds, ensuring a complete solution for information protection and data governance.

Risk Management and Compliance

Microsoft Purview assists in identifying data risks and managing regulatory requirements, ensuring high compliance levels for your organization. It also prevents data loss with intelligent detection and control of sensitive information, protecting data across apps, services, and devices.

REPLY CLUSTER

Data Security Workflow

Our Approach

Explore and know your sensitive data

Knowing where your sensitive data resides is often the biggest challenge for many organizations. Microsoft Purview Information Protection data classification helps you to **discover** and accurately **classify** ever-increasing amounts of data that your organization creates.

Information Protection

It’s a comprehensive data protection solution that classifies, **encrypts**, and **restricts access** to sensitive documents. It ensures that only authorized users can access protected data. Key features include sensitivity labels, encryption, and access controls to safeguard sensitive information.

Data Loss Prevention

Deploy Microsoft Purview Data Loss Prevention (DLP) policies to govern and **prevent the inappropriate sharing, transfer, or use** of sensitive data across apps and services. These policies help users make the right decisions and take the right actions when they're using sensitive data.

Inside Risk Management

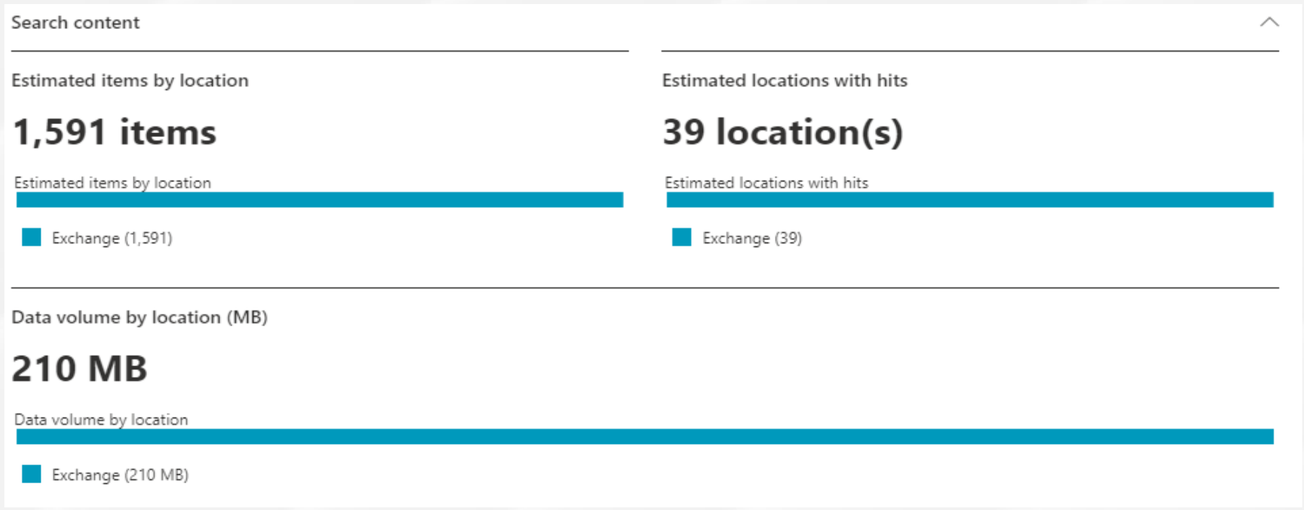
Insider Risk Management helps minimize **internal risks** by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization. Insider risk policies allow you to define the types of risks to identify and detect in your organization.

Explore and know your sensitive data

Microsoft Purview allows for the identification and classification of sensitive information, such as **personal and financial data**, across a wide range of data sources, both in cloud and on-premises environments. This is made possible through an automatic detection and accurately classifies sensitive information.

Additionally, it provides a detailed search function that
enables the search for specific data using precise business and technical terms.

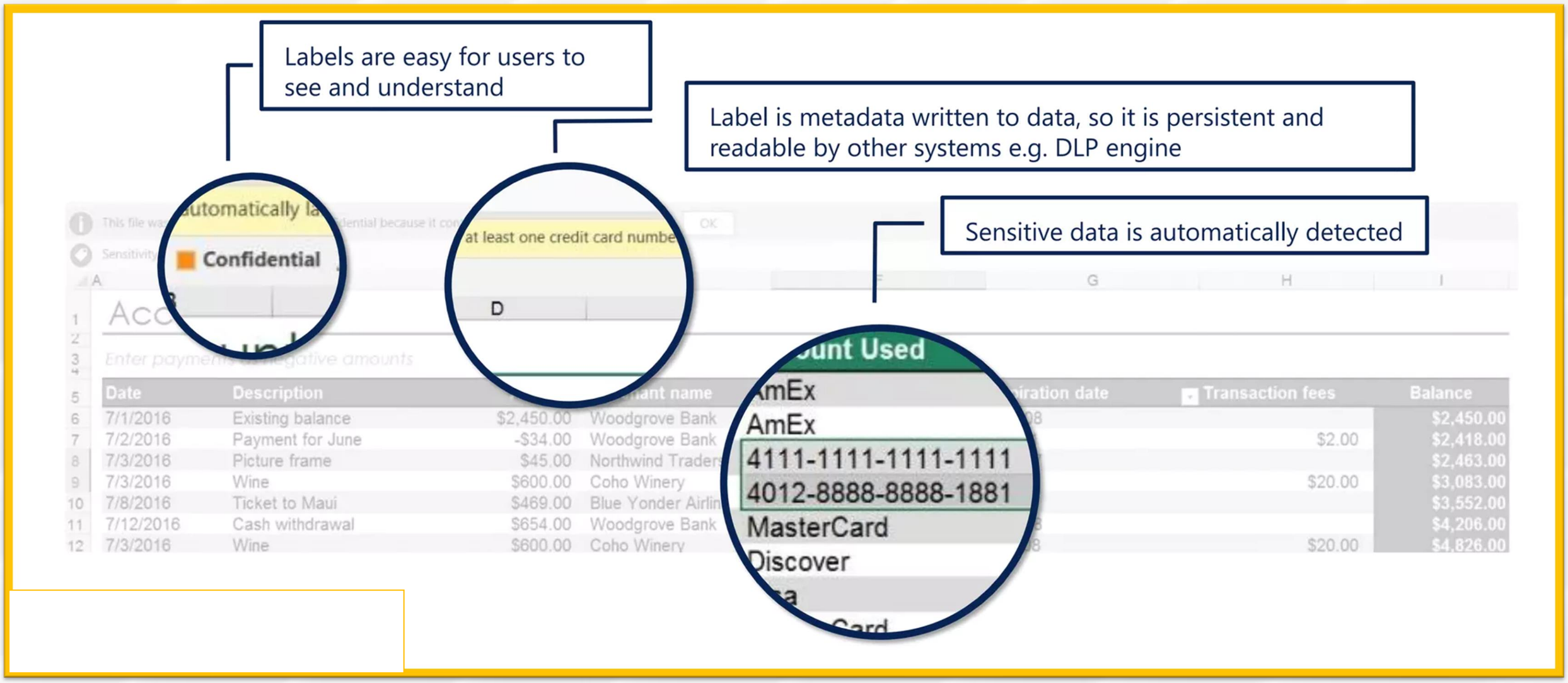
The system includes an integrated glossary (sensitive info type) that simplifies the process of searching for and identifying the necessary data.



REPLY CLUSTER

How sensitive data are detected?

Microsoft Purview SIT harnesses **pattern matching**, **evaluation functions**, and **AI** to pinpoint sensitive data, offering **multilingual support** and **customization** with adjustable **confidence levels** for precise, global data protection.



REPLY CLUSTER

Information Protection

Assigning labels to files or emails, you can efficiently manage and control access permissions for all files categorized under a specific **sensitivity label.**

Being in the public domain, this information does not require special protection

Contains information for general use within the organization

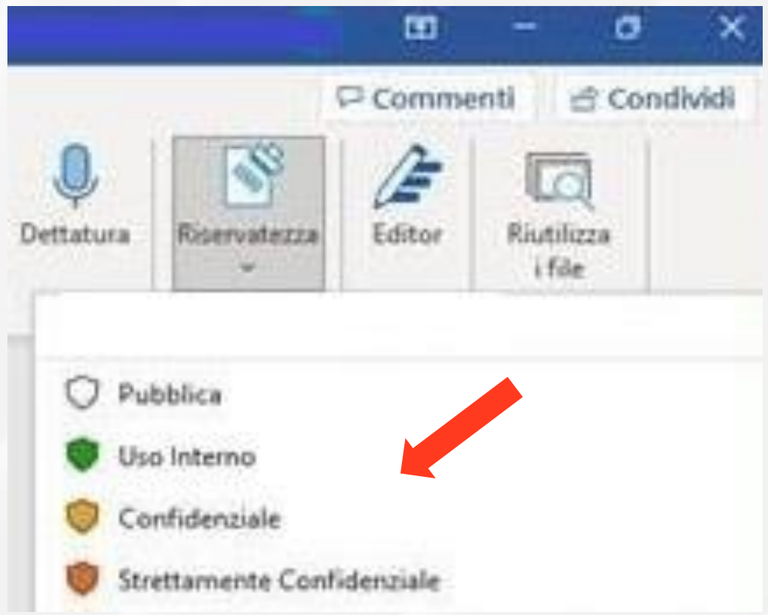
Contains private information,
any disclosure of this information may have a significant impact

Contains critical information,
any disclosure of information have serious or catastrophic impacts

REPLY CLUSTER

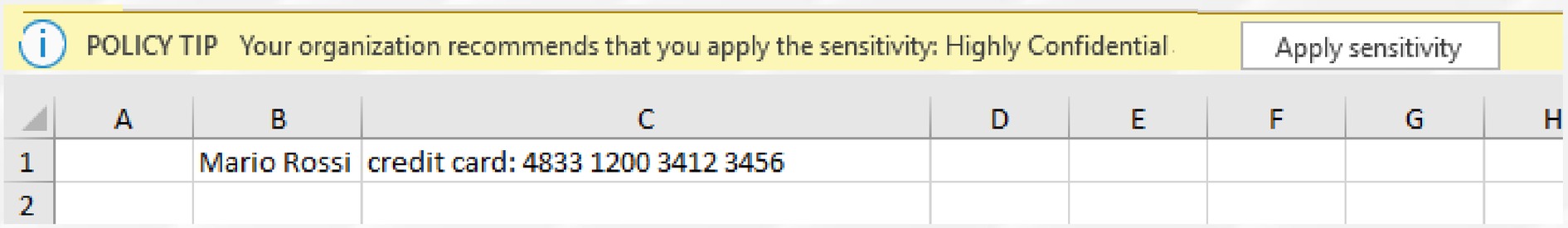
Label management

1. Manually applied by user interaction
   (By simply clicking on a ribbon built into the office apps)

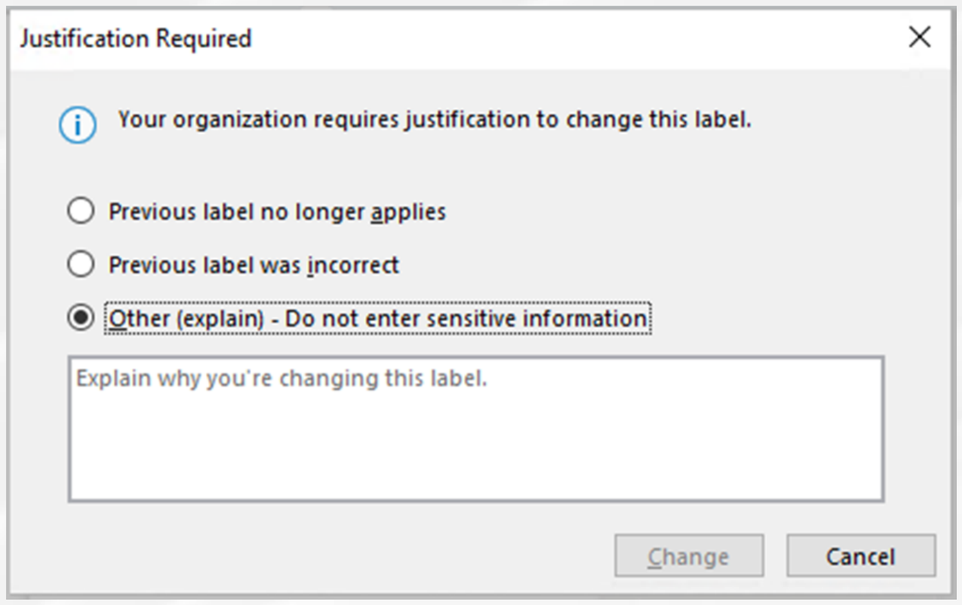


2. Default applied on a new files

3. Automatically applied by AI



4. Justification on downgrade



REPLY CLUSTER

Rights Management with Encryption

For each label, several operations are logged in **Activity Explorer**, such as reads, changes, file sends or uploads, label changes, renaming...

Activity	File	Location	User	Happened	Sensitivity label
Label removed		Endpoint devices	ignazio@MSDx836854.onmi...	Apr 3, 2024 11:32 AM	
Label applied	https://msdx836854-my.sharepoint.com/person...	Endpoint devices	admin@MSDx836854.onmic...	Mar 22, 2024 6:02 PM	Public
Label changed		Endpoint devices	ignazio@MSDx836854.onmi...	Mar 22, 2024 12:40 PM	Highly Confidential...

Once the data is classified, you can granularly apply rights management with encryption to each label. For instance:

For label Confidential you can allow access and modification to all authenticated users (even with other providers i.e Google)

For the label Highly Confidential allow access and modification only to insiders, and for outsiders read-only. It will also be possible to set special permissions to individual users or groups through custom rights

With encryption you can also prevent unauthorized users to copy content, screen share, edit file and permission, forward email.

REPLY CLUSTER

Data Loss Prevention

In Microsoft Purview, you can monitor, restrict, or block various events using Data Loss Prevention (DLP) policies:

Sensitive File Sharing: Implement stringent controls to monitor and restrict the sharing of files containing sensitive data, ensuring that only authorized personnel have access.

Confidential Email Transmission: Enforce policies that prevent the dissemination of sensitive information via email to unauthorized parties.

Website Access Management: Block access to unauthorized websites, maintaining security and adherence to compliance standards.

Inter-device Data Transfer: Prohibit the unauthorized movement of sensitive information between devices within the network.

Controlled Information Sharing: Regulate the distribution of proprietary business information through chat and messaging applications.

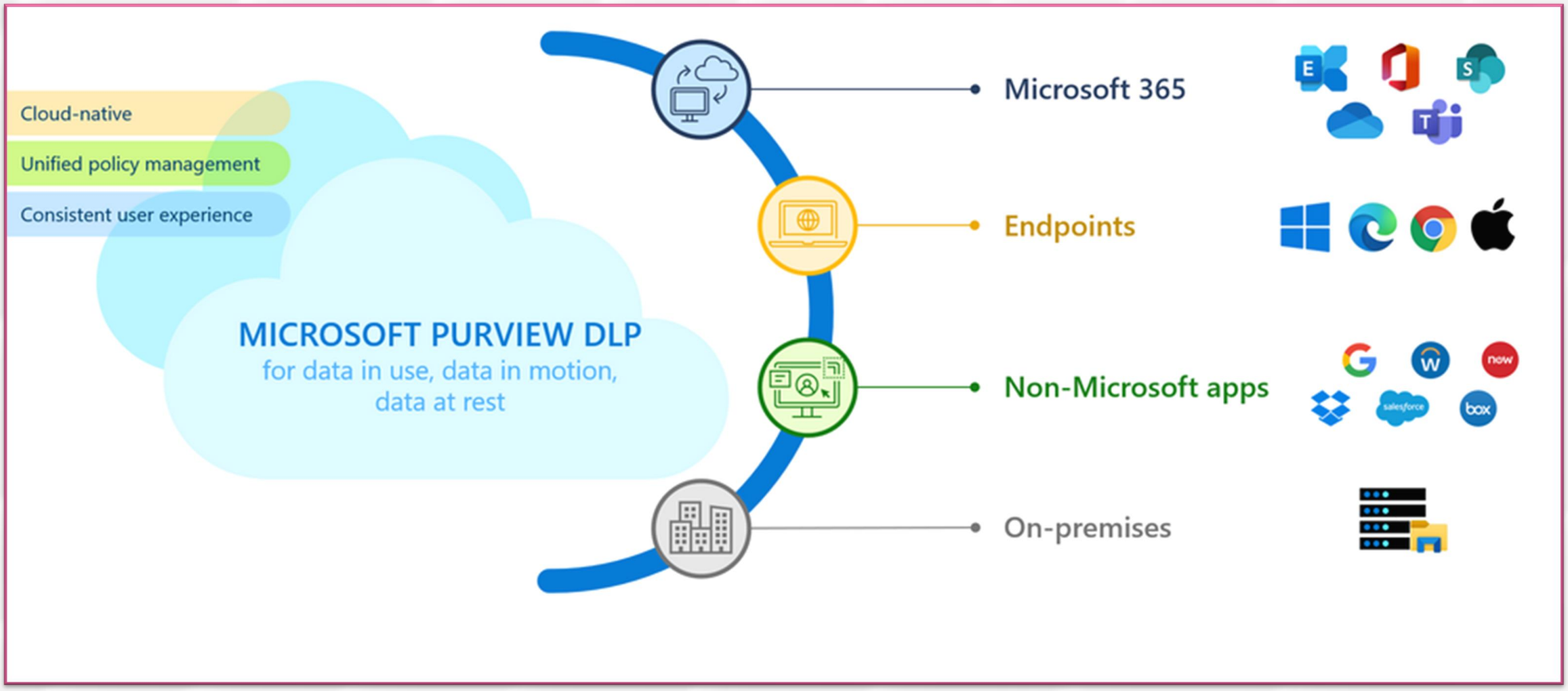
Geographical Access Restrictions: Limit access to cloud-based resources from specified geographical locations to comply with regional regulations.

Cloud Service Download Monitoring: Oversee and control the downloading of files from cloud services like OneDrive and SharePoint to prevent data leakage.

REPLY CLUSTER

Data Loss Prevention

To help protect sensitive you need a way to help **prevent** users from inappropriately sharing sensitive data with people who shouldn't have it.

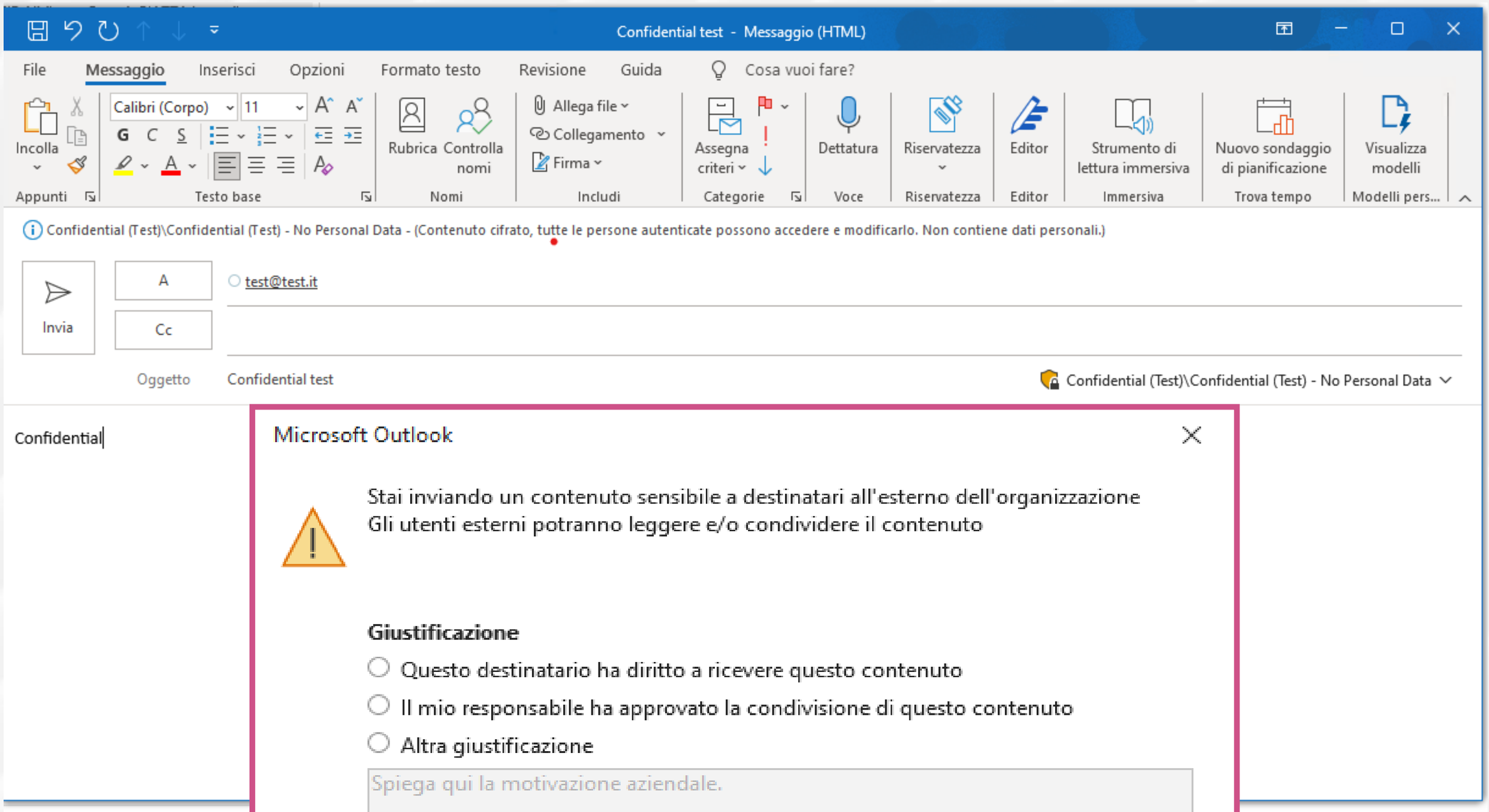


Prevention can be performed in 3 different ways:

1. Audit and suggestion to users with policy tips
2. Block with override
3. Block

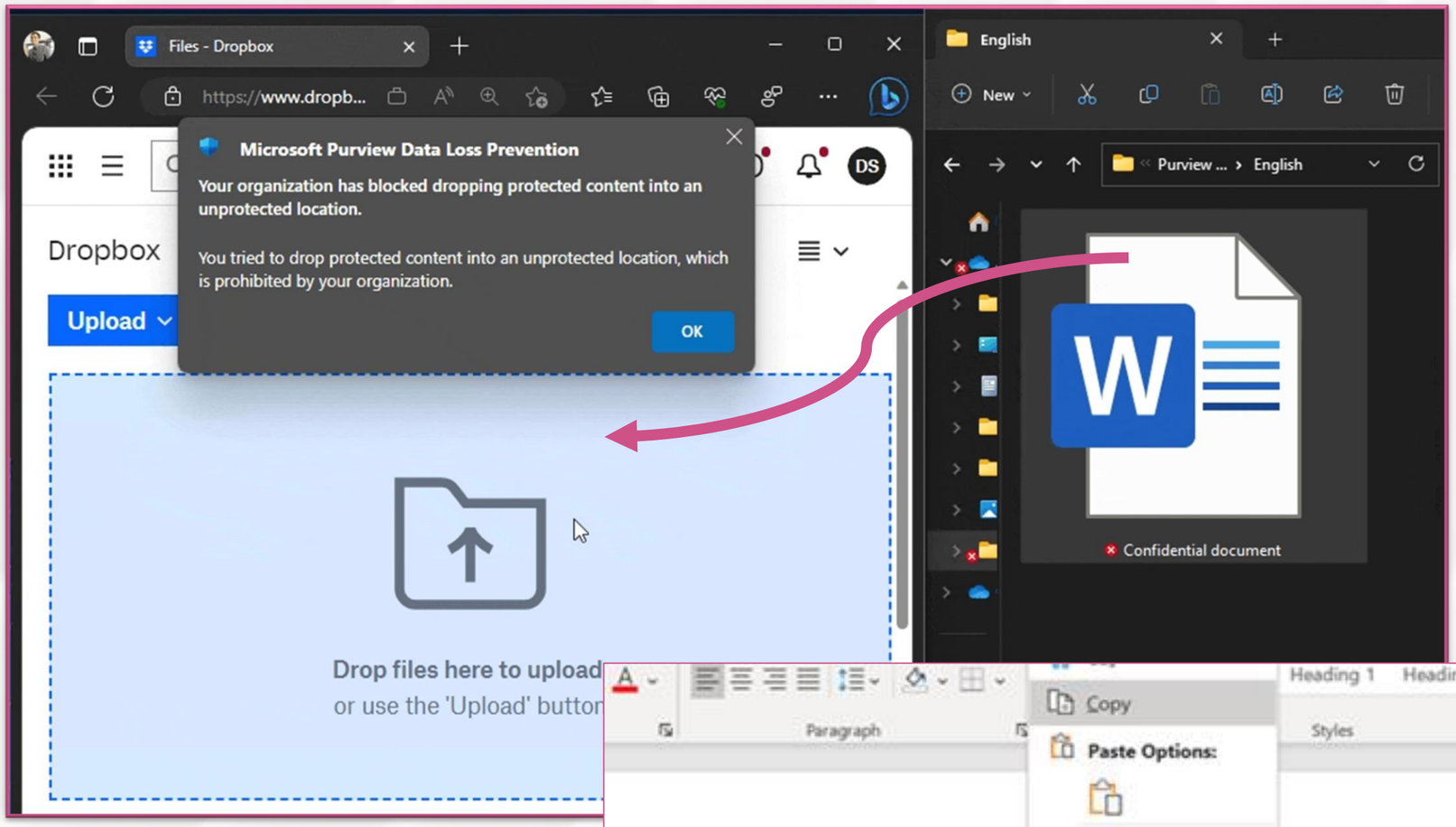
Use cases examples

Justification is required when users send confidential mail to an external recipient.



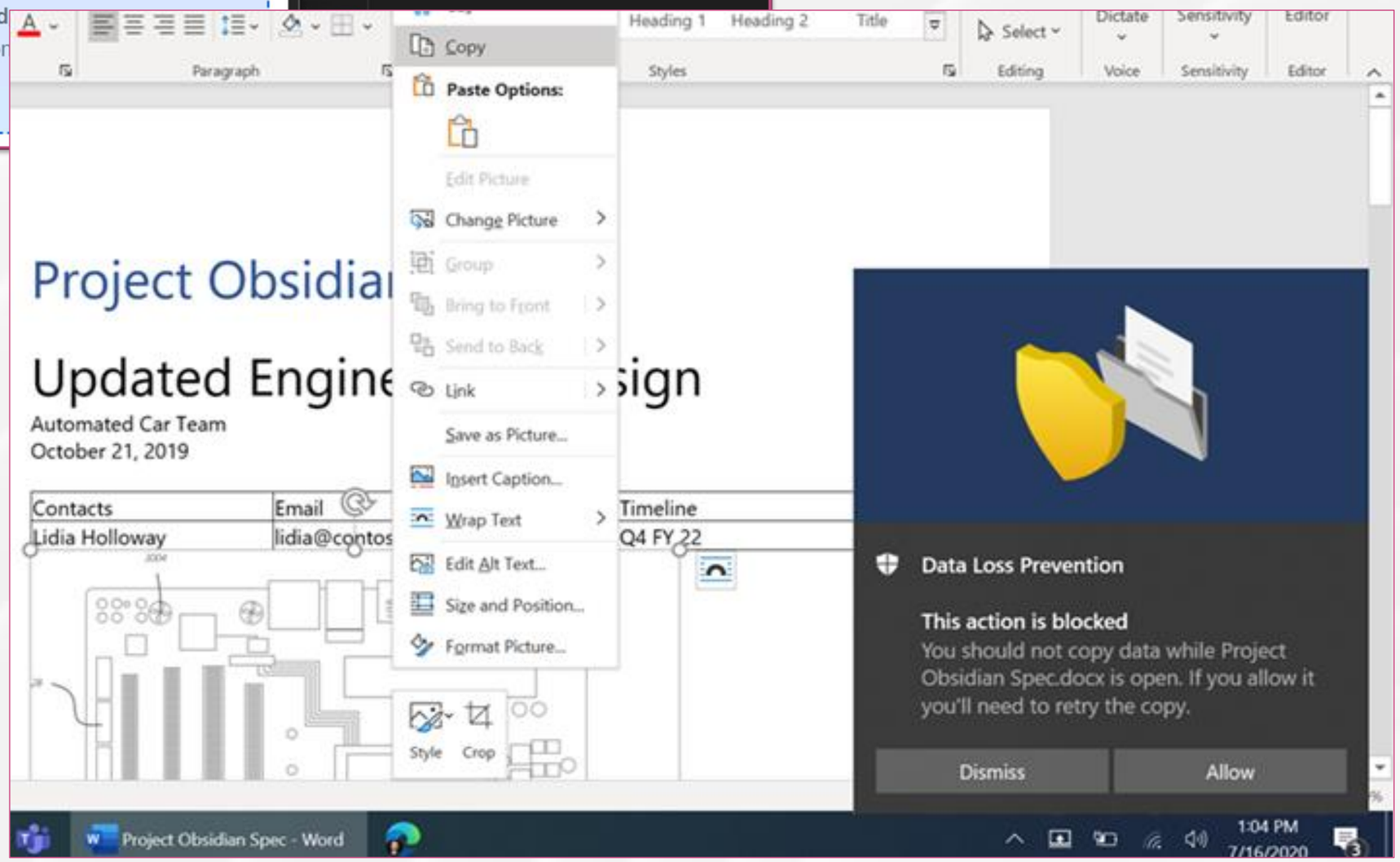
REPLY CLUSTER

Use cases examples



Block upload on untrusted domain

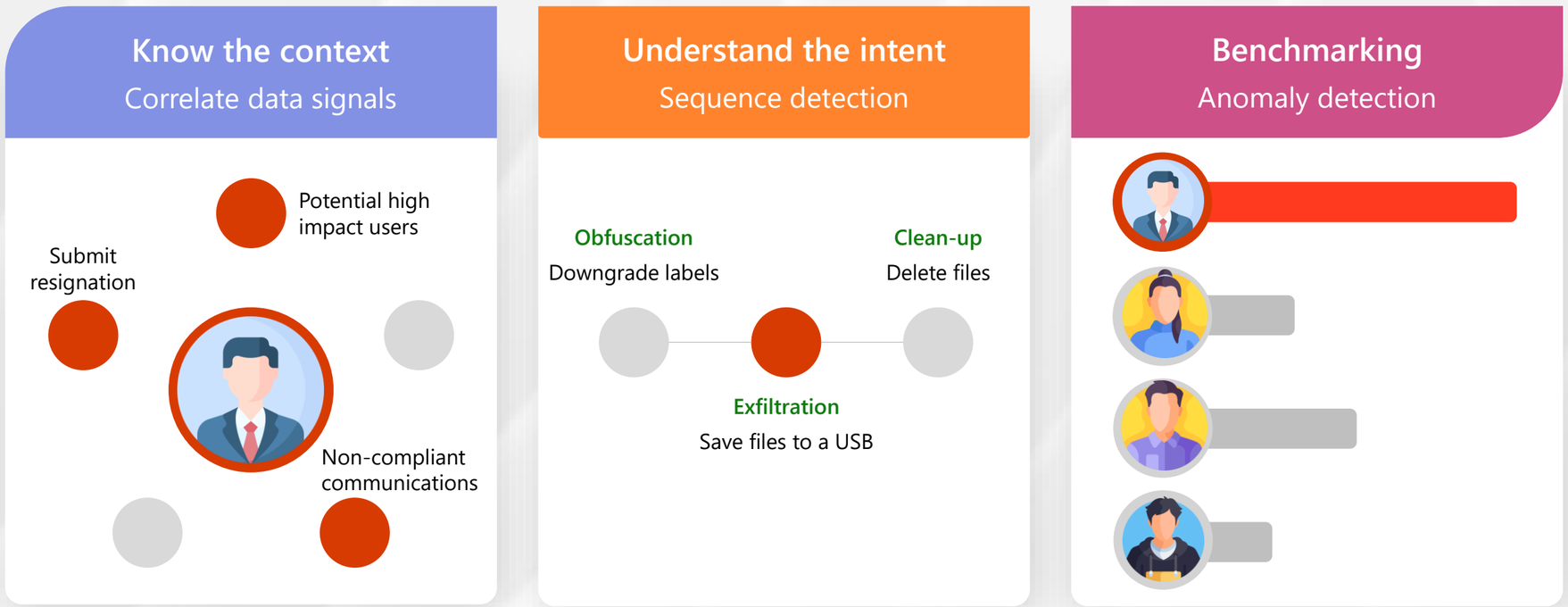
Alert the user when they attempt to copy or paste a section containing sensitive information



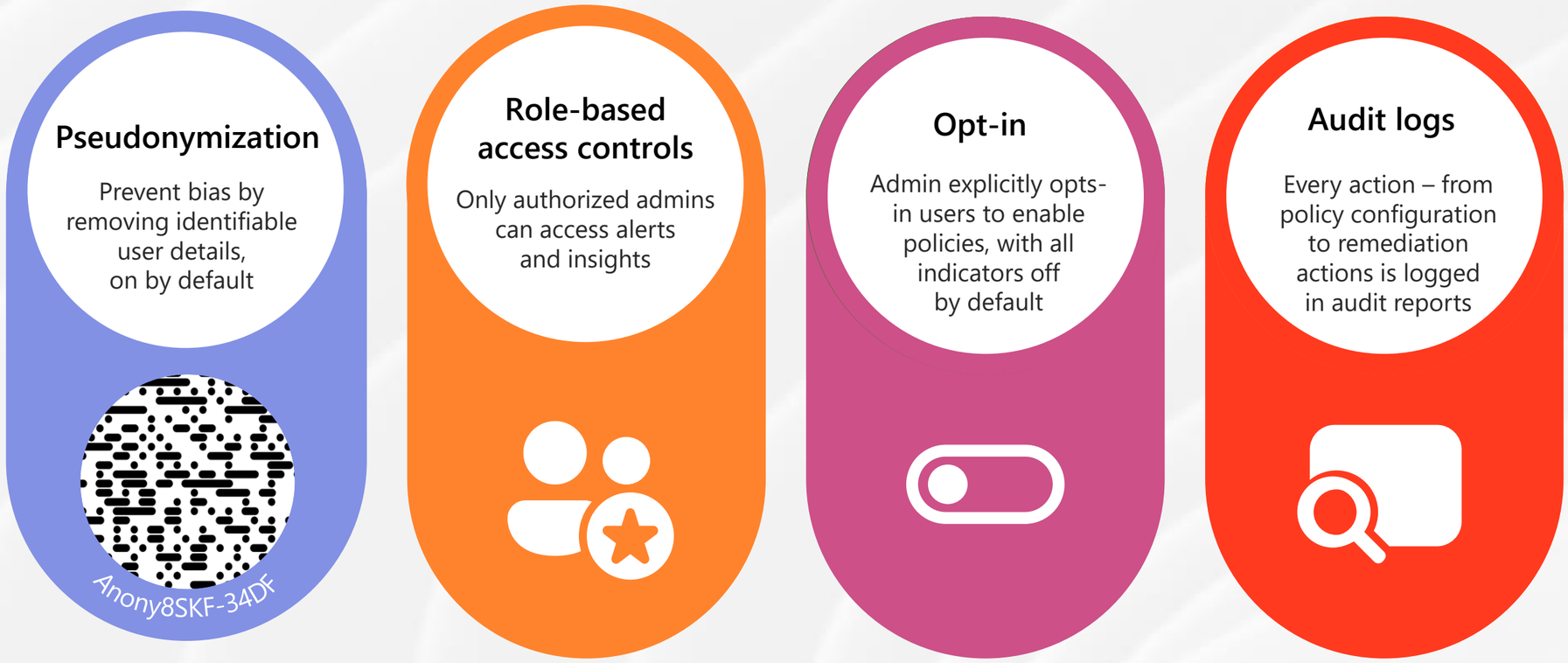
REPLY CLUSTER

Insider Risk Management

Data doesn’t move itself: **users move data**. You need to understand the **context** and user **intent** around your data to effectively protect it.



Insider Risk Management intelligently detect and mitigate internal risk, correlates various signals to identify potential **malicious** or **inadvertent** insider risks (IP theft, data leakage and security violations) and allows to create policies to manage security and compliance. User **privacy** is maintained every step of the way:



REPLY CLUSTER

Insider Risk Management Features

Insider Risk Management can detect internal risks with over **100 built-in machine learning models** and **indicators**, simplifying a lot the collection and correlation of events and risky activities.

Once internal risks are detected, it may take too long to act. Insider Risk Management provides additional investigation tools such as **Adaptive Protection**, which applies the most effective DLP controls on users with high risk levels to help mitigate internal risks at an early stage, before full investigations can take place.

Privacy

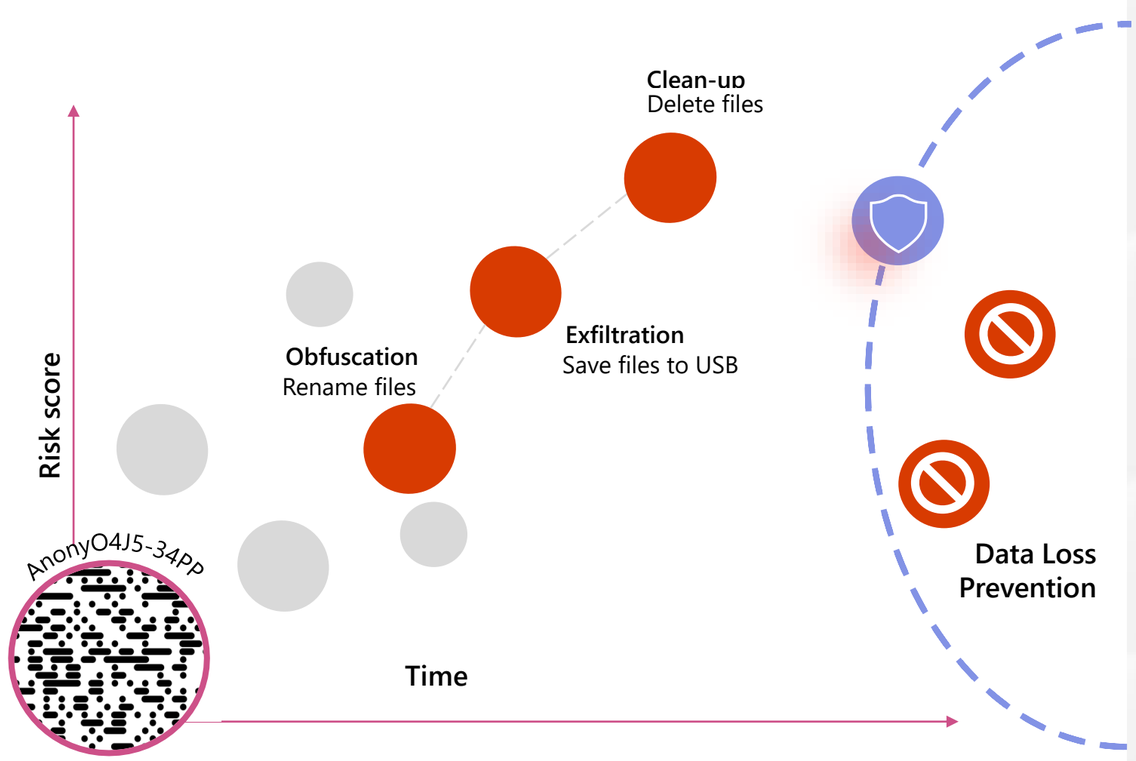
Protect user trust and build a holistic insider risk program with **pseudonymization** and strong privacy controls.

Simplicity

Identify hidden risks with **100+ built-in machine-learning models** and **indicators**, requiring no endpoint agents.

Acceleration

Expedite mitigation with enriched investigations and **Adaptive Protection** that enforce DLP controls dynamically.



REPLY CLUSTER

Insider Risk Management Workflow

- **Analytics**: allows you to assess potential internal risks in your organization without configuring policies in advance. This assessment identifies higher-risk areas and events to determine better the type and scope of policies to configure.
- **Policy → Alerts**: After setting policies, alerts are generated for new risky user activities.
- **Triage → Investigate:** If an alert is analyzed and identified as an actual risk, an associated case is created that has tools for deeper investigation: A chronological timeline of all alerts, alert details, the current risk score for the user, and the sequence of risk events.
- **Action:** to remedy cases it is possible to perform different case actions, ranging from a simple reminder email to the opening of an investigation involving the legal team.

REPLY CLUSTER

Recap on our approach

Explore and know your sensitive data

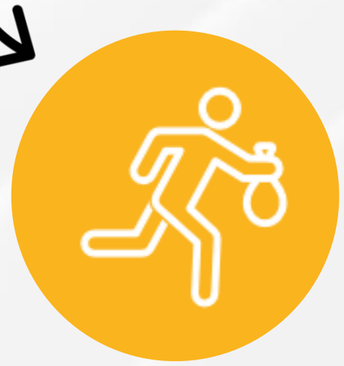
Knowing where your sensitive data resides is often the biggest challenge for many organizations. Microsoft Purview Information Protection data classification helps you to **discover** and accurately **classify** ever-increasing amounts of data that your organization creates.

Information Protection

is a comprehensive data protection solution that classifies, **encrypts**, and **restricts access** to sensitive documents. It ensures that only authorized users can access protected data. Key features include sensitivity labels, encryption, and access controls to safeguard sensitive information.

Data Loss Prevention

Deploy Microsoft Purview Data Loss Prevention (DLP) policies to govern and **prevent the inappropriate sharing, transfer, or use** of sensitive data across apps and services. These policies help users make the right decisions and take the right actions when they're using sensitive data.



Inside Risk Management

Insider Risk Management helps minimize **internal risks** by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization. Insider risk policies allow you to define the types of risks to identify and detect in your organization.

DATA & AI

REPLY CLUSTER

Contact us!

Marco Bersaglia
m.bersaglia@reply.it

Ignazio Massaro
i.massaro@reply.it

WWW.CLUSTERREPLY.IT