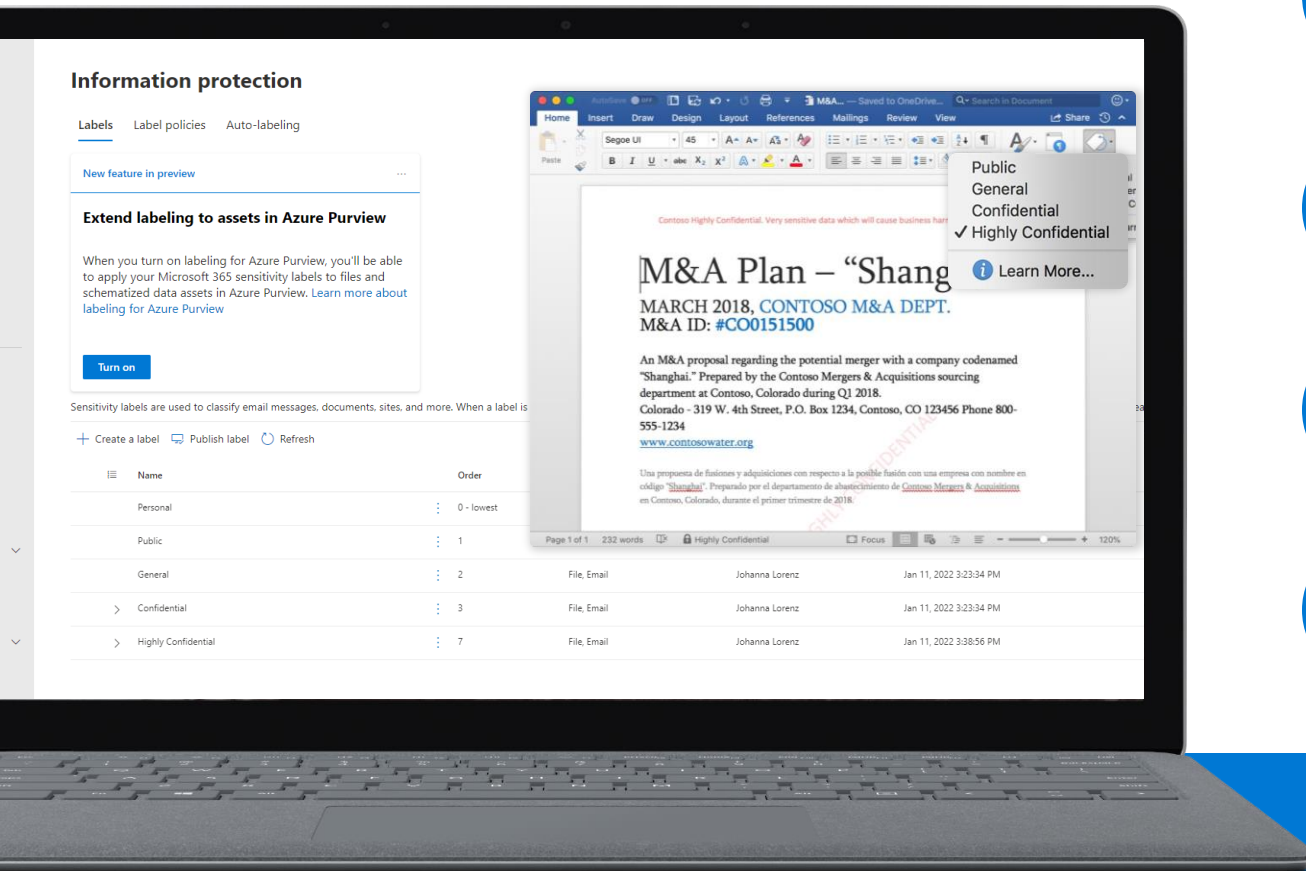


# Microsoft Purview Information Protection

A built-in, intelligent, unified, and extensible platform and solution to protect sensitive data



## Built in

Built-in labeling and protection experience in Office apps, Office 365 services, other MS services like Power BI, Edge, and Windows



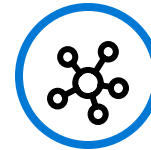
## Intelligent

Accuracy in classification via ML based trainable classifiers exact data match and named entities



## Unified

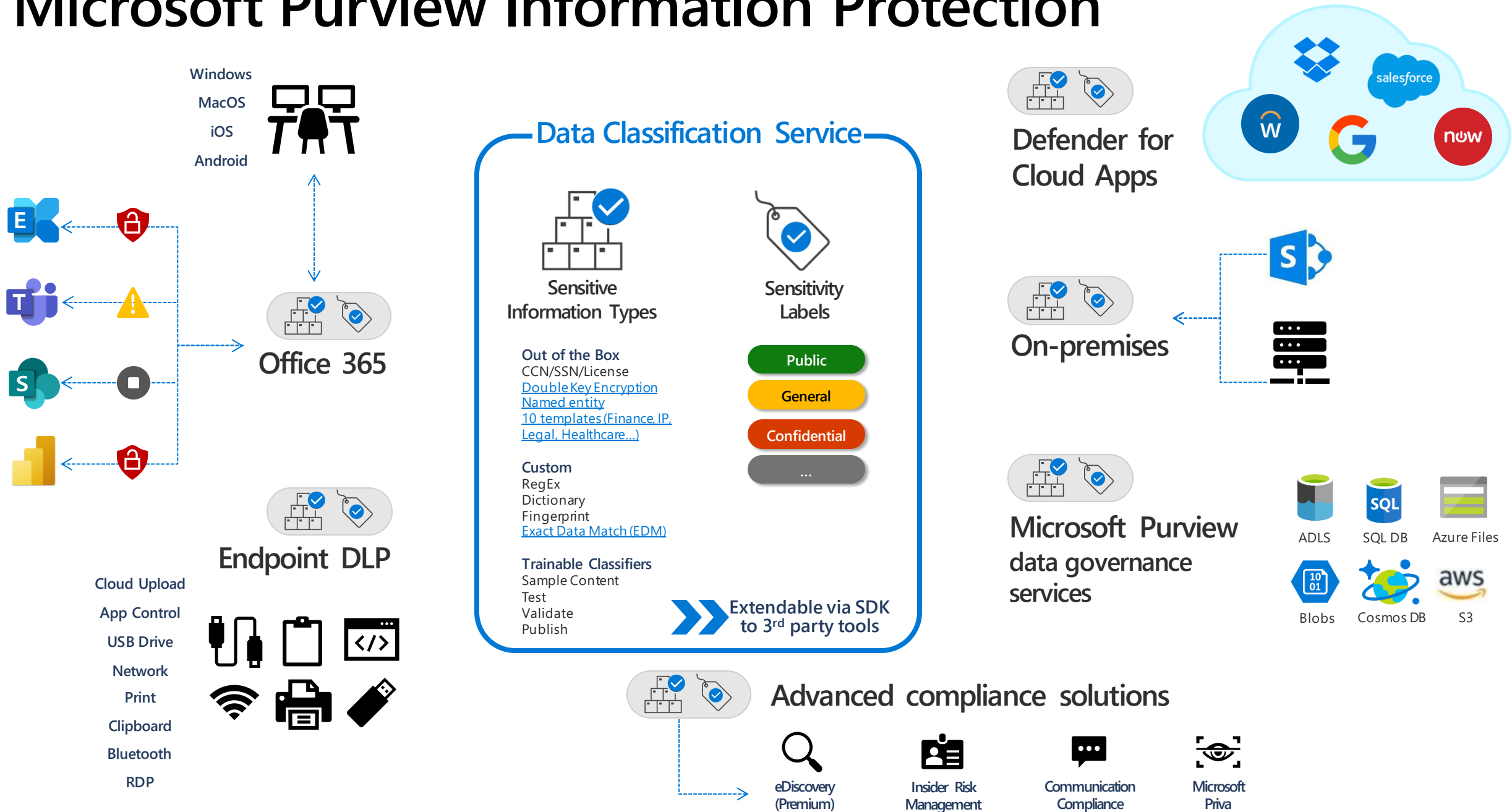
Single admin console to configure and manage your policies and view analytics across on-premises, Office apps, Microsoft 365 services, third-party services (via Microsoft Defender for Cloud Apps), and devices



## Extensible

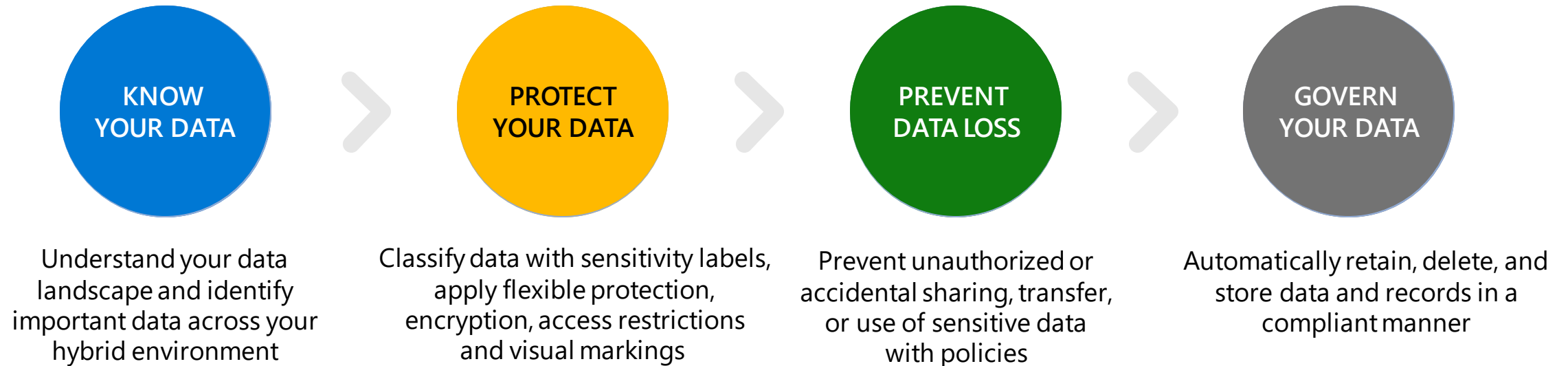
MIP SDK extends the protection experience, in a consistent way, to popular non-Microsoft apps and services

# Microsoft Purview Information Protection



# Information protection & governance

Protect and govern data wherever it lives



## POWERED BY AN INTELLIGENT PLATFORM

Unified approach to automatic data classification, policy management, analytics, and APIs



Devices



Apps



Cloud services



On-premises



ISV/3<sup>rd</sup> party

# Data classification

- Overview
- Trainable classifiers
- Sensitive info types
- Exact data matches
- Content explorer
- Activity explorer

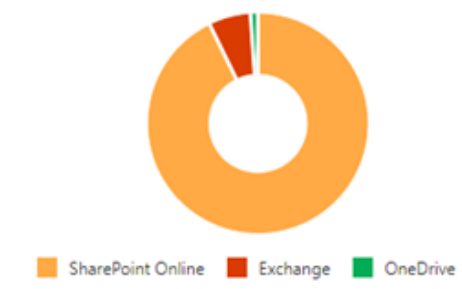
Get snapshots of how sensitive info and labels are being used across your organization's locations. [Learn more](#)

## Top sensitive info types



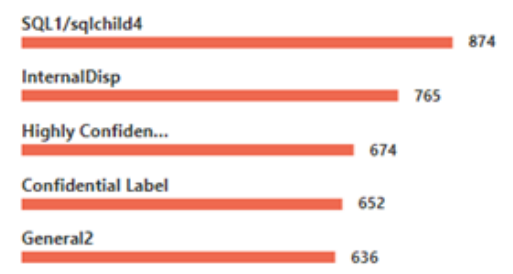
[View all sensitive info types](#)

## Locations where sensitivity labels are applied



[View details](#)

## Top sensitivity labels applied to content



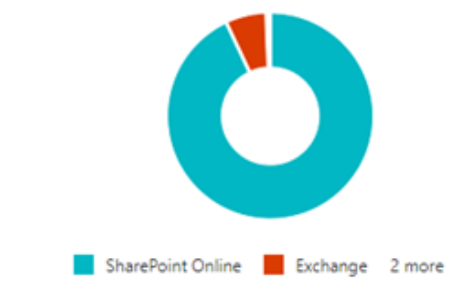
[View all applied sensitivity labels](#)

## Top retention labels applied to content



[View all applied retention labels](#)

## Locations where retention labels are applied



[View details](#)

# Protect your data

Classify data and apply unified sensitivity labels to sensitive data



## NEW AND RECENT ADVANCEMENTS

- Protect content with Sensitivity Labels using double-key encryption
- Auto-labeling on SPO/ODB and EXO DIT with additional conditions & increased scopes
- Enhanced simulation mode

Excel

Confidential... Confidential\All Employees • Saving... MOD Administrator

File name: Confidential Customer List.xlsx

Location: 02-Confidential Contoso » Shared Documents » Seed data

Version History

Sensitivity: admin@M365x02473751.onmicrosoft.com

Personal

Public

General

✓ Confidential

Highly Confidential

Conditional Formatting

Format as Table

Cell Styles

Cells

Editing

Analyze Data

Sensitivity

	C	D	E	F
1	Muhammed MacIntyre	3	-213.25	38.94
2	Barry French	293	457.81	208.16
3	Barry French	293	46.71	8.69
4	Clay Rozendal	483	1198.97	195.99
5	Carlos Soltero	515	30.94	21.78
6	Carlos Soltero	515	4.43	6.64
7	Carl Jackson	613	-54.04	7.3
8	Carl Jackson	613	127.70	42.76
9	Monica Federle	643	-695.26	138.14
10	Dorothy Badders	678	-226.36	4.98
11	Neola Schneider	807	-166.85	4.28
12	Neola Schneider	807	-14.33	3.95
13	Carlos Daly	868	134.72	21.78
14	Carlos Daly	868	114.46	47.98
15	Claudia Miner	933	-4.72	5.28
16	Neola Schneider	995	782.01	39.80

Mobile

Contoso Confidential. Sensitive business data that

# M&A Plan –

January 2019, CONTOSO I

M&A ID: #CO0151500

An M&A proposal regarding the potential  
“Shanghai.” Prepared by the Contoso Merg  
department at Contoso, Colorado during Q  
Colorado - 319 W. 4th Street, P.O. Box 123  
555-1234

[www.contosowater.org](http://www.contosowater.org)

Sensitivity

Public

General

Confidential

Highly Confidential

Learn More...

Outlook & OWA

U.S. Sales

Private group • 7 members

Send email

This month

U.S. Sales

Sensitivity: Confiden

To

Cc

Add a subject

Personal

Public

General

✓ Confidential

Highly Confidential

Anyone (unrestricted)

✓ All Employees

Trusted People

Unified & Built-in: Native labeling across all apps and modalities

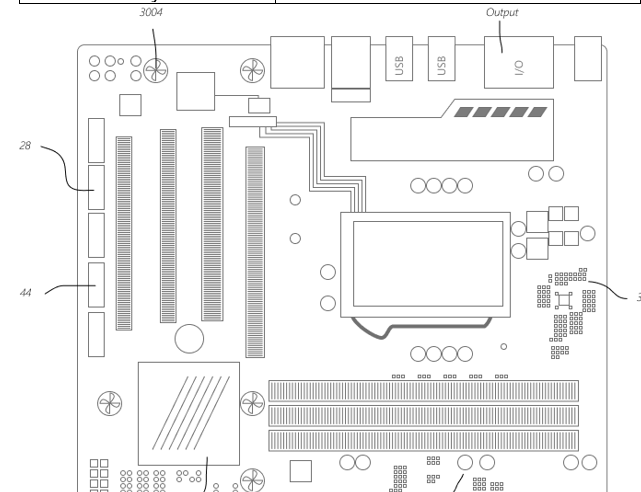
# Project Obsidian

# Updated Engine Chip Design

Automated Car Team

Feb 4, 2022

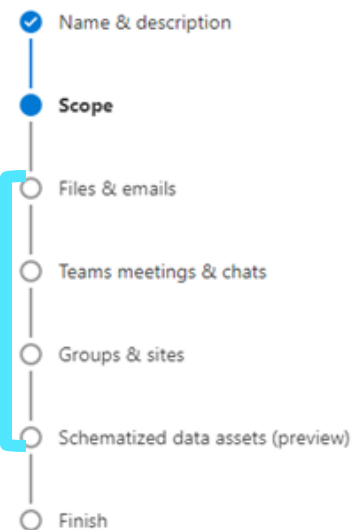
Contacts	Email	Timeline
Lidia Holloway	lidia@contosoelectronics.com	Q4 FY 22



**Built-in:** End user manual labeling in Office apps across Windows, Mac, iOS, and Android

With our new investments in automated cars we need to redesign the AI500 chip to pull more

## New sensitivity label



### Define the scope for this label

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. [Learn more about label scopes](#)

- ☒ **Files & emails**  
Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.
- ☒ **Meetings**  
Configure access and permission settings for Teams meetings and content restrictions for Teams chats.
- ☒ **Groups & sites**  
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.
- ☒ **Schematized data assets (preview)**  
Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

Unified: Labeling across Microsoft 365 & schematized data assets

## Edit sensitivity label

- ✓ Name & description
- ✓ Scope
- Files & emails
- Encryption
- Content marking
- Auto-labeling for files and emails
- Teams meetings & chats
- Groups & sites
- Schematized data assets (preview)
- Finish

## Encryption

Control who can access files and email messages that have this label applied. [Learn more about encryption settings](#)

- ☐ Remove encryption if the file or email is encrypted
- ☒ Configure encryption settings

① Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. [Learn more](#)

## Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

## User access to content expires ①

Never

## Allow offline access ①

Always

## Assign permissions to specific users and groups \* ①

[Assign permissions](#)

9 items

Users and groups	Permissions		
Abraham@ediscosdf.onmicrosoft.com	Co-Author		
Carol@ediscosdf.onmicrosoft.com	Co-Author		
DeerPark@ediscoSdf.onmicrosoft.com	Co-Author		
FINRACompliantTeam@ediscoSdf.onmicrosoft.com	Co-Author		
Russel@ediscosdf.onmicrosoft.com	Co-Author		
allemployees@ediscoSdf.onmicrosoft.com	Co-Author		
ediscoSdf.onmicrosoft.com	Co-Author		
tesdt@ediscoSdf.onmicrosoft.com	Co-Author		
tu1@ediscoSdf.onmicrosoft.com	Co-Author		

Unified: Double key encryption & User defined permissions protection

☒ Use Double Key Encryption ①

Back

Next

Cancel

# Project Obsidian

(This document contains

## Updated

Automated Car Team  
Feb 4, 2022

### Contacts

Lidia Holloway

3004

28

44

33

3004

28

44

33

3004

28

44

33

3004

28

44

33

3004

28

44

33

3004

28



44

33



Permission

☒ Restrict permission to this document

Specify users by email address or domain (Ex: 'someone@example.com' or '@example.com') separated by semicolons or click the Read or Change buttons to select from the address book.

☐ Read...   

Can read this document, but can't change, print or copy content.

☐ Change...   

Can read, change, and copy content from this document, but can't print it.

Built-in: User defined permissions when applying label

# Project Obsidian

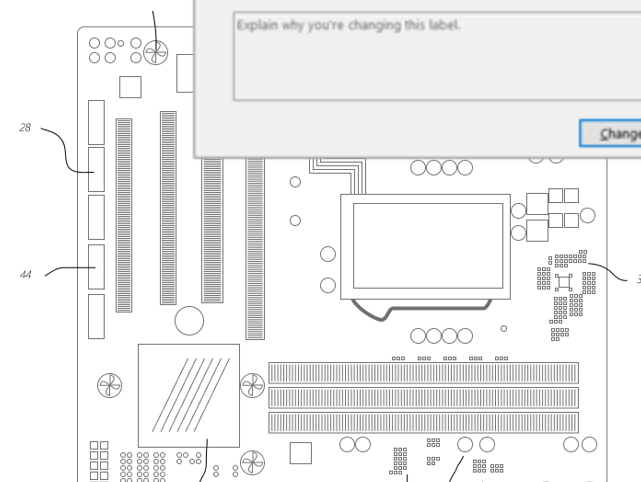
## Updated Engine Chip Design

Automated Car Test  
Feb 4, 2022

### Contacts

Lidia Holloway

3004



Justification Required

Your organization requires justification to change this label.

☒ Previous label no longer applies

☐ Previous label was incorrect

☐ Other (explain)

Explain why you're changing this label.

Change Cancel

Built-in: Option of business justification on label downgrade

With our new investments in automated cars we need to redesign the A1500 chip to pull more

- Info to label
- Name
- Locations
- Policy rules
- Label
- Policy mode
- Finish

## Choose info you want this label applied to

Choose an industry regulation to see the policy templates you can use to classify that info or create a custom policy to start from scratch.

**Check out our new enhanced policy templates.** These enhanced templates extend several of the original templates by also detecting named entities (such as full names and physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

Search for specific templates

All countries or regions

### Categories

- Financial
- Medical and health
- Privacy
- Custom
- Enhanced

### Templates

- U.S. Gramm-Leach-Bliley Act (GLBA) Enhanced
- Australia Health Records Act (HRIP Act) Enhanced
- U.S. Health Insurance Act (HIPAA) Enhanced
- Australia Privacy Act Enhanced
- General Data Protection Regulation (GDPR) Enhanced
- Japan Personally Identifiable Information (PII) Data Enhanced
- Japan Protection of Personal Information Enhanced
- U.S. Patriot Act Enhanced
- U.S. Personally Identifiable Information (PII) Data Enhanced
- U.S. State Breach Notification Laws Enhanced

### U.S. Health Insurance Act (HIPAA) Enhanced

Helps detect the presence of information subject to United States Health Insurance Portability and Accountability Act (HIPAA). This enhanced template extends the original by also detecting people's full names, medical terms and conditions, and U.S. physical addresses.

#### Protect this information:

- PII Identifiers
- ICD-9/10 code descriptions
- All Full Names
- All Medical Terms And Conditions
- U.S. Physical Addresses

### Trainable classifiers

Search

- Select all
- Source codeMicrosoft Corporation
- Offensive languageMicrosoft Corporation
- HarassmentMicrosoft Corporation
- ProfanityMicrosoft Corporation
- ThreatMicrosoft Corporation
- ☒ Project ObsidianContoso

Add

Cancel

Intelligent: OOB & Custom classifiers to label data

# General Data Protection Regulation (GDPR) Enhanced

Turn on policyRestart simulationEdit policyDelete policy

Simulation overviewItems to review

## Recommendation

### Turn on policy or review sample of matching files

We're done detecting all files that match your policy, but we're still putting together sample files to review. You can review the ones we've gathered so far or, if you're satisfied with the results, turn on the policy now. It will take around 1 day to apply the label to matching files in your org.

Turn on policy

Review matching files

## Files ready to review

### 47 matched files to review

Number of files displayed is a sample of the total matching files from each site included in the policy (up to 100 files per site).

#### Sensitive info types



## Total matching files per policy rule

### 47 matching files from 63 sites

Breakdown of how many files match your policy's rules. When the policy is turned on, it will take around 1 day to apply the label to these files.

Rule	Location	Matched items
General Data Pro...	OneDrive	24
General Data Pro...	SharePoint	23

## Details

### Policy name

General Data Protection Regulation (GDPR) Enhanced

### Status

Simulation complete

### Simulation start date/time

Yesterday at 5:21 PM

### Label and policy settings

Label Confidential/All Employees  
Exchange overwrite label false

### Info to label

Austria Physical Addresses  
Belgium Physical Addresses  
Bulgaria Physical Addresses  
Croatia Physical Addresses  
Cyprus Physical Addresses  
Czech Republic Physical Addresses  
Denmark Physical Addresses  
Estonia Physical Addresses  
Finland Physical Addresses  
France Physical Addresses  
Germany Physical Addresses  
Greece Physical Addresses  
Hungary Physical Addresses  
Ireland Physical Addresses  
Italy Physical Addresses  
Latvia Physical Addresses  
Lithuania Physical Addresses  
Luxembourg Physical Addresses  
Malta Physical Addresses  
Netherlands Physical Addresses  
Poland Physical Addresses  
Portuguese Physical Addresses  
Romania Physical Addresses

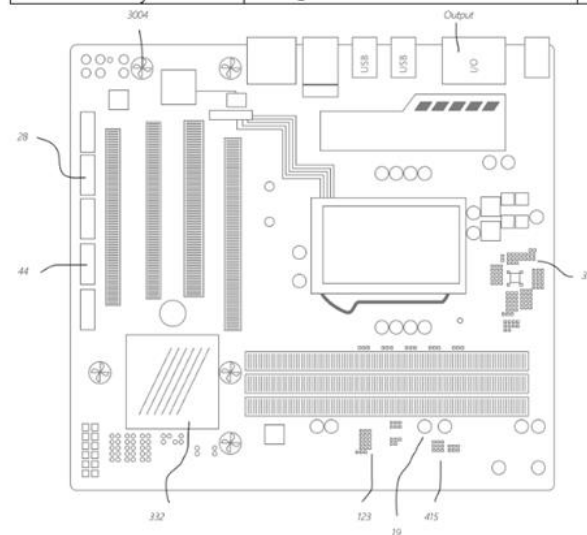
Intelligent: Simulation mode to test policy effectiveness

# Project Obsidian

## Updated Engine Chip Design

Automated Car Team  
October 21, 2019

Contacts	Email	Timeline
Lidia Holloway	lidia@contosoelectronics.com	Q4 FY 22



With our new investments in automated cars we need to redesign the AI500 chip to pull more throughput and reduce overheating.

Auto-labeling in Office Apps

credit card information:

Visa: 4538-1978-4719-4203 Exp: 08/2023

Home

Compliance Manager

Data classification

Data connectors

Alerts

Reports

Policies

Permissions

Trials

Solutions

Catalog

App governance

Audit

Content search

Communication compliance

Data loss prevention

eDiscovery

Data lifecycle management

Information protection

Information Barriers

Insider risk management

Records management

Privacy Risk Management

Privacy Subject Rights Requests

Settings

More resources

Internal Engineering Tools

Tools

Prototypes

Custom

Information protection

OverviewLabelsLabel policiesAuto-labeling

Take control of the sensitive info

Protect your org's sensitive info by quickly activating our recommended set of information protection features that help detect and classify content containing credit card numbers.  
[Learn more about these features and how they'll impact users](#)

What happens when I activate these features?

Admins

- Get alerts when credit card numbers are detected in Teams messages and files on devices

Finish setting up featuresChoose what to set up

Protect these items containing credit card numbers

Sharepoint and OneDrive files  
597

Teams messages activities  
4427

Devices' file activities  
551

Top sensitivity labels applied to content

SQL1/sqlchild4	874
InternalDisp	765
Highly Confidential1 test test	674
Confidential Label	652
General2	636

View all applied sensitivity labels

Top activities detected

2947143 activities

1483.3K File deleted

699.9K File copied to network share

689.2K DLP rule

View all activities

Locations where sensitivity labels are applied

SharePoint OnlineExchangeOneDrive

View details

Information protection resources

Stay informed about information protection

We're constantly updating our information protection features to make sure your organization can classify and protect sensitive info across the expanding Microsoft 365 landscape. Check these resources often to keep up-to-date on the latest enhancements.

Read the official docs

Get the latest news

Watch recent videos

Intelligent: Default labels & policies with simple one-click turn on

Home

Compliance Manager

Data classification

Data connectors

Alerts

Reports

Policies

Permissions

Trials

Solutions

Catalog

App governance

Audit

Content search

Communication compliance

Data loss prevention

eDiscovery

Data lifecycle management

Information protection

Information Barriers

Insider risk management

Records management

Privacy Risk Management

Privacy Subject Rights Requests

Settings

More resources

Internal Engineering Tools

Tools

Prototypes

Information protection

OverviewLabelsLabel policiesAuto-labeling

Take control of the sensitive info

Protect your org's sensitive info by quickly activating our recommended set of information protection features that help detect and classify content containing credit card numbers.  
[Learn more about these features and how they'll impact users](#)

What happens when I activate these features?

Admins

- Get alerts when credit card numbers are detected in Teams messages and files on devices

Finish setting up features

Choose what to set up

Protect these items containing credit card nu

Sharepoint and OneDrive files  
597

Teams messages activities  
4433

Devices' file activities  
551

Top sensitivity labels applied to content

SQL1/sqlchild4	874
InternalDisp	765
Highly Confidential1 test test	674
Confidential Label	652
General2	636

View all applied sensitivity labels

Top activities detected

2949932 activities

1486.1K File deleted

699.9K File copied to network share

689.2K DLP rule

View all activities

Locations where sensitivity labels are applied

Donut chart showing distribution across SharePoint Online, Exchange, and OneDrive.

View details

Information protection

Stay informed

We're constantly updating info across the experience

Read the o

Get the late

Watch rece

Set up recommended information protection features

Learn more about our recommended features and decide which ones you want to activate now. Don't worry...you can always edit them after they're created, and we'll provide a way to quickly set up any you might skip this time around.

Create data loss prevention (DLP) policies

551 unmonitored Endpoint devices

4433 Sensitive info found in Teams

Get notified when credit card numbers are shared in Teams messages or detected in device activity so you can apply restrictions if needed.

What we'll set up for you

- DLP policy that detects when credit card numbers are shared in Teams chats and channel messages.
- DLP policy that detects when files on users' devices containing credit card numbers are involved in activities like printing or copying to the clipboard.

Learn more about these settings

User impact

- Detected activity in Teams and on devices is only audited for your review. No activity is blocked.
- After reviewing activity, you can edit the policies to apply restrictions or show policy tips to users.

☒ DLP for Teams

☒ DLP for Endpoint Devices

Intelligent: Flexibility to further configure and learn more

Activate recommended features

Skip for now

# Get started with Microsoft Purview Information Protection



Learn more about Microsoft Purview Information Protection from our [webpage](#)



Get a deeper view of Microsoft Purview Information Protection from our tech docs: [aka.ms/MIPdocs](https://aka.ms/MIPdocs)



Start a free trial of Microsoft Purview: [aka.ms/PurviewTrial](https://aka.ms/PurviewTrial)