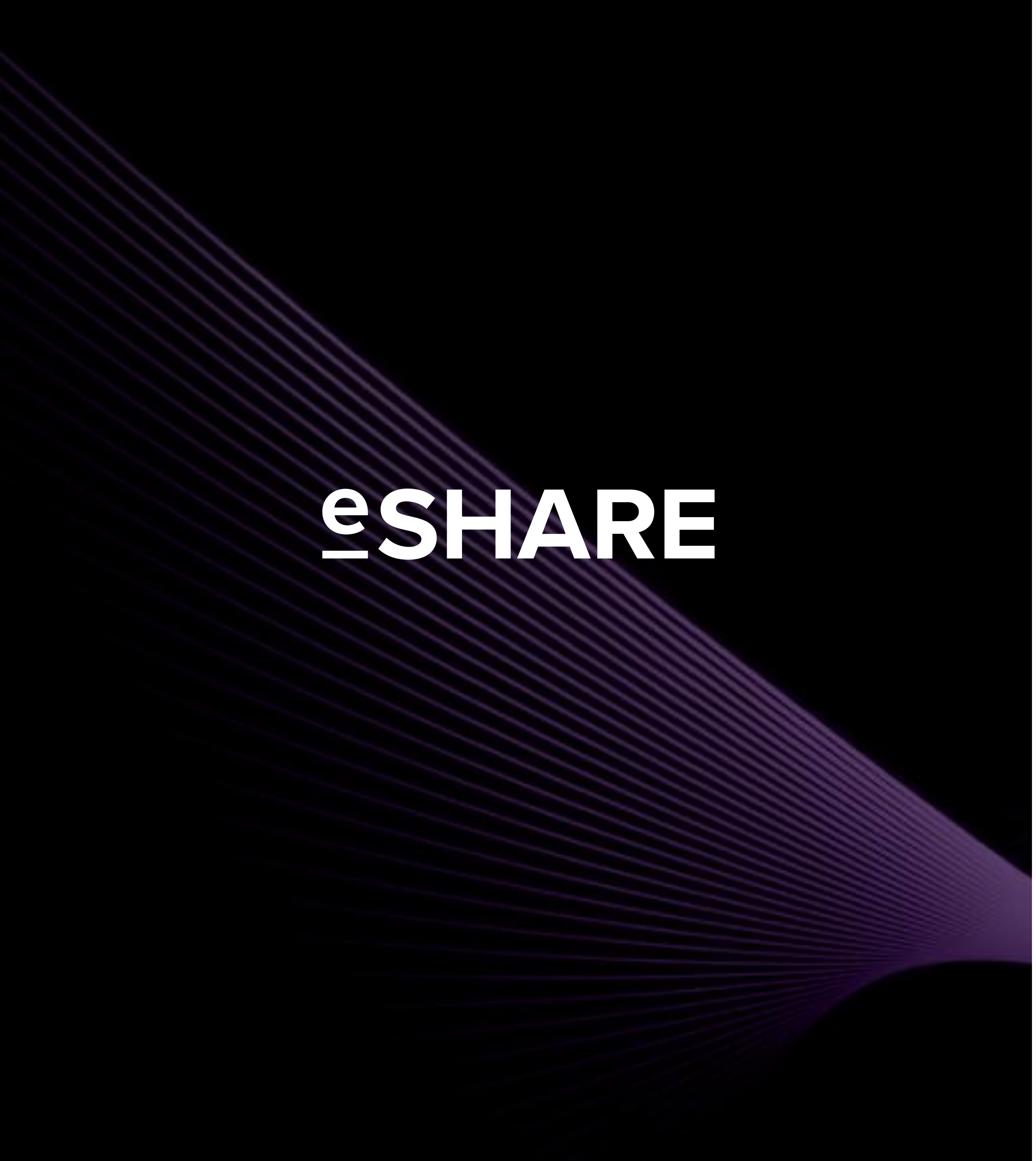


DLP in the Modern World:

Extending your DLP model to File Sharing and Modern Collaboration using SharePoint, Teams, OneDrive File Sharing

Collaboration reimagined

eSHARE

You want to be able to externally share files from SharePoint, Teams, and OneDrive…

- A natural extension of your internal file sharing
- Allows for co-authoring and collaboration
- Eliminates file duplication and version confusion
- Benefits from existing data governance capabilities (e.g., data retention)

But…

It breaks your existing DLP and incident response process!

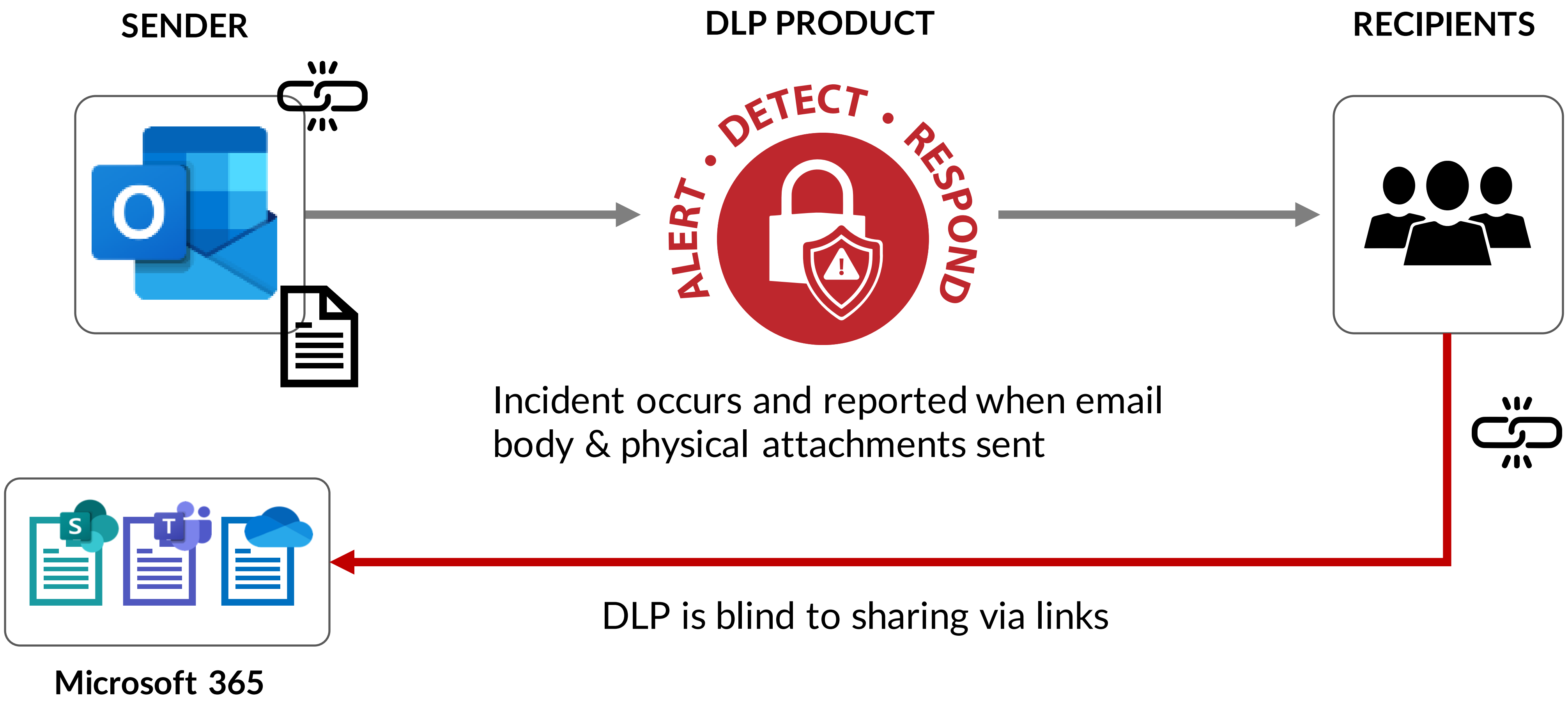
- **You can't inspect the link as it gets sent because *__the file never goes anywhere__***
- **Modern Collaboration uses links that:**
  - Could be a file – which can be changed and edited
  - Could be a folder – where files could be added and deleted
- **The content is changeable after sharing**

How can I make modern collaboration fit my existing DLP model…

when I don’t have sensitivity labels or auto-classification enabled across Teams, SharePoint Online and OneDrive?

eSHARE

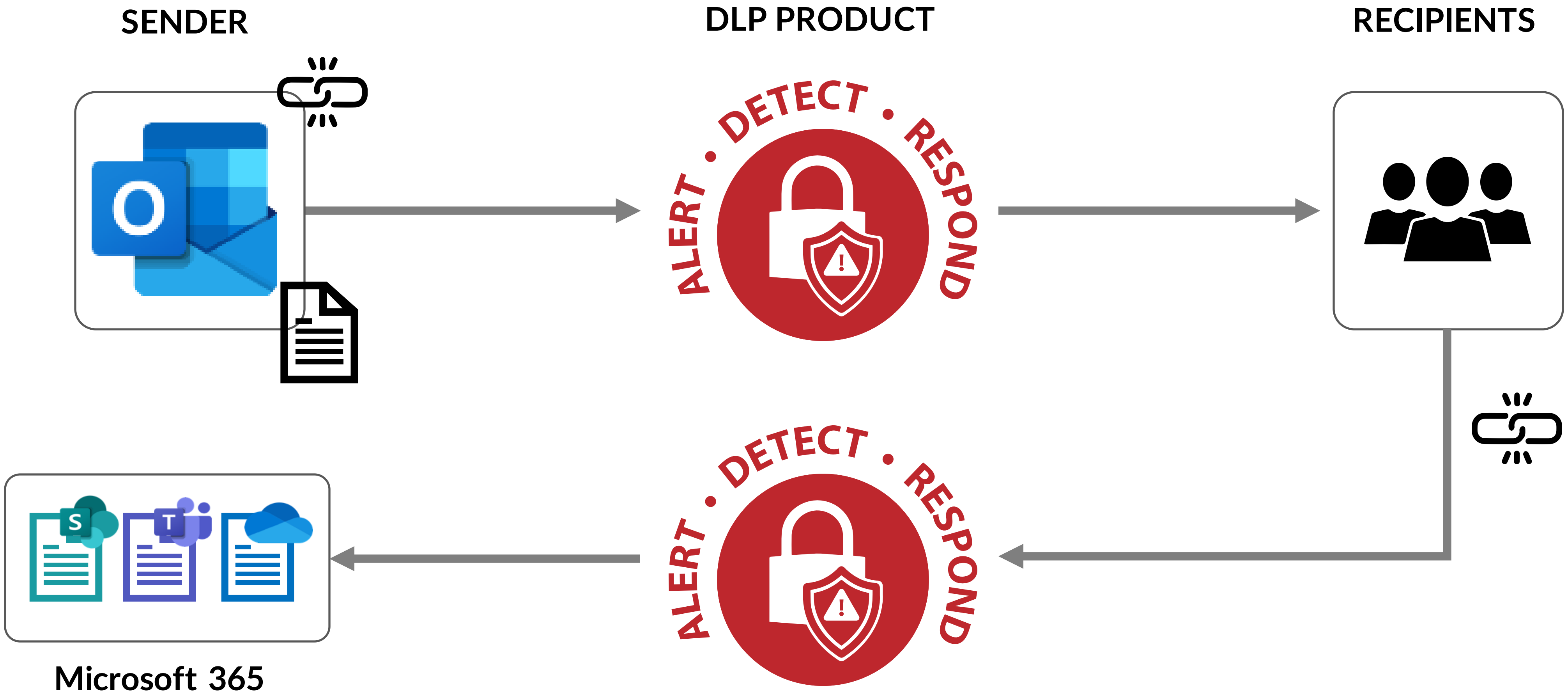
What does DLP look like today (e.g., email)?



Incident occurs and reported when email body & physical attachments sent

DLP is blind to sharing via links

How is DLP performed with eShare (e.g., email)?



DLP-driven sharing policies evaluated at time of sharing and time of access

Extend Your Current DLP Model In 4 Easy Steps

STEP ONE 1

Enable Microsoft DLP policies for SharePoint Online, Teams, and OneDrive
(possibly mirroring policies from other DLP systems)

STEP TWO 2

Define ”DLP Tags” based on DLP rules and associate to sharing policies
(co-exist with and act like sensitivity labels)

STEP THREE 3

Import your DLP rule alerts and join with eShare activity logs to create Tag <> File database

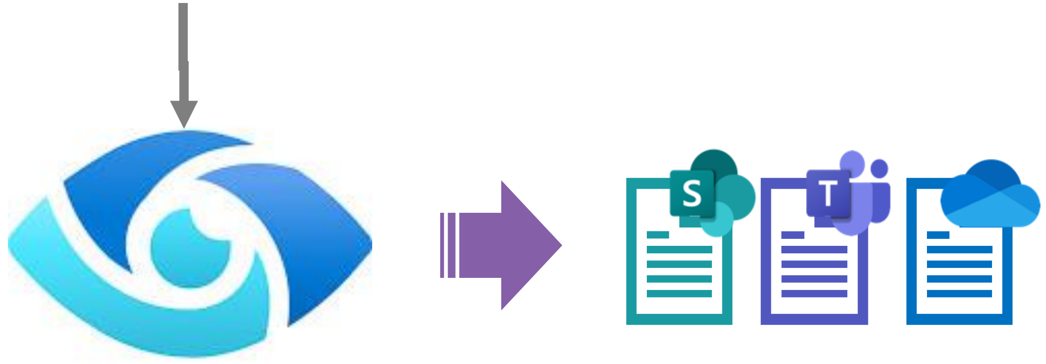
STEP FOUR 4

Incorporate eShare’s on-access, DLP-enriched audit events into your incident response flow

STEP ONE 1

Enable Purview DLP policies for SharePoint Online, Teams, and OneDrive

Optionally map* existing DLP policies to Purview policies



Microsoft Purview DLP Policies

DLP rules evaluated with each user file action, including file creation, creating alerts

- Policy rules defined using Sensitive Info Types (SITs): PHI, PCI, PII etc.
- Available with E3 licenses

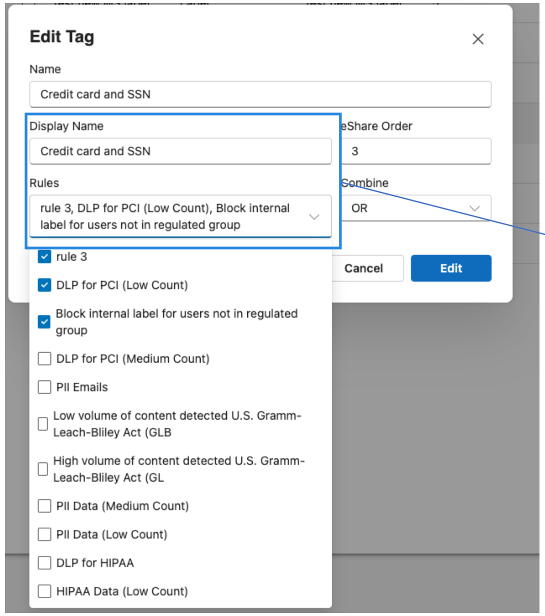
*** eShare Advisory Services can do this for you**

eSHARE

STEP ONE 2

Define “DLP Tags” based on DLP rules and associate to sharing policies

Microsoft Purview DLP Policies & Their Rules Imported Into eShare



Edit Tag

Name: Credit card and SSN

Display Name: Credit card and SSN

eShare Order: 3

Rules: rule 3, DLP for PCI (Low Count), Block internal label for users not in regulated group

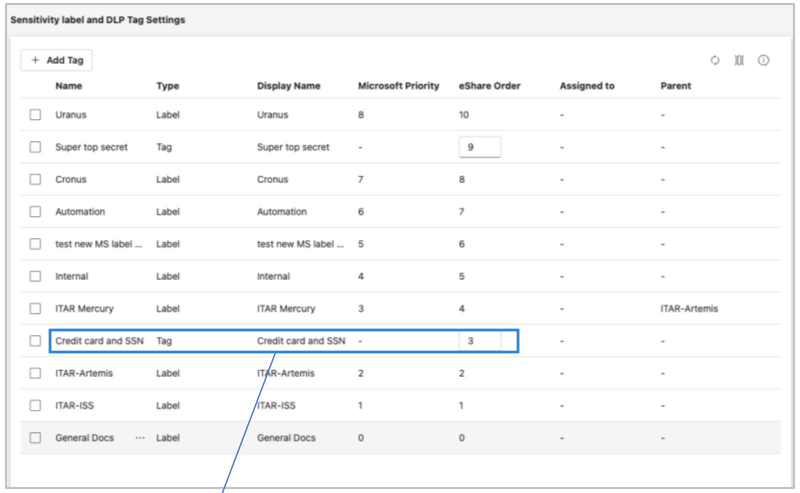
Combine: OR

Cancel | Edit

- ☑ rule 3
- ☑ DLP for PCI (Low Count)
- ☑ Block internal label for users not in regulated group
- ☐ DLP for PCI (Medium Count)
- ☐ PII Emails
- ☐ Low volume of content detected U.S. Gramm-Leach-Bliley Act (GLB
- ☐ High volume of content detected U.S. Gramm-Leach-Bliley Act (GL
- ☐ PII Data (Medium Count)
- ☐ PII Data (Low Count)
- ☐ DLP for HIPAA
- ☐ HIPAA Data (Low Count)

Tags = AND/OR combination of DLP Rules

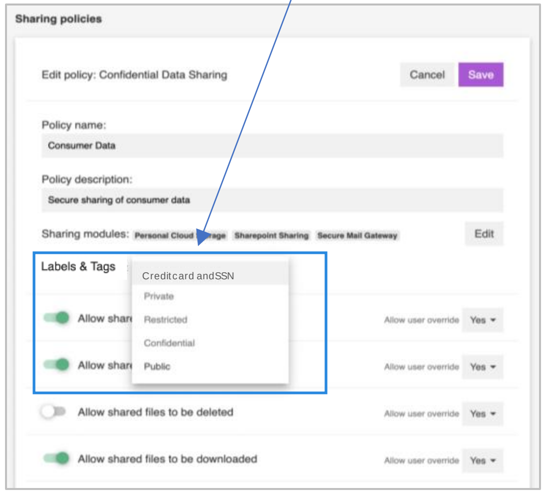
Tags are ordered relative to labels (if any)



Sensitivity label and DLP Tag Settings

+ Add Tag

	Name	Type	Display Name	Microsoft Priority	eShare Order	Assigned to	Parent
☐	Uranus	Label	Uranus	8	10	-	-
☐	Super top secret	Tag	Super top secret	-	9	-	-
☐	Cronus	Label	Cronus	7	8	-	-
☐	Automation	Label	Automation	6	7	-	-
☐	test new MS label ...	Label	test new MS label ...	5	6	-	-
☐	Internal	Label	Internal	4	5	-	-
☐	ITAR Mercury	Label	ITAR Mercury	3	4	-	ITAR-Artemis
☐	Credit card and SSN	Tag	Credit card and SSN	-	3	-	-
☐	ITAR-Artemis	Label	ITAR-Artemis	2	2	-	-
☐	ITAR-ISS	Label	ITAR-ISS	1	1	-	-
☐	General Docs ···	Label	General Docs	0	0	-	-



Sharing policies

Edit policy: Confidential Data Sharing

Cancel | Save

Policy name: Consumer Data

Policy description: Secure sharing of consumer data

Sharing modules: Personal Cloud Storage, Sharepoint Sharing, Secure Mail Gateway — Edit

Labels & Tags: Creditcard andSSN, Private, Restricted, Confidential, Public

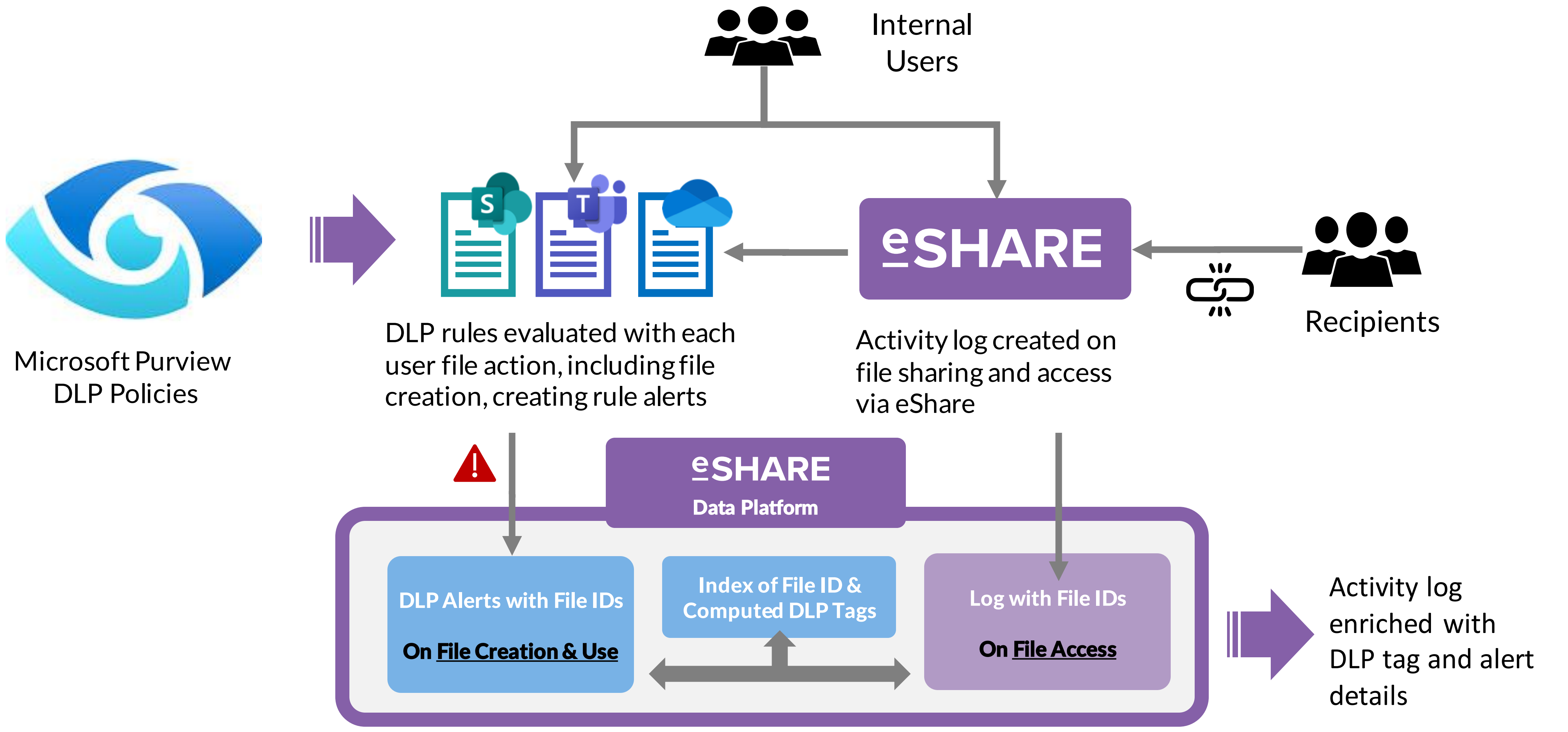
- Allow share… — Allow user override: Yes
- Allow share… — Allow user override: Yes
- Allow shared files to be deleted — Allow user override: Yes
- Allow shared files to be downloaded — Allow user override: Yes

Tags assigned to sharing policies

eSHARE

STEP THREE 3

Import your DLP rule alerts and join with eShare activity logs to create Tag <-> File database

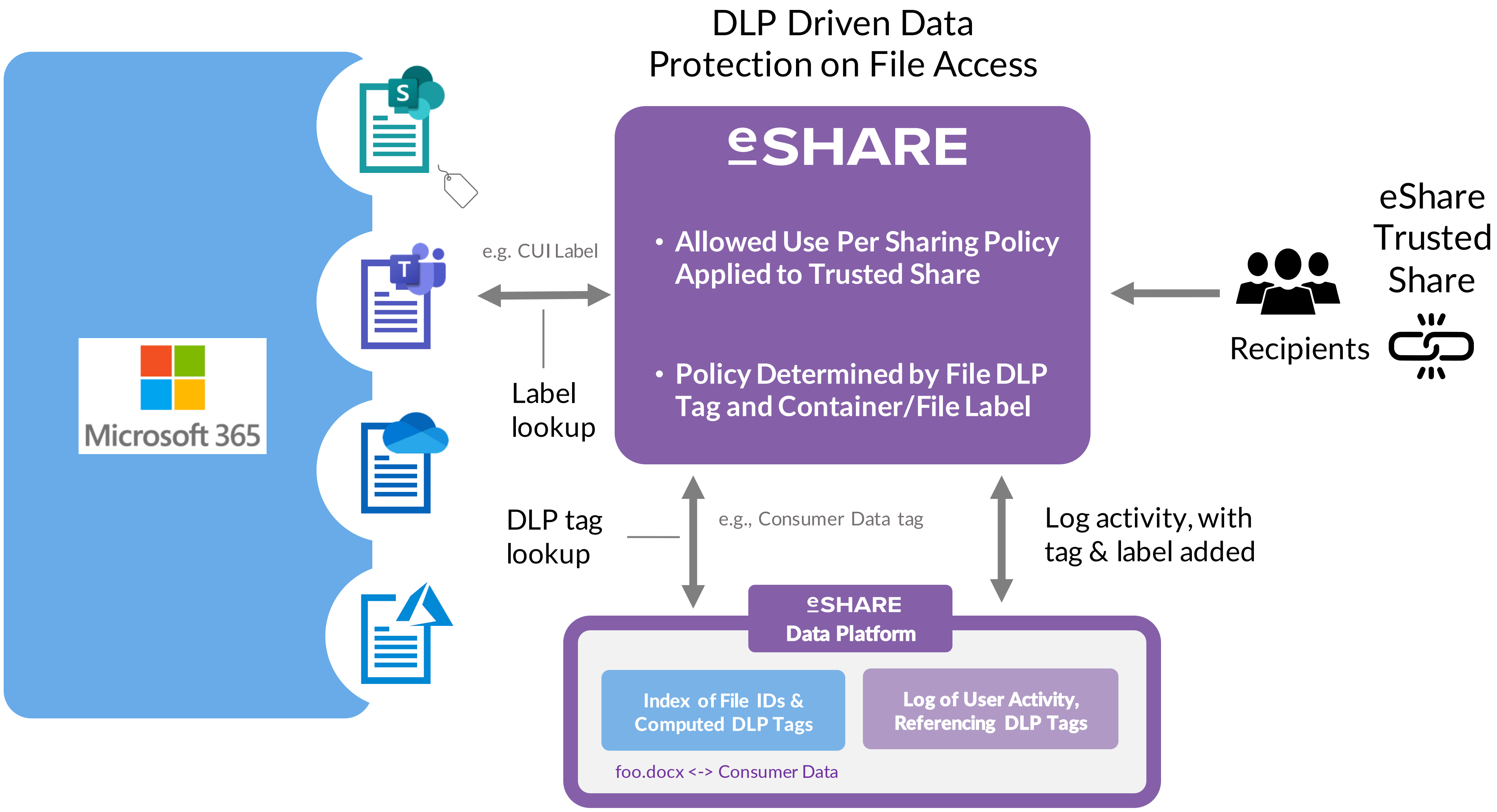


Internal Users
Microsoft Purview DLP Policies
DLP rules evaluated with each user file action, including file creation, creating rule alerts
eSHARE
Activity log created on file sharing and access via eShare
Recipients
eSHARE
Data Platform
DLP Alerts with File IDs
On File Creation & Use
Index of File ID & Computed DLP Tags
Log with File IDs
On File Access
Activity log enriched with DLP tag and alert details

Defined DLP Tags computed and applied to files based on ingested alerts

eSHARE

DLP Tags in Operation



DLP Driven Data Protection on File Access

eSHARE

- Allowed Use Per Sharing Policy Applied to Trusted Share
- Policy Determined by File DLP Tag and Container/File Label

Microsoft 365

e.g. CUI Label

Label lookup

eShare Trusted Share

Recipients

DLP tag lookup

e.g., Consumer Data tag

Log activity, with tag & label added

eSHARE Data Platform

Index of File IDs & Computed DLP Tags

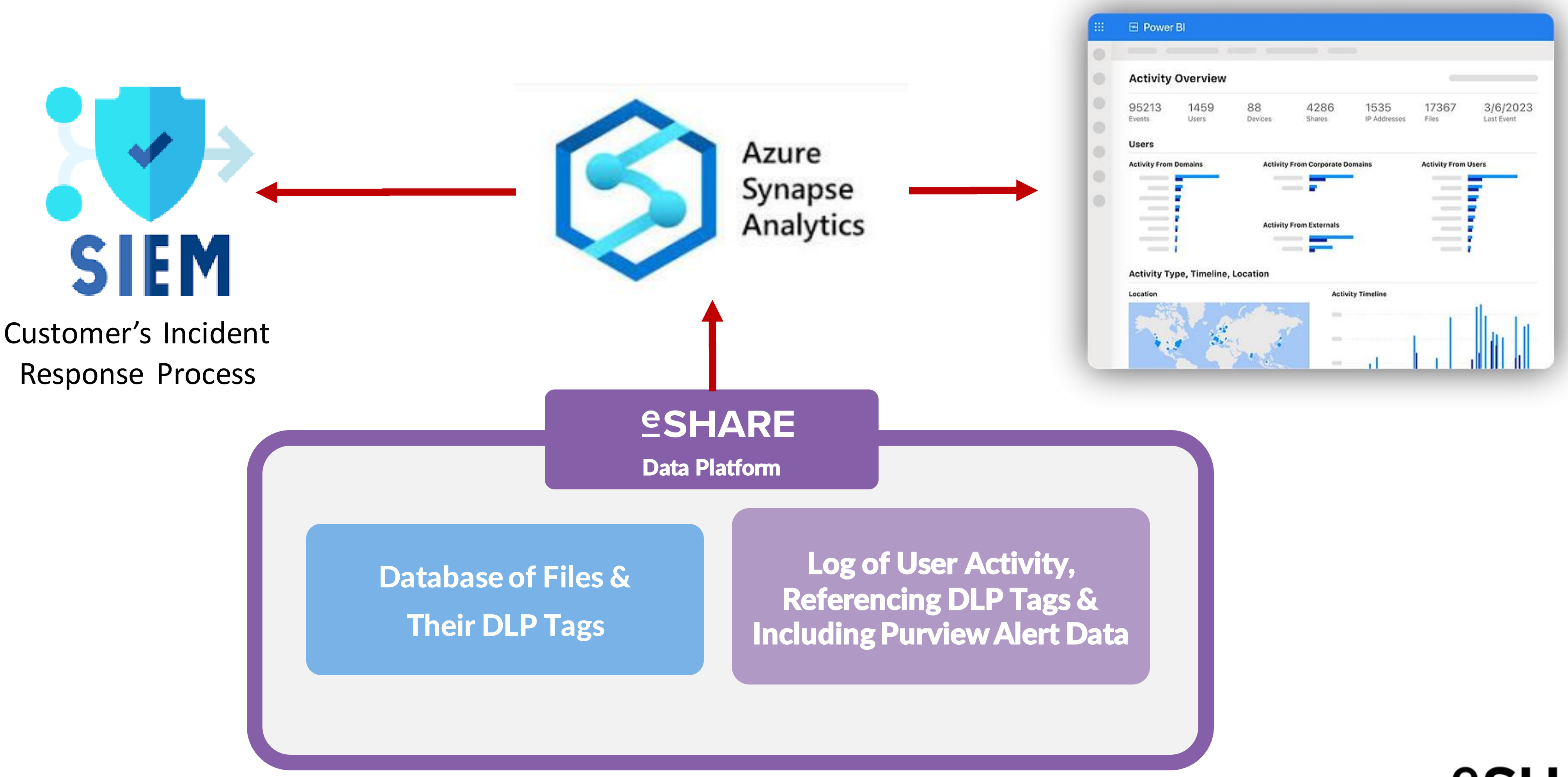
Log of User Activity, Referencing DLP Tags

foo.docx <-> Consumer Data

STEP FOUR 4

Incorporate eShare's DLP-enriched audit events into your incident response flow, complemented by out-of-the-box analytics

eShare Analytics in Power BI



Power BI

Activity Overview

95213	1459	88	4286	1535	17367	3/6/2023
Events	Users	Devices	Shares	IP Addresses	Files	Last Event

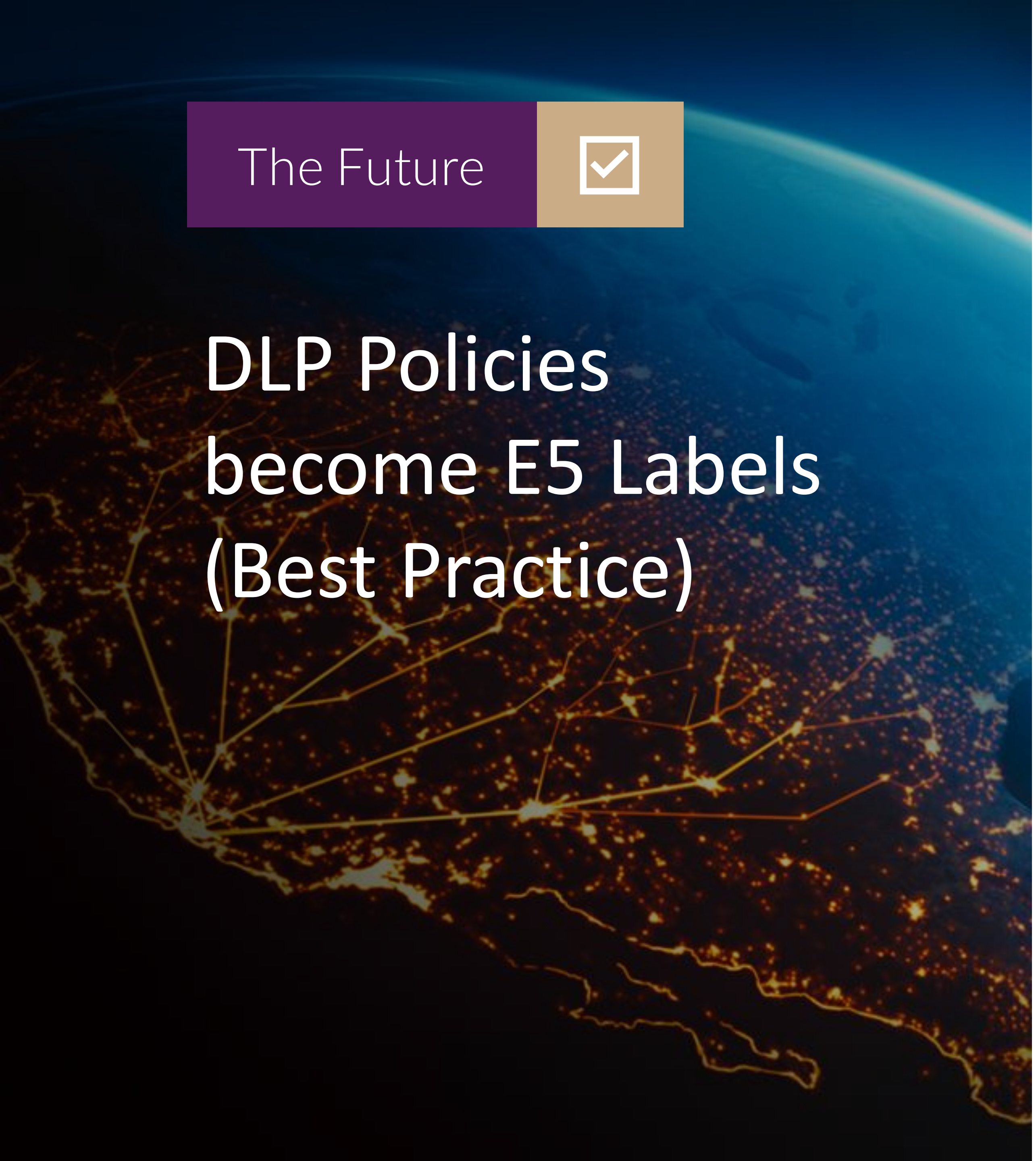
Customer's Incident Response Process

Database of Files & Their DLP Tags

Log of User Activity, Referencing DLP Tags & Including Purview Alert Data

eShare provides unmatched DLP-driven visibility & control over external file sharing using M365

- **Reporting of all sensitive data that was accessed by Trusted Share participants**
  - User
  - Device
  - Location
  - IP
  - File Accessed
  - Label and/or Tag
  - Actions
    - View
    - Edit
    - Download
    - Upload
    - eSignature
- **Fine-grained, DLP-tag & label driven control**
  - Any combination of view, download, edit
  - Allow sharing with internal user justification
  - Allow access with external & internal user justification
  - Allow with stepped up authentication
  - Allow with custom Terms of Use
  - Allow with configurable marking and watermarking on view & download



The Future ☑

DLP Policies become E5 Labels (Best Practice)

As your Microsoft Deployment Evolves and Matures:

- Migrate to E5 Licensing
- Enable Data Labeling and Auto Classification
- Use your Purview DLP Policies as the templates for Data Labeling Policies

eSHARE

eSHARE

Greater Productivity
Better User Experience
Better Security and Compliance