

# Purview strategies for when your data has no boundaries



Åsne Holtklampen

**Copilot  
Community  
Conference**

Admin-Track



**Åsne Holtklampen**

Senior Architect - SoftwareOne

Microsoft Copilot MVP & MCT

<https://AgderInThe.Cloud>

20 + years within Microsoft

Focused on Microsoft Purview & data governance



# Today's Agenda

01

## The Problem

Why data without boundaries is everyone's problem — and nobody's fault

02

## Spot the Pattern

Finding oversharing signals before they become incidents

03

## Advanced Discovery

Using Purview to expose sensitive-data hotspots across your estate

04

## Automate Classification

Making your data stop behaving like an unsupervised intern

05

## Access Boundaries + Detox Plan

Guardrails, governance, and what you do on Monday morning

01

TAKEAWAY 1

# The Problem

*Why data without boundaries is everyone's problem - and nobody's fault*

**Some organisations have a sharing culture.**

**Others have a sharing problem.**

---

### Accidental access

People can read files they were never meant to see — and nobody knows.

### Forgotten permissions

That guest from 2021 still has edit rights. The project ended. They didn't.

### Sensitive files, wrong places

Salary data in a team channel. Medical records in a shared OneDrive. Classic.



# How did we get here?

2020

Teams deployed overnight



"Just create teams and share." Nobody said 'govern.'

2021+

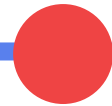
SharePoint sprawl



Sites, channels, libraries. Everyone, external, links never expire.

Now

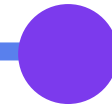
Permissions forgotten



Your data archaeologists are the only ones who know what's where.

Today

Copilot arrives



AI hovers up everything your users technically have access to. Gulp.



# The real cost of ungoverned data



This isn't about scare tactics.

Admin Track

# The real cost of ungoverned data



This isn't about  
scare tactics.

Admin Track

# 02

TAKEAWAY 2

## Spot the pattern

*before they become security incidents*



# Oversharing is a pattern, not an accident

## What to look for:

These are your early warning signals. If you see one, you have a pattern. If you see all four, you have a problem that is already compounding.



"Everyone" or "Everyone except external"



External sharing links with no expiry



Orphaned sites and teams



Guest accounts without review



Where to look first

03

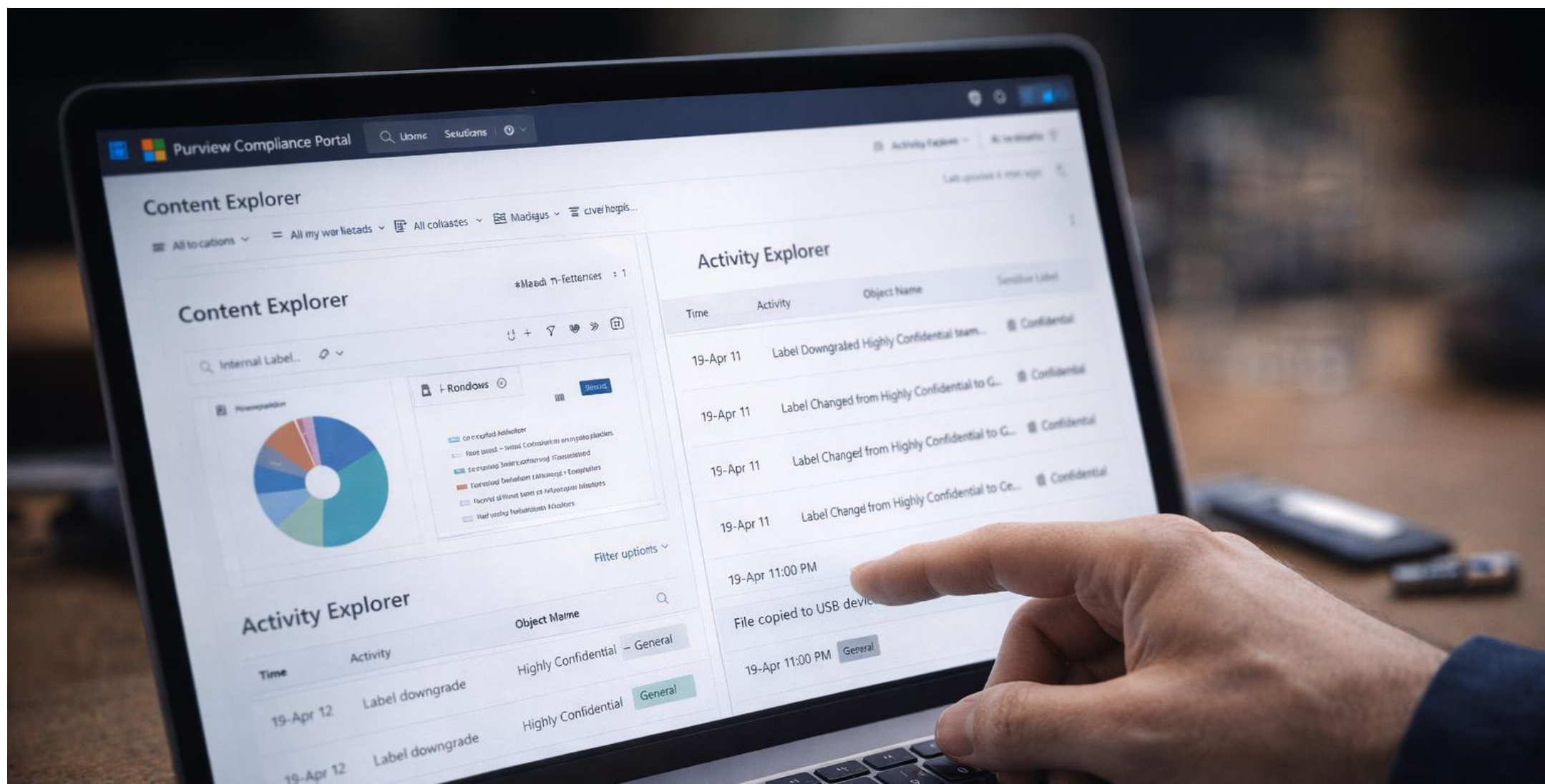
TAKEAWAY 3

# Advanced Discovery

*expose sensitive-data hotspots*



# Find the hotspots before they find you



# Beyond Microsoft 365: The Purview Data Map



SharePoint & OneDrive



Azure SQL & Databases



Azure Storage



Purview  
Data Map



3rd Party Sources



Exchange & Teams



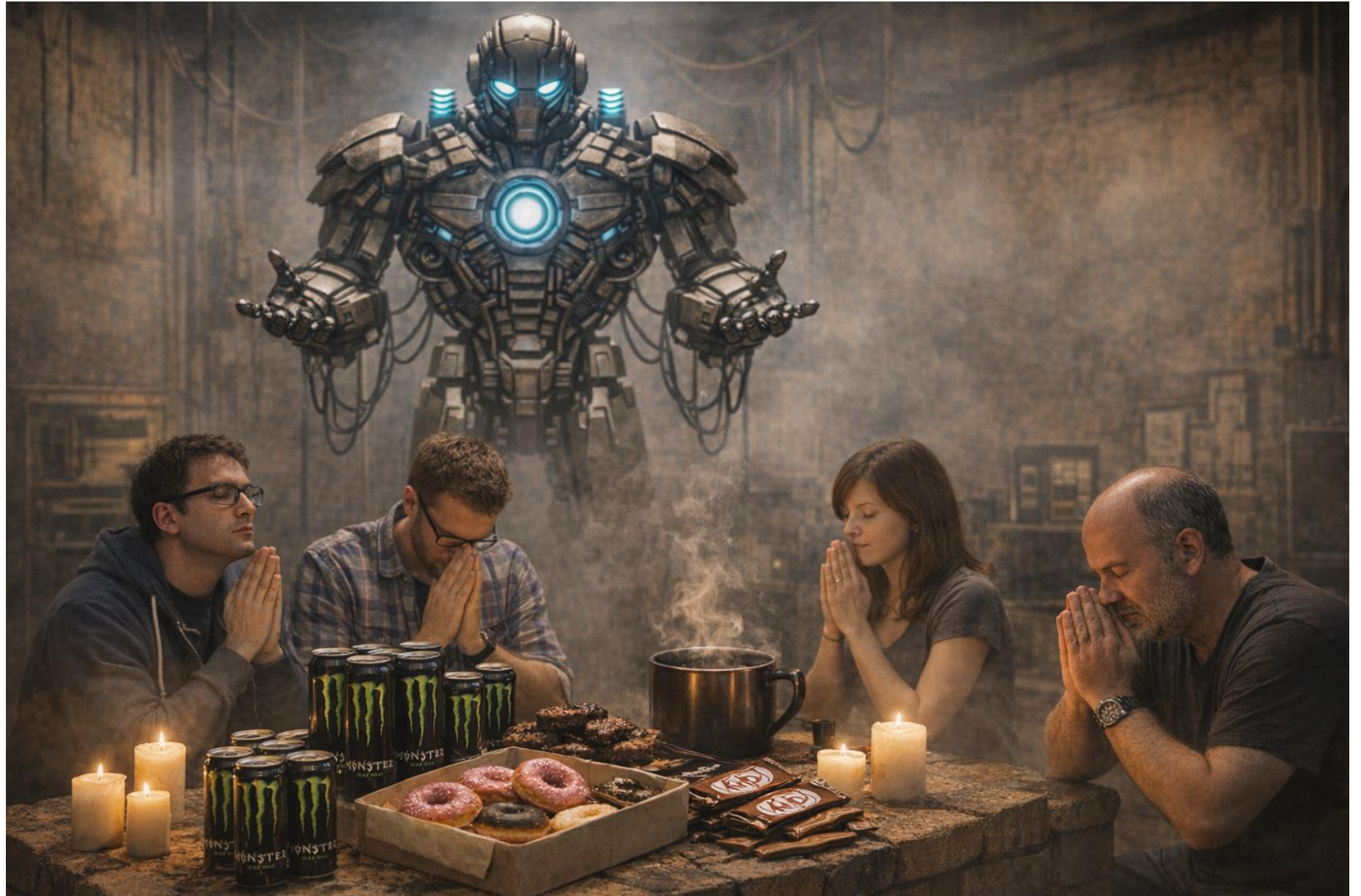
3rd Party Sources

D

E

M

O



# 04

TAKEAWAY 4

## Automate Classification

*stop the unsupervised intern behaviour*



# "Your users are not data-classification engineers."

*They're busy. They're distracted. They're inconsistent. And that's normal.*

## What they're told

*"Please make sure to label every document appropriately based on its sensitivity level."*

## What they hear

*Something about labels. And clicking. Whatever, I have a deadline.*

## What you need

*Automation that doesn't require user intent to work correctly.*



# Sensitive Information Types

- the backbone of everything

SITs are the detection patterns Purview uses to find sensitive data, and to trigger auto-labelling and DLP.

**The quality of your SITs determines the quality of everything downstream.**

*Weak SITs = false positives = automation failure = users stop trusting the system = zero real protection.*

## Good SIT design

- Precise patterns
- Business-specific
- Tested in simulation
- Combined with confidence levels
- Low false-positive rate validated in your content

## Bad SIT design

- Any 6-digit number = employee ID
- False positives on every invoice, date, postcode
- Automation drowns in noise
- Users ignore DLP alerts — every single one
- "Protection" gone: system never trusted again



# The label taxonomy that works

## Highly Confidential

Encryption + strict ACLs. Board data, M&A, HR individual records.

## Confidential

Restricted access. Financial, legal, customer PII.

## General / Internal

Standard business content. Internal use only.

## Public

Safe to share externally. Marketing, public docs.

## Never set a default label

Users stop thinking. Documents get mislabelled at scale.

## Remove 'Let users decide access'

They won't. Or they'll decide wrong.

## Simulation mode before enforcement

Review what gets labelled before you enforce. Trust the data.



D

E

M

O



05

TAKEAWAY 5

# Healthy Access Boundaries

*without fighting endless permission wars*



# Guardrails that work even when humans don't

## Mandatory labelling

- Turn on across all Office apps
- No unlabelled documents allowed
- Users choose - no auto-default
- Consistent: SharePoint, OneDrive, Teams, endpoints

## DLP that enables, not blocks

- Start with notification policies, not hard blocks
- Justify-and-proceed for borderline cases
- Hard blocks only for clear high-risk scenarios
- Block external sharing of Highly Confidential

## Conditional Access + Labels

- Require managed device for Highly Confidential
- Block download on Confidential for unmanaged
- Revoke access when label changes
- Tie label to encryption for external sharing



# AI is now reading your data estate.

## Is it ready for that?

Copilot respects sensitivity labels



Copilot respects access permissions, not appropriateness



Personal Content Mode is the safety net, not the solution



Real fix: label and classify before you deploy AI



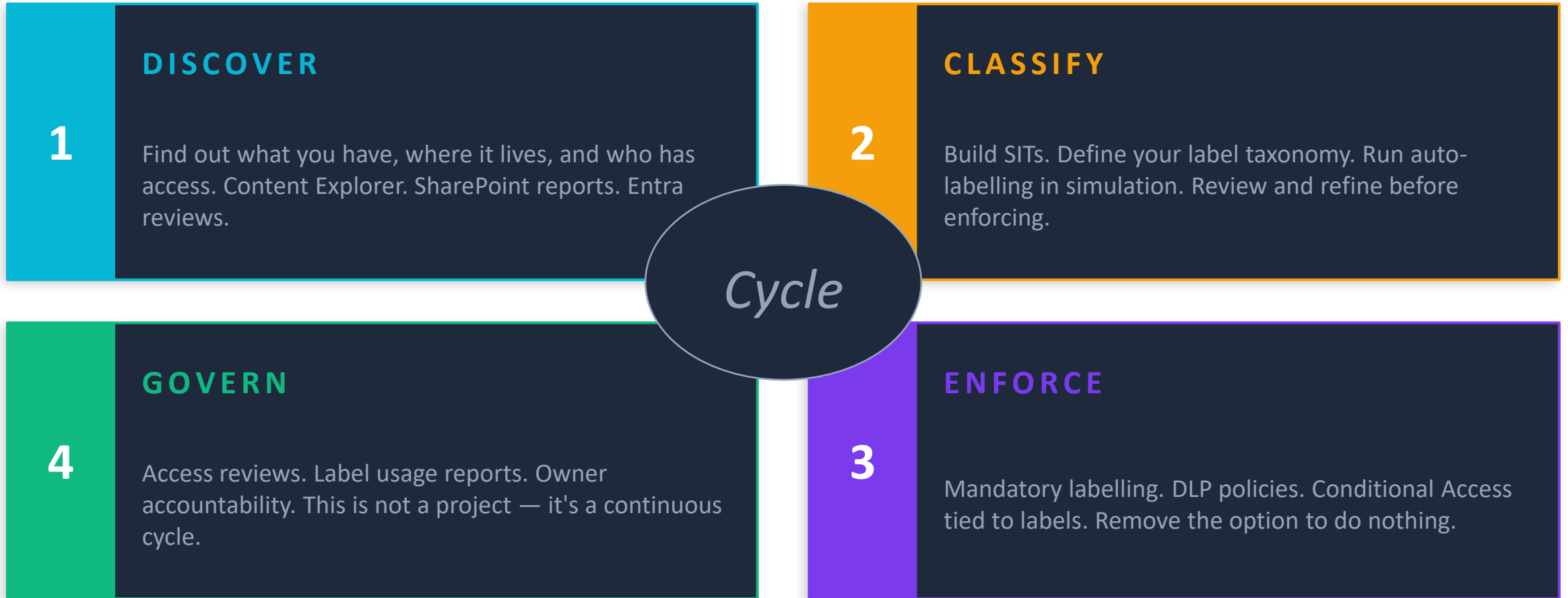
05

TAKEAWAY 5

# The Data Detox Plan

*clean, controlled and calm — long after today*





# Where to start on Monday morning

**1** Open Content Explorer

**2** Run the SharePoint sharing report

**3** Review your label taxonomy

**4** Set up one SIT, run in simulation

**5** Schedule a guest access review in Entra



# Key Takeaways

1

Oversharing is a pattern. Spot the signals — Everyone links, expired guests, orphaned sites — before they become incidents.

2

Content Explorer and Activity Explorer are already in your tenant. Open them. The data is there. The visibility wasn't.

3

Automate classification — but build precise SITs first. Noisy automation fails faster than no automation.

4

Guardrails that work don't block collaboration. They remove the option to do nothing.

5

The detox plan is a cycle: Discover, Classify, Enforce, Govern. Not a project. A practice.



# Questions?



Feedback

**Åsne Holtklampen**

<https://agderinthe.cloud>

[linkedin.com/in/aasneholtklampen](https://www.linkedin.com/in/aasneholtklampen)



Admin Track