proarch

What to Configure in Microsoft Purview Before Deploying Microsoft 365 Copilot

ProArch Webinar • Wednesday, May 13, 2026 • 2 PM ET

MEET OUR PRESENTERS

Mike McClain

Senior Security Consultant

Jim Spignardo

Director, Cloud Strategy & AI Enablement

Todd Brink

Senior Security Architect

What you'll learn by the end of this webinar...

1. **The Copilot Pilot Reality**
   What happens when Copilot rollout is rushed
2. **Why Purview First**
   Governance as the enablement layer
3. **Purview Implementation Approach**
   Discover, Classify, Protect, Govern
4. **Purview Capabilities Deep Dive**
   Oversharing · DSPM for AI · DLP for Copilot
5. **Getting Started**
   30-60-90-day roadmap for your team

proarch

The Copilot Pilot Reality:

What Happens When Rollout is Rushed

Microsoft 365 Copilot is Already Delivering Measurable Results

70%

of Fortune 500 use Microsoft 365 Copilot

3 hrs.

saved per week, per person on average in enterprise deployments

92 mins

saved per week per person at Amgen — nearly two weeks per person annually

67%

faster content creation reported by marketing teams using Copilot

Source: Microsoft FY25 Q1 Earnings, Oct 2024

What Happens When Copilot Rollout is Rushed

SENSITIVE CONTENT SURFACES ON DAY 1

Copilot surfaces salary info, M&A documents, and HR data to users who technically already had access. No one realized until now.

PILOTS STALL AT 20 – 30 USERS

Leadership pauses expansion after the first oversharing incident. Momentum and executive sponsorship are lost.

TRUST AND ADOPTION ERODE

Users stop trusting answers.
Security teams lock things down reactively.
Adoption stalls and everyone loses.

Copilot Does NOT Change

Existing user and group permissions in SharePoint, OneDrive, and Teams

Which files a user can technically open today

Your sensitivity labels, retention policies, or DLP rules

The Microsoft 365 service boundary and your tenancy

Copilot DOES Change

How fast users find content they already have access to

How far content travels once surfaced: summaries, chat, new documents

The visibility of pre-existing governance debt — it all shows up

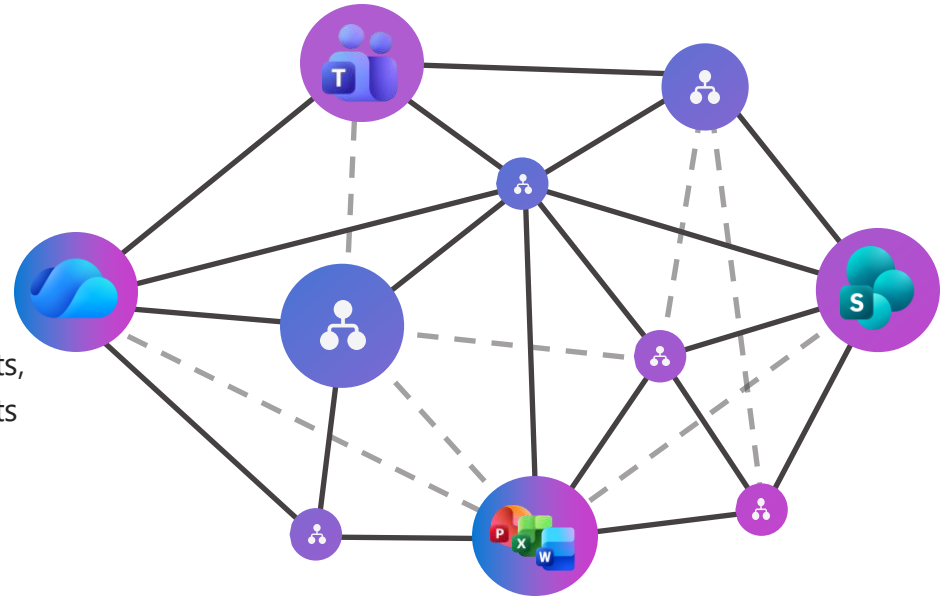
The cost of doing nothing about oversharing

Microsoft 365 Copilot is built on trust

Where Oversharing Typically Lives

Teams Channels

Private chats and channels with standing members who've long since left the project.



OneDrive Files

Anyone-with-the-link sharing, external guests, and orphaned accounts from leavers.

SharePoint Sites

Org-wide 'Everyone' sites, open team sites, and legacy project sites nobody owns.

Stale Content

Inactive sites with sensitive data — invisible to users but fully visible to Copilot.

proarch

Why Purview First:
Governance as the Enablement Layer

What is Microsoft Purview?

Unified security solution that helps your organization better mitigate data risks across your digital estate

- Comprehensive visibility and AI-driven aggregated insights that help uncover hidden risks
- Protection against unauthorized use of data across cloud, devices, and generative AI applications
- Fast investigations and responses to data security incidents

The Governance Order Matters

Permissions cleanup after a pilot is extremely difficult and time-consuming

AI “Pandoras Box” situation

Every sensitive file Copilot surfaces becomes an incident ticket

Baseline Purview controls let you pilot quickly and safely

80%
of leaders cite leakage of sensitive data as their main Gen AI concern

Purview Decisions Directly Shape

Trust in Copilot responses
Users stop second-guessing answers

Confidence in Data Security to expand rollout
IT and Compliance teams see risk, not surprises

Executive willingness to scale
Leadership approves broader investment

Safe & Secure Copilot Use: 6 Key Purview Capabilities

1 Address Oversharing

Identify and remediate overshared sites and files before Copilot surfaces them.

2 Protect Against Data Loss

Sensitivity labels, DLP for Copilot, and file-level protection that travels with the file.

3 Manage Insider Risk

Detect risky AI use, sequence risk alerts, and auto-tighten policies for high-risk users.

4 Audit & Retain Interactions

Keep or delete Copilot prompts and responses to match your retention strategy.

5 Legal Hold & eDiscovery

Include Copilot content in litigation, investigations, and admin searches.

6 Regulatory Compliance

Map EU AI Act, NIST AI RMF, ISO 42001 and 23894 controls with Compliance Manager.

proarch

How ProArch Implemented Purview: Discover, Classify, Protect, Govern

How ProArch Implemented Purview: 4 Phases

1

Discover

Find where sensitive data and overshared content live.

Oversharing reports across the tenant

Risk-ranked backlog: HIGH / MEDIUM / LOW

Data Security Investigations

2

Classify & Label

Apply sensitivity labels that travel with files.

Simple 3-4 tier taxonomy users will apply

Auto-labeling for top sensitive info types

Label inheritance and file-level encryption

3

Protect

Stop what you can now see.

DLP for Copilot: block labeled content

Insider Risk Management: detect risky patterns

Endpoint DLP beyond the M365 boundary

4

Govern

Meet regulatory and lifecycle requirements.

Audit, retain, and legal-hold AI interactions

Map to EU AI Act / NIST / ISO 42001

DSPM for AI: single-pane risk posture

Phase 1: Discover

Find where the risk lives

- Run SharePoint oversharing reports across our tenant
- Identify sites with sensitive data, broad permissions, and high access
- **Triage into a risk-ranked backlog:** not a boil-the-ocean project
- **Run Data Security Investigations:** create labels, weed out false positives, and beyond through a hand-held approach

Phase 2: Classify & Label

Make sensitivity visible

- **Sensitivity labels:** simple 3-4 tier taxonomy that's more palatable for users to adopt
- **Auto-labeling:** detect credit cards, M&A terms, HR data, etc.
- **Label inheritance:** Copilot responses inherit the highest-priority label
- **File-level protection:** encryption and usage rights travel with the file

Risk Triage

HIGH: sensitive data + broad access + high volume

MEDIUM: sensitive data OR broad access

LOW: limited exposure, monitor and apply controls

Phase 3: Protect

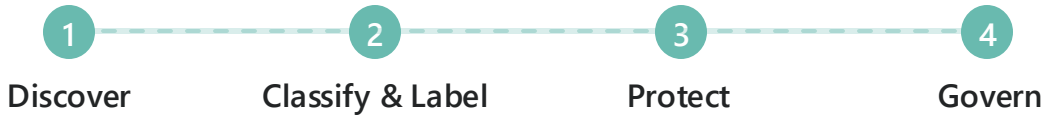
Stop what you can now see

- **DLP for Copilot:** block processing of labeled files; disallow AI interactions with PII and legal content
- **Insider Risk Management:** detect risky prompts, sequence alerts over time, dynamically tighten policies
- **Endpoint protection:** block paste and upload of sensitive content to AI tools, extends beyond M365

Phase 4: Govern

Meet regulatory & lifecycle needs

- **Audit:** every Copilot prompt, response, and referenced file captured
- **Data Lifecycle:** retain or delete Copilot interactions per policy
- **Legal hold & eDiscovery:** include Copilot content in litigation holds
- **Compliance Manager:** map to EU AI Act, NIST AI RMF, ISO 42001
- **DSPM for AI:** single-pane dashboard for AI risk posture



proarch

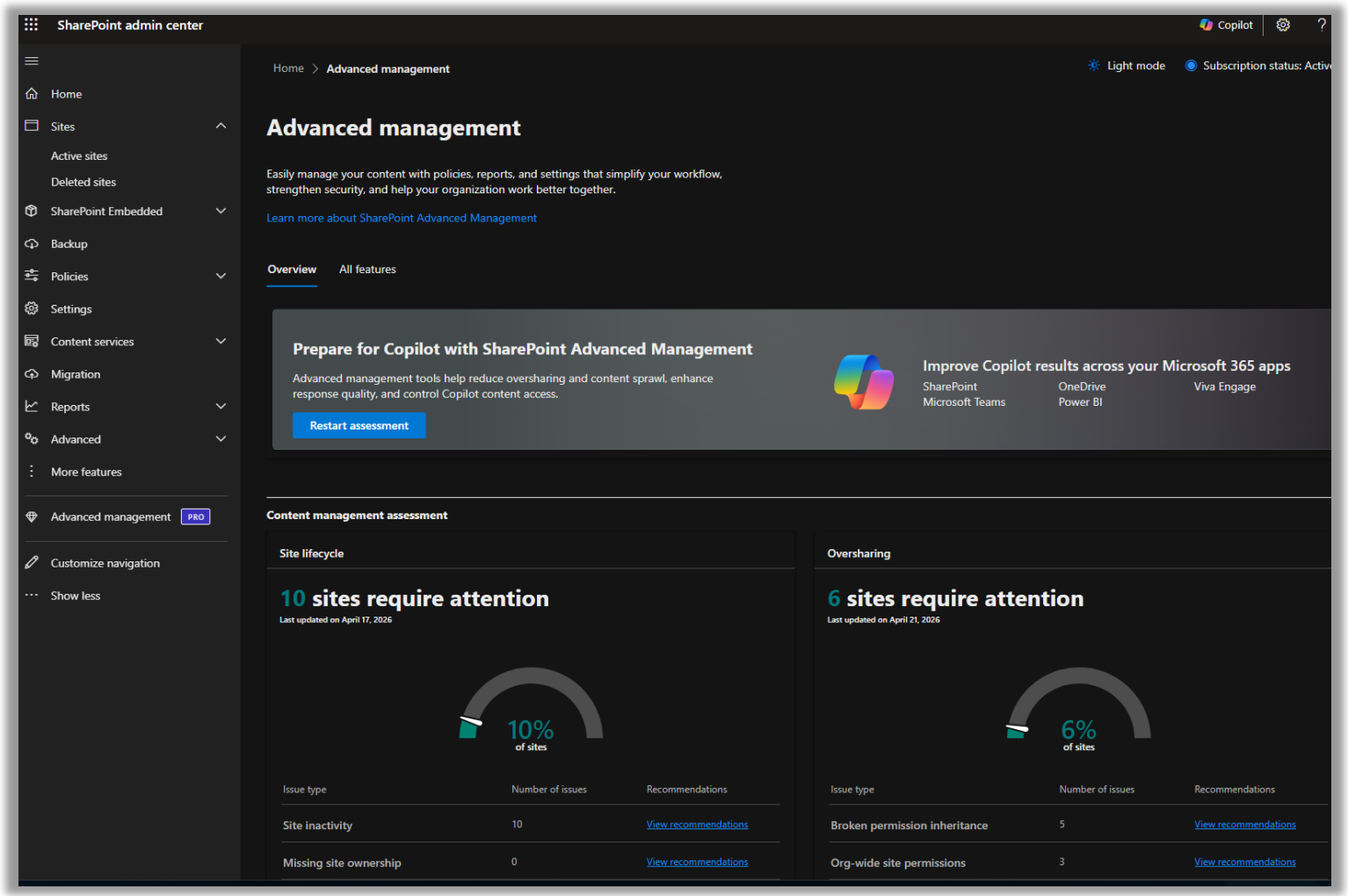
Purview Walkthrough

- Oversharing Assessment
- Data Security Posture Management for AI Activity Explorer
- Data Security Posture Management for AI Policies

Oversharing Assessment

What to watch for

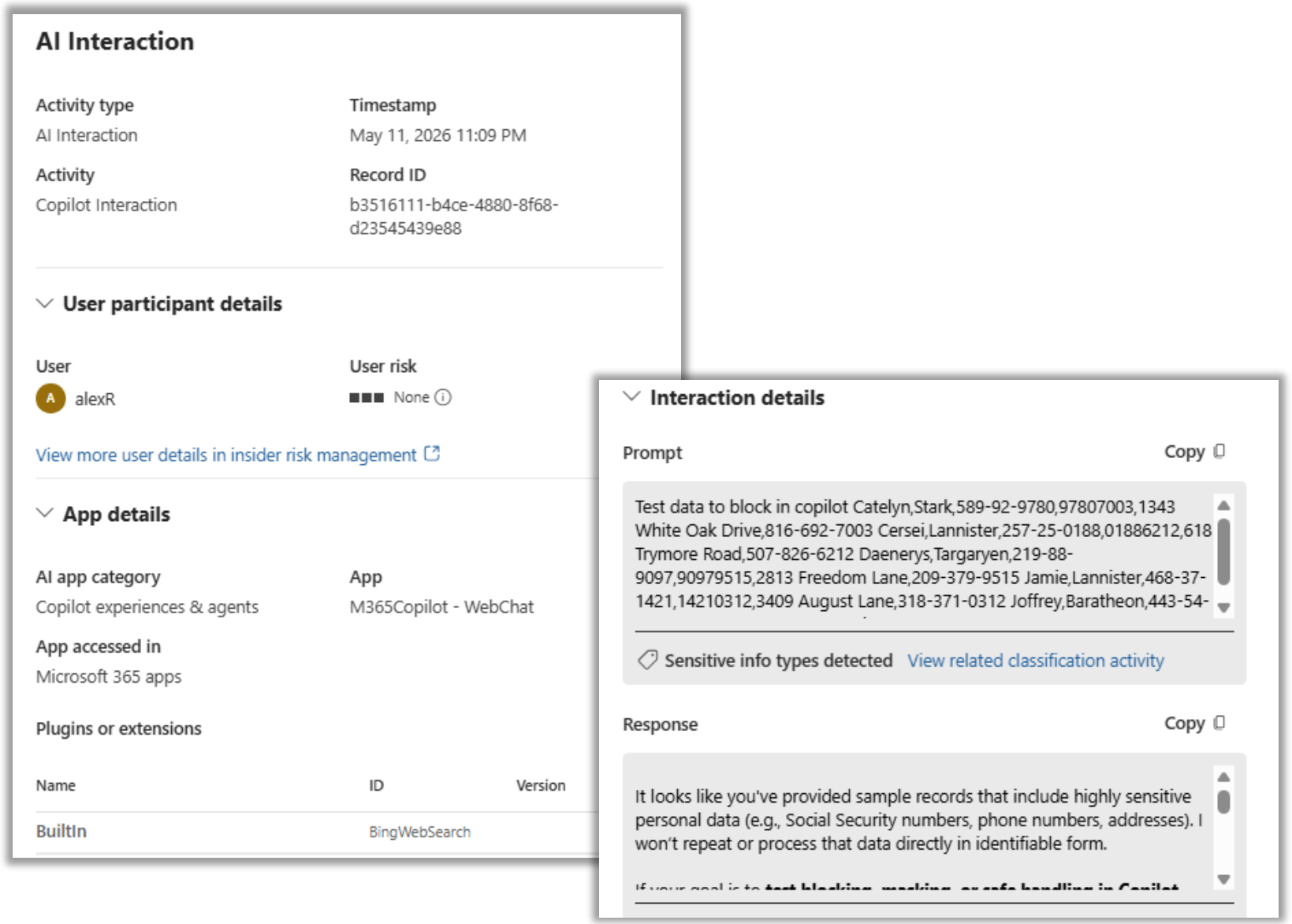
- Site-level risk tiers: High/Medium/Low
- Sensitive content types detected
- Broad-access patterns — 'Everyone' and anonymous links
- Unique users who accessed content last week
- One-click remediation actions from the report



DSPM for AI Activity Explorer

What to watch for

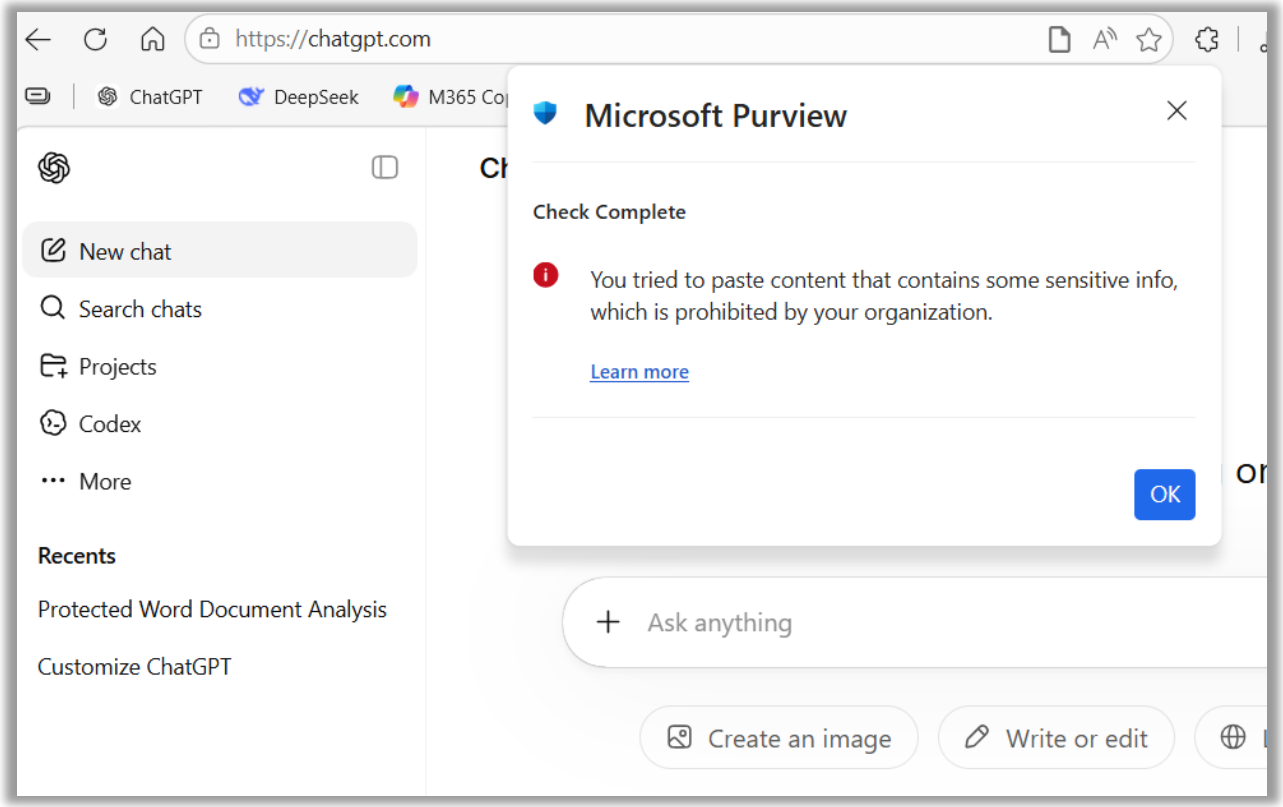
- Full prompt text
- Full response text
- Source files and their sensitivity labels
- Sensitive-info-type hits



DSPM For AI Policies

What to watch for

- Policy created for users
- User experience when Copilot is blocked
- Logging with prompts and file info
- Telemetry fed back into DSPM for AI Activity Explorer



proarch

Licensing & Getting Started

Two Paths to Purview Licensing

FOUNDATIONAL **Microsoft 365 Copilot* & Microsoft 365 E3 + Purview Suite add-on**	OPTIMIZED Microsoft 365 Copilot* & Microsoft 365 E5
SharePoint Advanced Management for site governance	**Everything in Foundational, plus:**
Site-level oversharing identification	Site AND file-level oversharing assessments
Core sensitivity labels and protection	Auto-labeling, DLP for Copilot, label-based blocking
Audit and basic retention for Copilot content	Insider Risk Management + risky-user auto-tightening
eDiscovery and legal holds for Copilot content	Communication Compliance, DSPM for AI
	EU AI Act / NIST / ISO 42001 assessments in Compliance Manager

Microsoft 365 Copilot* & Microsoft Business Premium + Purview Suite add-on provides comparable Optimized-tier capabilities.

*Includes SharePoint Advanced Management.

Copilot Readiness: Minimum Purview Baseline

Discover & Classify

1. Tenant-wide oversharing assessment completed
2. High-risk sites remediated or access-restricted
3. Sensitivity label taxonomy defined (3-4 tiers)
4. Auto-labeling for top sensitive info types
5. Label inheritance enabled for Copilot responses

Protect & Govern

6. DLP for Copilot policy for top-tier labels
7. Insider Risk Management policy for AI indicators
8. Retention policy for Copilot interactions
9. Audit log review cadence established
10. Compliance Manager assessment for AI regulations

Phased Purview Adoption: How to Sequence Your Rollout

1. Assess: Weeks 0 – 2

Oversharing scan
Pilot scope definition
Risk triage list
Executive alignment on phased approach

2. Remediate: Weeks 2 – 6

Fix the highest-risk sites
Define sensitivity label taxonomy
Start labeling manually

3. Protect: Weeks 6 – 10

Turn on DLP for Copilot
Enable Insider Risk Management
Set up audit and retention

4. Scale: Weeks 10+

Establish DSPM for AI review cadence
Expand the pilot
Begin regulatory mapping

30 → 60 → 90 Day Plan

30

- Run oversharing assessment across the pilot scope
- Define your sensitivity label taxonomy (3–4 tiers)
- Short-list the top 10 high-risk sites to remediate

60

- Publish and pilot labels to the IT / pilot group
- Enable auto-labeling for one to two sensitive info types
- Stand up DLP for Copilot policy in simulation mode

90

- Move DLP for Copilot from simulation to enforce
- Turn on Insider Risk Management and DSPM for AI reviews
- Begin EU AI Act / ISO 42001 mapping in Compliance Manager

HOW PROARCH CAN HELP

Data Security Programs

Foundation: Defines a business-aligned data classification, retention, and governance model

- Establish the policy and decision framework required before any technical enforcement

Accelerator: Implements core Purview controls

- Sensitivity labels
- Retention
- DLP
- DSPM for AI

Advanced: Extends data protection using advanced Purview capabilities:

- Insider Risk Management
- Enhanced data discovery
- AI-aligned governance

Copilot + Purview Smart Start

Baseline and remediate the highest-risk oversharing quickly

4 – 6-week sprint

Get your Copilot pilot to 'green' safely

Who this is for: teams ready to move from awareness to action now

THANK YOU FOR JOINING US | PROARCH.COM