



# Navigating Microsoft Defender & Purview with Insider Risk Management

**Perparim Abdullahu** – Azure Solutions Architect Expert |  
#PerparimLabs



#PerparimLabs #MicrosoftSecurity #MicrosoftPurview  
#InsiderRisk #CloudSecurity

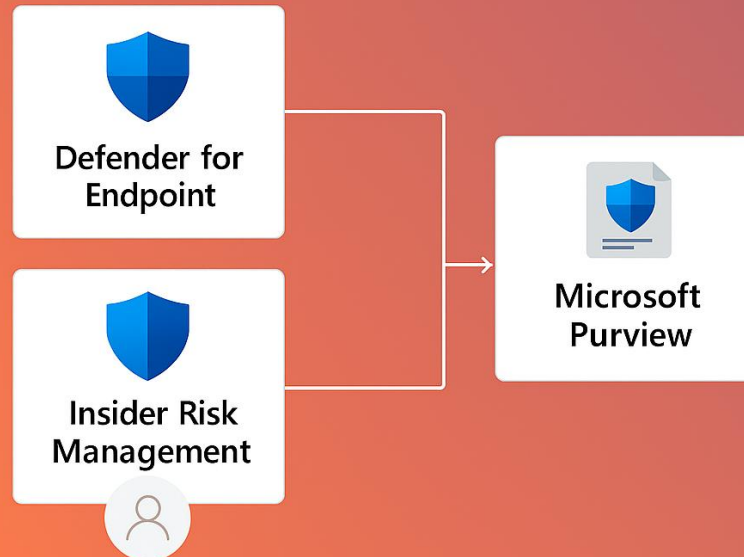


# Microsoft<sup>+</sup><sub>o</sub> 365 Security Ecosystem

• *Both are interconnected → can't master one without the other*

- **Defender** = Security & threat protection

Navigating Microsoft Defender & Purview with Insider Risk Management



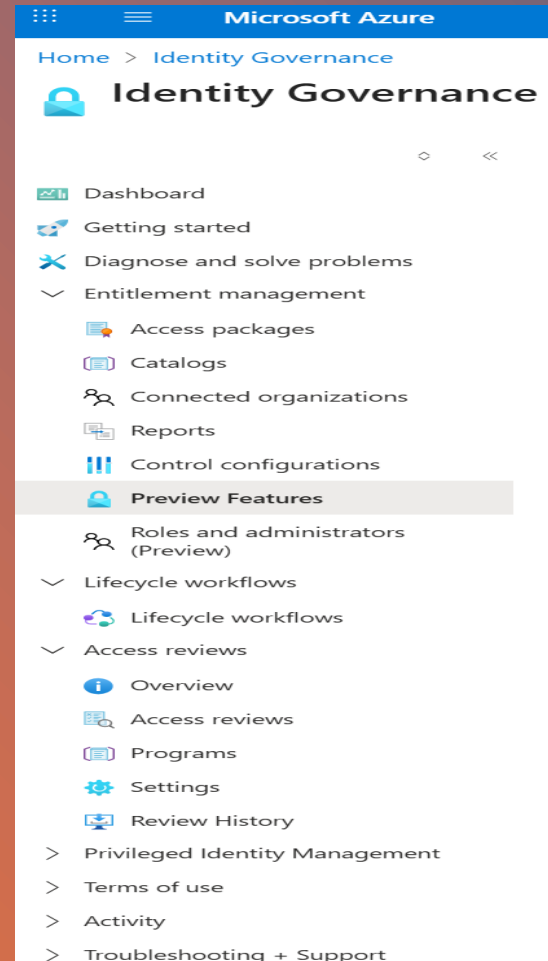
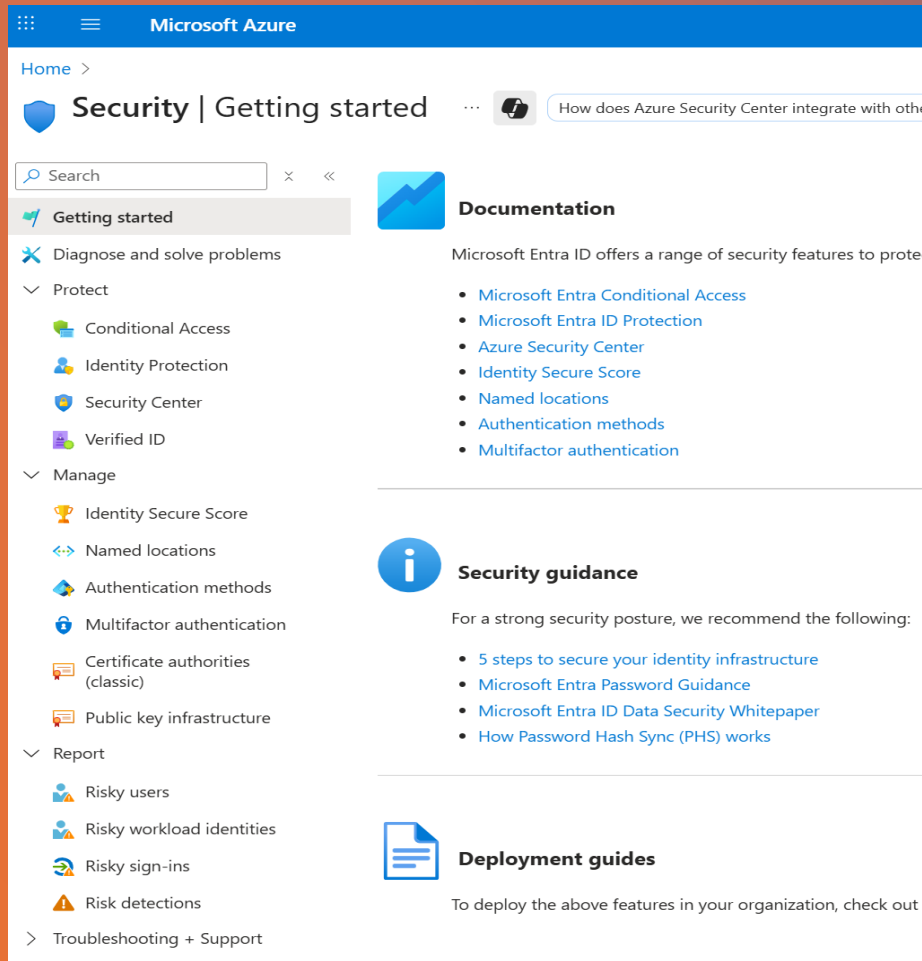
- **Purview** = Compliance & governance

#PerparimLabs #MicrosoftSecurity #MicrosoftPurview  
#InsiderRisk #CloudSecurity

# Accessing the Admin Centers

**Defender (Security portal):** Found under **Microsoft 365 admin center → Security**. Focused on threat protection, alerts, and investigations

**Purview (Compliance portal):** Found under **Microsoft 365 admin center → Compliance**. Focused on governance, data protection, and insider risk management



- Centralized **Entitlement Management**
- Built-in **Lifecycle Workflows** for onboarding/offboarding
- Automated **Access Reviews** for compliance
- Strengthens **Zero Trust & Audit Readiness**

👉 Admins typically work in one or the other depending on role — but both connect to the same Microsoft 365 tenant.

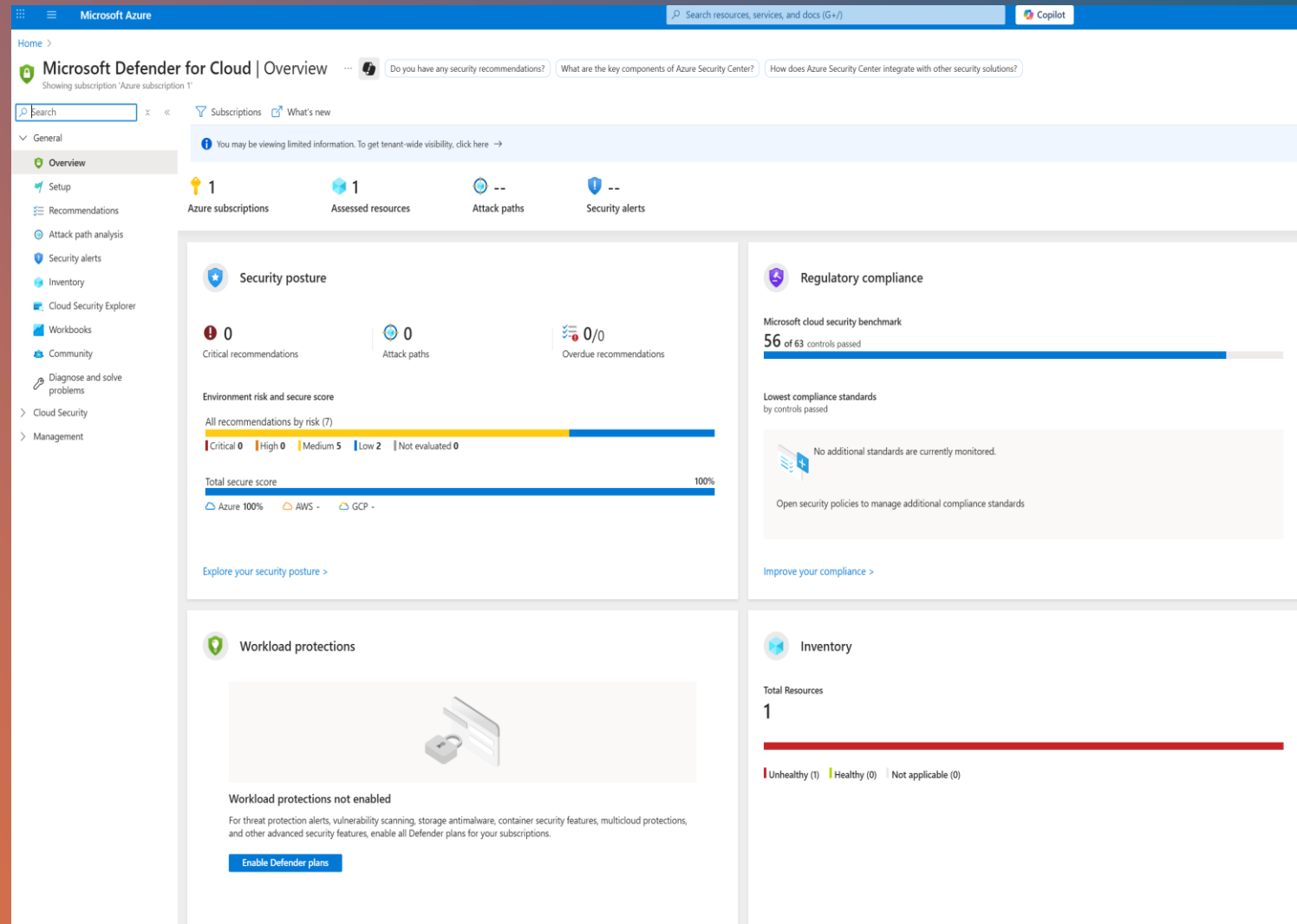
+

# Defender Admin Center

○

- Central hub for:
  - Threat protection (Defender for Office 365, Cloud Apps, Identity, Endpoint)
  - Policy enforcement
- Licensing delay → features may take up to 60 minutes to show

Microsoft 365 Defender unifies incidents, hunting, and threat protection across Endpoint, Office 365, Identity, and Cloud Apps.



# Purview Admin Center

Compliance-focused:

- Policies for data governance
- Auditing, Insider Risk, eDiscovery

Microsoft Purview unifies compliance, risk, and data governance in one platform. It gives organizations visibility and control to secure data wherever it lives.

The screenshot displays the Microsoft Purview Admin Center interface. At the top, there's a navigation bar with the Microsoft Purview logo, a search bar, and a Copilot icon. The main content area features a large banner for 'Maximize productivity with Security Copilot in Microsoft Purview' with a 'Get started' button. Below this, there are three featured cards: 'Data Security Posture Management', 'Data Loss Prevention', and 'Insider Risk Management', each with a 'Learn more' button. A blue banner below these cards provides information about relocated features. A row of solution tiles follows, including 'Data Security Investigations (preview)', 'Data Catalog', 'Information Protection', 'Data Loss Prevention', 'Insider Risk Management', 'DSPM for AI', 'Audit', 'Settings', and 'Compliance alerts'. The 'Featured insights' section at the bottom shows two horizontal bar charts: 'Know your data' (top platforms with data) and 'Top 3 sensitive info types by platform'. The first chart shows 'Microsoft 365' as the top platform. The second chart shows 'Diseases', 'All Medical Terms And Conditions', and 'Taiwan National ID' as the top sensitive info types. A 'View more platforms' link is present at the bottom left of the featured insights section.

Microsoft Purview

Search

Copilot

Home Solutions Agents Learn Settings

Maximize productivity with Security Copilot in Microsoft Purview

Use the power of AI to accelerate data discovery, analysis, and policy improvements

Get started Learn more

Data Security Posture Management

Get centralized visibility into data security risks

Ask for insights into your current posture and recommended policy controls.

Learn more

Data Loss Prevention

Dive into incidents with ease

New enhanced hunting prompts go deep into incident data and users involved.

Learn more

Insider Risk Management

Identify risky user behavior, faster

Quickly understand user intent, activity timing, and top risk factors.

Learn more

Having trouble finding specific features or solutions?

Some features and solutions from the classic portals either have a new home or were retired. To find the ones that moved, try searching for them above. [Review list of relocated and retired features](#)

Data Security Investigations (preview) Data Catalog Information Protection Data Loss Prevention Insider Risk Management DSPM for AI Audit Settings Compliance alerts View all solutions →

Featured insights

Know your data

Top platforms with data

Microsoft 365

View more platforms

Top 3 sensitive info types by platform

Diseases

All Medical Terms And Conditions

Taiwan National ID

Microsoft 365

View more sensitive items

Insider Risk Management, DLP, Audit, Records Management, eDiscovery Premium.

#PerparimLabs #MicrosoftSecurity #MicrosoftPurview

#InsiderRisk #CloudSecurity



# Key Connection

- **Defender protects** → detects risks
- **Purview governs** → ensures compliance & policy alignment

# What is Insider Risk Management?

- A **Purview toolset** for detecting & investigating insider threats
- Risks can be:
  - Accidental (data spillage, mistakes)
  - Malicious (IP theft, fraud, insider trading)

Insider Risk Management in Purview helps detect risky activities like data leaks or insider threats. Built-in policies and analytics provide recommendations to strengthen security and compliance.

The screenshot shows the Microsoft Purview Insider Risk Management interface. The left sidebar contains navigation links: Home, Solutions, Agents, Learn, Settings, and Insider Risk Management. The main content area is titled 'Overview' and displays a list of recommended actions for 'Perparim Abdullahu'. The actions include turning on auditing, analytics, getting to know insider risk management, configuring settings, creating a first policy, and making sure the team can get their jobs done. Each action has a status (Required or Optional), an estimated time, and a link to a video tutorial. A 'Summary' section below the actions shows 'No policy data found' and 'No data available at this moment'. A 'Reports' section is at the bottom right, with a link to 'View all reports'.

**Microsoft Purview** Search Copilot

## Insider Risk Management

### Overview

Perparim Abdullahu, here are your top recommended actions [All recommended actions →](#)

Action	Status	Estimated Time	Includes video tutorial
<input type="radio"/> <b>Turn on auditing</b> Start recording user and admin activity to the audit log.	Required	2 min	
<input type="radio"/> <b>Turn on analytics to scan for potential risks</b> Scans run daily and provide real-time insights to help detect activity that matters most.	Optional	48 hours	<a href="#">Includes video tutorial</a>
<input type="radio"/> <b>Get to know insider risk management</b> Learn about the solution...what it is, best practices, common terms, and more.	Optional	10 min	
<input type="radio"/> <b>Configure insider risk settings</b> Define settings that apply to all insider risk features and workflows.	Required	10 min	<a href="#">Includes video tutorial</a>
<input type="radio"/> <b>Create your first policy</b> Use predefined templates to detect risk activities, such as data theft.	Required	5 min	
<input type="radio"/> <b>Make sure your team can get their jobs done</b> Assign permissions by adding other admins to insider risk management role groups.	Required	10 min	<a href="#">Includes video tutorial</a>

### Summary

No policy data found  
No data available at this moment

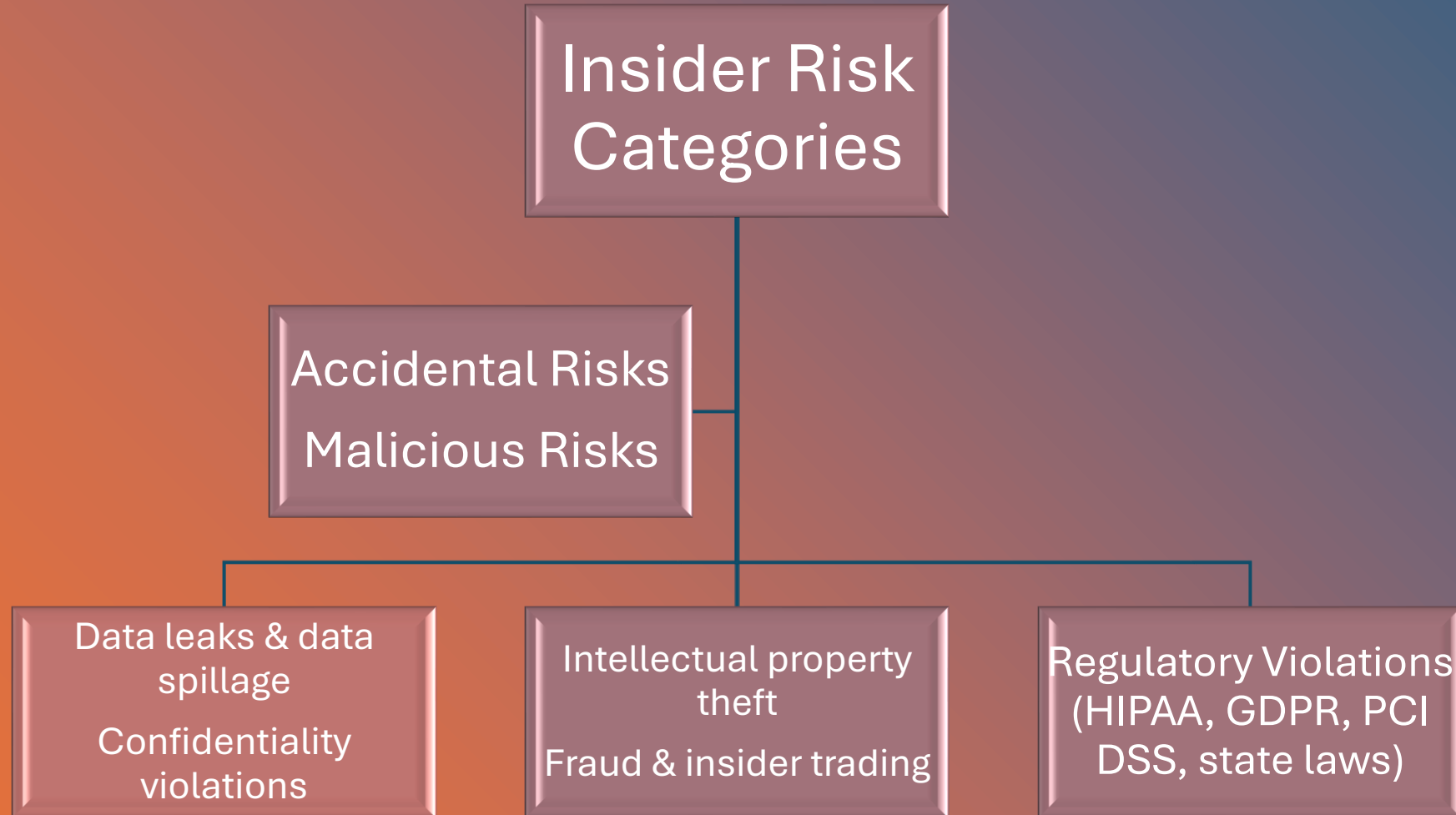
### Reports

[View all reports →](#)



# + • Modern Risk Pain Points

- 





# IRM Principles

- **Transparency** – balance privacy vs protection
- **Configurable Policies** – templates + customization
- **Integrations** – across Microsoft 365 apps
- **Actionable Alerts** – insights + notifications

Microsoft Purview

Search

Home  
Solutions  
Agents  
Learn  
Settings  
Insider Risk Management

Insider Risk Management

Overview  
Recommendations  
**Policies**  
Reports  
Forensic Evidence  
Adaptive Protection

Related solutions

- Communication Compliance
- Data Security Investigations (preview)
- Data Loss Prevention

## Policies

**Attention:** You currently aren't assigned to a role group that allows you to view alerts. Consider assigning somebody to this role. [Learn which role groups are needed to review alerts](#)

Policy warnings | Policy recommendations | Healthy policies

0 | 0 | 0

Scan for potential risks in your org. Turn on analytics to scan user activity daily. You'll get real-time, pseudonymized insights to help you set up and refine policies so you're detecting the most relevant activity. [Learn more](#)

**Review collection policies.** Collection policies control what activities can be detected by device indicators. We recommend reviewing your org's collection policies to ensure they're set up to detect the device activities you want to monitor. [Learn more](#)

+ Create policy | Start scoring activity for users | Refresh

Policy name ↑ ↓	Status ↓	Users in scope ↓	Active alerts ↓	Confirmed alerts ↓
You don't have any policies yet.				

We recommend starting with a data leaks quickstart. [Get started](#)

# IRM Workflow

- Define policies → trigger **alerts**
- Triage alerts → prioritize by severity
- Investigate cases (dashboards, content explorer, activity history)
- Take action (training, discipline, escalate to legal via **eDiscovery Premium**)

Investigate cases (dashboards, **Activity explorer**, Content explorer...)

#PerparimLabs #MicrosoftSecurity #MicrosoftPurview  
#InsiderRisk #CloudSecurity

**Create a data leak policy**

**Time to complete**  
2 min

Data leaks can range from accidental oversharing of info outside your organization to data theft with malicious intent. Most organizations with insider risk programs have a data leaks policy in place.

[How do quick policies work?](#)

Review the policy name and user scope we suggested and make changes if needed.

**Policy name \***

Data leaks quick policy -

**User scope \***

Include all users and groups (Recommended for best coverage)

**Settings we filled in for you**

Settings below are based on the latest analytics scan. You can edit them later or click 'Customize' now to configure settings using the full policy wizard.

**Triggering event** ⓘ

User performs an exfiltration activity

**Indicators** ⓘ

- Sharing SharePoint files with people outside the organization
- Sharing SharePoint folders with people outside the organization
- Sharing SharePoint sites with people outside the organization
- Downloading content from SharePoint
- Sending email with attachments to recipients outside the organization
- Sending email with attachments to free public domains
- Sending email with attachments to self
- Downloading content from Teams
- Download then exfiltrate ⓘ
- Detect when a user's exfiltration activities exceed organizational norms

**Overall, how easy or difficult did you find it to create your policy?**

Help our product team improve your experience by answering two short questions

**Create policy** **Customize**



# IRM Policies (Templates)

- Data theft by departing users
- Leaks of sensitive information
- Priority / risky users
- Patient data misuse (HIPAA)
- Risky browser usage

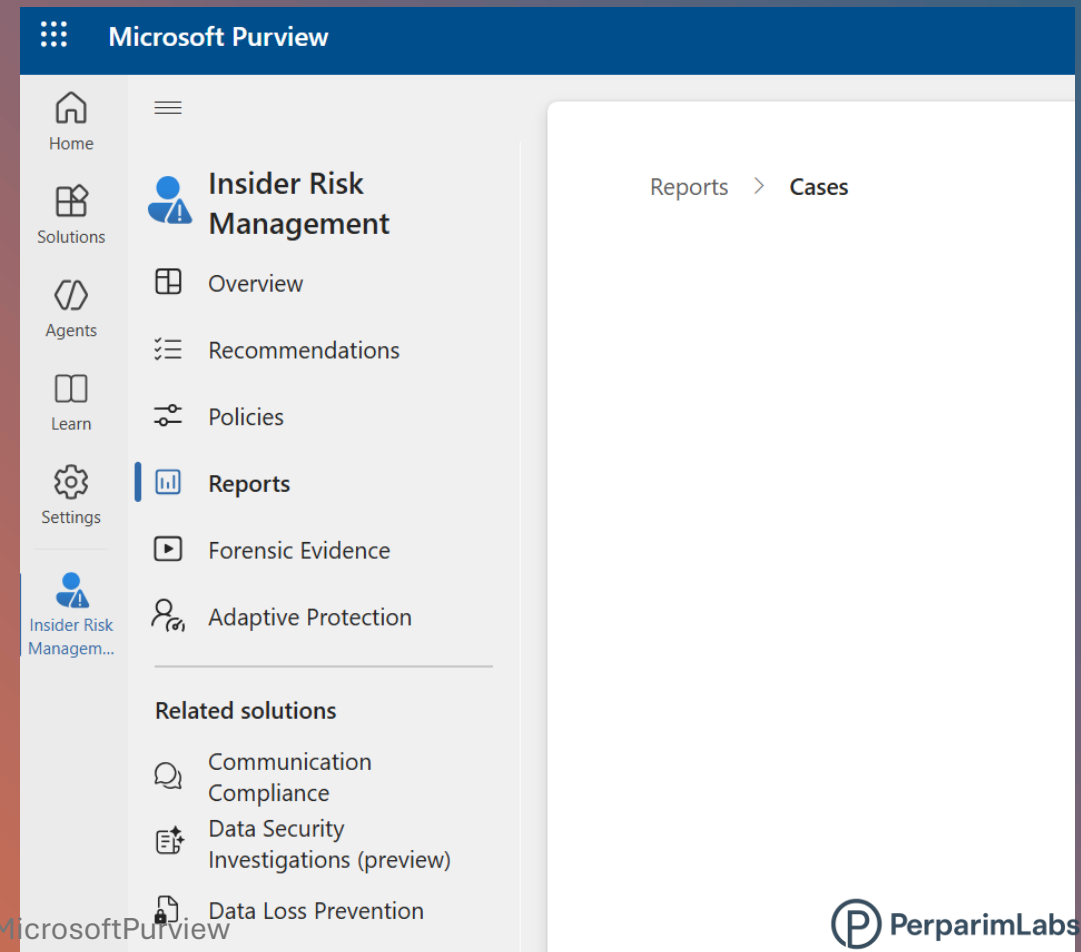
The screenshot displays the Microsoft Purview Insider Risk Management dashboard. The left sidebar contains navigation options: Home, Solutions, Agents, Learn, Settings, and Insider Risk Management. The main content area is titled 'Reports' and includes a search bar. Below the title, a paragraph explains that reports help understand the insider risk program landscape. A table lists four report categories: Alerts, Analytics (marked as 'Unavailable'), Cases, and Forensic Evidence. Each category has a brief description of the data it covers.

Report name	Description
Alerts	Review reports of alerts generated, alerts addressed over time, alerts by policy, and more.
Analytics	Unavailable
Cases	Review reports of cases created, case actions over time, case statuses by policy and region, and more.
Forensic Evidence	

# Alerts & Case Management

- Alerts dashboard: ID, severity, time, case status
- Escalation possible to **eDiscovery Premium** for legal workflows

Case Management lets analysts escalate insider risk alerts into formal cases, assign investigators, and track resolution — all in one dashboard.





# From Detection to Action

Possible outcomes:

- Train employees (**accidental**)
- Disciplinary action
- Legal escalation (insider trading, fraud, IP theft)
- Integration with SIEM for reporting & monitoring

IRM doesn't stop at detection — organizations must follow through with actions to reduce risk.



# Final Takeaways

- Defender & Purview are **two sides of Microsoft 365 security**
- Insider Risk Management = a **critical Purview tool**
- End-to-end process:  
**Detect → Investigate → Act → Comply**

Insider Risk isn't just IT's problem — it's a business-wide responsibility.

[perparimlabs.github.io](https://perparimlabs.github.io)  
[linkedin.com/in/perparim-abdullahu-2b0530324](https://linkedin.com/in/perparim-abdullahu-2b0530324)

#PerparimLabs #MicrosoftSecurity #MicrosoftPurview  
#InsiderRisk #CloudSecurity

