



# Navigating Microsoft Defender & Purview with Insider Risk Management

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

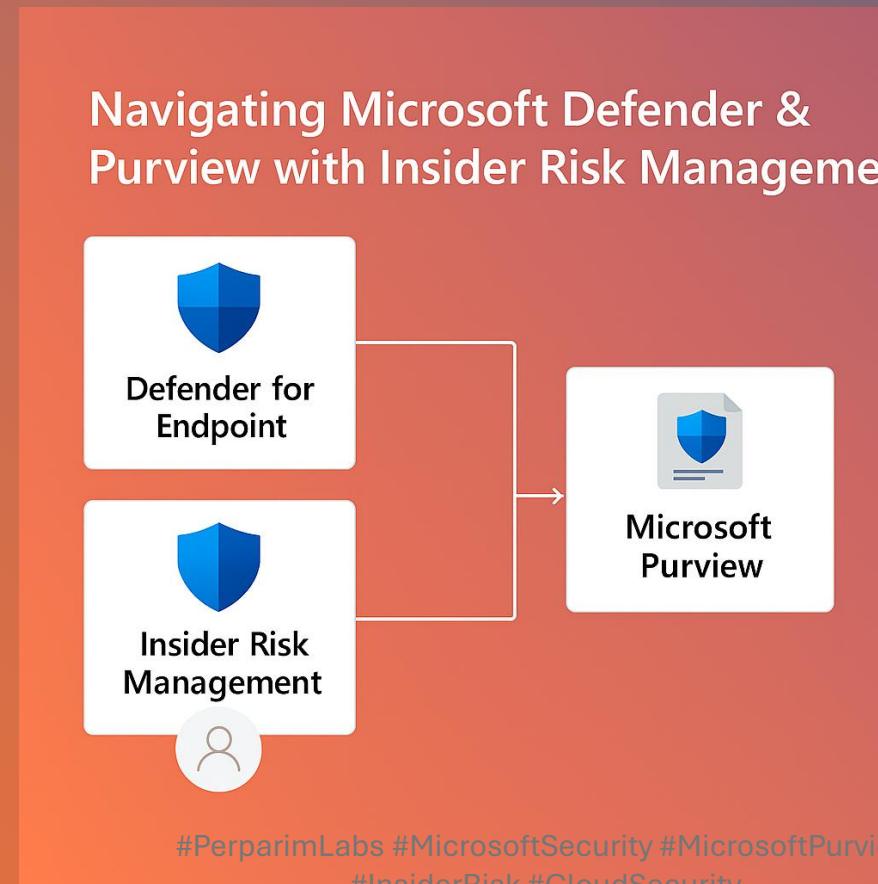


#PerparimLabs #MicrosoftSecurity #MicrosoftPurview  
#InsiderRisk #CloudSecurity



# Microsoft 365 Security Ecosystem

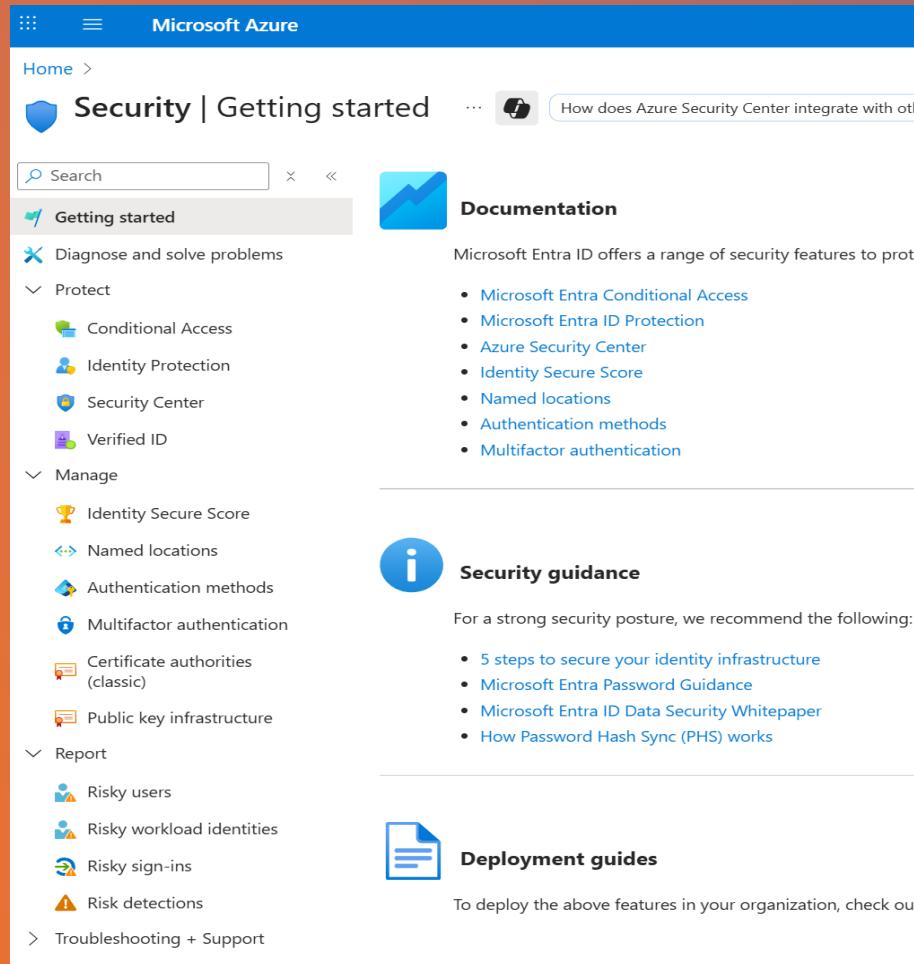
- **Defender** = Security & threat protection
- Both are *interconnected* → can't master one without the other
- **Purview** = Compliance & governance



# Accessing the Admin Centers

o

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



Microsoft Azure

Home > Security | Getting started

Search

Getting started

Documentation

Microsoft Entra ID offers a range of security features to protect...

- Microsoft Entra Conditional Access
- Microsoft Entra ID Protection
- Azure Security Center
- Identity Secure Score
- Named locations
- Authentication methods
- Multifactor authentication

**i** Security guidance

For a strong security posture, we recommend the following:

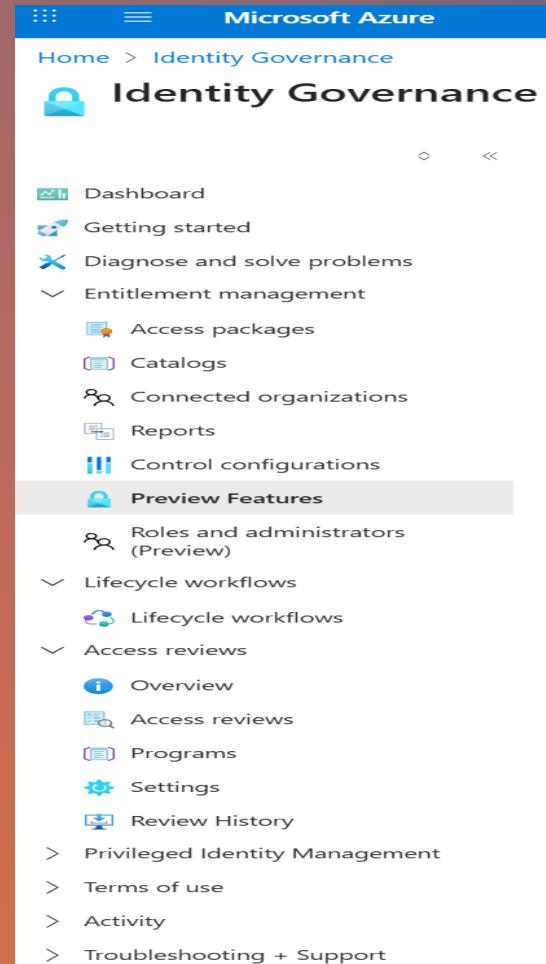
- 5 steps to secure your identity infrastructure
- Microsoft Entra Password Guidance
- Microsoft Entra ID Data Security Whitepaper
- How Password Hash Sync (PHS) works

**Deployment guides**

To deploy the above features in your organization, check out

- Protect
- Manage
- Report

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



Microsoft Azure

Home > Identity Governance

Identity Governance |

Dashboard

Getting started

Diagnose and solve problems

Entitlement management

- Access packages
- Catalogs
- Connected organizations
- Reports
- Control configurations
- Preview Features

Roles and administrators (Preview)

Lifecycle workflows

Access reviews

- Overview
- Access reviews
- Programs
- Settings
- Review History

Privileged Identity Management

Terms of use

Activity

Troubleshooting + Support

- 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.

The screenshot shows the Microsoft Defender Admin Center Overview page. The top navigation bar includes 'Microsoft Azure', a search bar, and a 'Copilot' button. The main content area is titled 'Microsoft Defender for Cloud | Overview' and shows 'Showing subscription 'Azure subscription 1''. It features a summary section with four metrics: 1 Azure subscriptions, 1 Assessed resources, 0 Attack paths, and 0 Security alerts. Below this are four main cards: 'Security posture' (0 Critical recommendations, 0 Attack paths, 0 Overdue recommendations, environment risk score 100%, total secure score 100%), 'Regulatory compliance' (Microsoft cloud security benchmark 56 of 63 controls passed, lowest compliance standards by controls passed, no additional standards monitored, open security policies to manage additional compliance standards), 'Workload protections' (Workload protections not enabled, enable all Defender plans), and 'Inventory' (Total Resources 1, unhealthy 0, healthy 0, not applicable 0).

# 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.

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

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 [View list](#)

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 [View chart](#)

Microsoft 365 [View more platforms](#)

Top 3 sensitive info types by platform [View chart](#)

Diseases [View more sensitive items](#)

All Medical Terms And Conditions [View more sensitive items](#)

Taiwan National ID [View more sensitive items](#)

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

#PerparamLabs #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.

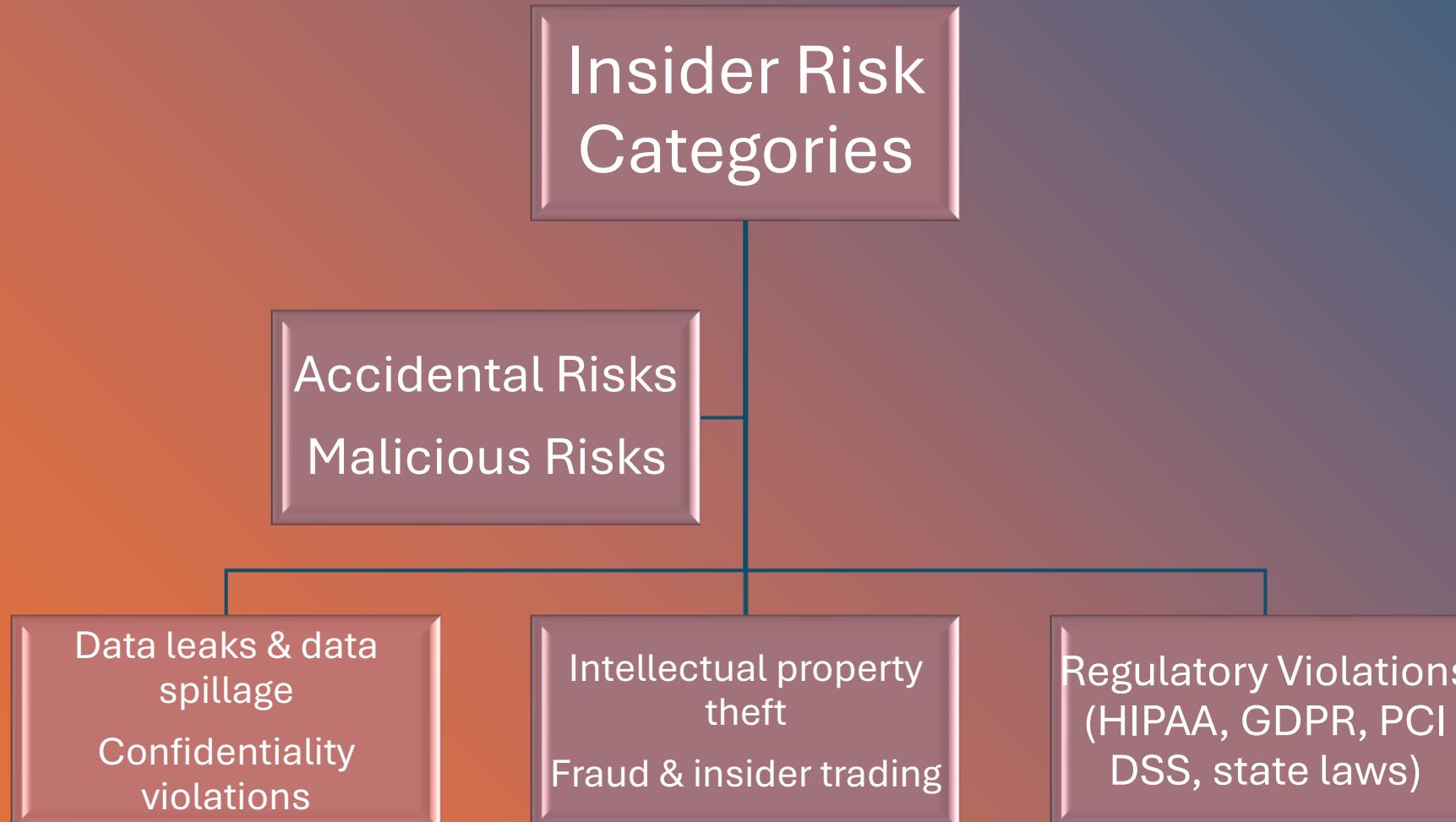
The screenshot shows the Microsoft Purview Insider Risk Management interface. The left sidebar includes Home, Solutions (Insider Risk Management, overview, Recommendations, Policies, Reports, Forensic Evidence, Adaptive Protection), Learn, Settings, and Related solutions (Communication Compliance, Data Security Investigations (preview), Data Loss Prevention). The main content area has a header "Overview" and a sub-section "Perparim Abdullahu, here are your top recommended actions". It lists six items with descriptions, required status, and duration:

- Turn on auditing (Required, 2 min)
- Turn on analytics to scan for potential risks (Optional, 48 hours, includes video tutorial)
- Get to know insider risk management (Optional, 10 min)
- Configure insider risk settings (Required, 10 min, includes video tutorial)
- Create your first policy (Required, 5 min)
- Make sure your team can get their jobs done (Required, 10 min, includes video tutorial)

Below this is a "Summary" section with "No policy data found" and "No data available at this moment". The "Reports" section shows a preview of the Microsoft 365 Activity Explorer with a table of audit logs and a duration of 4 min. The bottom right has a "View all reports" link. The footer includes the PerparimLabs logo and hashtags: #PerparimLabs #MicrosoftSecurity #MicrosoftPurview #InsiderRisk #CloudSecurity.

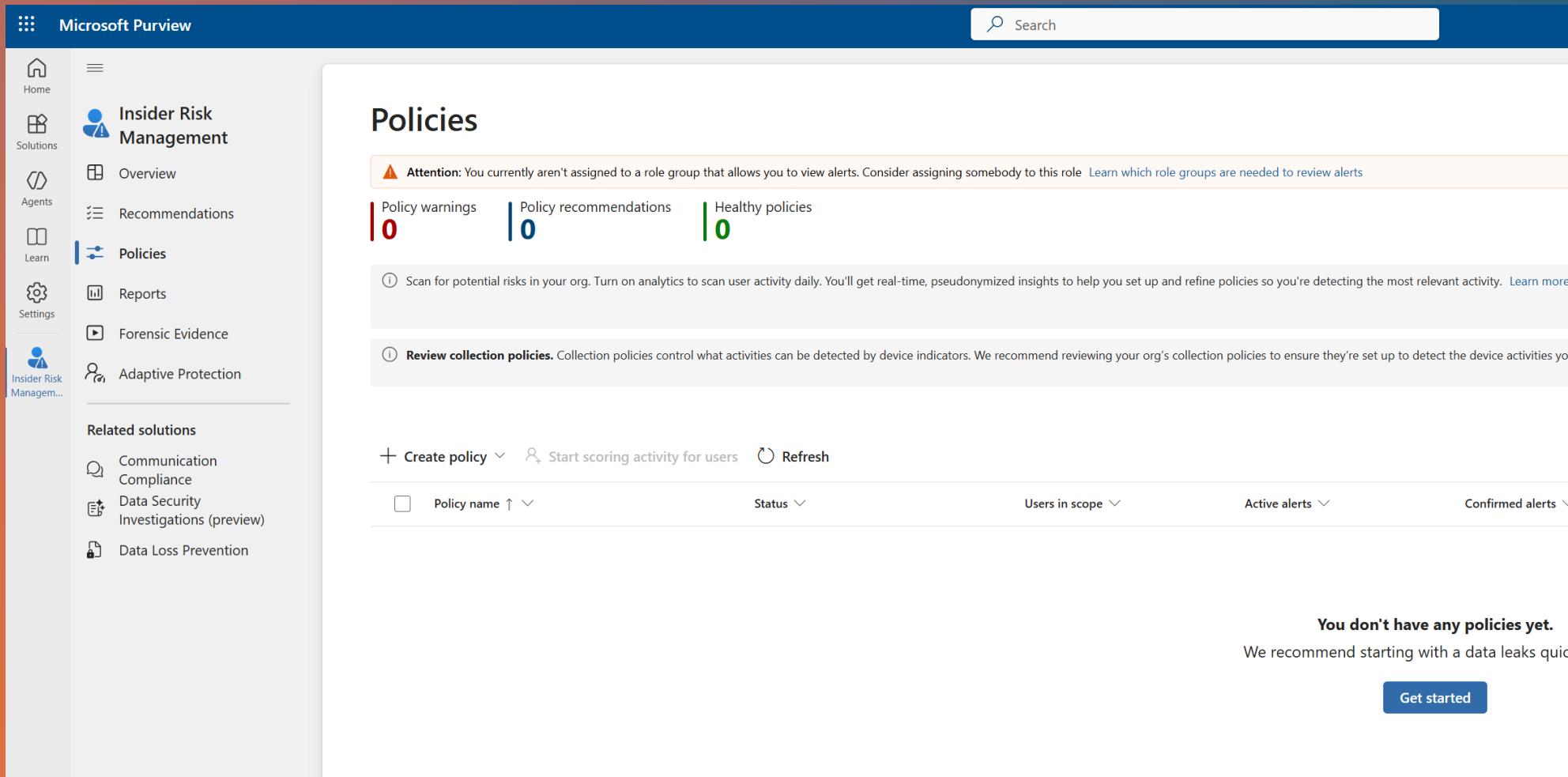
# Modern Risk Pain Points

- +
- 
- 



# IRM Principles

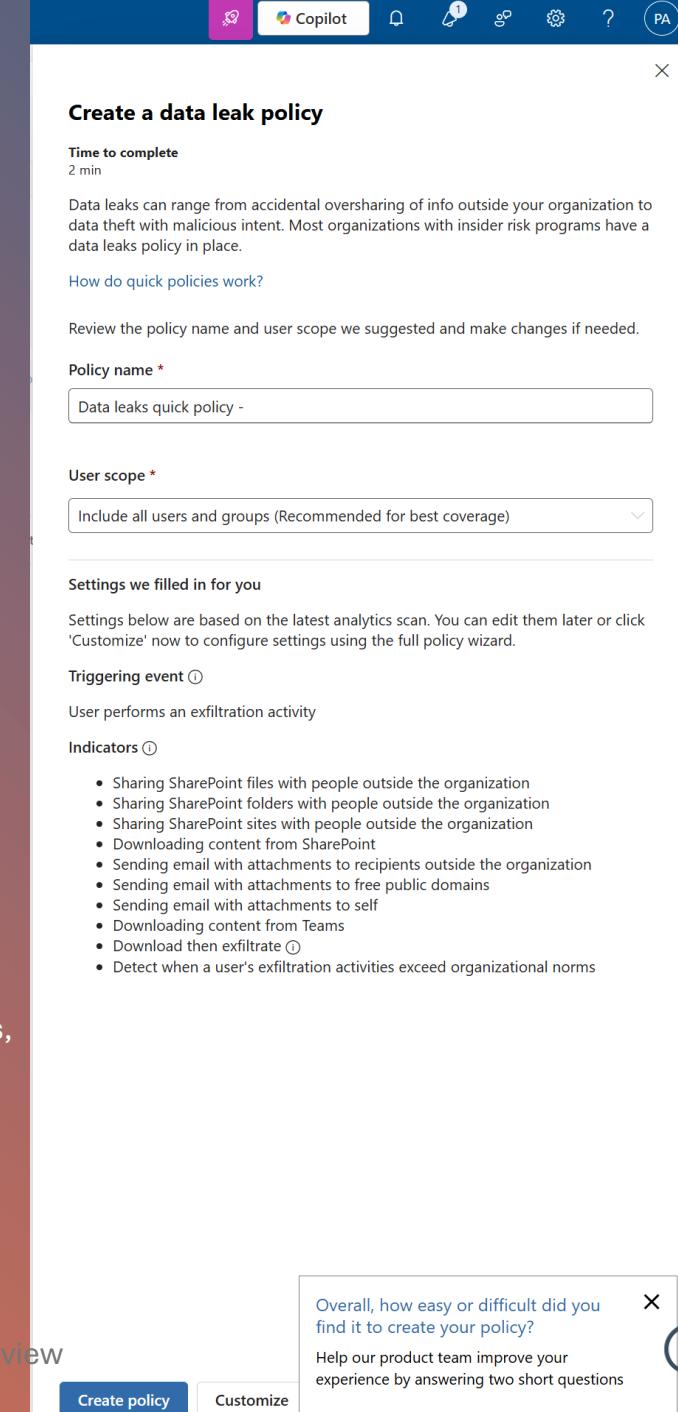
- **Transparency** – balance privacy vs protection
- **Configurable Policies** – templates + customization
- **Integrations** – across Microsoft 365 apps
- **Actionable Alerts** – insights + notifications



The screenshot shows the Microsoft Purview Insider Risk Management Policies page. The left sidebar includes links for Home, Solutions (Insider Risk Management, Overview, Recommendations, Policies, Reports, Forensic Evidence, Adaptive Protection), Agents, Learn, Settings, and a related solutions section for Communication Compliance, Data Security Investigations (preview), and Data Loss Prevention. The main content area is titled 'Policies' and displays three metrics: 'Policy warnings' (0), 'Policy recommendations' (0), and 'Healthy policies' (0). A warning message states: '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](#)'. Below the metrics, there are two informational cards: 'Scan for potential risks in your org' and 'Review collection policies'. At the bottom, there are buttons for 'Create policy', 'Start scoring activity for users', and 'Refresh', followed by filters for 'Policy name', 'Status', 'Users in scope', 'Active alerts', and 'Confirmed alerts'. A message at the bottom right says: 'You don't have any policies yet. We recommend starting with a data leaks quickstart' and a 'Get started' button.

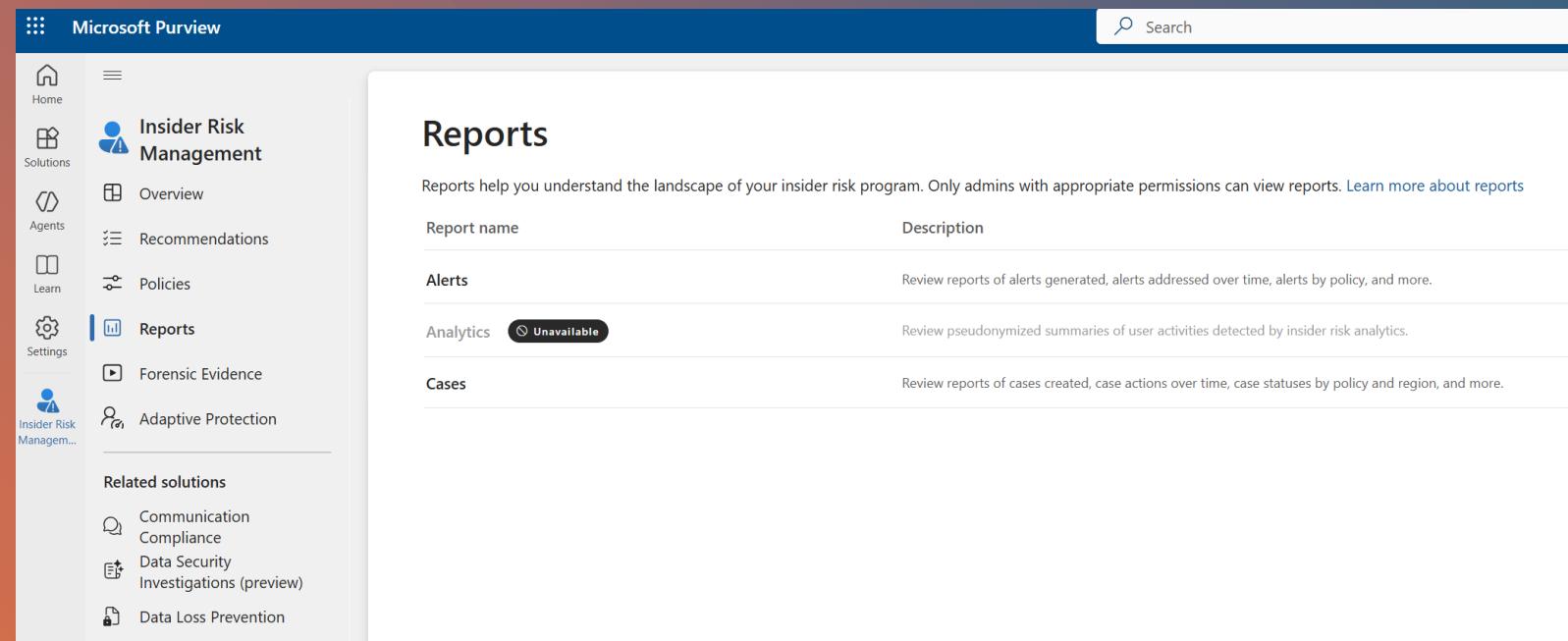
- Define policies → trigger alerts
- Triage alerts → prioritize by severity
- Investigate cases (dashboards, content explorer, activity history)
- Take action (training, discipline, escalate to legal via **eDiscovery Premium**)

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



# IRM Policies (Templates)

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



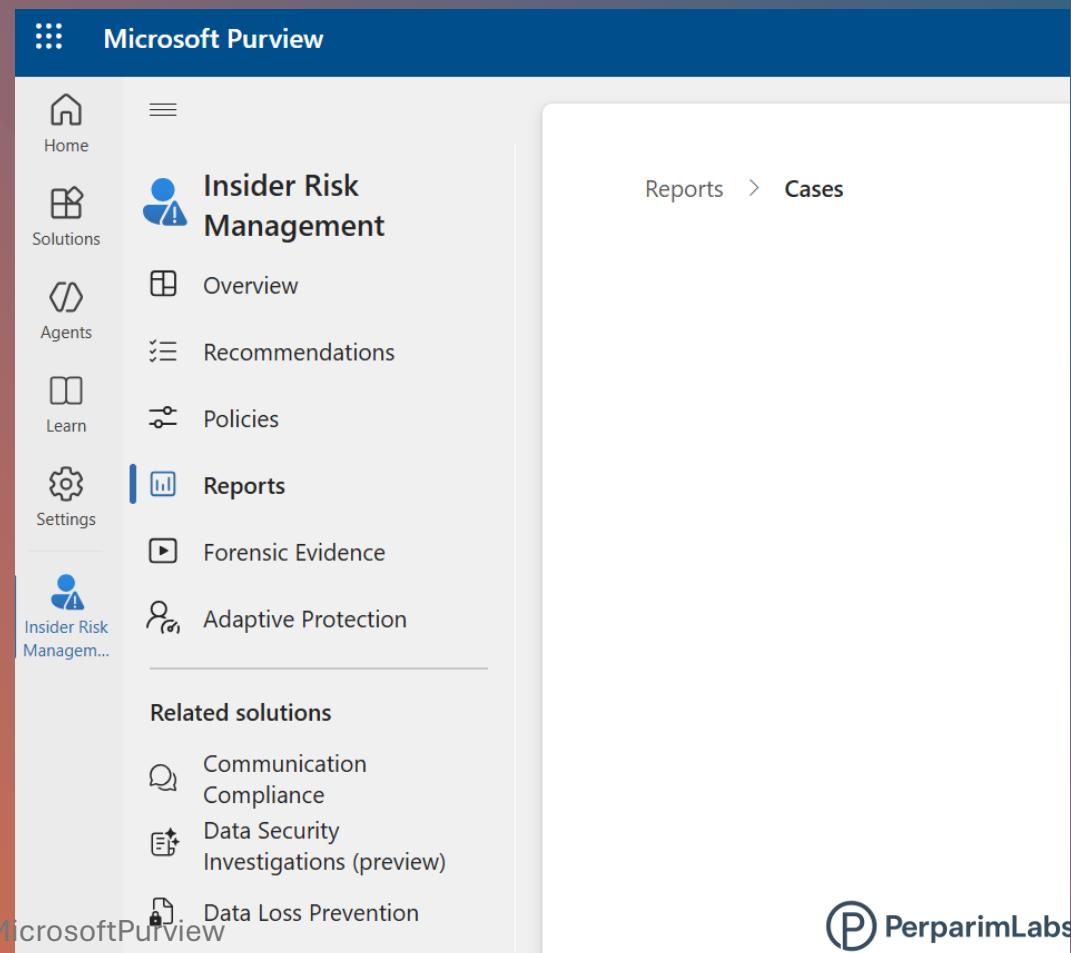
The screenshot shows the Microsoft Purview Insider Risk Management (IRM) Policies (Templates) page. The left sidebar includes links for Home, Solutions, Agents, Learn, Settings, and a related solution for Data Loss Prevention. The main content area is titled 'Reports' and describes how reports help understand the insider risk program landscape. It lists four report types: 'Alerts' (Review reports of alerts generated, alerts addressed over time, alerts by policy, and more.), 'Analytics' (Review pseudonymized summaries of user activities detected by insider risk analytics, currently marked as 'Unavailable'), and 'Cases' (Review reports of cases created, case actions over time, case statuses by policy and region, and more.).



# 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)

