Navigating Microsoft Defender & Purview with Insider Risk Management

Perparim Abdullahu – Azure Solutions Architect Expert |

#PerparimLabs

#PerparimLabs #MicrosoftSecurity #MicrosoftPurview
#InsiderRisk #CloudSecurity

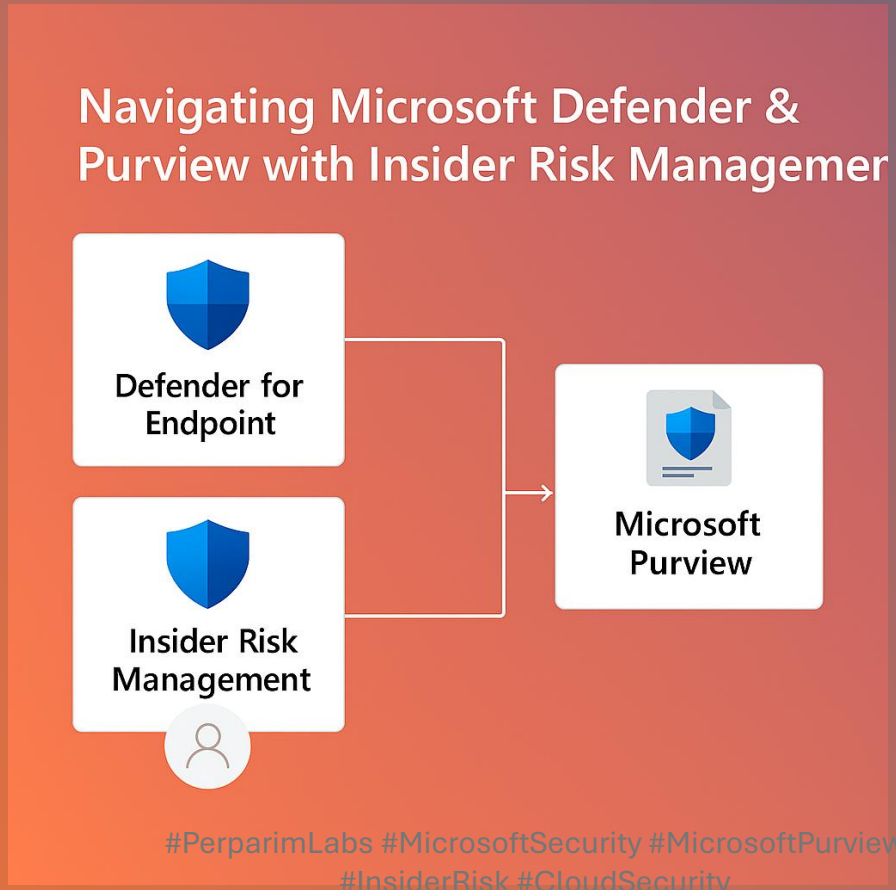
PerparimLabs

Microsoft 365 Security Ecosystem

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

- **Defender** = Security & threat protection

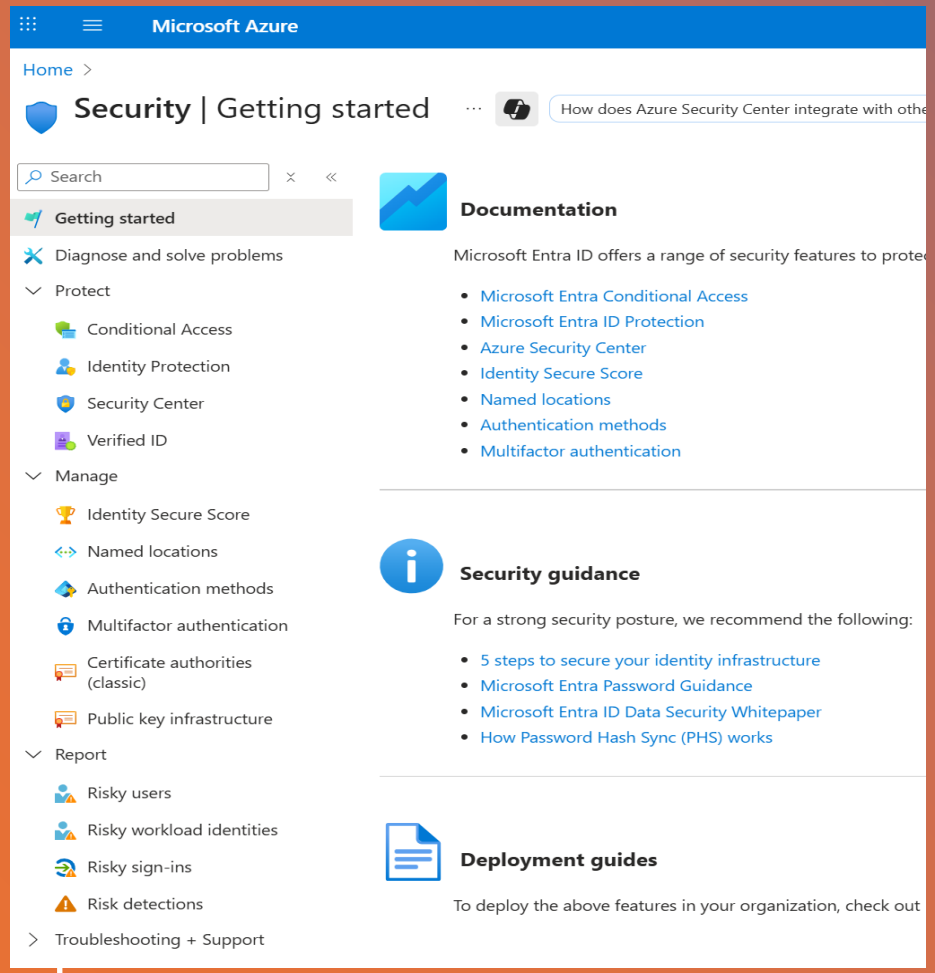
- **Purview** = Compliance & governance



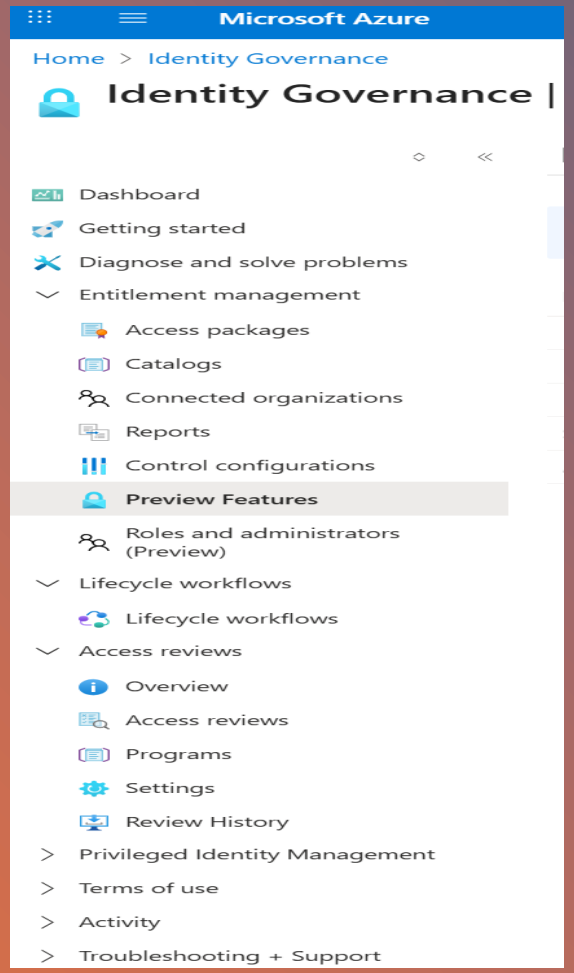
PerparimLabs

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.*

PerparimLabs

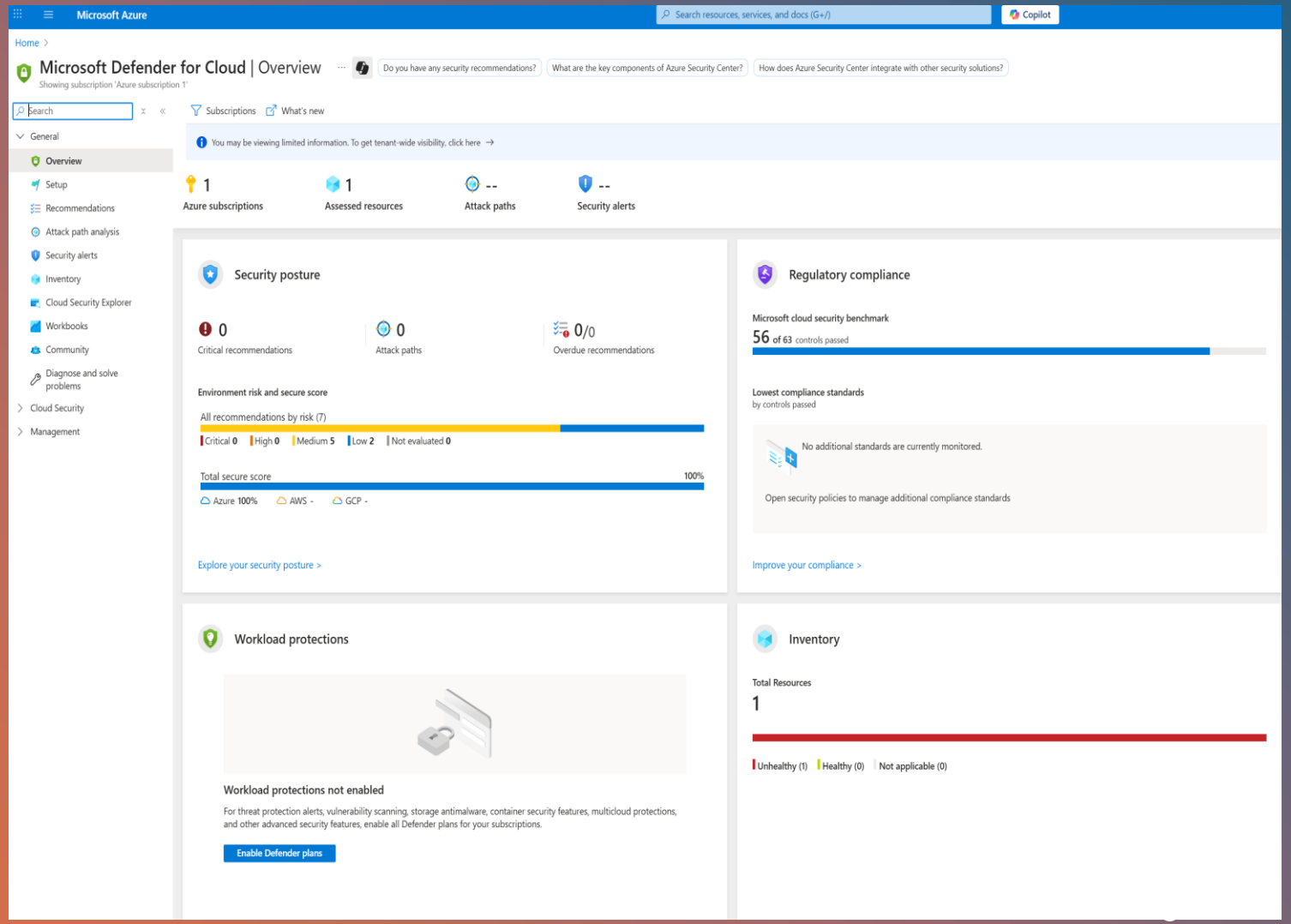
Defender Admin Center

- 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.



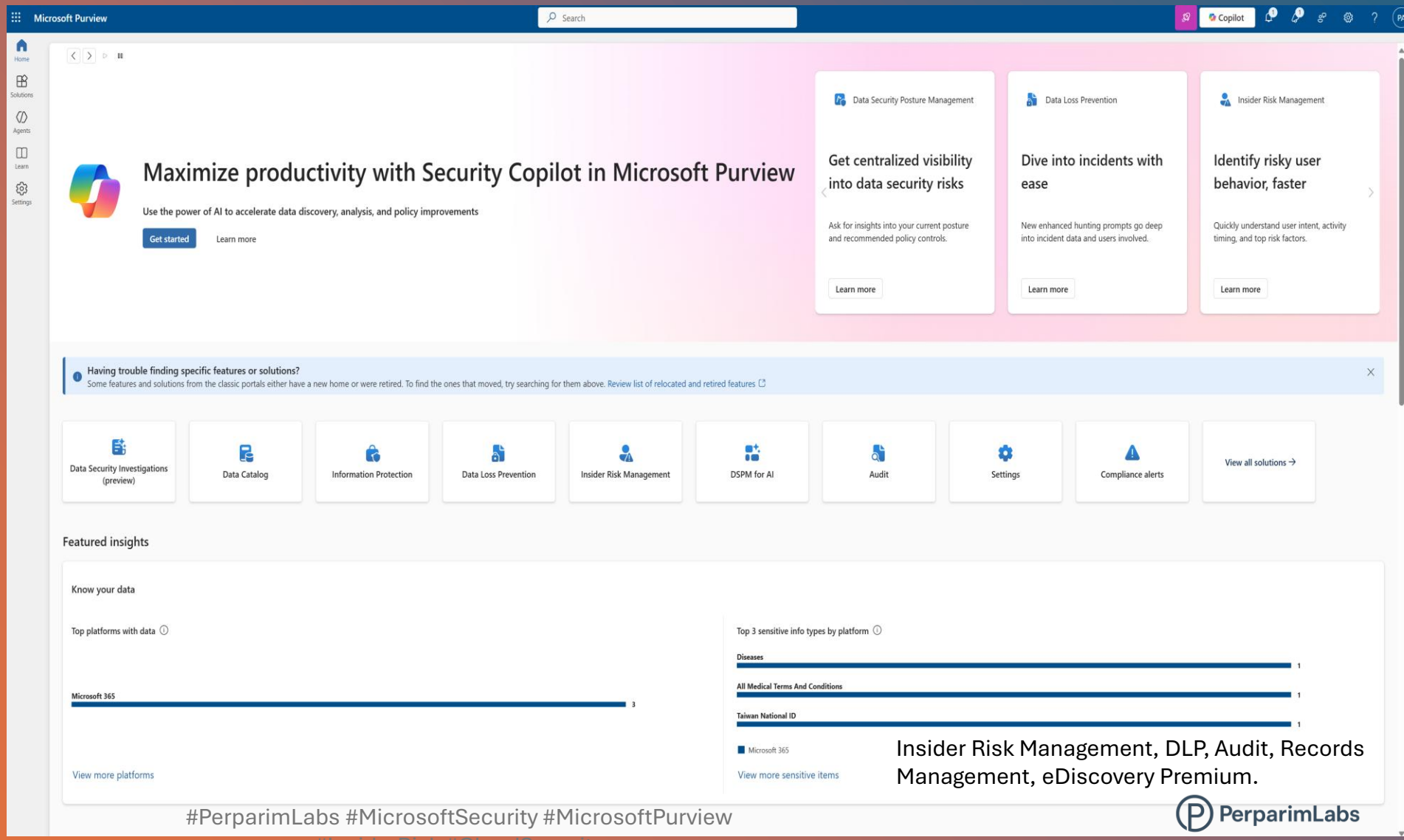
#PerparimLabs #MicrosoftSecurity #MicrosoftPurview #InsiderRisk #CloudSecurity

PerparimLabs

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.

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

#PerparimLabs #MicrosoftSecurity #MicrosoftPurview #InsiderRisk #CloudSecurity

PerparimLabs

Key Connection

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

#PerparimLabs #MicrosoftSecurity #MicrosoftPurview #InsiderRisk #CloudSecurity

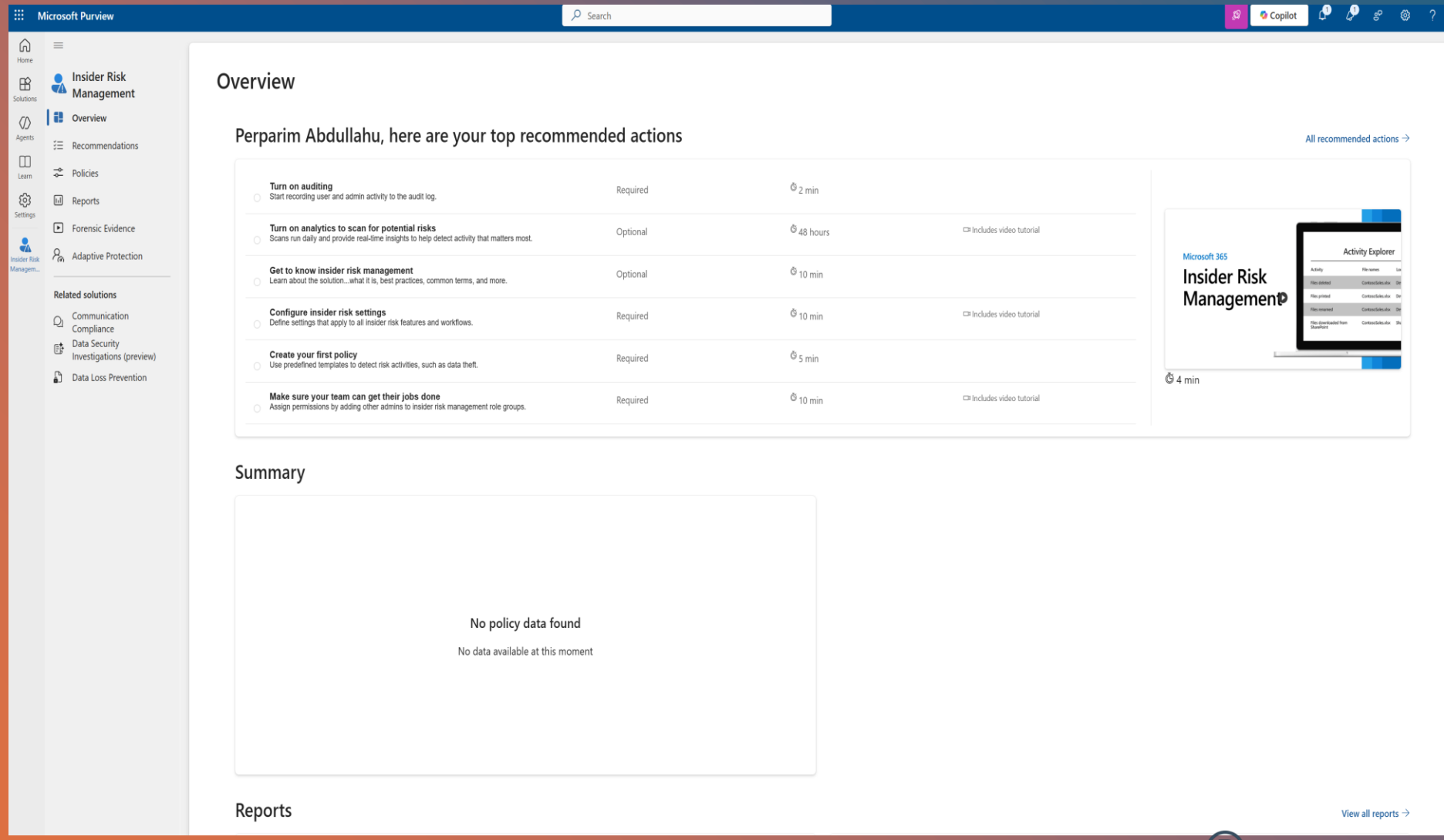
PerparimLabs

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)

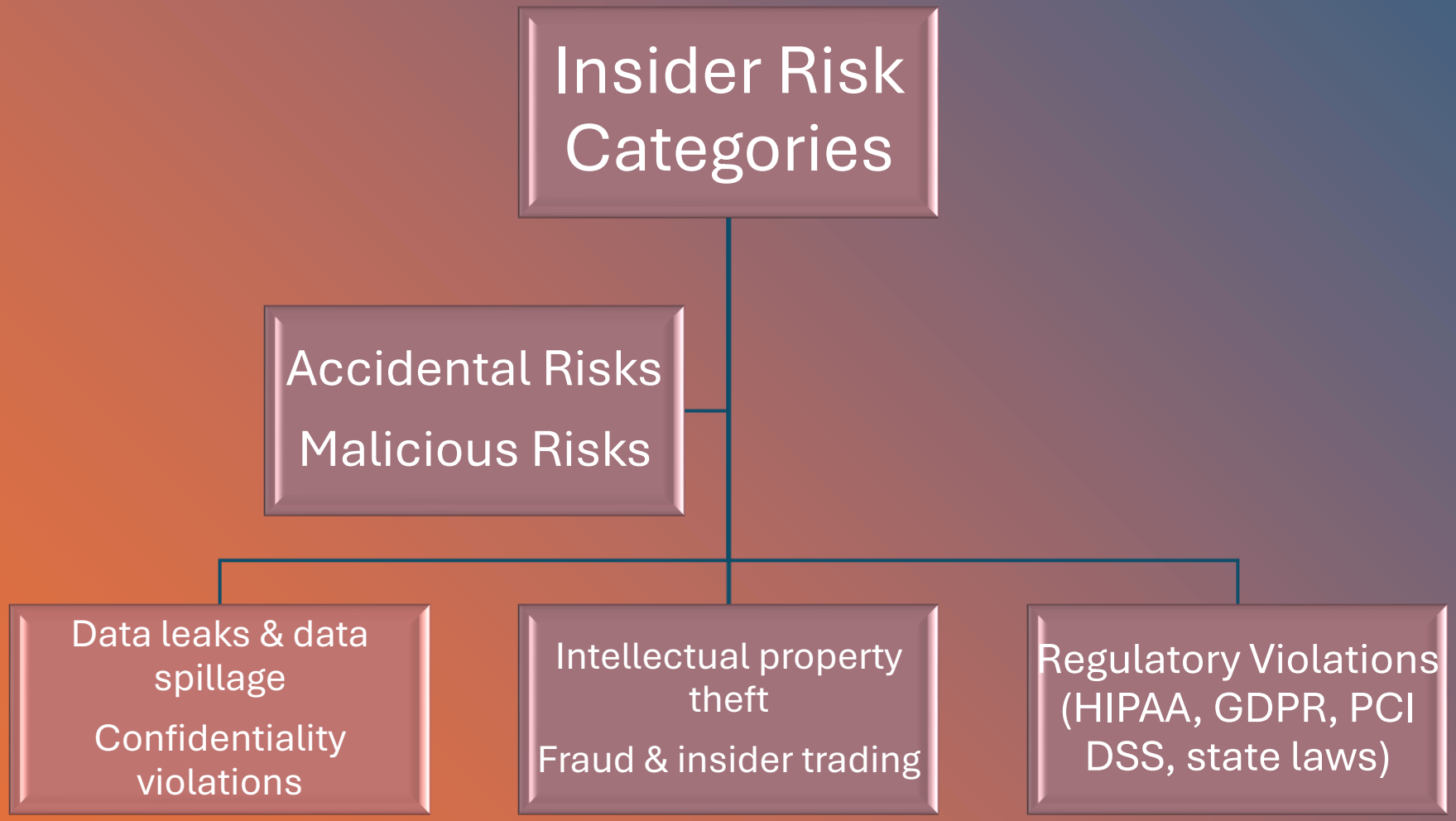
Insider Risk Management in Purview helps detect risky activities like data leaks or insider threats. Built-in policies and analytics provide recommendations to strengthen security and compliance.



#PerparimLabs #MicrosoftSecurity #MicrosoftPurview
#InsiderRisk #CloudSecurity

PerparimLabs

Modern Risk Pain Points

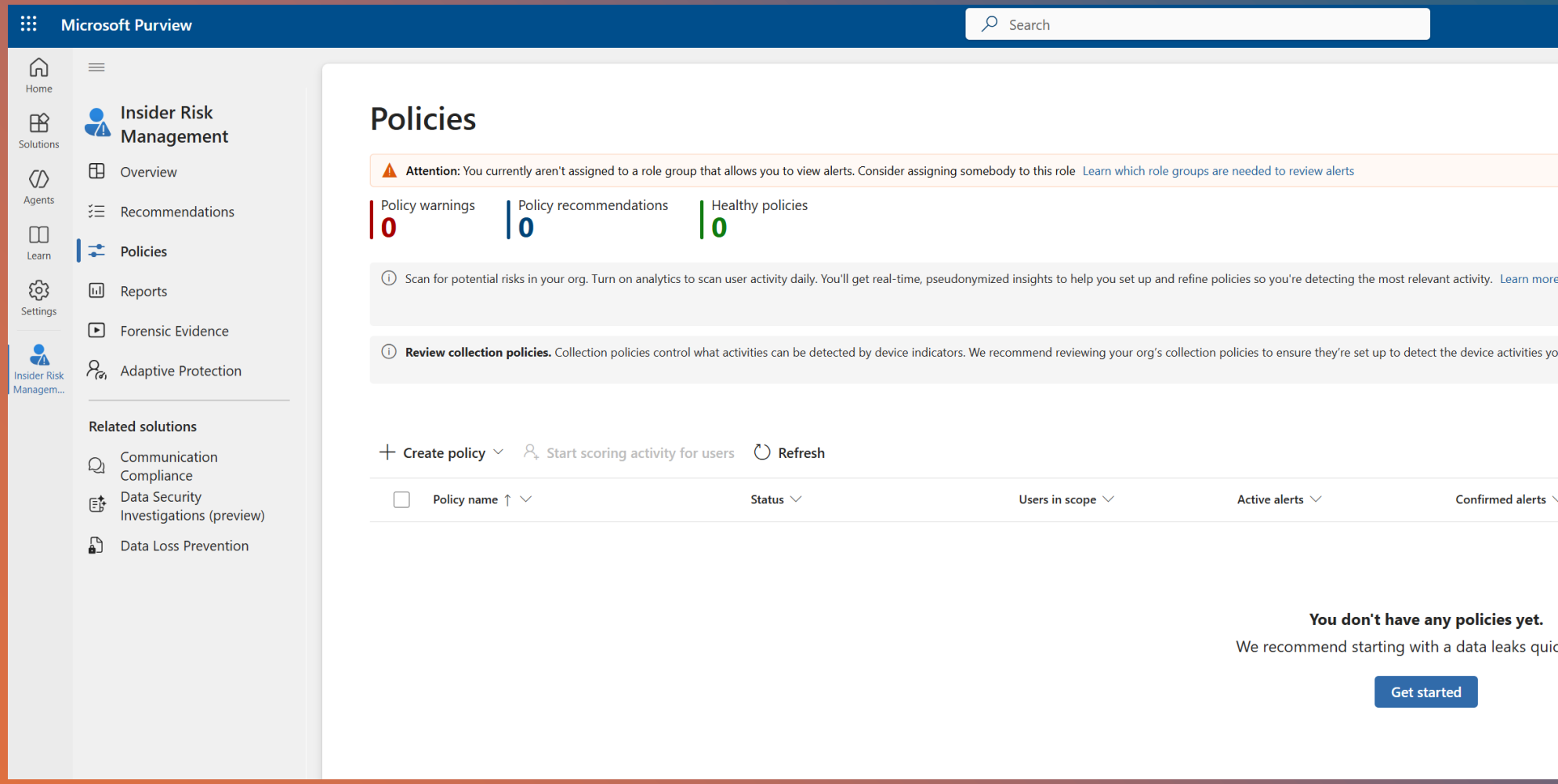


#PerparimLabs #MicrosoftSecurity #MicrosoftPurview #InsiderRisk #CloudSecurity

PerparimLabs

IRM Principles

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



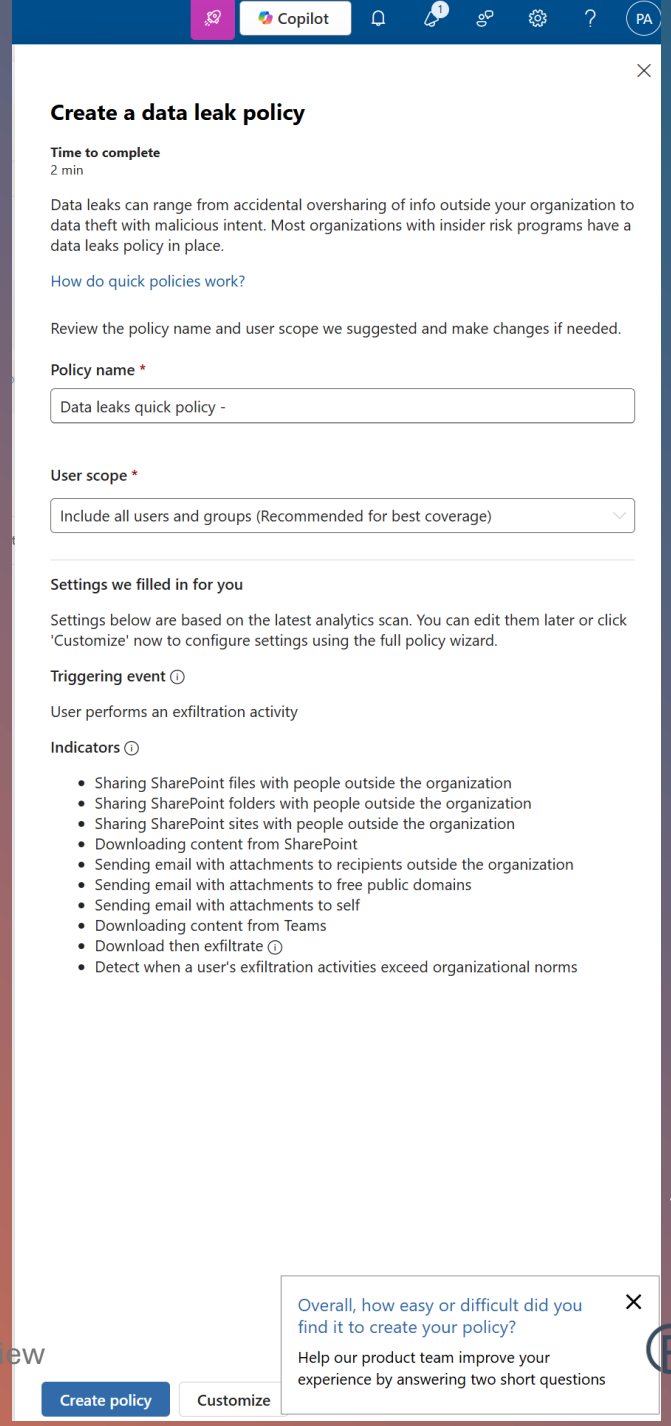
#ParparimLabs #MicrosoftSecurity #MicrosoftPurview #InsiderRisk #CloudSecurity

PerparimLabs

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…)

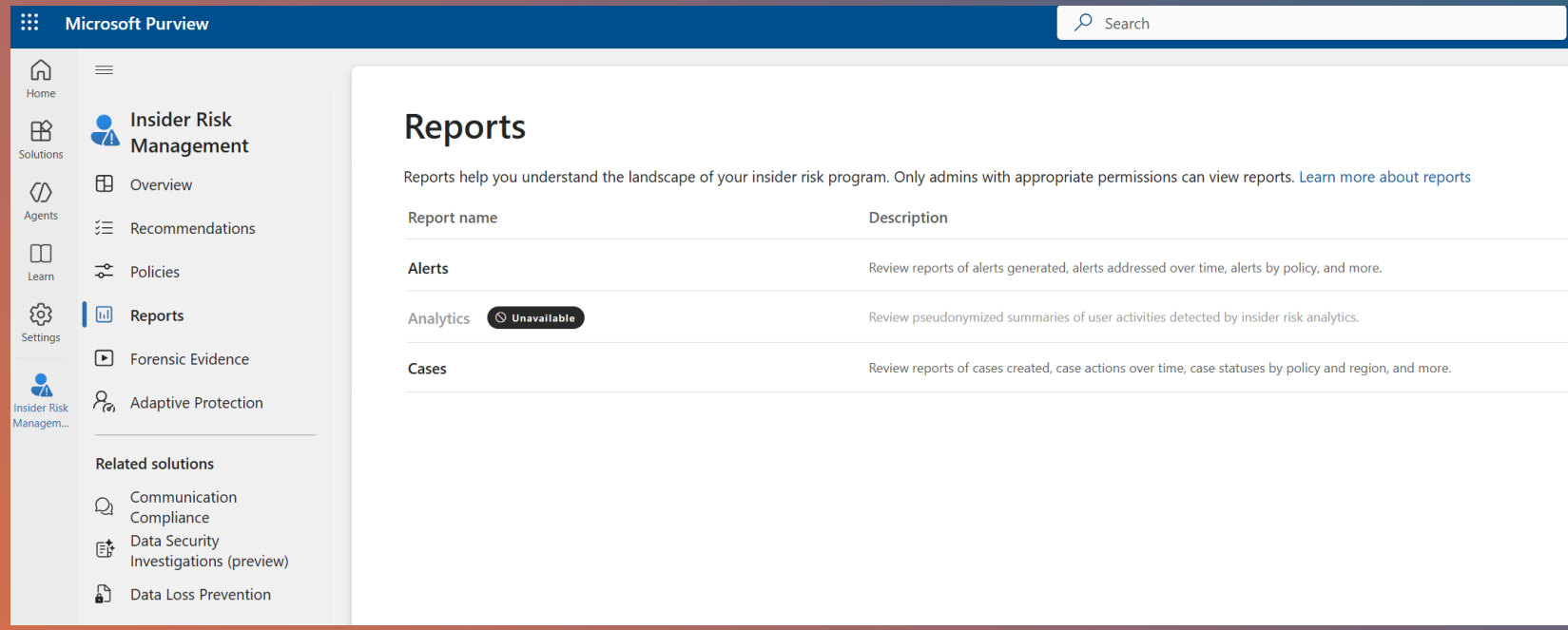


#ParparimLabs #MicrosoftSecurity #MicrosoftPurview #InsiderRisk #CloudSecurity

PerparimLabs

IRM Policies (Templates)

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



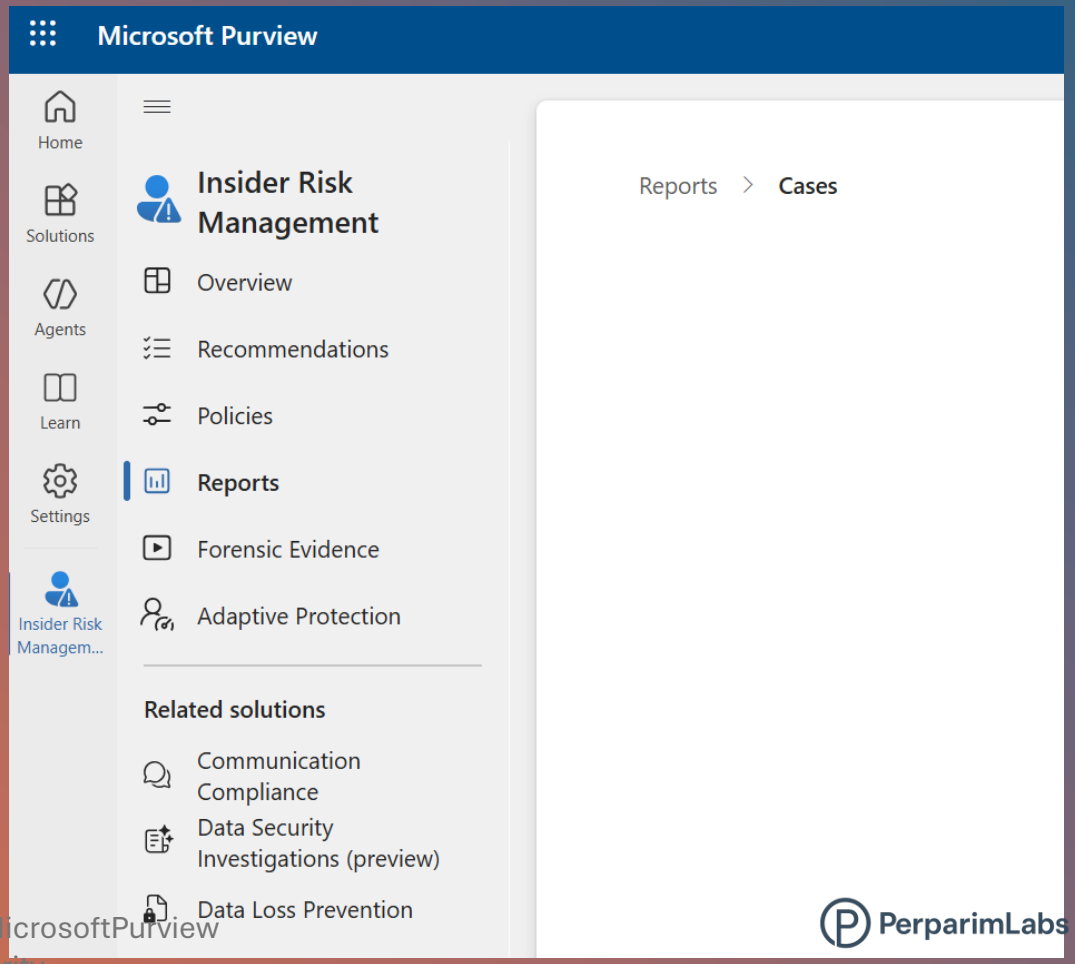
#ParparimLabs #MicrosoftSecurity #MicrosoftPurview
#InsiderRisk #CloudSecurity

PerparimLabs

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.

#PerparimLabs #MicrosoftSecurity #MicrosoftPurview #InsiderRisk #CloudSecurity

PerparimLabs

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
linkedin.com/in/perparim-abdullahu-2b0530324

#PerparimLabs #MicrosoftSecurity #MicrosoftPurview
#InsiderRisk #CloudSecurity

PerparimLabs