Microsoft Power Platform

Governance and security for your enterprise copilot

Diganta Kumar
Principal Product Manager, Microsoft Copilot Studio & Conversational AI

Zohar Raz
Principal Group Program Manager, Microsoft Power Platform Governance

Agenda

1. Security challenges & investments
2. Customer Story
3. Ensure data protection
4. Govern & scale with innovation
5. Visibility in user activities & monitoring

Microsoft Copilot Studio

Data Protection Landscape is Changing

Growing sophistication of attacks

Drive to leverage data to unlock AI-driven scenarios

Data access demands from an increasingly dynamic workforce

Evolving regulatory and legal requirement

Trust Pillars for Enterprise

Full control over access for data protection

How can I control access to data and generative AI?

Data security

- Purview Sensitivity labels
- Data masking
- CMK

Network Layer protection

- Azure subnet
- IP Firewall/Cookie binding
- Endpoint filtering
- CAE

How can I prevent data exfiltration via AI vectors?

Access controls

- DLP
- Sharing limits
- Client apps access control
- Privileged Identity Mgmt.
- Managed identities
- Granular guest access

Full visibility over usage and benefits

What is the cost/benefit of using Power Platform and generative AI?

- Licensing reports
- Tenant & environment reports

How can I gain visibility into user and generative AI activity?

- User & admin activity logging in Purview
- Dataverse audit
- Microsoft Sentinel
- Copilot page

Always safe and compliant

How can I stay compliant with new AI regulations?

- Data residency
- GDPR
- Regulatory compliance
- Lockbox
- Audit logs (ISO, SOC. New EU AI Guidelines)

How can I assess the risk of reliability and safety of generative AI?

- Purview Compliance
- Purview Data Map
- Responsible AI

Security posture management


LUMEN
Corporate Headquarters

Microsoft Power Platform

Lumen

Andrew Gaskins

Global Power Platform Lead at Lumen Technologies

Ensure data protection

- **Govern** access to copilot connectors and features
- **Recommendations** for copilots
- **Warn** makers to secure copilots
- **Authentications** in copilot
- **Prevent** data leaks by masking sensitive data

Data Loss Prevention policy to prevent data exfiltration

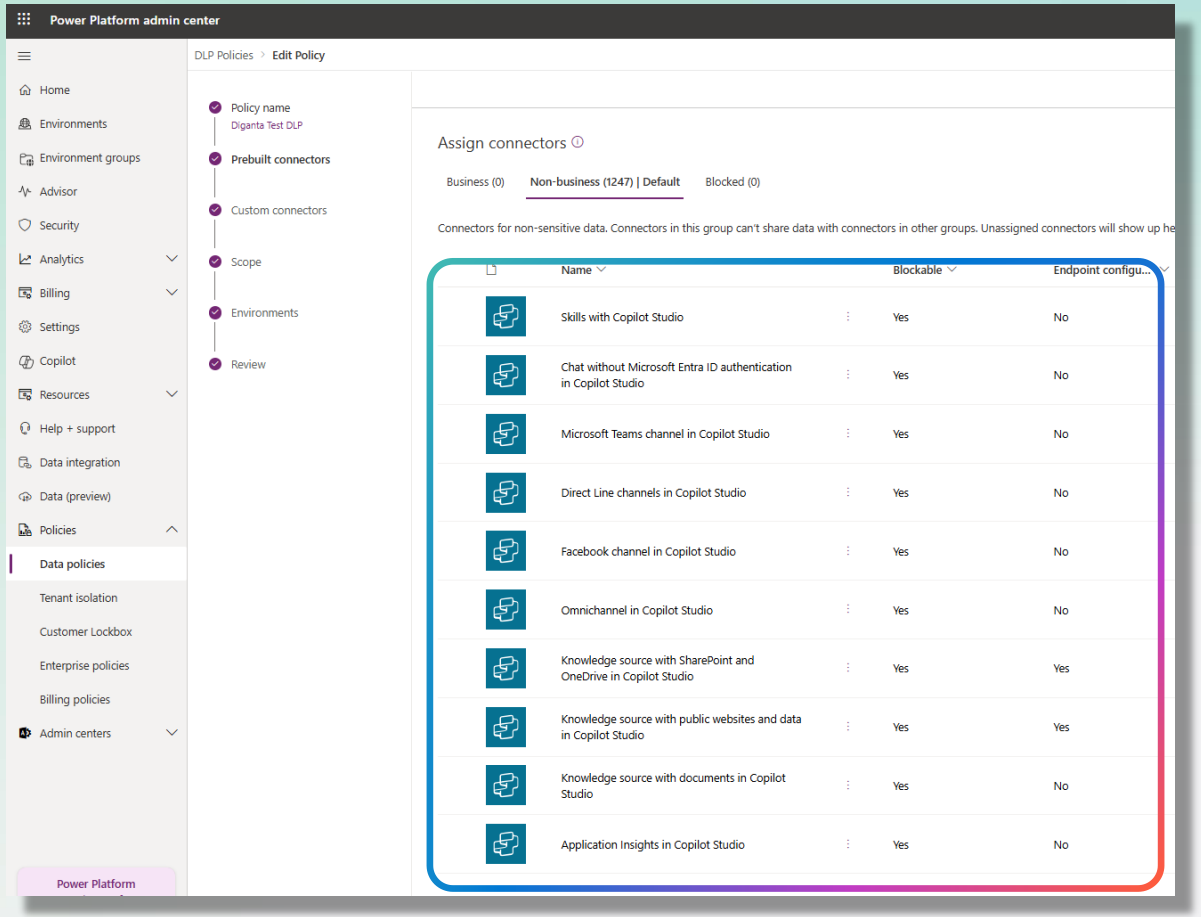
Generally available

Secure copilot by disabling **copilot publish**

Secure copilot by disabling **access from internet** to chat

Govern **copilot knowledges and Actions**

Exempt copilot from DLP while troubleshoot



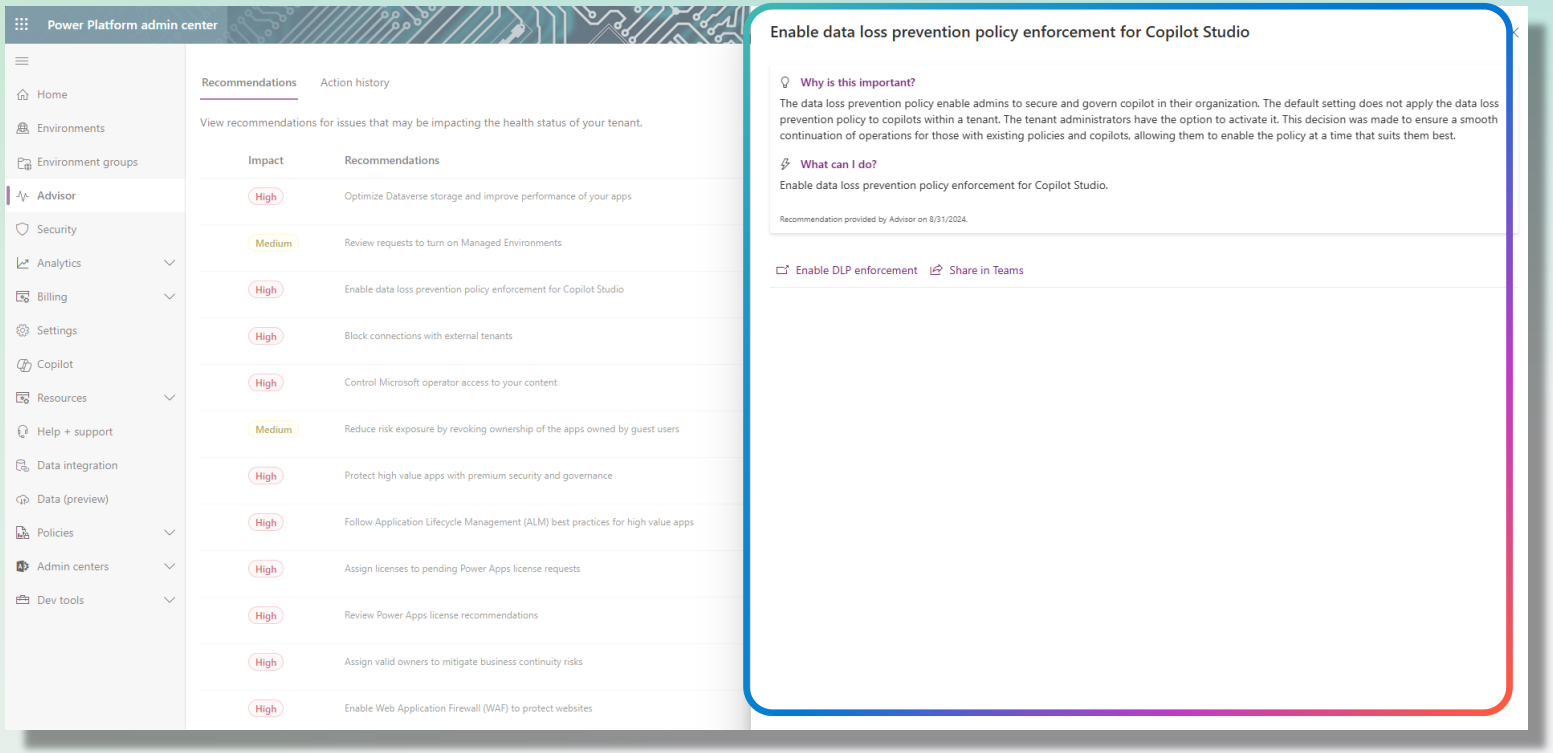
"The DLP capabilities for Copilot Studio are far more robust than what we are used to. The level of detail provided to both the user and the admin are incredibly useful, especially the Excel download. We hope to see this implemented across the board for troubleshooting. Great job!" – **Andrew Gaskins, Lumen**

New

Advisor recommendations for copilots

Generally available

Enforce data loss prevention policy for Microsoft Copilot Studio copilots



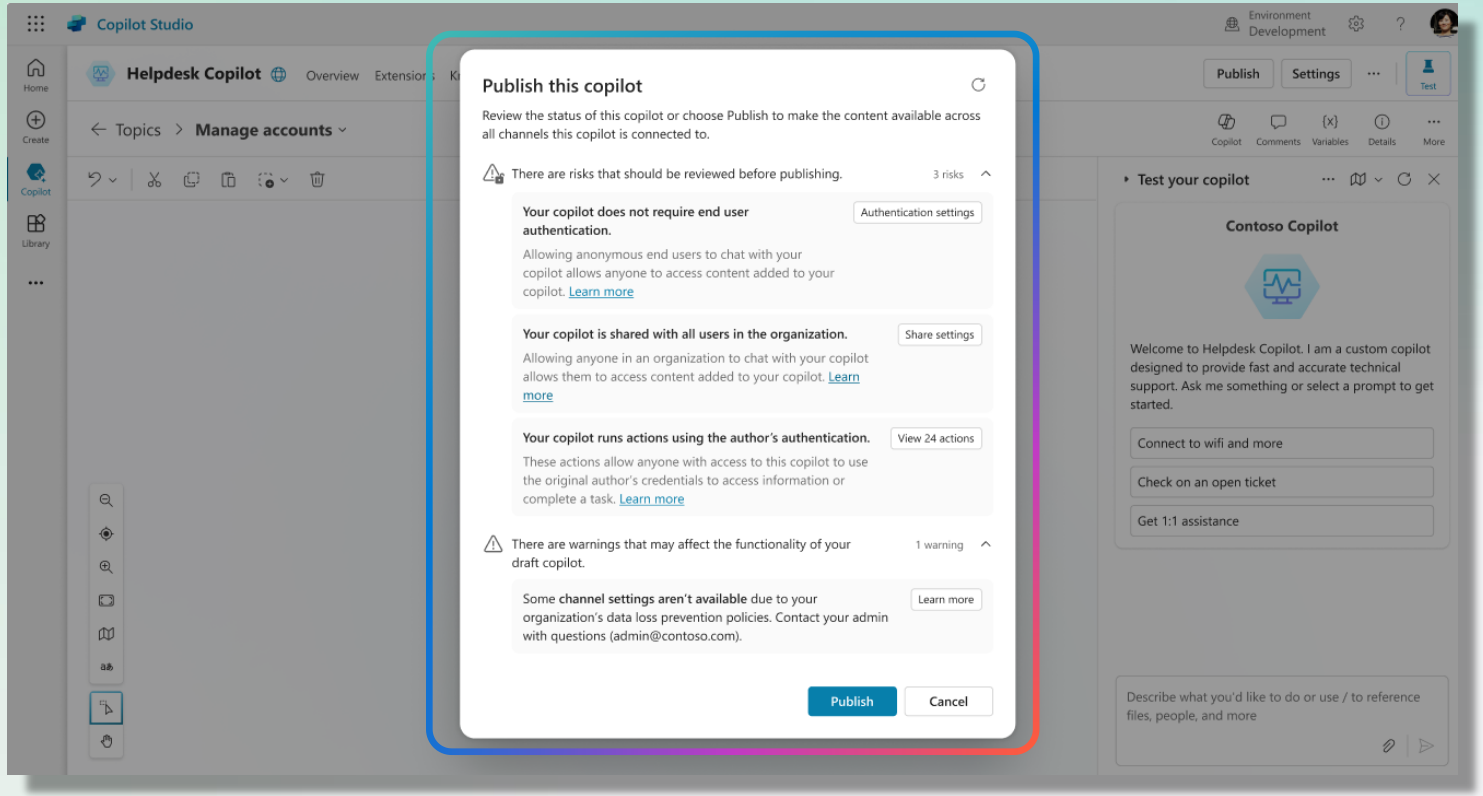
New

Warn makers to Secure copilots

Generally available

Maker can **monitor, protect, & manage** security of copilots

Copilot warn makers when secure by defaults settings are changed and suggest steps to enhance copilot security



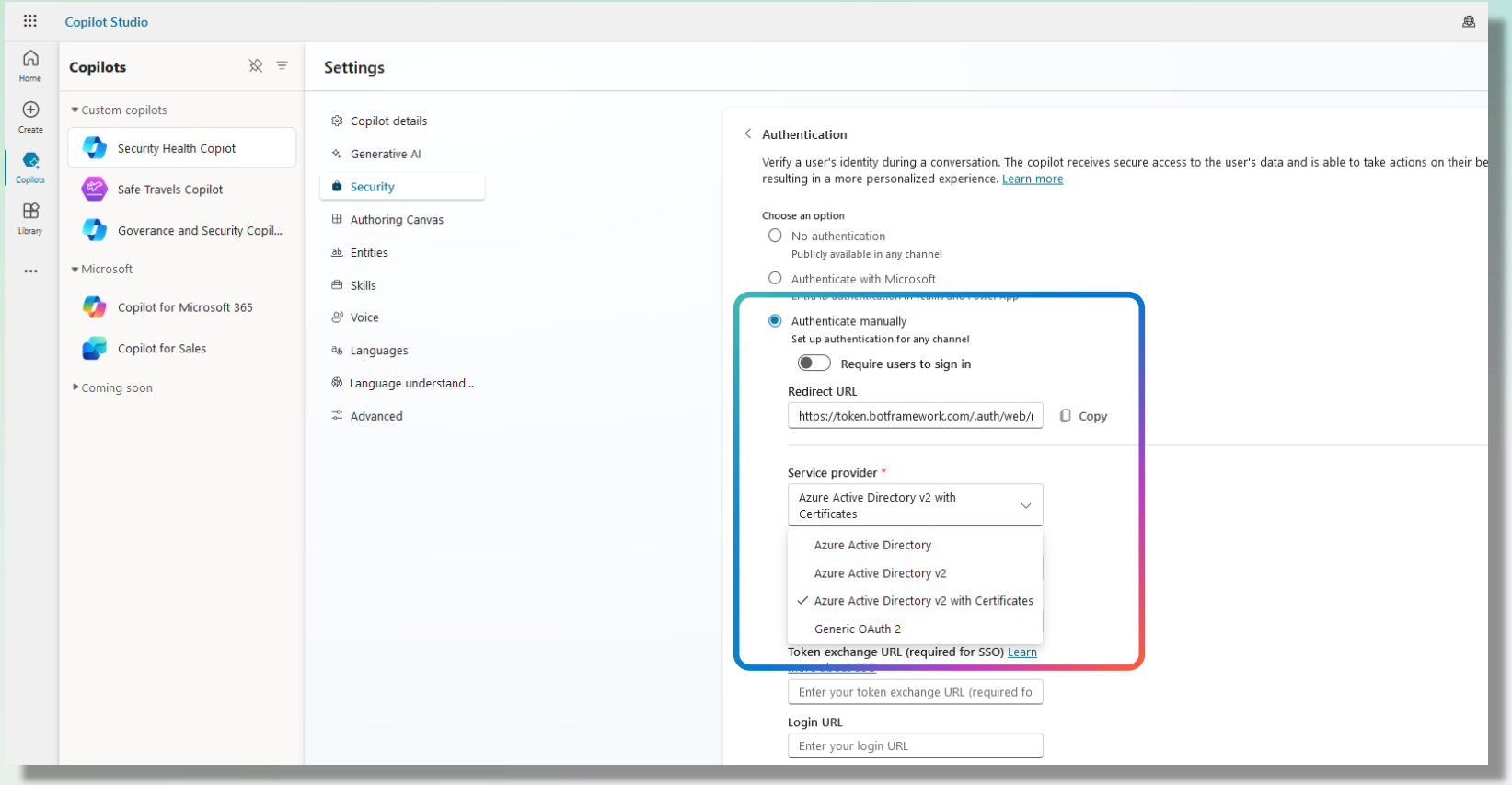
Authentications in copilot

Generally available

Copilot authentication is **secure** by default

Makers can select other **authentication options – Microsoft or Manual**

Admin can disable **no authentication option** for copilot



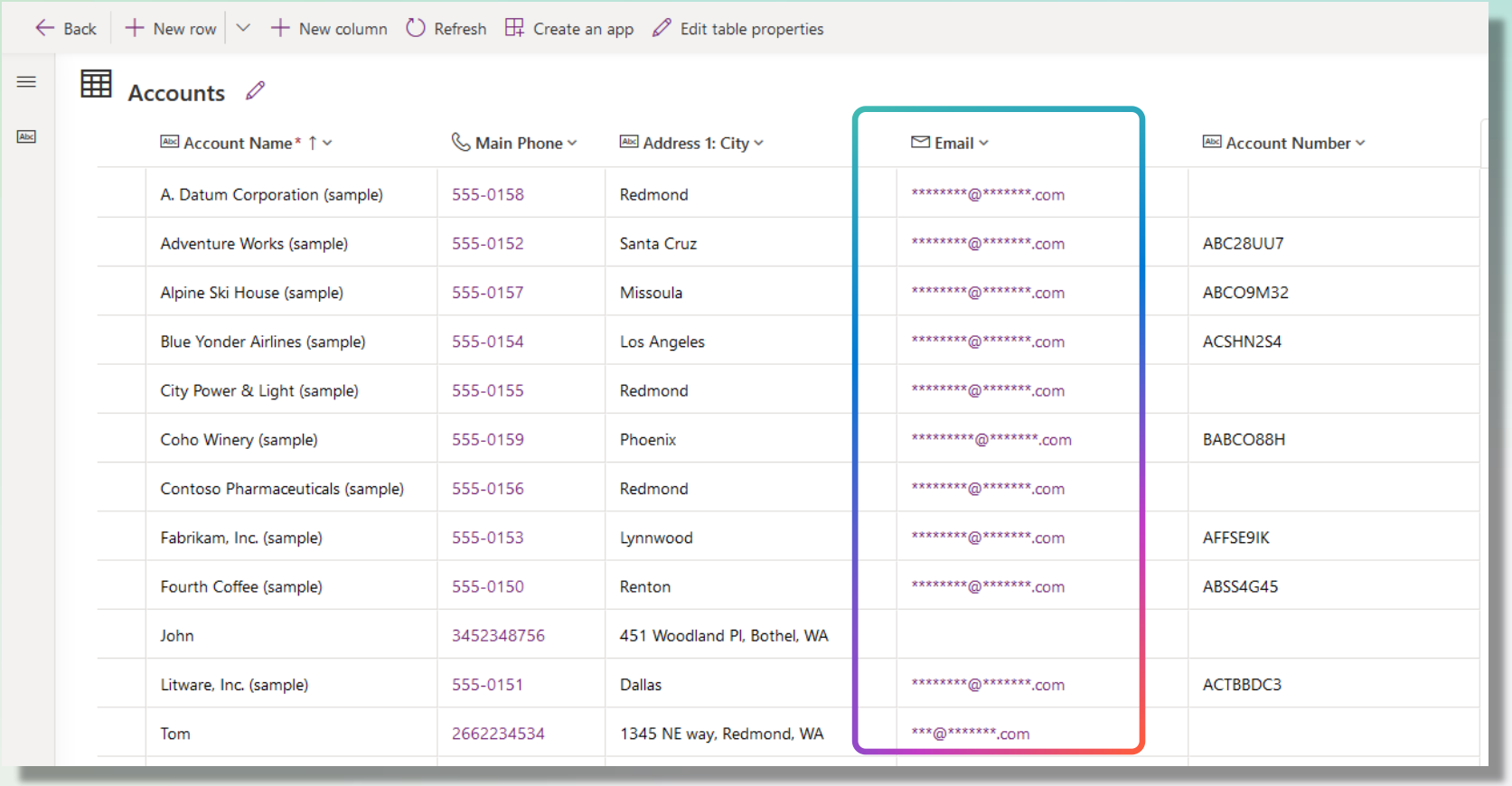
New

Data Mask sensitive copilot data

Public preview

Configure **sensitive data to be masked** when shown to users

Integrated with **column level security and RBAC policies** to secure user access



Microsoft Power Platform

Demo: Ensure data protection

Govern with scale & innovation

- **Environment routing for copilot**
- **Maker welcome message** makers to secure copilots
- **Sharing limits** for copilots
- **Solutions & Pipeline in** Copilot Studio

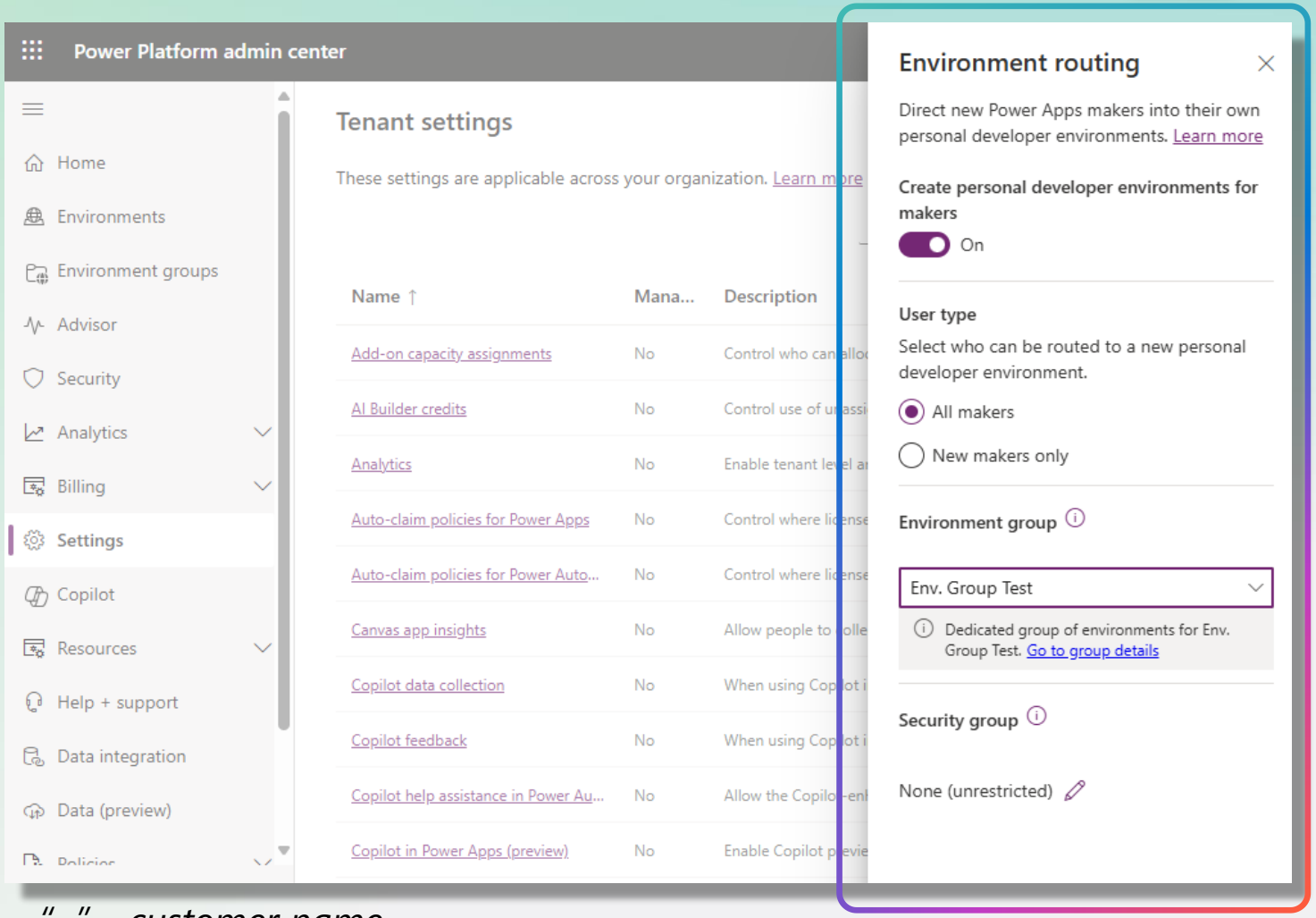
Environment routing for copilot

Generally available

New

Configure environment routing to help scale copilot governance

Maker can **build copilots in personal environments** without the fear of others accessing their copilot



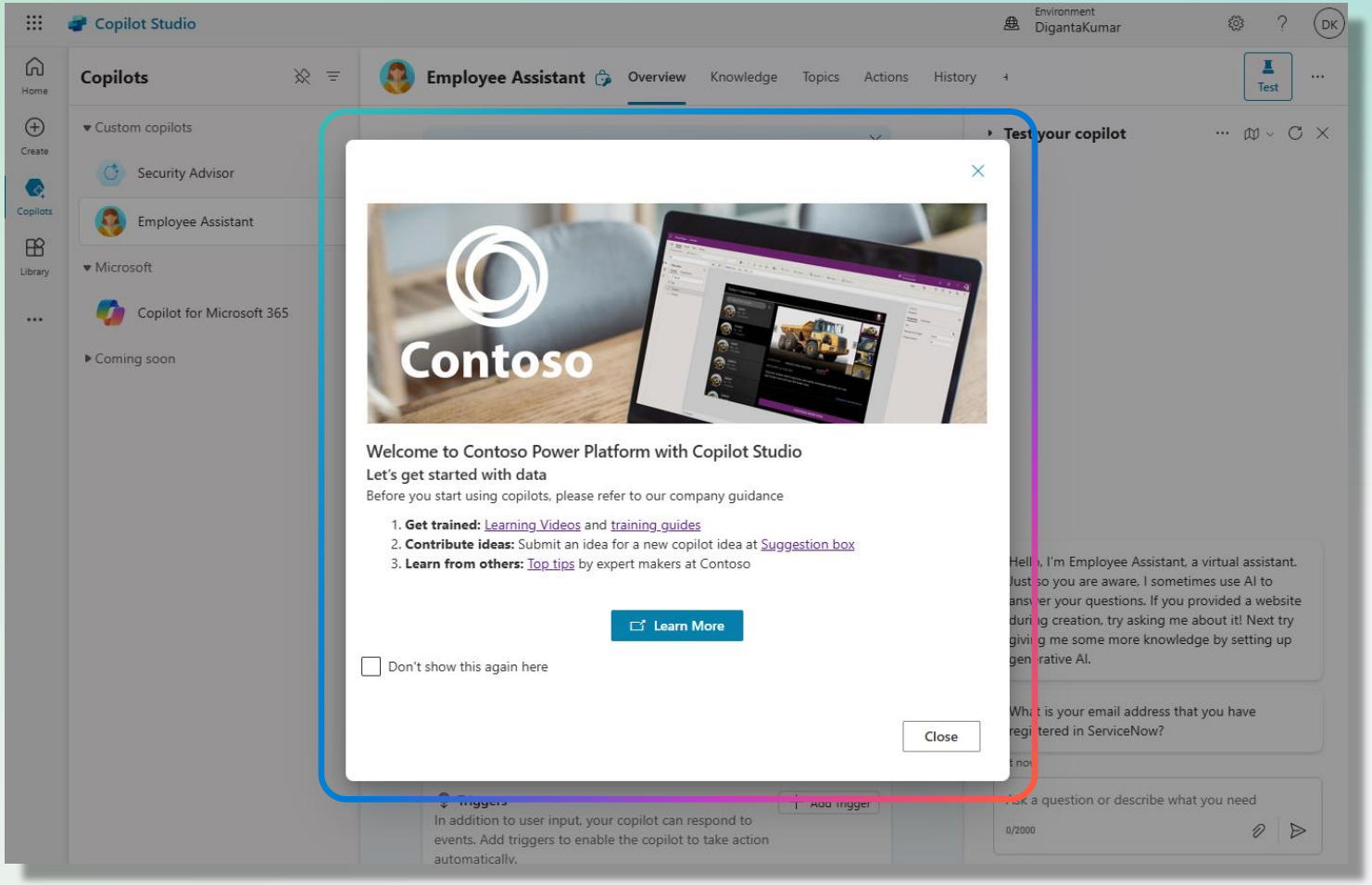
"..." – customer name

New

Maker welcome message for copilots

Generally available

Maker welcome message to inform copilot authors about important privacy and compliance requirements



"..." – customer name

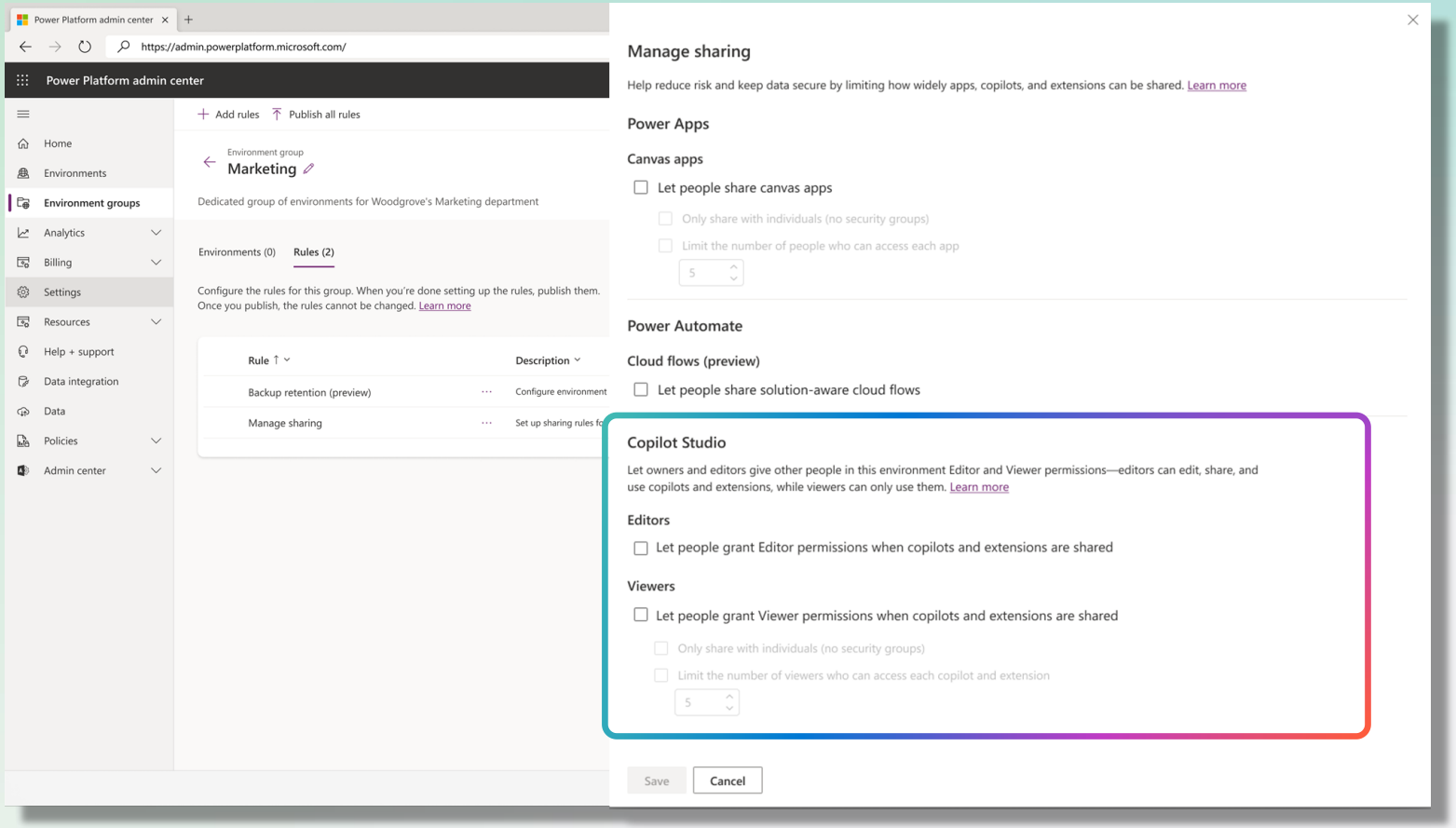
New

Sharing limits for copilot

Private preview

Disable sharing to co-authoring

Limit end users who chats with the copilot using a numeric value or security groups



New

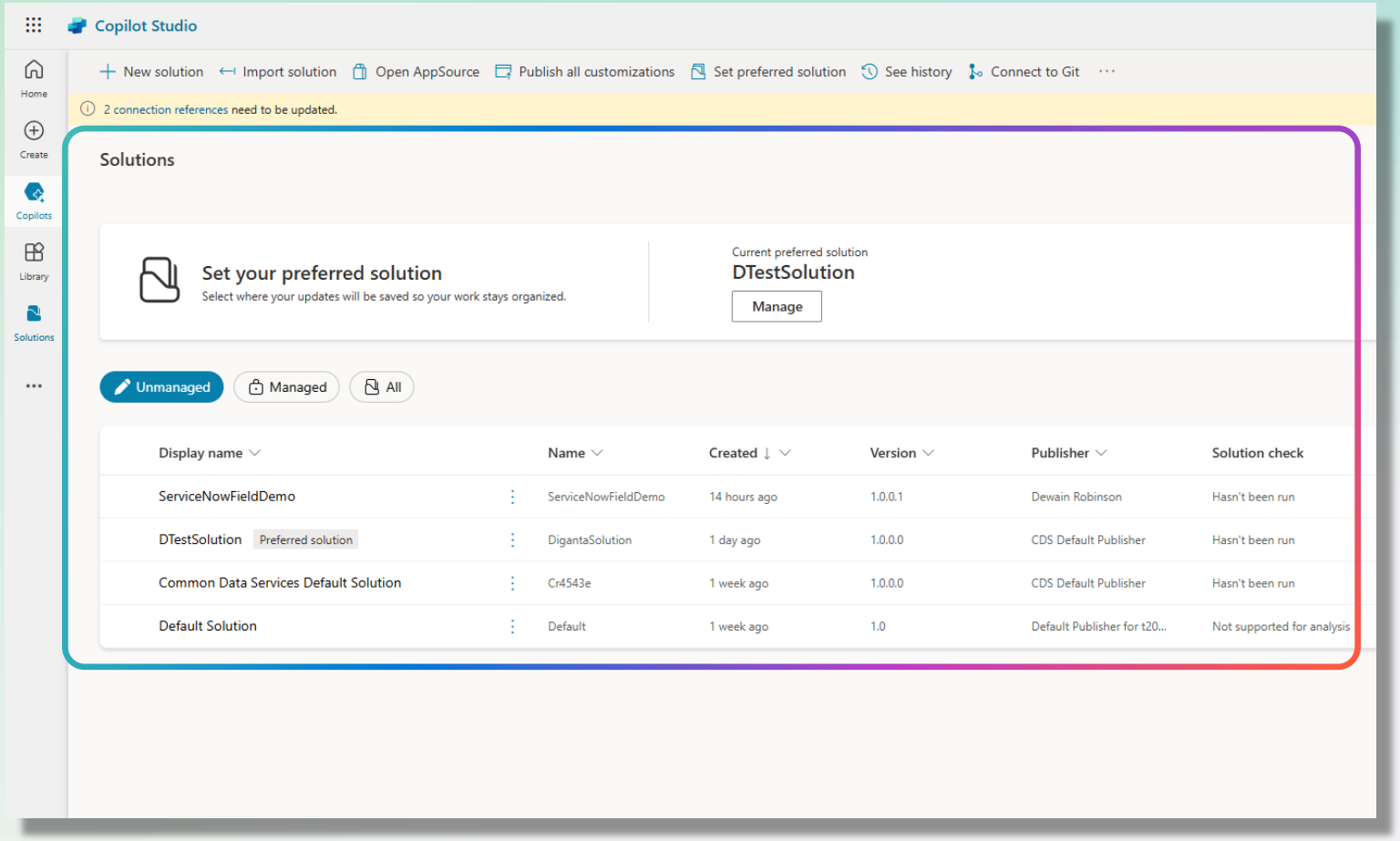
Solutions & Pipelines in copilot

Public preview

Create and manage solutions in Microsoft Copilot Studio

Set preferred solution for copilot solution

Deploy copilot solution using Pipelines from development to production environments



Microsoft Power Platform

Demo: Govern with scale & innovation

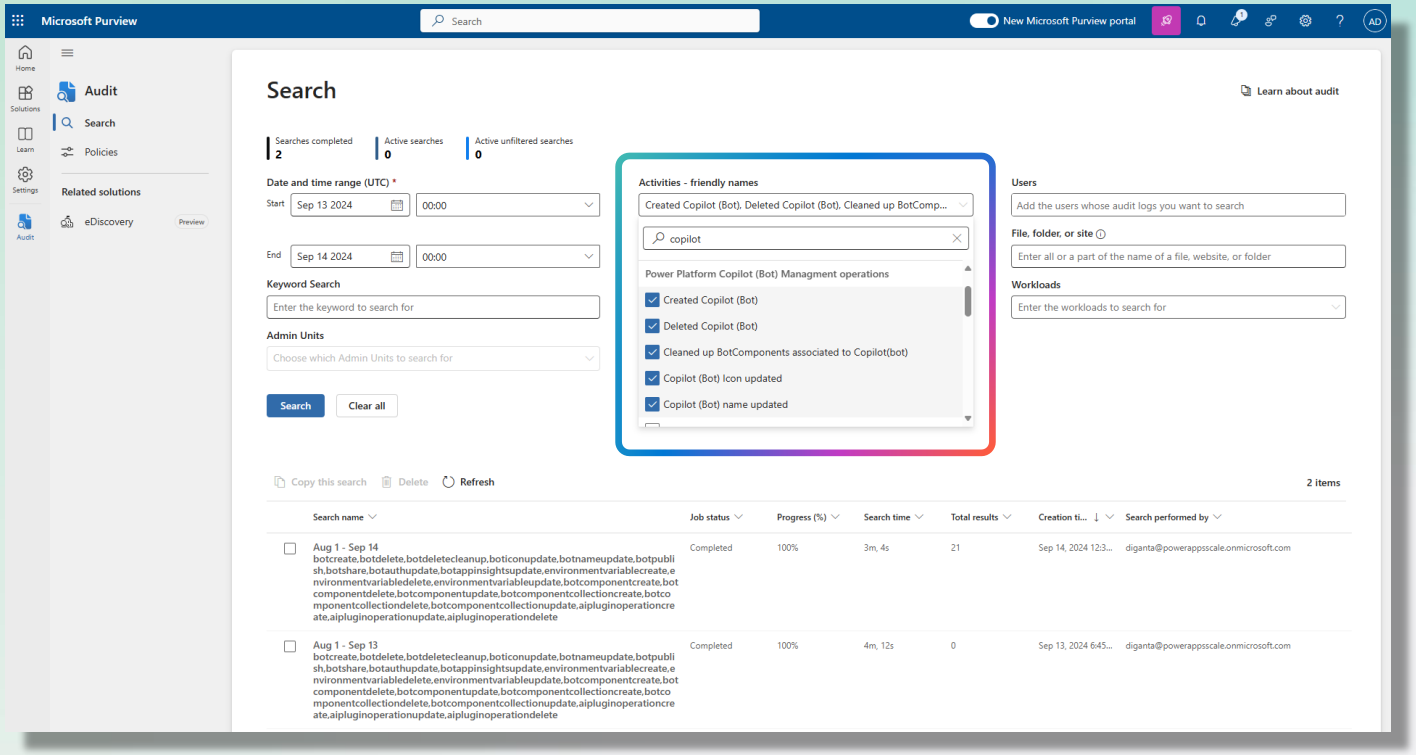
Visibility in user activities and monitoring

- Copilot audit logs in Microsoft Purview
- Copilot audit logs in Microsoft Sentinel

Copilot audit logs in Microsoft Purview

Generally available

Audit log capabilities for admins to respond to security events and compliance obligations.



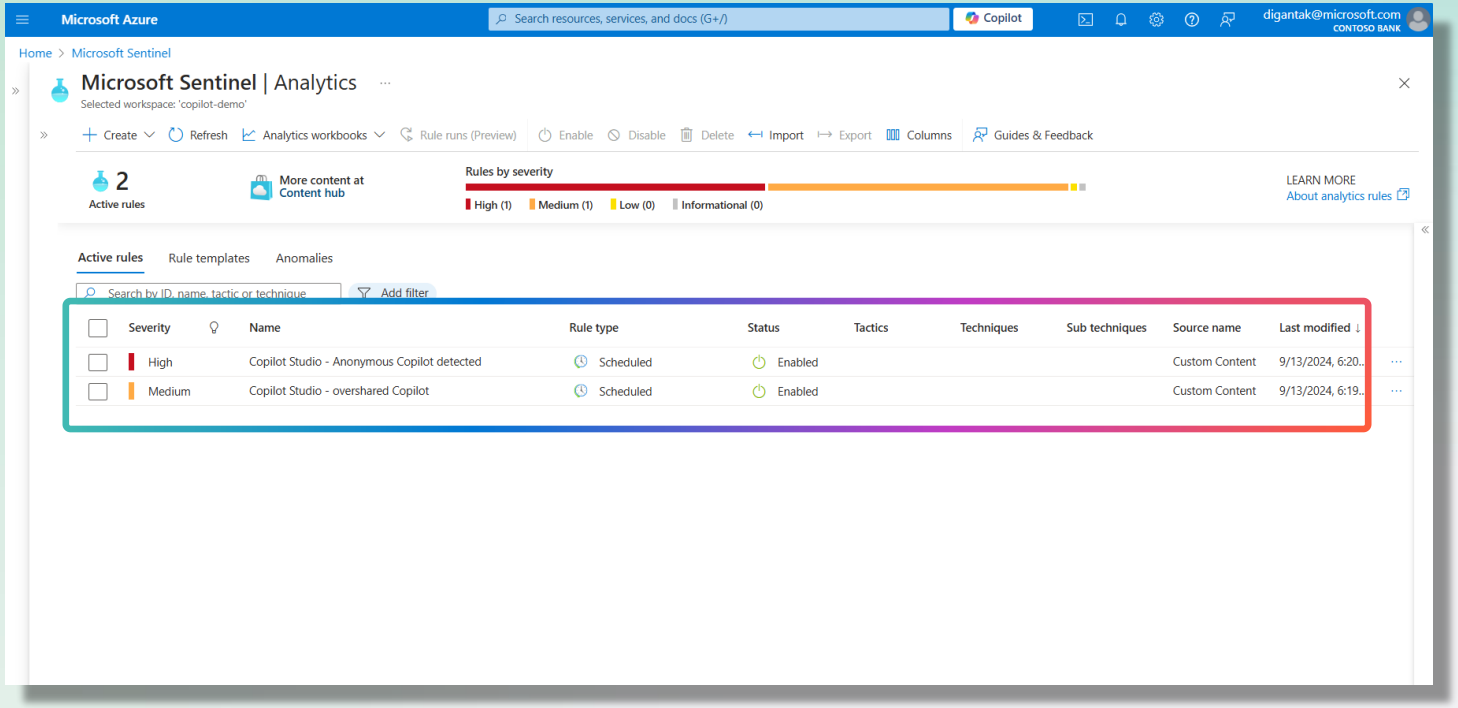
New

Copilot audit log in Microsoft Sentinel

Public preview

Stay ahead of attackers' threats with Sentinel

Detect and alert admins when anonymous copilots are created and oversharing occurs



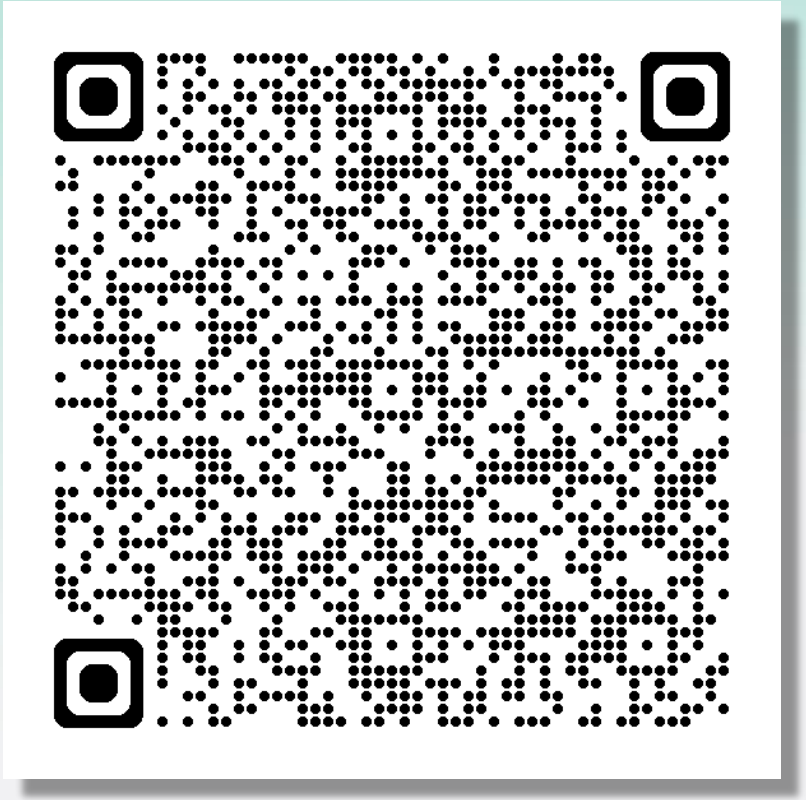
Copilot rules to monitor and detect suspicious or malicious activities

Microsoft Power Platform

Demo: Visibility in user access and activities

Call To Actions

- Try Advisor **recommendations**
- Enable Copilot Studio **DLP** enforcement
- Checkout the **copilot audit logs** in Microsoft Purview
- Set alerts in Microsoft Sentinel with **copilot logs**
- Try **env. routing** & **welcome message** in copilot
- Sign up for **copilot sharing limit preview** (QR code)
- Read **aka.ms/CopilotStudioSecurity** & **aka.ms/MCSgov**



Copilot Studio