roca NETWORKS

Investigating AI Activity with Microsoft Purview Audit

Visibility after the AI interaction happens

SC-200 course recap

Agenda

A simple flow from AI activity to audit evidence.

1. **Investigating AI activity**
2. **From protection to investigation**
3. **What AI activity can be audited**
4. **What an audit record tells us**
5. **Example investigation**
6. **Why this matters and licensing**

Goal: Purview Audit helps answer “what happened?” after AI is used.

Investigating AI Activity with Microsoft Purview Audit

AI security is not only about blocking risky actions. It is also about visibility.

What Purview Audit adds

A searchable record of user, admin, and service activity related to Microsoft 365 and supported AI interactions.

Why AI changes the question

With AI, we may need to know what app was used, who used it, and what files or resources were involved.

Practical outcome

Instead of guessing, IT and security teams can review audit evidence and decide the next step.

From Protection to Investigation

Amr covered protection. This section focuses on investigation after the interaction.

Protect

Sensitivity labels, DLP, policies, and controls help reduce risky AI use before it happens.

Audit

Audit keeps records that help us check user activity, AI interactions, and admin changes.

Investigate

We use the records to answer who, what, when, where, and what resources were involved.

Protection reduces risk; audit gives evidence.

What AI Activity Can Be Audited?

Audit can cover Microsoft Copilot and other AI activity depending on configuration and licensing.

Microsoft Copilot interactions

For example, Copilot activity in Microsoft 365 or Security Copilot.

Custom or connected AI apps

For example, Copilot Studio or AI apps connected to the organization.

Non-Microsoft AI app activity

Can require pay-as-you-go audit logging to be enabled.

Admin changes

Copilot settings, plugins, promptbooks, workspaces, or related configuration.

Important: Audit is visibility. It does not replace DLP or access controls.

What Does an AI Audit Record Tell Us?

The record gives context so the activity can be reviewed instead of guessed.

Who

The user or admin account involved.

When

The date and time of the AI interaction.

Where

The app, workload, or place the interaction happened.

What

The operation type, such as CopilotInteraction.

Resources

Files, sites, emails, or resources referenced by AI.

Evidence

Details that help confirm whether the activity was expected.

Note: Audit records provide investigation context. They may not always include full prompt or response text for every AI scenario.

Why This Matters

AI can make users faster, but security teams still need accountability and evidence.

Accountability

Shows which account performed the activity and when it happened.

Investigation

Helps security and IT teams review suspicious or unusual AI usage.

Compliance

Supports reporting, audit reviews, and internal questions about data use.

Good AI governance needs both prevention and investigation.

Licensing / Key Takeaway

Keep the licensing answer simple and verify against the tenant.

Audit Standard

Included with many Microsoft 365 / Office 365 plans.

Microsoft Copilot audit logs require Copilot to be licensed and used.

Non-Microsoft AI

Some third-party or connected AI app audit logs may require pay-as-you-go features to be enabled.

Audit Premium

Adds longer retention, custom retention policies, and stronger investigation value.

roca NETWORKS

Thank you!

+1 647 476 7680

www.rocanetworks.com