Microsoft Purview Deployment blueprints

What are they?

- Evolution of Deployment Accelerator Guides (DAG)
- Short and prescriptive guidance with high level activity plan
- Scenario focused = more about how customer should use and less about product features list
- Created by Microsoft Engineering (CXE + PM)
- Updated when new features enhances the scenario
- Foundation to white papers, playbooks, articles and detailed guides

Microsoft Security Copilot in Purview

Onboarding

Activities

- Get started with Security Copilot
- Assign roles to users
- Microsoft Purview source in Security Copilot

Outcomes

Get started with Security Copilot

Efforts

1 day

Microsoft Purview portal powered by Copilot

Activities

- Alerts and matches Summarization
- DLP policy insights
- Data hunting with Activity Explorer
- Fortifying Data Security Posture

Outcomes

Accelerate investigation and response

Efforts

1 week

Scale with Automation

Activities

- Automation with Purview Agents
- Use repeatable playbooks and automate your task
- Call into Copilot from a Logic App workflow

Outcomes

Productivity boost by scaling operations horizontally

Efforts

1 week

Use Natural Language to extend investigation

Activities

- Considerations for Copilot prompts
- Cross-solution Hunting
- Copilot Knowledge Base

Outcomes

Gain insights across data security solutions using integrated solution

Efforts

Situational

Onboarding

- Onboard to Security Copilot
- Assign roles to users
- Microsoft Purview source in Security Copilot

Onboard to Security Copilot

- Onboarding to Security Copilot is a two-step process:
  (1) Provision capacity
  (2) Set up default environment

For more information, see Get started with Microsoft Security Copilot

Assign roles to users

- After Security Copilot is onboarded for your organization, configure Security Copilot RBAC to determine users' access to the Security Copilot platform. Then layer your security coverage with conditional access policies.

For more information, see, Get started with Microsoft Security Copilot Create and deploy a data loss prevention policy | Microsoft Learn Get started with insider risk management | Microsoft Learn Get started with communication compliance | Microsoft Learn and Assign permissions in eDiscovery | Microsoft Learn

Microsoft Purview source in Security Copilot

- Copilot in Purview is enabled by default. Copilot in Purview must be enabled for both the standalone and embedded experiences to work.
- To enable or disable sources (plugins) in Security Copilot, follow Security Copilot in Microsoft Purview
- M365 data sharing: Privacy and data security in Microsoft Security Copilot | Microsoft Learn

Microsoft Purview portal powered by Copilot

- Alerts and matches summarization
- DLP policy insights
- Data hunting with Activity Explorer
- Fortifying data security posture

DLP alerts summarization and policy insights

- The DLP alert summary can identify and prevent data risks with a comprehensive overview of an alert (i.e. policy rules, source, files involved).
- Enhanced hunting prompts allow for a deeper dive into DLP alert summaries providing detailed exploration of data and users involved in incidents. This includes actions taken on the data and the specific sensitive information type (SIT) that triggered the alert.
- The embedded Security Copilot-powered policy insights skill summarizes the intent, scope, and resulting matches of existing DLP policies in natural language. This helps admins quickly identify and address gaps in protection.

For more information, see Security Copilot in Microsoft Purview

IRM alerts summarization

- Copilot offers valuable insights, enabling users to quickly access, summarize, and act upon Insider Risk Management information. Users can instantly generate a comprehensive and concise summary of the alert to focus on critical investigation path.
- Leverage suggested prompts to delve deeper into specific activities. For more information, see Investigate insider risk management activities

Communication Compliance message summarization

- You can use Copilot in Communication Compliance to provide a contextual summary of a Teams, email, or Viva Engage message included in a policy match. The summary provided is in the context of one or more trainable classifiers that flag the message. For more information, see Investigate and remediate communication compliance alerts

Microsoft Purview portal powered by Copilot

- Alerts and matches summarization
- DLP policy insights
- Data hunting with Activity Explorer
- Fortifying data security posture

eDiscovery summarization

- The eDiscovery quick case summarization designed to streamline case management by providing an intuitive at-a-glance overview. It allows users to quickly access a comprehensive summary of eDiscovery cases, holds, and searches.

- The contextual summary provided is in the context of text included in a selected item. This summary can save time for reviewers by quickly identifying information helpful when tagging or exporting items. Copilot summarizes the entire item, including any documents, meetings transcripts, or attachments. For more information, see Group and view documents in a review set in eDiscovery (Premium

- The Natural Language Query KeyQL builder option in search allows you to use natural language and Microsoft Security Copilot to quickly generate a Keyword Query Language (KeyQL) statement. You can also choose to use prompt suggestions as a starting point to create and refine KeyQL queries for common or custom search scenarios. For more information, see Create a search query for a case in eDiscovery

Microsoft Purview portal powered by Copilot

- Alerts and matches summarization
- DLP policy insights
- Data hunting with Activity Explorer
- Fortifying data security posture

DLP policy insights

- This enhancement helps DLP admins understand the policies construct and where they're active. DLP admins can get these insights on all the policies or on few selected policies. They will be able to use prompts to gain deeper level view of how a policy is configured for their digital landscape. This helps admins align their data posture on a regular basis and make corrections to policy posture as needed.

For more information, see Test your DLP policies

Data hunting with Activity Explorer

- Activity Explorer prompt help admins efficiently drill down into Activity data to identify activities, files with sensitive information, and additional details that are relevant to an investigation.

For more information, see Get started with Activity explorer

Microsoft Purview portal powered by Copilot

- Alerts and matches summarization
- DLP policy insights
- Data hunting with Activity Explorer
- Fortifying data security posture

Fortifying data security posture

- Microsoft Purview Data Security Posture Management (DSPM) allows you to quickly and easily monitor cross-cloud data and user risk through dynamic reports and trend analysis.
- By processing and correlating across other Microsoft Purview data security and risk and compliance solutions, DSPM helps you identify vulnerabilities with unprotected data and quickly take action to help you improve your data security posture and minimize risk.
- Data security insights are generated from scanned data across DLP, IRM, and Microsoft Purview Information Protection solutions.
- Use Security Copilot to quickly dive into the details and get answers about unprotected sensitive data assets and potentially risky user activities in your organization.
- Suggested prompt responses automatically scope insight data and provide quick answers in a separate flyout pane. You can select additional built-in prompts to automatically update and generate new responses in the flyout pane. Create custom prompts directly in Copilot to generate responses from AI-driven analytics based the scanning results from your organization.

For more information, see Use Microsoft Security Copilot with Data Security Posture Management

Scale with Automation

- Automation with Purview Agents
- Use repeatable playbooks and automate your task
- Call into Copilot from a Logic App workflow

Automation with Purview Agents

- Microsoft Purview's Security Copilot Agents are AI-powered assistants that automatically triage Data Loss Prevention (DLP) and Insider Risk Management alerts, identifying those that pose the greatest risk so your security team can address them first.
- These agents streamline data security operations by sorting alerts into priority categories (like "Needs attention" for critical issues versus "Less urgent"), enabling faster response times and allowing analysts to focus on truly high-risk incidents.
- Microsoft Purview agents continuously learn and adapt based on administrator feedback (provided in natural language) to fine-tune their alert prioritization logic, ensuring the system aligns with your organization's evolving data security priorities over time.
- For more information, see Get started with the Microsoft Purview Agents | Microsoft Learn

Scale with Automation

- Automation with Purview Agents
- Use repeatable playbooks and automate your task
- Call into Copilot from a Logic App workflow

Use repeatable playbooks and automate your task

- Leverage the prebuilt promptbooks, serve as ready-to-use workflows templates to automate repetitive tasks. For more information, see Using promptbooks.
- Utilize the prebuilt promptbooks in Microsoft Purview's Data Security Posture Management (DSPM) Copilot to automate repetitive security tasks. These promptbooks act as ready-to-use workflow templates that streamline investigations such as identifying risky users or sensitive data exposure using natural language. For more information, see Use Microsoft Security Copilot with Data Security Posture Management | Microsoft Learn.
- Create your own promptbook to automate investigation flows and optimize repetitive tasks that customized to your needs and requirements. For more information, see Build your own promptbooks

Call into Copilot from a Logic Apps workflow

- Logic Apps connector enables seamless integration between your Logic Apps workflows and Security Copilot. The connector exposes two actions: submit a Copilot prompt and submit a promptbook. For more information, see Logic Apps connectors

Use Natural Language to extend investigation

- Considerations for Copilot prompts
- Cross-solution Hunting
- Copilot Knowdge Base

Considerations for Copilot prompts

- Prompts are the primary input Security Copilot needs to generate answers that can help you in your security-related tasks.
- Promptbooks are a series of prompts that have been put together to accomplish specific security-related tasks.
- The prompts and promptbooks library in Security Copilot helps you quickly harness the power of the platform in a way that aligns with your role. These set of prompts and promptbooks are designed to guide you through features and capabilities most relevant to your work.
- Effective prompts give Security Copilot adequate and useful parameters to generate a valuable response. Consider the following elements when writing a prompt:
  - **Goal** - specific, security-related information that you need
  - **Context** - why you need this information or how you plan to use it
  - **Expectations** - format or target audience you want the response tailored to
  - **Source** - known information, data sources, or plugins Security Copilot should use

For more information, see Prompting in Microsoft Security Copilot

Use Natural Language to extend investigation

- Considerations for Copilot prompts
- Cross-solution Hunting
- Copilot Knowdge Base

Cross solution hunting

- Leverage cross solution promptbooks such as 'Identity compromise and DLP investigation-3P' to investigate potential data loss and identity compromise incidents. For more information, see: Cybersixgill is a Proud Participant in the Microsoft Copilot for Security Partner Ecosystem

Copilot Knowledge Base

- Access AI-powered insights directly within Microsoft Purview through the embedded Copilot experience. It enables users to summarize product documentation and alerts, investigate data risks using natural language prompts, understand policy behavior and sensitive data exposure, and review alerts from DLP, Insider Risk, and Communication Compliance from a single, integrated interface. For more information, see: https://learn.microsoft.com/en-us/purview/copilot-in-purview-overview#key-features-in-the-embedded-experience