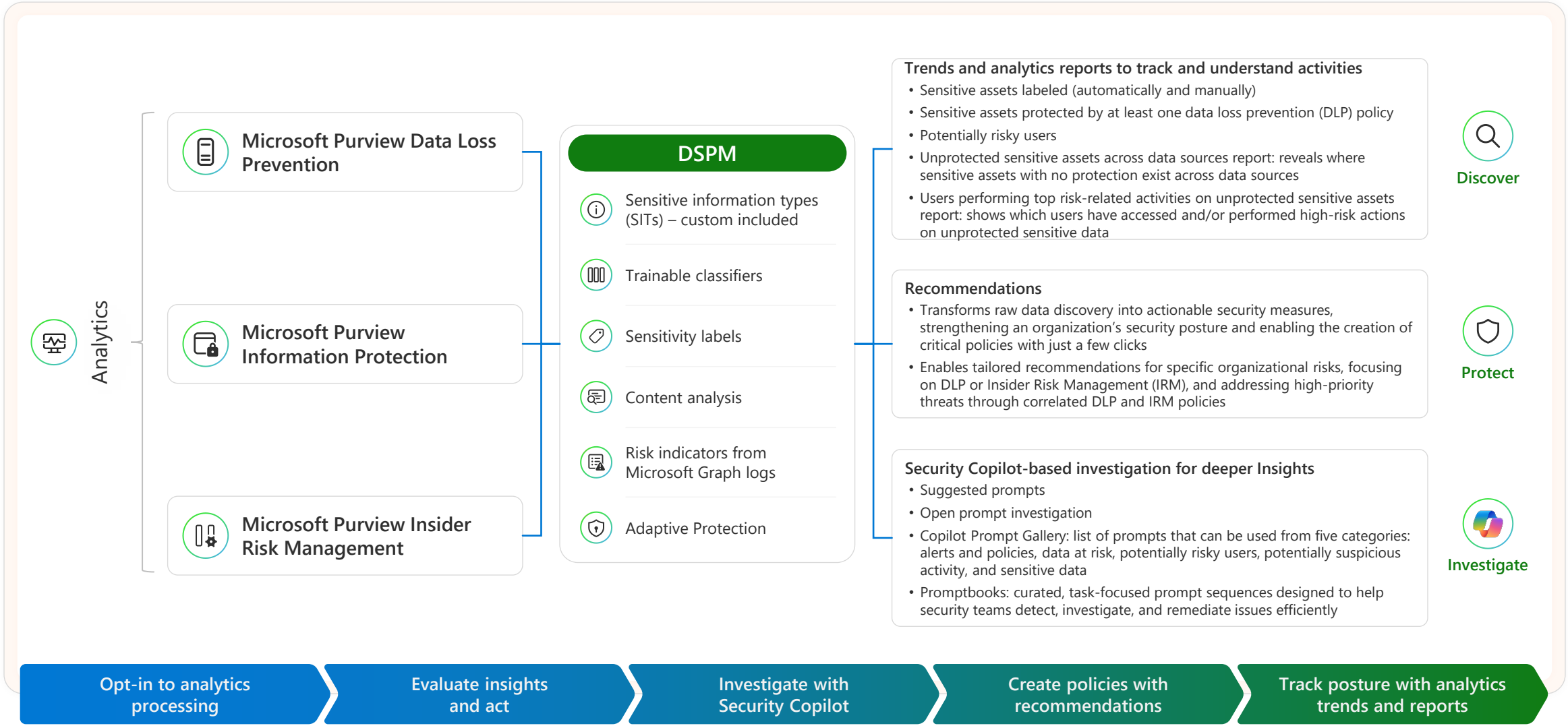
Microsoft Purview Data Security Posture Management (DSPM)



Deploy and Use Data Security Posture Management (DSPM)

Assumptions

Recommended foundational elements

Activities

- Out-of-box and custom SITs for organization identified
- Labeling schema is configured
- Insider Risk Management (IRM) program defined
- Security Copilot is enabled (optional)

Outcomes

Full data estate is understood and accessible

Efforts

0 to 7 days
+ 3 weeks (if no data security)

Integrations

Initial access and configuration

Activities

- Assign a role with least privilege
- Enable Data Loss Prevention (DLP) analytics
- Enable Insider Risk Management analytics
- Initial scan will automatically start

Outcomes

DSPM starts pulling insights

Efforts

3 days

Insights

Understand data landscape and risks

Activities

- Leverage DSPM reports and trends to get details on both unprotected and protected sensitive assets, and potentially risky user activities
- Review DSPM recommendations to understand current risk and determine next steps every 30 days

Outcomes

Assess risks and strengthen overall data security posture

Efforts

Monthly iteration

Maintenance

Take action and investigate with Copilot

Activities

- Create DLP/IRM policies based on recommendations
- Investigate users with Security Copilot in recommendations
- Promptbooks and Copilot Prompt Gallery to handle sensitive data and investigate risky users

Outcomes

Take actions to secure the environment and gain key understandings

Efforts

Ongoing

Last updated: October 9th, 2025

Assumptions

Recommended foundational elements

- Out-of-box and custom SITs for organization identified
- Labeling schema is configured
- Insider Risk Management program defined
- Security Copilot is enabled (optional)

Out-of-box and custom SITs for organization identified

- This ensures that when reviewing recommendations and doing any form of analysis, the admin is aware of what needs to be prioritized
- Good starting point for organizational requirements and can be improved after investigation

Labeling schema is configured

- Not required but extremely helpful in identifying how files should be handled and in setting up DLP policies later
- Helps improve recommendations and gives better insights on DSPM reports

Insider Risk Management program defined

- Enables organizations to proactively address insider threats, ensuring compliance with regulations
- With DLP and Adaptive Protection, DSPM has a stronger landscape

Security Copilot is enabled (optional)

- Enables custom investigations, usage of the DSPM Promptbooks, and ease in understanding AI's role in making investigations more efficient.

Integrations

Initial access and configuration

- Assign a role with least privilege
- Enable Data Loss Prevention analytics
- Enable Insider Risk Management analytics
- Initial scan will automatically start

Assign a role with least privilege

- Assign to one of the following roles or role groups:
  - Data Security Management role group
  - Data Security Viewer role (**required to use Security Copilot in DSPM)**
  - Insider Risk Management Admins role
  - Microsoft Entra ID Global Administrator role
  - Microsoft Entra Compliance Administrator role
- It is advisable to use roles with the fewest permissions, reducing the number of users with the Global Administrator role enhances security for an organization.

Enable Data Loss Prevention and Insider Risk Management analytics

- Processes and correlates data states, signals, and user activities based on the configuration of other data security and compliance solutions (Purview)
- Two ways to enable: Opt-in to DSPM or, enabled individually for both DLP and IRM

Initial scan will automatically start

- DSPM simplifies initial setup and policy creation for data security, risk, and compliance by initiating once the analytics are turned on
- Scans your organization's data and activities, offering baseline insights and recommendations that are helpful whether you're working with a new or existing Purview environment
- Initial scan can take up to 3 days to complete

Insights

Understand data landscape and risks

- Leverage DSPM reports and trends to get details on both unprotected and protected sensitive assets, and potentially risky user activities
- Review DSPM recommendations to understand current risk and determine next steps every 30 days

Reports

- Each of the reports have options to help with filtering, reviewing, evaluating, and exporting DSPM insights
- Analytics reports go into two main areas of focus, Unprotected sensitive assets across data sources and Users performing top risk-related activities on unprotected sensitive assets.
  - The Unprotected sensitive assets across data sources report is similar to content explorer but covers the entire data estate giving insights on what isn't protected by DLP and/or what is not labeled with access control
    - Shows the location of the files and their associated classifiers
  - The Users performing top risk-related activities on unprotected sensitive assets report is associated with IRM and flags based on IRM identifiers such as (not limited to) departing users and high-risk users.
    - Also includes activities based on classifiers not included in DLP

Trends

- These are on the Overview page and highlight history based on recent activity around the sensitive data and users
  - Sensitive assets labeled (automatically + manually): percentage of assets per week that had sensitivity labels applied
  - Sensitive assets protected by at least one DLP policy: percentage of sensitive assets in your organization with a classifier (or more) being protected one DLP policy (or more)
  - Potentially risky users: number of users per week who were assigned insider risk severity levels (low, medium, high)

Recommendations

- Generated from the processed data, current state of unprotected sensitive assets, and user activities that put these assets at risk
- Enables organizations to act fast by creating DLP and IRM policies (mitigate data security risks) and identifies gaps in existing DLP and IRM policies
- Automatically updates including when any recommendations older than 30 days are removed

Maintenance

Take action and investigate with Copilot

- Create DLP/IRM policies based on recommendations
- Investigate users with Security Copilot in recommendations
- Promptbooks and Copilot Prompt Gallery to handle sensitive data and investigate

Create DLP/IRM policies based on recommendations

- Ability to create one or more DLP policies and/or IRM policies after clicking into the recommendation
  - These help mitigate risk identified in the recommendation
  - Provides step-by-step guidance that can be used to create the policy without leaving the DSPM page (customizable)
  - Takes a few minutes for each policy to be created and about 24 hours for triggering event to happen (policies can be found in each solution's page)
  - Additional recommendations may be generated for this type of activity that can help with policy updates and tuning based on initial creation
- Admins can use guidance to update existing policies instead of creating new policies; recommendations will be updated accordingly following admin actions

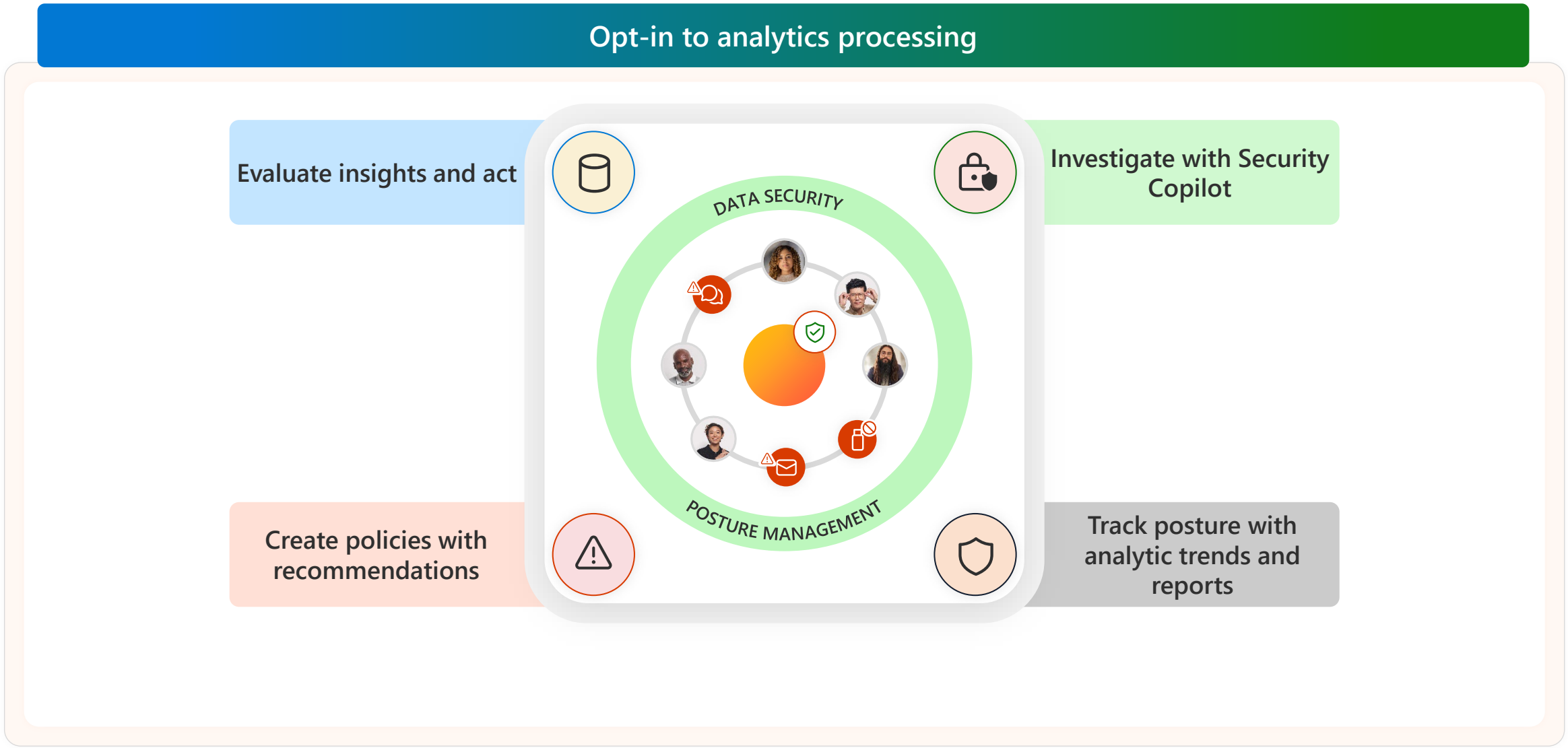
Investigate users with Security Copilot in recommendations

- Use the Show Users Involved button within the initial recommendation to start an interaction with Security Copilot to get more details
- Follow-up prompting will allow for a deep dive into the activity surrounding the recommendation and take the admin into the AI interaction-based event/action hunting
- Open Security Copilot from the top of the DSPM page to investigate any action or user
  - Examples: provide a list of events where sensitive files were shared externally (or to _____ domain) or List all the sensitive files that were uploaded to cloud in the last week

Promptbooks and Copilot Prompt Gallery to handle sensitive data and investigate risky users

- These sets of prompts help to get admins started on overall investigations or find deeper insights by giving examples of prompts to use to dive deep into DSPM
  - Risky user investigation: this promptbook has a 6-prompt sequence designed to aid in identifying users handling sensitive data, show their data activities, anomalies, and related alerts (input a UPN and timeframe of days with a max of 30 days)
  - Sensitive data protection: a 6-prompt sequence to identify and protect sensitive data across the organization and that suggests recommended policy changes and data loss prevention rules (input SIT or label, and duration with max of 30 days)
- Copilot Prompt Gallery now includes sample prompts to aid in investigations

DSPM, Simplified Visual



Acronyms

Acronym	Definition
OOB	Out-of-Box
IRM	Insider Risk Management
DLP	Data Loss Prevention
DSPM	Data Security Posture Management
AI	Artificial Intelligence
SITs	Sensitive Information Types
DS	Data Security