Microsoft Security

# Securing your data with Microsoft Purview: a practical handbook

**Get started with a dynamic approach to securing data, emphasizing the integration of people, processes, and technology in alignment with Microsoft's best practices**

**This resource is designed for security leaders who seek to enhance their company's data security through a holistic approach based on the best practices derived from the extensive experience of Microsoft experts and insights from customers.**

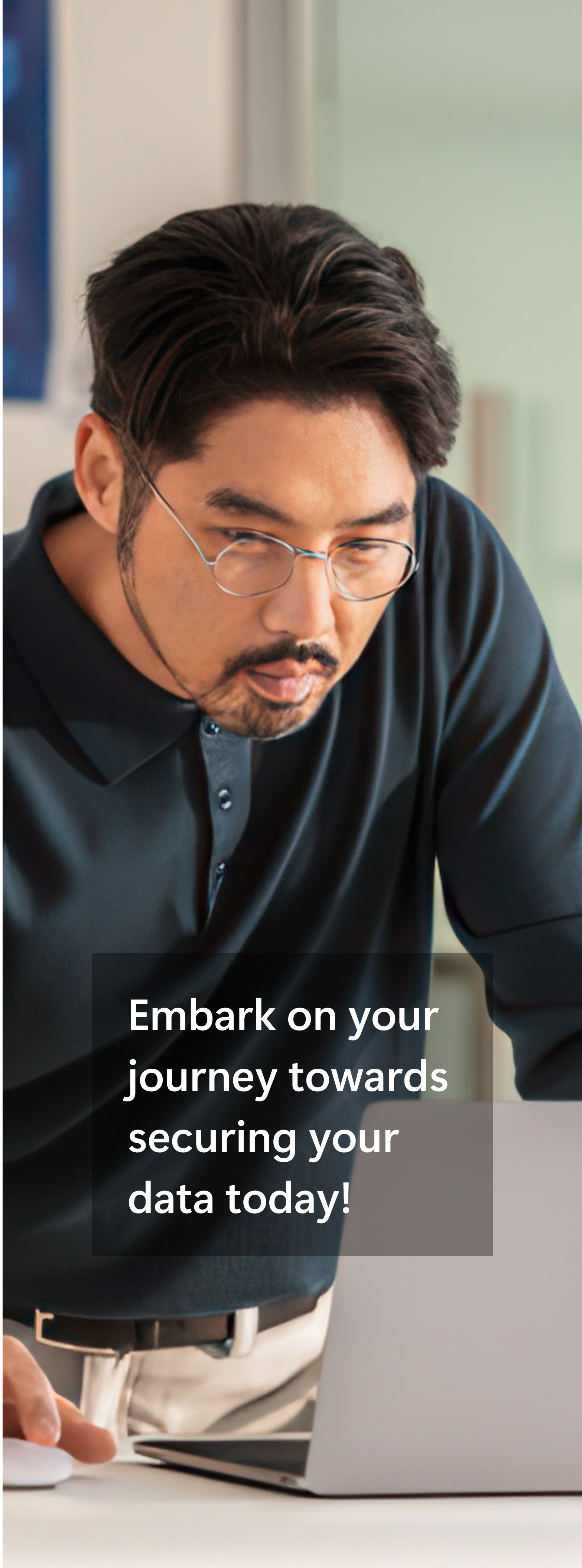
This handbook emphasizes the critical elements amongst people, process, and technology that will empower you to protect your organization's most valuable data assets. You'll be able to understand how to integrate data and user context across your cloud applications, services, devices, and generative AI tools.

First, you will explore best practices at Microsoft for preparing to secure your data, including:

- Identifying your data security requirements
- Formulating a robust strategy
- Engaging cross-functional stakeholders
- Determining your organization's risk tolerance
- Implementing security controls
- Committing to continuous improvement

The subsequent sections of the handbook outline our recommended approach to implementing Microsoft Purview, encompassing:

- Assessing your data environment
- Understanding and preparing your data
- Fine-tuning and revisiting your policies
- Enhancing data security scenarios and set up Adaptive Protection



Embark on your journey towards securing your data today!

# Contents

# Introduction

Data security challenges are unique to each organization, shaped by factors such as regulatory requirements, data volumes, and the complexity of different IT environments. Whether you're embarking on your data security journey, moving from a previous solution, or enhancing an established program, building a robust and adaptable strategy is essential to protect sensitive information effectively.

In this context, data security involves not only safeguarding information but also understanding where data resides, classifying it accurately, and understanding user activities to ensure responsible access and usage. It's about creating a framework that manages and governs data holistically, so organizations can confidently meet compliance standards, maintain user trust, and mitigate risks.

Learn more about data security and risks your data might be vulnerable to.

This guide represents the expertise at Microsoft, developed through years of working closely with customers to navigate these challenges and optimize their data security practices. Drawing from real-world insights, this guide will take you step-by-step through maximizing the data security capabilities of Microsoft Purview—from the early planning stages to continuous improvement and sustained operational excellence.

**By reading this guide, you'll learn how to:**

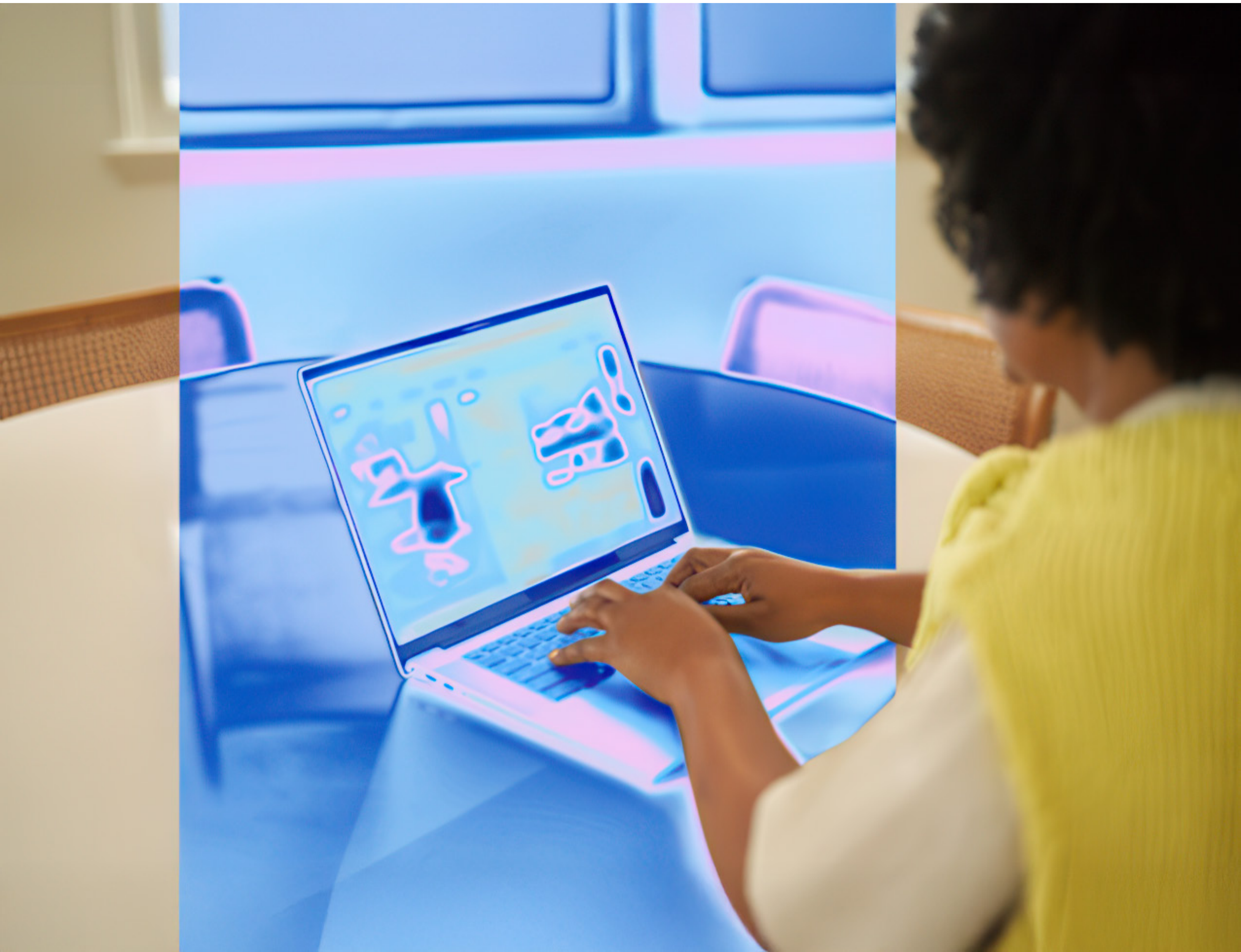
- Start small and build momentum with your implementation.
- Design a cross-functional stakeholder engagement plan to streamline cooperation.
- Determine your risk tolerance.
- Balance security controls with end-user productivity.

This guide was built to help your data security teams operationalize your program and tasks when adopting Microsoft Purview. Keep reading for a deep dive into this important topic, including six steps to prepare your organization, the four phases of implementing data security, as well as troubleshooting and optimizing after implementation.

# Preparing to secure your data

Nearly all data security principles are focused on three core goals—ensuring the availability of data for properly vetted use, discovering and protecting the confidentiality of sensitive data, and preserving the integrity of data. Implementing effective data security, however, goes beyond just deploying technology; it's a combined effort that requires people, processes, and technology to work seamlessly together. Establishing clear processes, training your teams, and aligning technology with organizational goals can help create a resilient, adaptable data security posture.

With the implementation of any new technology, proper preparation can help you avoid major roadblocks and lead to greater efficiency and value for your organization looking forward. In this section, you'll find six key steps to take before implementing Microsoft Purview.



# Frame your goals

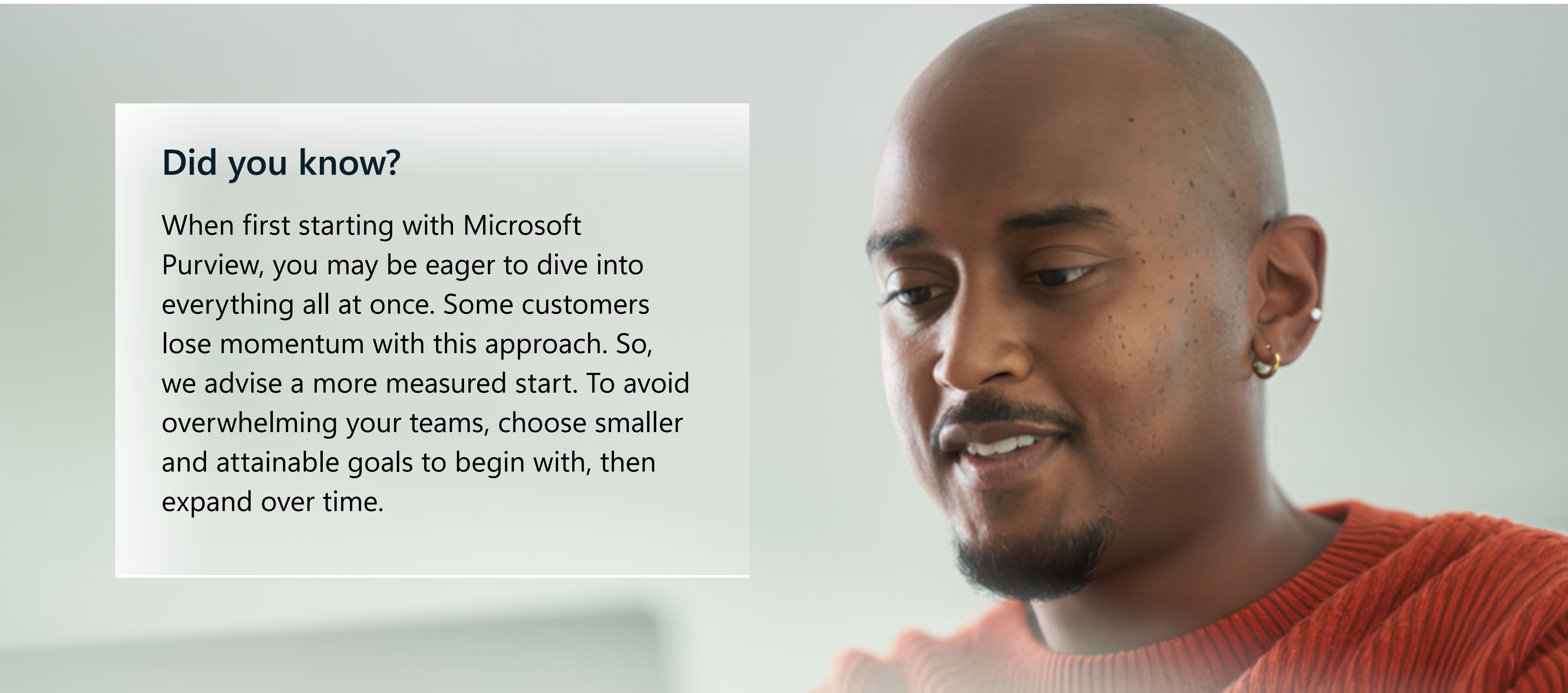
To kick off your data security operationalization with Microsoft Purview, understanding your goals can help form the frame for your data security journey. What are the biggest data challenges for your organization? What are your top business needs? What are your most exciting opportunities? We recommend starting with goals that are actionable, attainable, and promise a fast impact to drive greater user adoption and data security coverage.

Here are a few other considerations to guide the foundation of your data security goals:

- **Preferred security journey:** Different teams and organizations can choose to manage their data security in different ways with different solutions or customized paths to achieve their goals. This journey is tailored to the specific needs, resources, risk tolerance, and maturity levels of each organization. As data security is not a one-size-fits-all solution, different organizations will prioritize and implement security controls in ways that best align with their operational needs and risk landscape.
- **Data security maturity:** Understanding where you are in your data security journey helps you identify what your initial priorities should be, laying the foundation for how to implement and operationalize a data security solution. How do different verticals within your organization work together to make decisions regarding data security issues? What current technologies and processes should you consider? What potential training does my organization need?
- **Initiative participants:** Evaluate who needs to be involved in preparing for this implementation and how they can best contribute to the creation of your organizations data security goals. What teams and departments need to be aware, involved, or accountable for different aspects of your data security journey? What people should you consider involving or are they already involved and accountable for data security within your organization? This will help you identify which stakeholders will influence this operationalization process.
- **Business objectives:** Frame each goal with a mindset of how achieving it will serve your business needs.

## Did you know?

When first starting with Microsoft Purview, you may be eager to dive into everything all at once. Some customers lose momentum with this approach. So, we advise a more measured start. To avoid overwhelming your teams, choose smaller and attainable goals to begin with, then expand over time.



# Determine your approach

Start with secure-by-default principles to set your organization up for success with Microsoft Purview. When your data security strategy is built on the Zero Trust security model, your processes and policies will support stronger data protection, speedier detection and remediation, and better data-breach containment.

- Consider your main business processes and services that need data security coverage and visibility.
- Understand the different data security requirements of the various regions of the world in which your organization operates.
- Determine how your organization will educate stakeholders, staff, and third parties about data classification, safer ways to interact with sensitive data and preventive controls/ protective measures.

## Technology planning

Monitor and protect your data at rest, data in use, and data in motion across Microsoft 365 services, Windows 10, Windows 11, and macOS (the three latest-released versions) devices, on-premises file shares, and on-premises SharePoint. There are planning implications for the different locations, the type of data you want to monitor and protect, and the actions to be taken when a policy match occurs.

## Business processes planning

Policies can block users from performing prohibited activities, like inappropriate sharing of sensitive information via email. As you plan your data security policies, you must identify the business processes that touch your sensitive items. The business process owners can help you identify appropriate user behaviors that should be allowed and inappropriate user behaviors that should be protected against. You should plan your policies and deploy them in simulation mode and evaluate their impact before running them in more restrictive modes.

## Organizational culture planning

A successful data security program implementation is as much dependent on getting your users trained and acclimated to data loss prevention (DLP) practices as it is on well-planned and tuned policies. Since your users are heavily involved, be sure to plan training for them too. You can strategically use policy tips to raise awareness with your users before changing the policy status from simulation mode to more restrictive modes.

### The challenge of balance

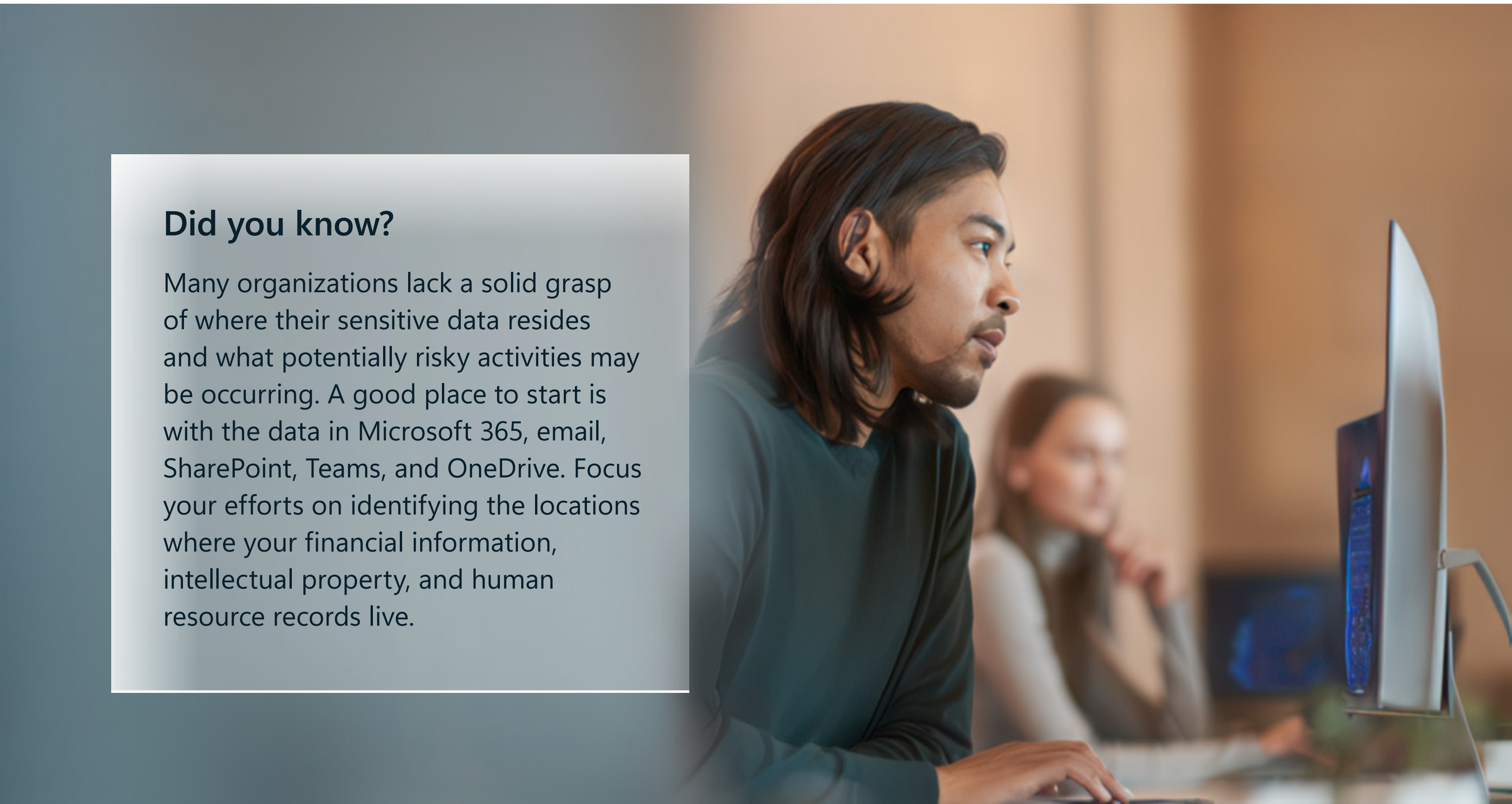
Balancing employee productivity with data security needs is a continuous challenge. When organizations establish their risk tolerance or endure an incident, they may want to deploy broad baseline or blanket policies—like encrypting all their data on OneDrive or blocking all sharing of data with external emails. But implementing policies based solely on certain data security patterns can be detrimental to business outcomes and result in employee dissatisfaction and inefficiency. Before policies are put in place, the needs of the business must be clearly understood, and with that understanding, security can be maintained without surprising business leaders or disrupting established business workflows. This challenge can also be addressed with solutions that dynamically reinforce protections based on different levels of risky behavior, such as Adaptive Protection in Microsoft Purview, that we'll cover later in this guide.

# Understand your data risk tolerance and non-negotiables

Understanding your risk tolerance as well as your data security non-negotiables can help you land on the right mix of security policies and coverage for your organization. Then, you can connect with your designated stakeholders to validate your risk and non-negotiable assumptions to ensure you're on the right path to protecting your data and aligned with other areas of the organization as well.

Other critical considerations that play a part in this process include:

- Determining what your organization considers sensitive data. Recognize that for most organizations, just a part of the data is truly sensitive—most often (but not always), sensitive data includes personally identifiable information (PII), human resources data, financial data, confidential projects, or data related to research and development or the intellectual property of your business.
- Strategizing how to secure data without blocking business initiatives. Some organizations, for instance, find server- and container-level protection for their sensitive workflows is the easiest way to balance security and accessibility.
- Deciding on how much risk is appropriate or tolerable for your organization. While some organizations can't tolerate much risk at all, others would rather focus on the detection of specific risks to avoid overwhelming team members or creating unnecessary alert fatigue. Your organization's risk tolerance may be somewhere in between these two ends of the spectrum.
- Setting and socializing policies for when you will block business initiatives to protect against data security threats. Transparency around your data security standards might help educate and manage commitment from teams.



## Did you know?

Many organizations lack a solid grasp of where their sensitive data resides and what potentially risky activities may be occurring. A good place to start is with the data in Microsoft 365, email, SharePoint, Teams, and OneDrive. Focus your efforts on identifying the locations where your financial information, intellectual property, and human resource records live.

# Engage a cross-functional team

While each organization's needs differ, every company needs to include a cross-functional team to gain alignment and fuel momentum for widespread adoption of data security measures. For optimal results, consider the following key steps:

**Identify your key stakeholders:** Connect with representatives of each area of importance to your organization's data security and for whom your data security program might have more impact. At a high level, the team could likely include representation from risk and compliance (privacy), security, data lifecycle management, IT, business teams, legal, and human resources. Consider including a project management role for timing and scheduling, milestone-progress tracking, and communication. When deciding on the best representative from each area of expertise, look for individuals who have deep knowledge of what data must be protected. It will be important to bring stakeholders along in the journey and to take their teams' needs and concerns into consideration when building the data security strategy.

**Determine the level of engagement:** Establish which representatives need to be informed, involved, deeply engaged, and which should be part of approval processes and policies alignment. Consider the cadence of engagement and what relevant events make sense to align with (many organizations align engagement to their ongoing compliance and reporting requirements).

**Educate across teams:** When approaching prospective team members, share with them why the organization is adopting Microsoft Purview. Share how the implementation will impact the company, their team, and the role they need to play throughout the implementation and beyond. Understanding possible data risk scenarios and vulnerabilities, as well as the data security "vision," will help get stakeholders' buy-ins to your data security strategy.

Note: Executive leadership can help set the tone for the importance of your cross-functional team.

**Anticipate hurdles and limitations:** Structure your stakeholder team to match your organization's specific challenges and goals and ensure contingency plans are in place for transitions, such as when a stakeholder departs or needs to hand off responsibilities. Set a clear, actionable plan with achievable milestones to foster commitment and alignment across your cross- functional team from the outset.

Potential concerns and needs from stakeholders might be:

| Risk and Compliance | Security | IT | Legal | Human Resources | Business Manager |
|---|---|---|---|---|---|
| *"I need to make sure we're meeting all of our company's and regulatory commitments."* | *"I'm responsible for protecting all of our most sensitive data."* | *"We govern and maintain all aspects of the Microsoft 365 environment."* | *"I need to discover all relevant content in a timely manner for requests and investigations."* | *"I need to know the impact to our employees and train them to comply with any new policies."* | *"I need a data security strategy that protects our business outcomes and reputation without affecting productivity."* |

## How many people do we need for deployment?

Your organization’s size and structure matter quite a bit when determining how many team members should handle the implementation and maintenance of Microsoft Purview.

When sizing data security teams, organizations should consider the scope and complexity of their data environment, as well as specific regulatory and compliance requirements, which often dictate the level of specialized staff needed. The team’s size should align with the organization’s security maturity—established teams may focus on optimization, while newer teams need resources to build foundational processes. Additionally, the risk profile and threat landscape are essential factors, with higher-risk industries requiring dedicated roles for proactive detection and response.

Taking advantage of technology and automation, such as Microsoft Purview, can streamline routine tasks, allowing teams to concentrate on strategic initiatives. Cross-functional collaboration is also crucial, as data security often involves IT, legal, compliance, and operations.

Lastly, growth projections should inform team structure to ensure scalability as data and organizational needs evolve. A well-balanced team considers all these aspects to meet immediate security demands while staying adaptable to future challenges.

# Define what success looks like to your organization

You can't measure your success with Microsoft Purview without first knowing what success looks like for you. Organizations should decide up front on clear metrics for evaluating the effectiveness of their Microsoft Purview deployment, which will facilitate the identification of improvement opportunities in the future. Documenting your "why" for each desired achievement can help facilitate knowledge transfer when an individual team member moves on, so new team members know why each policy exists and why a strategy was implemented. Examples of success metrics include:

**The percentage of sensitive data classified:** The proportion of sensitive data that has been identified and labeled out of the total dataset.

**Alert confirmations:** The number of security alerts that have been reviewed and confirmed as actual incidents.

**The ratio of false positives to true detections:** A measure of the accuracy of the security system, indicating how many false alerts are generated compared to real threats.

**The number of data loss incidents detected:** The count of events where sensitive data was identified as being potentially leaked or accessed in an unauthorized manner.

**The number of data loss incidents prevented:** The count of attempts to exfiltrate data that were successfully blocked by security measures.

**The completion of pilot:** Indicates whether a trial run of the security program or a specific security measure has been successfully finished.

**The creation of deployment policies:** The development of guidelines and rules for the implementation of security measures across the organization.

**Workloads completed:** The number of tasks or processes related to the security program that have been finished.

The bottom line is, when determining your success metrics, look for what keeps you up at night and resolve the biggest risks to the organization first. And you can always modify or add to your success metrics and your organization's data security challenged and maturity level changes.

# Prerequisites and where to start

Microsoft Purview is a comprehensive set of solutions that can help your organization protect and manage data wherever it lives.

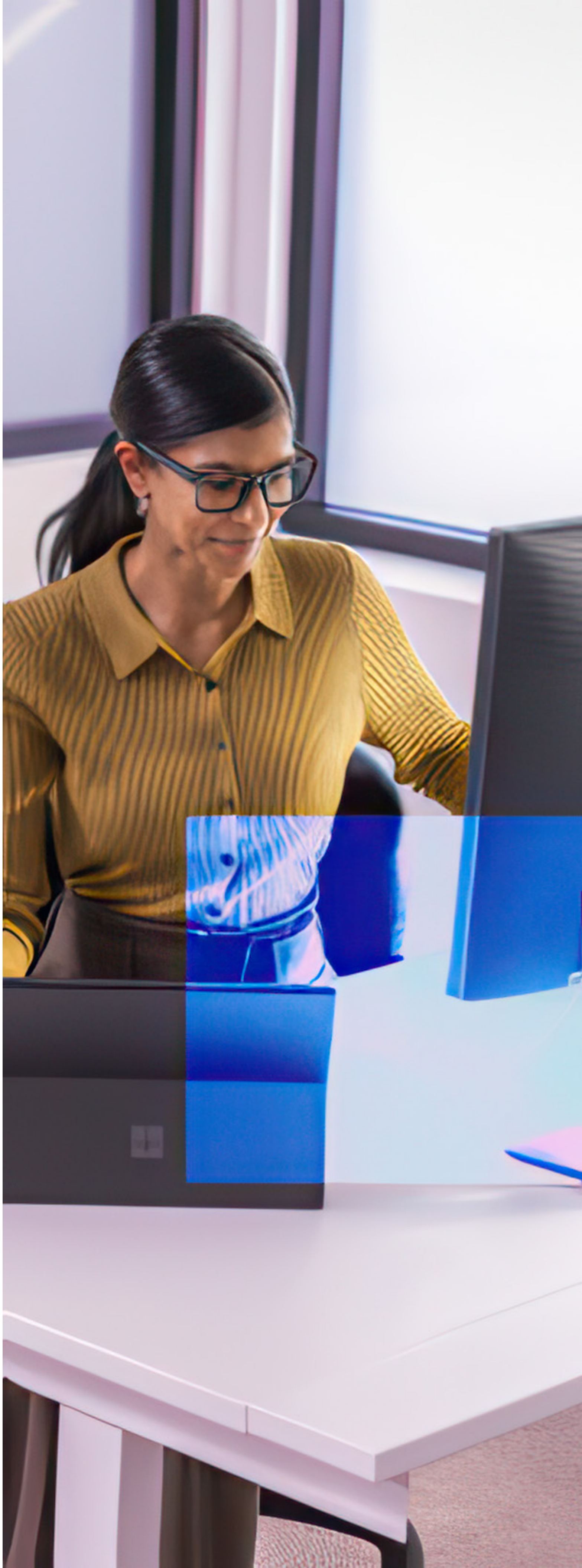
## Common prerequisites

- **Device onboarding:** This is a major step for DLP and Insider Risk Management workloads, in particular for the former as it relates to endpoint DLP.
- **Browser extension review:** This prerequisite can help you gain visibility into how sensitive information is being shared and apply endpoint DLP policies to warn or block users from oversharing sensitive information.
- On-premises-specific requirements.
- Non-tactical prerequisites, such as training your users on how to label their documents.

## Where to start

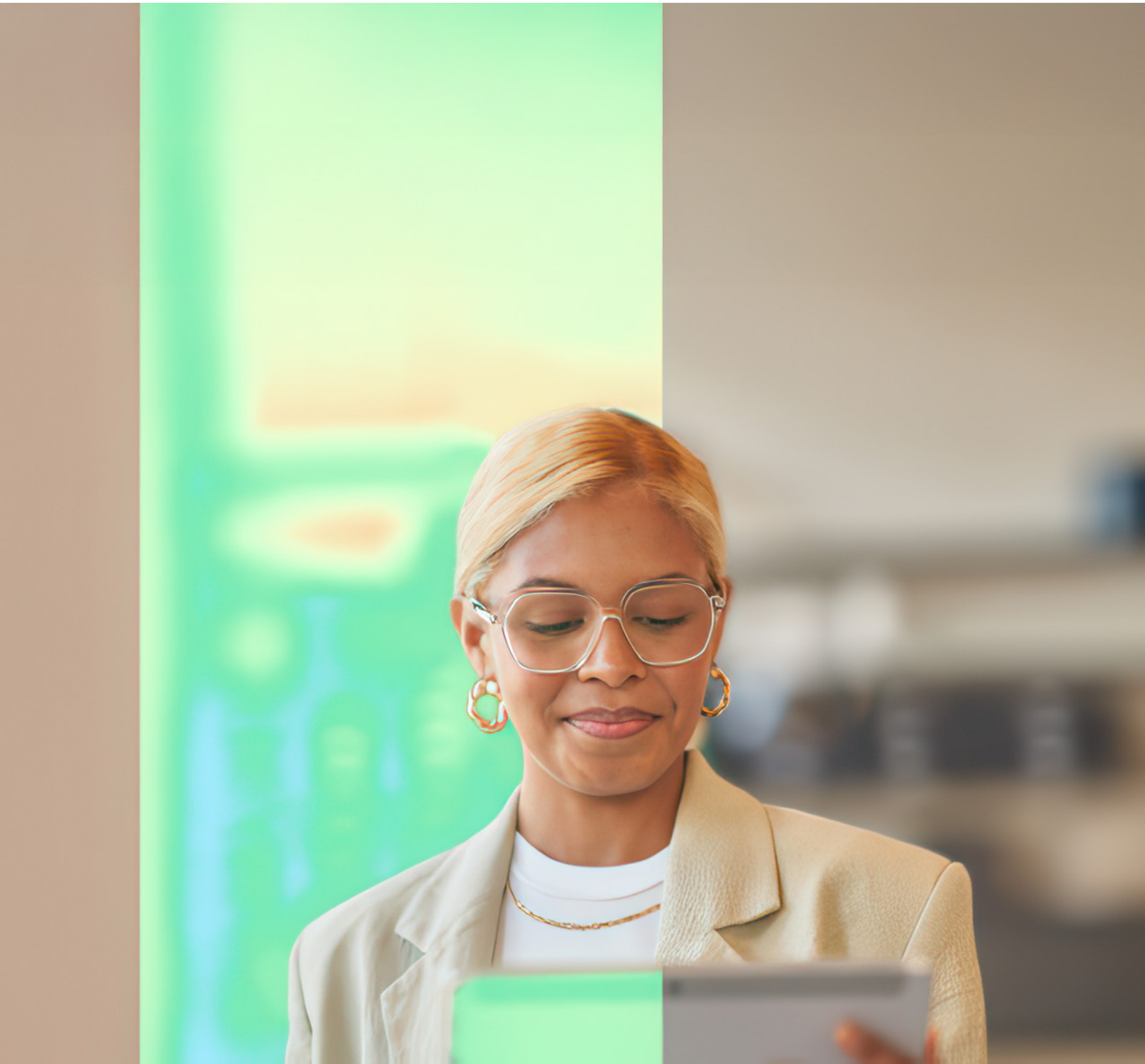
Each organization will choose their own priorities, but here are a few examples of where organizations start to help you determine where to begin your own deployment of Microsoft Purview.

- **Short pilot:** Choose a data workload or data type that lends itself to a short-term pilot, ideally four-to-six weeks from beginning to key completed milestone.
- **Per policy:** Deploy one key policy first then analyze and fine-tune over time.
- **Per workload:** Start with email or Teams, SharePoint, or OneDrive.
- **HR connector:** Choose an HR data type to import based on the specific policy template you wish to deploy.



# Optimizing implementation of Microsoft Purview

You've completed the preliminary planning, and you're ready to start benefiting from the capabilities of Microsoft Purview to protect your data. But what does that involve? In this section, we'll share a four-phase action plan for operationalizing and getting started with Microsoft Purview.



# Assessment

Just as you begin creating the goals for your data security strategy with Microsoft Purview, you should start assessing your environment in short and actionable steps. You can also start involving and engaging with your previously identified stakeholders to validate the outcomes that might show up from the initial understanding of your data environment.

Through assessment, you'll start working with the three core Microsoft Purview data security solutions:

**Microsoft Purview Information Protection (IP):** Empowers organizations to discover, classify, label, and safeguard sensitive information, ensuring protection follows the data wherever it resides or moves.

**Microsoft Purview Data Loss Prevention (DLP):** Assists in adhering to business standards and industry regulations by identifying, monitoring, and automatically securing sensitive information across various data environments.

**Microsoft Purview Insider Risk Management (IRM):** Aids in reducing internal risks by detecting, investigating, and acting upon potentially risky activities within the organization, taking advantage of signals from user activity, HR systems, and other contextual sources.

We will get into more details about how you'll work with each of the solutions in the next phase of the process.

**Initiation stage:** The first stage is about starting to evaluate where your organization is today regarding information security and compliance with your goal of defining a strategic direction for your organization. Using this strategy will foster the adoption of a solution by gathering the requirements of supporting systems, the impact on end users, and the skillset needed for each role owner. The crawl phase describes the steps you should take at the beginning of any deployment, whether your requirements are basic or advanced. It includes the steps for product education, defining requirements, and evaluation or testing.

As part of the assessment phase for your organization, consider the following tasks and ideas:

- **Analyze the data processed in the tenant:** To do this, head to the Microsoft Purview portal, where you can find details in the activity explorer and content explorer tabs. If you can't find what you need there, explore the on-premises scanner for more information.
- **Prepare for data classification:** Identify sensitive information types, map data locations, and access the content explorer to understand your data's classification.
- **Deploy the Information Protection Scanner:** Set up a Windows Server with necessary permissions, install the scanner, configure scan jobs, and run scans on key data repositories.
- **Review and protect data:** Analyze scan results in the activity explorer in order to apply appropriate protection policies, such as sensitivity labels or DLP, based on findings.

- **Turn on Insider Risk Management analytics:** This process is seamless and conducts an evaluation of potential insider risks in your organization without configuring any insider risk policies. It also provides real-time guidance on configuring indicator-threshold settings.
- **Interview business process owners and process-analysis professionals to collect relevant data security use cases:** Encourage business and service owners to list the top information that should be identified and protected within their processes (for example, credit card, IBAN, contract number, purchase order, resume or CV, project proposal, blueprints, or intellectual property).
- **Raise awareness:** Tell employees about the data security capabilities of Microsoft Purview by developing user manuals and enabling business and non-technical users to feel confident about using the solution.
- **Tighten data usage and develop consistent expectations around a sensitivity-labeling strategy:** Labeling is a top concern of many customers, and we advise being thorough in identifying your sensitive data. Most sensitive data is related to an organization's intellectual property—research and development, finance, or leadership.

If you're a ME5 or E5 Compliance customer, you also have the valuable opportunity of turning on Microsoft Purview Data Security Posture Management (DSPM).

DSPM provides visibility into data security risks and recommends controls to protect data, offering contextual insights into data, its usage, and continuous risk assessment of your evolving data landscape, helping to mitigate data risks and strengthen your data security posture.

- **Opt-in to analytics processing:** To get started with DSPM (preview), you must enable and opt in to:
  - Insider Risk Management analytics.
  - DLP analytics.
  - Analytics processing in DSPM (preview) to scan for unprotected data in your organization.
- **Evaluate insights and take action:** After the automated analytics processing is completed, you can evaluate the insights created by DSPM (preview) to help mitigate risks for unprotected data.
- **Actions:**
  - Investigate with Security Copilot: Use built-in and custom prompts with Security Copilot to help identify specific areas of risk.
  - Create policies with recommendations: Use recommendations to quickly create Insider Risk Management and DLP policies to help mitigate data security risks for unprotected data assets.
- **Track posture with analytic trends and reports:** Use analytic trends and reports to view your posture over time and for data locations across your organization.
  - For organizations starting with Microsoft Purview, DSPM (preview) simplifies configuration and policy creation across data security solutions. It automatically scans data, providing baseline insights and recommendations for unprotected data, aiding quick setup in DLP, information protection, and Insider Risk Management.
  - For existing users of these solutions, DSPM (preview) identifies any gaps in current policy coverage, highlighting unprotected data at risk without the need for extensive policy review and testing.

# Understand and prepare your data

In the first few weeks after adoption, take the time to prepare your data by exploring the data security solutions within Microsoft Purview. Within the first 30 days, aim to complete critical data preparation tasks:

**Compliance and regulatory requirements:** Review the European Union's General Data Protection Regulation (GDPR), Personal Information Protection and Electronic Documents Act, Health Insurance Portability and Accountability Act (HIPAA) requirements, and evaluate these regulations based on the region where your organization operates. Make sure you're reinforcing the right data retention, access, and usage policies.

**Data ownership and classification:** Assign data stewards and classify data as public, internal, confidential, or restricted.

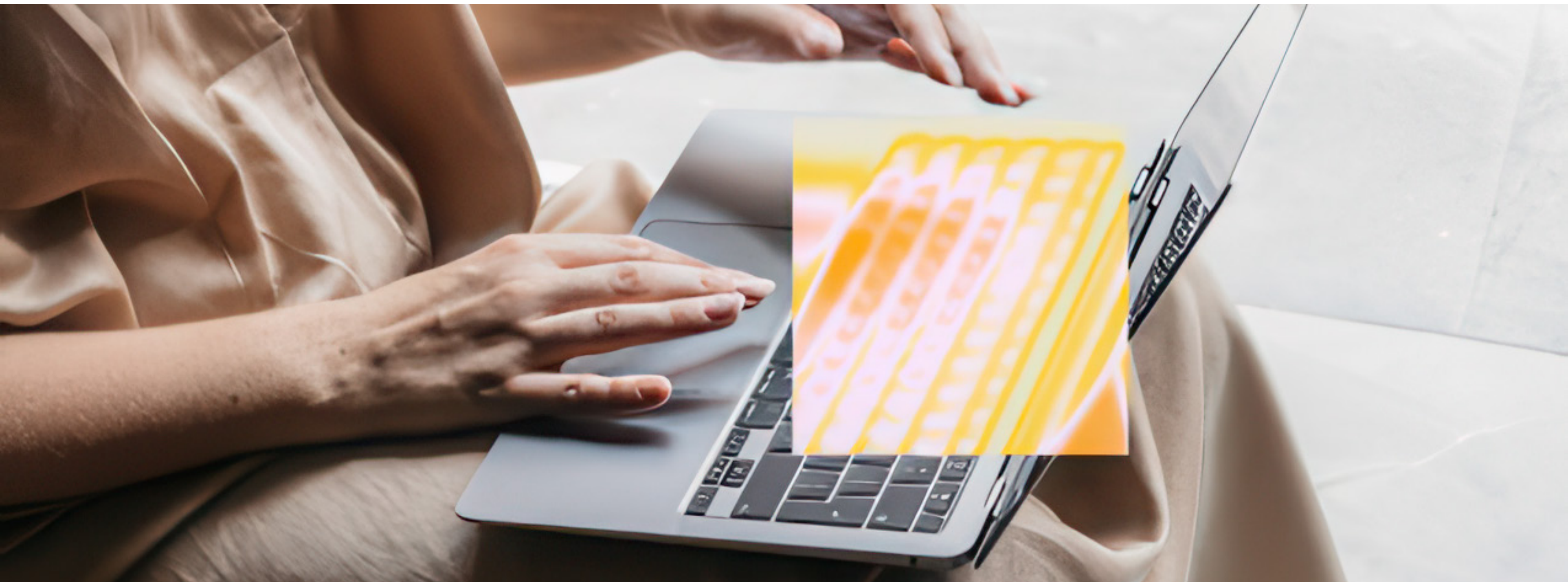
**Define and manage sensitive data:** Create a document listing examples of sensitive data—such as PII and financial records—and develop guidelines for storing, accessing, and sharing sensitive data securely.

**Incident response and management:** Develop or review your incident response plan describing steps to take if there's a data breach.

**User management and access control:** Define roles (for example, admin, manager, employee) with specific access permissions. Use Microsoft Entra ID for automatic account creation or deletion and implement multifactor authentication (MFA) for all employees.

**Explore analytics across your solutions:** You've already turned on Insider Risk Management analytics, now gain valuable insights to guide you across your data security environment. Turning it on early helps you realize value quickly. Plus, this enables you to identify gaps.

**Start with what's important to you:** While you should start with whichever data security solution you prioritize, many organizations start with Insider Risk Management because they don't have to label anything, there are minimal prerequisites, and they can get started quickly without having an impact on end users (the business).



## What you'll be able to implement with Microsoft Purview data security solutions

| Information Protection | Data Loss Prevention | Insider Risk Management |
|---|---|---|
| • Develop your label taxonomy, such as 'general confidential', 'public', 'finance', 'HR', 'highly sensitive'<br>• Utilize built-in features to identify sensitive content and consider implementing autolabeling.<br>• Establish governance across your data estate.<br>• Ensure all data is classified appropriately, determining what requires encryption, for whom it is intended, and what can be generally classified. | • Review the locations where sensitive information is stored.<br>• Develop and implement policies to minimize data leaks, data thefts and other exfiltration activities involved with sensitive information.<br>• Create custom policies or categories specific to your industry, such as health or finance. | • Identify hidden risks with 100+ built-in machine-learning models and indicators, requiring no endpoint agents.<br>• Use templates to develop policies for data leaks, data thefts, and security violations by risky users.<br>• Expedite mitigation with enriched investigations and Adaptive Protection that enforce DLP controls dynamically. |

**Execution Stage:** The second stage builds the foundation for a successful, scalable, and sustainable deployment. In this phase, you plan the details of your implementation, and you build the solution. You may also run a pilot or a proof of concept with a selected group of users or locations.

## Microsoft Information Protection (MIP)

The built-in capabilities from MIP can help your organization discover, classify, protect, and govern sensitive information wherever it lives or travels. You have information residing across all the Microsoft 365 services and on-premises. Identifying which items are sensitive and gaining visibility into how they're being used is central to your Information Protection practice. Microsoft Purview includes:

- Sensitive information types to identify sensitive items by using built-in or custom regular expressions or functions.
- Trainable classifiers to identify sensitive items by using examples of the data you're interested in rather than identifying elements in the item.
- Data classification to provide a graphic identification of items in your organization that have a sensitivity label, a retention label, or have been classified and the actions your users are taking on them.

Consider starting with data classification rather than labeling if you're feeling overwhelmed by labels. Think of the steps of operationalizing Microsoft Purview as a series of building blocks with no set order.

MIP provides a framework and capabilities to discover, classify, and protect sensitive data across on-premises, SharePoint, OneDrive, Exchange, Teams, endpoints, and non-Microsoft clouds by applying sensitivity levels to data. It helps manage critical data risks and regulatory requirements with three core concepts: know your data, protect your data, and prevent data loss.

Learn more about Information Protection, then complete the following steps to begin protecting your first workload:

1. Foundational steps: Start with recommended labels to protect new or updated content. Sensitivity labels are organizational tags that are meaningful and intuitive to end users. The strategy for applying labels often starts with manual labeling, then client-side auto- labeling with sensitive information types (SIT), followed by service-side auto-labeling (at rest) with SIT and contextual conditions.

a. Start with default labels (public, general,

confidential, highly confidential) and protection at file and site level.
b. Turn on data security prerequisites and advanced analytics.
c. Train users on managing exceptions.

2. Managed steps: Address files with highest sensitivity to protect priority content. Identify your priority sites from well-known sites, including sites from leadership teams, content explorer with high numbers of sensitive documents, reporting, and Graph API for sites with high quantities of sensitive information.

   a. Manually configure priority sites default library labeling.
   b. Auto-label for credentials and contextual conditions.

3. Optimized steps: Expand your entire Microsoft 365 data estate to protect historical content and apply policies progressively in scenarios. Auto-labeling is best for scenarios where you need higher sensitivity than your default label.

   a. Auto-label sensitive files on clients (low thresholds).
   b. Simulate auto-labeling sensitive files at rest.
   c. Reduce false positives with advanced classifiers.
   d. Automate and improve Microsoft 365 protection to historical and in-use data.

4. Strategic steps: Operate, expand, and perform retroactive actions to protect beyond Microsoft 365.

   a. Perform an operational review of user labeling behaviors.
   b. Iterate with new labeling scenarios.
   c. Set up accountability chain and lifecycle management.
   d. Extend protection to Azure SQL and non-Microsoft 365 storage.

### Did you know?

The best approach is multipronged. Use a combination of labeling methods, including automatic labeling, manual labeling, mandatory labeling, and default labeling. While labeling is important, you don’t have to complete it before starting a second workstream. Strengthen your security for multiple workstreams while working on labeling at the same time, as things like country-specific labels and industry-specific considerations take time.

## Anatomy of a policy

When you create an information protection label policy, these are the factors you’ll have to consider:

- Choose sensitivity labels to publish (among personal, public, general, confidential, highly confidential, project related, etc.). When published, the labels you choose will be available in specified users’ Office apps (Word, Excel, PowerPoint, and Outlook), SharePoint and Teams sites, and Microsoft 365 Groups.

- Assign admin units. Choose the admin units you’d like to assign this policy to. Admin units are created in Microsoft Entra ID and restrict the policy to a specific set of users or groups. Your selections will affect the location options available to you in the next step.

- Publish to users and groups. The labels you select will be available for the users, distribution groups, mail-enabled security groups, and Microsoft 365 Groups you choose here.

- Put in place policy-specific settings such as "Users must provide a justification to remove a label or lower its classification," or "Require users to apply a label to their emails and documents."
- Apply default settings to documents. The label you choose will automatically be applied to documents, meetings, emails, sites, groups and other content when they're created or modified.
- Use default policies as-is, create new ones, tweak them however you prefer, or completely customize them to best suit your individual business requirements.

### Did you know?

Microsoft Purview Information Protection for Microsoft 365 apps and services, SQL Server, Azure Data Lake Storage, and Microsoft Fabric let you add sensitivity labels to your data. Then, Microsoft 365 Copilot inherits labels from these files. You can even set up auto-labeling, which applies sensitivity labels to files and emails based on sensitive data input. In fact, Microsoft 365 E5 indexes everything out of the box; 99% of labeling is automated.

## Insider Risk Management (IRM)

IRM lets you minimize data security risks through detection of, investigation of, and action against malicious, negligent, or inadvertent insider activities. It correlates various signals to identify potential insider risks, such as IP theft, data leakage, and security violations. As many as 59% of employees admit they take data with them when they leave an organization.* Insider Risk Management uses the full breadth of Microsoft 365 services, Fabric, and third-party indicators to help you quickly identify, triage, and act on potentially risky activity. By using logs from across Microsoft environment and even 3rd-party apps, Insider Risk Management allows you to define specific policies to identify risk indicators. After identifying the risks, you can take action to mitigate these risks, and if necessary open investigation cases and take appropriate legal action.

Learn more about Insider Risk Management, complete the following steps to create your first Insider Risk Management policy, and start analyzing your insider risk landscape:

1. Enable permissions for Insider Risk Management: There are six role groups used to configure Insider Risk Management features. To make Insider Risk Management available as a menu option in Microsoft Purview and to continue configuration, you must be assigned to one of the groups. available as a menu option in Microsoft Purview, and to continue configuration, you must be assigned to one of the groups.
2. Enable the Microsoft 365 audit log: The Microsoft 365 audit logs are a summary of all activities within your organization, and Insider Risk Management policies may use these activities for generating policy insights.
3. Configure prerequisites for policies: Configure the appropriate prerequisites for the policies you plan to configure so your policy indicators generate relevant activity alerts.
4. Configure insider risk settings: These settings control privacy, indicators, global exclusions, detection groups, intelligent detections, and more, and are configured using the settings button located at the top of the Insider Risk Management pages.
5. Create an Insider Risk Management policy: Policies include assigned users and define which types of risk indicators are configured for alerts. Before potentially risky activities can trigger alerts, a policy must be configured. Use the policy wizard to create new Insider Risk Management policies.

*Departing workers often steal data from ex-employers: study | CBC News

a. **Policy recommendations from analytics:** Microsoft Purview Insider Risk Management uses analytics to provide policy recommendations. These recommendations are based on the analysis of user activities and other signals, helping to identify potential risks and suggest appropriate policies to mitigate them.

b. **Quick policies from recommended actions:** From the recommended actions provided by the analytics, organizations can quickly create policies. This feature allows for a rapid response to identified risks by generating policies that address specific risky behaviors or activities.

Scenarios available:

- Critical assets protection detects activities involving your organization's most valuable assets. Loss of these assets could result in legal liability, financial loss, or reputational damage.
- Data leaks detect potential data leaks from all users in your organization, which can range from accidental oversharing of sensitive info to data theft with malicious intent.
- Data theft by departing users detects potential data theft by users near their resignation or termination date or based on their account being deleted from Microsoft Entra ID.
- Email exfiltration detects when users email sensitive assets outside your organization. For example, users emailing sensitive assets to their personal email address.

c. **Policy created from zero:** Organizations also have the flexibility to create policies from scratch. This means they can define custom policies tailored to their unique requirements and risk scenarios, without relying on the automated recommendations.

These explanations should give you a clear understanding of how Microsoft Purview Insider Risk Management assists in policy creation and risk management. If you have any more questions or need further details, feel free to ask!

After you've completed these steps, you'll start to receive alerts from activity indicators after

about 24 hours. To learn more about investigating insider risk alerts and the alerts dashboard, see Insider Risk Management activities.

### Did you know?

By setting insider risk policies, you can define the types of risks to identify and detect in your organization. Once you detect and triage risks, you can escalate cases to Microsoft eDiscovery (Premium) for additional investigation, if needed.

## Anatomy of a policy

When you create an Insider Risk Management policy, these are the factors you'll have to consider:

- Policy templates can specify the conditions and indicators that define the risk activities you want to be alerted to, based on the main inside risk use cases (playbooks).
- Choose if policy will apply to all users and groups of if you'll limit coverage to specific users, groups, and adaptive scopes.
- Content prioritization: You can prioritize content based on factors like where it's stored, types of files, and how it's classified (sensitivity). Risk scores are increased for any activity that contains priority content, which in turn increases the chance of generating a high-severity alert.
- Choose one or more triggering events to determine when a policy will begin assigning risk scores to a user's activity. You can then set custom or recommended thresholds for

each event. By setting thresholds, you can define which activities should trigger a closer evaluation for potential insider risks and can reduce noise to generate more high-value alerts.

- Choose the indicators that will be part of that policy and will be used to generate alerts for the activity detected by the policy template you selected. You can choose indicators such as from Office, devices, cloud storage, Fabric, or even custom indicators.
- Choose your advanced detection options, such as:
    - **Sequences:** A group of two-or-more activities performed one after the other over a period of 7 days that might suggest an elevated risk. Specific indicators are used to detect each step in a sequence, which are organized into four main types of activity: download, exfiltrate, obfuscate, and delete.
    - **Cumulative exfiltration detection:** Detects when the number of exfiltration activities that a user performs over a certain time exceeds the normal amount performed by users in your organization over the past 30 days.

## Data Loss Prevention (DLP)

DLP helps you identify and prevent risky or inappropriate sharing, transfer, or use of sensitive data across cloud apps, devices, on-premises repositories, and more. Sensitive data can include financial data, proprietary data, credit card numbers, health records, social security numbers, and more.

Many organizations choose to implement DLP to comply with various governmental or industry regulations, for example, the European Union's GDPR, HIPAA, or the California Consumer Privacy Act (CCPA). They also implement DLP to protect their intellectual property. However, the starting place and ultimate destination in the DLP journey vary.

Organizations that know their sensitive information often start their DLP journey at the platform or workload level, or with the type of sensitive information they wish to prioritize protecting. For organizations still determining what their sensitive information includes and where it lives, they may go straight to defining policies and reviewing the outcomes to refine them later. It doesn't matter where you start; DLP is flexible enough to accommodate various types of information-protection journeys from start to a fully realized DLP strategy.

When first setting up DLP:

- Start with audit-only mode. You can then review the alerts to decide what types of sensitive data or activities to block or caution against. Audit mode makes sure you don't interfere with important business processes in which sensitive data needs to be shared internally or outside of the organization.
- Use the moderation feature for emails to manage exceptions.
- Understand that data exfiltration happens through the endpoint, where users often copy data to a USB stick or print and forward to a personal email address.
- Recognize what DLP analytics and simulation mode are missing. (Ideally, customers create policies and run them in simulation mode before deployment.)

Learn more about Purview Data Loss Prevention, then explore the following steps to begin identifying, mapping, and preparing your data for DLP policy design:

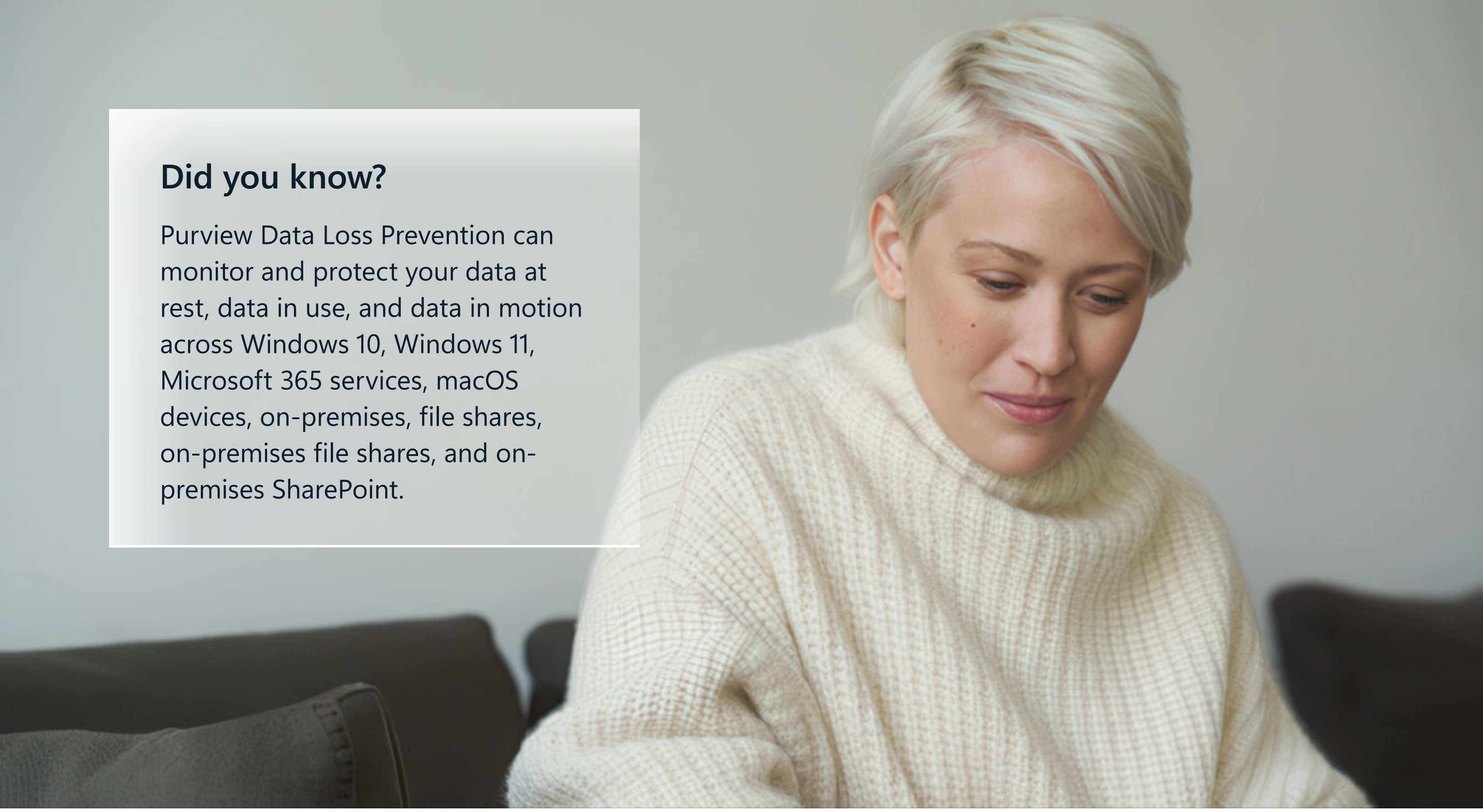
1. Identify the categories of sensitive items to be protected and the business processes they're used in; Microsoft Purview Compliance Manager can help you start with a default assessment and a set of controls for key regulations and standards.
2. Prioritize which data should be protected first based on the sensitivity of the items and risk involved.
3. Determine the risky behavior that should be limited. Start by defining your control objectives and how they apply across each respective workload.
4. Design your policies. Draft a policy that embodies your objectives. Feel free to start with one workload at a time, or you can look across multiple workloads. You can start from a predefined template and create a policy in just a few clicks, or you can design your own from the ground up.

When you reach the stage of designing a policy, review the DLP policy design best practices advised by Microsoft. Taking the time to design a policy before you implement it gets you to the desired results faster than if you create and fine-tune it by trial and error alone, and you'll experience fewer unintended issues. Having your policy designs documented will also help you with communications, policy reviews, troubleshooting, and further tuning.

Designing a policy is mostly about clearly defining your business needs, documenting them in a policy intent statement, and then mapping those needs to  policy configuration. You use the decisions you made in your planning phase to inform some of your policy design decisions. With your key stakeholders identified, your next steps are to:

- Define the intent for the policy.
- Map business needs to policy configuration.
- Describe the categories of sensitive information to protect.
- Set your goals and strategy.
- Define your policy deployment plan.

5. Implement policy in simulation mode. Actions defined in a policy aren't applied while the policy is in simulation mode. It's ok to apply the policy to all workloads in simulation mode so that you can get the full breadth of results, but you can start with one workload if you need to.
6. Monitor outcomes and fine-tune the policy. While in simulation mode, monitor the outcomes of the policy and fine-tune it so that it meets your control objectives while ensuring you aren't adversely or inadvertently having an impact on valid user workflows and productivity.
7. Outline the DLP policy match event review and remediation process. Set protection goals and develop an implementation plan.
8. Enable the control and tune your policies.
9. Make sure you:
   - Turn on DLP policies for labeled content.
   - Turn on DLP for content that is not labeled.
   - Turn on Adaptive Protection and data leak behavioral rules.
10. Analyze generated DLP alerts. DLP generates an alert when a user performs an action that meets the criteria of a DLP policy, and you have incident reports configured to generate alerts. DLP posts the alert for investigation in the DLP alerts dashboard. Use the DLP alerts dashboard to view alerts, triage them, set investigation status, and track resolution. Alerts are also routed to Microsoft Defender  portal where you can do all the alert dashboard tasks plus more.



### Did you know?

Purview Data Loss Prevention can monitor and protect your data at rest, data in use, and data in motion across Windows 10, Windows 11, Microsoft 365 services, macOS devices, on-premises, file shares, on-premises file shares, and on-premises SharePoint.

## Anatomy of a policy

When you create a DLP policy, these are the factors you'll have to consider:

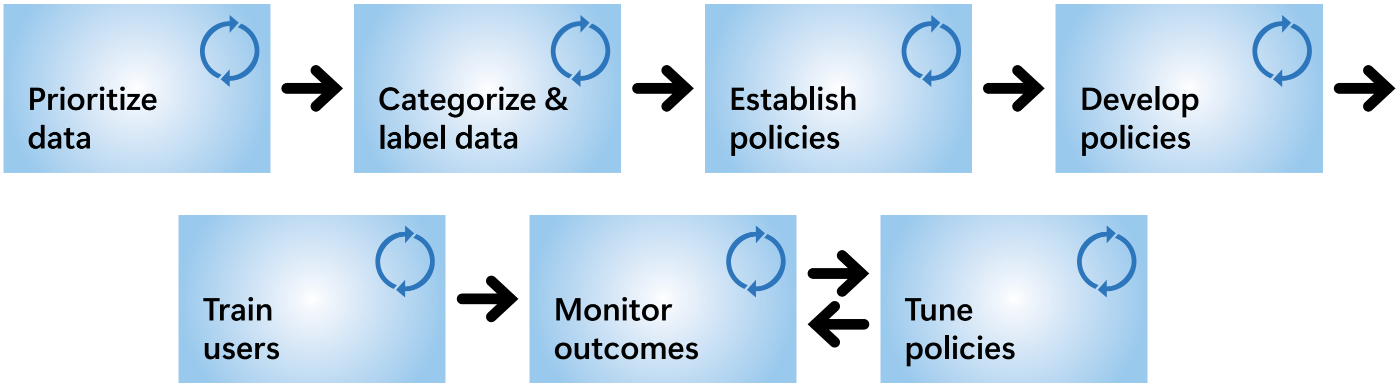
- Start with a template or create a custom policy. Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch.
- Assign admin units. Choose the admin units you'd like to assign this policy to. Admin units are created in Microsoft Entra ID and restrict the policy to a specific set of users or groups.
- Choose where to apply the policy based on data that's stored in the locations you choose, such as email, SharePoint sites, One Drive accounts, devices, Teams, etc.
- Customize advanced DLP rules such as specific conditions, exceptions, actions to impact the target user, notifications, override options, incident report, and if you want to allow dynamic controls based on insider risk levels (learn more about automatic controls enabled by Adaptive Protection in the next phase of this guide).

### A real life story

One organization experienced the exfiltration of a huge number of gigabytes of files—including some containing sensitive data—in a single day. Before adopting Microsoft Purview, it didn't have the visibility to detect an incident like this. In fact, it wouldn't have known how much sensitive data was in those files. The organization shared that this incident reinforced why it deployed Microsoft Purview in the first place: because visibility helps prevent data loss incidents from happening.

# Fine-tune and revisit your policies

Once you have established the first stages of implementing and operationalizing data security with Microsoft Purview in your organization, your interactions with these solutions can be very frequent or more spread out. Remember, depending on your organization's size and maturity level, it could take months, or even years, to deploy every single step to explore all Microsoft Purview data security capabilities.



Organizations usually implement policies that address their top concerns first. But some sensitive information may generate alerts that become overwhelming and make too much noise. Conversely, you may get fewer alerts than anticipated and worry that you haven't configured your policies properly. Fine-tuning and reviewing your policies are critical parts of data security operationalization and key activities of ongoing management.

If you want to set a timeframe on revisiting policies, consider aligning to a risk management framework, like the one developed by the National Institute of Standards and Technology. This involves reviewing all security-related policies annually as part of your overall process.

Microsoft Purview gives you the ability to slightly tweak definitions of your policies with the push of a button. And you should continually fine-tune your policies as you discover what works best for your organization and as you identify new potential risks. Whether that means making tweaks every day or every week will be unique to your organization, industry, and compliance requirements.

When rolling out new solutions, set up enforcement actions. Some customers aren't comfortable putting encryption on documents, enforcing traffic-light-protocol controls, or taking other measures because they fear major business impact. But strengthening cybersecurity is why you started your data security journey in the first place. And to achieve this, you should define a path from alert to enforcement.

**Scale stage:** The last stage is about optimizing the solution for Microsoft 365. In this phase you will set up an automated scalable approach for each solution.

## Insider Risk Management

Because of the nature of the information and breadth of signals, Insider Risk Management can be a good candidate for fine-tuning focus to avoid noise and unnecessary alerts.

Learn more about designing and fine-tuning DLP policies here: Fine-tune exclusions in Insider Risk Management by creating detection groups and modifying built-in indicator variants (preview) - Microsoft Learn.

For Insider Risk Management, you have the option of "tuning for more accurate alerts." There is a recommended action in the product called, "explore best practices for tuning alerts." It includes some great tips on tuning, including using the following features: allowed domains, file type, keyword exclusion, and SIT exclusion. You can take advantage of in-product guidance for tuning as well, such as using available scenario- based policy templates.

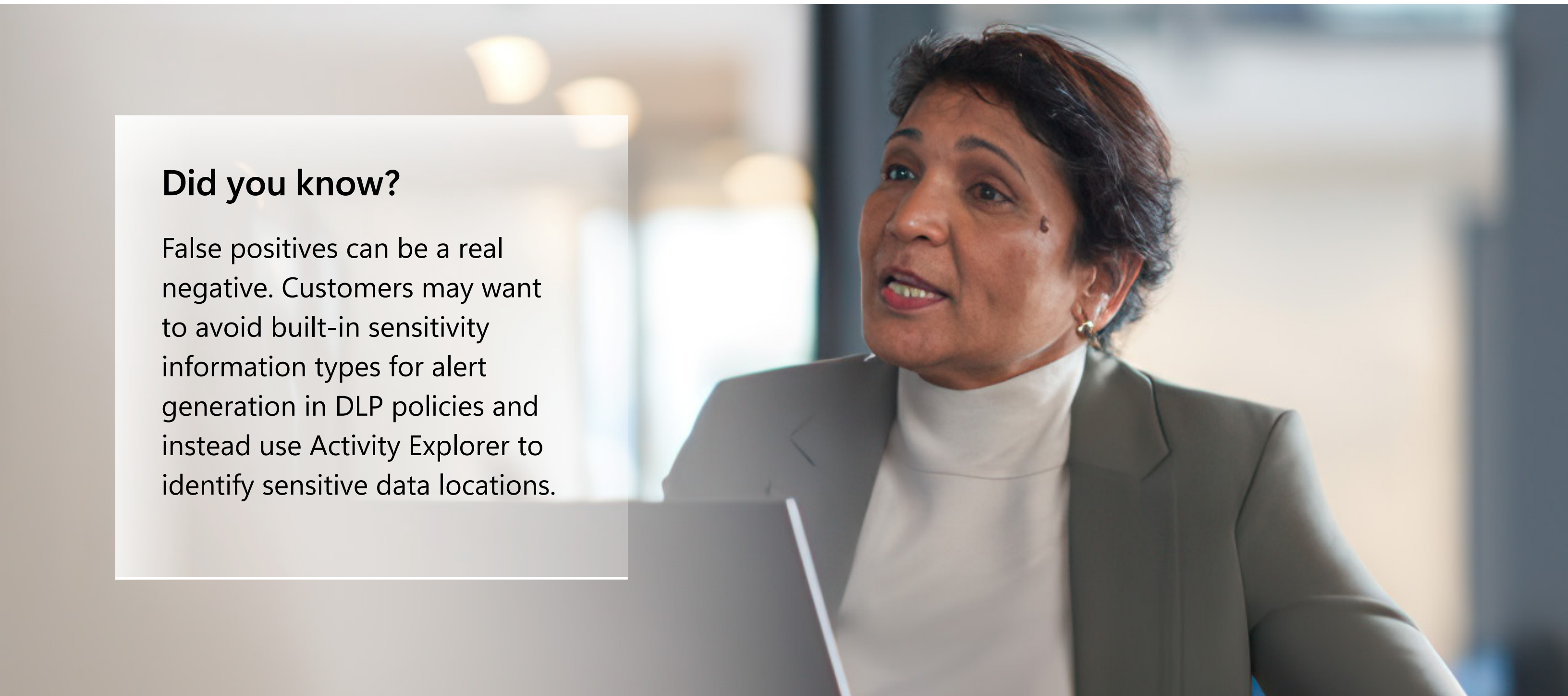
## Data Loss Prevention

To fine-tune Microsoft Purview Data Loss Prevention policies, begin by deploying them in simulation mode to assess their impact without enforcing restrictions. This approach allows you to monitor outcomes and identify potential false positives. During this phase, you will collect feedback from users who receive policy alerts and adjust the policies accordingly to minimize disruptions. Key adjustments may include refining the conditions that trigger policy actions, modifying the scope of monitored locations, and updating the list of sensitive information types. Once the policies effectively balance protection and usability, activate them fully and continue to monitor their performance, making further refinements as necessary to adapt to evolving data protection needs.

Learn more about designing and fine-tuning DLP policies here: Design a Purview Data Loss Prevention policy - Microsoft Learn.

### A customer story

A healthcare company deployed incident response management within the US and turned its data loss program into an insider threat program. A small team of three-to-four people managed the program but had questions about how to make it effective. Two of them came to Microsoft and worked with our experts to get their questions answered..



### Did you know?

False positives can be a real negative. Customers may want to avoid built-in sensitivity information types for alert generation in DLP policies and instead use Activity Explorer to identify sensitive data locations.

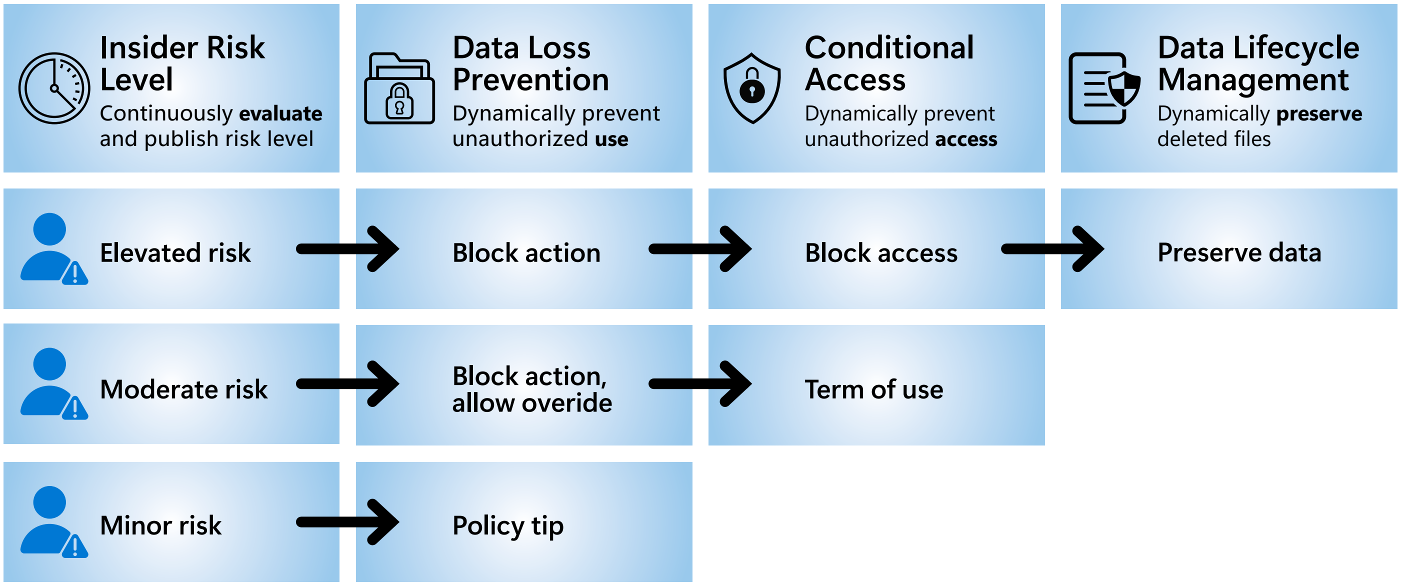
# Enhance data security scenarios and set up Adaptive Protection

Understandably, organizations usually implement policies that address their top concerns. Fine-tuning is often sparked by the initial alerts if alerts become overwhelming, and you want to reduce the noise by landing on the policies that are most critical. Or you may get too few alerts and worry you haven't configured your policies properly. When reviewing alerts and the events that trigger them, consider the opportunities to further enhance your data security:

- Support relevant data protection and security-based scenarios.
- Complete an assessment of insider risk scenarios.
- Roll out Insider Risk Management and configure and fine-tune Insider Risk Management policies.
- Enable the assessment of third-party data connectors if they are needed and applicable. For instance, the HR data connector should be assessed for whether or not it shares resigned users between HR and IT security.
- Investigate DLP alerts and reinforce controls.
- Investigate Insider Risk Management alerts all the way to creating an eDiscovery case.

Once your data security program is more mature and your policies are better tuned to reflect key scenarios that protect and enable your team to focus on investigating what matters, your organization might feel confident enough to start applying more automatic data security controls.

## Adaptive Protection in Microsoft Purview



| **Insider Risk Level**<br>Continuously **evaluate** and publish risk level | **Data Loss Prevention**<br>Dynamically prevent unauthorized **use** | **Conditional Access**<br>Dynamically prevent unauthorized **access** | **Data Lifecycle Management**<br>Dynamically **preserve** deleted files |
|---|---|---|---|
| Elevated risk → | Block action → | Block access → | Preserve data |
| Moderate risk → | Block action, allow overide → | Term of use | |
| Minor risk → | Policy tip | | |

## Setting up Adaptive Protection

Adaptive Protection is a Microsoft Purview capability that integrates insider risk levels to dynamically enforce controls on riskier users that are interacting with data and access in your organization. When insider risk identifies a user who is engaging in risky behavior, they are dynamically assigned to an inside risk level. Adaptive Protection can then automatically be attached to a DLP policy, a Microsoft Entra Conditional Access, or to Data Lifecycle Management to help protect the organization against the risky behavior that's associated with that inside risk level. As insider risk levels change in Insider Risk Management, the DLP policies applied to users can adjust, for example.

Adaptive Protection can be used to monitor risk levels without enforcing any block actions immediately, when you run Microsoft Purview policies in audit mode or in simulation mode. Be aware that when creating new policies, you'll want to run in audit or simulation mode for these policies until you see the alerts being generated to avoid inadvertently blocking productivity.

After all, many organizations tell us they adopted Microsoft Purview in part because they don't want to disrupt collaboration between users working on the same file or similar instances where productivity could be impacted. With their previous systems, they say, they had specific checkout rules or a lockdown scenario where such simultaneous collaboration wasn't possible.

## Steps to configure Adaptive Protection

The **quick setup option** is the fastest way to get started with Adaptive Protection. With this option, you don't need any preexisting Insider Risk Management, DLP, Data Lifecycle Management, or Conditional Access policies, and you don't need to preconfigure any settings or features. You can get started by selecting **Turn on Adaptive Protection** from the Adaptive Protection cards on the Microsoft Purview portal home page or the DLP overview page. You can also get started with the quick setup process by going to **Insider Risk Management > Adaptive Protection > Dashboard > Quick setup.** The **custom setup** option allows you to customize the Insider Risk Management policy, the insider risk levels, and the DLP and Conditional Access policies configured for Adaptive Protection.

1. Create an Insider Risk Management policy.
2. Configure insider risk level settings.
3. Create or edit a DLP policy.
4. Create or edit a Conditional Access policy.
5. Turn on Adaptive Protection.

While tuning Adaptive Protection, your organization may be concerned with the scale of disruption that blocking users using Adaptive Protection might cause. The potential for inadvertent disruption to productivity can be mitigated by using predictable definitions for risk levels and by editing your DLP and Conditional Access policies to use less disruptive actions.

To reduce the likelihood of disrupting productivity, we recommend using the following definitions for your risk levels. These definitions are the least likely to produce false positives:

- **Elevated:** Confirmed alert of any severity
- **Moderate:** High or medium severity alert generated
- **Minor:** High, medium, or low severity alert generated

To reduce the disruption to the end user, you can configure your Adaptive Protection DLP and Conditional Access policies to apply non-blocking actions that will still mitigate risk. For DLP, you can configure your policy to warn risky users or to block with override. For Conditional Access, you can configure your policy to serve risky users terms of use, require them to configure MFA, or block them from certain SharePoint sites.

Read more about quick and custom setup options for Adaptive Protection.

# Troubleshooting and continual improvement

Launching Microsoft Purview is just the beginning. You'll want to review and revisit your policies to ensure your success metrics are being met and apply changes when they're not. While you continue fine-tuning your use of Microsoft Purview, don't let perfect get in the way of progress.

## Data security program maintenance strategies

- Tackle one workload, entity, or challenge at a time to start with achievable milestones and build momentum from there. Repeat this strategy whenever you're determining what's next in a sequence of work.
- Monitor data security for a month and set new DLP policies based on your findings. Surprises will always crop up that you couldn't have anticipated. You can also keep revisiting your policies to ensure they align with new or changing regulations and compliance requirements.
- Check in with your change management professionals or HR to revisit training regularly and whenever new employees are onboarded. It's imperative for all employees to have a clear understanding of your organization's data security strategy.
- Plan for employee turnover and employees moving into new roles by avoiding single-threaded dependencies. Expect that roles will change over time and be ready for it to avoid any knowledge gaps.
- Recognize that just as training is a continual process, so is maintenance of the solution. Maintenance is about continual improvement as your IT team adapts solution training, integrations, policies, and troubleshooting to align with your unique needs.
- Optimize your use of Adaptive Protection by configuring risk levels to be more appropriate for your organization.

## Learning and building momentum

- Extend your ambitions beyond your previous solution. Many organizations assume that they're limited by what they were limited by with their old solution.
- Study your analytics for insights on which policies you should create. Within the first three months, you'll gain valuable insights on how lines of business use data, on your entire data estate, and you will gain confidence in monitoring and identity.
- Fast-track your deployment by shifting to a model where you come up with a clear plan based on achieving bite-sized outcomes—like deploying a policy to a few users—and measurable goals. And everyone on the team should hold everyone accountable for hitting those milestones.
- As you have fine-tuned your policy use and receive fewer false positives, you can focus less time on triaging alerts and more time on addressing true alerts, threshold adjustments, and policy adjustments.
- Add a process for handling new Microsoft Purview features to account for how new capabilities can affect and improve the data security of your organization.

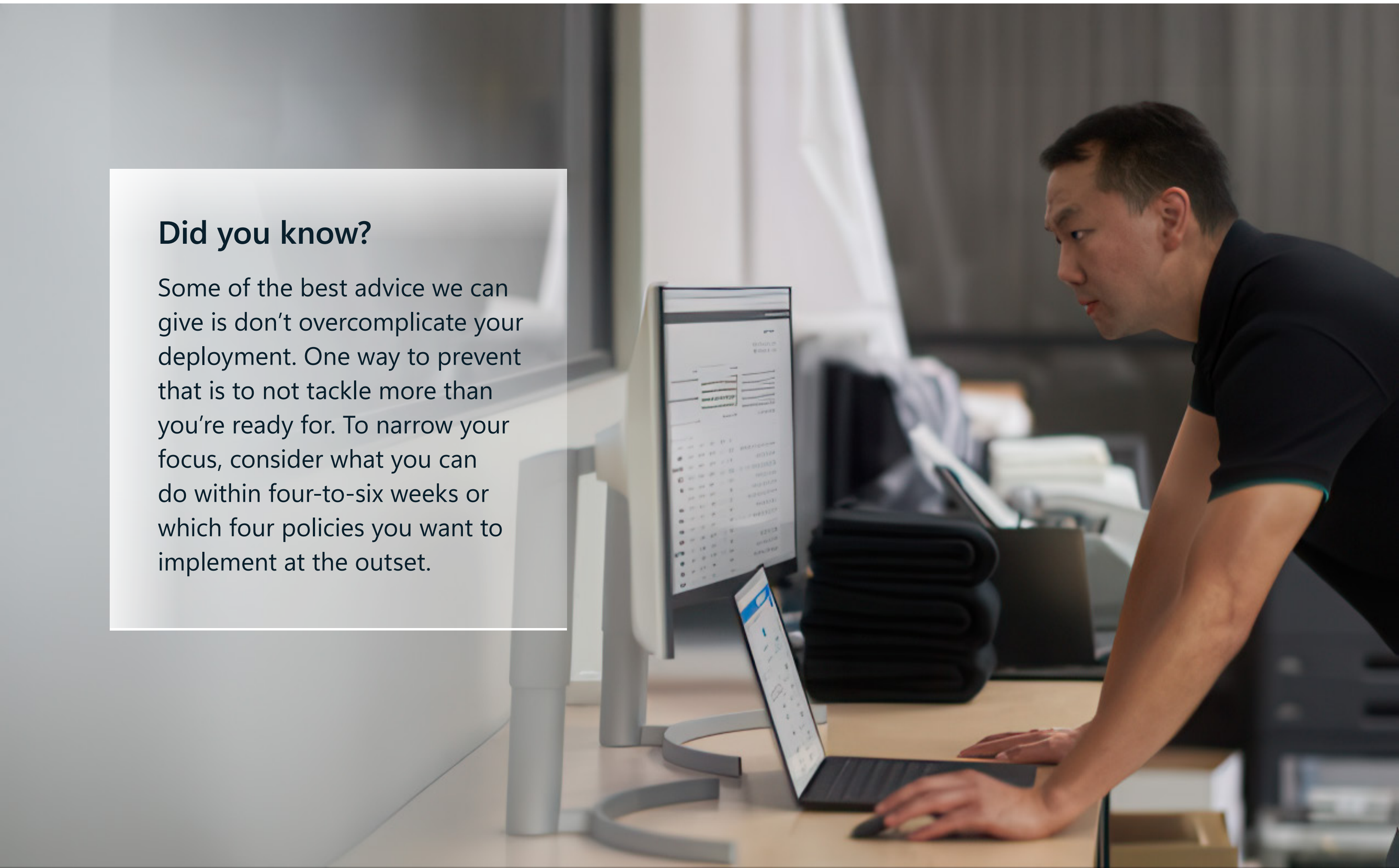
## Communicating and training

- Minimize the impact on business productivity.
- Think about how "painful" too much blocking can be for the business.

- Determine how much trust to put in users and their ability to label correctly and consistently; utilize automatic labeling wherever possible.
- Consider when you should revisit your policies.

Deploying Microsoft Purview for data security involves many steps, but a range of resources is available to support you throughout the process:

1. **Deployment models:** These guides, developed by the engineering team at Microsoft, offer prescriptive deployment guidance based on real-world customer experiences. They provide high-level overviews and detailed steps tailored to specific business scenarios. Microsoft Learn
2. **Setup guides:** Comprehensive setup guides are available to help you configure various Microsoft Purview solutions, including Information Protection, Data Lifecycle Management, and eDiscovery. These guides offer step-by-step instructions to streamline your deployment process. Microsoft Learn
3. **Security best practices:** To help ensure a secure deployment, it's essential to follow best practices. Microsoft provides detailed recommendations on configuring Microsoft Purview securely, including network isolation and access controls. Microsoft Learn
4. **Readiness checklist:** Before deployment, reviewing a readiness checklist can help identify prerequisites and ensure your environment is prepared. This checklist covers planning, organizational readiness, and foundational setup steps. Microsoft Learn
5. **Microsoft Support and community forums:** For personalized assistance, you can reach out to Microsoft Support or engage with the Microsoft Purview community forums. These platforms allow you to ask questions, share experiences, and learn from other users.



## Did you know?

Some of the best advice we can give is don't overcomplicate your deployment. One way to prevent that is to not tackle more than you're ready for. To narrow your focus, consider what you can do within four-to-six weeks or which four policies you want to implement at the outset.

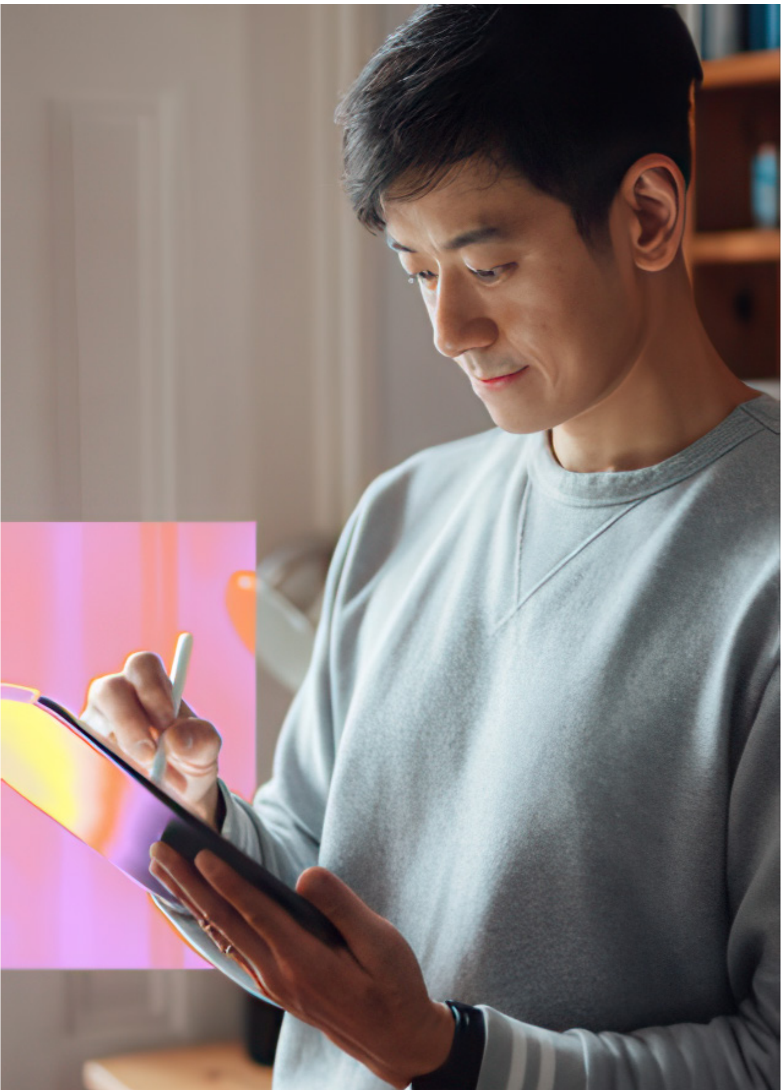
# Continuing your data security journey

Launching Microsoft Purview is just the beginning. You'll want to review and revisit your policies to ensure your success metrics are being met and apply changes when they're not. While you continue fine-tuning your use of Microsoft Purview, don't let perfect get in the way of progress.

## Microsoft Purview Data Security Posture Management for AI

Microsoft Purview Data Security Posture Management for AI (DSPM for AI) is currently in preview and provides easy-to-use graphic tools and reports to quickly gain insights into AI use within your organization. One-click policies help you protect your data and comply with regulatory requirements.

Read more about the Microsoft Purview DSPM for AI.



## Microsoft Security Copilot

Microsoft Security Copilot is a cloud-based AI platform that can assist security and compliance professionals in protecting their organization's data. With Security Copilot embedded in Microsoft Purview, teams can use it to identify, summarize, triage, and remediate issues within Microsoft Purview solutions.

Current main scenarios for data security admins to take advantage of Security Copilot embedded in Microsoft Purview:

- Uncover hidden risks in your data security environment with starting insights, guided investigation, and open prompt analysis in Data Security Posture Management. For more information, see Use Microsoft Security Copilot with Data Security Posture Management (preview) | Microsoft Learn.
- Get insights into policies. Security Copilot can help you understand what your policies are doing in your organization and where they're active. For more information, see Get insights with Security Copilot.
- Summarize alerts in Insider Risk Management. For more information on this and how to access Copilot in Insider Risk Management, see Investigate Insider Risk Management activities.

For more information about what Copilot for Security can do and the different scenarios it supports, read What is Microsoft Security Copilot?

## Microsoft Purview integration with Microsoft Defender XDR

To empower security operations center (SOC) investigations with the right data and user-intent information to better triage and prioritize incidents, we provide data security context into Defender XDR. Teams can manage Microsoft Purview DLP alerts and access IRM user context directly in the Microsoft Defender portal. From the Defender portal, you can:

- View all your DLP and IRM alerts grouped under incidents in the Microsoft Defender XDR incident queue and hunt for compliance logs along with security under Advanced Hunting.
- In-place admin remediation actions on user, file, and device.
- SOC analysts with the required customer-determined permissions can access an insider risk summary of user exfiltration activities that may lead to potential data security incidents.

Read more about Microsoft Purview integration with Microsoft Defender XDR.

## Data Security Investigations

To streamline and simplify this process, organizations have shared their need for a unified, purpose-built solution that enables them to rapidly identify and mitigate risks from sensitive data exposure.

Microsoft Purview Data Security Investigations (DSI) is a new solution that enables data security teams to identify incident-related data, investigate that data with generative AI-powered deep content analysis, and mitigate risk within one unified solution. DSI uncovers key security and sensitive data risks and facilitates secure collaboration between partner teams to mitigate those identified risks, simplifying previously complex, time-consuming tasks. This solution links data security investigations to Defender XDR incidents and Purview Insider Risk Management cases.

With AI at its core, DSI is designed to tackle the most complex, high volume, and time-sensitive data security incidents, redefining how data security teams investigate and mitigate risk.

Read more about Data Security Investigations.

## Data governance and compliance

Microsoft Purview offers a comprehensive suite of solutions designed to help organizations manage, protect, and govern their data across various environments—covering data security, data compliance, and data governance.

Microsoft Purview compliance products like Compliance Manager and Communication Compliance help organizations meet regulatory standards and manage risks. Compliance Manager provides a unified dashboard to assess and improve compliance against standards like GDPR and HIPAA, offering templates, risk assessments, and recommendations. Communication Compliance ensures internal communications adhere to policies using AI to detect non-compliance, helping organizations maintain a compliant communication ecosystem.

Closely related to data compliance is the Microsoft Purview Data Governance suite, which ensures that data is appropriately managed, trusted, and usable for business decision-making. Data governance solutions like Microsoft Purview Data Catalog and Microsoft Purview Data Insights focus on metadata management, data lineage, and data quality monitoring, helping organizations organize and govern data assets effectively. These tools enable organizations to understand where their data comes from, how it's transformed, and ensure that high-quality, accurate data is accessible to users. Effective data governance not only improves compliance but also enhances data discoverability and facilitates better data-driven decision-making.

The interconnectedness between these areas is critical—secure data is more easily governed, and governed data is easier to ensure compliance with, creating a unified approach to protecting and managing data across its entire lifecycle.

# Conclusion

Data security is an imperative in the era of AI. Choosing Microsoft Purview is a major leap toward stronger data security in your organization. Following the strategies in this guide can maximize the full value of your investment.

Securing your organization's data is not just about implementing the right tools, but also about fostering a culture of security awareness and collaboration. By leveraging Microsoft Purview and following the best practices outlined in this guide, you can create a robust data security strategy that protects your valuable assets and supports your business objectives.

Learn more about Microsoft Purview, Information Protection, Purview Data Loss Prevention, and Insider Risk Management. Discover how Microsoft 365 Copilot can be your AI assistant in your mission of stronger data security.

Microsoft Security