

Fortify data security with Microsoft Purview

Start here



How secure is your data?

When it comes to securing data, there are a few questions we always ask our customers. Do you know what kinds of sensitive data you have and where it lives? How are you currently securing sensitive data across all your environments and preventing its loss? And how do you manage insider risks?

We know that data security is hard. You need to secure emails, messages, shared storage, and cloud apps—not to mention all the devices that data is accessed on. Plus, the average company's data footprint keeps growing exponentially. Imagine this: people create 2.5 quintillion bytes of data and send 333.2 billion emails every single day.¹ And with more than 300 million people working remotely all over the world, data security incidents can happen anytime, and anywhere.

It's a conundrum, and today's organizations are struggling with a fragmented solution landscape. On average, organizations use ten or more different tools to meet their data security needs.² However, this approach can be costly, hard to manage—and still leave gaps. A holistic approach to data security is essential.

That's where Microsoft Purview data security solutions can help.

1. Microsoft, "Data Security Index," 2023



59

data security incidents experienced on average in the past year with 20% of them being severe.¹



74%

of organizations experienced an incident with business data in the past year.¹



2.8X

more data security incidents for organizations that employ more security tools (16+) than those with fewer.¹

Introducing Microsoft Purview

With expertise in providing data security solutions to businesses like yours, we recommend addressing data security challenges by implementing multiple controls. These controls include protecting data from unauthorized use across workloads, preventing data loss, and manage insider risk.

Microsoft Purview delivers the various controls you need to create a comprehensive data security solution to help you better understand and mitigate your data security risks.

As part of the solution, you can easily create a holistic, up-to-date map of your data landscape with automated data discovery and sensitive data classification. Available as a single platform, Microsoft Purview helps you govern and protect data across your multicloud, multiplatform data estates while meeting compliance regulations.



Protect sensitive data with Microsoft Purview Information Protection, which offers visibility into where your data lives, classifies sensitive information through comprehensive labeling, and applies built-in encryption to protect your data.



Prevent data loss with Microsoft Purview Data Loss Prevention, which provides controls to prevent data loss or unauthorized use of that data, such as improperly sharing, copying, or printing.



Manage insider risk with Microsoft Purview Insider Risk Management, which provides user context around data and leverages built-in, ready-to-use machine learning models to detect and mitigate the most critical data security risks around that data.

Where do data security incidents come from?

Broadly speaking, users cause data security incidents. Sometimes the intent could be malicious; data and IP theft from departing employees is, unfortunately, not uncommon. Other times, it's inadvertent exposure. For instance, an employee might accidentally send a document to the wrong person, or leave it unprotected.

But regardless of when and how that data was exposed the larger issue is that most organizations have no visibility into how their data is being used and accessed. And without visibility, you just don't know what your risk is.



Protect sensitive data with Microsoft Purview Information Protection

Securing data requires that you understand and discover where it lives in your organization. Therefore, you need a solution that gives you visibility across your entire data estate—whether that’s on-premises, in the cloud, hybrid, or multi-cloud.

With Microsoft Purview Information Protection, you’ll get a unified view of structured and unstructured data across your entire data estate. This view includes the volume, type, and location of sensitive information. From here, you can understand your data estate better so you can start labeling your data and then apply controls consistently across data types.

Microsoft Purview Information Protection also helps safeguard data throughout its lifecycle, with persistent labeling and encryption built into productivity tools. And that’s not all; because organizations need to protect data where people work from multiple environments, the visibility and protection of sensitive information are extended across your entire data estate, whether on-premises, hybrid, or cloud.



Let us help you protect your information using Microsoft Purview, so you can:

- Discover and classify data at scale using automation and machine-learning.
- Safeguard data throughout its lifecycle with labeling and encryption built into productivity tools.
- Extend protection across environments to help safeguard data wherever it lives.



Prevent data loss with Microsoft Purview Data Loss Prevention

People work remotely. Teams collaborate nationally and internationally. The average worker is using not just a computer, but also mobile devices. They're working across apps too, in hybrid models. In short, your data is everywhere.

That's why it's imperative to secure information beyond the document level by ensuring all your egress channels prevent exfiltration and unauthorized use. But it's also important not to lock down data too much, because productivity plummets when users can't access the data they need. How do you solve these challenges? Enter Microsoft Purview Data Loss Prevention (DLP).

This comprehensive solution works across the different applications, services, and devices where sensitive data is stored, used or shared, whether it's Microsoft-native platforms or non-Microsoft services and apps. Because Microsoft Purview DLP is cloud-native, you don't need to install costly on-premises infrastructure or agents. Additionally, it can help you increase efficiency, because you can consolidate the disparate DLP policies across various workloads, such as email, endpoints, and apps, with a unified policy.



Microsoft Purview can help you prevent data loss because you can:

- **Eliminate the need for on-premises infrastructure and agents** with a cloud-native solution that builds protection into Microsoft 365 apps, services, and Windows endpoints.
- **Balance protection and productivity** with granular policy controls and manage all workloads from a single location.
- **Take an integrated approach to data** by leveraging native integration with data classification, user activity insights, and security incident management.



Manage insider risk with Microsoft Purview Insider Risk Management

Data doesn't move itself; people move data. In other words, data breaches are commonly caused by internal actors, whether it's departing employees exfiltrating data, malicious data theft or inadvertent overexposure that may lead to potential security incidents.

The key is understanding how and why people are accessing data; when you understand the context, you can identify the potential data security risks and risky user activities that can lead to incidents. Organizations need a holistic approach to managing insider risk by bringing together the right people, processes, training, and tools.

Microsoft Purview Insider Risk Management correlates various signals to identify potential malicious or inadvertent insider risks. These risks include IP theft, data leakage, and security violations. Insider Risk Management provides more than 100 ready-to-use indicators and machine learning models to help you quickly detect critical risks. Built with privacy-by-design principles, users are pseudonymized by default, and role-based access controls and audit logs are in place to help ensure user-level privacy.



We have rich knowledge in deploying Microsoft Purview so you can:

- **Put privacy first by protecting user trust and building a holistic insider risk program** with pseudonymization and strong privacy controls.
- **Simplify data security by identifying hidden risks** with 100+ built-in and ready-to-use machine-learning models and indicators, requiring no endpoint agents.
- **Accelerate and expedite mitigation** with enriched investigations and Adaptive Protection that enforce effective controls dynamically.

Fortify your data security with an integrative approach

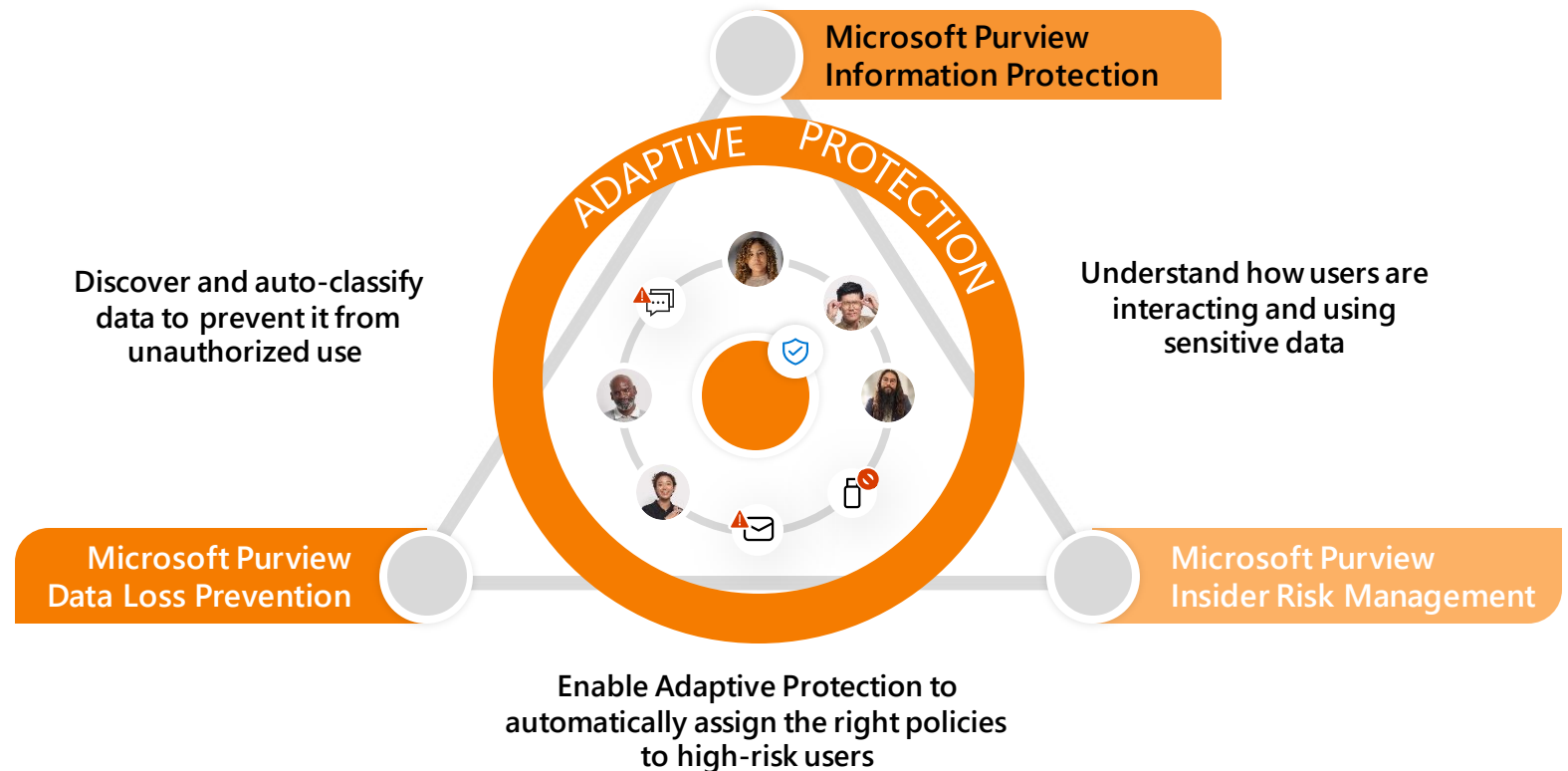
As a trusted technology advisor to businesses like yours, we recommend Microsoft Purview. Here's why. First, it strengthens data security by offering Information Protection, Insider Risk Management, Data Loss Prevention, and Adaptive Protection in a single unified platform. Secondly—and more importantly—these four different layers of protection don't just help to secure data from potential data security incidents, they also work together as a single platform to strengthen your data security.

Think of it this way. If you use Information Protection and Data Loss Prevention together, you can discover and auto-classify data to prevent unauthorized use.

Similarly, using Information Protection and Insider Risk Management together helps you understand the user intent around sensitive data to identify the most critical data risks in your organization.

If you use Insider Risk Management and Data Loss Prevention, you can enable what we call "Adaptive Protection," which assigns appropriate DLP policies based on user's risk levels. With Adaptive

Protection, you can understand the context in which users are accessing information and how they're interacting with it. Then you can calculate and assign appropriate risk levels, and automatically tailor the appropriate DLP controls based on a user's risk levels. And when you put them all together, Microsoft Purview helps you strengthen your data security.



Get ahead of data security incidents with Adaptive Protection

In today's modern workplace, data security risk is dynamic. The type of content changes, just as the people who interact with that data shifts. What people do with data changes too. That means data security is even more complicated to manage. Unfortunately, broad, static policies no longer work; at one extreme, they run the risk of not doing anything and on the other, they can overprotect data to the point that people can't get anything done at all. Far too often, admins scramble to manually adjust policy scope and triage alerts to identify critical risks.

Many of the businesses we work with struggle with these challenges, which is why we regularly recommend Microsoft Purview. It includes Adaptive Protection, which helps you solve these issues by addressing most critical risks dynamically. With Adaptive Protection, built-in indicators and machine learning models continuously detect and mitigate the most critical risks for both content and users. It helps you gain a better understanding of risk by using Insider Risk Management to understand user context, and gain insights into how that data is being used.

Then, Adaptive Protection automatically adjusts the right level of mitigation controls based on the risks detected. For instance, high-risk users can be scoped in a stricter control while low-risk users can work as usual. And it's constantly adjusting; the control can be dialed up and down when user's risk levels change.

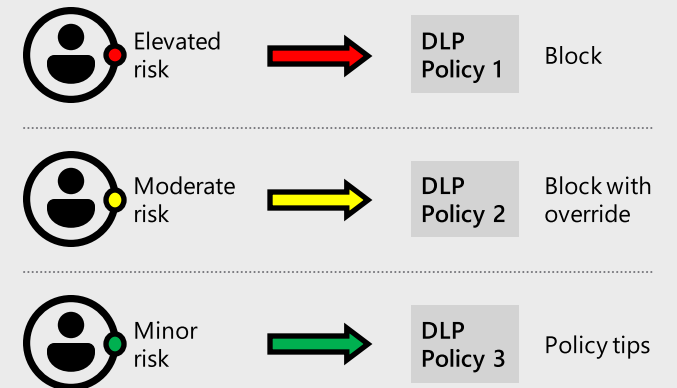
As a result, Adaptive Protection not only helps reduce the security team's workload, but also makes DLP more effective by continuously optimizing policies.

Insider Risk Management

Detect risky users and assign risk levels

Data Loss Prevention

Dynamically apply preventative controls



Strengthen your data security today!

In today's world, there are no geographical limits to sensitive data; it travels across people, places, and devices around the world. We know that the key to data security is securing that data anywhere it happens to go—and we want to help you build a data security strategy for today's global, collaborative business landscape.

We have a robust security practice, along with the expertise you need to assist you with every stage of your security strategy. Whether you need an assessment of your current environment, help navigating licensing structures, deployment, customization, training or managed services, we've got you covered.

Let us help you get started.

Contact us for more details.

Kapalins Cybersecurity | Email: enquiry@kapalins.com

