# Data Security Engagement

**83% of organizations experience more than one data breach in their lifetime.**

The cybersecurity landscape is rapidly changing, with new risks emerging alongside our expanding digital presence. According to research, 20% of data breaches are attributed to internal actors, with an average cost of €4.4M in cases involving malicious insiders. While external threats once dominated, data leaks and internal theft are now prominent vulnerabilities that organizations can no longer ignore.

Data security incidents can happen anytime anywhere.

## Intelligently investigate and take action on data security risks

Proactively detecting, investigating, and mitigating data security risks is essential for maintaining trust, ensuring workplace safety, and protecting both company assets and the privacy of employees and customers. The Data Security Engagement offers the critical insights necessary to comprehend the data security, privacy, and compliance risks within your organization.

As your business-critical data expands and your workforce shifts to remote work, having an integrated approach to mitigating and controlling privacy and regulatory risks is more important than ever.

## What can you expect?

By the end of this engagement, our experts will provide you with a

- ☑ A Security Check report that includes findings and insights from the automated discovery process.
- ☑ A list of recommendations and actionable next steps that will help mitigate the identified risks.
- ☑ Clear look into Microsoft's approach to data security and mitigating and controlling insider risks.
- ☑ Optional Compliance Manager Tenant Assessment report with suggestions and top key improvement actions.
- ☑ Set of long-term recommendations on your compliance strategy, with key initiatives and tactical next steps.

Microsoft Funding Available*

# Data Security Engagement

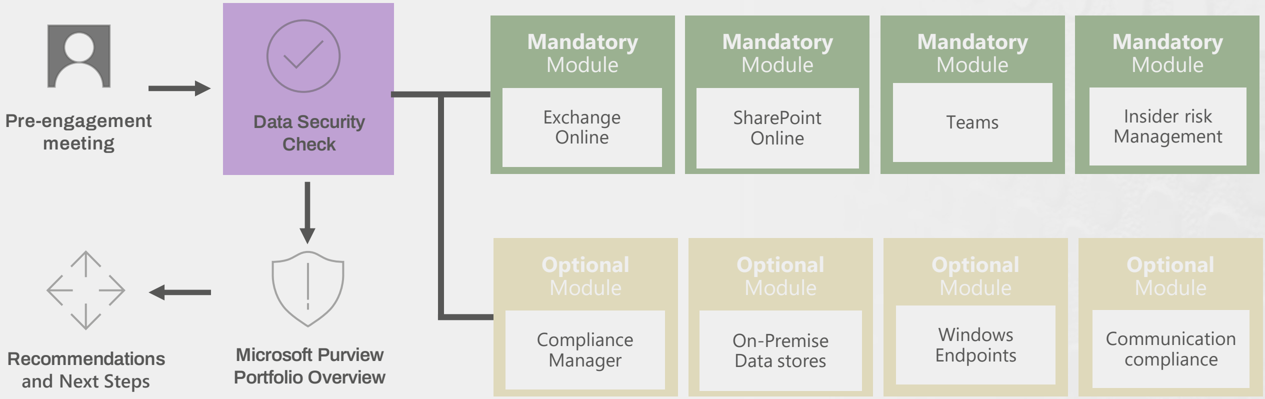
The cornerstone of our Data Security Engagement is the Data Security Check, designed to identify potential risks that could jeopardize your organization. As a key element of this engagement, the Data Security Check utilizes Microsoft Purview tools and services through an automated process to:

- Discover data that is stored in the Microsoft 365 Cloud and analyse it for the presence of artifacts that may impose data security risks to the organisation.

- Analyse user behavior for events that impose a risk to the customers organisation. These vulnerabilities range from the loss of intellectual property to workplace harassment and more.

The Data Security Check is built around the common Microsoft 365 services and the associated data repositories that organizations rely on. At its core, it analyzes user behavior and scans data repositories, including those related to email, collaboration, and document storage.

Optional modules can expand the Data Security Check to cover on-premises data repositories, Windows 10/11 endpoints, and more. All activities follow a unified framework, enabling you to identify the risks present in your organization and create a strategic roadmap to mitigate those risks and safeguard your company's information.



* Funding subject to Microsoft's terms and conditions