
CLOUD/LIFE.
Data Protection
/for Copilot
Member of
Microsoft Intelligent
Security Association
Microsoft Security

Data is everywhere

Protect your data, secure AI

While copilot wins back our precious time and makes our lives easier, it also comes with new responsibilities. Copilot means new data is generated more quickly, insights in scattered data is easier and AI & employees can access sensitive information within seconds, which can lead to data breaches and data theft.

User data

Data on devices

Data from Apps

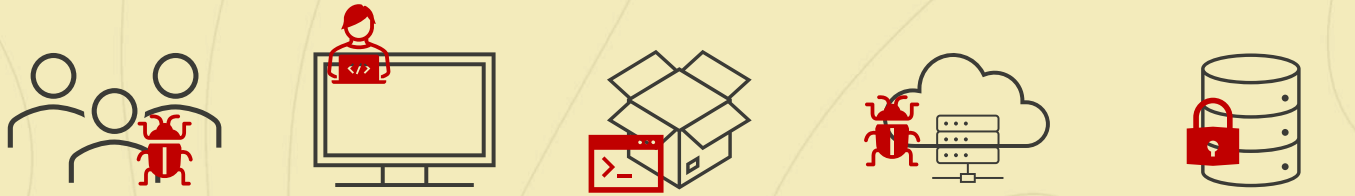
Data in infrastructure

Scattered data / hybrid

The risks are everywhere, too

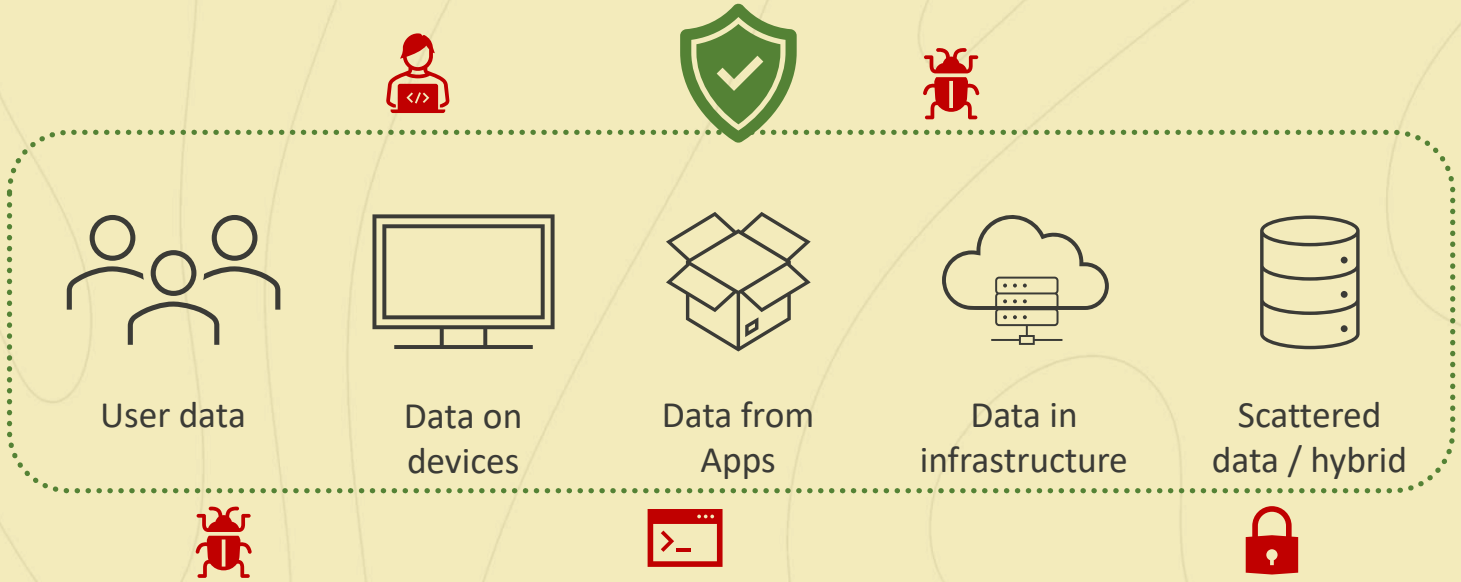
Protect your data, secure AI
The complexity and diversity of risks associated with data, particularly when processed and stored across various locations and workloads, increase exponentially with Copilot integration.

But it doesn’t have to be.



User data | Data on devices | Data from Apps | Data in infrastructure | Scattered data / hybrid

Data Protection for Copilot



Data Protection for Copilot – Assessment (1 day)

What it does - Solutions Summary

Data Loss Prevention
- Check if there are DLP Policies in place
- Check for customized or default DLP Policies for Company Sensitive Information, ePHI (USA, HIPAA / HITECH Act), Personally Identifiable Information (worldwide), Sensitive Financial Information (worldwide), GDPR (EU), NIS2 (EU), Government Data (worldwide, such as ITIN, SIN, SSN, INSEE, CNI, etc.)
- Check if policies are published organization-wide

Microsoft Information Protection
- Check if there are MIP labels in place
- Check if labels are published organization-wide
- Check if labels have encryption enabled
- Check if auto labeling is available and, if yes, enabled
- Check if labels are published to most important applicable SKU's (SPO, EXO, Teams, OfB)

- **Data Lifecycle Management**
- Check if there are retention policies in place
- Check if retention policies are applied to at least Exchange Online (where copilot interaction is stored in hidden folder)
- Check for integration with eDiscovery

Communication Compliance
- Check for internal and external communications configuration
- Check on interactions with Microsoft Copilot configuration

Insider Risk Management
- Check for policies for (departing) employee data theft
- Check if there are policies for data breaches
- Check if alerting has been configured
- Check if alerting works

eDiscovery
- Check if eDiscovery (Premium) is available and used
- Check if cases are being made
- Check for the ability to manage the end-to-end workflow to preserve, collect, review, analyze, and export content that's responsive to the organization's internal and external potential investigations.

Audit
- Check if Alert Policies on activities that are indicators of a potential security issue or data breaches are active.

Data Protection for Copilot – Deployment (1 week)

What it does - Deployment Summary

Data Loss Prevention
- Configures and deploys applicable DLP Policies per geographic, e.g. for Company Sensitive Information, ePHI (USA, HIPAA / HITECH Act), Personally Identifiable Information (worldwide), Sensitive Financial Information (worldwide), GDPR (EU), NIS2 (EU), Government Data (worldwide, such as ITIN, SIN, SSN, INSEE, CNI, etc.)
- Configures Policies to run in audit-mode to not be intrusive
- Configures and deploys customized policies (on request)

Microsoft Information Protection
- Configures and deploys standard set of MIP labels (public, general, confidential (internal / external), secret (internal / external))
- Configures auto-labeling / manual labeling (depending on available license and preference of organization)

- **Data Lifecycle Management**
- Configures and deploys retention policy for Exchange Online

Communication Compliance
- Configures Communication Compliance
- Configures and provides e-learning on the usage of Communication Compliance to monitor Copilot usage

Insider Risk Management
- Configures policies for (departing) employee data theft
- Confgures policies for data breaches
- Configures alerting

eDiscovery
- Configures eDiscovery
- Configures and provides e-learning on the usage of eDiscovery to Configures cases for search and how to place holds for legal

Audit
- Configures Alert Policies on activities that are indicators of a potential security issue or data breaches.

CLOUD/LIFE. | Microsoft Advanced Specialization Partner

www.securityfor.ai

Member of
Microsoft Intelligent Security Association

Microsoft Security