Microsoft Security

PSM
TECHNOLOGY | TALENT

UPDATE before use

Data Security Engagement

Pre-engagement meeting

<your name>
<your role>
PSM Partners
sales@psmpartners.com
312-940-7830

Microsoft Security

PSM
TECHNOLOGY | TALENT

UPDATE before use

Data Security Engagement

Engagement kick-off meeting

<your name>
<your role>
PSM Partners
sales@psmpartners.com
312-940-7830

Disclaimer

The Data Security Engagement provides a summary of an organization's data protection and compliance stature and recommendations to improve data protection and compliance.

The information, results, and scoring provided through the Data Security Engagement are recommendations and provided for general informational purposes only. They do not constitute legal advice, certifications, or guarantees regarding regulatory compliance; it is up to each organization to evaluate the effectiveness of these recommendations in their respective regulatory environment prior to implementation. Organizations should consult with their own legal professionals to determine how standards or regulations apply to their organization and how to best ensure compliance.

We hope the Data Security Engagement helps identify technologies and additional steps that organizations can implement to simplify their compliance efforts.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS Data Security Engagement. Microsoft disclaims any conditions, express or implied, or other terms that use of the Microsoft products or services will ensure the organization's compliance with regulations or standards. This Data Security Engagement toolkit is provided "as-is." Information and recommendations expressed in the Data Security Engagement toolkit may change without notice.

The Data Security Engagement toolkit does not provide the user with any legal rights to any intellectual property in any Microsoft product or service. Use of the tool is for internal, reference purposes only; however, Microsoft partners may distribute the Data Security Engagement toolkit to their customers for such customers' internal, reference purposes only. Any distribution of the Data Security Engagement toolkit by a Microsoft partner to its customers must include terms consistent with those set forth in this disclaimer.

Agenda

Introduction

Data Security
Why it is important to know and protect your data

The Data Security Engagement
Objectives, scoping, and deliverables

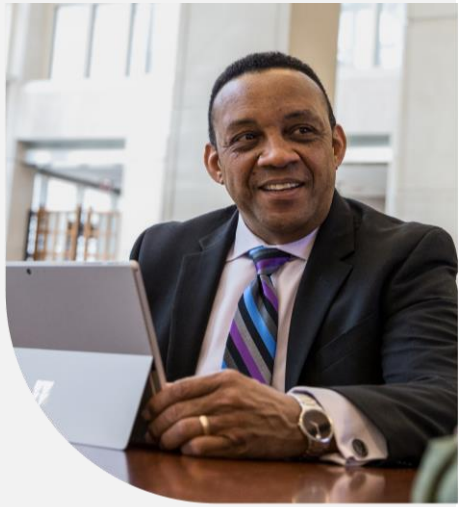
The Data Security Check
Identifying data security risks in your organizational data

The engagement
Approach, timelines, and governance

Q&A

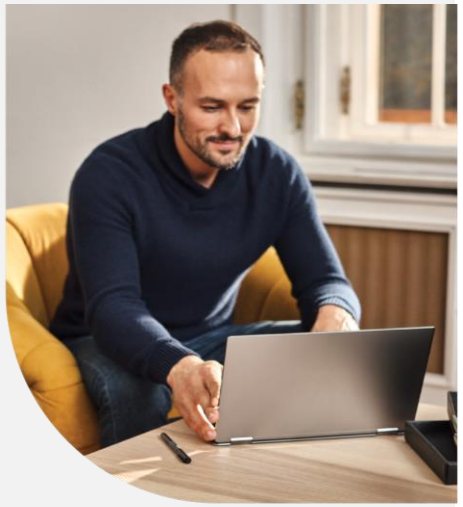
Team introductions

Activity



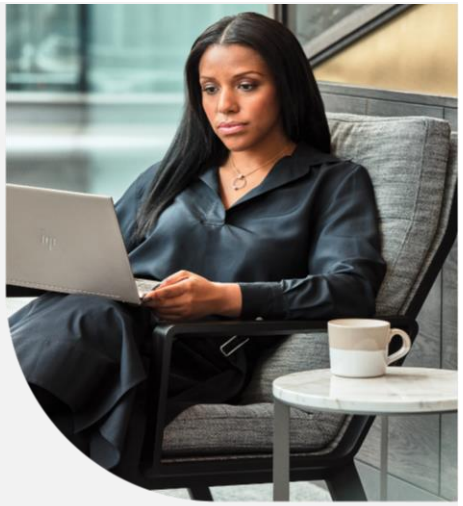
Name

Please share your name and where are you based.



Role

Please share your role in the company, which business unit or team you are part of, what other roles you have had. (Internal/External)



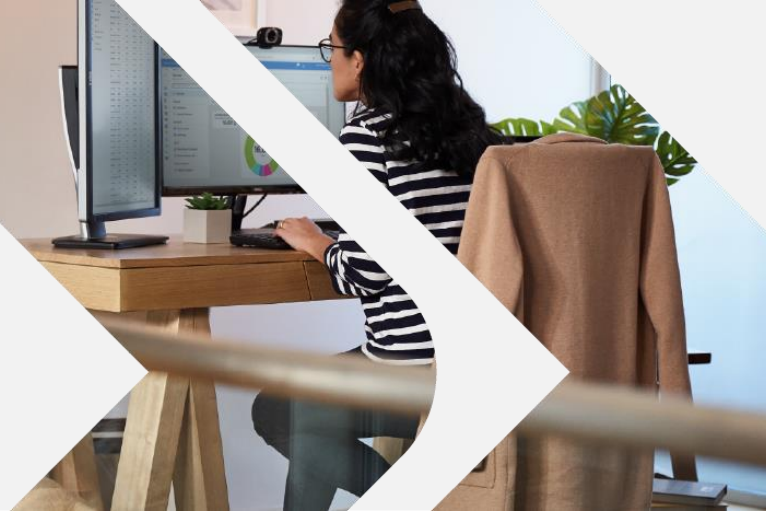
Expectations

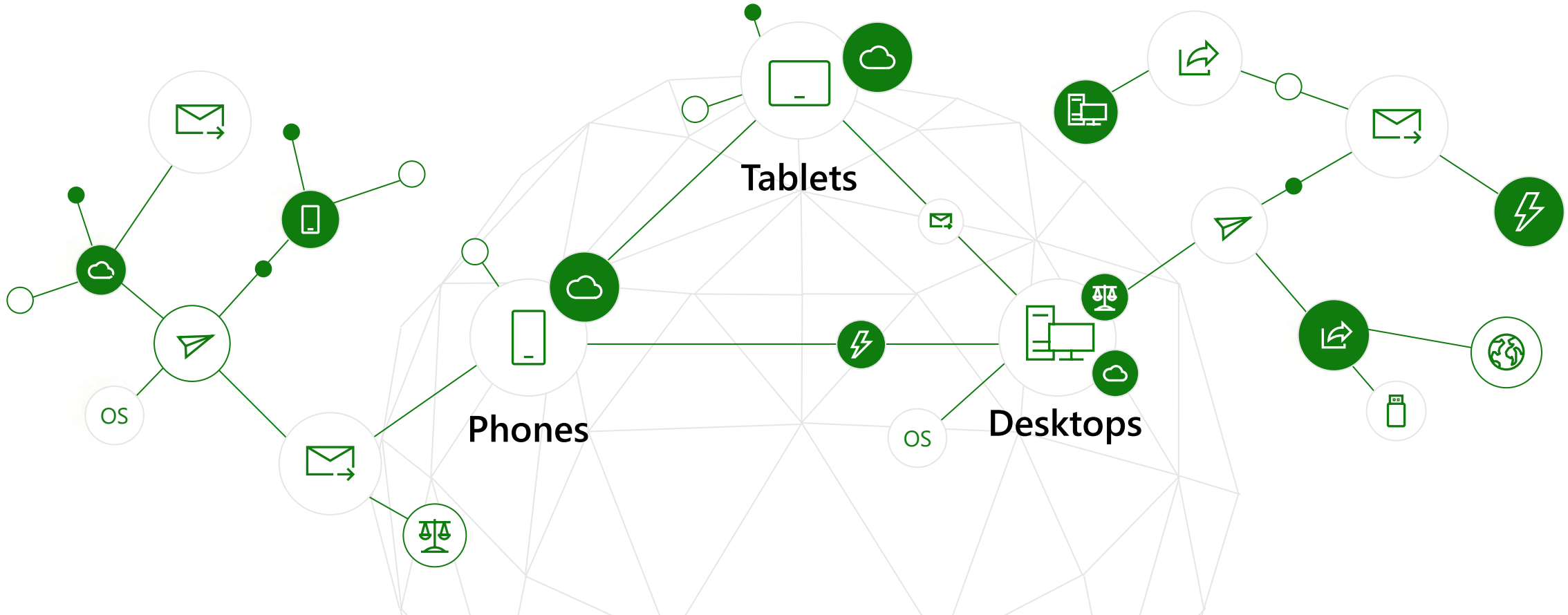
Please share your expectations of the Data Security Engagement.

Data Security

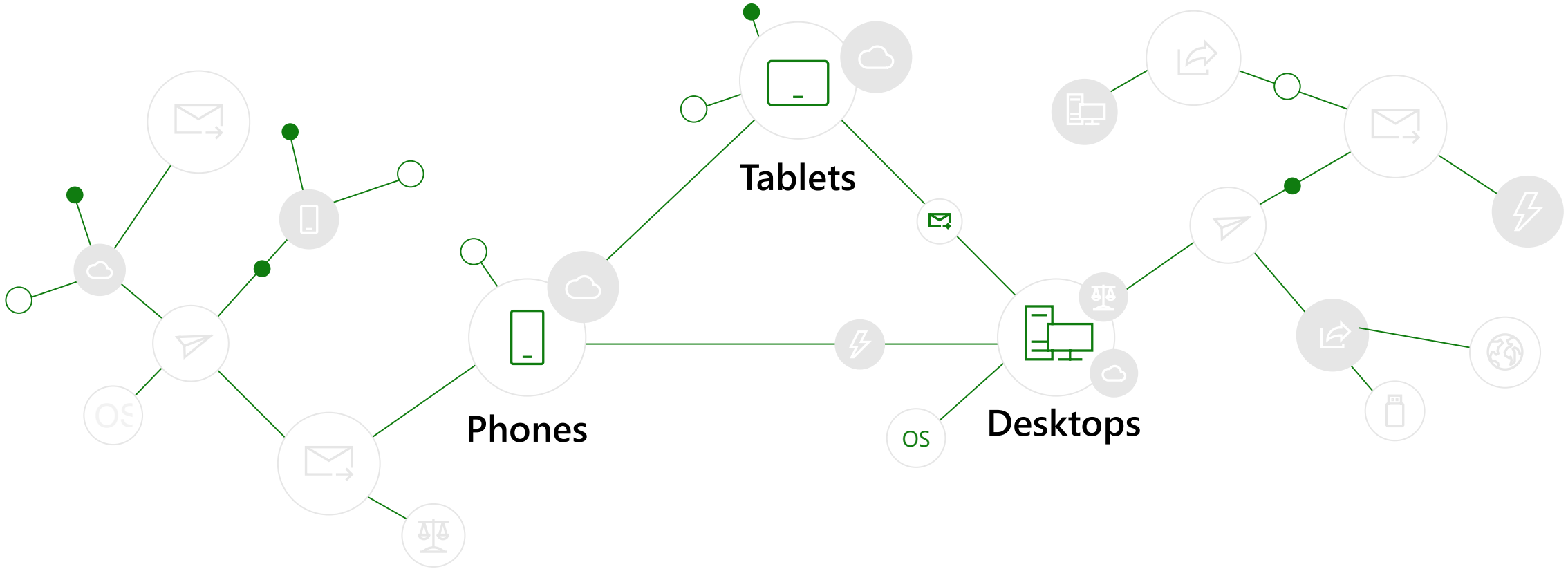
Why it is important to know and protect your data

Data usage is evolving and complex, moving outside of the traditional borders of business





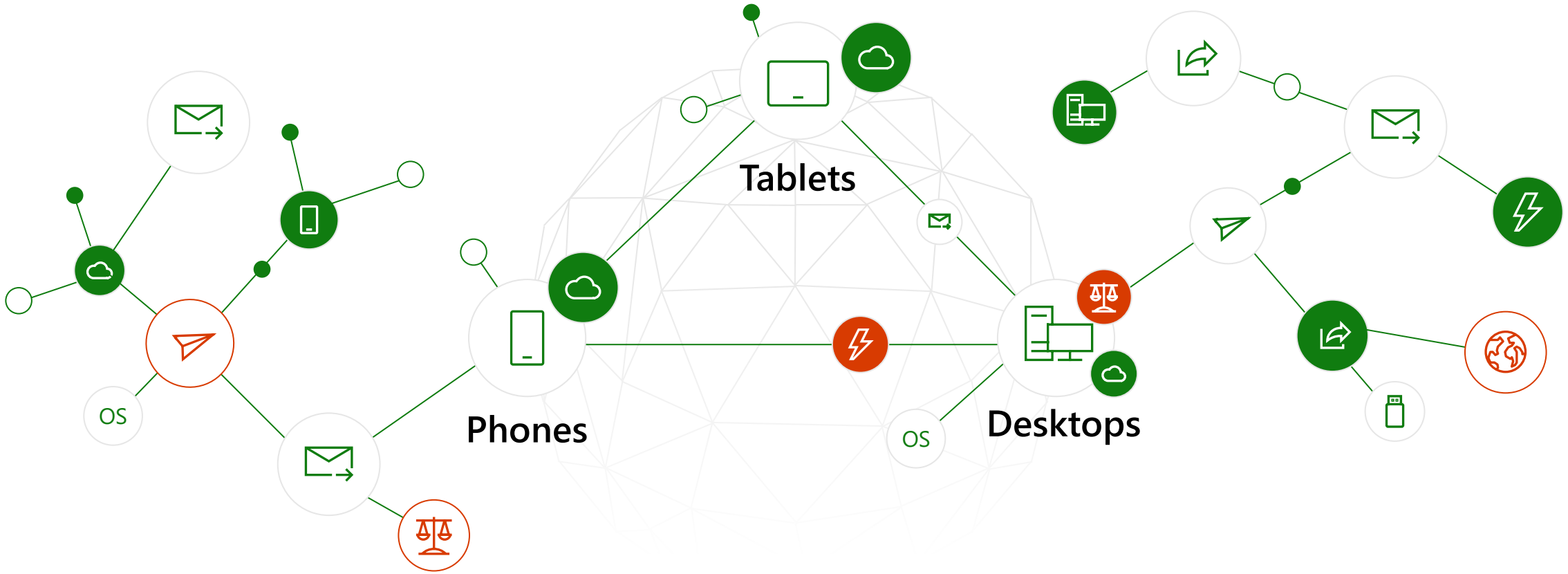
Organizations lack visibility into their data estate



Year over year, the amount of data available doubles

93% of data within an organization is dark

The landscape is fragmented, creating risks



Exposure gap

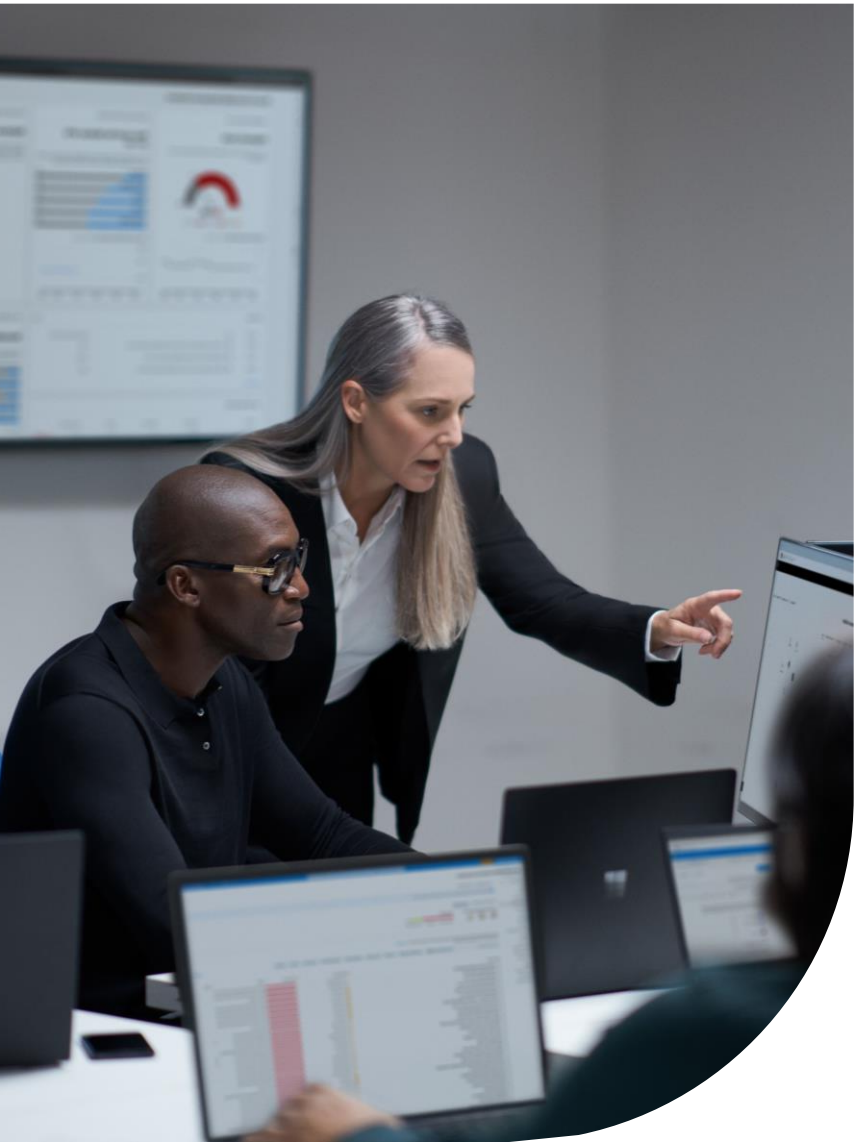
Missed regulatory requirements

Impeded digital transformation

Failed audits

Brand reputation at risk

Data Security is critical for strong cybersecurity!



Data security incidents are widespread	**83%**	of organizations experience more than one data breach in their lifetime[1]
Insiders account for 20% of data breaches, adding to costs	**$15.4M**	Total average cost of activities to resolve insider threats over 12 month period[2]
Organizations are concerned about data leak in Generative AI	**80%+**	of leaders cited leakage of sensitive data as their main concern around adopting Generative AI[3]

Source:

1,2 Microsoft Data Security Index report

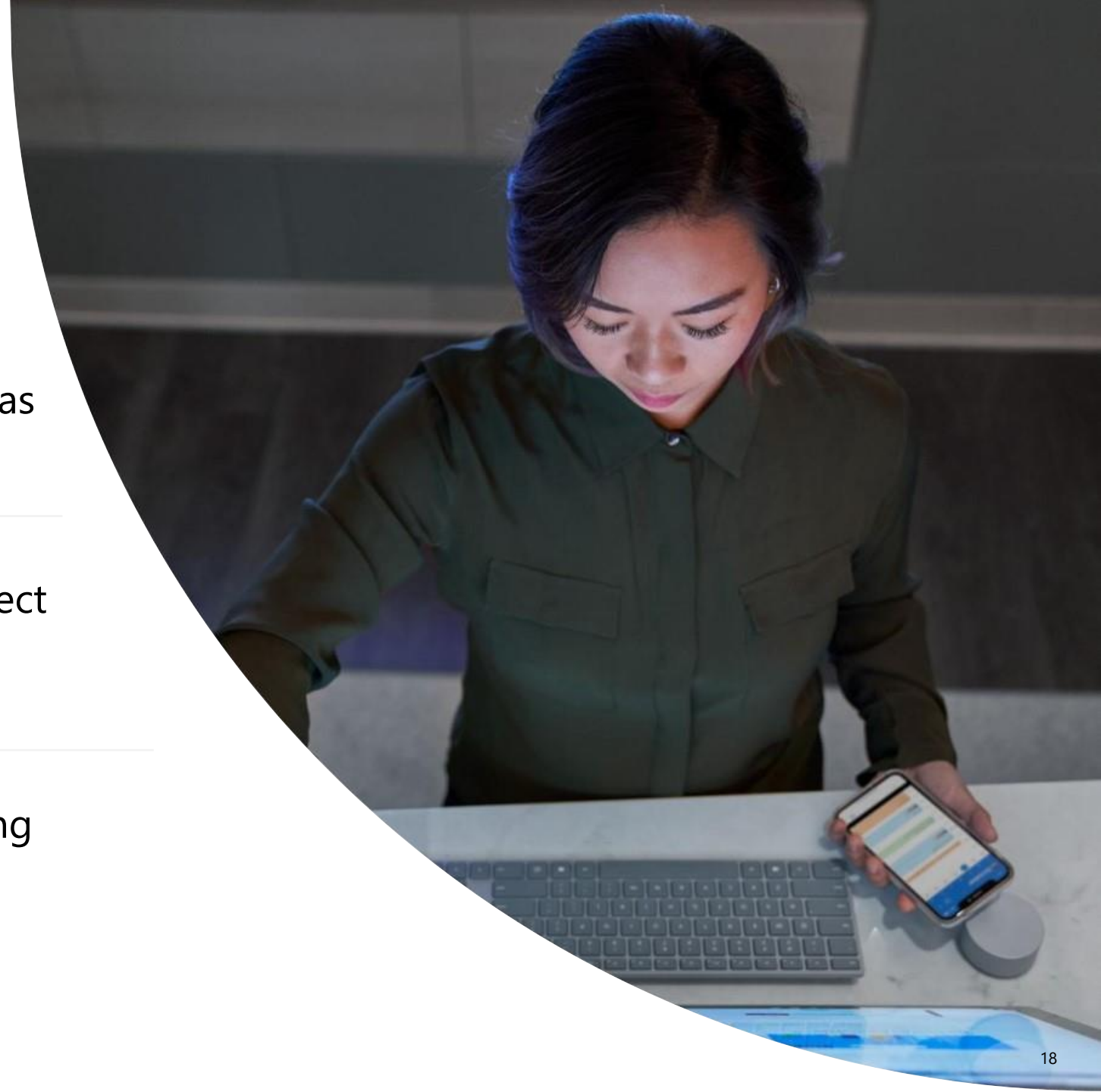
3 First Annual Generative AI Study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400

Let’s hear from you

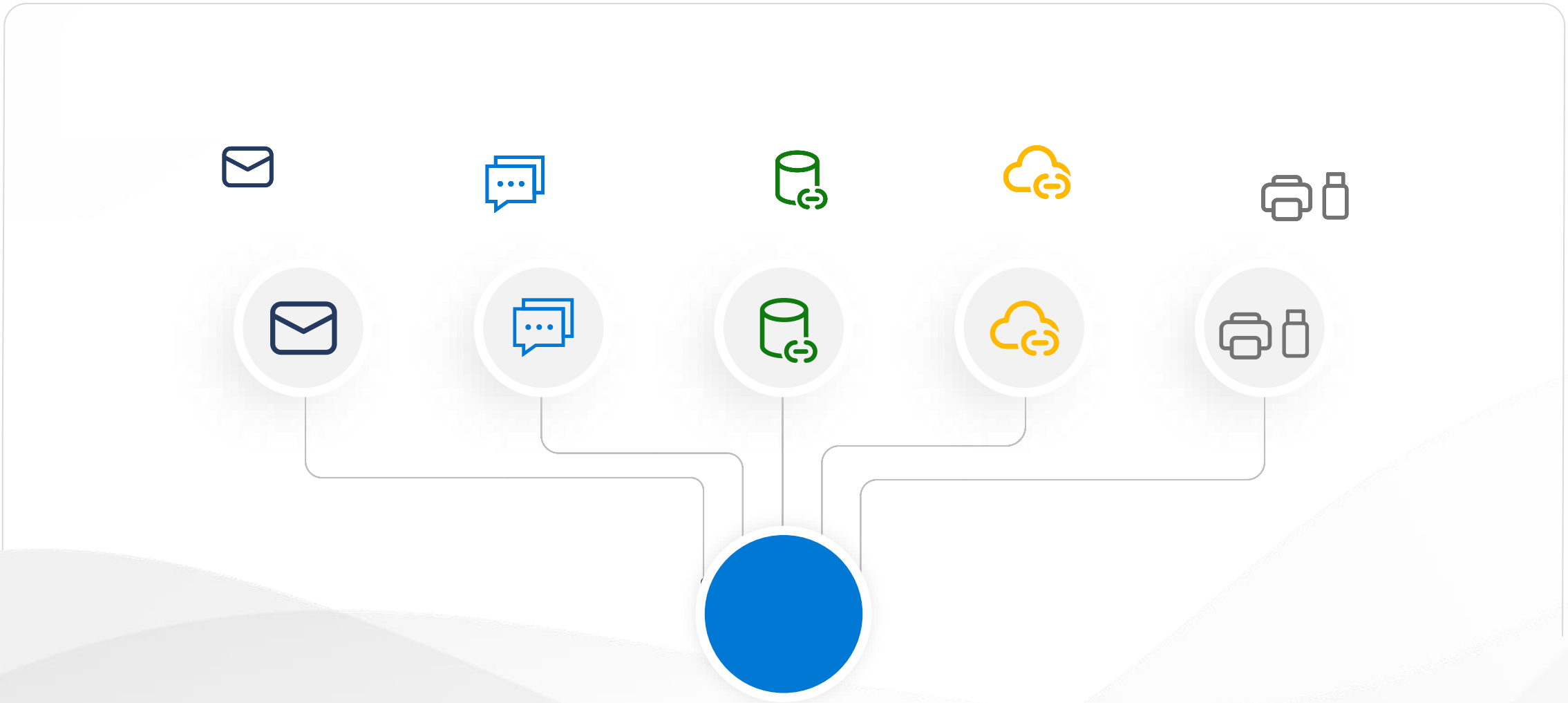
Does your organization know the types of sensitive information it has and where it lives?

How does your organization protect sensitive data across your environments?

How is your organization preparing for the digital transformation powered by generative AI?



Your data footprint is growing rapidly



Why is data security so difficult?

Data security incidents can happen anytime anywhere

Data doesn't move itself; people move data

Email

Received a confidential file via email

Messages

Shared a copy of the file with a few colleagues via Teams

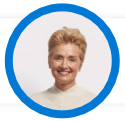
Cloud apps

Uploaded a copy to a personal Dropbox account to share with external vendors

Devices

Downloaded a copy of the file to devices to work offline

Inadvertent



Data exposure → Data leak → Data hoarding

Shared storage

Downloaded and deleted an unusual volume of confidential files from SharePoint

Email

Sent a copy of one file to an external recipient via email

Cloud apps

Uploaded two confidential files to a personal Dropbox account

Devices

Printed one confidential file

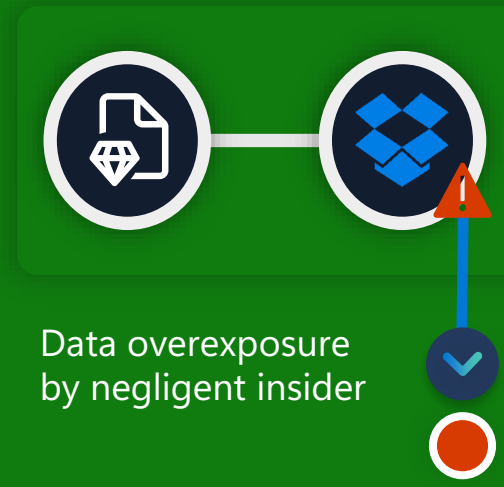
Saved three confidential files to a USB

Malicious

Data sabotage → Data theft → Data theft → Data theft

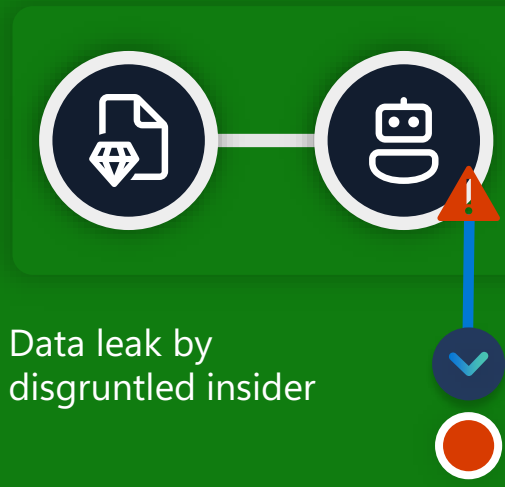
Generative AI is reshaping the world but there are associated data security risks..

User creates document without proper access controls making it easy for other users to reference it in Copilot



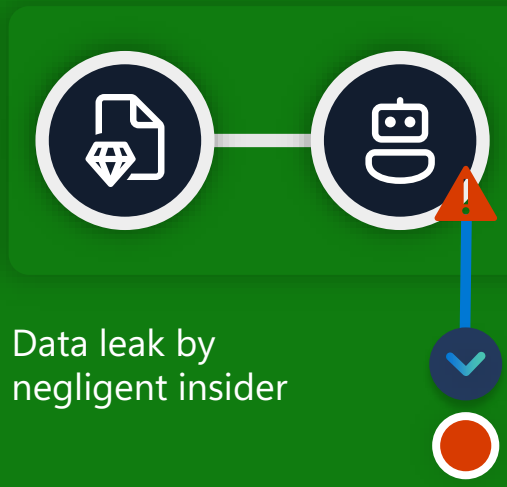
Data overexposure by negligent insider

User asks generative AI to find information on a secret project and leaks it to the press for personal gain



Data leak by disgruntled insider

User negligently shares sensitive data in consumer generative AI apps



Data leak by negligent insider

A story of negligent users exposing corporate data

Trusted employees, John and Alice inadvertently expose sensitive information

John and Alice

Manager and Project Manager at Contoso, a Fortune 500 company

John is working on a confidential project called Project Obsidian which only a few Contoso employees know about.

Alice, overhears about Project Obsidian and asks Copilot for M365 to find information about it and Copilot provides her with a summary with the link to the document.

Out of curiosity, Alice wants to see what ChatGPT would summarize, so she pastes the content of the file in ChatGPT.

Contoso did not have policies to automatically detect and label Project Obsidian documents

Copilot was able to find the information for Alice since the file had open permissions

Contoso did not have DLP policies to prevent leak of sensitive data. The information became part of the ChatGPT 's training data

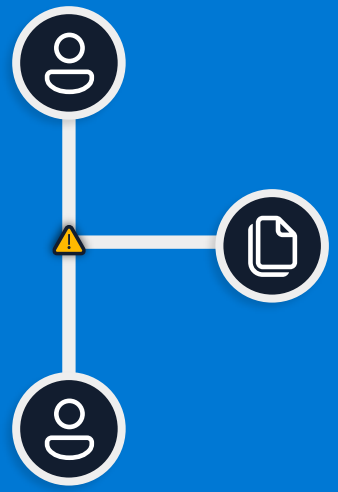
Sensitive data was exposed

Impact

The information about the Project Obsidian leaked in the public, resulting in bad PR for Contoso and there was a significant impact to Contoso's share price.

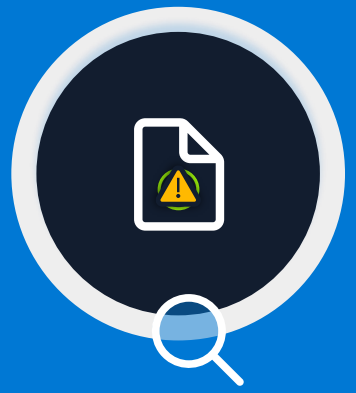
To secure their data, organizations need to…

Discover hidden risks to data wherever it lives or travels

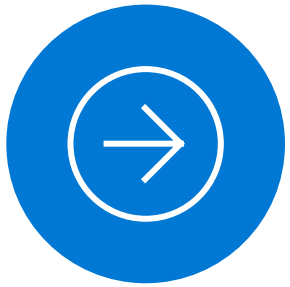


Protect and prevent data loss across your data estate

Quickly investigate and respond to data security incidents



Balance data security and productivity



But where to start and how?

The Data Security Engagement

Identifying data security risks in organizational data and understanding how to mitigate them

How the Data Security Engagement can help

Understand the risks of *Dark Organizational Data*
Discuss and understand the hidden data security risks of dark data and how to mitigate.

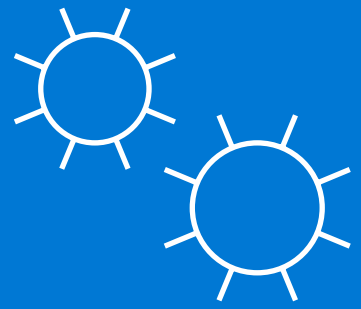
Understand the risks organizational insiders may impose
Learn how to identify and respond to insider actions and behaviors that can impose risks on the organization.

Assess the customers Microsoft 365 environment
Assess against a set of controls for key regulations and standards for data protection and general data governance.

Analyze and report
Analyze the findings and associated data security risks. Provide insight and highlight most impactful.

Learn about tools and services that can mitigate risks
How can cloud services help and what does this mean for the end user.

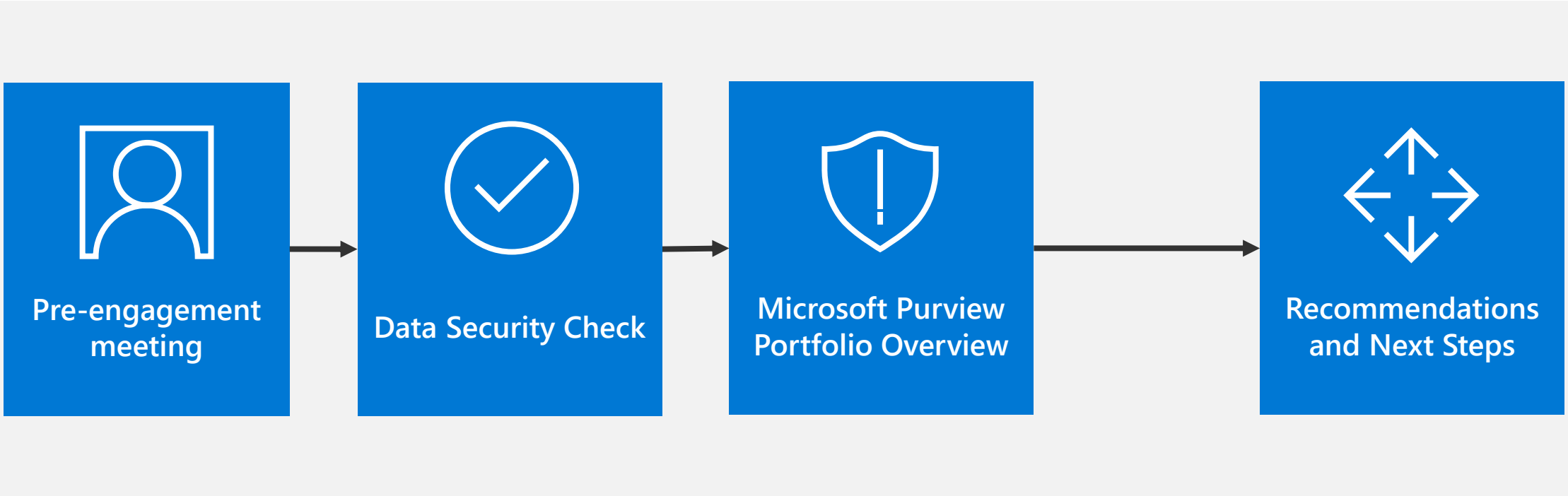
Recommendations and next steps
Provide recommendations for risk mitigation and define actionable next steps



Engagement Objectives

Data Security Engagement

The Data Security Engagement



Defining the engagement team

Roles and responsibilities

Executive Sponsor
Owner of the business case, project alignment to organization strategic and portfolio

IT Architect
Overall architectural guidance and insights

Compliance Architect
Architectural guidance and insights into compliance policies and standards

Security Architect
Architectural guidance and insights into security policies and standards

Compliance & Security administrators
Technical guidance and insights into currently deployed security and compliance controls

Microsoft 365 tenant administrators
Insight into existing Microsoft 365 usage
Access to tenant and service configuration

Activity

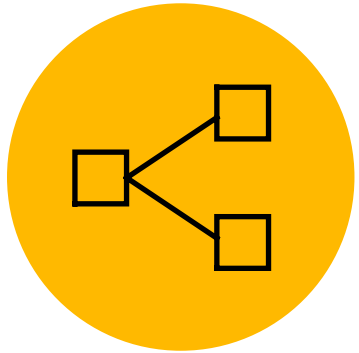
Document the engagement team

Defining the engagement team

Activity

Name	Role	E-mail	Phone	Organization
	Executive sponsor			Customer
	IT Architect			Customer
	Compliance Architect			Customer
	Security Architect			Customer
	Compliance Administrator			Customer
	Security Administrator			Customer
	Microsoft 365 Tenant administrator			Customer
	Delivery Architect / Consultant			Partner
	Security Consultant			

Your responsibilities



Provide access to key resources

Subject Matter Experts are needed to implement, configure, and enable required cloud discovery services.

Provide an executive sponsor

A single executive sponsor is required to oversee and support the engagement.

Data Security Check

Identifying data security
risks in your data

What is the Data Security check?

“An automated Process that leverages Microsoft Purview services to look for customer relevant sensitive information and risky user behavior that may impose a data security risk.”

The Data Security Check

Enable and Configure

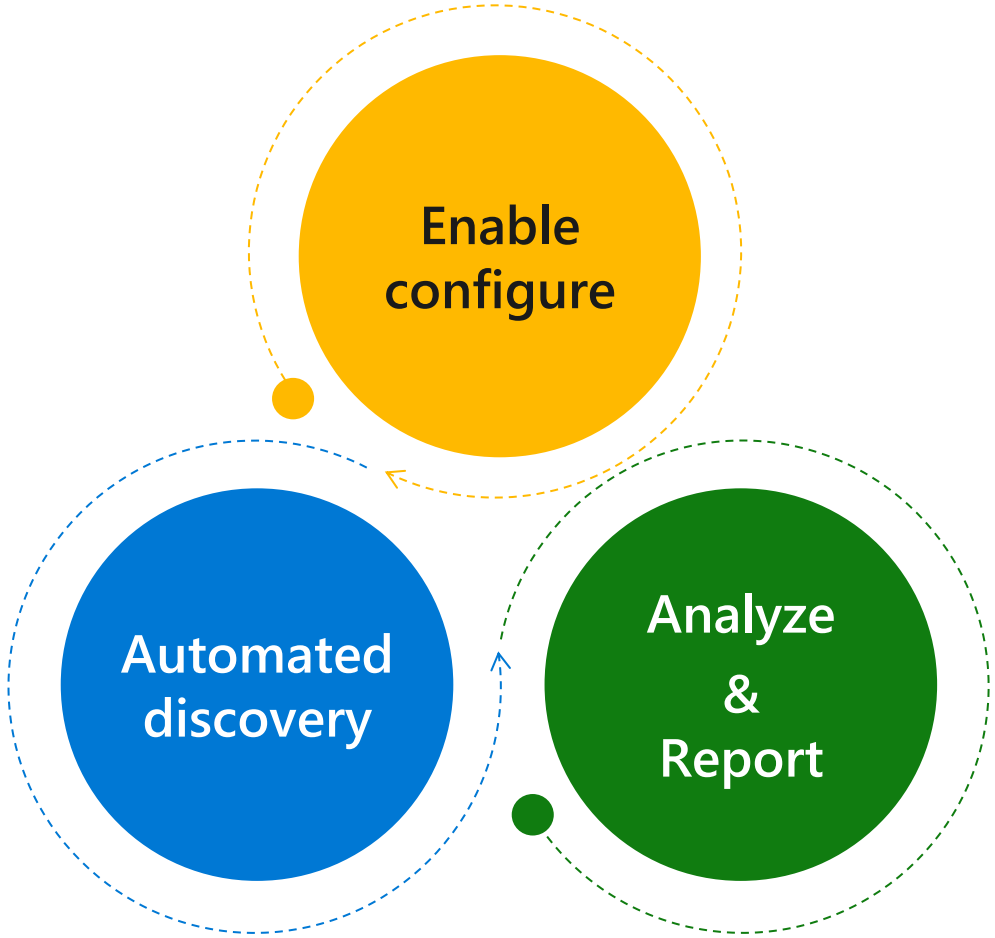
Enable the services for **automated discovery, configure** the **search artifacts**

Automated Discovery

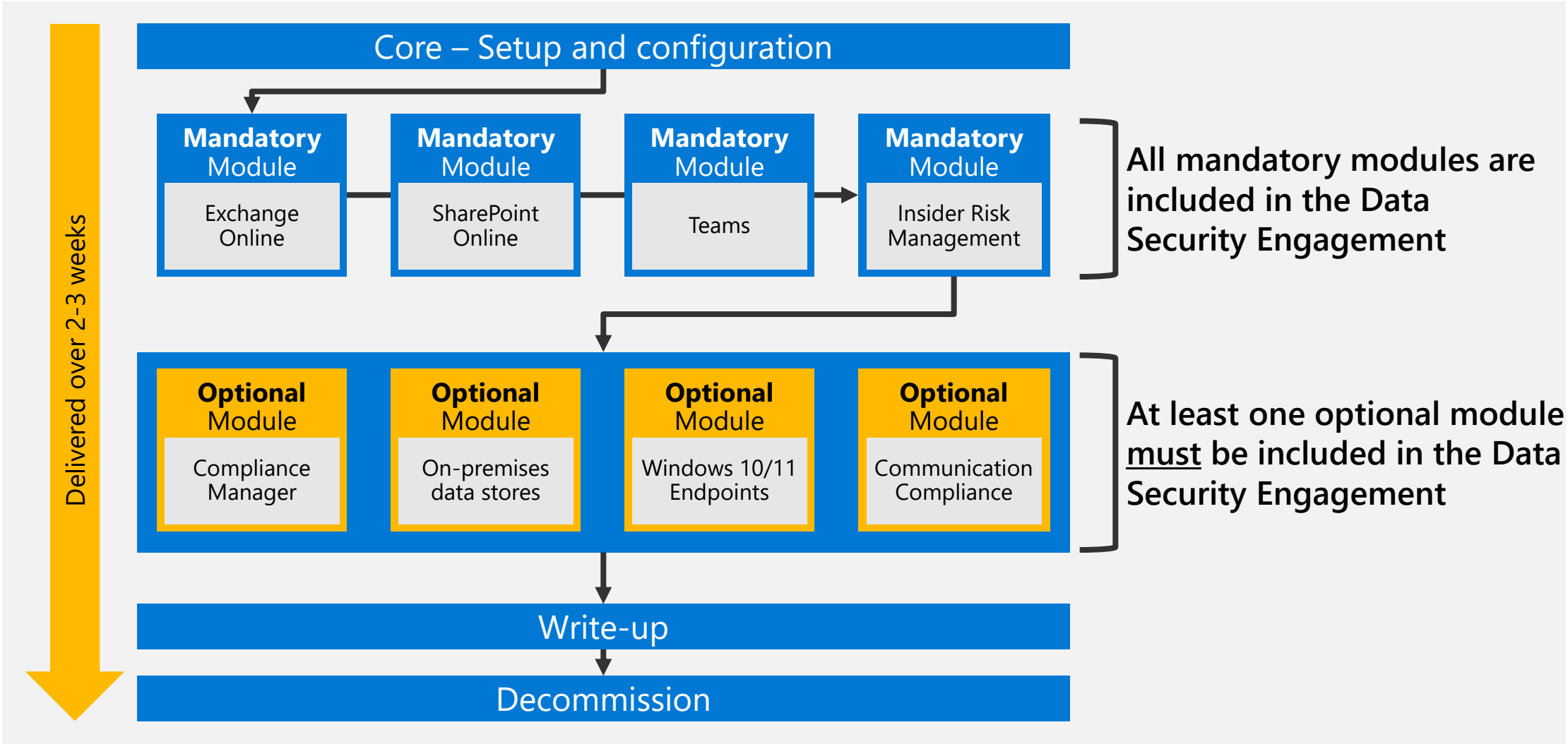
Two weeks of **automated discovery** searching for data security risks and risky user behavior in organizational data

Analyze & Report

Analyze the findings and **report** on the identified data security risks.



Data Security Check's modular design



Default scope

For the Data Security Check activity

Core Activities

Enable Data Security Check discovery services

Exchange Online, SharePoint Online, Teams, Insider Risk Management

Optional activities as necessary

Automated discovery of sensitive data and user behavior

Identify sensitive information in Microsoft 365 data repositories, monitor for risky user behavior.

Analysis and Reporting

Collect reports, logs, and dashboard information.
Analyze findings, map to solutions, and provide recommendations.

Optional Modules

Optional scope

For the Data Security Check activity

At least one (1) module must be delivered as part of the default scope

Compliance Manager

Assess the current Microsoft 365 environment against a set of controls for key regulations and standards for data protection and general data governance.

On-Premises Data Stores

Scan on-premises data repositories such as file shares and SharePoint server document libraries for sensitive data utilizing Purview Information Protection Scanner

Windows Endpoints

Identify risky behavior of users working with sensitive data on their Windows 10 or 11 workstations and laptops utilizing Data Loss Prevention for Endpoints

Communication Compliance

Monitor communications for sensitive information and risky activity that can cause data security risks.

Out-of-scope

Data Security Check will not assess….

Non-Microsoft Cloud services

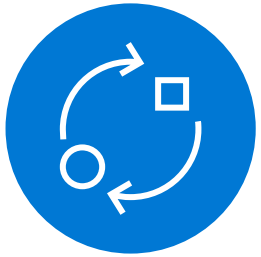
Proof of concept or pilot deployment

People & Processes

Data Security Check Deliverables

Data Security Check findings

Structured & categorized overview highlighting the most important findings.



Recommendations for risk mitigation

Mapping the identified risks to solutions.

Actionable next steps

Prioritized list of next steps, to implement solutions to control and mitigate data security risks and improve the organization’s compliance posture

Automated Discovery & data privacy

Only for “authorized people”, defined by you

Access to discovery results is governed through Role Based Access Control.
Access will only be granted for people that you have identified.
Findings and results are only visible for authorized people.

Personal Identifiable Data (PII) can be removed

Usernames or identifiable data repositories can be obfuscated or removed.

Data Security Check – Team members with access

Activity

Name	Role	Type of access
Adele Vance	ÌT Admin – security	
Alex Wilber	IT Admin – Compliance	
Allan deYoung	IT Admin – Identity	
Bianca Pisani	Compliance Officer	

Automated Discovery

Identifying data security
risks in your data

Core Activities

Default scope – mandatory modules

What Automated Discovery looks for

Sensitive Information

Artifacts that are relevant to your organization and impose a data security risk.

Stale Data

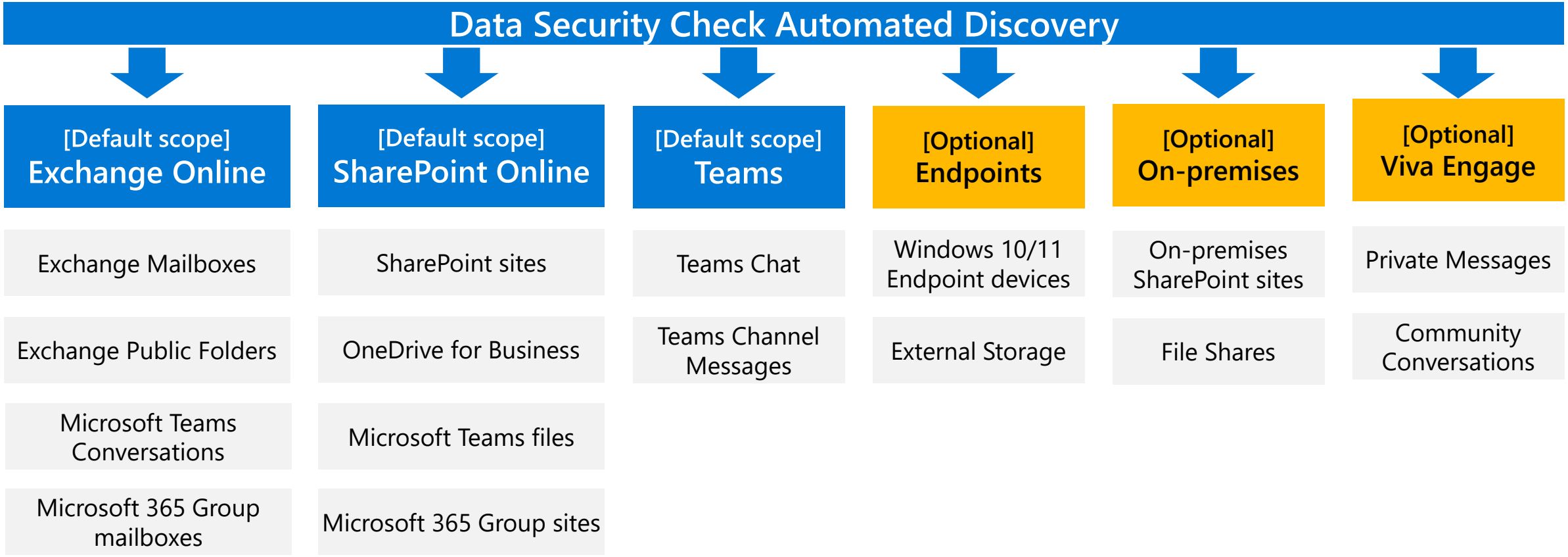
E-mails, documents that should have been deleted years ago

Risky user activity

Copying sensitive data to endpoints, USB drives, or other uncontrolled locations.

Auto Discovery target data repositories

Where the Automated Discovery service searches for data security risks



Sensitive information comes in many forms

Internal

Business intellectual property
Business plans, product designs, confidential projects

Employee or customer information
HR Information, resumés, employment records, salary information

Highly confidential information
Mergers and Acquisition, workforce reduction

External

Geographical Requirements
GDPR (Europe), CCPA (US: California)

Industry Requirements
PCI-DSS, HIPAA

Regulatory Requirements
GLBA(US), PIOCP (UK), DPA (France)

Classifiers used in the Data Security Check

Sensitive info types

300+ out of the box info types like SSN, CCN

Clone, edit, or create your own

Supports regex, keywords, and dictionaries

Named entities

50+ entities covering person name, medical terms, and drug names

Best used in combination with other sensitive info types

Trainable classifiers

23 new pre-trained ready-to-use trainable classifiers in GA

15 more in product preview

Create your own classifier based on business data

Credentials SITs

42 new SITs for digital authentication credential types

Use in auto-labeling and DLP policies to detect sensitive credentials in files

Sensitive data types to include in auto discovery

Activity

Out-of-box Sensitive Information type(s)	Remark
Credit card number	
All physical addresses	
Netherlands passport numbers	
Slovakia personal number	
SQL Server connection string	
U.S. social security number (SSN)	

Sensitive information type entity definitions - Microsoft Purview (compliance) | Microsoft Learn

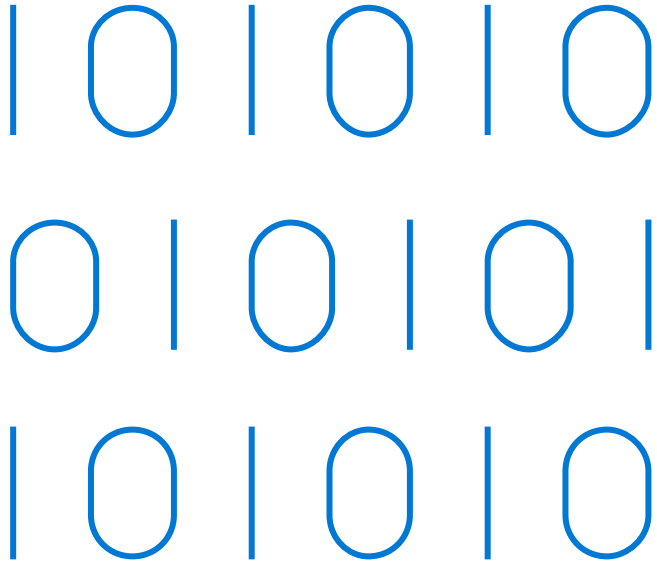
Custom Sensitive Information type(s)	Type	Remark
Employee number	RegEx	
Confidential	Static Keyword	
Customer number	RegEx	
Project Enigma	Static Keyword	

Stale data

Much data becomes stale right after creation
Stale data can impose risk and financial liability if exposed.

Keep everything strategy
Automated retention & deletion often not implemented.

Data older than six months, one year
Customizable search, configurable document age.



Risky user activity

Insider Risk Discovery

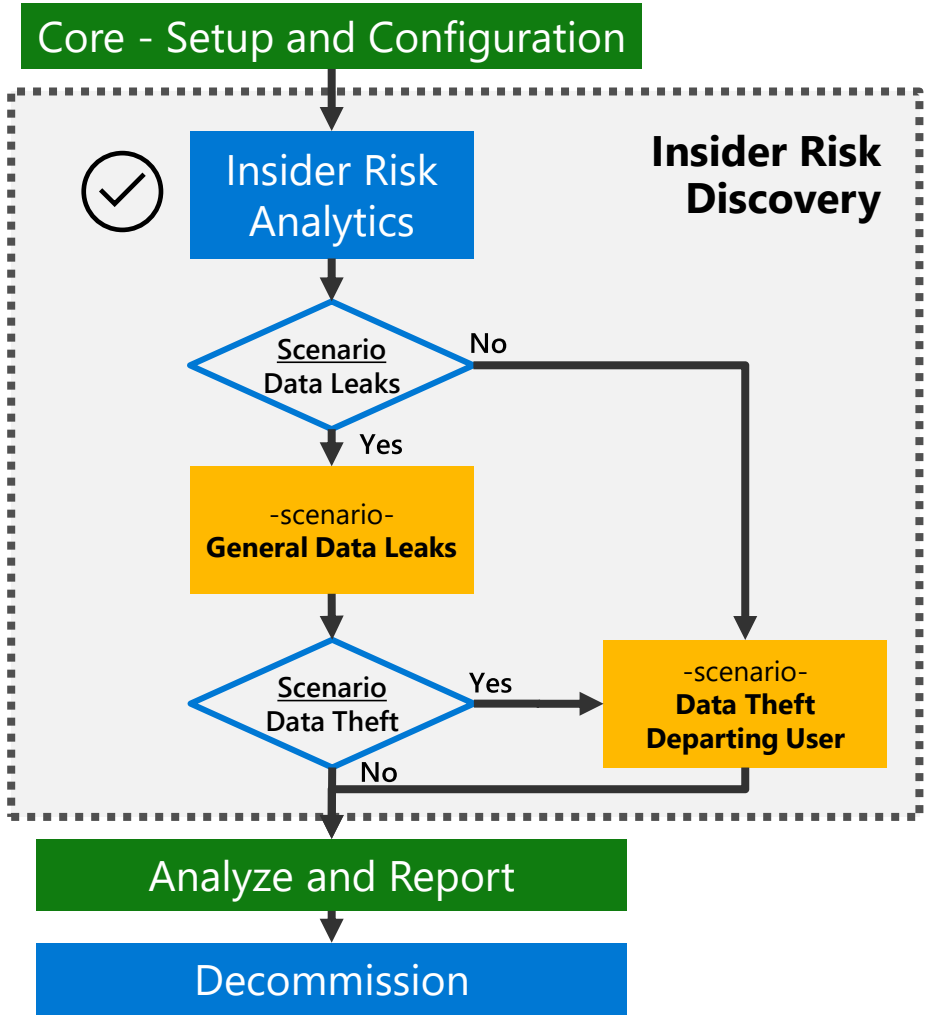
Detect malicious and inadvertent activities in the organization by enabling Purview Insider Risk Management and configuring policies that will define the types of risks to identify and detect.

Insider Risk Analytics

- The first activity for Insider Risk Management

Choose at least one of the additional scenarios:

- General data leaks
- Data theft by departing user

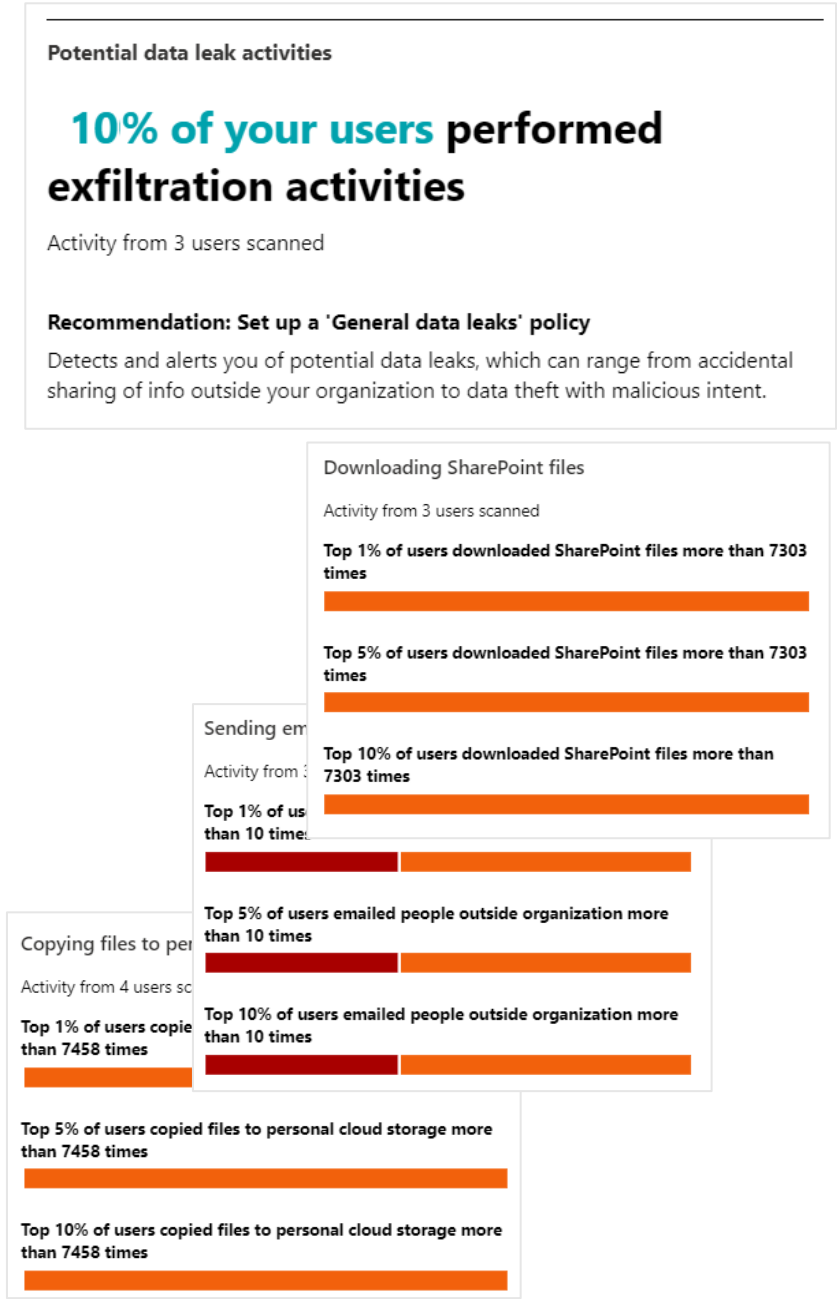


Risky user activity

Insider Risk Analytics

Evaluation of potential insider risks

- First activity for Insider Risk Discovery
- Insights based on the same signals used by insider risk management
- Works out of the box without configuring policies
- Identify potential areas of high user risk
- Help determine type and scope for policies to consider



Activity

Risky user activity

Scenarios and policy templates

Insider Risk Management Templates

Pre-defined policy conditions that define the types of risk indicators and risk scoring model used, define the types of risks to identify and detect.

Scenario's available for the Data Security Check

1

General Data Leaks

Monitors for accidental oversharing of information outside your organization or data theft with malicious intent. Automatically examines the high severity DLP alerts,

2

Data theft by departing users

Specific risk indicators typically associated with potential data theft by departing users. include downloading files from SharePoint Online, printing files, and copying data to personal cloud messaging and storage services near their employment resignation and end dates.

Activity

Risky user activity

Optional indicators and triggers

(Virtual) HR connector

Resignation or termination date indicator from HR connector or Azure Active Directory account deletion. Correlate risk indicators with user employment status

Azure Active Directory account deletion

Automatically check for user account deletion in Azure Active Directory for your organization, correlate risk indicators with user status

Endpoint integration

Uses signals from endpoints enrolled in Microsoft Purview. Includes policy indicators for activity such as sharing files over the network or with devices and browser signal detection (e.g. Microsoft Edge and Google Chrome).

(Requires devices to be enrolled into Purview)

Insider Risk Discovery

Scenarios, indicators and triggers

Activity

Scenario	Implement	Remark
Insider Risk Analytics	✓	
General Data Leaks	✗ / ✓	
Data theft by departing users	✗ / ✓	

Indicators and triggers	Implement	Remark
HR Connector configured for termination and resignation date indicators	✗ / ✓	Implemented as <virtual / physical> connector
Azure Active Directory account deletion	✗ / ✓	
Endpoint integration	✗ / ✓	Requires devices enrolled into Microsoft Purview

Optional Modules

Data Security Check

Optional modules

Optional modules

What Automated Discovery can additionally identify or assess

Compliance Posture

Assess the current Microsoft 365 environment against a set of controls for key regulations and standards for data protection and general data governance.

On-premises infrastructure and data storage

Scan on-premises data repositories such as file shares and SharePoint server document libraries for sensitive data

Windows endpoints

Identify risky behavior of users working with sensitive data on their Windows 10 or 11 workstations and laptops.

User communication

Inappropriate text, sensitive information, conflict of interest

Included optional modules

Activity

Name	Include	Remark
Compliance Manager Tenant Assessment	✗ / ✓	
On-premises data sources	✗ / ✓	
Windows 10/11 endpoints	✗ / ✓	
Communication Compliance	✗ / ✓	

Note: At least one (1) module must be delivered as part of the default scope

Optional Modules

Compliance Manager Tenant Assessment

Compliance Manager Tenant Assessment

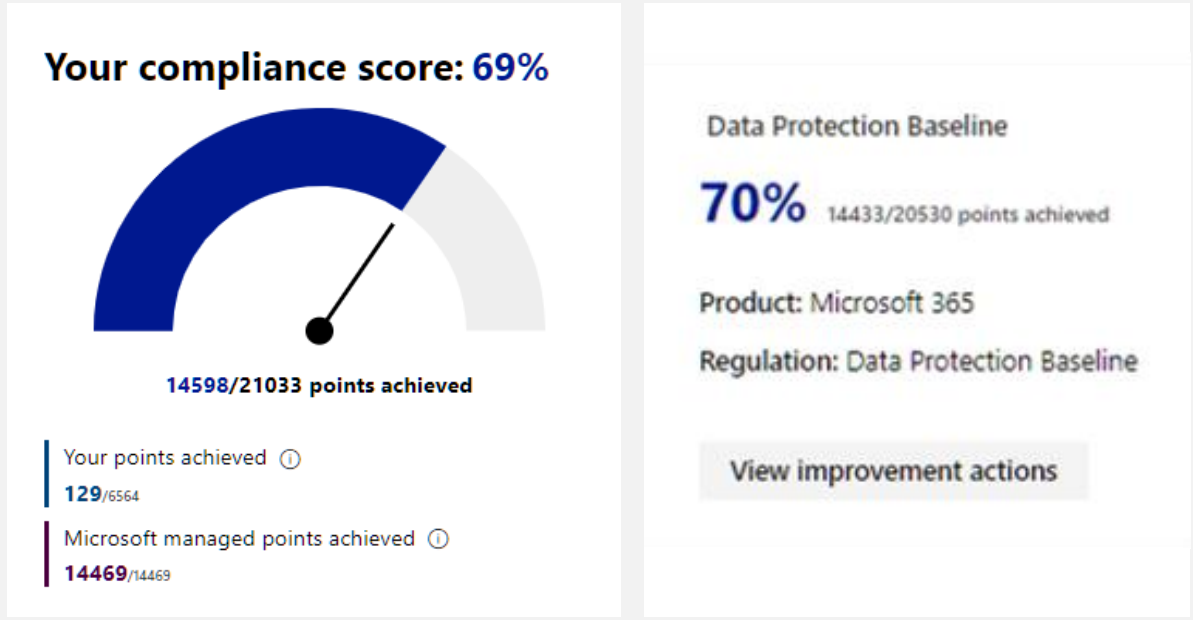
Assess performance relative to key data protection standards and regulations.

Generic and customer specific assessments

- Data Privacy Baseline Assessment
- Regulatory templates that align to customer specific requirements
  - Aligned to Region, Industry or type of organization
  - Over 300+ assessments to choose from

Recommendations for improvement together with implementation guidance.

New and updated scenarios are published regularly.



Compliance Manager - Assessments to implement

Activity

#	Name	Remark
1. (Mandatory)	**Data Protection Baseline Assessment**	Draws elements primarily from NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) and ISO (International Organization for Standardization), as well as from FedRAMP (Federal Risk and Authorization Management Program) and GDPR (General Data Protection Regulation of the European Union).
2. (Mandatory)	<Customer defined regulatory template #1>	
3. (Optional)	<Customer defined regulatory template #2>	
4. (Optional)	<Customer defined regulatory template #3>	

Reference: [Compliance Manager regulatory template list (Microsoft Learn)]

Optional Modules

On-premises data stores

Purview Information Protection Scanner

Connect to on-premises resources

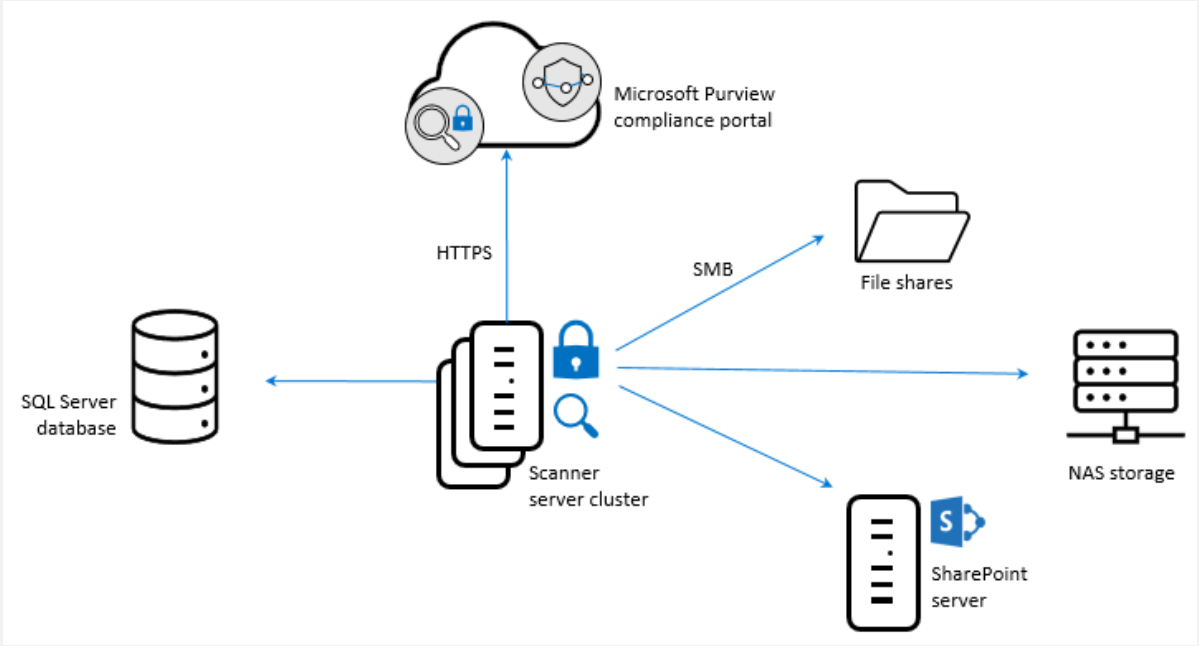
- UNC paths for network shares that use the SMB or NFS (Preview) protocols.
- SharePoint document libraries and folder for SharePoint Server 2019 through SharePoint Server 2013.

Leverages the Azure Information Protection client.

- Classifies the same types of files as the client.
- Re-uses the already configured sensitive information types

Runs as a service on Windows Server

- Requires SQL Server



Discover only mode

- No changes to the data
- No protection applied
- No data encryption

On-premises auto discovery – data repositories

Activity

Location	Type	Contains
\\FS01\Sales	File share	Office documents
http://sharepoint.contoso.com/Shared%20Documents/Folder	SharePoint server library	Office documents

Optional Modules

Data Loss Prevention for Endpoints

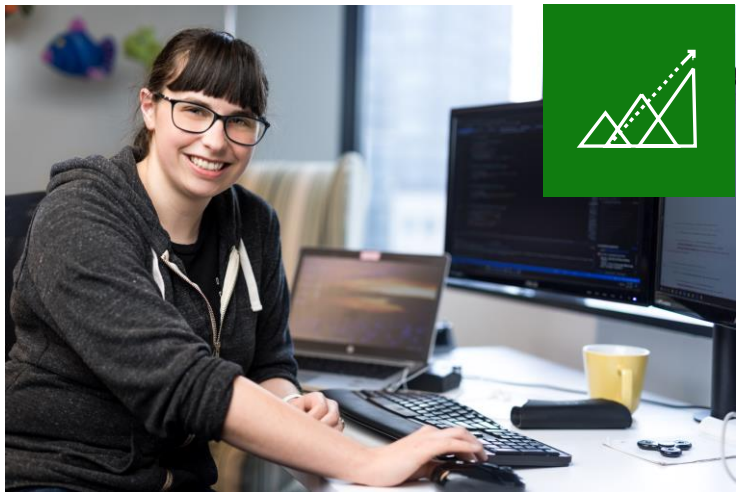
Data Loss Prevention for Endpoints

Endpoint activity monitoring and Data Loss Prevention.

Evaluate files against DLP policies and identify risky behavior by users working with sensitive data on their workstations or laptops.

Collect information on audited activity

Capture activity details when sensitive information is copied, moved, created, printed, etc.



Leverage Activity Explorer to review activities

Gain visibility into discovered content and where that content is. Monitor what's being done with your sensitive data.

Data Loss Prevention for Endpoints

Activity

Workstation / group	Owner	Operating system	On-boarding method
All Sales laptops	All members of the sales team	Windows 11	Through Group policy
WS-01	Adele Vance	Windows 11	Manual
WS-02	Alex Wilber	Windows 11	Manual
LAP-10	Allan Deyoung	Windows 10	Intune
LAP-11	Bianca Pisani	Windows 10	Intune

Optional Modules

Communication Compliance

Module - Communication Compliance

Activity overview

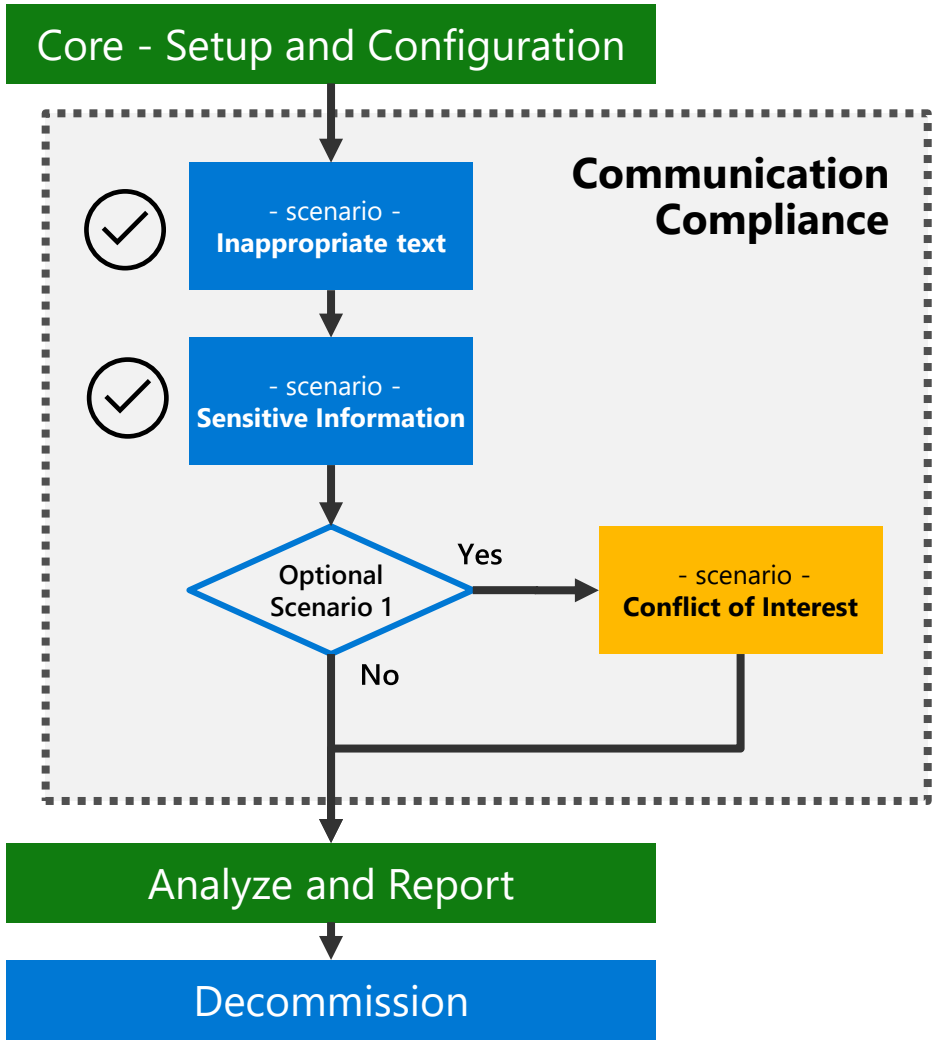
Detect communication risks in the organization by enabling Communication Compliance and configuring policies that will define the types of inappropriate content to identify and detect.

This activity covers:

- Inappropriate text
- Sensitive information

You can add an optional scenario:

- Conflict of interest



Inappropriate text
Module - Communication Compliance

Monitor communications for Inappropriate text

- Exchange Online, Microsoft Teams, Viva Engage
- Inbound, outbound, or internal only
- Review 100% of communications
- Inappropriate text classifier
- **Only monitors users participating in the Data Security Check**

Anti-harassment and cyber bullying monitoring requirements

Machine learning, artificial intelligence, and keywords help identify inappropriate messages

Sensitive information
Module - Communication Compliance

Monitor communications for sensitive information

- Exchange Online, Microsoft Teams, Viva Engage
- Inbound, outbound, or internal only
- Review 100% of communications
- Sensitive information, out-of-the-box content patterns and types, custom dictionary option
- **Only monitors users participating in the Data Security Check**

Monitoring legitimate communications between employees, or between employees and outside parties

Data theft with malicious intent

Conflict of interest

Module - Communication Compliance

Optional activity

Monitor communications between two groups or two users to help avoid conflicts of interest

- Exchange Online, Microsoft Teams, Viva Engage
- Internal
- Review Percentage: 100%
- **Only monitors users participating in the Data Security Check**

Monitor communications between two groups of users to watch for collusion or conflict of interest

Individuals with competing professional obligations or personal or financial interests

Communication compliance – scenarios to deploy

Activity

Scenario	Included	Remark
Inappropriate text	✓	
Sensitive information	✓	
Conflict of Interest	✗ / ✓	

Microsoft Purview portfolio overview

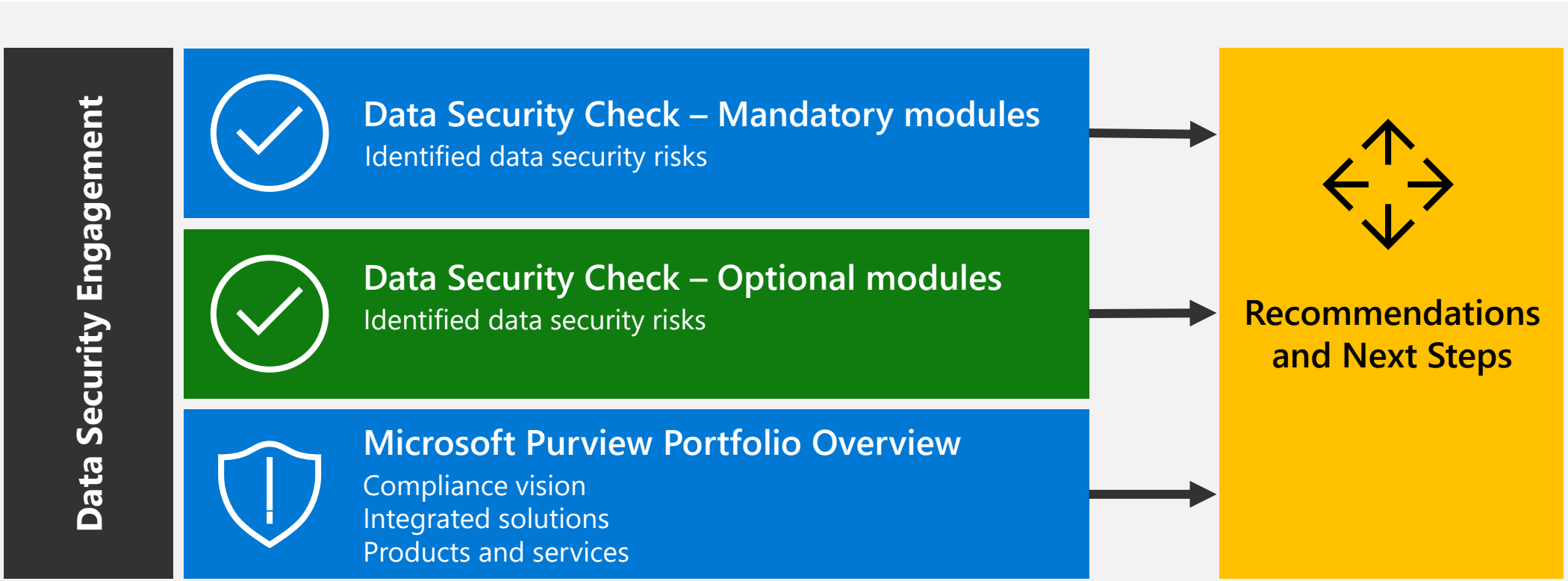
Microsoft Purview portfolio overview

Insight into vision, products, and services

- Microsoft's compliance vision and strategy
- Microsoft Purview products and services
- The benefits of end-to-end data security

Recommendations and next steps

Recommendations and next steps

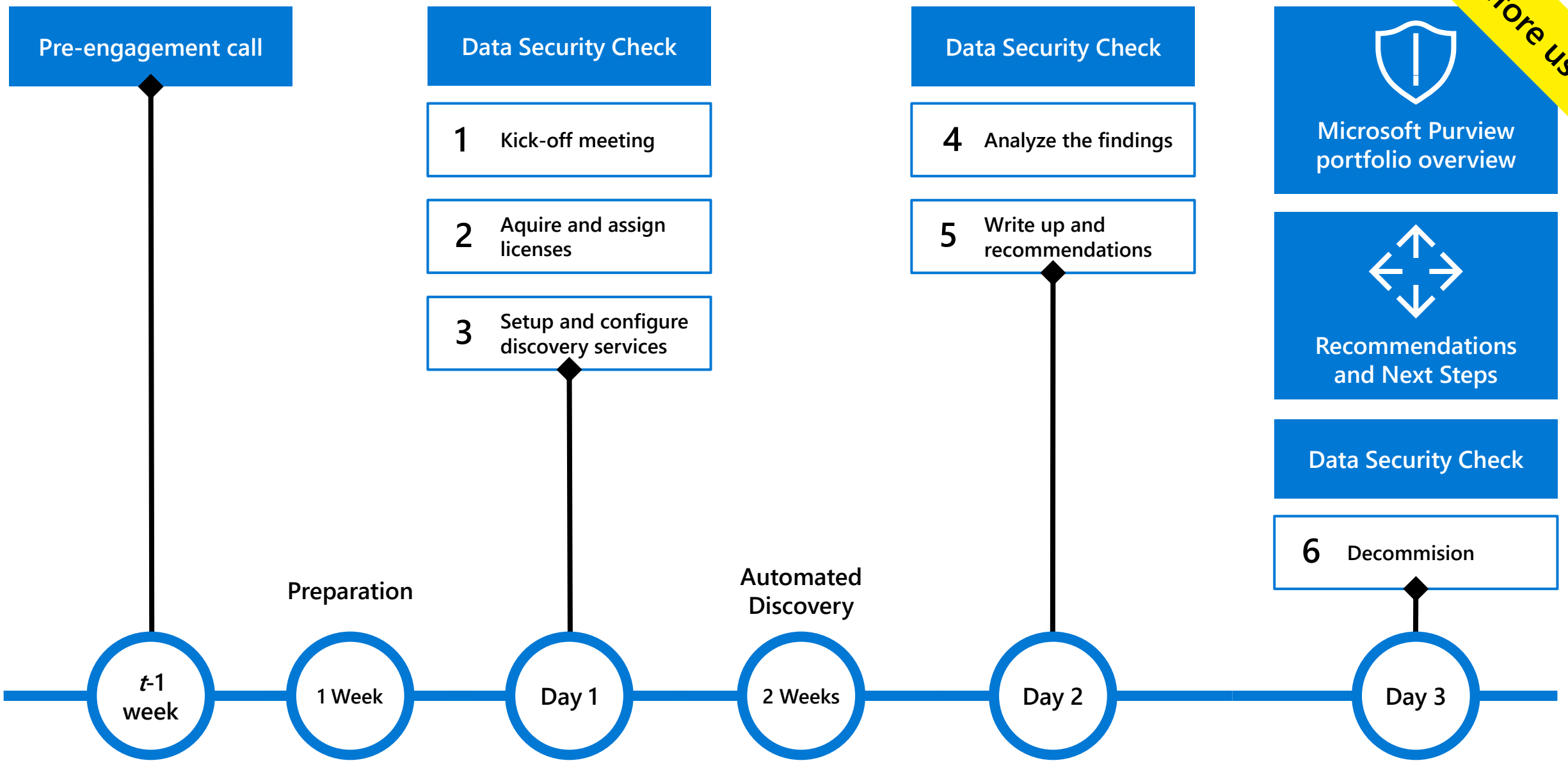


The engagement

Approach, timelines and governance

Engagement timeline

UPDATE before use



Governance

Risk and issues management

- Covering business, technology and project execution.
- Describe the escalation path.

Date recorded	Risk/Issue description	Probability	Impact	Mitigation plan

Change management

- Describe the change management workflow.

Success Criteria

- Discuss and agree on what a successful engagement would look like.

Q&A

Microsoft Security

Thank you