



# SIT - Quick Start (Sensitive Info Types)

Please consider this a “Work in Progress”

# Sensitive Info Types



# Where do SIT's fit in Data Governance

Information  
Protection

Information  
Governance

Records  
Management

Collaboration  
Governance

SIT's, Sensitivity Labels & Retention Labels

Exchange

SharePoint

Teams

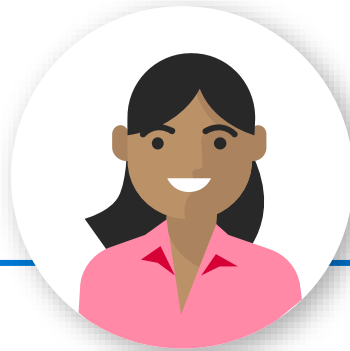
Azure/M365 Security Platform & DLP Policies

# Data protection & challenges

## Data protection day to day challenges



“As an **administrator**, how can I ensure the organizational data is **protected**, and **prevent access** to unauthorized data?”



“As a **data owner**, how can I ensure the organizational data I work with is **protected**”?  
“How can my **productivity** stay high while using those & ensure compliance?”



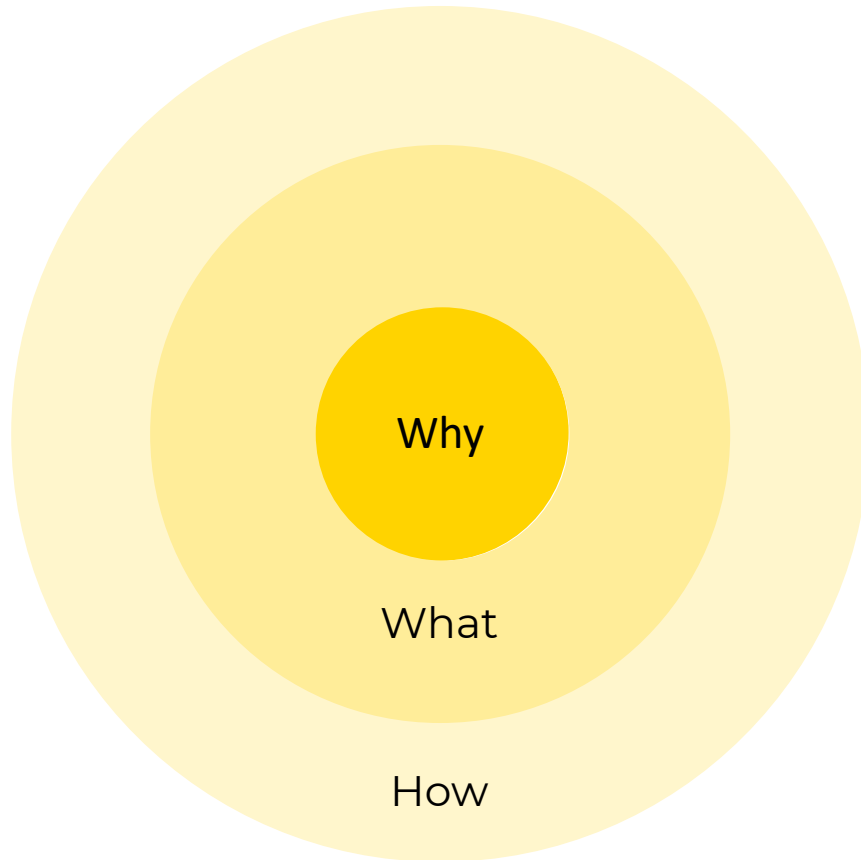
“As an **administrator**, how do I gain **oversight** of the sensitive data stored in my tenant, where, and by whom it's accessed?”



“As an **Auditor**, how can I ensure that our Organization ensures we meet our **privacy & regulatory requirements** and are compliant?”

Is the business workflow/process's documented or still in tribal knowledge?

# Before you start:



## Why

- + What is the business impact of what you are trying to protect?
- + Can you quantify the impact?
- + If not, is it worth the effort?

## What

- + Do you have samples of what you are trying to protect
- + Do you know how many times it currently occurs?
- + What is the impact on down the line processes? (If you create 100 events will this be 100 incidents?)

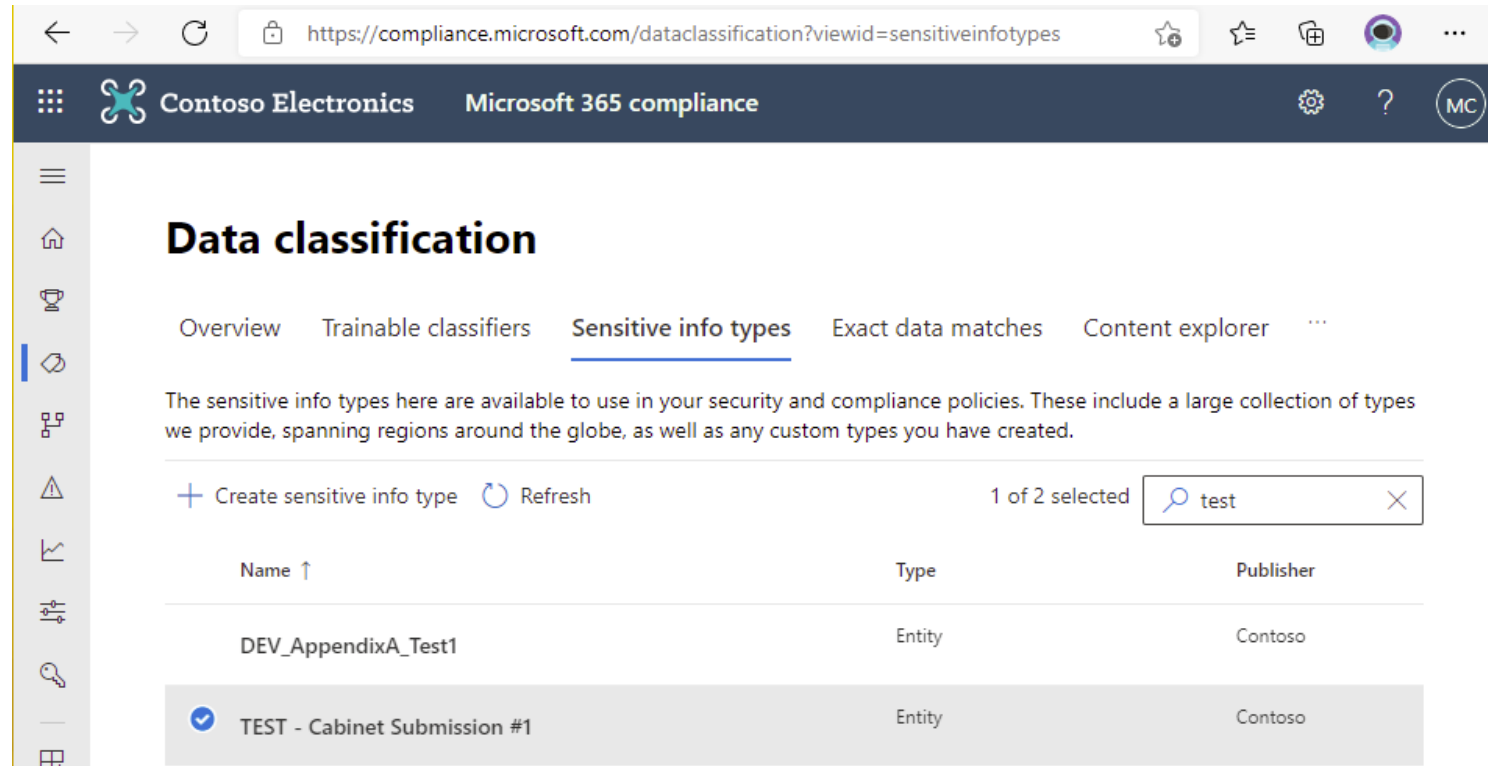
## How

- + Is there a current SIT that you can use as an example of what you are trying?
- + Can you draw a flowchart of the logic you are applying?
- + Now we can look at the technology to implement SITs

# SIT's: Quick Start

Data Classification can be broken down as:

- + Trainable Classifiers
- + Sensitive Info Types (SIT's)
- + Exact Data Matches (typically from DB)



The screenshot shows the Microsoft 365 compliance center interface. The browser address bar displays the URL: <https://compliance.microsoft.com/dataclassification?viewid=sensitiveinfotypes>. The page title is "Data classification". The navigation tabs include "Overview", "Trainable classifiers", "Sensitive info types" (which is selected), "Exact data matches", and "Content explorer". Below the tabs, a message states: "The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created." Below this message, there are buttons for "+ Create sensitive info type" and "Refresh". To the right, it says "1 of 2 selected" and there is a search box containing the text "test". Below the search box is a table with the following columns: "Name", "Type", and "Publisher". The table contains two rows: one for "DEV\_AppendixA\_Test1" and another for "TEST - Cabinet Submission #1". The second row is highlighted in blue, indicating it is selected.

Name	Type	Publisher
DEV_AppendixA_Test1	Entity	Contoso
TEST - Cabinet Submission #1	Entity	Contoso

# SIT's: Quick Start

Apart from Sensitive Info Types (SIT's) **Data Classification** can be broken down as:

- + Trainable Classifiers
- + Sensitive Info Types (SIT's)
  - + 204+ Out of Box – new and improved & can be copied/edited
- + Exact Data Matches (typically from DB)
- + Doc Fingerprinting (exchange only)

See details in Speaker notes for summary + links

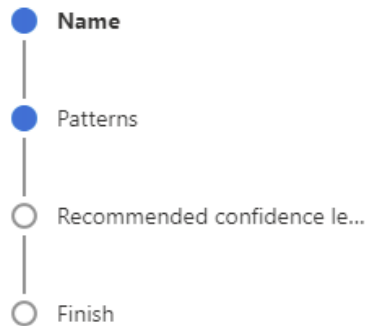
In this session we will be focusing on Sensitive Info Types (SIT's) only

# SIT's: Quick Start

Sensitive Info Types (SIT's):

- + Copy an Out of Box SIT or create new
- + Creating a SIT requires = Name & Description (naturally)

Sensitive info types > Edit sensitive info type



## Name your sensitive info type

This name and description will appear in compliance policies that support sensitive info types, so be sure to enter text that helps admins easily understand what info will be detected.

Name \*

TEST - Cabinet Submission #1

Description \*

TEST - Cabinet Submission #1

Next

Cancel



# SIT's: Quick Start

Sensitive Info Types (SIT's):

- + Creating a SIT requires  
= Define the pattern –  
here's where we get  
serious

The screenshot shows the 'Edit sensitive info type' page in the Microsoft 365 compliance center. The breadcrumb trail is 'Sensitive info types > Edit sensitive info type'. On the left, a progress bar shows four steps: 'Name' (completed), 'Patterns' (active), 'Recommended confidence level', and 'Finish'. The main content area is titled 'Define patterns for this sensitive info type' and includes a descriptive paragraph. Below this, there is a '+ Create pattern' button and a table with one pattern named 'Pattern #1' set to 'High' confidence. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons. A help icon is visible in the bottom right corner.

https://compliance.microsoft.com/dataclassification?viewid=sensitiveinfotypes

Contoso Electronics Microsoft 365 compliance

Sensitive info types > Edit sensitive info type

Progress bar: Name (checked), **Patterns** (active), Recommended confidence level, Finish

### Define patterns for this sensitive info type

Sensitive info types are defined by one or more patterns. Each pattern must contain a primary element and confidence level, but you can also include supporting elements and additional checks to further refine the evaluation and detection of matching items. [Learn about defining patterns](#)

+ Create pattern 1 pattern

Name	Confidence level	
Pattern #1	High	

Back Next Cancel

# SIT's: Quick Start

Sensitive Info Types (SIT's):

- + Creating a SIT requires =
- + Edit pattern
- + Set for low confidence (for now)
- + Can be tweaked later...

The screenshot displays the 'Define patterns for' interface. On the left, a sidebar shows a 'Create pattern' button and a list of patterns, with 'Pattern #1' selected. The main area shows the 'Edit pattern' modal. The modal has a title bar with a close button. Below the title, there is a descriptive text: 'At minimum, a pattern should have a confidence level and primary element to detect. Adding supporting elements, character proximity, and additional checks will help increase accuracy.' The modal contains several sections: 'Confidence level' with a dropdown set to 'High confidence'; 'Primary element' with a text field containing 'Dictionary (large keywords): Cabinet Submission #1'; 'Character proximity' with a checkbox for 'Anywhere in the document' and a text field for '300 characters'; and 'Supporting elements' which is currently empty. At the bottom of the modal are 'Update' and 'Cancel' buttons. The background interface shows 'Back' and 'Next' buttons at the bottom.

## Define patterns for

Sensitive info types are defined by one or more patterns. You can define a pattern by a single element, but you can also include supporting elements to match items. [Learn about defining patterns](#)

+ Create pattern

Name

▼ Pattern #1

### Edit pattern

At minimum, a pattern should have a confidence level and primary element to detect. Adding supporting elements, character proximity, and additional checks will help increase accuracy.

Confidence level \* ⓘ

High confidence ▼

Primary element \* ⓘ

Dictionary (large keywords): Cabinet Submission #1 ⓘ 🗑️

Character proximity ⓘ

Detect primary AND supporting elements within 300 characters

☐ Anywhere in the document

Supporting elements ⓘ

Update Cancel

Back Next

# SIT's: Quick Start

Sensitive Info Types (SIT's):

+ Creating a SIT requires =

+ New/Edit pattern

+ What to choose here?

## New pattern

At minimum, a pattern should have a confidence level and primary element to detect. Adding supporting elements, character proximity, and additional checks will help increase accuracy.

Primary element

- Regular expression
- Keyword list
- Keyword dictionary
- Functions

+ Add primary element

Character proximity ⓘ

Detect primary AND supporting elements within  characters

☐ Anywhere in the document

Supporting elements ⓘ

Create Cancel

# SIT's: Quick Start

Sensitive Info Types (SIT's):

- + SIT can be based on the following:
  - + Regular Expressions (not covered here – see speaker notes)
  - + **Keyword Lists** - use by default unless you have phrases over 50 characters
    - + Use keyword lists when you want have few keywords (limit is 2K keywords) and each keyword is less than 50 characters.
    - + Keyword lists have granular features like choosing to do a string match vs full word match, case sensitive vs case insensitive etc.
  - + **Keyword Dictionary**
    - + Use keyword dictionaries when you have thousands of phrases some of which might be over 50 characters long.
  - + Functions (not covered here – see speaker notes)

# SIT's: Quick Start


Sensitive Info Types (SIT's):

+ Creating a SIT

+ Add a Keyword List:


## Add a keyword list

Keyword lists identify the words and phrases you want this info type to detect. For example, the keyword list to identify Netherlands VAT numbers is 'VAT number, vat no, vat number, VAT#'. [Learn how to create keyword lists](#)

 Choose from existing keyword lists

ID \* 

Enter the keyword list name

Keyword group #1 \* 



Case insensitive

Enter keywords, separated by a new line. Each keyword is limited to 50 characters, and casing isn't a factor when detecting matches.

Case sensitive

Enter keywords, separated by a new line. Each keyword is limited to 50 characters, and exact casing is required to detect matches.

☒ Word match ☐ String match

Done

Cancel



# SIT's: Quick Start

Sensitive Info Types (SIT's):


+ Creating a SIT

+ Add a Keyword Dictionary:

+ HINT:

+ Take example doc & save as text using Unicode – this can now be used as an upload

+ Remove all words that may cause noise to reduce false positives

 Upload a dictionary ▾


Upload TXT file


Upload CSV file


Selected dictionary will be saved for use in

## Add keyword dictionary


Unlike keyword lists (which are limited in size) keyword dictionaries provide easier management of keywords and at a much larger scale. [Learn how to create keyword dictionaries](#)

 Choose from existing dictionaries

 Upload a dictionary ▾

Name \* 

<Name of Dictionary>

Keywords \* 

APPENDIX A  
OFFICE USE ONLY  
CONFIDENTIAL  
CABINET SUMMARY SHEET  
SUBMISSION NO.  
DATE RECEIVED  
TITLE OF CABINET MINUTE  
MINISTER'S NAME, TITLE AND RELEVANT PORTFOLIO  
IMPLEMENTING AGENCY  
PURPOSE (objective of proposal)  
COSTING/FINANCIAL IMPLICATIONS  
Is proposal covered by existing/approved forward estimates?  
IF NO, DOES PROPOSAL HAVE AN ADDITIONAL IMPACT ON:  
Expense Limit  
Net Operating Balance  
Net Debt  
FTE Increases  
IS PROPOSAL TO BE FUNDED (FULLY OR PARTIALLY) VIA:  
Re-prioritisation of savings  
Reduction in cash balance  
Royalties for Regions  
Increase in appropriation  
Increase in retained revenue

Done

Cancel

# SIT's: Quick Start

Sensitive Info Types (SIT's):

- + Creating a SIT
- + Add a Keyword Dictionary:
- + Compare the new Keyword Dictionary to the original Doc and notice the intersection?

CONFIDENTIAL

**CABINET SUMMARY SHEET**

APPENDIX A

OFFICE USE ONLY

SUBMISSION NO.

DATE RECEIVED

TITLE OF CABINET MINUTE

MINISTER'S NAME, TITLE AND RELEVANT PORTFOLIO

IMPLEMENTING AGENCY

PURPOSE (objective of proposal)

COSTING/FINANCIAL IMPLICATIONS

Is proposal covered by existing/approved forward estimates?

Yes

No

IF NO, DOES PROPOSAL HAVE AN ADDITIONAL IMPACT ON:

Expense Limit

Yes

No

Net Operating Balance

Yes

No

Net Debt

Yes

No

FTE Increases

Yes

No

IS PROPOSAL TO BE FUNDED (FULLY OR PARTIALLY) VIA:

Re-prioritisation of savings

Reduction in cash balance

Royalties for Regions

Increase in appropriation

Increase in retained revenue

## Add keyword dictionary

Unlike keyword lists (which are limited in size) keyword dictionaries provide easier management of keywords and at a much larger scale. [Learn how to create keyword dictionaries](#)

Choose from existing dictionaries

Upload a dictionary

Name \* ⓘ

<Name of Dictionary>

Keywords \* ⓘ

APPENDIX A  
OFFICE USE ONLY  
CONFIDENTIAL  
CABINET SUMMARY SHEET  
SUBMISSION NO.  
DATE RECEIVED  
TITLE OF CABINET MINUTE  
MINISTER'S NAME, TITLE AND RELEVANT PORTFOLIO  
IMPLEMENTING AGENCY  
PURPOSE (objective of proposal)  
COSTING/FINANCIAL IMPLICATIONS  
Is proposal covered by existing/approved forward estimates?  
IF NO, DOES PROPOSAL HAVE AN ADDITIONAL IMPACT ON:  
Expense Limit  
Net Operating Balance  
Net Debt  
FTE Increases  
IS PROPOSAL TO BE FUNDED (FULLY OR PARTIALLY) VIA:  
Re-prioritisation of savings  
Reduction in cash balance  
Royalties for Regions  
Increase in appropriation  
Increase in retained revenue

Done


Cancel





# SIT's: Quick Start

Sensitive Info Types (SIT's):

- + Creating a SIT
- + Add a Keyword Dictionary:
- + Once created use the test button
- + Upload the original docx
- + Then start modifying docx and retesting
- + Tweak and retest
- + Retest on true and false positive examples

## TEST - Cabinet Submission #1



 Test  Copy  Edit  Delete

Description

### Match results

We have detected the following in [Example\\_APPENDIX A.docx](#)

#### 1. TEST - Cabinet Submission #1

Low - 45 matches

Matches	Supporting elements
(Regulatory proposals with Economically Significant ...	-
(If yes, complete Regulatory Impact Assessment secti...	-
MINISTER'S NAME, TITLE AND RELEVANT PORTFOLIO	-
Re-prioritisation of savings	-
PURPOSE (objective of proposal)	-
(to be detailed in Consultation section of cabinet mi...	-
Consultation	-
Regulatory Impact Assessment	-
TIMING OF ANNOUNCEMENT	-



# SIT's: Quick Start

Sensitive Info Types (SIT's):

- + Always evaluate ALL doc's that are \*mandated\* to be in the solution
  - + Having said that - that's for a Prod deployment
  - + For a PoC best to be agile and nimble - so it comes down to picking a "good" demo doc
- + The more precise & focused the better



CONFIDENTIAL

## CABINET SUMMARY SHEET

APPENDIX A

OFFICE USE ONLY

SUBMISSION NO.

DATE RECEIVED

TITLE OF CABINET MINUTE									
MINISTER'S NAME, TITLE AND RELEVANT PORTFOLIO									
IMPLEMENTING AGENCY									
PURPOSE (objective of proposal)									
COSTING/FINANCIAL IMPLICATIONS									
Is proposal covered by existing/approved forward estimates? <input type="checkbox"/> Yes <input type="checkbox"/> No									
IF NO, DOES PROPOSAL HAVE AN ADDITIONAL IMPACT ON:									
Expense Limit		Net Operating Balance		Net Debt		FTE Increases			
<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Yes	<input type="checkbox"/> No		
IS PROPOSAL TO BE FUNDED (FULLY OR PARTIALLY) VIA:									
<input type="checkbox"/> Re-prioritisation of savings		<input type="checkbox"/> Reduction in cash balance							
<input type="checkbox"/> Royalties for Regions									
<input type="checkbox"/> Increase in appropriation		<input type="checkbox"/> Increase in retained revenue							



Something like this

# SIT's: Quick Start

Sensitive Info Types (SIT's):

- + Always evaluate ALL doc's that are \*mandated\* to be in the solution
- + Creating a SIT – can be 3 different Patterns - this is only needed if there are a "number" of User Stories and Doc's of differing degrees
  - + High/Med/Low - choosing between these comes down to the Org's risk appetite + details above
- + Different patterns may alert at different levels in business workflow
- + For a PoC, this is likely not needed – so use the KISS principal



CONFIDENTIAL

## CABINET SUMMARY SHEET

APPENDIX A

OFFICE USE ONLY

SUBMISSION NO.

DATE RECEIVED

TITLE OF CABINET MINUTE									
MINISTER'S NAME, TITLE AND RELEVANT PORTFOLIO									
IMPLEMENTING AGENCY									
PURPOSE (objective of proposal)									
COSTING/FINANCIAL IMPLICATIONS									
Is proposal covered by existing/approved forward estimates? <input type="checkbox"/> Yes <input type="checkbox"/> No									
IF NO, DOES PROPOSAL HAVE AN ADDITIONAL IMPACT ON:									
Expense Limit		Net Operating Balance		Net Debt		FTE Increases			
<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Yes	<input type="checkbox"/> No		
IS PROPOSAL TO BE FUNDED (FULLY OR PARTIALLY) VIA:									
<input type="checkbox"/> Re-prioritisation of savings					<input type="checkbox"/> Reduction in cash balance				
<input type="checkbox"/> Royalties for Regions					<input type="checkbox"/> Increase in retained revenue				
<input type="checkbox"/> Increase in appropriation									

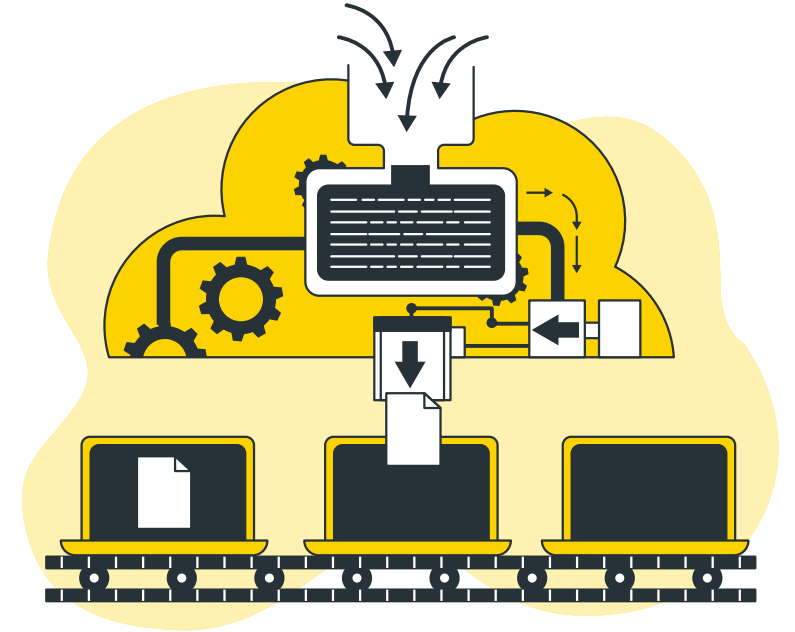


Something like this

# SIT's: Quick Start

Sensitive Info Types (SIT's):

- ✚ When creating the SIT be aware that the "Test" should be considered a "True Funnel" of what will match
  - ✚ If you create a High Confidence SIT and then "Test" = you will get matches for Low/Med/High (It's a True Funnel)
  - ✚ If you create a Low Confidence SIT and then "Test" = you will get matches for Low only (It's a True Funnel)



# SIT's: Quick Start

Sensitive Info Types (SIT's):

- ✚ So - when creating the SIT make sure you don't tweak it too far that you accidentally eliminate any True Positives
  - ✚ Be mindful that a SIT is **simply the first cut** - the next step is to use that SIT from either a DLP Policy or a policy to apply a Sensitivity or Retention Label
  - ✚ Both of these “Policies” have filters that can be used for filtering down to the "stuff" that is relevant
  - ✚ So make sure you haven't gone too far in the SIT, you may be missing TP's?
  - ✚ That's not good – so you may need to go back to the drawing board...
  - ✚ But at the same token you don't want false positives to be a couple of orders of magnitude – this needs balance



# SIT's: Quick Start

Sensitive Info Types (SIT's):

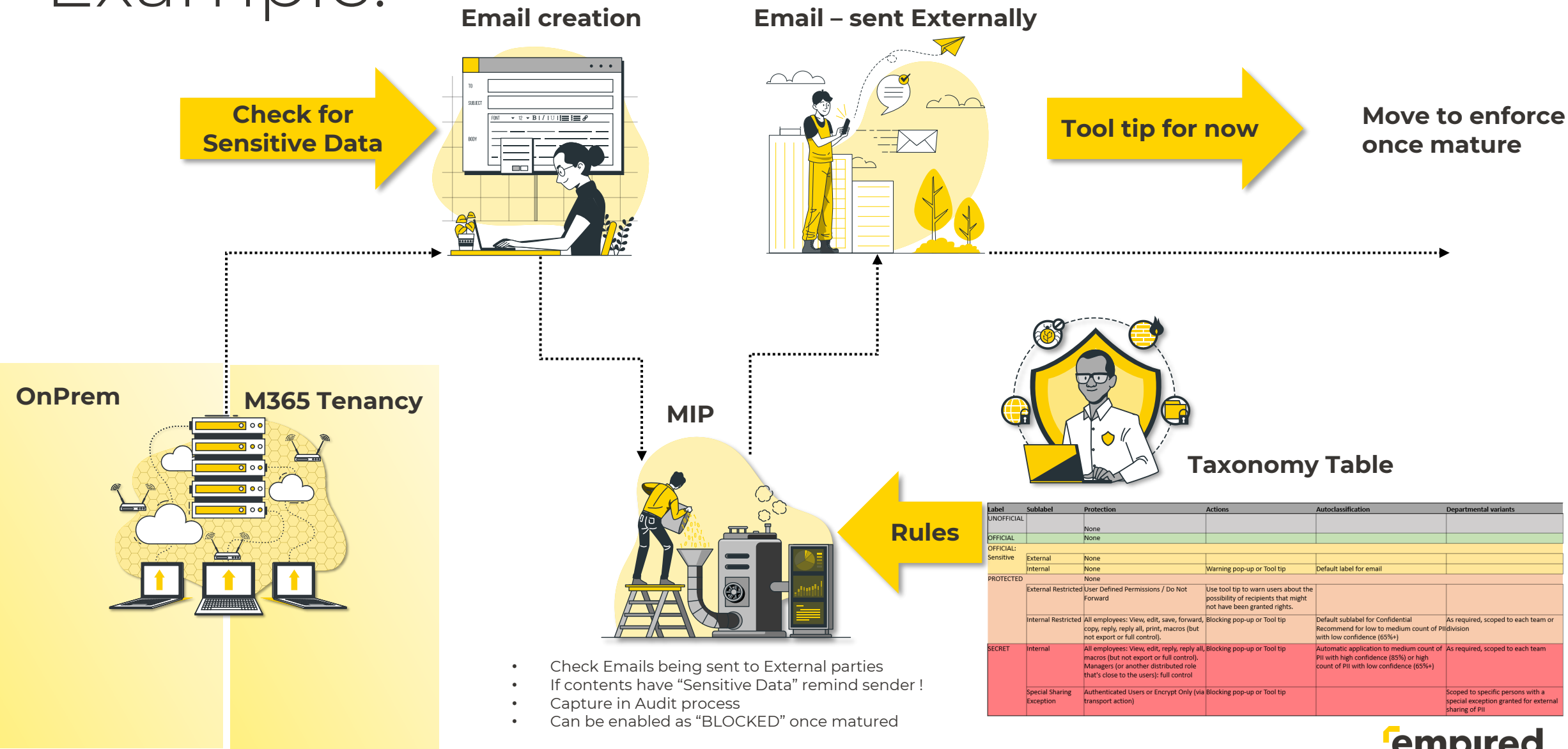
- + Further testing – enable policy in Teams
- + Now use Teams (in browser) and start referencing the keywords from that Keyword Dictionary example created earlier in a random chat
- + Here we can test in almost real-time the responses

The screenshot displays a Microsoft Teams chat window. On the left is a vertical sidebar with a circular profile icon labeled 'MC' and a green status indicator. The main chat area has a light pink background and contains several messages. Each message is preceded by a red flag icon and the text 'This message was flagged. What can I do?'. The messages are as follows:

- From 'Microsoft CDX' at 2:20 PM: 'chat about SUMMARY'. Below this message is a blue link that says 'Collapse all'.
- From 'Microsoft CDX' at 2:26 PM: 'OK - what about required'.
- From 'Microsoft CDX' at 2:27 PM: 'How about attaching a doc?'. Below this message is a document attachment card for 'Example\_APPENDIX A.docx' with a Word icon and a three-dot menu.
- Unsent message: 'so I'm guessing even FTE increases will trigger this as well?'.
- Unsent message: 'Net Debt'.
- Unsent message: 'TITLE OF CABINET MINUTE'.

At the bottom of the chat area is a white input field with the placeholder text 'Reply'.

# Example:





THANK  
*you*

empired



# Understanding sensitivity labels

+ Customizable

+ Persists as container metadata or file metadata

+ Readable by other systems

+ Determines DLP policy based on labels

+ Extensible to partner solutions



Manual or Automated Labels +

Apply to content or containers +

Label data at rest, data in use, or data in transit +

Enable protection actions based on labels +

Seamless end user experience across productivity applications +

Label	Sublabel	Protection	Actions	Autoclassification	Departmental variants
UNOFFICIAL		None			
OFFICIAL		None			
OFFICIAL:					
Sensitive	External	None			
	Internal	None	Warning pop-up or Tool tip	Default label for email	
PROTECTED		None			
	External Restricted	User Defined Permissions / Do Not Forward	Use tool tip to warn users about the possibility of recipients that might not have been granted rights.		
	Internal Restricted	All employees: View, edit, save, forward, copy, reply, reply all, print, macros (but not export or full control).	Blocking pop-up or Tool tip	Default sublabel for Confidential Recommend for low to medium count of PII with low confidence (65%+)	As required, scoped to each team or division
SECRET	Internal	All employees: View, edit, reply, reply all, macros (but not export or full control). Managers (or another distributed role that's close to the users): full control	Blocking pop-up or Tool tip	Automatic application to medium count of PII with high confidence (85%) or high count of PII with low confidence (65%+)	As required, scoped to each team
	Special Sharing Exception	Authenticated Users or Encrypt Only (via transport action)	Blocking pop-up or Tool tip		Scoped to specific persons with a special exception granted for external sharing of PII

Related DLP rules

Trigger	Example	DLP actions	Exception	Monitoring
Low count PII	1-2 Credit Card #s, SSNs, etc.	Block external sharing	If classified as non-business, Confidential External or HC Special Sharing Exception	Alert on repeat actions in a short period of time.
Medium count PII	3-9 Credit Card #s, SSNs, etc.	Block external sharing, Cloud Egress, copy to removable drive	If classified as Confidential External or HC Special Sharing Exception	Alert on repeat actions over time.
High count PII	10+ Credit Card #s, SSNs, etc.	Block external sharing, Cloud Egress, copy to removable drive	If classified as HC Special Sharing Exception (and/or sent to special allowed parties by specific allowed users)	Report on each individual action.

# Information Protection & Governance

Protect and govern data  
– **wherever** it lives

Understand your data landscape and identify important data across your hybrid environment

Apply flexible protection actions including encryption, access restrictions and visual markings



Automatically retain, delete, and store data and records in compliant manner

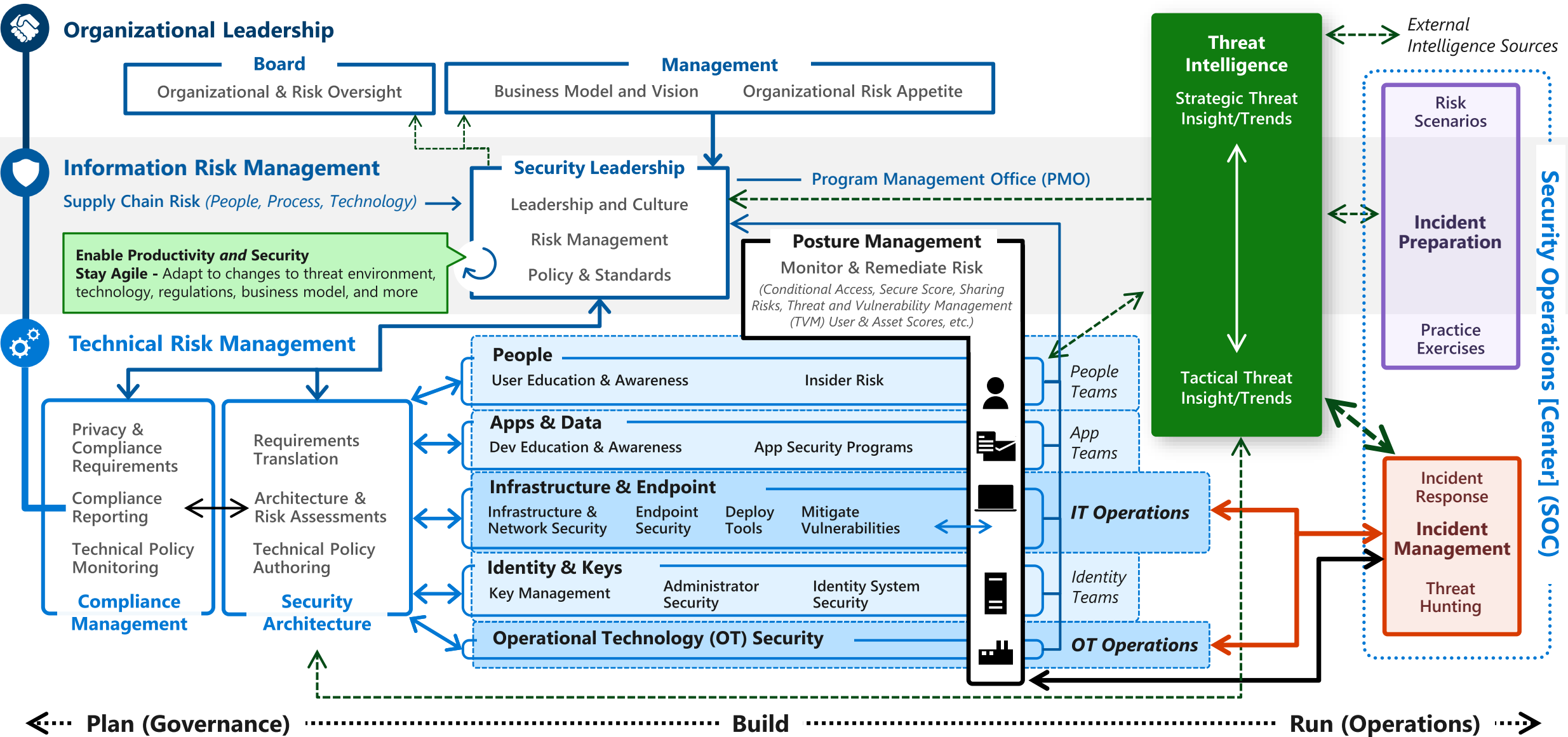
**Powered by an intelligent platform**

Unified approach to automatic data classification, policy management, analytics and APIs

# Managing Information\Cyber Risk

Security responsibilities or "jobs to be done"

May 2021 - <https://aka.ms/SecurityRoles>



## Security Operations / SOC

Threat Experts | Detection and Response Team (DART) | MSSP/MDR

**Azure Sentinel** – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT



# Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

May 2021 – <https://aka.ms/MCRA>

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Security Guidance

1. [Security Documentation](#)
2. [Microsoft Best Practices](#)
3. Azure Security [Top 10](#) | [Benchmarks](#) | [CAF](#) | [WAF](#)

## Software as a Service (SaaS)

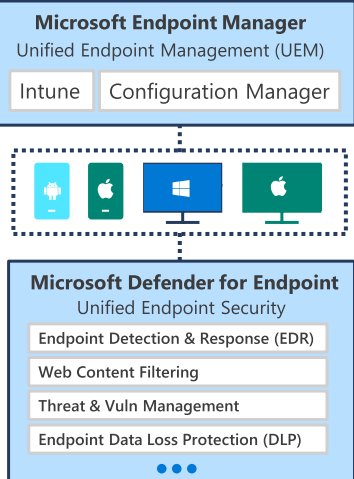


## Identity & Access

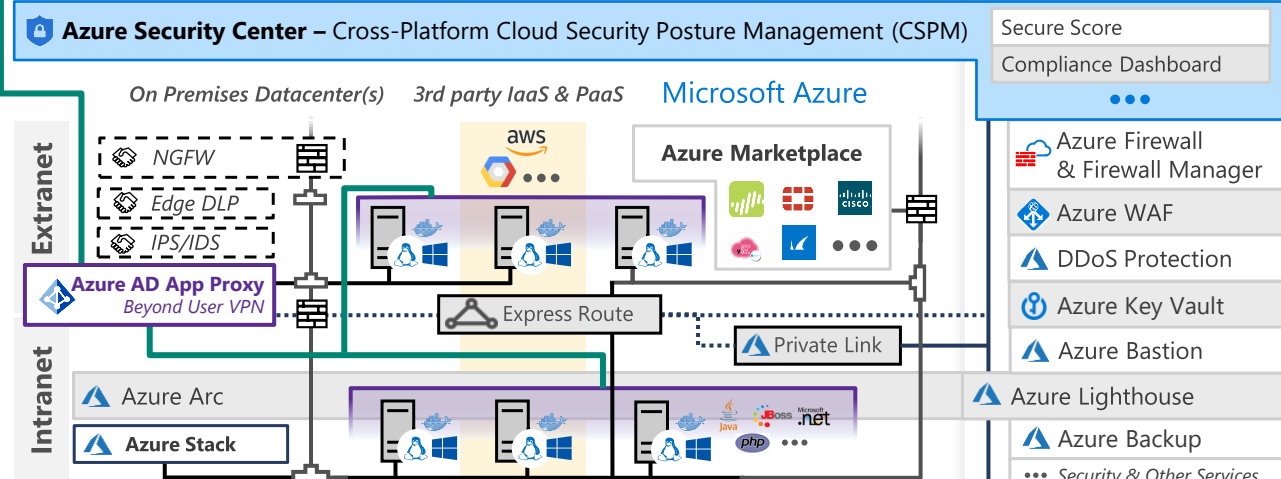


**Conditional Access** – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

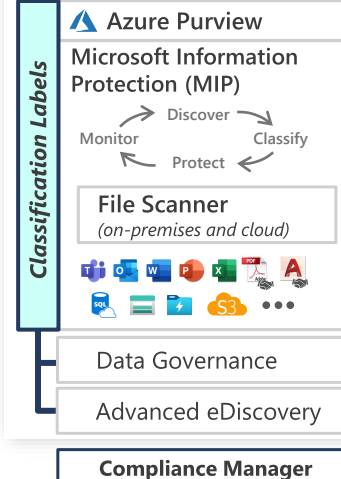
## Endpoints & Devices



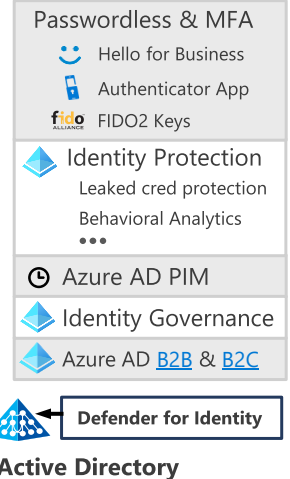
## Hybrid Infrastructure – IaaS, PaaS, On-Premises



## Information Protection



## Azure Active Directory



**Securing Privileged Access** – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users

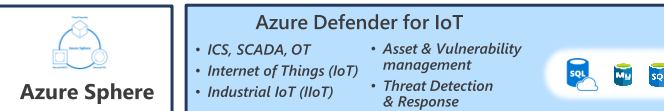
**Privileged Access Workstations (PAWs)** – Secure workstations for administrators, developers, and other sensitive users

**Microsoft Secure Score** – Measure your security posture, and plan/prioritize rapid improvement with included guidance

**Microsoft Compliance Score** – Prioritize, measure, and plan improvement actions against controls



## IoT and Operational Technology (OT)



**Azure Defender** – Cross-Platform, Cross-Cloud XDR Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses

## People Security



**GitHub Advanced Security** – Secure development and software supply chain

**Threat Intelligence** – 8+ Trillion signals per day of security context

**Service Trust Portal** – How Microsoft secures cloud services

**Security Development Lifecycle (SDL)**

# Cross-cloud and cross-platform

Comprehensive Security, Compliance and Identity capabilities that integrate with your existing solutions

## Industry Partnerships

NIST / CIS / The Open Group / Others

Microsoft Intelligent Security Association

Solution Integration and MDR/MSSP Partners

CERTs / ISACs / Others

Law Enforcement

...



## Microsoft Security, Compliance, and Identity Capabilities

 Threat Intelligence – 8+ Trillion signals per day of security context

**Access Control**  
Identity and Network

**Modern Security Operations**  
Rapid Resolution with XDR, SIEM, SOAR, UEBA and more

**Asset Protection**  
Information Protection and App Security / DevSecOps

**Technical Governance**  
Risk Visibility, Scoring, and Policy Enforcement

### People Security – User Education/Empowerment and Insider Threats



Endpoints & Devices

Software as a Service (SaaS)

Hybrid Infrastructure – IaaS, PaaS, On-Premises

IoT Devices

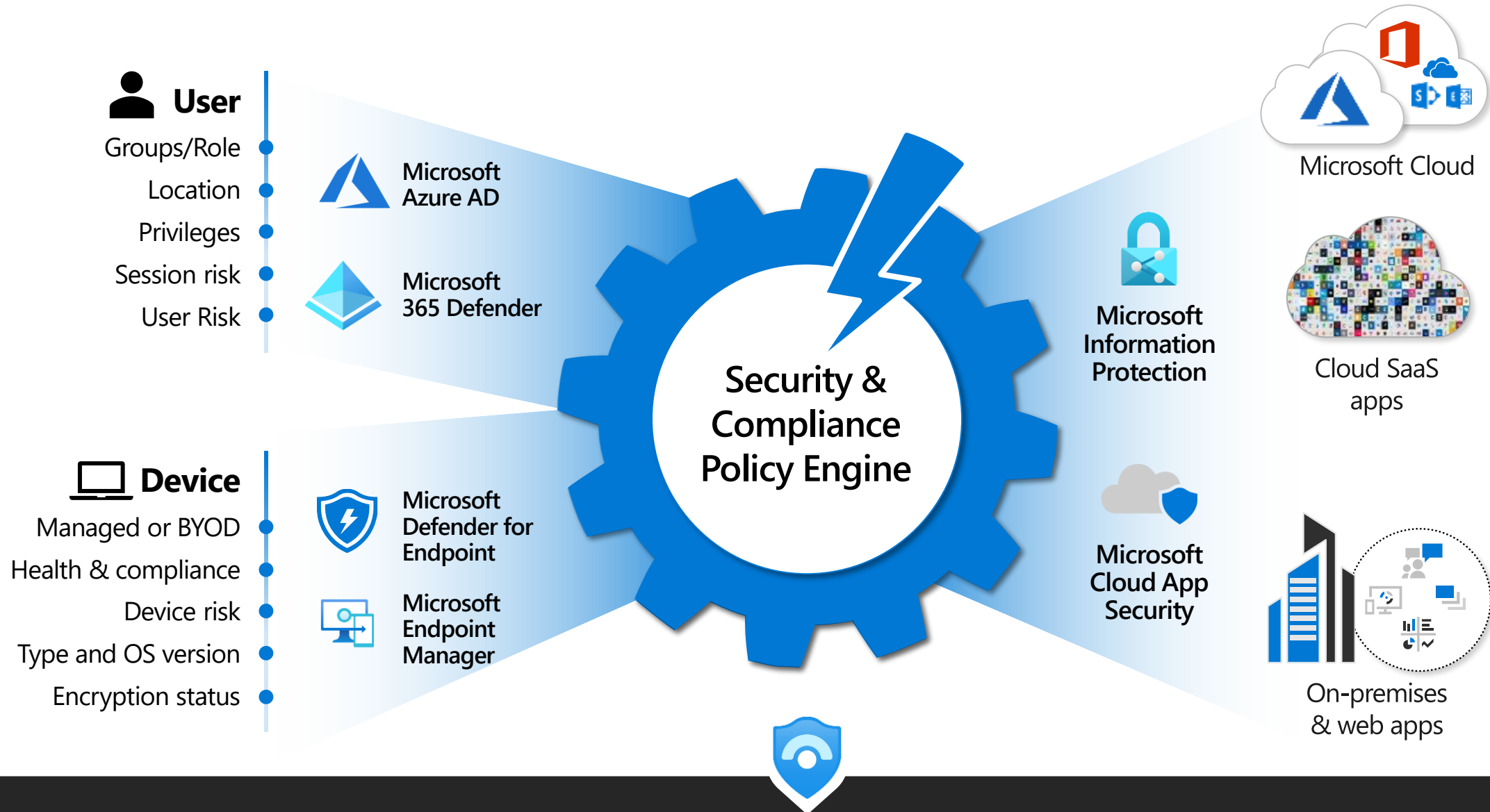
Operational Technology (OT)

Security Operations [Center] (SOC) – Reduce attacker time/opportunity to impact business



# Protect assets anywhere with Zero Trust

Verify **explicitly** | Use **least-privileged access** | Assume **breach**



Azure Sentinel

# Zero Trust User Access

## Conditional Access to Resources

