

# A Glimpse into Data Security with Sensitivity Labels

Hassan Anees

# Hassan Anees

Security Engineer@Brock Solutions



about-me.txt

## #Professional Background

Researcher > Software Engineer > Security Analyst

## #Education

University of Guelph.  
Computer Science > Psychology > Master of Cybersecurity and Threat Intelligence

## #Hobbies

I love traveling, spicy food, and snowboarding!

# What this talk is about - AGENDA

- Cloud computing
- Shared responsibility model
- What are practitioners protecting?
- Case Study
- Data Security
- Security Controls
- Data Classification
- Data Labeling with Sensitivity Labels
- Q & A

# What this talk is NOT about

- Not a sales pitch/recommendation to use one solution over another
- Does not represent the thoughts of my organization. My opinions are my own

# Raise your hands!



-  Elastic Compute Cloud (EC2)
-  Elastic Kubernetes Service (EKS)
-  Lambda
-  Simple Storage Service (S3)
-  Virtual Private Cloud
-  RDS
-  DynamoDB
-  Simple Notification Service
-  CloudWatch
-  CloudFormation
-  IAM
-  KMS



-  Virtual Machine
-  Azure Kubernetes Service (AKS)
-  Azure Functions
-  Blob Storage
-  Virtual Network
-  SQL Database
-  Cosmos DB
-  Service Bus
-  Monitor
-  Resource Manager
-  Active Directory
-  Key Vault



-  Compute Engine
-  Google Kubernetes Engine (GKE)
-  Cloud Functions
-  Cloud Storage
-  Virtual Private Cloud
-  Cloud SQL
-  Firebase Realtime Database
-  Firebase Cloud Messaging
-  Cloud Monitoring
-  Deployment Manager
-  Cloud Identity
-  Cloud KMS

# What really is cloud computing?

On-demand access to computer resources:

- Virtual servers
- Storage
- Network capabilities

# Why does the industry lean to cloud computing?

Reduced maintenance

Scalability

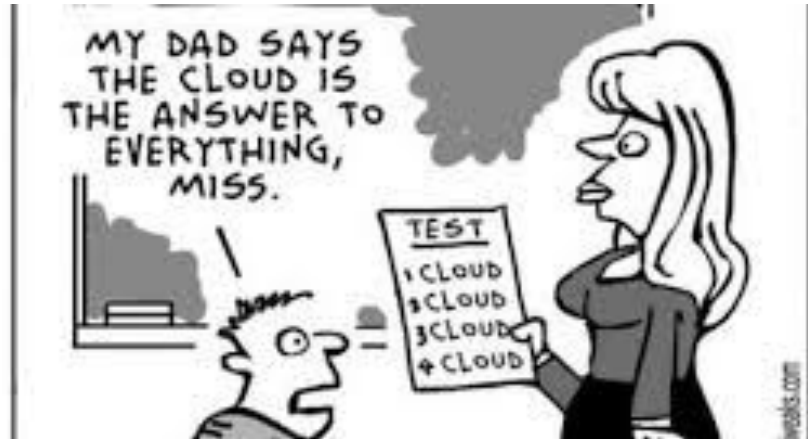
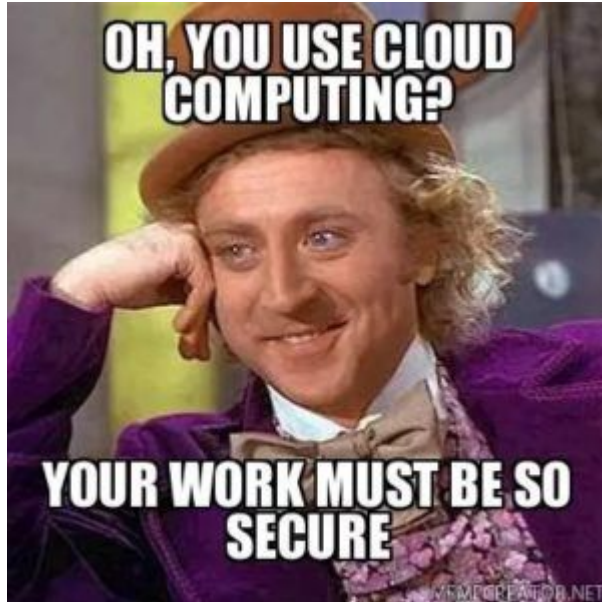
Regulatory compliance

Enhanced protection

Resiliency & Redundancy

- Disaster recovery
- Business continuity

# The Illusion





# Shared Responsibility Model

Responsibility		SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	Customer	Customer	Customer	Customer
	Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
	Accounts and identities	Customer	Customer	Customer	Customer
Responsibility varies by type	Identity and directory infrastructure	Shared	Shared	Customer	Customer
	Applications	Microsoft	Shared	Customer	Customer
	Network controls	Microsoft	Shared	Customer	Customer
	Operating system	Microsoft	Microsoft	Customer	Customer
Responsibility transfers to cloud provider	Physical hosts	Microsoft	Microsoft	Microsoft	Customer
	Physical network	Microsoft	Microsoft	Microsoft	Customer
	Physical datacenter	Microsoft	Microsoft	Microsoft	Customer



Microsoft



Customer



Shared

# What are security practitioners protecting?



# Case Study – Desjardins Data Breach (2019)

## OPC Investigation into Desjardins data breach

**What was it:** Insider risk security incident

**What kind of data?:** Personally Identifiable Information (PII)

**Impact:** 2.9 million people

**How did it happen:** Exfiltration activities over the course of 2 years

# Thought Experiment - could it be prevented?

- Access reviews/controls
- Least privilege principle
- Threat hunting / proper alerting
- **Sensitivity labels**

# Data Security

# Data Security - Holistic View

Practices that keep the CIA(AA) triad intact

- Preventing theft
- Corruption
- Disruption of availability
- How user's handle data (internal & external)

How do we do accomplish this?

- **Security controls!**

# Security Controls

Phase 1: Create **Policy, standard, and/or procedure** — this defines the "what" and "why"

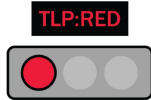
Phase 2: Enforce with (ideally) **technology** — this is the "how" or “mechanism”



# Data Classifications - The “What” & “Why”

## Traffic Light Protocol

- TLP:CLEAR
- TLP:GREEN
- TLP:AMBER
- TLP:AMBER+STRICT
- TLP:RED



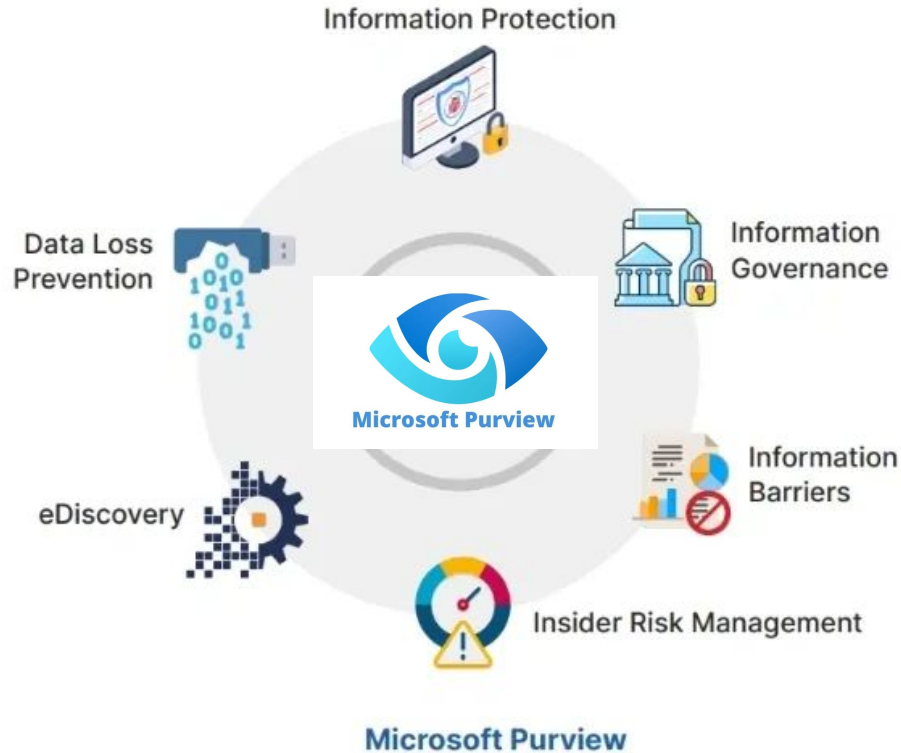
## Ontario Gov.

- Unclassified
- Low sensitivity
- Medium sensitivity
- High sensitivity

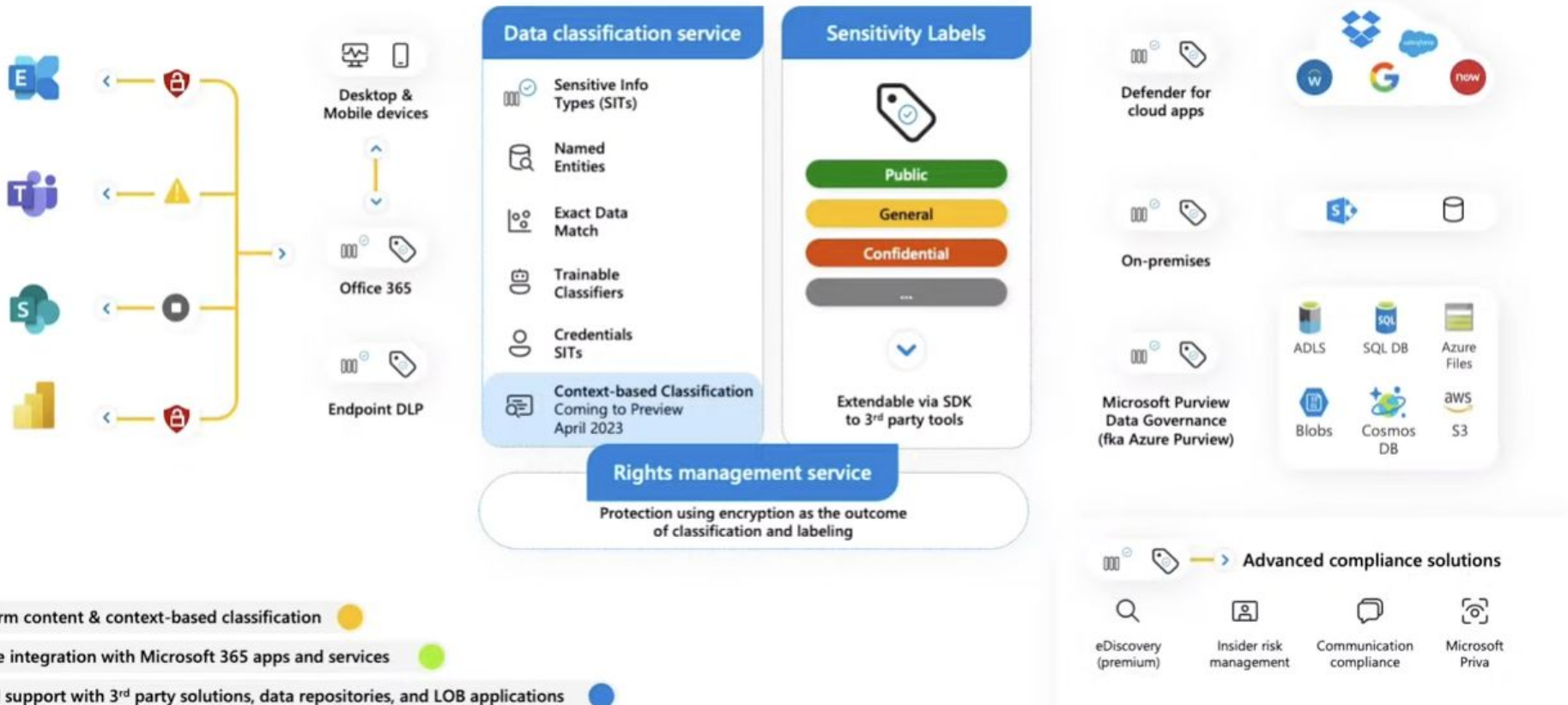
## US Gov. (DC Data Policy)

- Level 0 Open
- Level 1 Public
- Level 2 For District Government
- Level 3 Confidential
- Level 4 Restricted Confidential

# Purview (Technology) – The “How” / “Mechanism”



# Microsoft Purview Information Protection



# Strategic Prerequisites

1. Data inventory (understand what you hold)
2. Data classification scheme - (Planning for label names)
  - a. Align with compliance requirements (Ask Legal, HR, research your industry)
3. Strong communication plan -
  - a. Get a sponsor who can push policies (CISO, Executive leadership)
4. Stakeholders involved (HR, Legal, Finance, IT, Sales, Data governance...)
  - a. Business driven. NOT IT driven
5. **Security Education is paramount here**
  - a. Seminars
  - b. Training modules
  - c. More seminars
  - d. Clear documentation

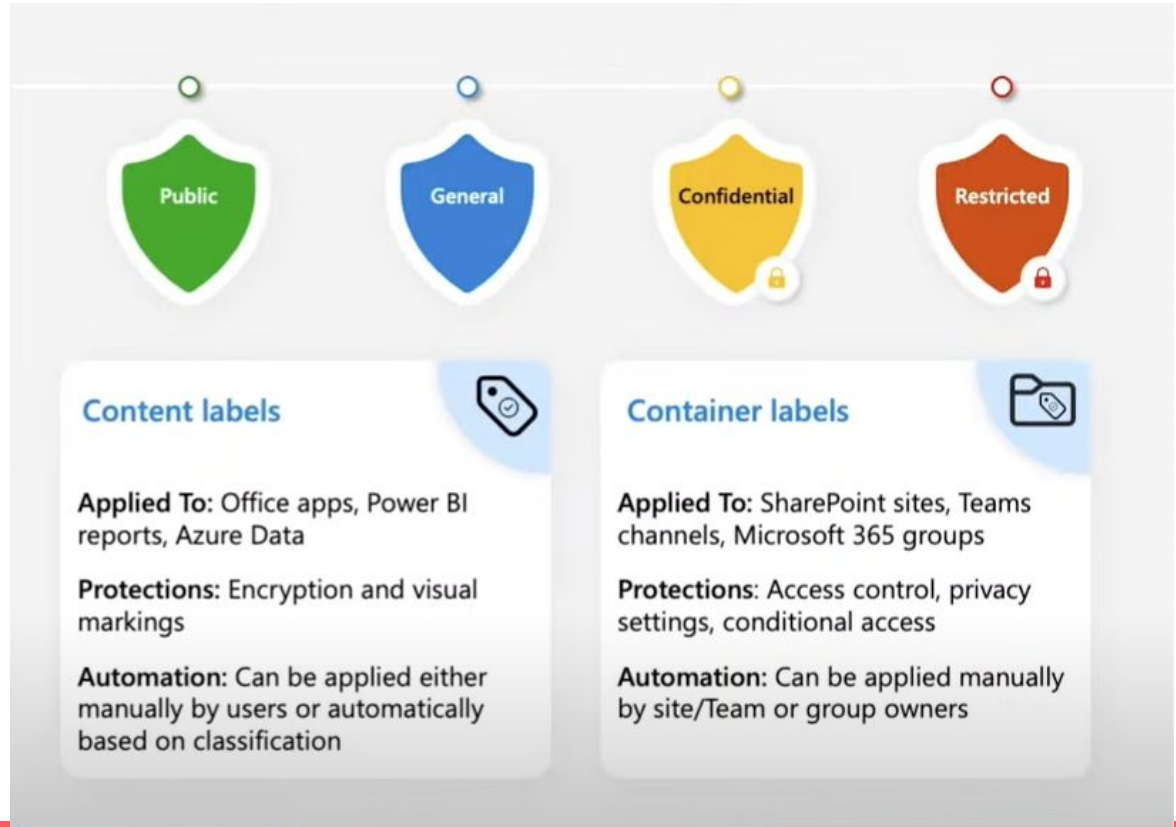
# Technical Prerequisites

1. Enable co-authoring
2. Enable labeling for containers (groups & sites)
3. Enable sharepoint permission extension

# What are Sensitivity Labels (Information Protection)

It is a stamp on (scope):

- Files
- Emails
- SharePoint sites
- Security Groups
- Teams channels



# What can Sensitivity Labels do?

## Mark content

- Watermarks
- Header & Footer content

## Establish access control

- Tracking & Revoking documents
- Apply expiration

## Apply Encryption

- Azure Right Management Service (RMS) under the hood
- Encryption at-rest and in-transit

## Link to Conditional Access Policies

# There is a lot..

## Define the scope for this label

Labels can be applied to data assets and containers (like SI know where you want this label to be used so we can show settings. [Learn more about label scopes](#)

### ☒ Files & other data assets

Label files and data assets in Microsoft 365, Microsoft other platforms.

### ☒ Emails

Label messages sent from all versions of Outlook.

### ☒ Meetings

Label calendar events and meetings schedules in Outlook

Parent label will automatically inherit meeting scope from sub labels

### ☒ Groups & sites

Con Microsoft Purview

Mic

Won 365 s this li

## New sensitivity label

- ☒ Label details
- ☒ Scope
- ☒ Items
- ☐ Groups & sites

### Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. [Learn more about access control settings](#)

- ☐ Remove access control settings if already applied to items
- ☒ Configure access control settings

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied

## Choose protection settings for the types of items you selected

The protection settings you configure will be enforced when the label is applied to items in Microsoft 365.

- ☒ **Control access**  
Control who can access and view labeled items.
- ☐ **Apply content marking**  
Add custom headers, footers, and watermarks to labeled items.
- ☐ **Protect Teams meetings and chats**

## Assign permissions

Only the users or groups you choose will be assigned permissions to use the content that has this label applied. You can choose from existing permissions (such as Co-Owner, Co-Author, and Reviewer) or customize them to meet your needs.

+ Add all users and groups in your organization

+ Add any authenticated users

+ Add use

+ Add just

+ Add spe

+ Add spe

Enter :

## Choose permissions

Choose which actions would be allowed for this user/group. [Learn more](#)

Editor

- ☒ View content(VIEW)
- ☒ View rights(VIEWRIGHTSDATA)
- ☒ Edit content(DOCEDIT)

## Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.


- ☐ **Control external sharing from labeled SharePoint sites**  
When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.
- ☒ **Use Azure AD Conditional Access to protect labeled SharePoint sites**  
You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.
- ☐ Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't hybrid




# What does it look like?


## Setting up a label


### Sensitivity


 Select a Label


**rsimone@vanarsdelltd.com**


 Personal

 Public

 General







 Confidential


 Highly Confidential


 [Learn More](#)

Untitled - Message (HTML)

File Message Insert Draw Options Format Text Review Help

   Calibri (Body) 11 **B** *I* U   


 Confidential\Recipients Only - Confidential data that requires protection and that can be viewed by the recipients only.

 Send

To

Cc

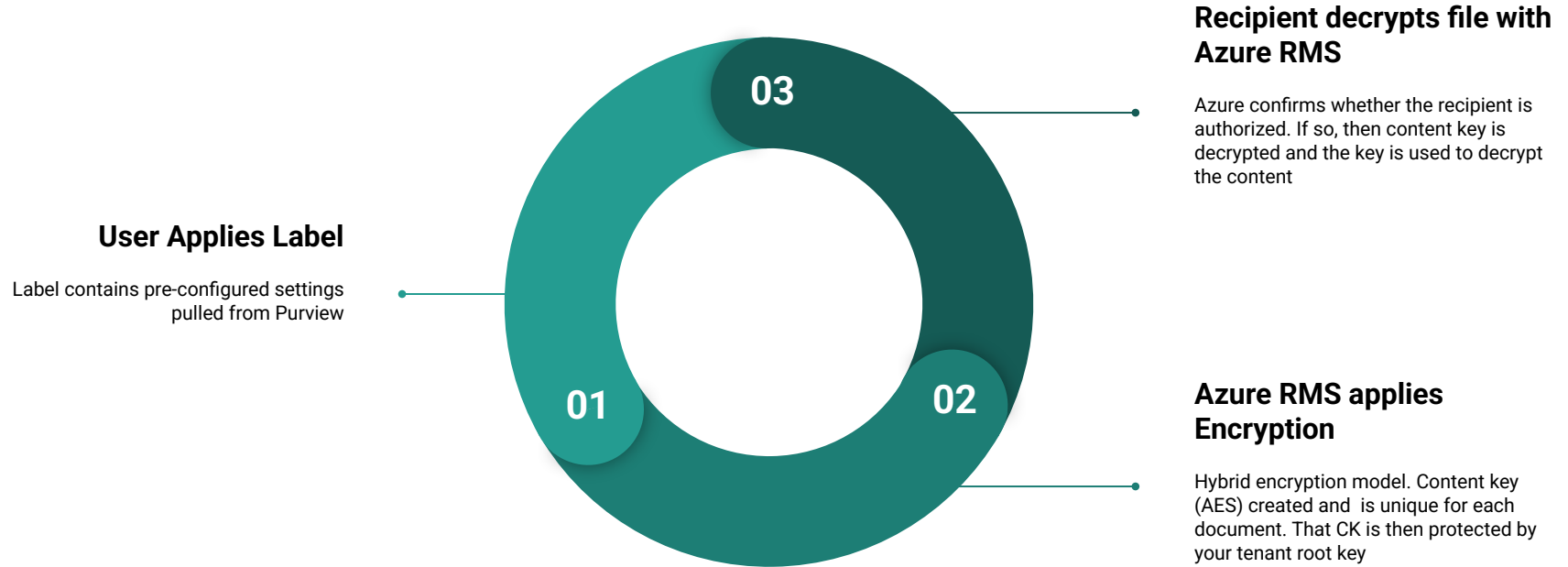
Subject

 Confidential\Recipients Only

Pro soluta aliquid lucilius at, mei graecis qualisque eu. Sumo eruditi deterruisset est te, te sed error simul aliquam. Eos ut laoreet omittam, cum ei nostro graecis, doming putant definitionem et eos.

# Under the hood - Azure RMS

Technology used to encrypt, assign rights, and control access



# What does it mean?

Threat actor is denied access to the data

File is protected regardless of location

- USB drive
- Local hard drive
- Dropbox, Google drive



# Key things for technical implementation

1. Choose your scope (Files, Emails, Containers...)
2. Priority of labels matter
3. Labeling policies
  - a. Default sensitivity label
  - b. Label automatically
  - c. Recommend users to apply
  - d. Require labels on document creation
4. Simulate manual labeling (limited users)
5. Simulate bulk labeling via containers (Container level labels)
6. Simulate auto-labeling
  - a. Trainable classifiers
7. Iterate and adjust as needed

# Again, cloud is not a magical solution

Any gaps? Are there ways threat actors still bypass this?

- Zero-day exploits
- Social engineering (all you need are credentials)
- Mislabeling
  - User error
  - Failed auto-labeling

# Limitations you should know..

- External sharing is clunky
- Performance hits
- Prone to user error (mislabeling)
- Require Microsoft account to leverage Azure RMS feature
- Expensive

# The Big Picture

# Technologies that can be tied with labeling

Retention labels

Data loss prevention

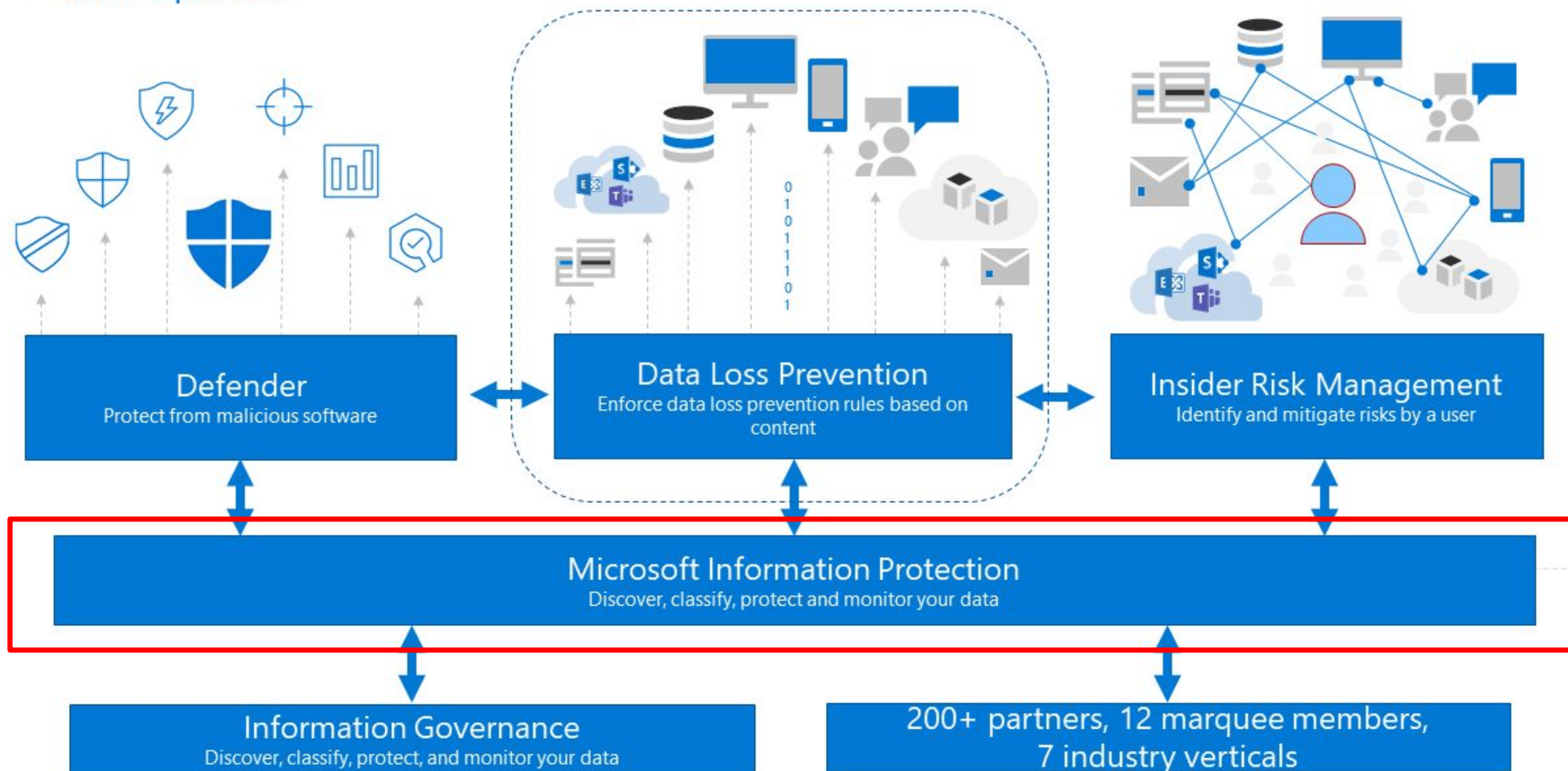
Insider risk management

Conditional access policies



# Microsoft Security and Compliance

Unified capabilities



# Wrapping up

The details matter

- Descriptions
- # of labels
- Colors
- Naming convention

Data labeling is business driven

Security education is paramount

This will be frustrating to implement

- Getting everyone to use labeling is difficult (behavior change)

# References

- Desjardins Data Breach Investigation :  
<https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-in-to-businesses/2020/pipeda-2020-005/>
- Shared Responsibility Model:  
<https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>
- Ontario data :  
<https://www.ontario.ca/page/corporate-policy-information-sensitivity-classification>
- TLP :  
[https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-us age](https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-us-age)
- US (DC Data Policy) : <https://opendata.dc.gov/pages/data-policy>

# Q & A

Thank you



**Hassan Anees**

Cyber Security Engineer | MSc Cybersecurity  
| ISC2 CC | Leveraging ☁️ 🖥️ AWS/Azure/G...



<https://hassananees.com/>