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!

aws	Azure	Google Cloud
Elastic Compute Cloud (EC2)	Virtual Machine	Compute Engine
Elastic Kubernetes Service (EKS)	Azure Kubernetes Service (AKS)	Google Kubernetes Engine (GKE)
Lambda	Azure Functions	Cloud Functions
Simple Storage Service (S3)	Blob Storage	Cloud Storage
Virtual Private Cloud	Virtual Network	Virtual Private Cloud
RDS	SQL Database	Cloud SQL
DynamoDB	Cosmos DB	Firebase Realtime Database
Simple Notification Service	Service Bus	Firebase Cloud Messaging
CloudWatch	Monitor	Cloud Monitoring
CloudFormation	Resource Manager	Deployment Manager
IAM	Active Directory	Cloud Identity
KMS	Key Vault	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

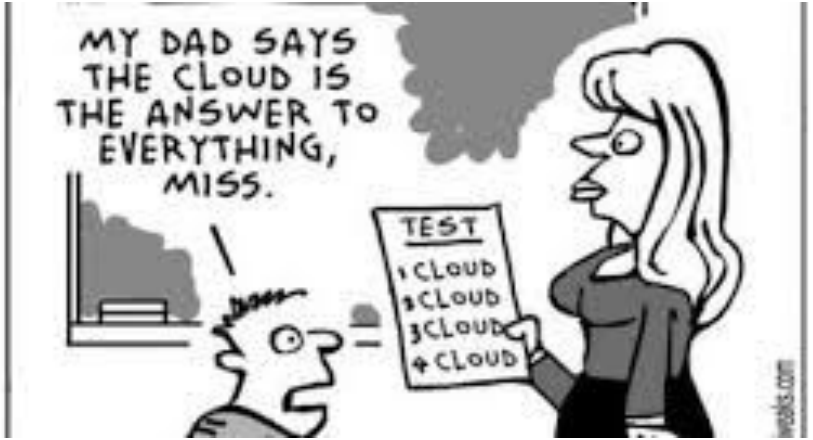
Regulatory compliance

Enhanced protection

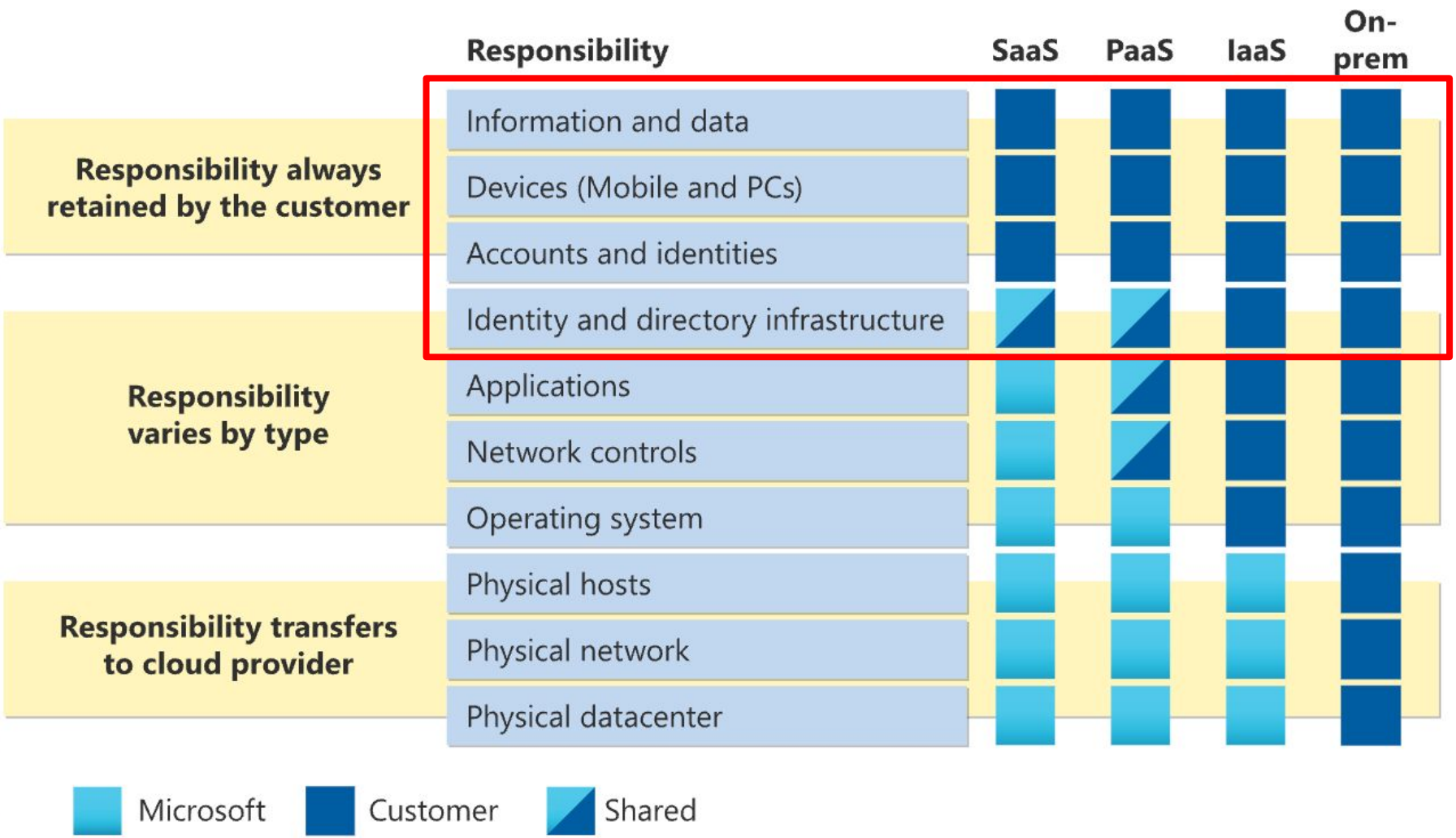
Resiliency & Redundancy

- Disaster recovery
- Business continuity

The Illusion



Shared Responsibility Model


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

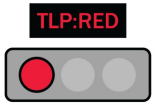
Phase 1: Create **Policy**, **standard,** and/or **procedure** — this defines the "what" and "why"

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



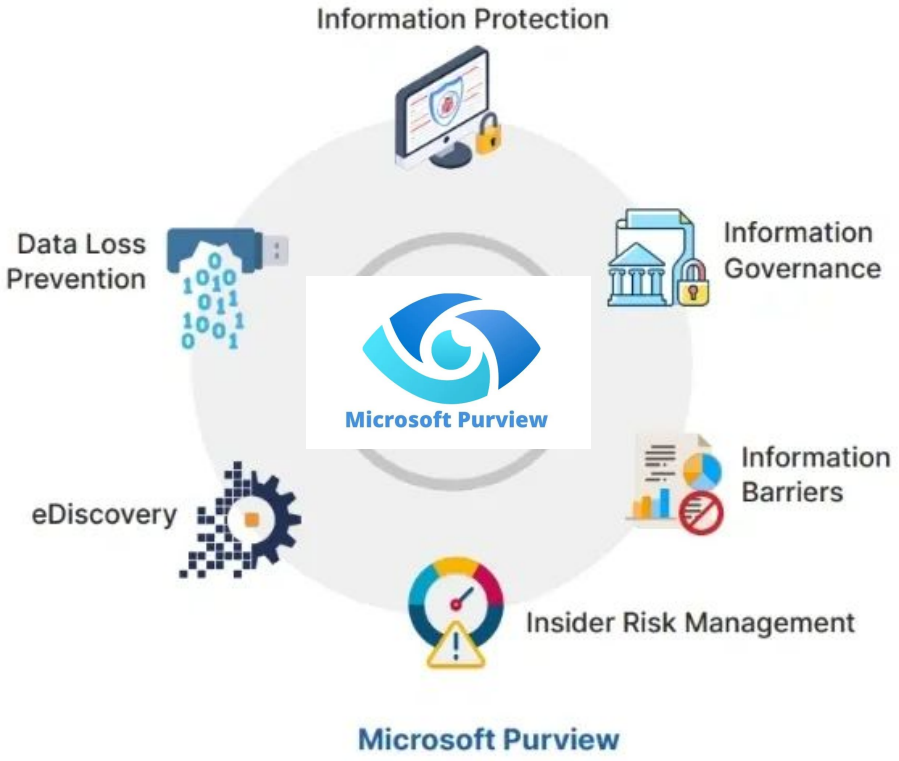
Ontario Gov.

- 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

- Uniform content & context-based classification
- Native integration with Microsoft 365 apps and services
- Broad support with 3rd party solutions, data repositories, and LOB applications

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

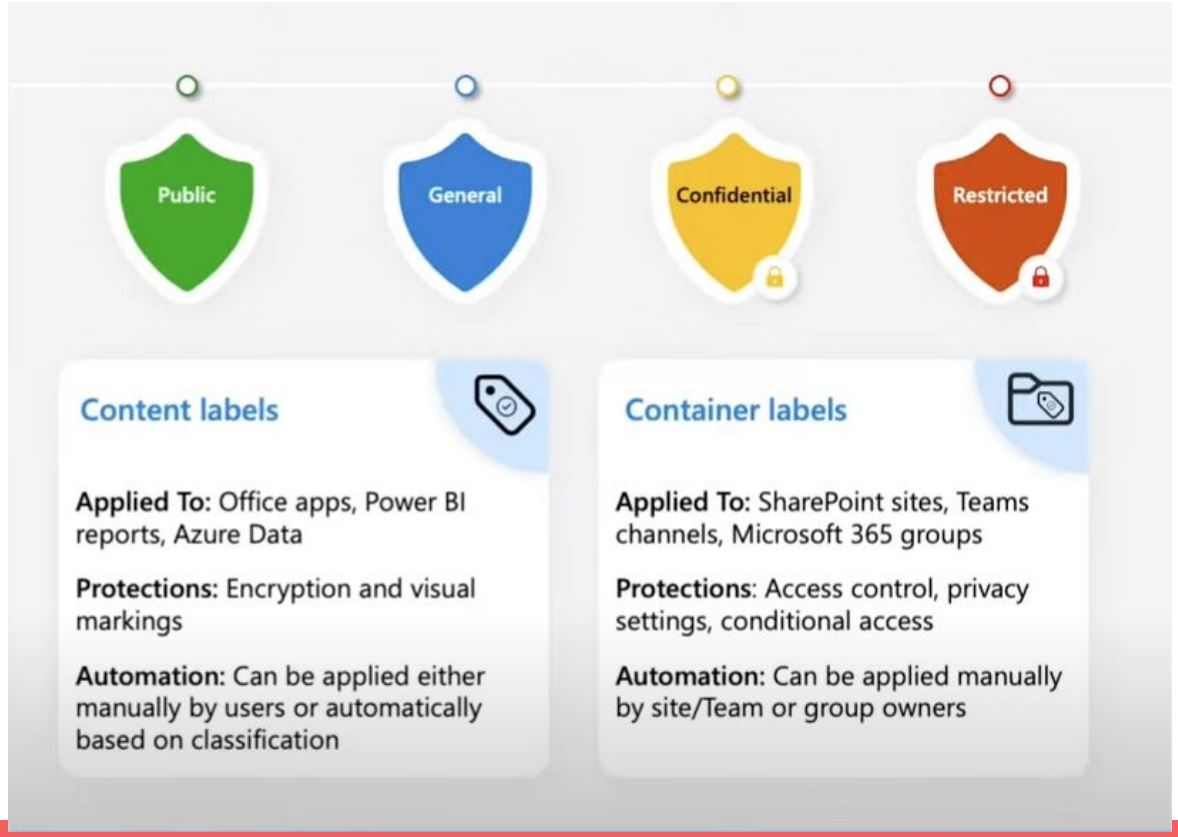
Technical Prerequisites

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

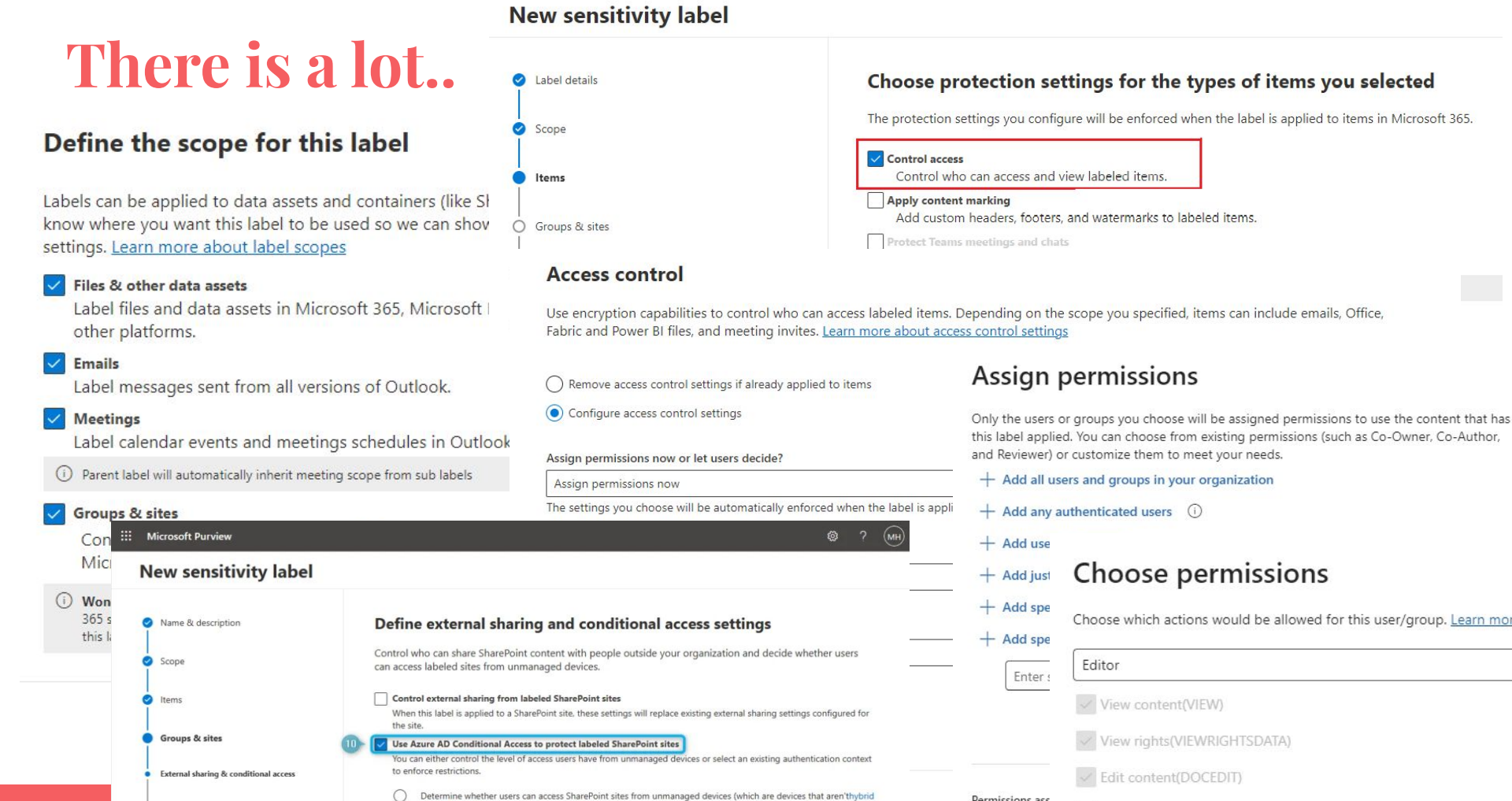
- Tracking & Revoking documents
- Apply expiration

Apply Encryption

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

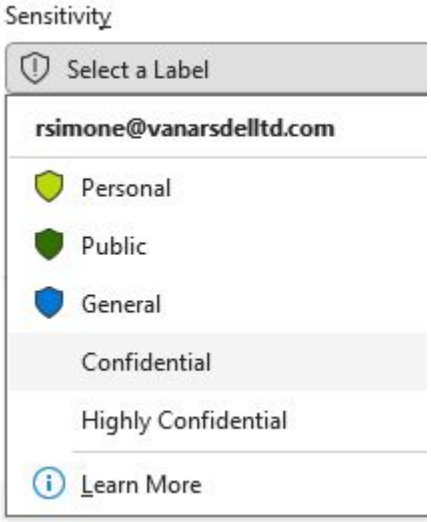
Link to Conditional Access Policies

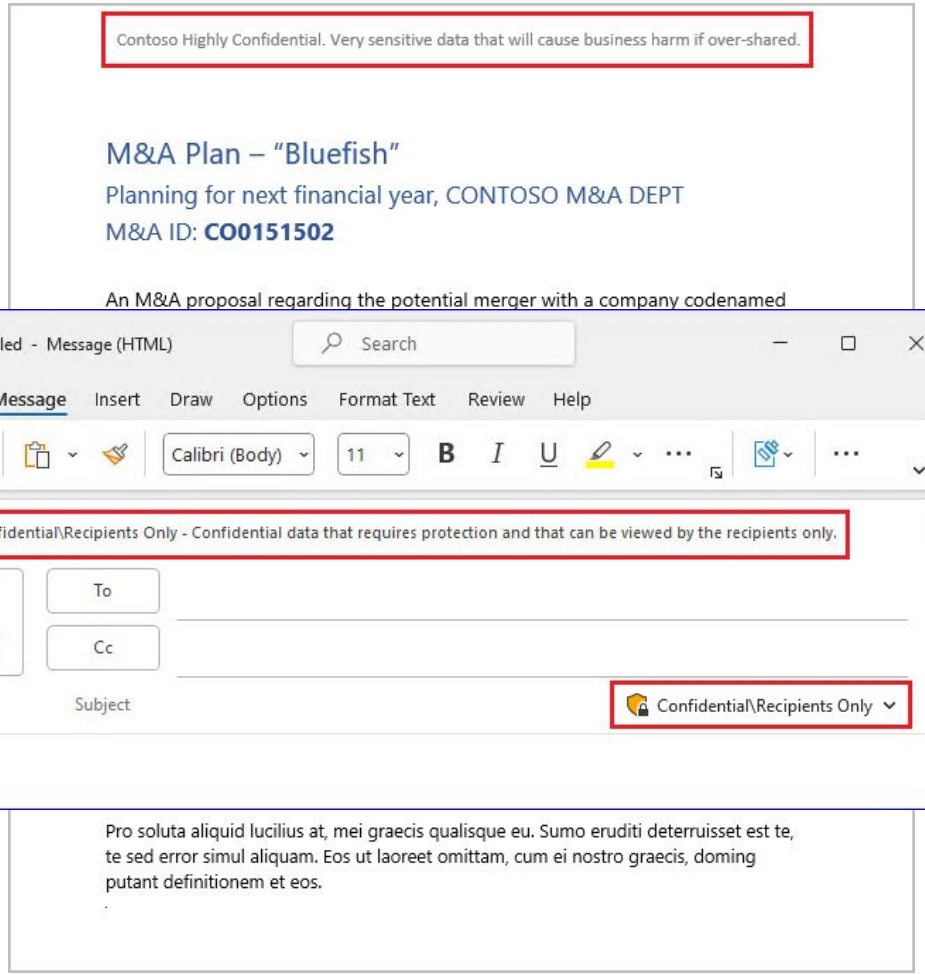
There is a lot..



What does it look like?

Setting up a label



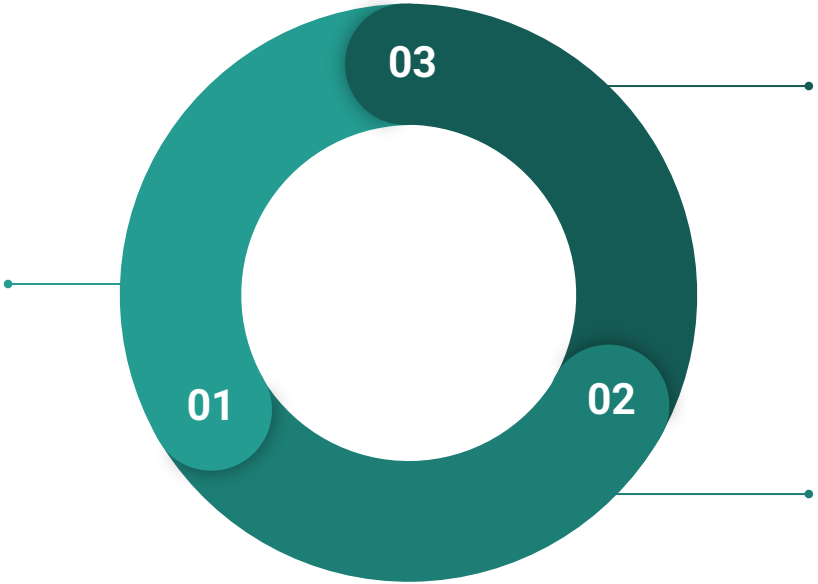


Under the hood - Azure RMS

Technology used to encrypt, assign rights, and control access

User Applies Label

Label contains pre-configured settings pulled from Purview



Recipient decrypts file with Azure RMS

Azure confirms whether the recipient is authorized. If so, then content key is decrypted and the key is used to decrypt the content

Azure RMS applies Encryption

Hybrid encryption model. Content key (AES) created and is unique for each document. That CK is then protected by your tenant root key

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

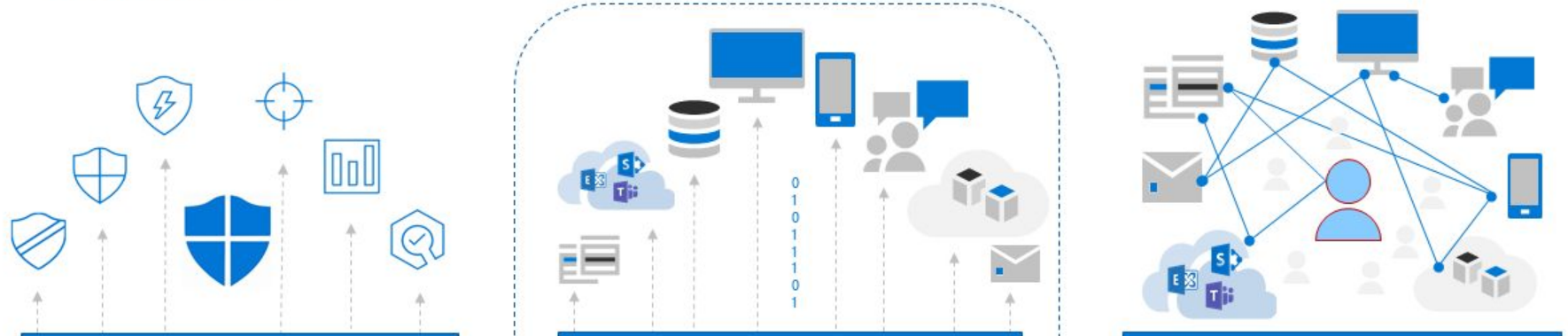
Data loss prevention

Insider risk management

Conditional access policies

Microsoft Security and Compliance

Unified capabilities



Defender
Protect from malicious software

Data Loss Prevention
Enforce data loss prevention rules based on content

Insider Risk Management
Identify and mitigate risks by a user

Microsoft Information Protection
Discover, classify, protect and monitor your data

Information Governance
Discover, classify, protect, and monitor your data

200+ partners, 12 marquee members, 7 industry verticals

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-into-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-usage
- US (DC Data Policy) : https://opendata.dc.gov/pages/data-policy

Q & A

Thank you

https://hassananees.com/