Planning for Security in Microsoft Online

Global Azure Bootcamp 2019

Jason Condo

Practice Director – Modern Workplace and Cloud Infrastructure

jcondo@bennettadelson.com

2019 Global Azure BOOTCAMP

BENNETT ADELSON

Company Highlights

- Established in 1996, with more than 1,000 clients serviced to date
- Headquartered in Cleveland, with a satellite office in Columbus
- Local and national clients, with international service delivery capabilities and experience

Eight Practice Disciplines

Architecture & Development

Business Intelligence

Information Worker

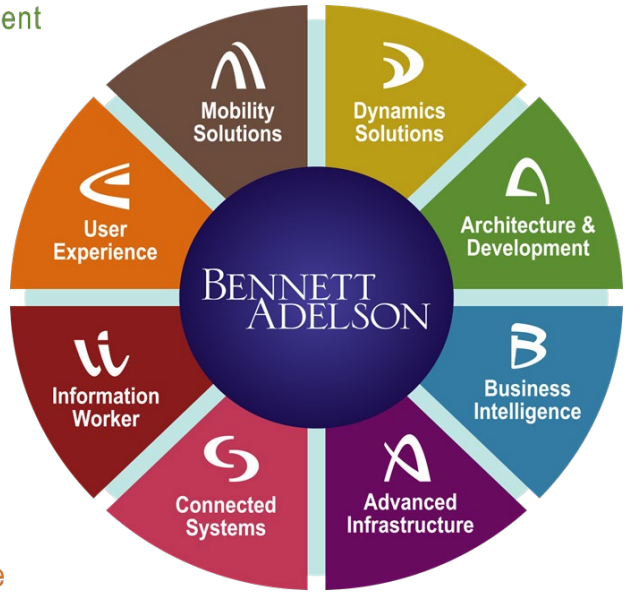
Advanced Infrastructure

Connected Systems

Mobility Solutions

Dynamics Solutions

User Experience



Significant Achievements

- 2017 and 2016 Top 200 Microsoft Partners, Redmond Channel Partners
- 2015 Top 100 Most Promising Microsoft Solution Providers, CIO Review
- 2011 Microsoft Partner of the Year, Heartland District
- 2010 Microsoft Partner of the Year Finalist
- Office 365 TAP Member
- Office 365 FastTrack Partner
- Office 365 Preferred Deployment Partner
- Member of Microsoft's SharePoint Patterns & Practices Council
- Members of the Microsoft Partner Advisory Council
- Founded the Cleveland SharePoint and .NET Special Interest Group
- Microsoft Gold Partners: Cloud, Collaboration and Content
- Microsoft Silver Partners: Cloud Productivity, Windows and Devices

What you should get out of this session

- Understand what some of the Microsoft tools are for security and compliance
- Understand impacts for end-users to adopt tools for security and compliance
- Best practice guidance on implementing security
- Some of what is and is not possible in the Microsoft cloud
- Sites to remember

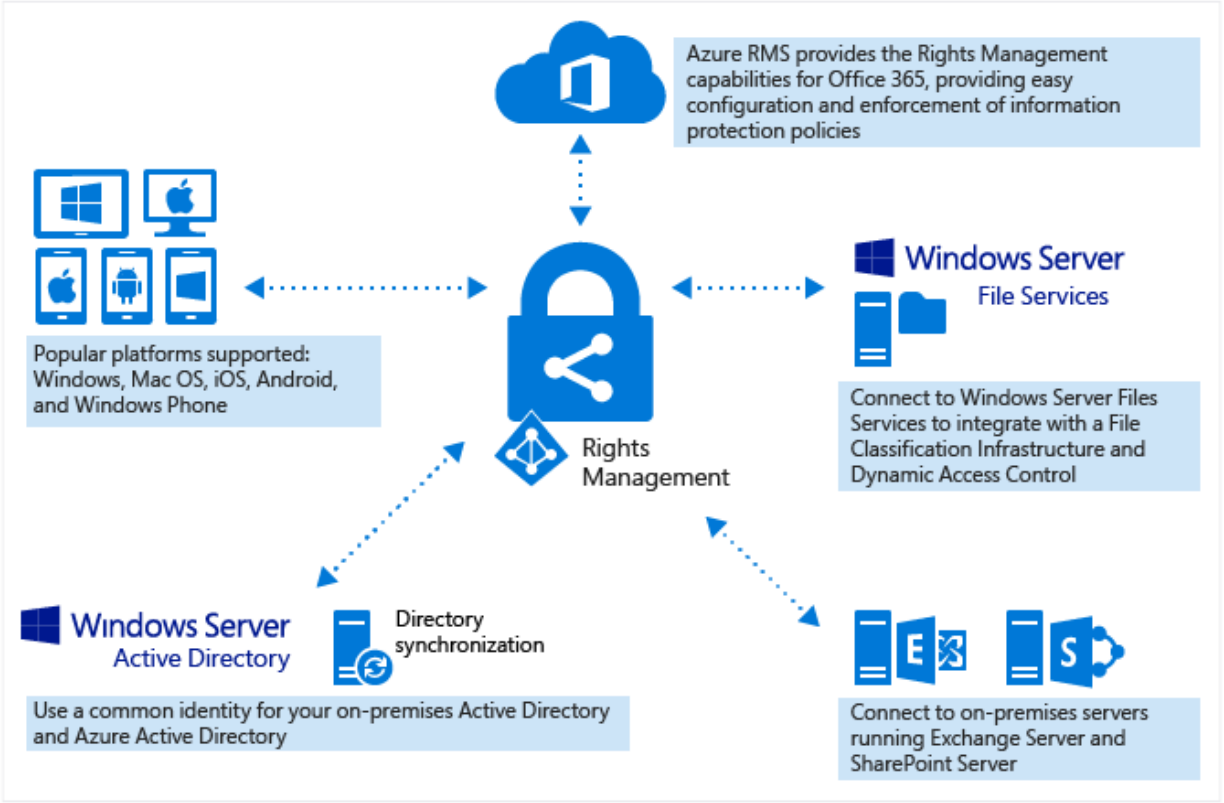
The Assets

- These are pillars that we must protect to enable collaboration from everywhere
  - Identity
  - Devices
  - Apps
  - Data

Evolution on Microsoft document/file protection

- Started with the on-prem
  - Active Directory
  - Active Directory Rights Management Service (RMS)
  - Server File Classification Infrastructure (FCI)

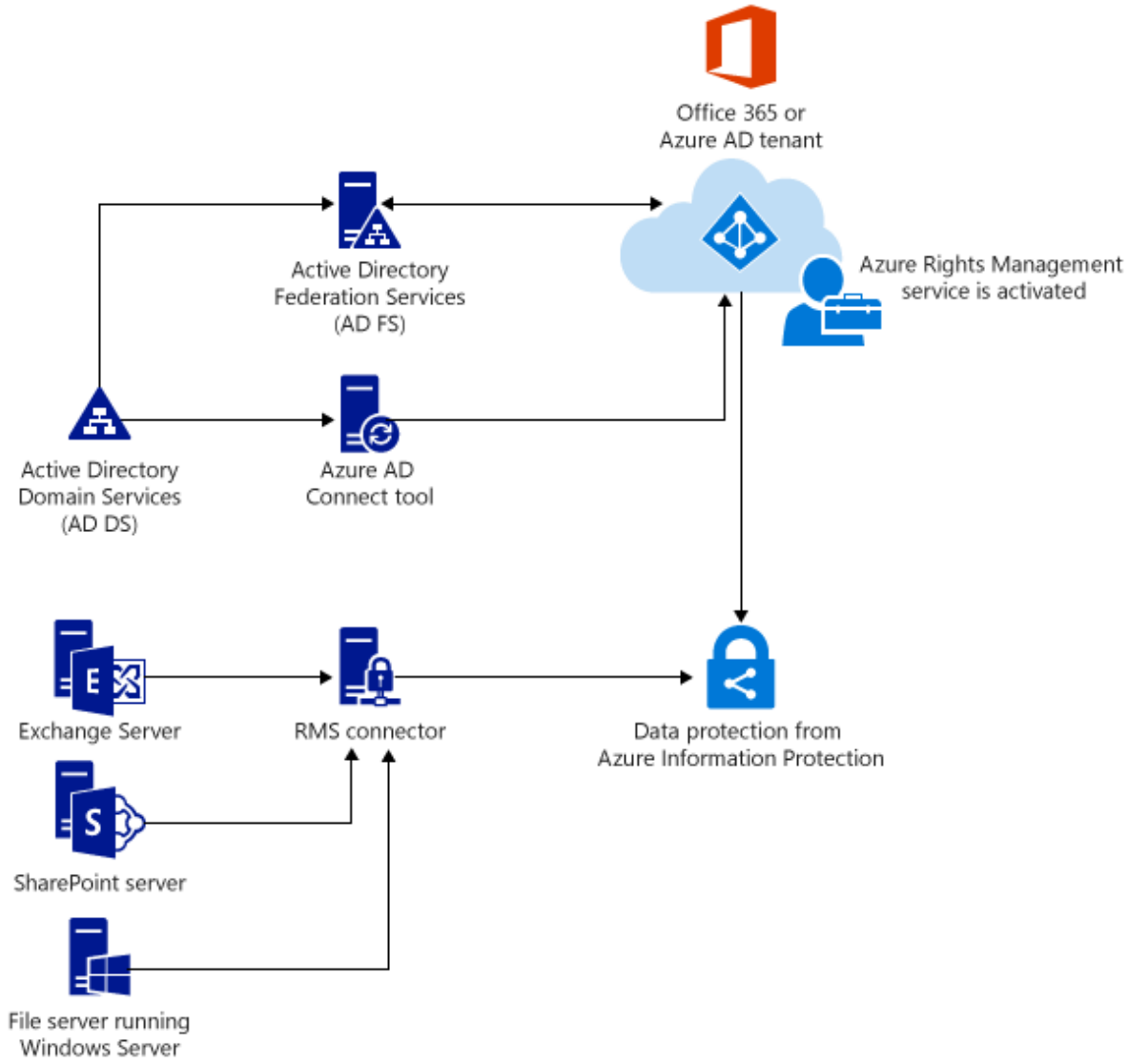
- Extending the walls
  - Expose AD RMS to the DMZ
  - Implement Active Directory Federation Server (AD FS)



Evolution on Microsoft document/file protection

BENNETT ADELSON

- Started with the on-prem
  - Active Directory
  - Active Directory Rights Management Service (RMS)
  - Server File Classification Infrastructure (FCI)
- Extending the walls
  - Expose AD RMS to the DMZ
  - Implement Active Directory Federation Server (AD FS)
- Move to the cloud (Hybrid)
  - Azure AD
  - Azure RMS
  - Azure Information Protection
  - Azure Information Rights Management



BENNETT ADELSON

Evolution on Microsoft document/file protection

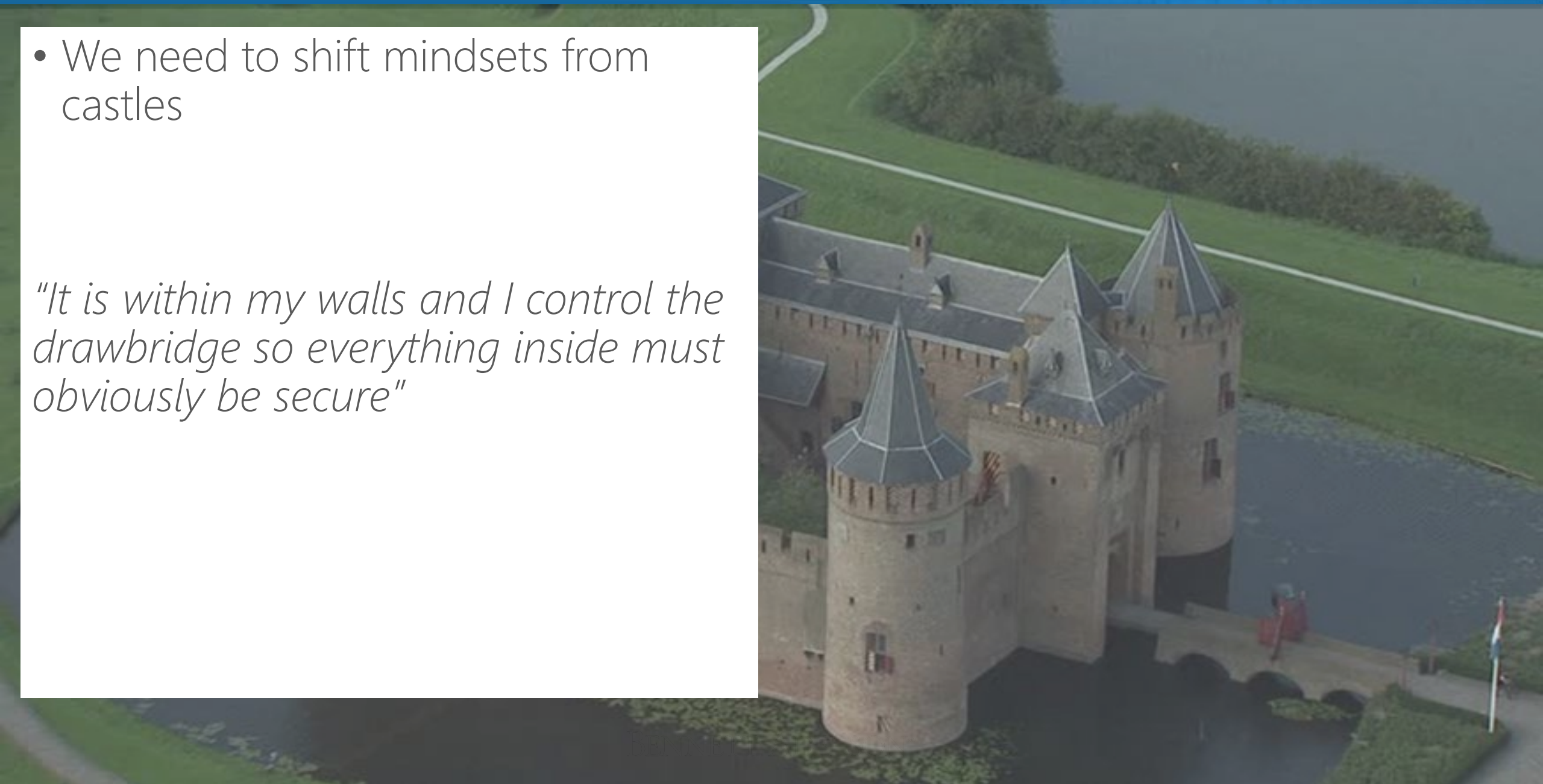
- Started with the on-prem
  - Active Directory
  - Active Directory Rights Management Service (RMS)
  - Server File Classification Infrastructure (FCI)
- Extending the walls
  - Expose AD RMS to the DMZ
  - Implement Active Directory Federation Server (AD FS)
- Move to the cloud (Hybrid)
  - Azure AD
  - Azure RMS
  - Azure Information Protection
  - Azure Information Rights Management
- Embrace the Cloud
  - Azure AD Joined Devices
  - Azure AD Identities
  - Microsoft Information Protection
  - Windows Information Protection
  - ATP and ATA, Security and Compliance Center

Old thoughts on security

BENNETT ADELSON

- We need to shift mindsets from castles

"It is within my walls and I control the drawbridge so everything inside must obviously be secure"



MICROSOFT'S INFORMATION PROTECTION SOLUTIONS

MICROSOFT CLOUD APP SECURITY

Visibility into 15k+ cloud apps, data access & usage, potential abuse

OFFICE 365 ADVANCED SECURITY MANAGEMENT

Visibility into Office 365 app usage and potential data abuse

WINDOWS INFORMATION PROTECTION

Separate personal vs. work data on Windows 10 devices and prevent work data from traveling to non-work locations

MESSAGE ENCRYPTION

Send encrypted emails in Office 365 to anyone – inside or outside of the company

CONDITIONAL ACCESS

Control access to files based on policy, such as identity, machine configuration, geo location

AZURE INFORMATION PROTECTION

Classify, label & protect files – beyond Office 365, including on-prem & hybrid

OFFICE 365 DLP

Prevent data loss across Exchange Online, SharePoint Online, OneDrive for Business

ISV APPLICATIONS

Enable ISV partners to consume labels, apply protection

OFFICE APPS

Protect sensitive information while working in Excel, Word, PowerPoint, Outlook

OFFICE 365 ADVANCED DATA GOVERNANCE

Apply retention and deletion policies to sensitive and important data in Office 365

SHAREPOINT & GROU

Protect files in libraries and l

Data Lifecycle Management

INFORMATION PROTECTION LIFECYCLE

Detect

Scan & detect sensitive data based on policy

Classify

Classify data and apply labels based on sensitivity

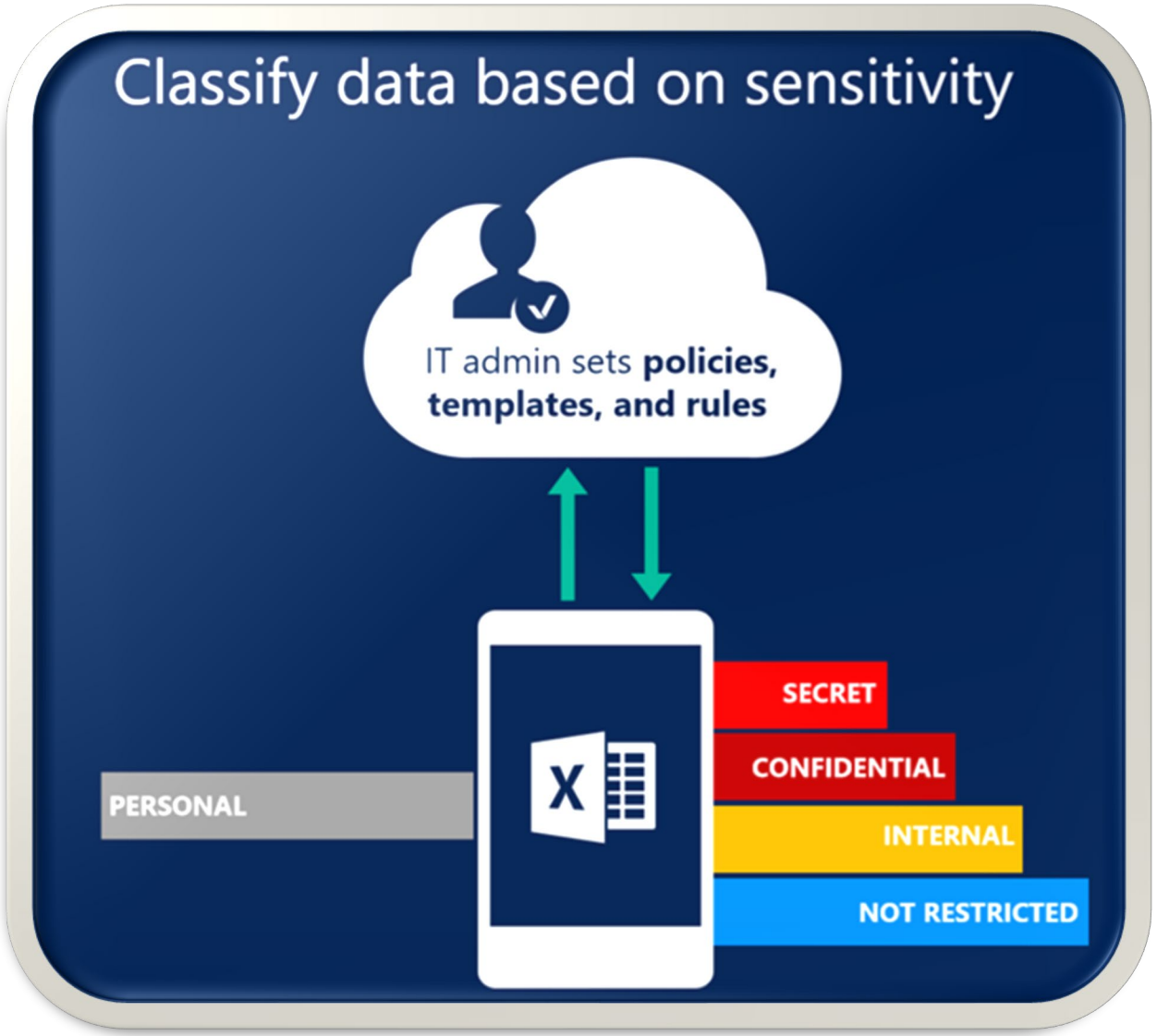
Protect

Apply protection actions, including encryption, access restrictions

Monitor

Reporting, alerts, remediation

Classify Data – Begin the Journey



- Start Simple
  - Start with data that is most sensitive
  - IT can set automatic rules, users can complement them
  - Associate actions such as visual markings and protection
- Key considerations:
  - Is there an automated way to discover important data?
  - Which regulations and compliance factors matter?
  - Is my data spread out across devices, cloud & on prem?
  - Is my data spread out geographically?
  - Are certain employees or groups more relevant for discovery?
  - Do I know the characteristics of sensitive or important data?

How **Classification** Works

BENNETT ADELSON

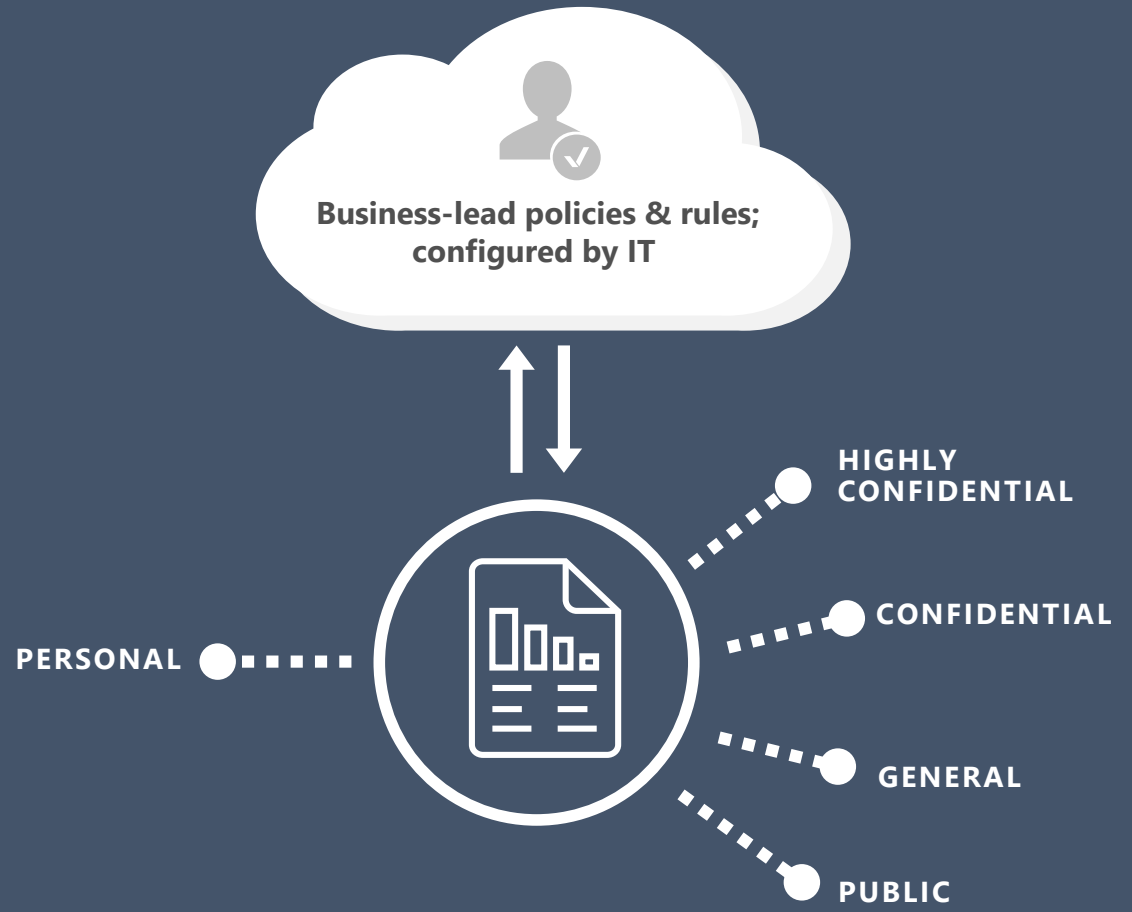
CLASSIFY INFORMATION BASED ON **SENSITIVITY**

Automatic classification
Policies can be set by IT Admins for automatically applying classification and protection to data

Recommended classification
Based on the content you're working on, you can be prompted with suggested classification

Manual reclassification
You can override a classification and optionally be required to provide a justification

User-specified classification
Users can choose to apply a sensitivity label to the email or file they are working on with a single click



SENSITIVITY LABELS **PERSIST WITH THE DOCUMENT**

Document labeling – what is it?

Metadata written into document files

Travels with the document as it moves

In clear text so that other systems such as a DLP engine can read it

Used for the purpose of apply a protection action or data governance action – determined by policy

Can be customized per the organization's needs

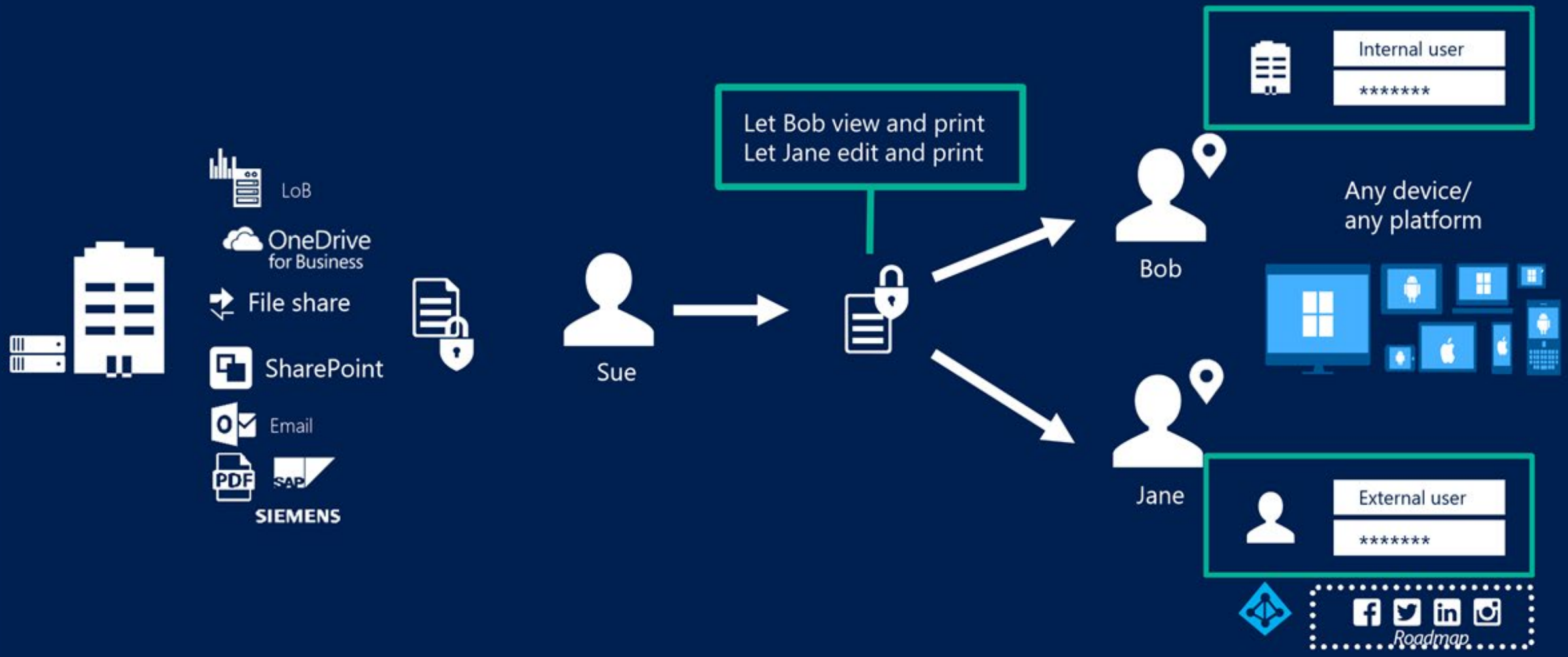
PROTECT SENSITIVE INFORMATION ACROSS CLOUD SERVICES & ON PREMISES

- Data encryption built into Azure & Office 365
- File-level encryption and permissions
- DLP actions to block sharing
- Control cloud app access & usage
- Email-level encryption and rights protection
- Revoke app access
- Policy tips to notify and educate end users
- Visual markings to indicate sensitive documents
- Retain, expire or delete documents

Share safely with anyone

BENNETT ADELSON

Share internally, with business partners, and customers



MONITOR INFORMATION PROTECTION EVENTS FOR GREATER CONTROL

Visibility

- Policy violations
- Document access & sharing
- App usage
- Anomalous activity
- End-user overrides
- False positives

Take Action

- Tune & revise policies
- Revoke access
- Quarantine file
- Quarantine user
- Integrate into workflows & SIEM

End User Impact

Labels

Can be confusing (What does “internal” even mean?)

How do you change if mislabeled?

How do you prevent everything getting labeled incorrectly because the user doesn’t care, is burdened, or actually wants to bypass the controls?

Tools

MIP

Security Center

Compliance Center

End User Implications

- What is Protection?
  - Controls vs Protection
  - Encryption
  - Restrictions (Rights)

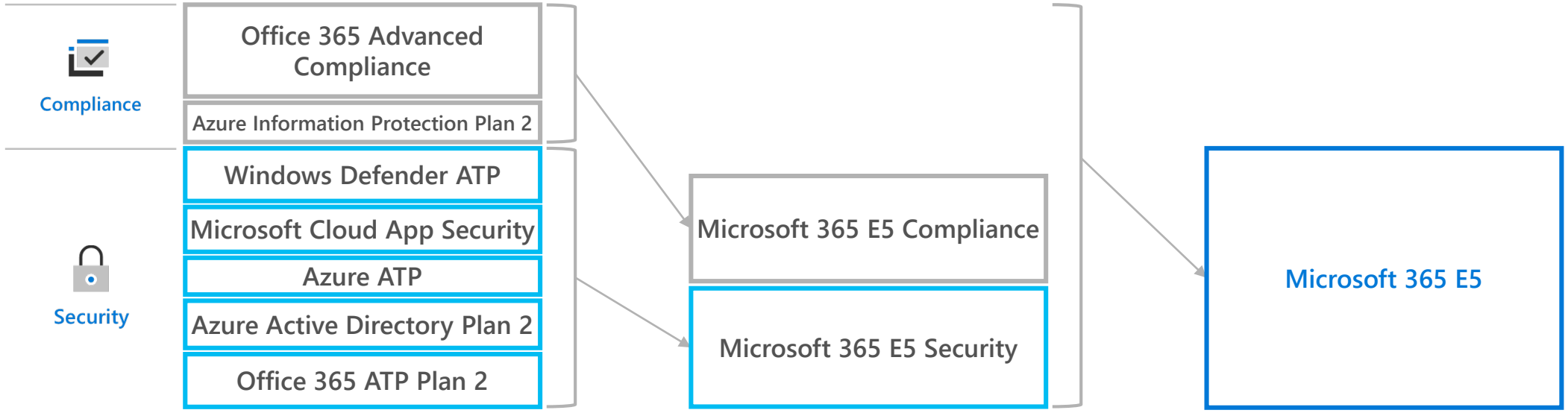
- Workflows
  - Justification for changing a label
  - Super Users for changing labels
  - Data Custodians

Technical Implications

BENNETT ADELSON

- Licensing
  - EMS E3 and EMS E5
  - Standalone and Mini Suites

Feature	Azure Information Protection Premium P1 (EMS E3)	Azure Information Protection Premium P2 (EMS E5)
View labels and watermarks in Office	Yes	Yes
Manual labeling (user driven)	Yes	Yes
Apply content marking and RMS protection in Office	Yes	Yes
Automatic and recommended labeling		Yes
Classification, labeling and protection with MCAS		Yes
HYOK (Hold you own key – multi RMS server support)		Yes



Technical Implications

- Tools
  - Platform agnostics – Protection on iOS, Windows, and Android
  - AIP Client
    - Normal and Unified Label client
  - AIP Scanner
    - Local Files (script to run on devices/servers)
    - Shares – close to data location and consider impact to shares
    - SharePoint Sites and Libraries
  - MCAS
    - Scanning of sensitive data types and auto apply of labels (and protection)
  - MIP

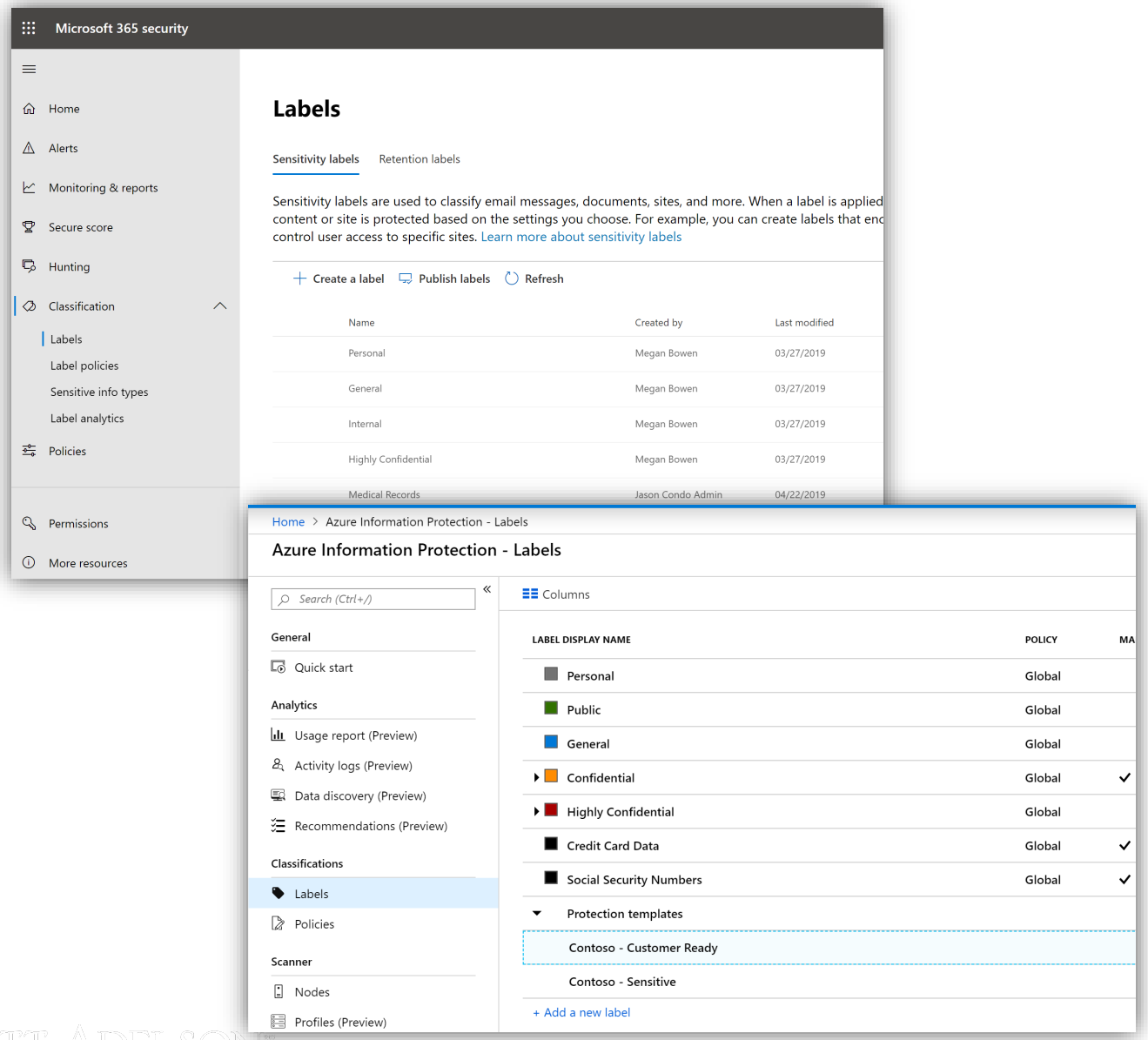
Process

- Where is the data
  - Cloud
  - On-Prem
- Who will be impacted
  - Important that some controls are global
  - Be careful enforcing if you are phasing a rollout
- Start simple
  - Default classifications
  - Detect and classify first
  - Leverage default template definitions first
- Executive sponsorship is key
  - The carrot doesn't always work

A wrench in the works …. MIP and Unified Labels

BENNETT ADELSON

- Unified labels are not AIP labels (and vice versa)
- Unified labels will become a single label based on a sensitivity type, but for now there are sensitivity labels (for protection) and retention labels (for governance)
- These labels are not AIP labels and are in a different console



Gotchas

- Encryption
- Protection vs Data Loss
- Exceptions or special needs
  - Super user for approvals to change classification
- Mergers, Acquisitions, Divestitures, and B2B
- Plan for MIP

Thank you!

- Please fill out the session feedback forms in order to win a chance of winning an Amazon gift card ☺

Thank You

BENNETT ADELSON℠