



Microsoft CISO Workshop 5 - Information Protection Strategy

Microsoft Cybersecurity Solutions Group





**“If you protect your paper clips
and diamonds with equal vigor...
...you’ll soon have more paper
clips and fewer diamonds.”**

Attributed to Dean Rusk, US Secretary of State 1961-1969

Information Protection

TRENDS AND STRATEGIES

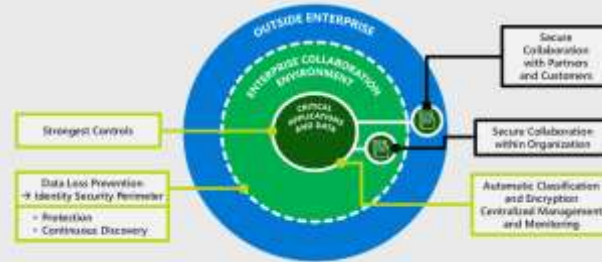
Evolution of information protection

MICROSOFT SECURITY PHILOSOPHY	Access Controls + Encryption	+ Rights Management	+ Full Lifecycle Protection (Auto Classification, SaaS)
SECURITY TRENDS	Fileshare and USB Stick Sprawl	SharePoint and Email/Mobile Sprawl	Cloud and Shadow IT Sprawl
INFORMATION TECHNOLOGY	Mainframe + PCs	+ Outsources + Mobile Devices	+ Cloud + Internet of Things (IoT)

STRATEGY AND CAPABILITIES

Information protection strategy

Ensure visibility and control for a modern hybrid enterprise



INFORMATION PROTECTION STRATEGY

The story of a file



SENSITIVE DOCUMENTS

Secure the data, not just the SQL database

Automated **discovery** of sensitive data
Labeling (tagging) sensitive data on column level with persistency
 Classification as **infrastructure for protection & compliance**
 Audit access to sensitive data
 Sensitivity metadata flows with data for **protection outside database boundaries**
 Hybrid – cloud + on-premises
 Centralized IP policy management



SQL AND STRUCTURED DATA

Evolution of information protection

MICROSOFT SECURITY PHILOSOPHY

Access Controls
+ Encryption

+ Rights Management

+ Full Lifecycle Protection
(Auto Classification, SaaS)

SECURITY TRENDS

Fileshare and
USB Stick Sprawl

SharePoint and
Email/Mobile Sprawl

Cloud and
Shadow IT Sprawl

INFORMATION TECHNOLOGY



Mainframes + PCs

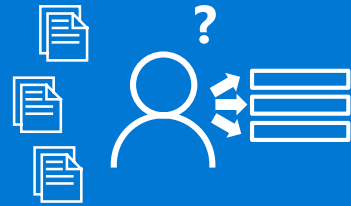


+ Datacenters + Mobile Devices



+ Cloud + Internet of Things (IoT)

Data security challenges



Reduce and Manage Risk of User Errors

Collaboration to create new business value requires data sharing and data mobility

Critically important to prevent unauthorized disclosure, modification, or destruction

Classification is Challenging

Manual user classification is impractical at scale

Large set of existing documents and more being created all the time

Data Must Be Protected Outside of the Network

Data must be protected as it traverses mobile devices and cloud services

Data created outside the network must be classified and protected

Compliance and Security Require a Complete Strategy

Compliance penalties are increasing and measuring outcomes vs. methods

Need full lifecycle protection for information assets (appropriate to valuation)

Top Information Protection Use Cases

DISCOVER – CLASSIFY – PROTECT – MONITOR

Information Protection and Data Governance Strategy

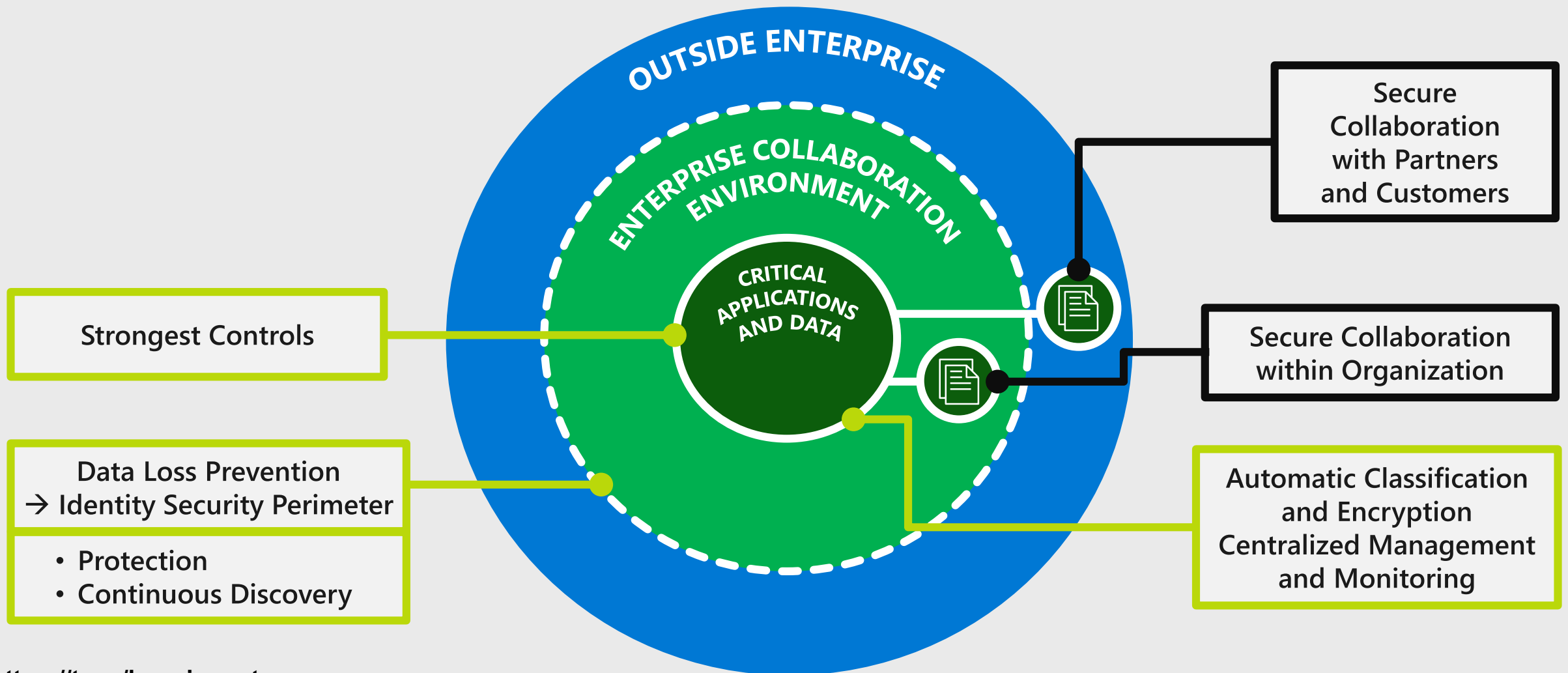
- Label, track, and show data loss or manipulation of a file.
- Implement corporate policies to protect different levels of sensitive data

Protecting sensitive information

- Challenging to discover and classify data across mobile devices, SaaS, cloud infrastructure, and on-premises
- Need full lifecycle data protection for identified data including encryption, permissions, visual markings, access revocation, retention and deletion

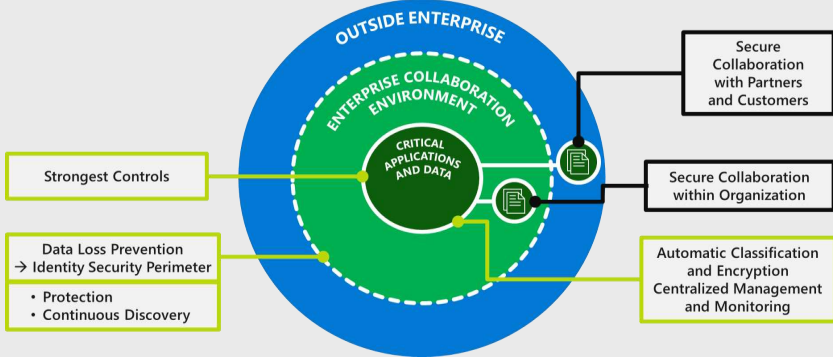
Information protection strategy

Ensure visibility and control for a modern hybrid enterprise



Strategy core goal

Protect at the appropriate level



3 HIGHEST VALUE ASSETS

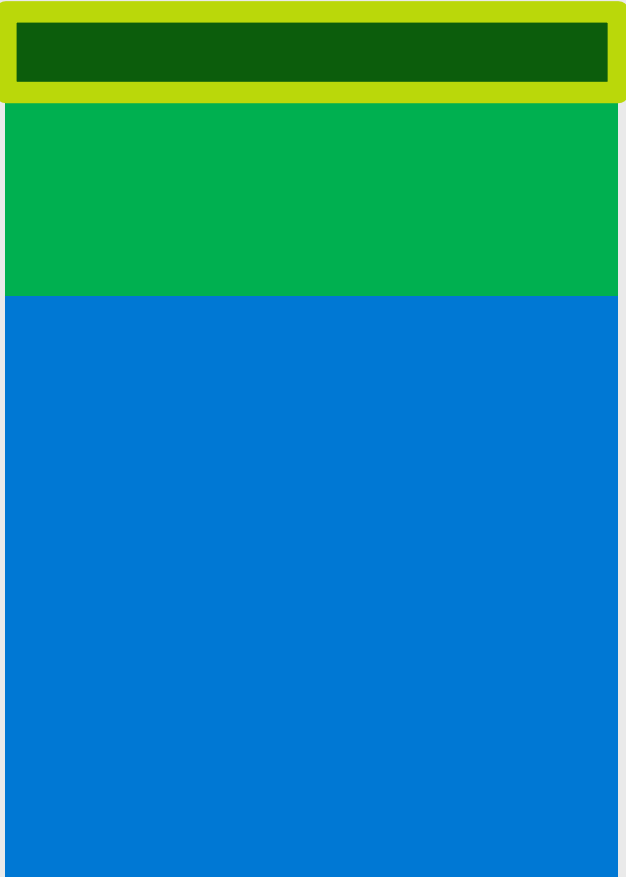
Level 2 + Specialized Protection and processes

2 SENSITIVE INFORMATION

Reduce risk of theft, modification, and destruction

1 BASELINE PROTECTION

Building an Identity Security Perimeter



Success criteria—information protection

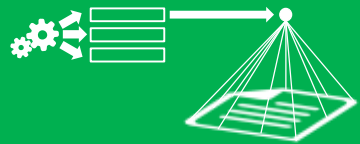
Information Protection and Data Governance Strategy



COVERAGE – Structured and unstructured, backups, SaaS, etc.

INTEGRATION – New capabilities with existing DLP processes (and tools)

Sensitive Information Success Criteria



Centralized control – Monitor and revoke access to documents

Automatic classification – Of new, existing, and exported documents



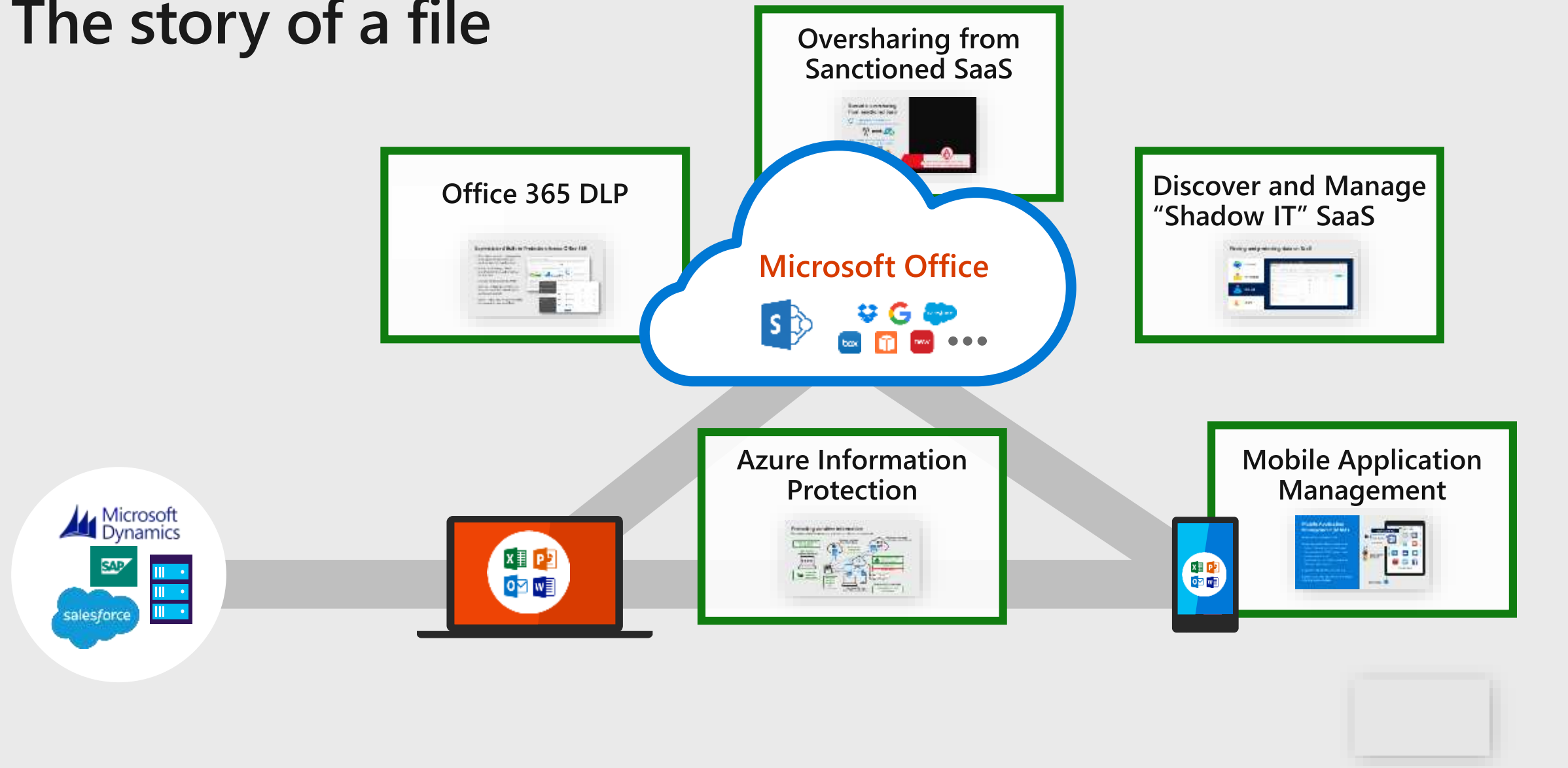
Embedded protection – Protect the data, not just storage/networks



Persistent protection – For your sensitive data anywhere it goes

FULL STACK FOR HIGHEST VALUE ASSETS – Host/device/identity/etc. security + user education
<https://t.me/learningnets>

The story of a file



Summary and Close →

Success criteria—information protection

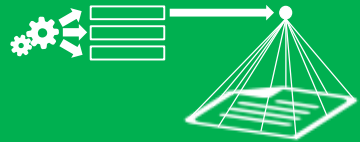
Information Protection and Data Governance Strategy



COVERAGE – Structured and unstructured, backups, SaaS, etc.

INTEGRATION – New capabilities with existing DLP processes (and tools)

Sensitive Information Success Criteria



Centralized control – Monitor and revoke access to documents

Automatic classification – Of new, existing, and exported documents



Embedded protection – Protect the data, not just storage/networks



Persistent protection – For your sensitive data anywhere it goes

FULL STACK FOR HIGHEST VALUE ASSETS – Host/device/identity/etc. security + user education
<https://t.me/learningnets>



Questions?

© Copyright Microsoft Corporation. All rights reserved. Microsoft, Windows, and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

<https://t.me/learningnets>

References

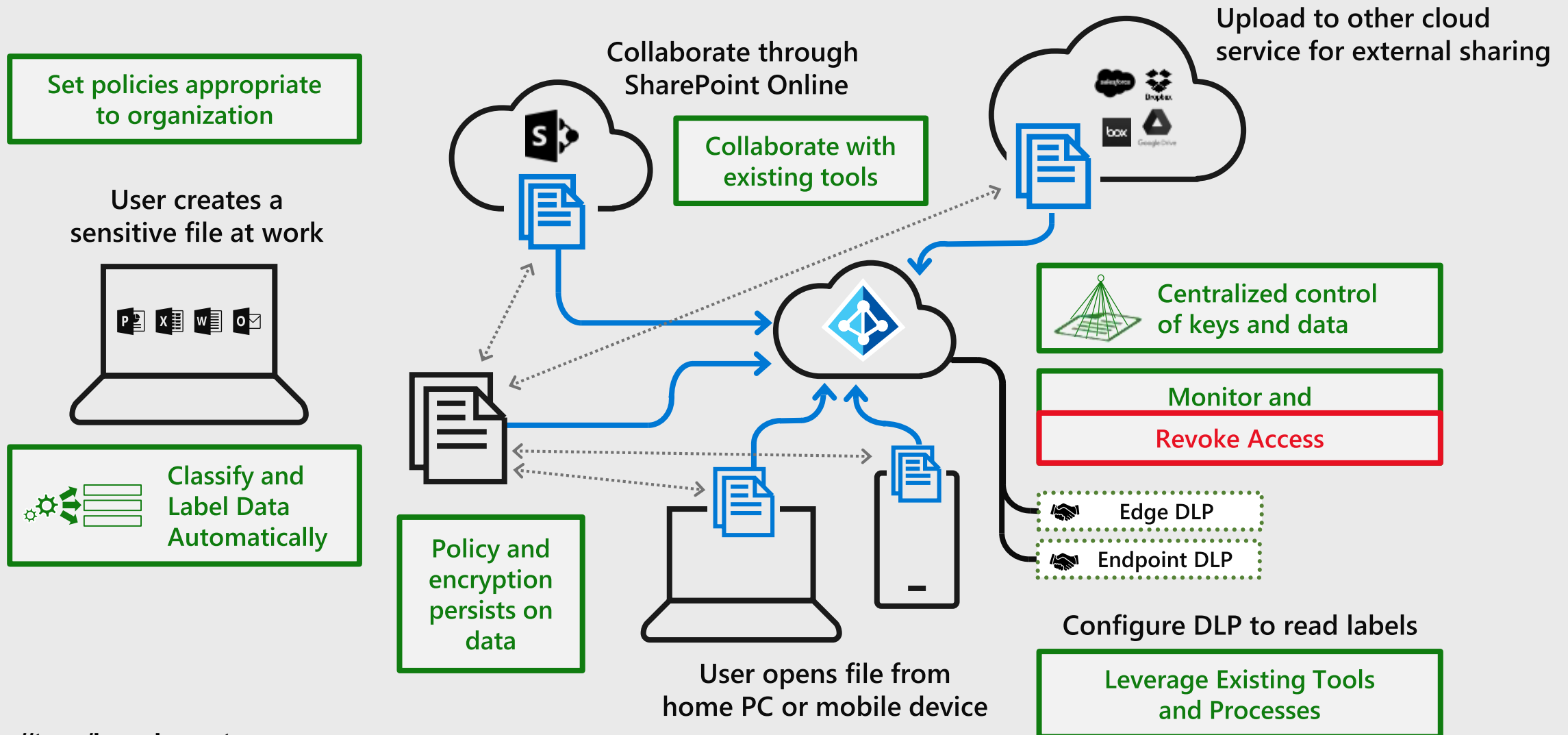
Additional Resources – Information Protection

Microsoft Cloud App Security integration with 3rd party DLP engines

<https://cloudblogs.microsoft.com/enterprisemobility/2018/01/30/microsoft-cloud-app-security-integrates-with-third-party-data-loss-prevention-solutions/>

Protecting sensitive information

Persistent classification and protection of your documents

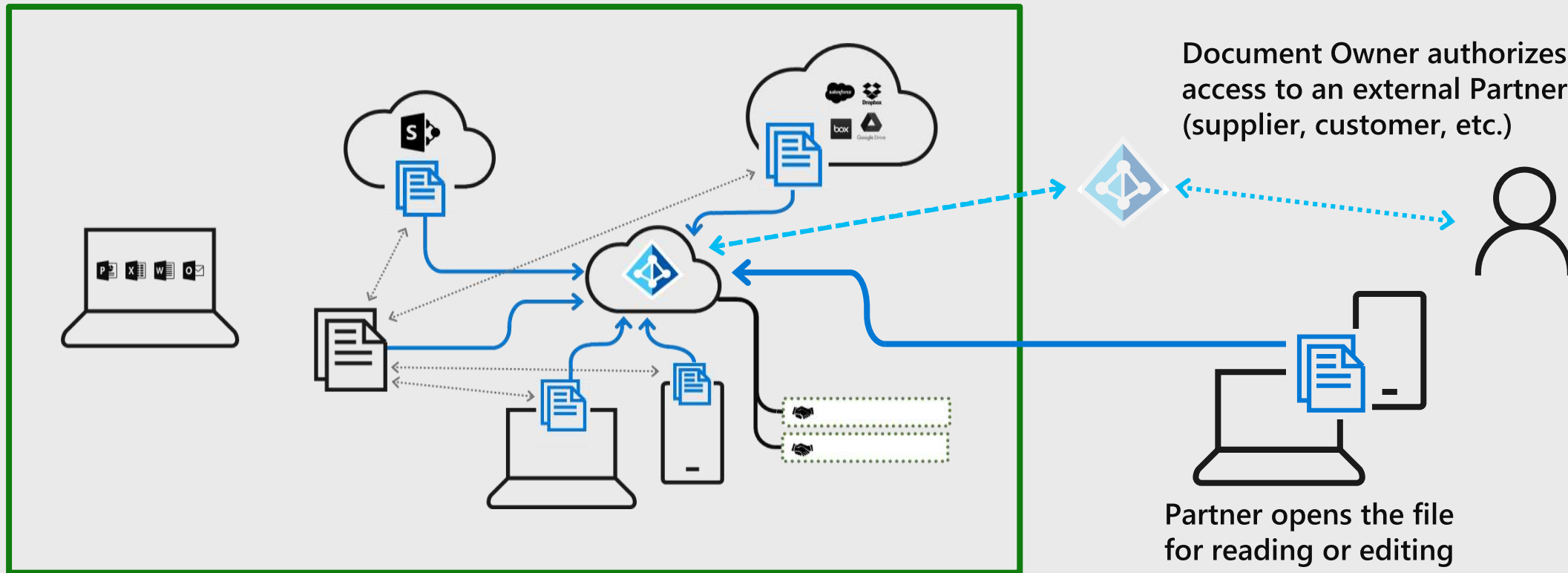


Modern information protection

Collaborate securely with partners

Documents restricted to only authorized users

Enable simple external collaboration



Key classification scenarios



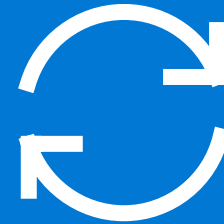
Automatic

Set policies to automatically applying classification and protection to data



Recommended

Prompt with suggested classification based on the content you're working on



Reclassification

Enable users to override a classification (and optionally require providing a justification)



User Set

Manually apply a sensitivity label to the email or file they are working on

Support required formats for sensitive data

Coverage for popular formats + extensibility

Microsoft Office Formats



Built into

Microsoft Office

PDF



Partner(s)



[...and more](#)

AutoCAD



Partner(s)

[SealPath](#)

Others



[SAP Data Export](#)

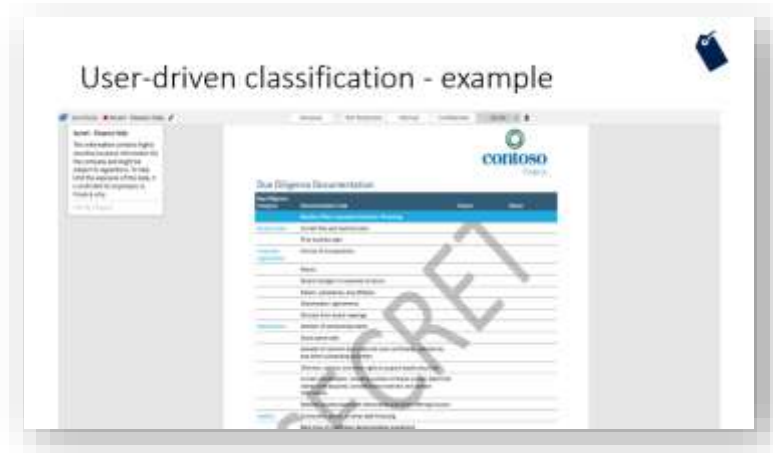
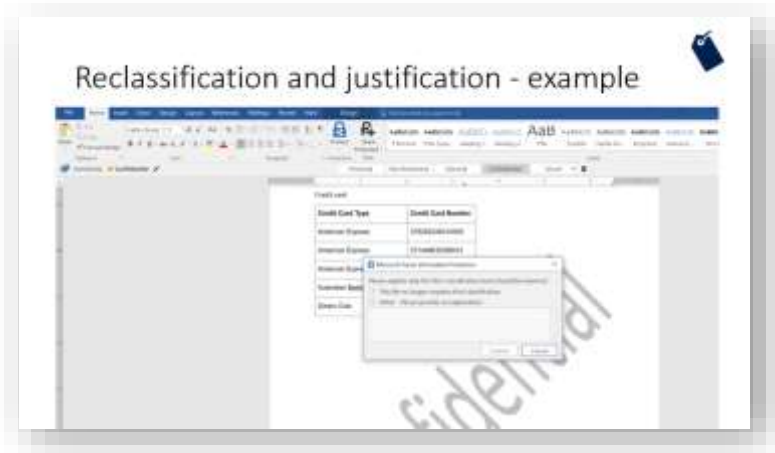
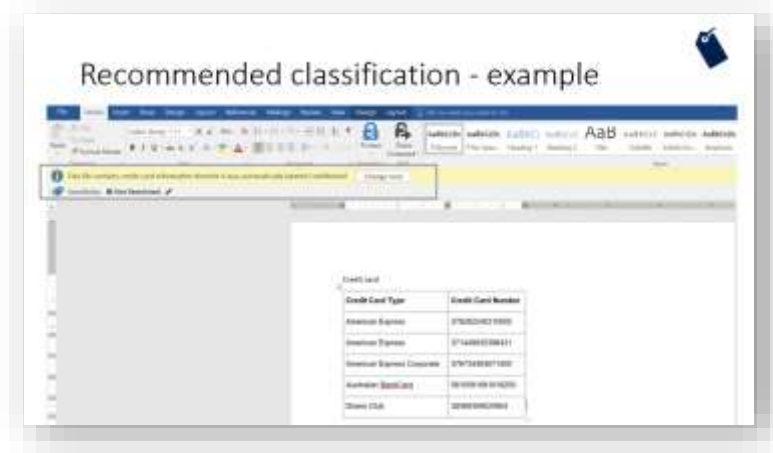
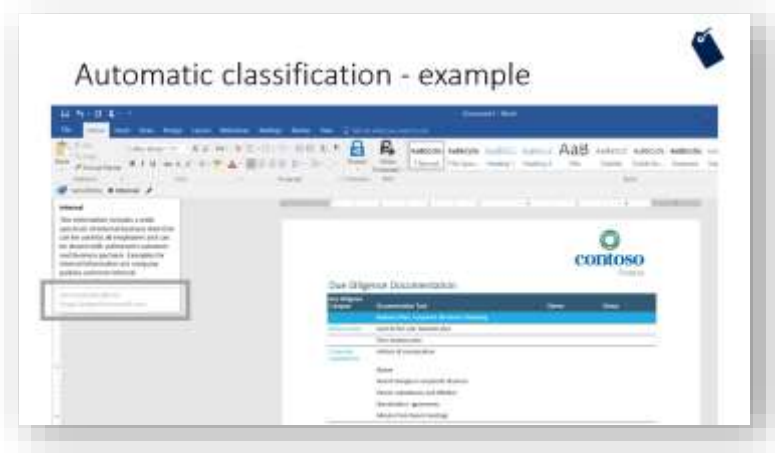


[...and more](#)



[Software Development Kit](#)

Azure Information Protection Experience



Finding and protecting data on SaaS



Discover



Investigate



Control



Alerts

Cloud App Security

Discover Investigate Control Alerts 34

Policy center

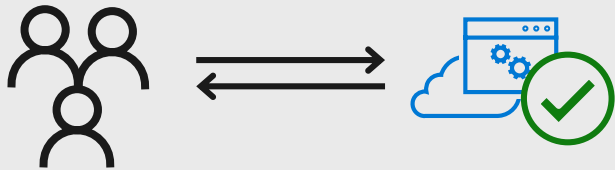
TYPE: Select type... RISK: [Green] [Yellow] [Red] NAME: Policy name... RISK CATEGORY: Select risk category... [Advanced]

1 - 6 of 6 Policies [Create policy] [Filter]

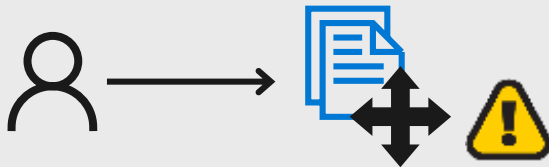
Report	Cases	Severity	Risk category	Action	Modified
PCI COMPLIANCE: Publicly shared files with credit card info This policy identifies files containing credit card numbers and are publicly shared. After...	2 matches	[Red]	Compliance	[Stop] [Refresh]	Jul 22, 2015
User logon from a non-categorized IP address Alert when a user logs on from an IP address that hasn't been included in a specific IP...	0 open alerts	[Red]	—	[Stop]	Mar 8, 2016
Anomaly Detection Policy ADP	0 open alerts	[Red]	—	[Stop]	Mar 8, 2016
Mass download by a single user Alert when a single user performs more than 30 downloads within 5 minutes.	0 open alerts	[Red]	—	[Stop]	Mar 14, 2016
testing	0 open alerts	[Green]	—	[Stop]	Mar 14, 2016
Demo for bla	0 open alerts	[Green]	—	[Stop]	Mar 17, 2016

Scenario: oversharing from sanctioned SaaS

- 1 IT department sanctions SaaS application and provisions user access



- 2 User uploads sensitive file to SaaS and shares openly with everyone



- 3a Cloud app security detects oversharing of sensitive document, quarantines it, and issues alert



3

Unknown parties find and access the document, creating business risk

Secure the data, not just the SQL database

Automated **discovery** of sensitive data

Labeling (tagging) sensitive data on column level with persistency

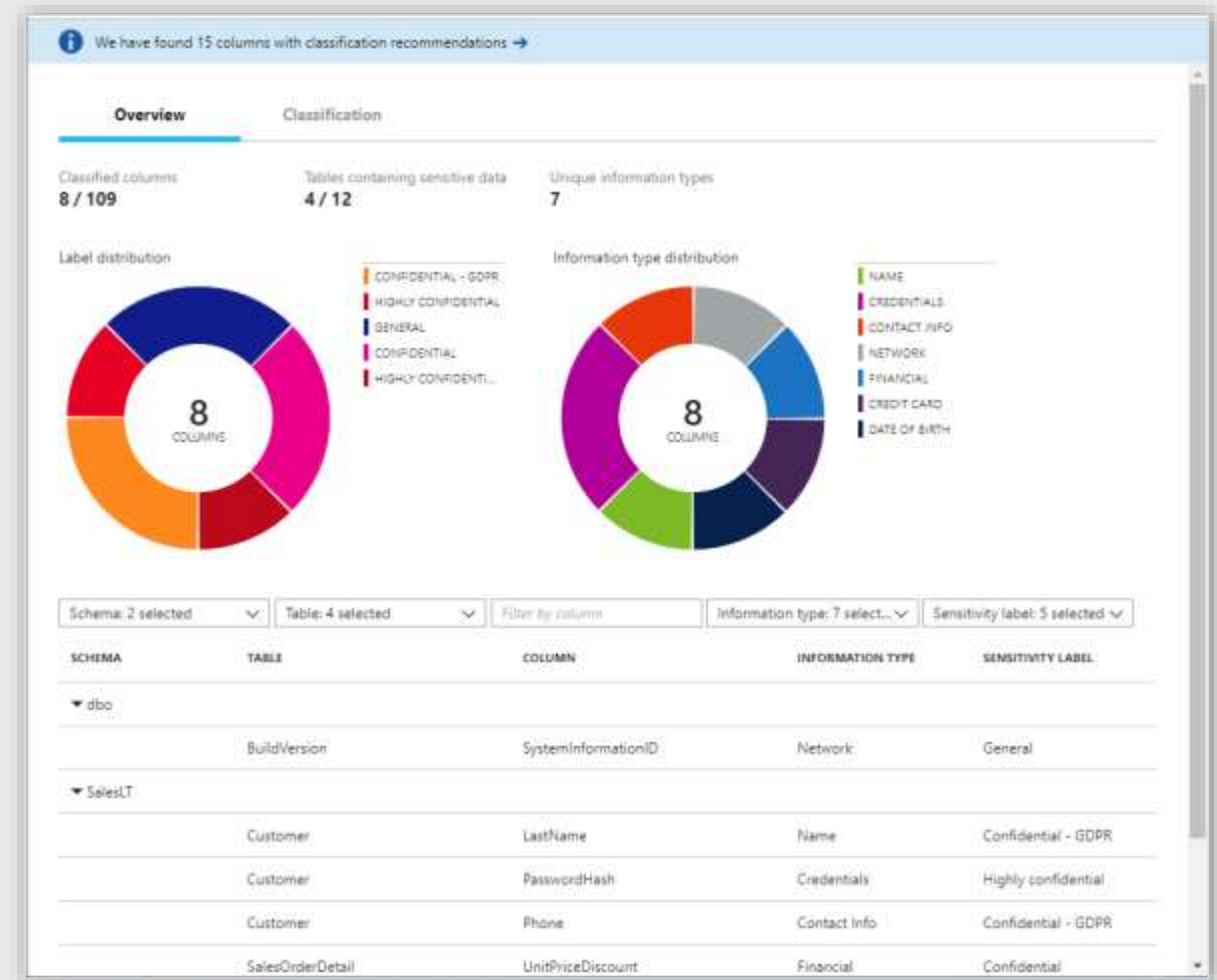
Classification as **infrastructure** for **protection & compliance**

Audit access to sensitive data

Sensitivity metadata flows with data for **protection outside database boundaries**

Hybrid – cloud + on-premises

Centralized IP policy management



Mobile Application Management (MAM)

Works with or without MDM

Strong protections for corporate data

- Restrict "Save as" and cut/copy/paste

- Secure viewing of PDFs, images, videos

- App encryption at rest

- App access control – PIN or credentials

- Managed web browsing

Support multi-identity applications

Selective wipe of corporate data without affecting personal data



Sophisticated Built-in Protection Across Office 365

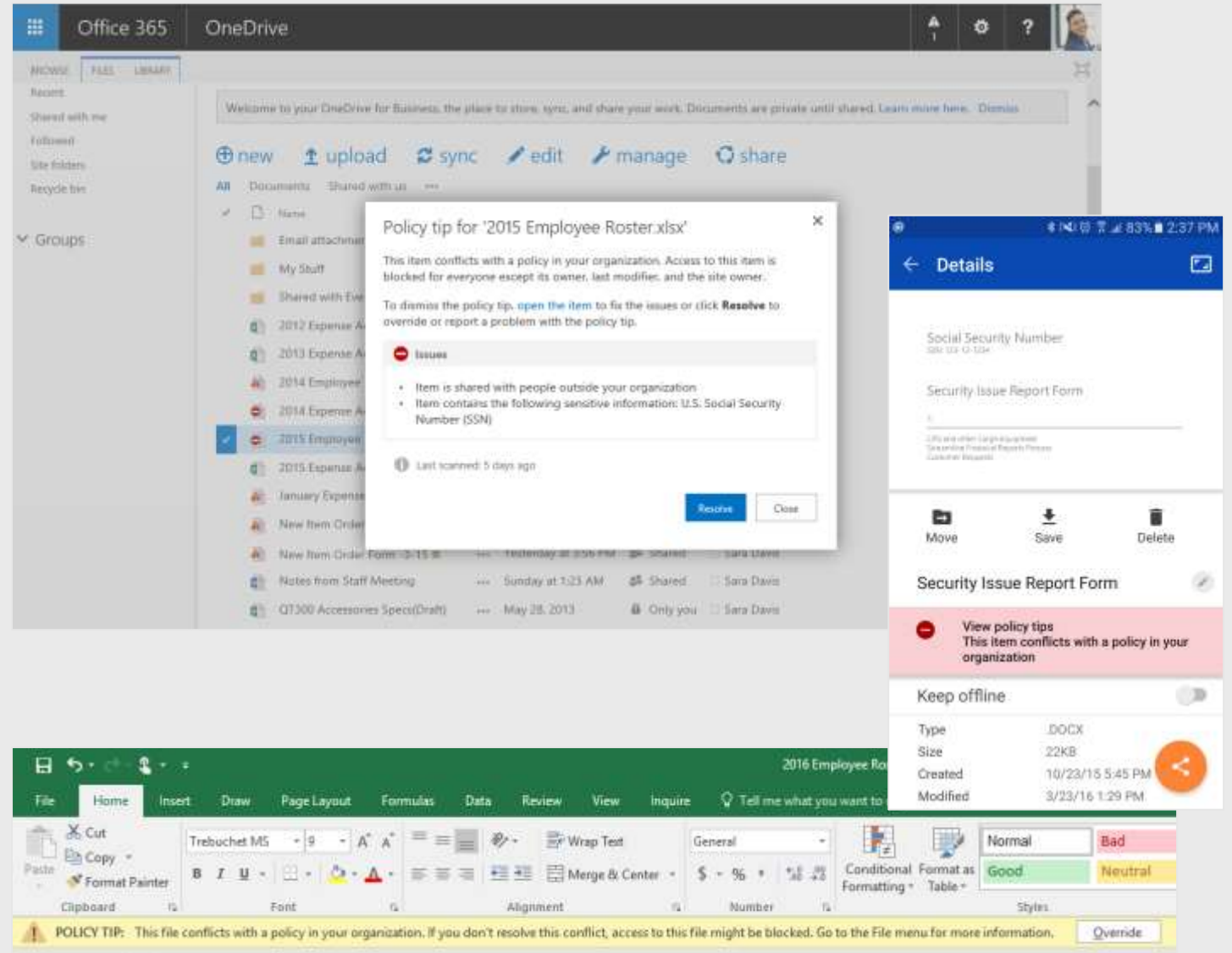
- Centralized console - define policy once, apply across Office 365 services and client end-points
- Built in to Exchange Online, SharePoint Online, and OneDrive for Business
- Focused on secure productivity
- Admins - Default policy for most common sensitive content (which can be customized)
- Users - Policy Tips integrate security education into user workflow

The screenshot displays the Office 365 Content Protection Policies console. The main dashboard includes a search bar, a 'Data Loss Prevention' activity chart, a 'Data volume covered by Retention Policy' bar chart, a 'Data by age' donut chart showing 178 TB of data, and a 'Policy matches' line chart. Below the dashboard is a 'Create a policy' section with a list of policy options. A 'Choose locations' dialog box is overlaid on the screen, showing a table of locations and their inclusion/exclusion status.

Status	Location	Include	Exclude
<input checked="" type="checkbox"/>	SharePoint sites	All Include	None Exclude
<input checked="" type="checkbox"/>	OneDrive accounts	All Include	None Exclude
<input checked="" type="checkbox"/>	Exchange email	All	None

Balancing User Productivity and Risk

- Policy Tips help educate users when they are about to violate a policy
- Available in desktop, web, and mobile apps



DLP Policy Rules - Conditions

- Describe the policy objective – model business risk and mitigation actions
- Set of conditions describing when rule applies
- Set of actions applied when conditions match
- Range of actions covering insights and automatic remediation
- Generic action behavior integrated for natural experience across each workload

U.S. Financial Data Low volume of content detected

Name **Conditions** Actions User notifications Admin alerts

^ Conditions

Use conditions to define what kind of content you want to protect.

When content contains sensitive information

any of these

Sensitive information type	Instance count		Match accuracy		
	min	max	min	max	
Credit Card Number	1	9	0	100	×
U.S. Bank Account Number	1	9	0	100	×
ABA Routing Number	1	9	0	100	×

[Add or change sensitive types](#)

+ Add sensitive information group

Content is shared with

Outside my organization

Detects when content is shared in an email message or shared in a document in SharePoint or OneDrive

+ Add a condition

DLP Policy Rules - Actions

- Describe the policy objective – model business risk and mitigation actions
- Set of conditions describing when rule applies
- Set of actions applied when conditions match
- Range of actions covering insights and automatic remediation
- Generic action behavior integrated for natural experience across each workload

The screenshot shows the configuration page for a DLP policy rule named "U.S. Financial Data". The "Actions" tab is selected and highlighted with a blue border. The "Restrict action to the content" section is expanded, showing options for SharePoint and OneDrive restrictions. The "User notifications" section is also visible, with a toggle for "Email notifications" turned on and the option "Let me choose who receives the notification" selected.

U.S. Financial Data Low volume of content detected

Name	Conditions	Actions	User notifications	Admin alerts
------	------------	---------	--------------------	--------------

^ Actions

Use actions to protect content when the conditions are met.

Restrict action to the content [X]

By default, people will be blocked from sharing or accessing shared content that matches this rule. You can also customize how users access sensitive content in different content locations.

SharePoint and OneDrive restrictions

- Block access to everyone except the person that owns the content, the last modifier of the content, and site admin where the content is stored.
- Allow internal people to access the content, but restrict all access to external recipients.

+ Add a condition +

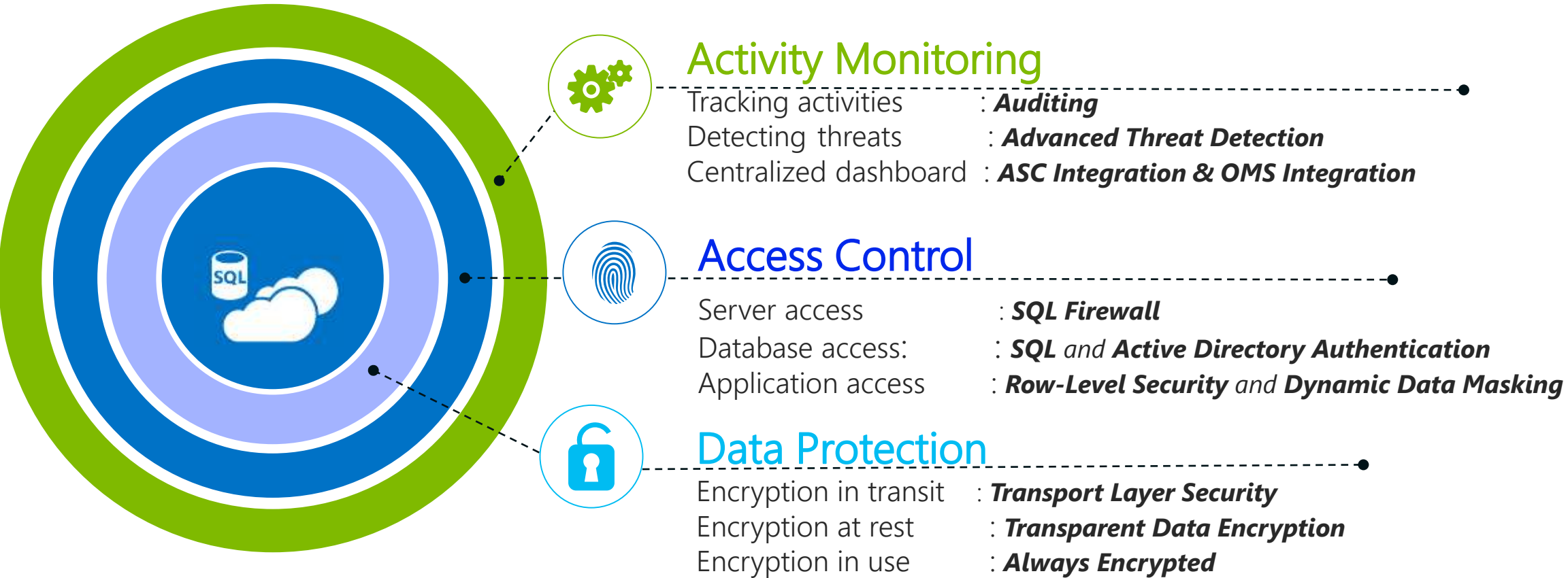
^ User notifications

Use Notifications to inform your users and help educate them on the proper use of sensitive information.

Email notifications

- Notify the user that sent, shared, or last modified the content.
- Let me choose who receives the notification
 - The person that sent, shared, or modified the content

Securing Structured Data in Azure SQL

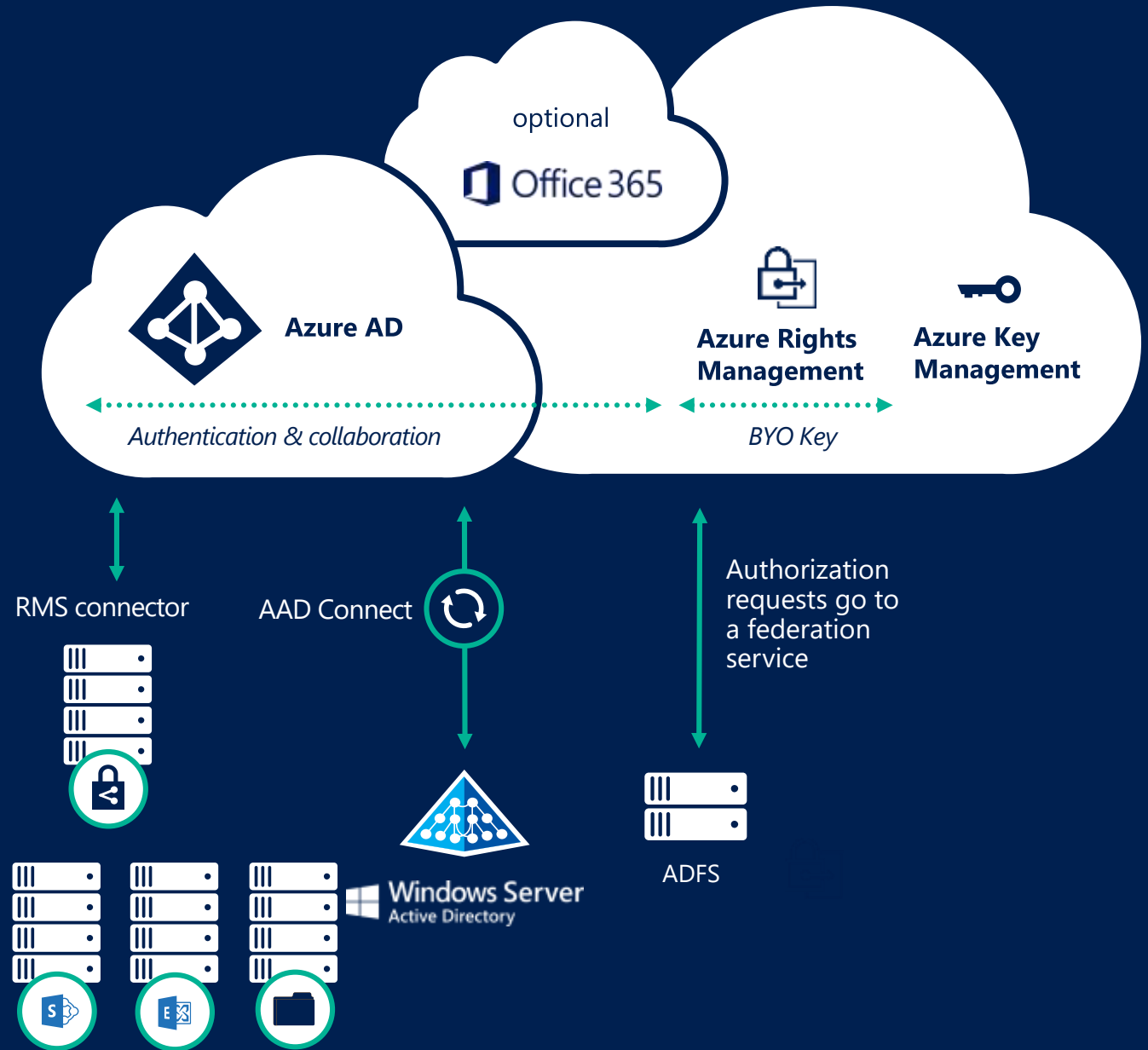


Compliance: FedRAMP, HIPAA, PCI, EU Model Clauses, UK G-Cloud, ISO,
(government), (medical), (payment), (personal), (public sector)

Recommended Topology

Azure Information Protection

- ▶ Data protection for organizations at different stages of cloud adoption
- ▶ Ensures security because sensitive data is not sent to the RMS server
- ▶ Integration with on-premises assets with minimal effort



Regulated Topology

Azure Information Protection

- ▶ Data protection for organizations at different stages of cloud adoption
- ▶ Ensures security because sensitive data is not sent to the RMS server
- ▶ Integration with on-premises assets with minimal effort
- ▶ Hold Your Own Key with on-premises key retention

<https://t.me/learningnets>

