



# Welcome to the Azure Information Protection Webinar Series

We will start at 2-3 minutes after the scheduled time to accommodate those still connecting.

**Questions?** Feel free to type them in the instant message window at any time. Note that any questions you post will be **public**. You have the option to post questions anonymously.

This webinar is being **recorded**. We'll post the recordings to our community forums at <https://aka.ms/AIPRecordings>.

Join our Community: <https://aka.ms/SecurityCommunity>

# Microsoft Information Protection: Discover, label and protect data at rest

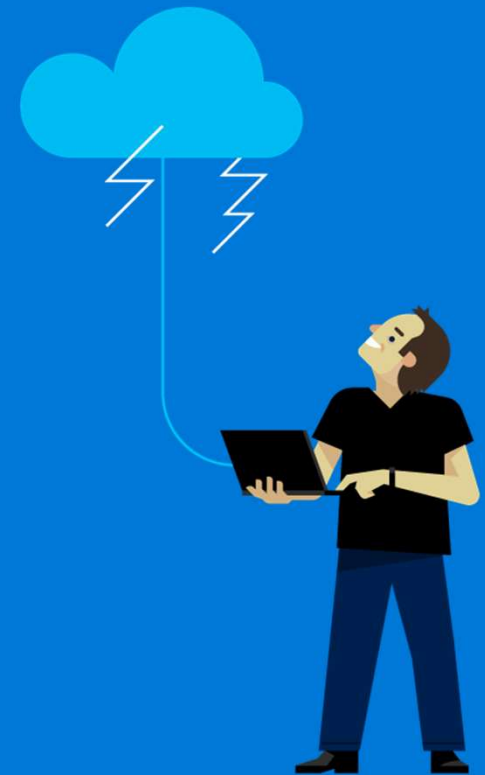


Denis Mizetski  
Sr Program Manager  
Azure Information Protection

**Microsoft**

# Agenda

- Discovery story in MIP
- On-perm data discovery
- Endpoint data discovery
- Cloud data discovery
- Best practices
- Roadmap



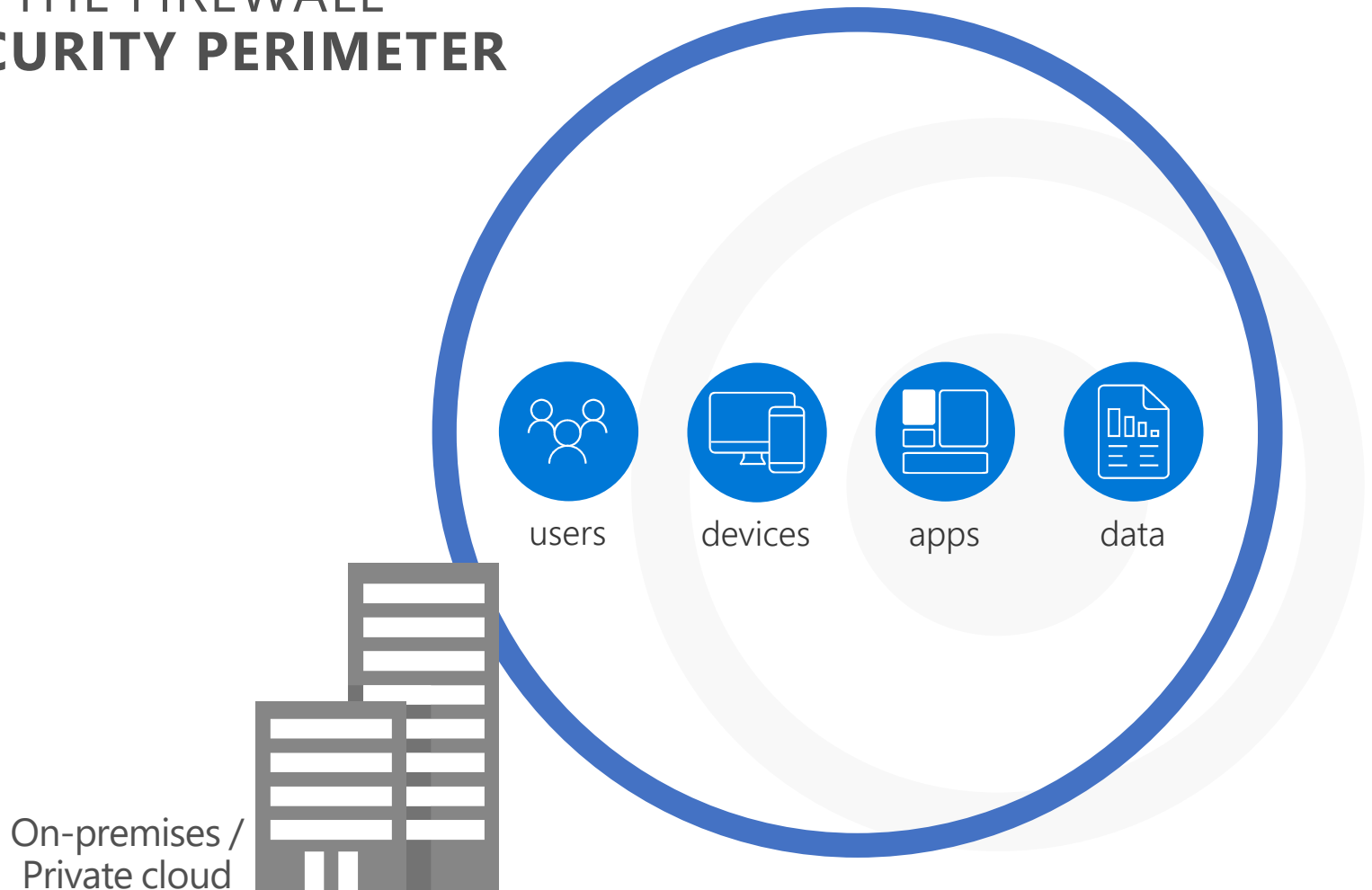
# Discovery in Microsoft Information Protection

No matter how much data your organization owns, losing it is costly. Every organization is a target and threats are increasing.

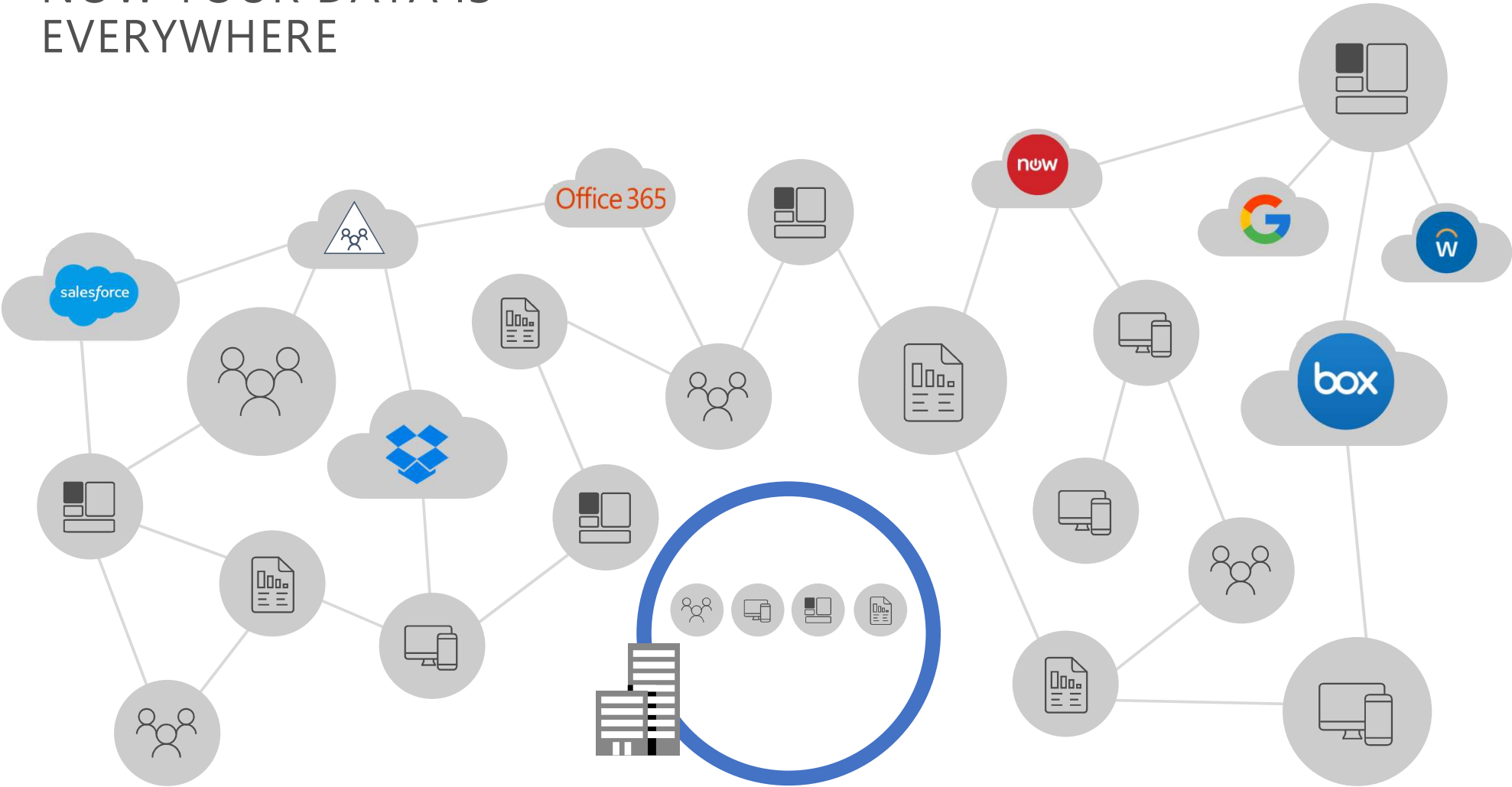
To **protect** what you own, you first need to **know** what you have, and classify each piece of data automatically according to its impact to your organization.

It sounds scary, but it doesn't have to be! With Microsoft Information protection you can help customers discover, classify, and protect all their data, no matter where it is stored or who it is shared with.

# IN THE PAST, THE FIREWALL WAS THE **SECURITY PERIMETER**



# NOW YOUR DATA IS EVERYWHERE



# Microsoft Information Protection

Discover and classify information anywhere it lives



Discover & classify  
sensitive information



Apply protection  
based on policy

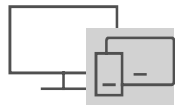


Monitor &  
remediate



Accelerate  
Compliance

Across



Devices



Apps



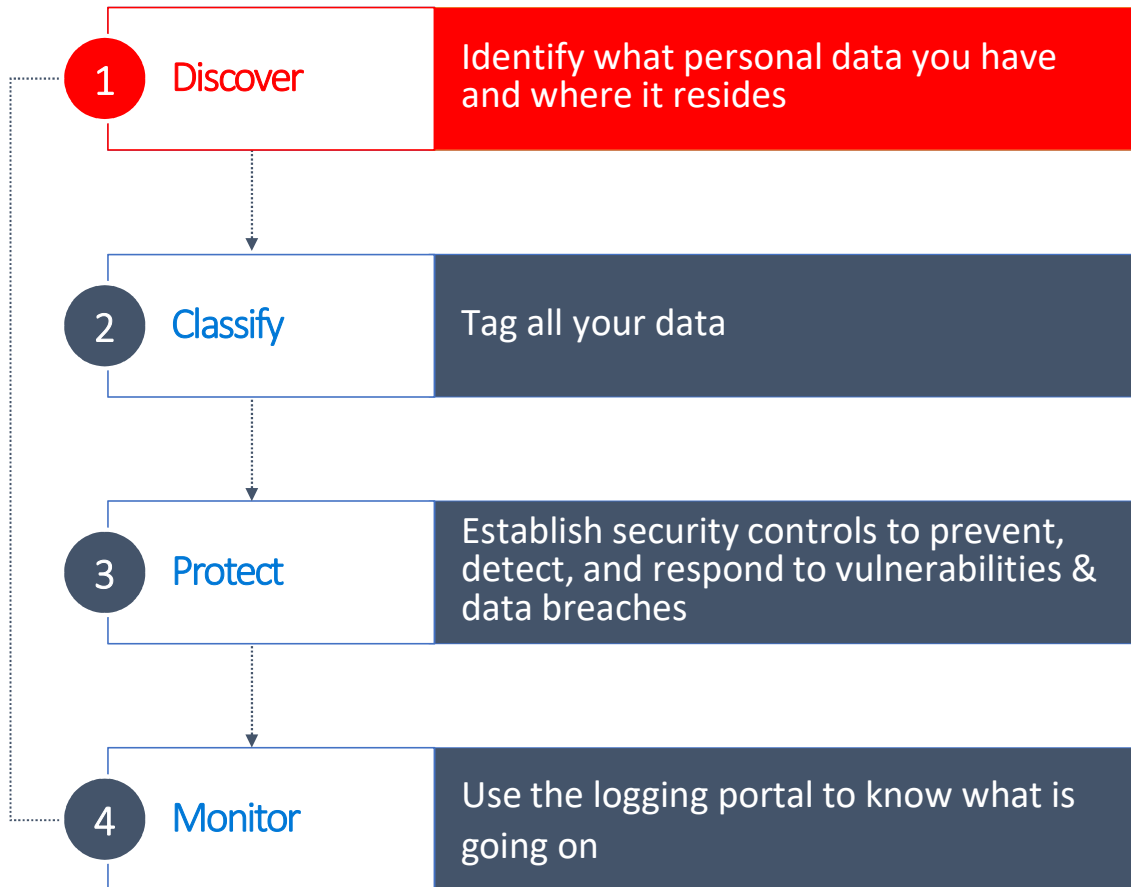
Cloud services



On-premises



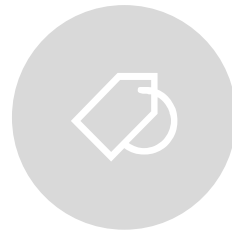
# How do I get started?





## Discover

Scan & detect sensitive data based on policy



## Classify

Classify data and apply labels based on sensitivity



## Protect

Apply protection actions, including encryption, access restrictions

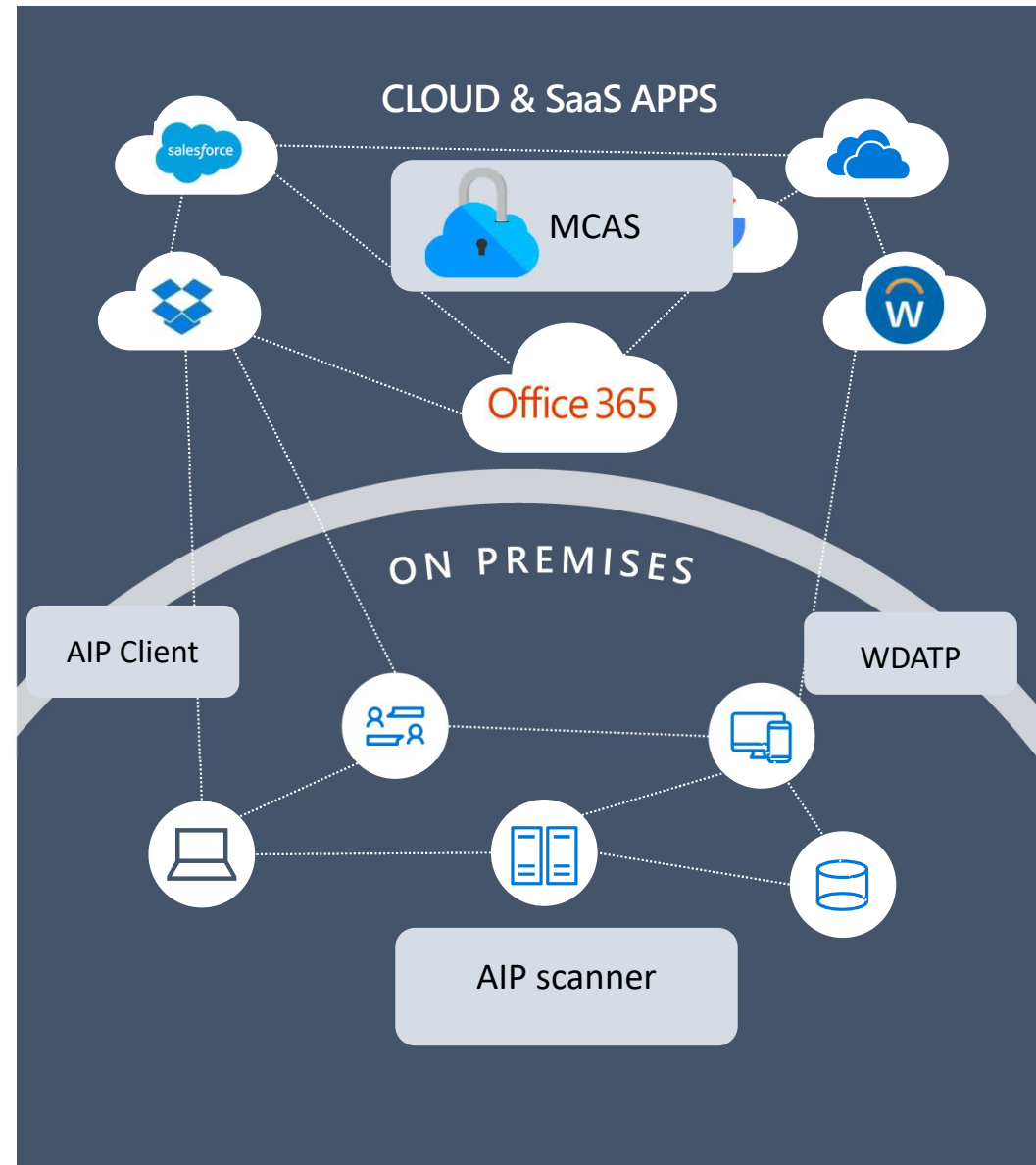


## Monitor

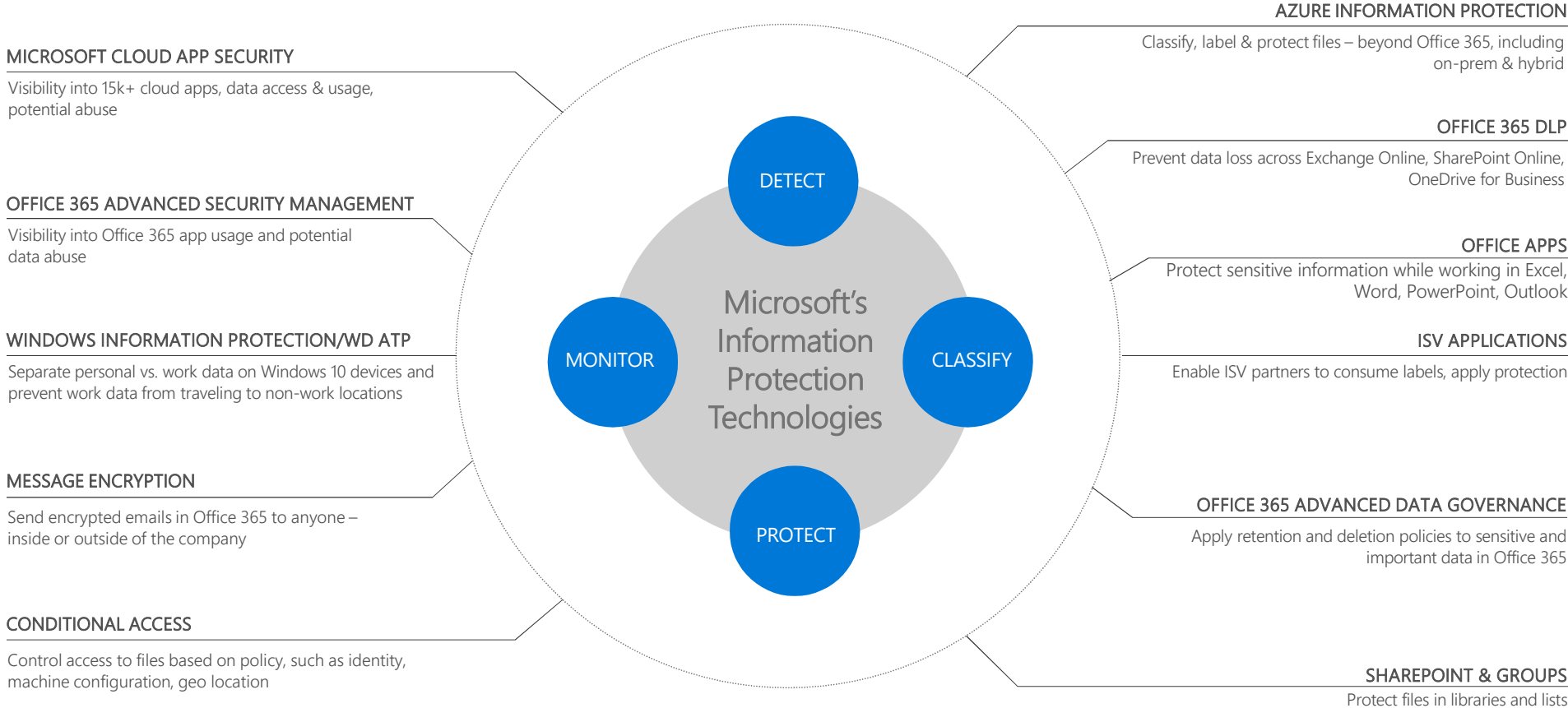
Reporting, alerts, remediation



# DETECT SENSITIVE INFORMATION



# MICROSOFT'S INFORMATION PROTECTION SOLUTIONS



# On-premises Repositories Discovery

# What AIP scanner does today?



Scans on-perm repositories: file shares, NAS or any other CIFS based repositories, or SharePoint 2013/2016



Discover data in the scanned repositories and match it against AIP policy (sensitive info types, location or custom property)



Labels and protects the discovered data per AIP policy. AIP scanner uses the same AIP policy as AIP clients.



Create a report of discovered data, including the matched conditions for found patterns

# What we hear from the customers

- Our business policy, compliance or regulation (GDPR) requires all files to be classified.  
We label new created data using AIP client, but
  - What about the data that was created before we started to use AIP?
  - We had another solution and we want AIP to leverage the existing 3<sup>rd</sup> label
  - Some files are generated by automatic processes rather than created by end users
- We want to migrate to the cloud, but
  - We want to know what is going to be migrated
  - We want to label and encrypt data before it's moved to the cloud
  - We want to decide what data is move to the cloud and what stays on perm

# Main use cases

- Discover sensitive data in on-prem repositories
  - Find where is your sensitive data
- Label and protect data per regulation or compliance requirements (ex GDPR)
  - Complement MIP story that covers endpoints (AIP client and native) and cloud repos (MCAS)
- Enable migration to cloud:
  - Decide what data can be migrated
  - Label and protect data before it's migrated to the cloud



- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support
- Azure Information Protection

Dashboard > Azure Information Protection - Profiles (Preview)

### Azure Information Protection - Profiles (Preview)

Search (Ctrl+/)

- General
- Quick start
- Analytics
  - Usage report (Preview)
  - Activity logs (Preview)
  - Data discovery (Preview)
  - Recommendations (Preview)
- Classifications
  - Labels
  - Policies
- Scanner
  - Nodes
  - Profiles (Preview)
- Manage
  - Configure analytics (Preview)
  - Languages
  - Protection activation
  - Unified labeling (Preview)

+ Add   ↓ Export   🗑 Delete

Search to filter items...

NAME	SCHEDULE	ENFORCE	REPOSITORIES
Demo	Manual		1
WKS1001QR8BC	Manual	✓	1
✓ US-WEST	Manual	✓	1
MININT-IHV3VE4	Manual		3

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support
- Azure Information Protecti...

### US-WEST

Save Discard Export Delete

\* Profile name

Description

#### Profile settings

Schedule

Info types to be discovered

Configure repositories  
2 repositories configured

#### Policy enforcement

\* Enforce

Label files based on content

Default label

Relabel files

Allow label downgrade

#### Configure file settings

Preserve "Date modified", "Last modified" and "Modified by"

File types to scan

Default owner

### Repositories

+ Add   ↓ Export   ↑ Import   🗑 Delete

Search to filter items...

PATH	DEFAULT LABEL	ENFORCE	
\\SCAN-WEU01\share1		✓	...
http://sp2013.local/Documents		✓	...

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support
- Azure Information Protecti...

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support
- Azure Information Protecti...

Dashboard > Azure Information Protection - Nodes

### Azure Information Protection - Nodes

Search (Ctrl+/)

#### General

Quick start

#### Analytics

Usage report (Preview)

Activity logs (Preview)

Data discovery (Preview)

Recommendations (Preview)

#### Classifications

Labels

Policies

#### Scanner

Nodes

Profiles (Preview)

#### Manage

Configure analytics (Preview)

Languages

Protection activation

Unified labeling (Preview)

Columns Refresh Delete Scan now Rescan all files Show archived

Search by computer name, status or version, for example type Idle to get all scanners with status Idle

COMPUTER NAME	DESCRIPTION	PROFILE NAME	STATUS	LAST SEEN	VERSION	DETAILS	SCAN RATE
demizets-surf.middleleas...		Demo	Idle	2 minutes ago	1.47.21.0	45 scanned ite	
MININT-IHV3VE4.middle...		MININT-IHV3VE4	Offline	1 month ago	1.45.29.1		
S12SCANNER01.res.local			Offline	2 months ago	1.38.7.0		
SCAN-WEU01		US-WEST	Error	4 seconds ago	1.48.9.0		
wks1001qr8bc		WKS1001QR8BC	Offline	3 weeks ago	1.45.32.0		

- Scan now
- Rescan all files
- Delete this node
- Archive this node

Microsoft Azure

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support
- Azure Information Protecti...

### Azure Information Protection - Data discovery (Preview)

Search (Ctrl+/)

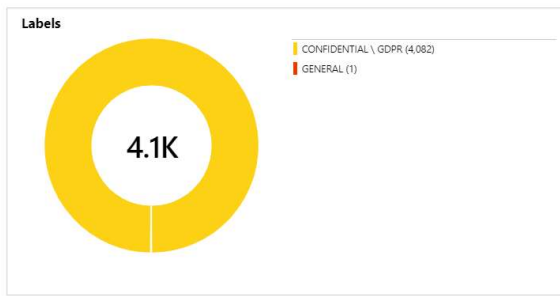
- General
- Quick start
- Analytics
  - Usage report (Preview)
  - Activity logs (Preview)
  - Data discovery (Preview)
  - Recommendations (Preview)
- Classifications
  - Labels
  - Policies
- Scanner
  - Nodes
  - Profiles (Preview)
- Manage
  - Configure analytics (Preview)
  - Languages
  - Protection activation
  - Unified labeling (Preview)

Columns Log Analytics

Location type: Any | Location: Search by location | Labels: Any | Protected: Any | Information Types: High, Any

Device risk: Any | Filter

#### Overview



#### Information Types

International Classification ...	6,915
Credit Card Number	2,717
CID	2,333
International Classification ...	2,301
USA Social Security Numb...	1,616
EU Phone Number	1,177

LOCATION TYPE	LOCATION	LABELLED FILES	PROTECTED FILES	FILES WITH INFORMATION TYPES
File repository	\\scan-weu01\share1\	4,059	0	9,915
File repository	\\wks1001qr8bc\share1\	23	0	33
File repository	\\demizets-sur1\share1\	1	0	4

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support
- Azure Information Protecti...

Dashboard > Azure Information Protection - Data discovery (Preview)

### Azure Information Protection - Data discovery (Preview)

Search (Ctrl+/)

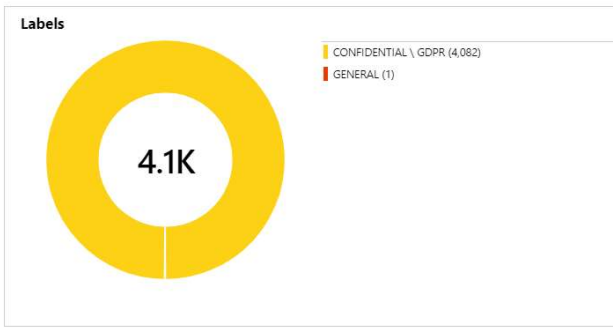
Columns Log Analytics

- General**
- Quick start
- Analytics**
- Usage report (Preview)
  - Activity logs (Preview)
  - Data discovery (Preview)
  - Recommendations (Preview)
- Classifications**
- Labels
  - Policies
- Scanner**
- Nodes
  - Profiles (Preview)
- Manage**
- Configure analytics (Preview)
  - Languages
  - Protection activation
  - Unified labeling (Preview)

Location type: Any | Location: Search by location | Labels: Any | Protected: Any | Information Types: High, 7 selected

Device risk: Any **Filter**

#### Overview



LOCATION TYPE	LOCATION	LABEL
File repository	\\scan-weu01\share1\	4,059
File repository	\\wks1001qr8bc\share1\	23
File repository	\\demizets-surf\share1\	1

Filter by name...

**Confidence**

- All
- Medium (75% and above)
- High (85% and above)

- Australia Medical Account Number
- Australia Tax File Number
- Azure DocumentDB Auth Key 6,915
- Azure IAAS Database Connection String and Azure SQL Connection String 2,717
- Azure IoT Connection String 2,333
- Azure Publish Setting Password 2,301
- Azure Redis Cache Connection String 1,616
- Azure Service Bus Connection String 1,177
- Azure Storage Account Key (Generic)
- Brazil CPF Number
- Brazil Legal Entity Number (CNPJ)
- Brazil National ID Card (RG)
- CID
- Canada Bank Account Number
- Canada Social Insurance Number
- Centrica Test
- Chile Identity Card Number
- China Resident Identity Card (PRC) Number
- Credit Card Number
- Drug Enforcement Agency (DEA) Number
- EU Debit Card Number
- EU Driver's License Number
- EU National Identification Number
- EU Passport Number
- EU Phone Number
- EU Social Security Number (SSN) or Equivalent ID

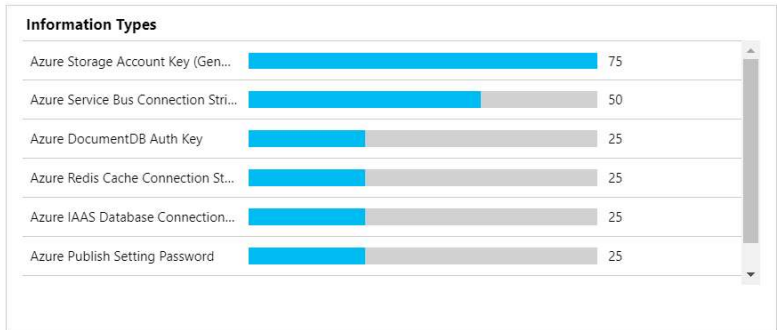
**INFORMATION TYPES**

### Files view

Log Analytics

Location type: 1 selected | Location: \\scan-weu01\share1\ | File path: search by path | Labels: Any | Protected: Any | Information Types: High, 7 selected | **Filter**

Overview



FILE PATH	NAME	LABEL	PROTECTION	INFORMATION TYPES MATCHES	LAST MODIFIED BY	LAST MODIFIED DATE
\\scan-weu01\share1\gnuht\984258844\azure sec...	7_azurestorageaccountkey.txt		No	Azure Service Bus Connection String	aipscannersvc@denis2019.onmicro...	26/02/2019
\\scan-weu01\share1\gnuht\984258844\azure sec...	azuresecret1.txt		No	Azure Publish Setting Password	aipscannersvc@denis2019.onmicro...	26/02/2019
\\scan-weu01\share1\gnuht\984258844\azure sec...	azure_secret_3.txt		No	Azure Storage Account Key (Generic)	aipscannersvc@denis2019.onmicro...	26/02/2019
\\scan-weu01\share1\gnuht\984258844\azure sec...	6_azureservicebusconnectionstri...		No	Azure Service Bus Connection String	aipscannersvc@denis2019.onmicro...	26/02/2019
\\scan-weu01\share1\gnuht\984258844\azure sec...	3_azureiotconnectionstring.txt		No	Azure IoT Connection String	aipscannersvc@denis2019.onmicro...	26/02/2019
\\scan-weu01\share1\gnuht\984258844\azure sec...	2_azureconnectionstring.txt		No	Azure IAAS Database Connection St...	aipscannersvc@denis2019.onmicro...	26/02/2019
\\scan-weu01\share1\gnuht\984258844\azure sec...	4_azureredisconnectionstring...		No	Azure Redis Cache Connection String	aipscannersvc@denis2019.onmicro...	26/02/2019
\\scan-weu01\share1\gnuht\984258844\azure sec...	1_azuredocumentdbauthkey.txt		No	Azure Storage Account Key (Generi...	aipscannersvc@denis2019.onmicro...	26/02/2019
\\scan-weu01\share1\gnuht\984258844\azure sec...	1_azuredocumentdbauthkey.txt		No	Azure Storage Account Key (Generi...	aipscannersvc@denis2019.onmicro...	26/02/2019
\\scan-weu01\share1\gnuht\984258844\azure sec...	10_azureemulatorstorageaccoun...		No	Azure Storage Account Key (Generic)	aipscannersvc@denis2019.onmicro...	26/02/2019
\\scan-weu01\share1\gnuht\837572301\azure sec...	azure_secret_3.txt		No	Azure Storage Account Key (Generic)	aipscannersvc@denis2019.onmicro...	26/02/2019

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support
- Azure Information Protecti...

# Endpoint Data Discovery



# Endpoint data discovery today

## AIP client

- Any set / remove / relabel event
- Sensitive info types and custom regexes on file Save (preview)
- Win 7/8/10 + Office 2010/13/16
- Requires AIP client
- Runs inside the app and inspect only files opened by app that uses AIP client

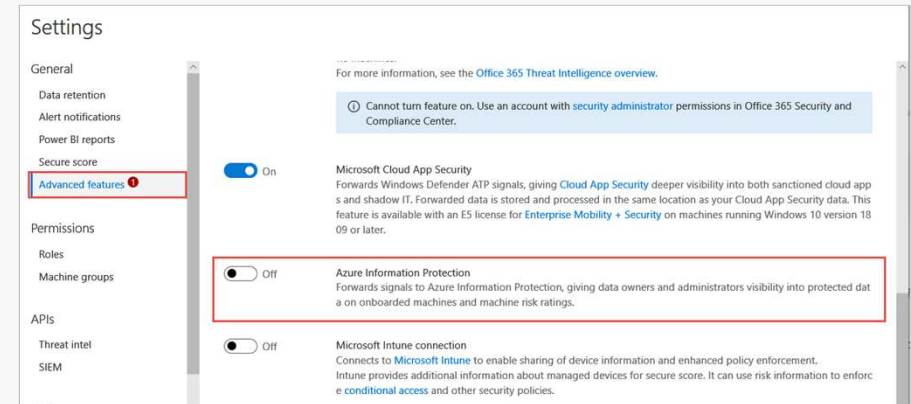
## WDATP and AIP integration

- Labeled files created (for ex. downloaded) or modified on the endpoint
- Sensitive info types and custom info-types matched in content (coming soon)
- Latest Win 10 (RS-5 at least)
- No additional SW required
- Runs on the OS level and inspect all newly created or modified files

# How to?

## WDATP

- Enable AIP integration on WDATP portal
- Upgrade Windows to build



- **AIP client discovery**
- Latest AIP preview client (1.48.1.0 and above)
- Currently in private preview and planned to be opened to public in Q2 CY2019

## Azure Information Protection - Data discovery (Preview)

Search (Ctrl+F)

### General

Quick start

### Dashboards

Usage report (Preview)

Activity logs (Preview)

Data discovery (Preview)

### Classifications

Labels

Policies

### Scanner

Nodes (Preview)

### Manage

Configure analytics (Preview)

Languages

Protection activation

Unified labeling (Preview)

Log Analytics

Location type

Any

Location

Search by location

Labels

Any

Protected

Any

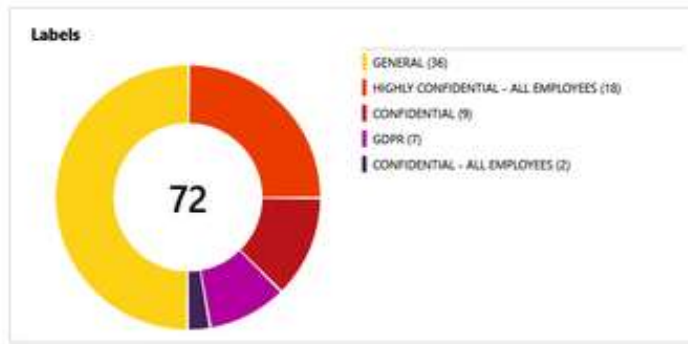
Information Types

Any

Device risk

Any

### Overview



### Information Types



LOCATION TYPE	LOCATION	LABELED FILES	PROTECTED FILES	INFORMATION TYPES MATCHES	DEVICE RISK
Endpoint	W10-IW-CLIENT1	28	0	0	Medium
Endpoint	W10-IW-CLIENT2	24	0	0	No known risks
File repository	\\islands\public\	20	0	20	N/A

# Endpoint Data Discovery - Demo

- +
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support
- Azure Information Protecti...

Dashboard > Azure Information Protection - Activity logs (Preview)

### Azure Information Protection - Activity logs (Preview)

Search (Ctrl+/)

- General
- Quick start
- Analytics
  - Usage report (Preview)
  - Activity logs (Preview)
  - Data discovery (Preview)
  - Recommendations (Preview)
- Classifications
  - Labels
  - Policies
- Scanner
  - Nodes
  - Profiles (Preview)
- Manage
  - Configure analytics (Preview)
  - Languages
  - Protection activation
  - Unified labeling (Preview)

Columns Log Analytics

Activity date:  User:  File path:  Activity:  Labels:

Protected:  Device name:  Application name:

DATE	TIME	USER	ITEM NAME	ACTIVITY	LABEL	PROTECTION	DEVICE NAME	APPLICATION
06/03/2019	02:31:17	admin@denis2019.onmic...	test .msg	New label	General	No	DEMIZETS-SURF.MID...	Outlook
06/03/2019	02:28:53	admin@denis2019.onmic...	test.msg	New label	General	No	DEMIZETS-SURF.MID...	Outlook
06/03/2019	02:17:07	admin@denis2019.onmic...	test.msg	New label	Confidential \ Recipients ...	Yes	DEMIZETS-SURF.MID...	Outlook
06/03/2019	00:51:12	admin@denis2019.onmic...	see the doc.msg	New label	Confidential \ Shared wit...	Yes	DEMIZETS-SURF.MID...	Outlook
06/03/2019	00:50:24	admin@denis2019.onmic...	document1	Access	Confidential \ Shared wit...	Yes	DEMIZETS-SURF.MID...	Word
06/03/2019	00:50:11	admin@denis2019.onmic...	document1	New label	Confidential \ Shared wit...	Yes	DEMIZETS-SURF.MID...	Word
06/03/2019	00:47:34	admin@denis2019.onmic...	lorem ipsum dolor sit ...	Access	Confidential \ Shared wit...	Yes	DEMIZETS-SURF.MID...	Word
06/03/2019	00:47:31	admin@denis2019.onmic...	lorem ipsum dolor sit ...	Upgrade label	Confidential \ Shared wit...	Yes	DEMIZETS-SURF.MID...	Word
06/03/2019	00:47:14	admin@denis2019.onmic...	document1	New label	General	No	DEMIZETS-SURF.MID...	Word
06/03/2019	00:45:40	admin@denis2019.onmic...	view only.docx	Access	General	Yes	DEMIZETS-SURF.MID...	Word
06/03/2019	00:43:13	admin@denis2019.onmic...	view only.docx	Access	General	Yes	DEMIZETS-SURF.MID...	Word
06/03/2019	00:42:43	admin@denis2019.onmic...	document1	New label	General	No	DEMIZETS-SURF.MID...	Word
06/03/2019	00:40:45	admin@denis2019.onmic...	new microsoft word d...	Access	General	Yes	DEMIZETS-SURF.MID...	Word
06/03/2019	00:40:45	admin@denis2019.onmic...	new microsoft word d...	New label	General	Yes	DEMIZETS-SURF.MID...	Word
05/03/2019	21:41:31	admin@denis2019.onmic...	usde this credits.msg	New label	Highly Confidential \ Cre...	No	DEMIZETS-SURF.MID...	Outlook

\* Displaying first 1000 records

# Cloud Data Discovery

# Gain deep visibility and granular controls into cloud app usage with Microsoft Cloud App Security

## Cloud discovery

Discover cloud apps used in your organization, get a risk assessment and alerts on risky usage.



## Data visibility

Gain deep visibility into where data travels by investigating all activities, files and accounts for managed apps.



## Data control

Monitor and protect personal and sensitive data stored in cloud apps using granular policies.



# Cloud data discovery does today?

- Repositories

- SharePoint Online / OneDrive
- 3<sup>rd</sup> party repositories (Box, G Suite)

- Classification

- Classification: O365 engine (built-in, custom info types, fingerprint)

- Remediation

- Label and protect
- Quarantine / Make private / Remove external sharing
- Access Policy (CA)



Settings

🔍 Search

- System
- Organization details
- Mail settings
- Export settings
- Cloud Discovery
- Score metrics
- Snapshot reports
- Continuous reports
- Automatic log upload
- App tags
- Exclude entities
- User enrichment
- Anonymization
- Delete data
- Information Protection
- Admin quarantine
- Azure Information Protection**
- Azure security
- Files
- Conditional Access App Control
- Default behavior
- User monitoring

### Azure Information Protection

#### Azure Information Protection settings

- Automatically scan new files for Azure Information Protection classification labels and content inspection warnings ⓘ
- Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant ⓘ

Get more info in the [Azure Information Protection integration guide](#)

We secure your data as described in our [privacy statement](#).

#### Inspect protected files

File policies can inspect content in Azure Information Protection protected files. To inspect protected files, grant Cloud App Security permission in Azure AD.

- Active**  
Protected files can be inspected by file policies. [Learn more](#)

### Edit file policy

**Policy template**  
No template

**Policy name**  
Info Protection Demo Policy

**Description**  
Policy for Ignite Policy

**Policy severity** Low | **Category** DLP

**Create a filter for the files this policy will act on**

FILES MATCHING ALL OF THE FOLLOWING Edit and preview results

File name contains words Confidential

**Apply to:** all files

**Apply to:** all file owners

**Content inspection method:** None

**Alerts**  
 Create an alert for each matching file [Use your organization's default settings](#)

- Send alert as email ⓘ
- Send alert as text message ⓘ

[Save these alert settings as the default for your organization](#)

### Governance

Box - 1 selected

- Send policy-match digest to file owner ⓘ
  - CC additional users ▾
- Remove external users
- Remove direct shared link
- Restrict to collaborators only
- Put in user quarantine
- Put in admin quarantine
- Notify last file editor
- Remove a collaborator ▾
- Apply classification label ▾

Select an Azure Information Protection classification label to be used to protect matching files:

Company Confidential Ignite

Protection will be applied to any file that is supported by native protection.

> Microsoft OneDrive for Business



> Microsoft SharePoint Online

> Dropbox

The rule was modified 2 days ago

- All Files
- Favorites
- Synced to Desktop
- Trash
- Messages
- Collaborators
- Admin Console
- Box Notes
- Dev Console

All Files > Info Protection Demo Folder

Name	Updated	Size
 Confidential Document.docx	Today by Julia	18.8 KB
 Confidential.xlsx [v2]	Sep 22, 2017 by Julia	33 KB

New Upload

Sharing Details





**No Collaborators**  
Collaborate by inviting people to this folder.

Share this Folder

- All Files
- Favorites
- Synced to Desktop
- Trash
- Messages
- Collaborators
- Admin Console
- Box Notes
- Dev Console

All Files > Info Protection Demo Folder

Name	Updated	Size
 Confidential Document.docx [V2]	Today by Julia	42 KB
 Confidential.xlsx [V2]	Sep 22, 2017 by Julia	33 KB

New Upload

Sharing Details



**No Collaborators**  
Collaborate by inviting people to this folder.

Share this Folder

Policies > Info Protection Demo Policy

Matching now | Quarantined | History

Advanced

AUTHORIZATION: [!], [✓] | APP: Select apps... | OWNER: Select owner (email)... | ACCESS LEVEL: Select access level... | FILE TYPE: Select type... | OWNER OU: Select organizational units...

1 - 20 of 33 files

File name	Owner	App	Collaborators	Policies	Detection date
Confidential Document.docx	Julia	Box	1	1 policy match	Sep 25, 2017
Confidential.xlsx	Julia	Box	1	1 policy match	Sep 22, 2017
Confidential File (22).docx.Ink	Gartner	Microsoft SharePoint Onlii	3 collaborators	1 policy match	Sep 22, 2017
Confidential File.docx	MOD Administrator	Microsoft OneDrive for Bu	1 collaborator	3 policy matches	Sep 22, 2017
G88 - Confidential labeled (6).docx	Aldo Muller	Microsoft SharePoint Onlii	4 collaborators	4 policy matches	Sep 22, 2017
Confidential File (6).docx	Gartner	Microsoft SharePoint Onlii	3 collaborators	3 policy matches	Sep 22, 2017
Confidential File.docx	Gartner	Microsoft SharePoint Onlii	27 collaborators	3 policy matches	Sep 22, 2017
G88 - Confidential labeled (3).docx	Yinon	Box	1 collaborator	1 policy match	Sep 22, 2017
Confidential File (4).docx	Gartner	Microsoft SharePoint Onlii	3 collaborators	3 policy matches	Sep 22, 2017

Policies > Info Protection Demo Policy

Matching now | Quarantined | History

Advanced

AUTHORIZATION: [!], [✓] | APP: Select apps... | OWNER: Select owner (email)... | ACCESS LEVEL: Select access level... | FILE TYPE: Select type... | OWNER OU: Select organizational units...

1 - 20 of 33 files

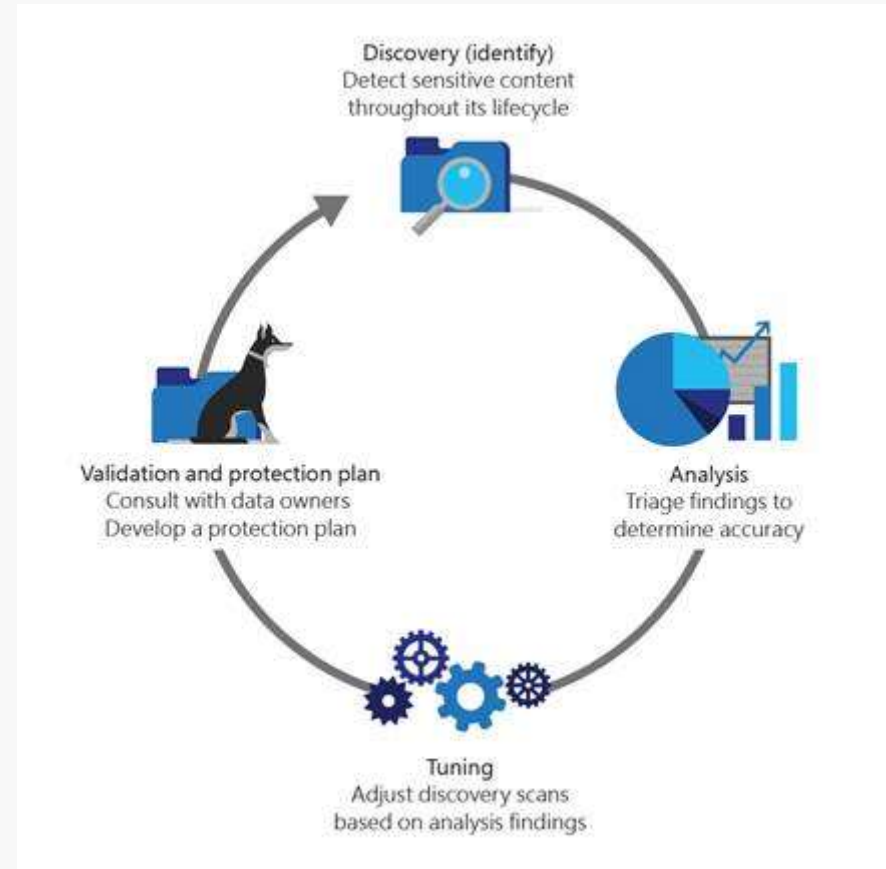
File name	Owner	App	Collaborators	Policies	Detection date
Confidential Document.docx	Julia	Box		1 policy match	Sep 25, 2017
Path: Loading...		URL: <a href="https://app.box.com/files/0/f/38742838840/1/f_229050303211">https://app.box.com/files/0/f/38742838840/1/f_229050303211</a>			
Type: document	Owner: <a href="#">casdemo2017@outlook.com (Julia)</a>	Created: Sep 25, 2017	Policies: <a href="#">Info Protection Demo Policy</a>		
MIME type: application/vnd.openxmlformats-officedocurr	Owner OU: —	Modified: Sep 25, 2017	Classification labels: —		
File identifiers: <a href="#">View file identifiers</a>	Collaborators: —	File size: ~42 KB	Scan status: <b>2 completed</b>		
Confidential.xlsx	Julia	Box		1 policy match	Sep 22, 2017
Confidential File (22).docx.Ink	Gartner	Microsoft SharePoint Onlii	3 collaborators	1 policy match	Sep 22, 2017
Confidential File.docx	MOD Administrator	Microsoft OneDrive for Bu	1 collaborator	3 policy matches	Sep 22, 2017
G88 - Confidential labeled (6).docx	Aldo Muller	Microsoft SharePoint Onlii	4 collaborators	4 policy matches	Sep 22, 2017
Confidential File (6).docx	Gartner	Microsoft SharePoint Onlii	3 collaborators	3 policy matches	Sep 22, 2017

# Best practices and roadmap



# How to start

- Start by discovery of your data, if you do not know what to search for just discovery all built-in infotypes
- Analyze the results and proceed to policy enforcement once you are confident
- Use discovery reports to find data at risk, abnormal behavior
- Use AIP client reports to find sensitive not scanner repos





# Tips

- AIP Scanner
  - Review [Optimizing the performance of the scanner](#)
  - Detect all known information types if you do not know how to start
  - Run scanner in one-time discovery → Analyze → Switch to Always + Enforce
  - Put the scanner near the scanned repo
  - Use repo settings if you have some repo specific behavior for repos in same profile: ex. discovery vs enforce
- AIP analytics
  - Use client discovery to identify repos with sensitive data and feed scanner with this info
  - Use discovery dashboard to identify discovered info types and set automatic rules
- MCAS
  - Set label discovery to identify labels from your org
  - Enable protected file inspection

# Sample queries

```
// Count of "Confidential" files set or changed by User
```

```
InformationProtectionLogs_CL
| where LabelName_s contains "Confidential"
| summarize dcount(ObjectId_s) by UserId_s
```

```
// Get all event reported by WDATP
```

```
InformationProtectionLogs_CL
| where Workload_s == "Windows Defender"
```

```
// Get all not protected files labeled as Highly Confidential
```

```
InformationProtectionLogs_CL
| where Protected_b == false and LabelName_s
contains "Highly Confidential"
```

```
// Get files with 3 credit cards or more
```

```
InformationProtectionLogs_CL
    | where TimeGenerated >= ago(30d)
    | where ProcessName_s contains
"msip.Scanner" or Workload_s =~ "Windows Defender"
    | where isnotempty(ObjectId_s)
    | where
isnotempty(DiscoveredInformationTypes_s)
        | mvexpand
expandedInfoTypes=todynamic(DiscoveredInformationTypes_s
)
    |
mvexpand details=todynamic(expandedInfoTypes)
    | where details.Name == "Credit Card Number"
    | mvexpand
expandedInfoTypes1=todynamic(DiscoveredInformationTypes_
s)
    |
mvexpand Count=todynamic(expandedInfoTypes)
    | where Count.Count >= 1
    | project MachineName_s, UserId_s, ObjectId_s ,
DiscoveredInformationTypes_s, details, Count
    | distinct MachineName_s, UserId_s, ObjectId_s ,
DiscoveredInformationTypes_s
```

# Roadmap



## Recent

- Scanner Operations UI (GA)
- Scanner Configuration UI (Preview)
- WDATP discovery of labeled file (Preview)
- GDPR and Azure credential sensitive information types
- Information protection analytics (preview)
- Inspection of protection files by MCAS



## On the horizon

- GA current previews
- WDATP discovery of sensitive information types (Preview)
- Scanner scale out
- Scanner support on unified labeling client
- Scanner support for custom info types and dictionaries
- Analytics recommendations





## Thank You for Joining Us!

We hope you will join us for the rest of the series. If you do not have the other occurrences, you can find them at <https://aka.ms/AIPWebinar>.

Recordings have been posted to our community forums at <https://aka.ms/AIPRecordings>.

Join our Community: <https://aka.ms/SecurityCommunity>



© 2017 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista 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. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.