



Andy Malone

Available Now



Shadows Rising is the electrifying sequel to Andy Malone's award winning, The Seventh Day. Set in both 1710 Scotland and the modern world, think Highlander meets the Davinci Code.

From historic Scottish villages, to the streets of New York and the ancient catacombs of Vatican City. Shadows Rising is a race against time thriller, packed with rich historical references entwined into a tense story that will leave you breathless and on the edge of your seat ...

Some secrets are better left undiscovered ...

Book Signing today @ Glasspaper Booth





Tinker, Tailor, **Hacker**, Spy!

Azure Information Protection inside out!



Andy Malone

(Scotland, UK)

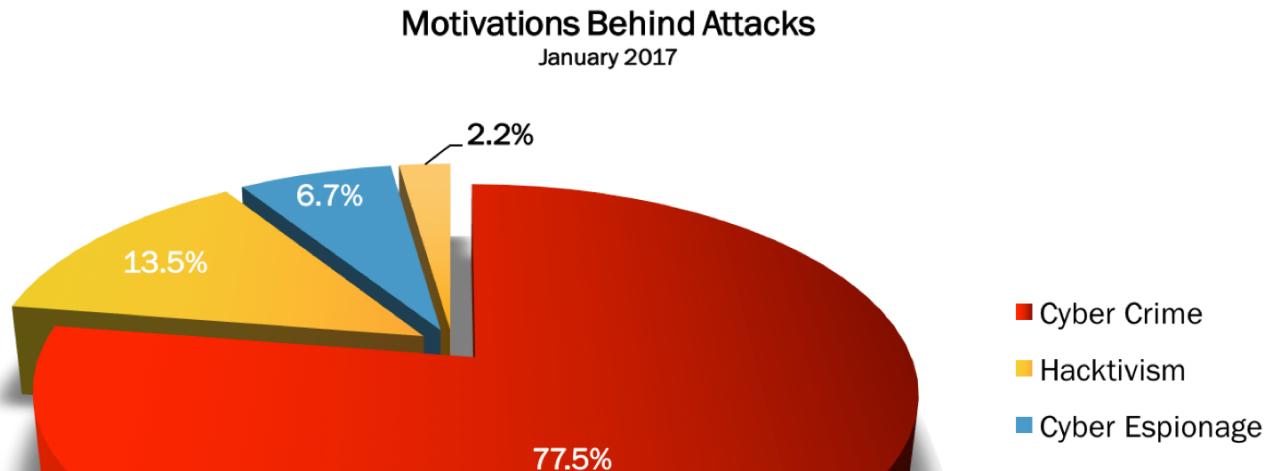
- Microsoft MVP (Enterprise Security 11 Years)
- Microsoft Certified Trainer (21 years)
- Microsoft Internal Staff Instructor
- Founder: Cybercrime Security Forum!
- Microsoft Ignite Speaker
- Author off the Sc-Fi Thrillers
- “The Seventh Day” & Shadows Rising”



Session Objectives

- Cybercrime Motivation Circa 2018
- Data Leakage: The great security dilemma
- Introducing Azure Information protection
- File Classification Explained
- AIP / ADRMS Architecture
- Rights Management Explained
- The Crypto Secret Recipe
- BYOK & HYOK Solutions
- Review

Current Motivation for Cybercrime in 2018





Fraud targeting senior executives is a "key threat", said Europol

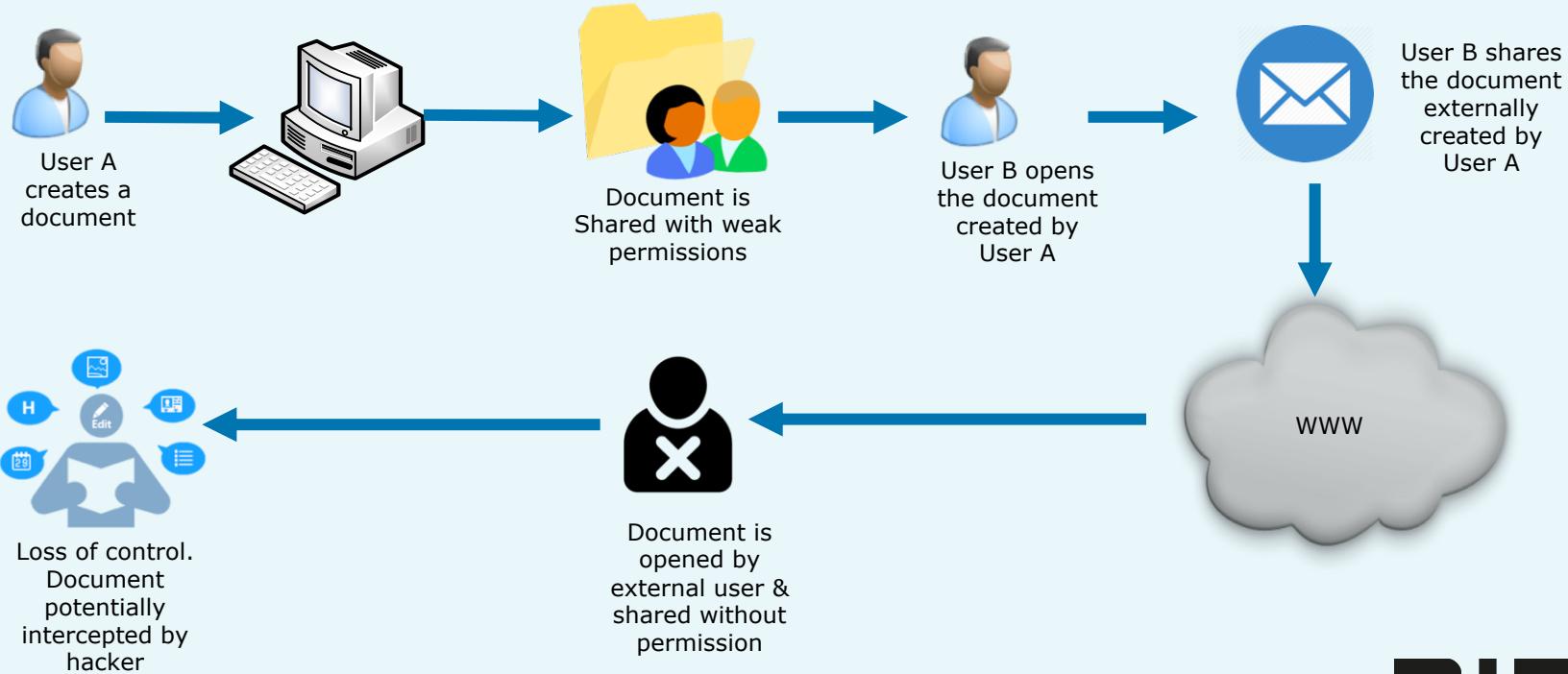
Shoddy data-stripping exposes firms' to hack attacks

9 hours ago | Technology

Large firms are vulnerable to targeted hack attacks because they do little to strip data from files on their websites, suggests research.

nic

The Problem: Traditional File Sharing



The Problem: Traditional File Sharing

- Prevents Permissions Bleed
- Once data is outside organization, its beyond the realm of your control
- Anyone can plagiarise
- Content easily copied
- Potential Copyright Infringement Issues
- Plausible Deniability Reins
- Lack of Compliance

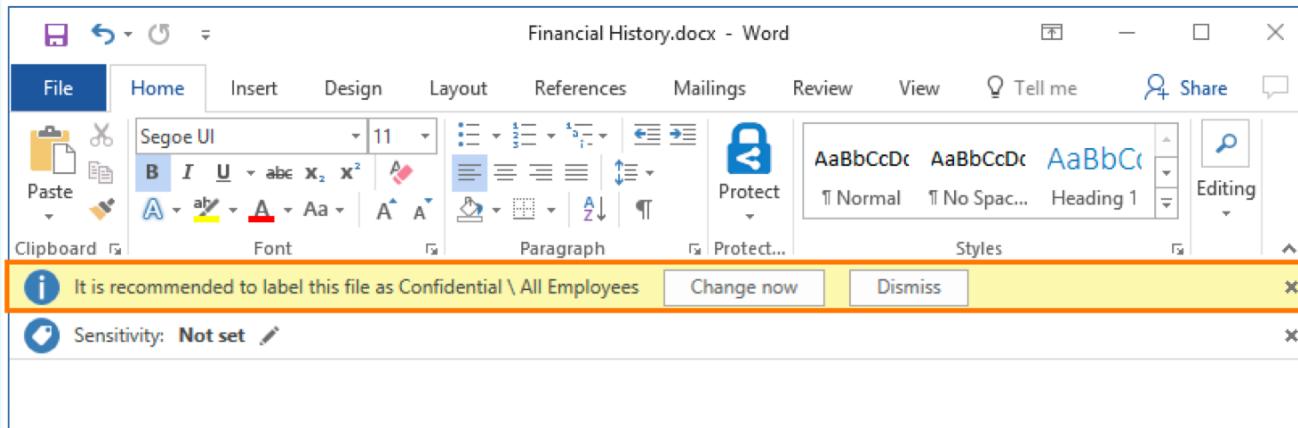


Demo

FOCA: The Dangers of poor file security

The Solution: Azure Information Protection?

- Azure Information Protection is Microsoft's cloud-based solution that helps an organization to classify, label, and protect its documents and emails.
- This can be done automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations.



But it has so many names!

- Cloud-based solutions
 - **Azure Rights Management** or **Azure Rights Management service**—frequently abbreviated to *Azure RMS*
 - **Azure Active Directory Rights Management**—occasionally abbreviated to *AADRM*
 - **Windows Azure Active Directory Rights Management**—often abbreviated to *Windows Azure AD Rights Management*
- On-premises solutions
 - **Active Directory Rights Management Services**—frequently abbreviated to *AD RMS*
 - **Windows Rights Management Services**—often abbreviated to *Windows RMS*

Information Protection: The Big Picture



Classification
and labeling



Encryption



Access
control



Policy enforcement



Document
tracking



Document
revocation



Email



Files



LOB apps



Share internally



Share externally (B2B)



Share externally (B2C)

On any device



In any part of the world

- US
- EU
- APAC
- China
- Germany



Azure information Protection Components



Identity & Authentication Services provided by Microsoft Azure Active Directory Services

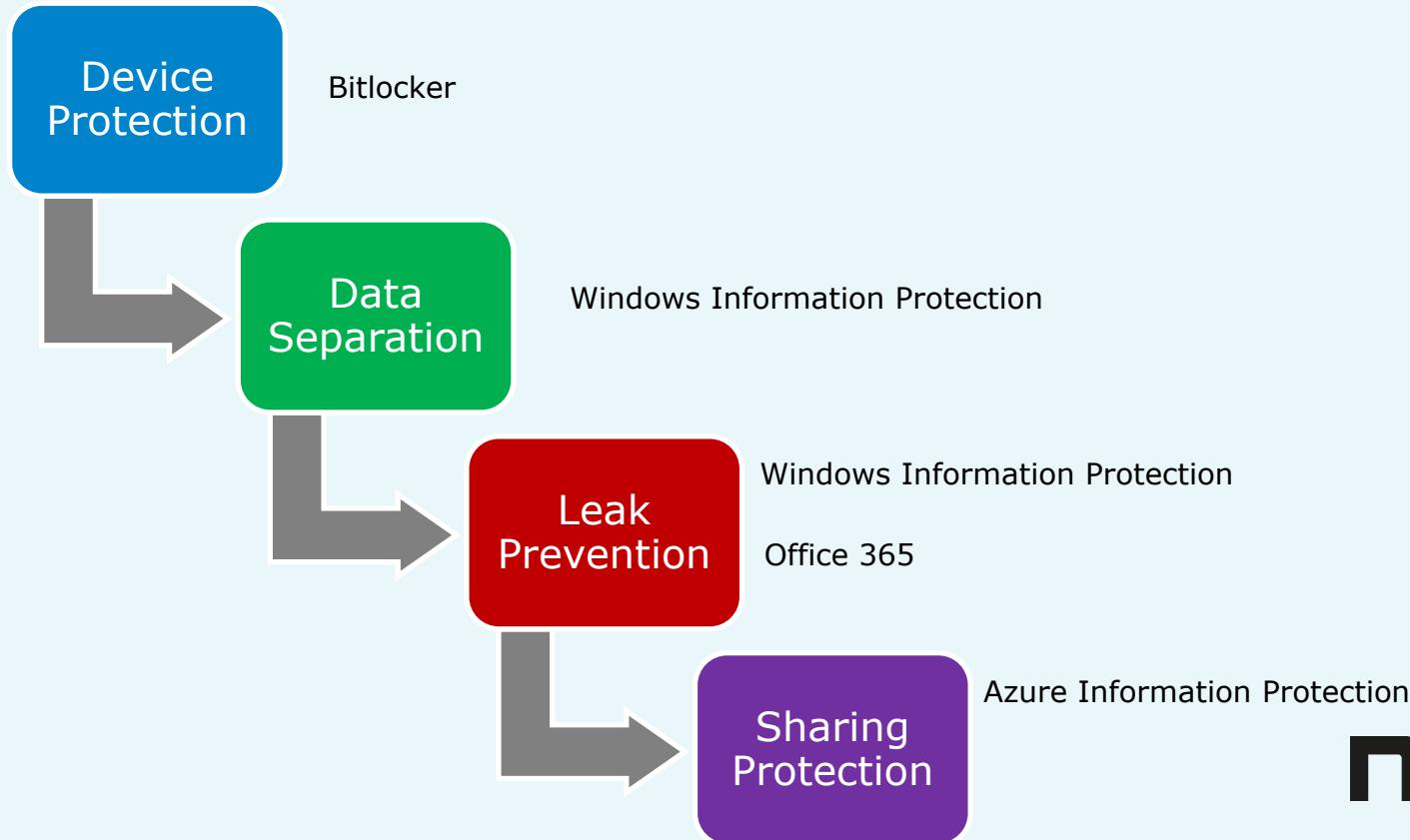


- Encryption using RSA 2048 for public key cryptography and SHA 256 for signing operations, and is FIPS 140-2 compliant.
- Default option is to let Microsoft store your encryption keys, but Bring Your Own Key (BYOK) is also supported
- information Rights Management (IRM)
Protects data by using encryption, identity, and authorization policies, even when files leave your organization, the protection provided by RMS remains in place



Policy-driven intelligent content categorization that analyses in real time from any source. Once file is classified, whether automatically or manually, a label is attached that determines whether it's encrypted and which users can access the data and what they can do with it once received

Multi Level Protection



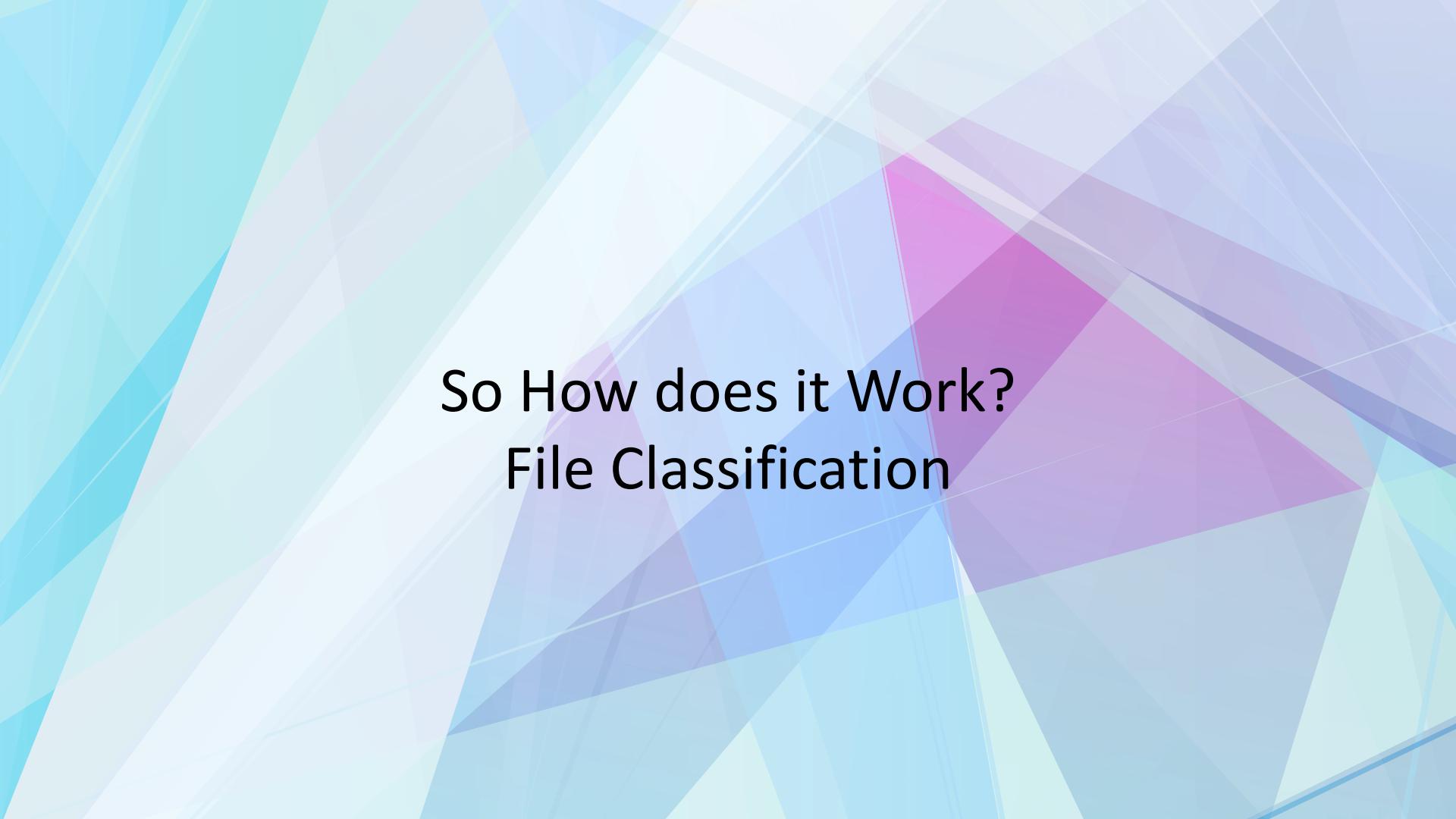
Azure Information Protection Requirements

- An Office 365 subscription that includes Azure AIP (EMS E3 at least)
- A subscription for Azure, so you can access the Azure portal
- Global administrator account to sign in to the Office 365 admin center or the Azure
- A computer running Windows (minimum of Windows 7 with Service Pack 1),
 - and which has installed either Office Professional Plus 2016, Office Professional Plus 2013 with Service Pack 1, or Office Professional Plus 2010
- Best results use Windows 10 & Office 2016
- MAC Running Office 2016 Pro Plus
- Information Protection Sharing Client
- <https://docs.microsoft.com/en-us/rights-management/information-protection/infoprotect-quick-start-tutorial>

Azure Information Protection Requirements

- **For classification, labelling, and protection,** you must have an Azure Information Protection plan
 - Office 365 “3” plan and above (E3,A3,G3)
 - Or Enterprise Mobility & Security Licence
 - Or Microsoft 365
 - Enable Azure RMS
- **For protection-only,** you must have an Office 365 plan that includes Rights Management
- Multi Factor Authentication
- Provides independence from “Device”
- Supports Onprem & Hybrid Solutions
- Must have a validated DNS Domain name in Azure
- User Accounts must authenticate with a verified UPN
- Apple & Android Apps require certificate-based authentication (CBA)

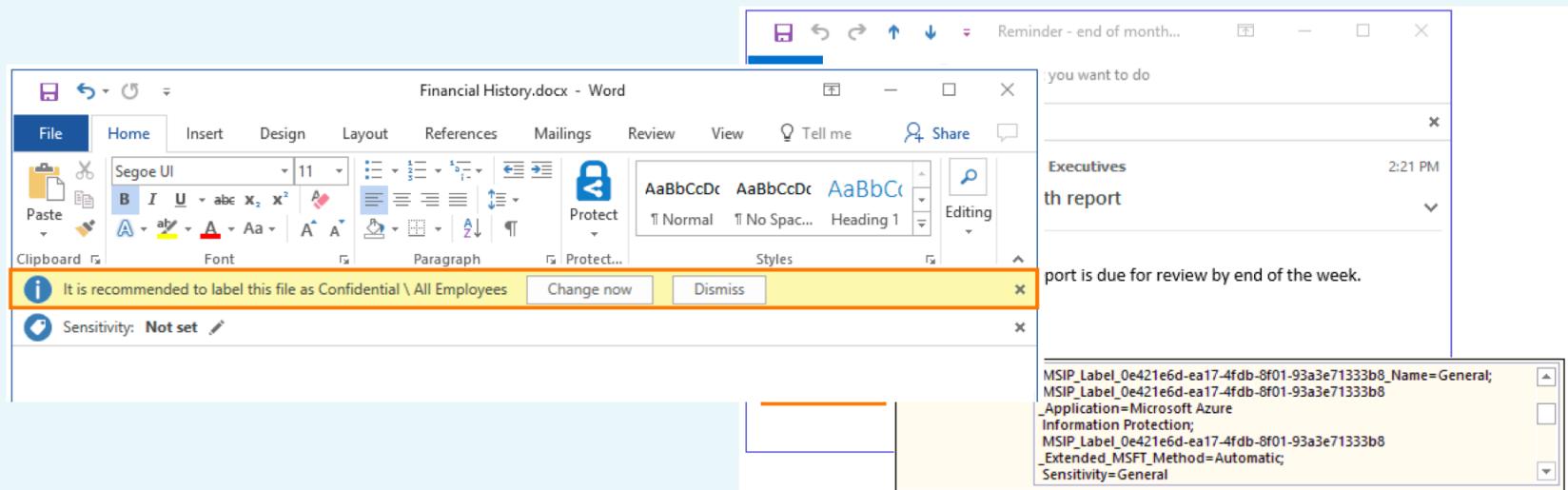




So How does it Work? File Classification

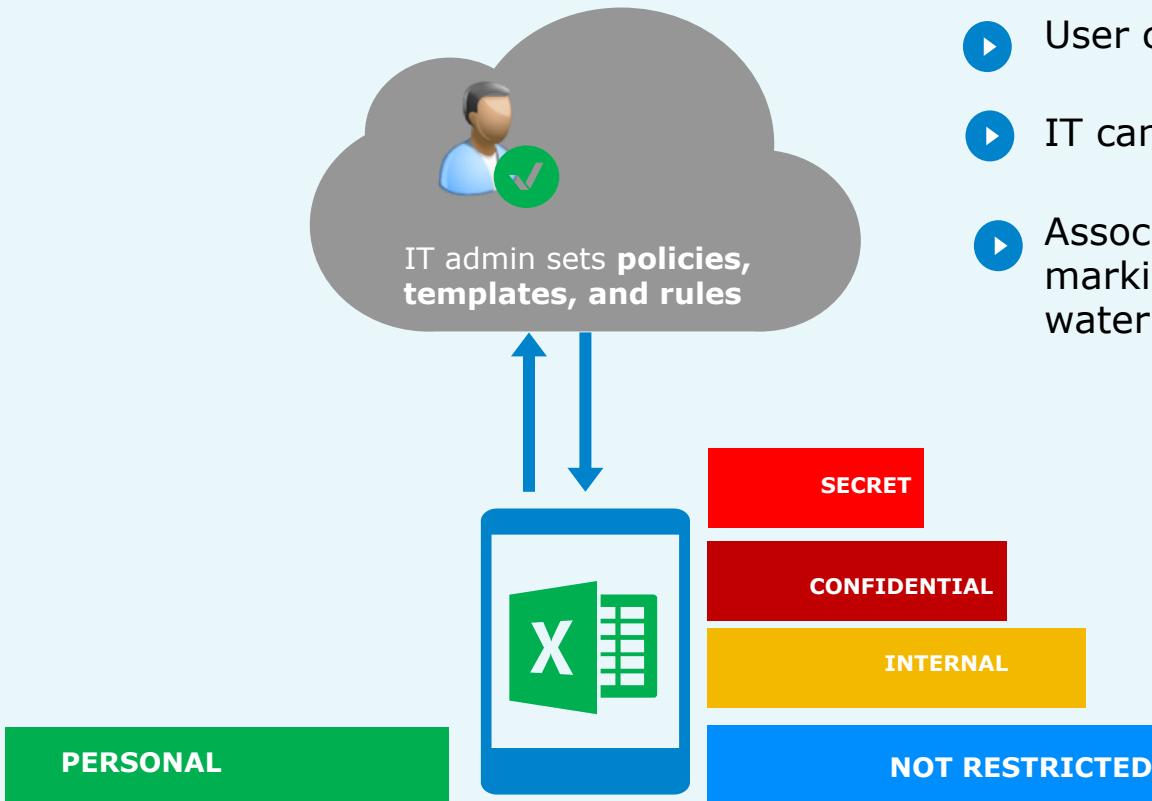
File Classification – What does it do?

- Helps an organization to classify, label, and protect its documents and emails
- Deployed automatically by administrators who define rules and conditions,
- Manually by users, or a combination where users are given recommendations.



How Classification Works

File classification based on sensitivity



- ▶ User can manually classify content
- ▶ IT can set automatic rules
- ▶ Associate actions such as visual markings and protection, such as watermarks

How Classification Works

Automated Classification

The screenshot shows a Microsoft Word document titled "Document1 - Word". The ribbon menu is visible at the top, with the "Home" tab selected. A "Sensitivity" sidebar is open on the left, showing the "Internal" option. The main content area contains a logo for "contoso Finance" and a table titled "Due Diligence Documentation".

Sensitivity: Internal

Internal

This information includes a wide spectrum of internal business data that can be used by all employees and can be shared with authorized customers and business partners. Examples for internal information are company policies and most internal

Set automatically for Hugo.Swope@contoso.com

Due Diligence Category	Documentation Task	Owner	Status
	Business Plan, Corporate Structure, Financing		
Business plan	Current five-year business plan		
	Prior business plan		
Corporate organization	Articles of incorporation		
	Bylaws		
	Recent changes in corporate structure		
	Parent, subsidiaries, and affiliates		
	Shareholders' agreements		
	Minutes from board meetings		

How Classification Works

Recommended Classification

This screenshot shows a Microsoft Word document interface with various toolbars and a status bar.

Toolbars:

- Home:** Contains Cut, Copy, Paste, and Format Painter buttons.
- Font:** Includes Calibri (Body) font, size 11, and style options (B, I, U).
- Paragraph:** Includes alignment, spacing, and protection buttons.
- Styles:** Shows a list of styles: Normal, No Spac..., Heading 1, Heading 2, Title, Subtitle, and Emphasis.

Status Bar:

- An information icon states: "This file contains credit card information therefor it was automatically labeled Confidential". A "Change now" button is present.
- A sensitivity indicator shows "Sensitivity: Not Restricted".

Table:

A table titled "Credit card" is displayed, containing the following data:

Credit Card Type	Credit Card Number
American Express	378282246310005
American Express	371449635398431
American Express Corporate	378734493671000
Australian BankCard	5610591081018250
Diners Club	30569309025904

How Classification Works

Reclassification & Justification

A screenshot of a Microsoft Word document titled "Credit card". The document contains a table with two columns: "Credit Card Type" and "Credit Card Number". The first row shows "American Express" and "378282246310005". The second row shows "American Express" and "371449635398431". The third row is partially visible with "Australian Bank". The fourth row shows "Diners Club". A Microsoft Azure Information Protection dialog box is overlaid on the document. The dialog title is "Microsoft Azure Information Protection". It asks, "Please explain why the file's classification level should be lowered:" and provides two options: "This file no longer requires that classification" and "Other - Please provide an explanation". There is a large watermark reading "Confidential" diagonally across the page.

Credit card

Credit Card Type	Credit Card Number
American Express	378282246310005
American Express	371449635398431
American Express	
Australian Bank	
Diners Club	

Microsoft Azure Information Protection

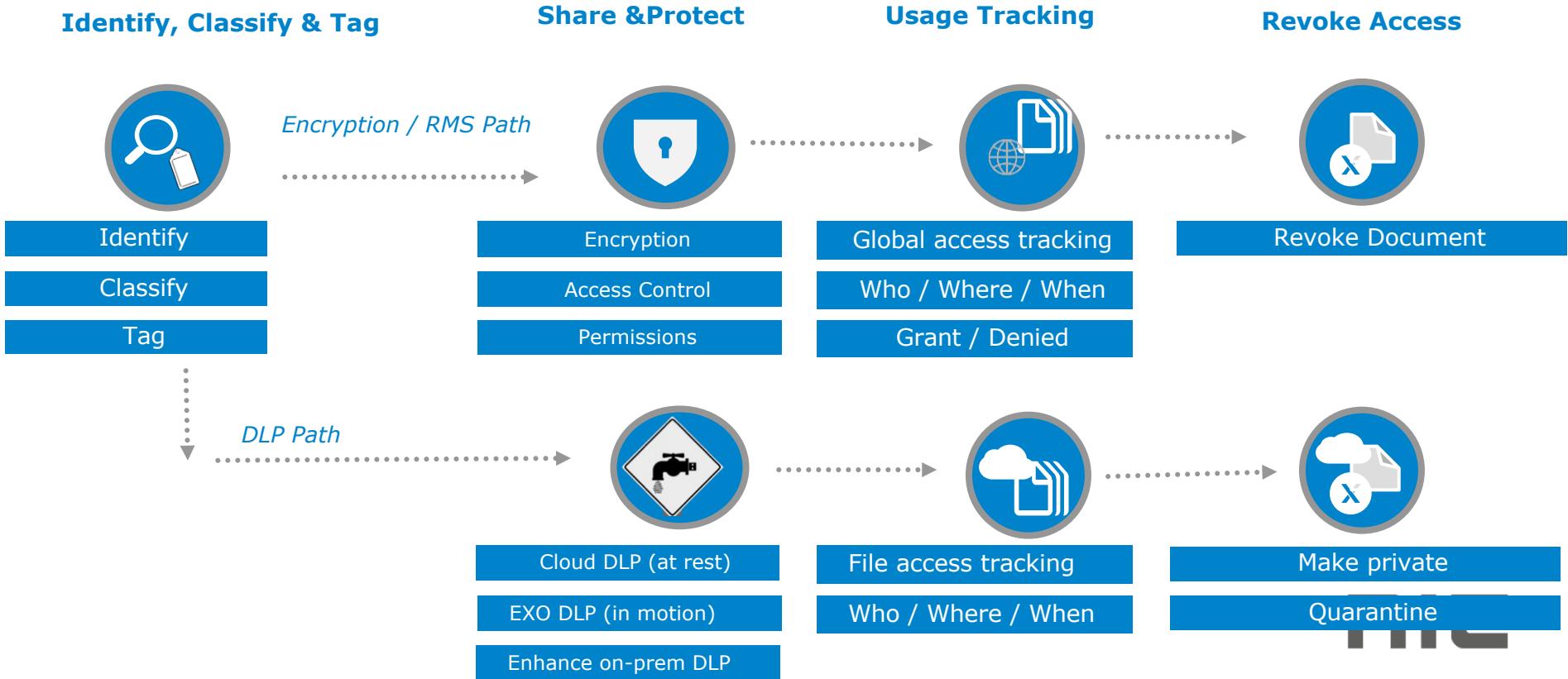
Please explain why the file's classification level should be lowered:

This file no longer requires that classification
 Other - Please provide an explanation

Confirm Cancel

Confidential

Data Classification Lifecycle

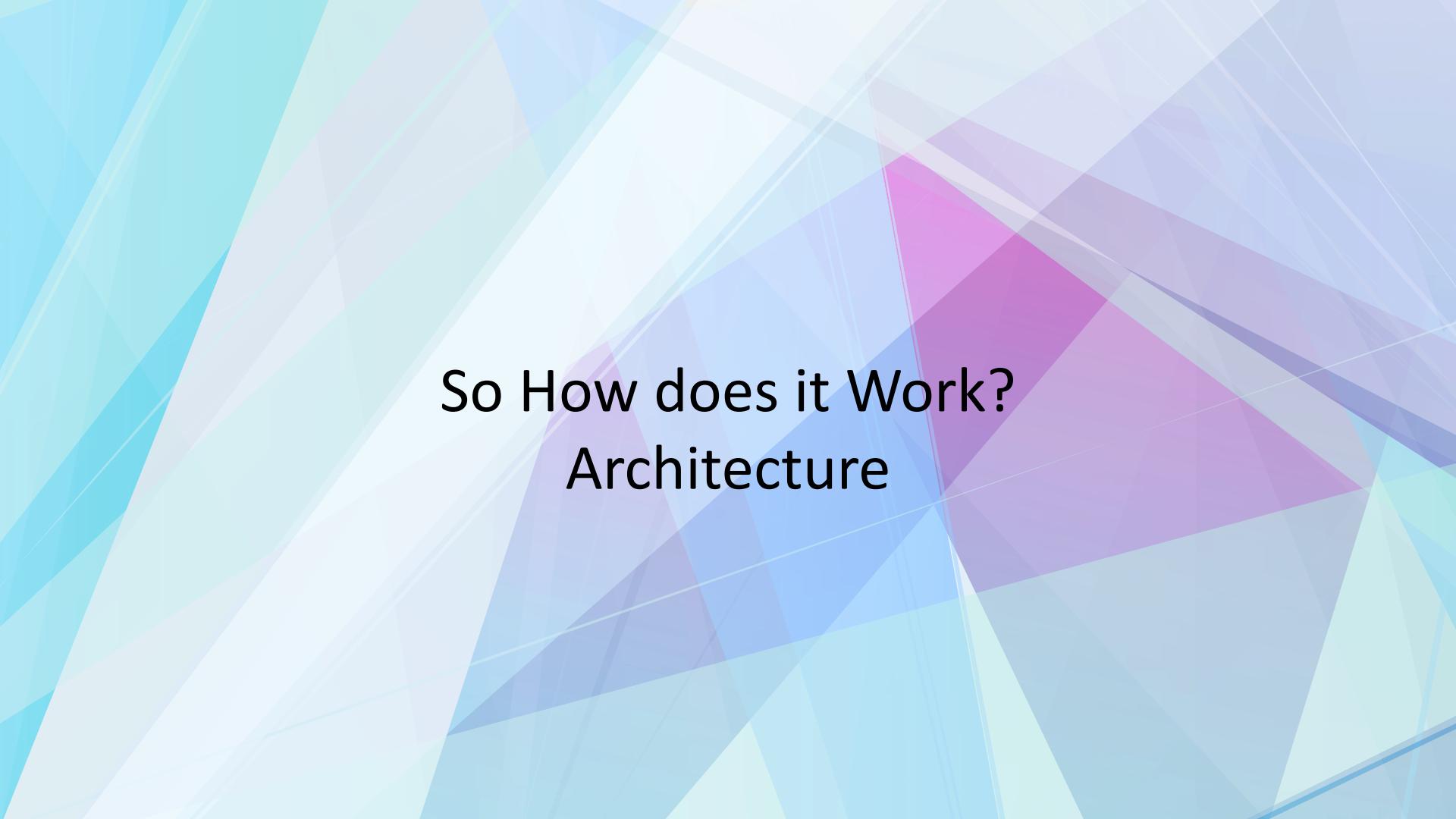


Where is Labelling & Classification information stored?

- AIP uses persistent metadata for classification, which includes a clear text label, this information can be read by DLP solutions and other applications
- For Microsoft Office & PDF documents, this metadata is stored in the following custom property: **MSIP_Label_<GUID>_Enabled=True**
- In emails, this information is stored in the xheader: msip_labels: **MSIP_Label_<GUID>_Enabled=True;**

Demo

AIP File Classification & Labelling



So How does it Work? Architecture

Architecture Clients – AIP

- **Functionality :**
 - Manual and automatic classification.
 - Tag files, apply content marketing, and apply RMS template
- Audit user classification actions
- Packaging : Office add-on
- Prerequisites : For Windows 7 and above
- **Interoperability** : MAC, Mobile, Office Online, 3rd party LOB applications (e.g. PDF, CAD, etc)
- Main product competitor: Titus enables classification of files and email from mobile

Architecture Clients – Microsoft Office

- For Windows / Mac Office 2016 Functionality :
 - Apply RMS template
 - Consume RMS protected documents
 - Manage RMS level permissions
 - For Outlook - Create ad-hoc protection template for the recipients – “Do Not Forward/Secure-Send”
- Supported platforms : Outlook, Word, Excel, PowerPoint, Visio, Project)
- Prerequisites : RMS client, Azure RMS active in tenant
- Now Available :
 - Mobile (iOS / Android)
 - O365 online
- Competition : Titus has RMS enabled e-mail and document mobile apps

Architecture: Clients – RMS Sharing Application

- For Windows :
 - Enhances File Explorer to allow RMS-protect and share a single file, or bulk protect multiple files as well as all files within a selected folder.
 - Protect more file types (pfile)
 - A built-in viewer for commonly used text, pdf, and image file types.
- For Mobile Devices / Mac :
 - Supports Open RMS-protected PDF files, pictures, text files, and any other file format protected as a .pfile.
 - Protect pictures with an RMS policy before you share them.

Architecture: Clients – Others

- FCI (File Classification Infrastructure)
 - Scan, classify(*) , and protect files on Windows Servers File Shares
 - Exchange on-prem RMS protection for e-mails- via Transport Rule
- Exchange online
 - RMS protection for e-mails – via **transport protection rules**
 - SharePoint on-prem
 - RMS protect files on download
 - SharePoint online – RMS protect files on download
 - RMS SDK – For 3rd parties
 - AIP SDK – For 3rd parties (roadmap)



So How does it Work? Rights Management

RMS Setup Step by Step

1. Confirm your subscription and assign user licenses
2. Prepare your tenant to use Azure Information Protection
 1. Tennet Key: Managed by Microsoft
 2. Tennet Key: BYOK
3. Configure and deploy classification and labelling
4. Prepare for Rights Management data protection
5. Configure your Azure Information Protection policy, applications, and services for Rights Management data protection
6. Use and monitor your data protection solutions
7. Administer the Rights Management service for your tenant account as needed



rights management



Rights management is activated

Rights Management safeguards your email and documents, and helps you securely share this data with your colleagues.

To disable Rights Management, click deactivate.

[deactivate](#)

additional configuration

You can configure advanced features for Rights Management using Microsoft Azure.

Don't have an Azure subscription? Before you click Advanced Features, sign up for a free 30 day trial .

[advanced features](#)

resources

- [What is Rights Management?](#)
- [Rights Management Deployment roadmap](#)
- [Using Rights Management](#)
- [FAQs For Rights Management](#)



Do you want to activate Rights Management?

Activating Rights Management enables users and administrators to encrypt and apply usage policies on Exchange Online email, SharePoint Online document libraries, and Office Suite documents.

[Learn more](#)

[activate](#)

[cancel](#)

Azure Information Protection: PowerShell Setup

- **Download**

WindowsAzureADRightsManagementAdministration_x64

<https://docs.microsoft.com/en-us/information-protection/deploy-use/install-powershell>

- **Install the Prerequisites**

- PowerShell V.2.0
- .Net Framework V4.5

- **Azure Information Protection cmdlets**

<https://docs.microsoft.com/en-us/information-protection/deploy-use/administer-powershell>

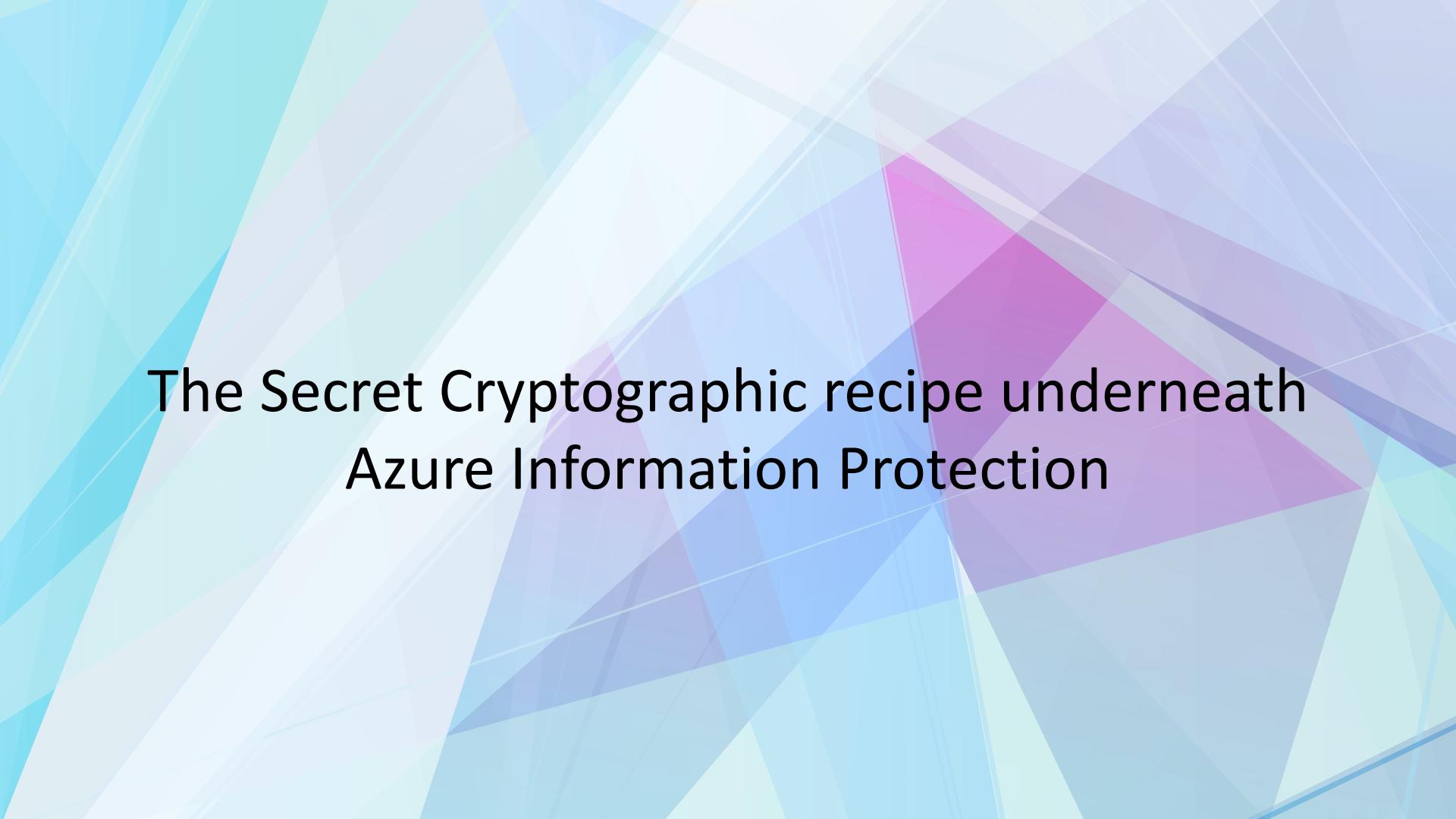
- **Connecting to Active Directory Rights Management**

```
PS C:\> Import-Module aadrm  
PS C:\> $UserCredential = Get-Credential  
PS C:\> Connect-AadrmService -Credential $UserCredential
```

Get-Command -Module AADRM

Get-Help <cmdlet_name>

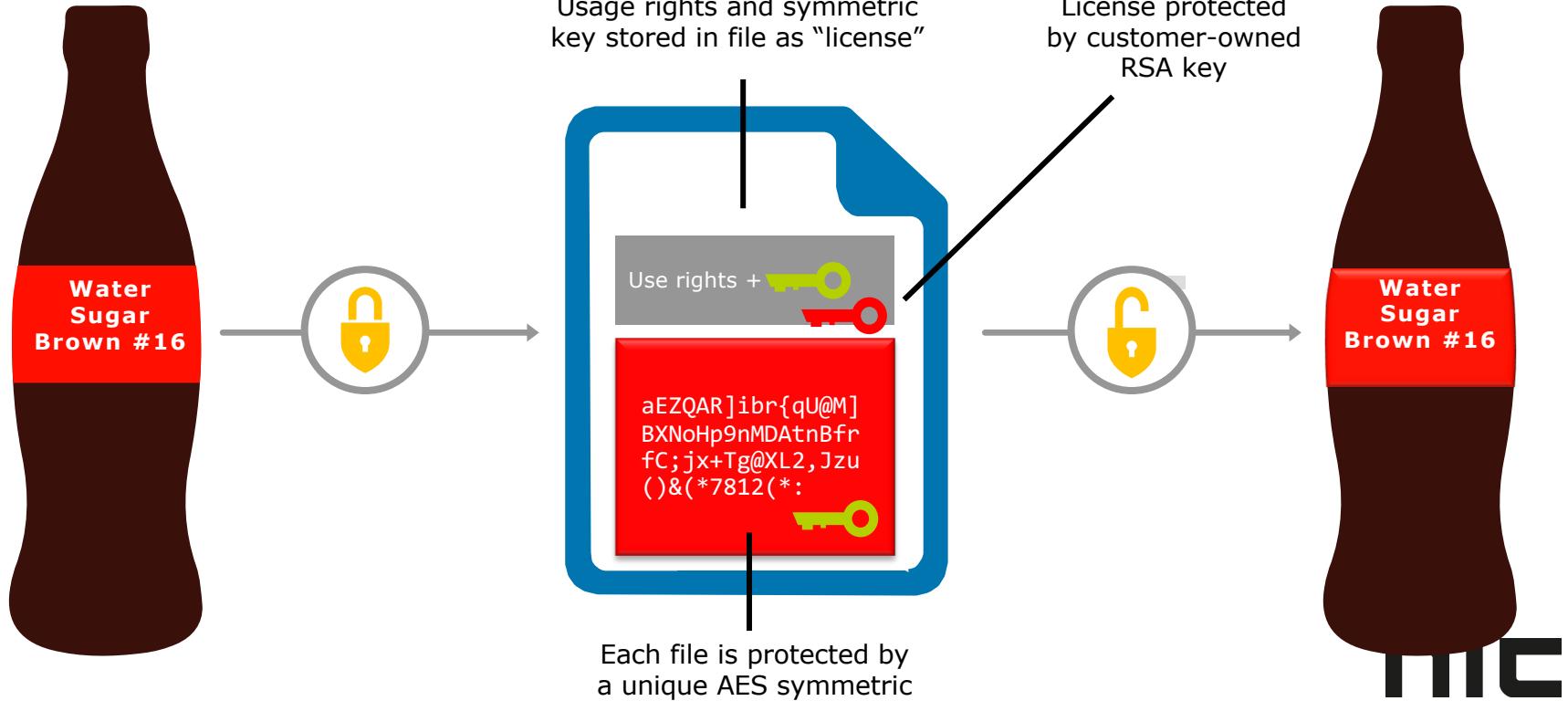




The Secret Cryptographic recipe underneath
Azure Information Protection

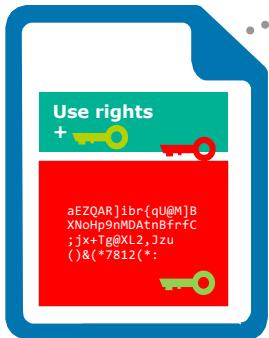


How AIP / RMS Protection Works



How RMS Protection Works

LOCAL PROCESSING ON PCS/DEVICES



File content is **never** sent to the RMS server/service



Apps protected with RMS **enforce rights**



Apps use the SDK to communicate with the RMS service/servers



Azure RMS never sees the file content, only the license



**Rights Management
Active Directory
Key Vault**



Cryptographic controls used by Azure RMS: Algorithms and key lengths

CRYPTOGRAPHIC CONTROLS

USE IN AZURE RMS

Algorithm: AES

Documentation protection

Key length: 128 bits and 256 bits [\[1\]](#)

Algorithm: RSA

Key protection

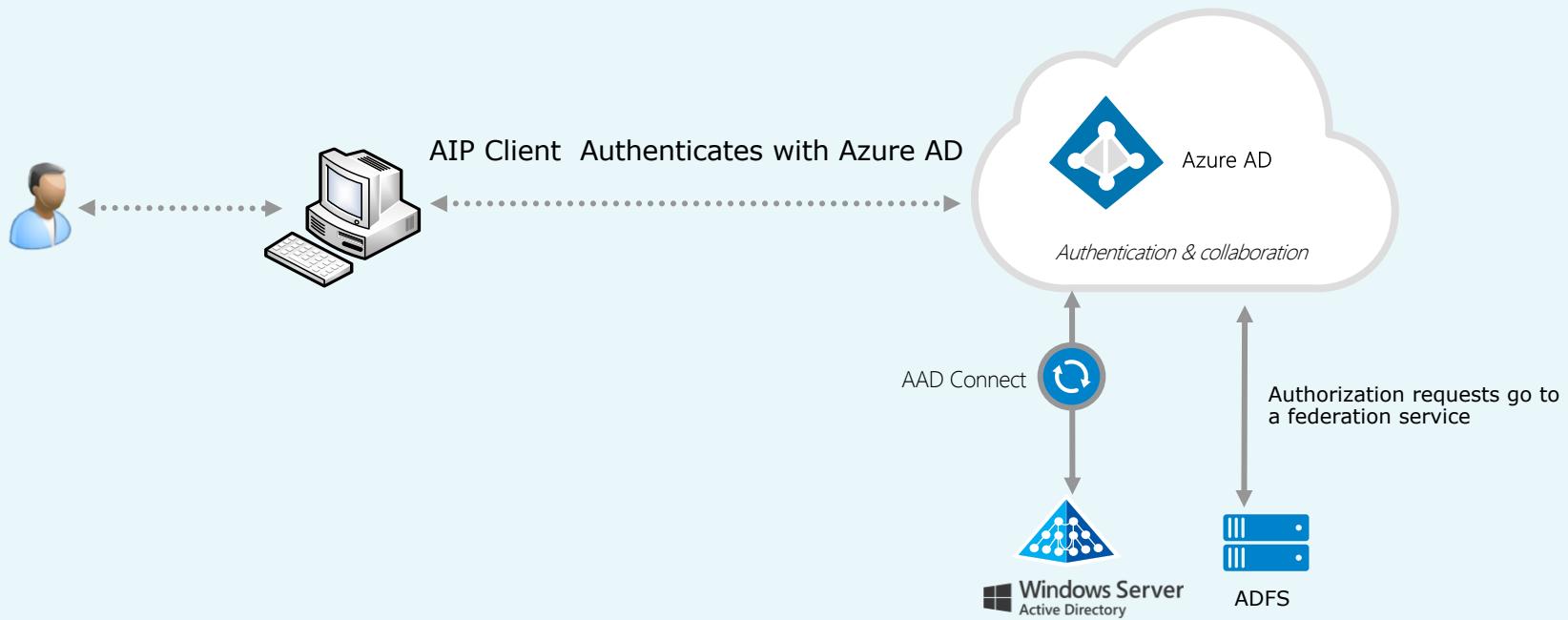
Key length: 2048 bits

SHA-256

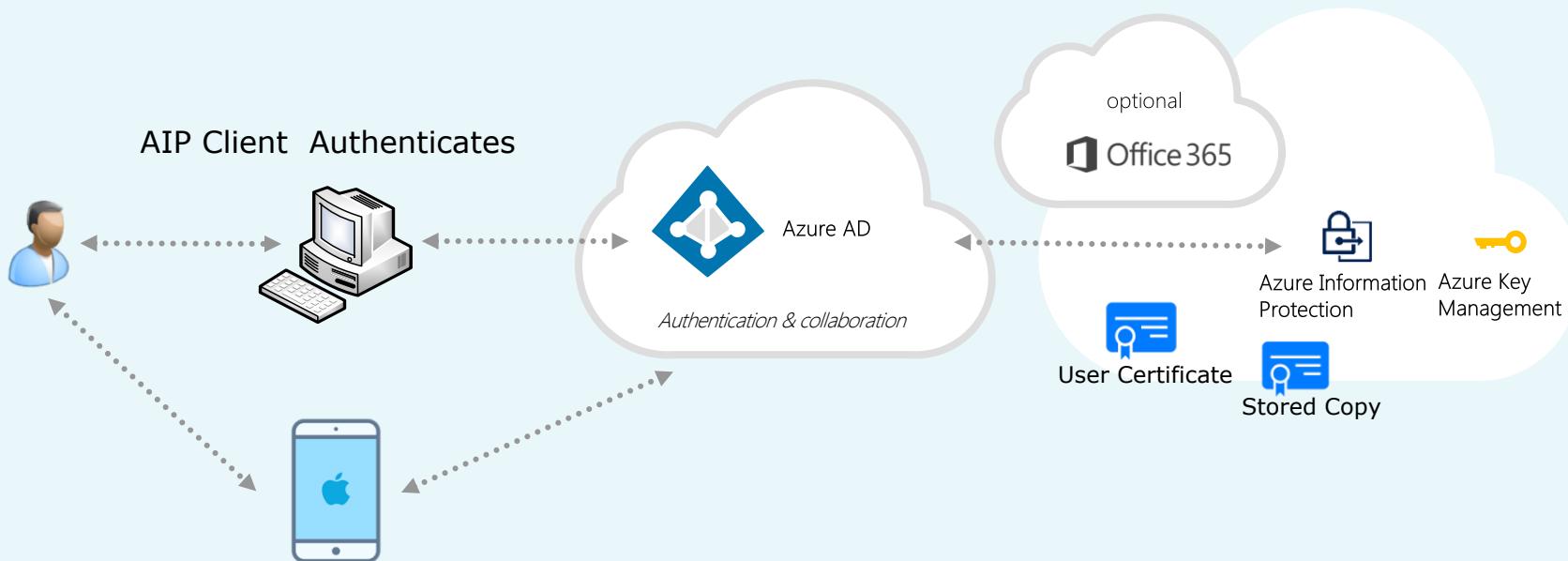
Certificate signing



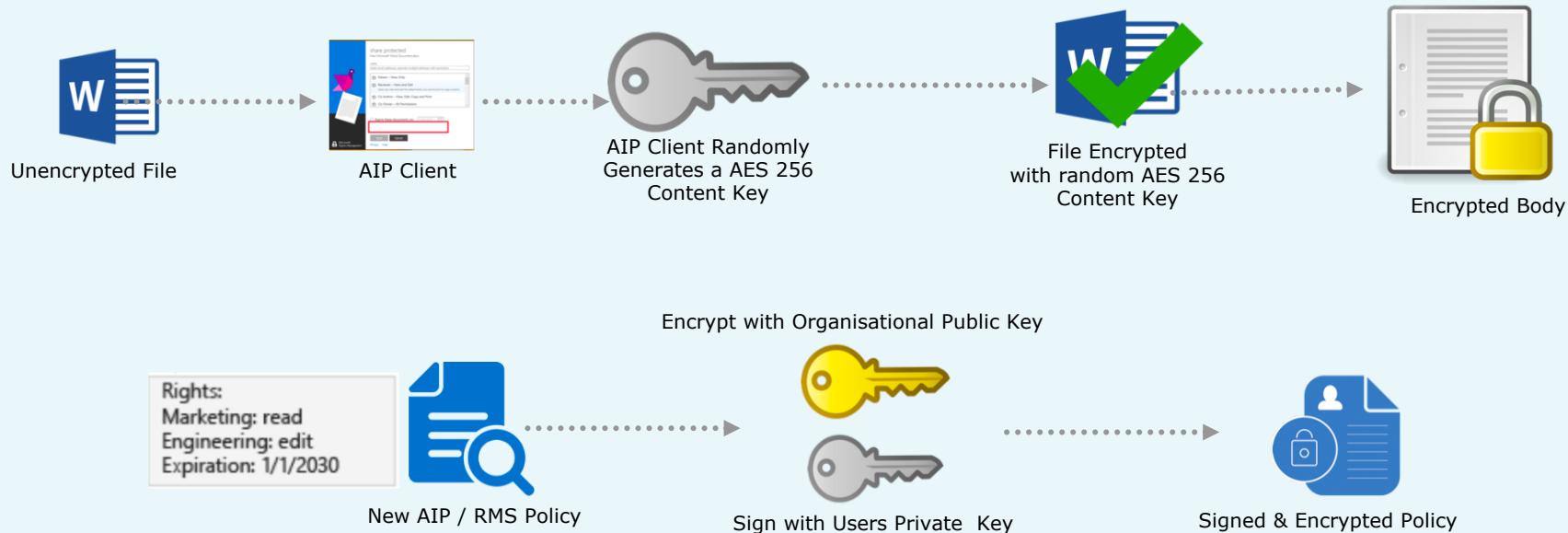
Initialing the User Environment



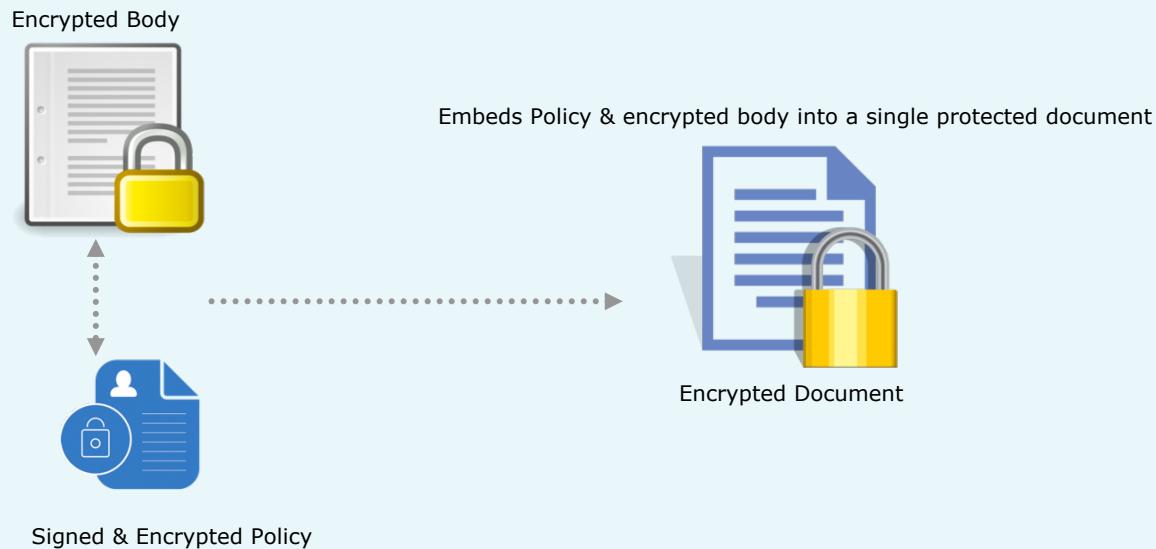
Initialing the User Environment



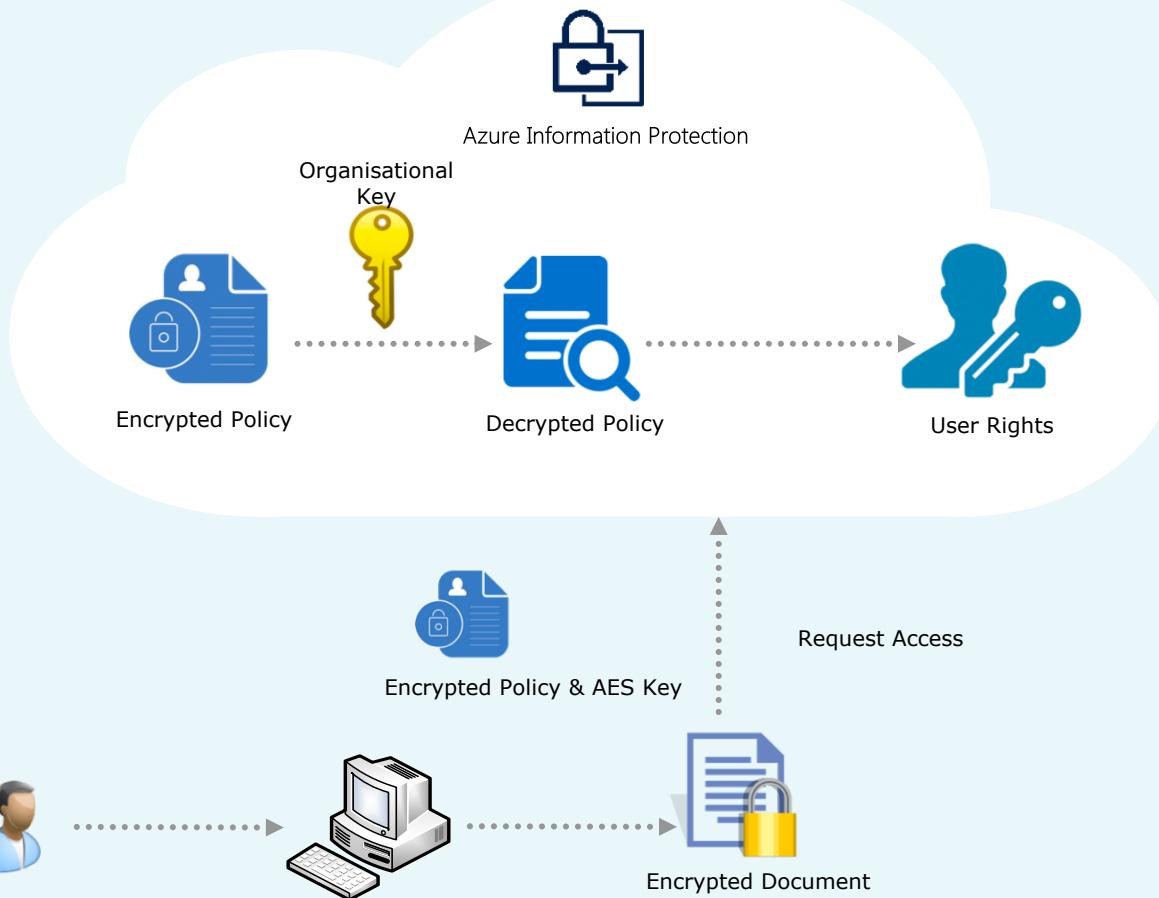
Content Protection



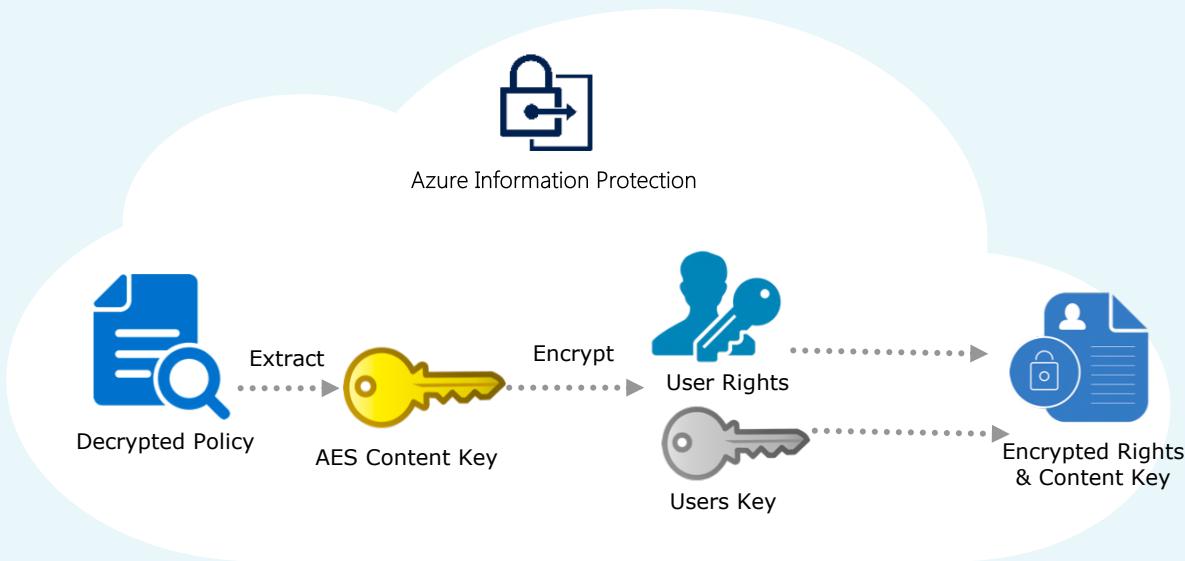
Content Protection



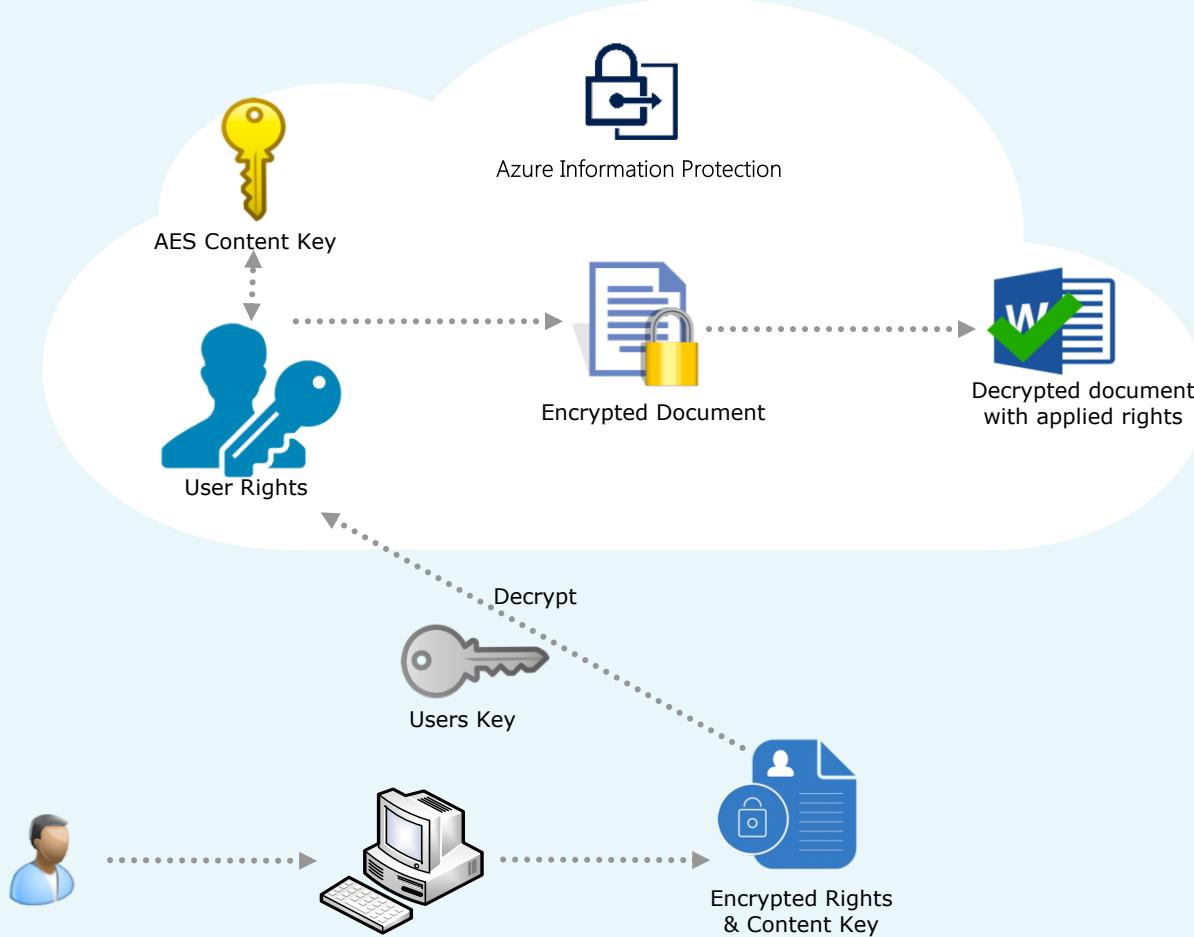
Content Consumption



Content Consumption



Content Consumption



What about mobile & other connectivity options?

- Mobile devices such as iPhone, Android – No registration process – get publication license and consumption license over TLS
- RMS Connector – Same flow but RMS connector acts as a relay between the on-prem services (e.g. Exchange, SharePoint) and Azure RMS.
- Generic protection (.pfile) – Same flow but client creates a policy that grants all rights. On consumption file is decrypted before it is passed to the native app.

Demo

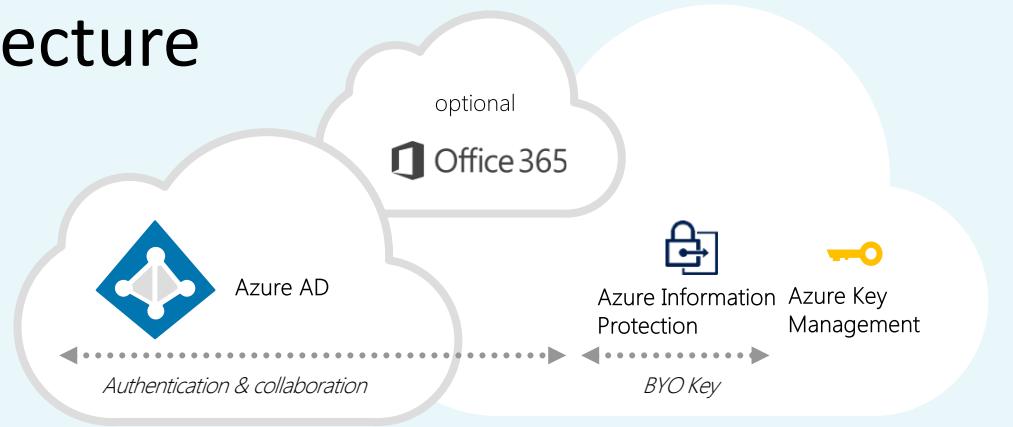
Information Protection / Rights Management In Operation



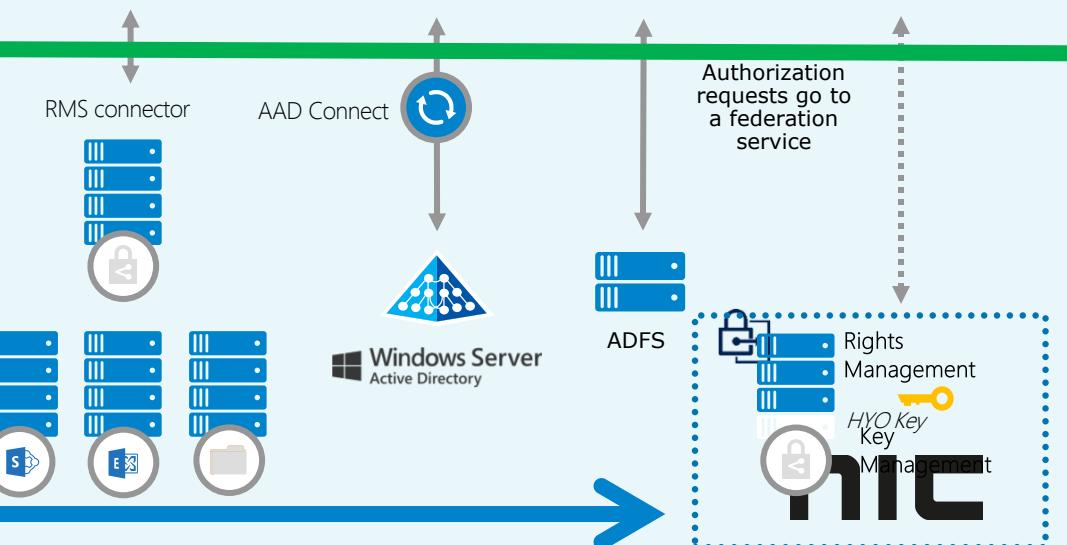
Bring Your Own Key (BYOK)
&
Host your Own Key (HYOK)

AIP Backend / Hybrid Architecture

Azure RMS Client

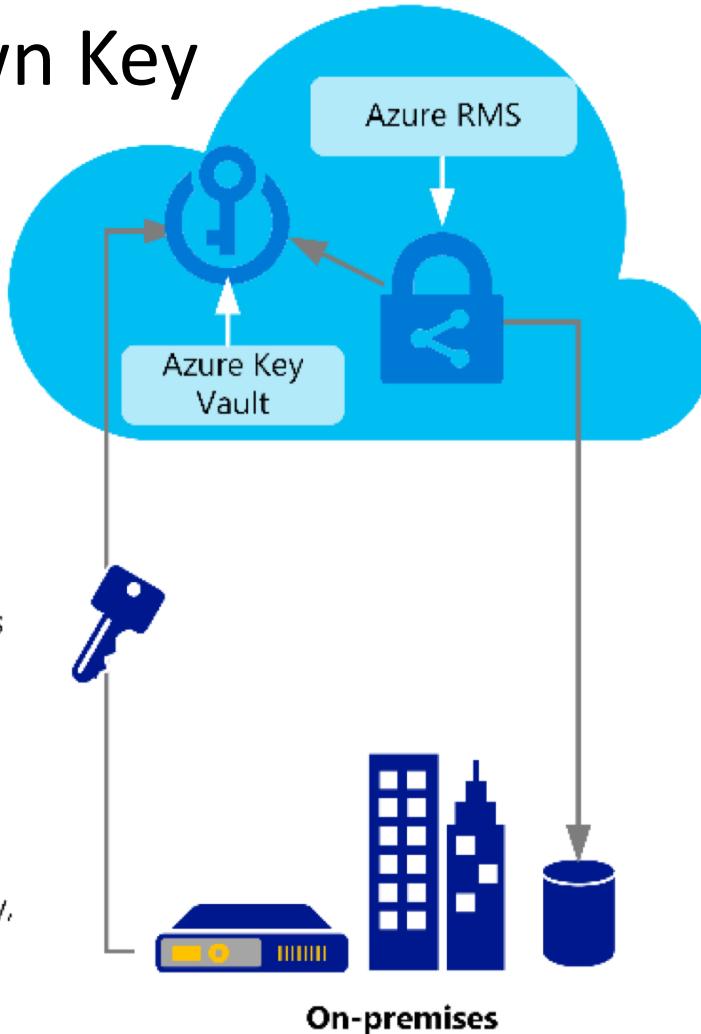


AD RMS Client



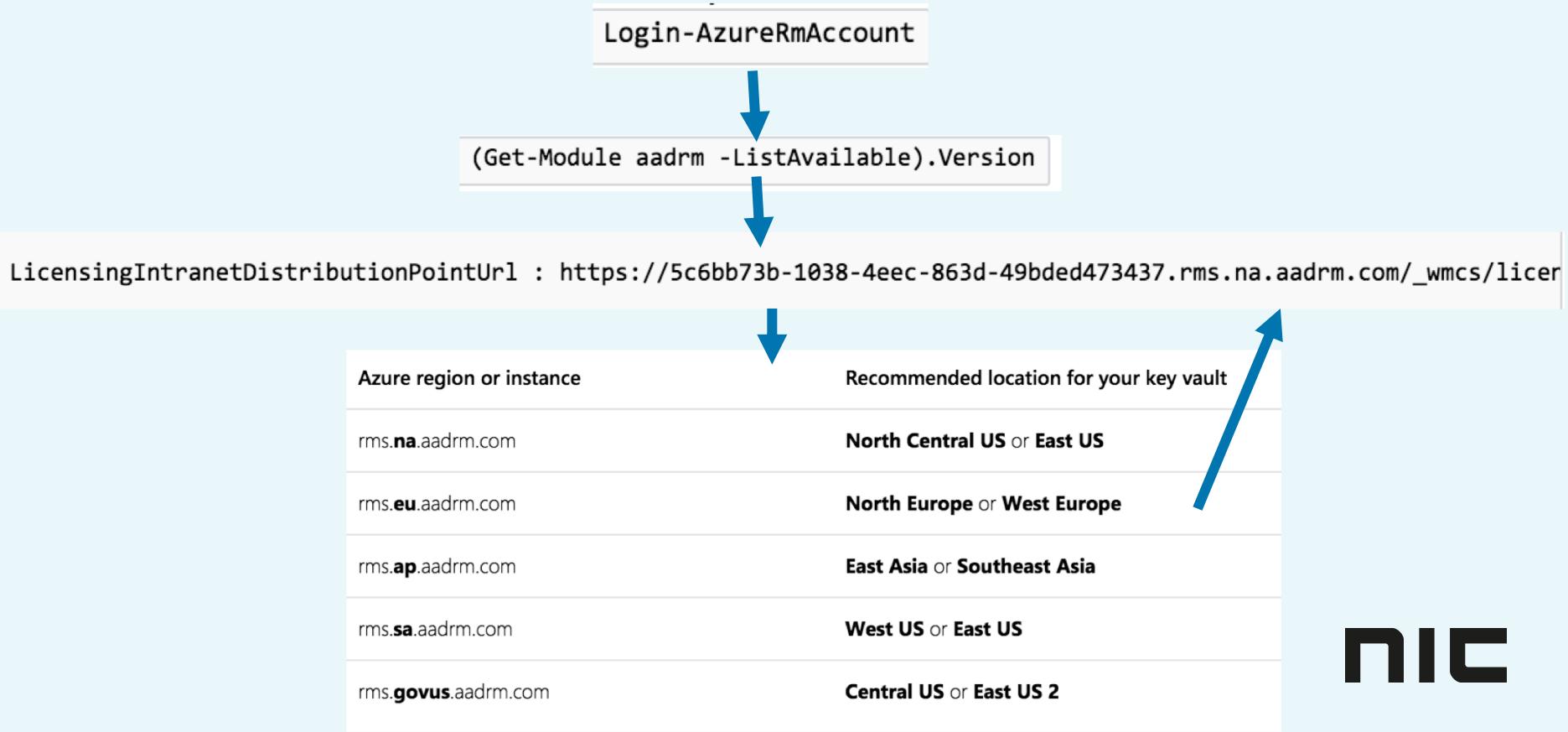
Bring Your Own Key

- 1 You generate your tenant key, keep the master copy, secure it, and back it up.
- 2 Securely transfer your own tenant key to Microsoft HSMs in the Azure Key Vault region or instance that you choose.
- 3 Your key stays protected by Azure Key Vault; Microsoft (and people on the Internet) cannot see your tenant key in the cloud.



- 4 You authorize your Azure RMS tenant to use the key.
- 5 Azure RMS can use your key to authorize users to open your documents.
- 6 Microsoft can replicate your tenant key across a controlled set of HSMs for scale or disaster recovery (within region or instance), but cannot export it.
- 7 Azure Key Vault and Azure RMS provides logging information to show how your tenant key and protected data are used.

Bring Your Own Key (BYOK)



Bring Your Own Key (BYOK) - Setup

- Use the Azure Key Vault documentation to create a key vault and the key that you want to use for Azure Information Protection
- Make sure that the key length is **2048** bits (recommended) or **1024** bit
 - Other key lengths are not supported by Azure Information Protection
- A key that is stored in Key Vault has a unique key ID
- This ID is a URL that contains the name of the key vault, the keys container, the name of the key, and the key version
- For example: <https://contosorms-kv.vault.azure.net/keys/contosorms-byok/aaaabbbbcccc111122223333>
- You must configure Azure Information Protection to use this key, by specifying its Key Vault URL

The Next Step: Authorising BYOK

Set-AzureRmKeyVaultAccessPolicy

```
PS C:\> Set-AzureRmKeyVaultAccessPolicy -VaultName 'Contoso03Vault' -UserPrincipalName  
'PattiFuller@contoso.com' -PermissionsToKeys create,import,delete,list -PermissionsToSecrets  
'set,delete'  
PS C:\> Set-AzureRmKeyVaultAccessPolicy -VaultName 'Contoso03Vault' -UserPrincipalName  
'PattiFuller@contoso.com' -PermissionsToSecrets set,delete,get -PassThru  
PS C:\> Set-AzureRmKeyVaultAccessPolicy -VaultName 'Contoso03Vault' -UserPrincipalName  
'PattiFuller@contoso.com' -PermissionsToKeys @() -PassThru
```

```
Set-AzureRmKeyVaultAccessPolicy -VaultName 'ContosoRMS-kv' -ResourceGroupName 'ContosoRMS-byok-rg' -  
ServicePrincipalName 00000012-0000-0000-c000-000000000000 -PermissionsToKeys decrypt,sign,get
```

Connect-AadrmService

```
Use-AadrmKeyVaultKey -KeyVaultKeyUrl "https://contosorms-kv.vault.azure.net/keys/contosorms-  
byok/aaaabbbbcccc111122223333"
```



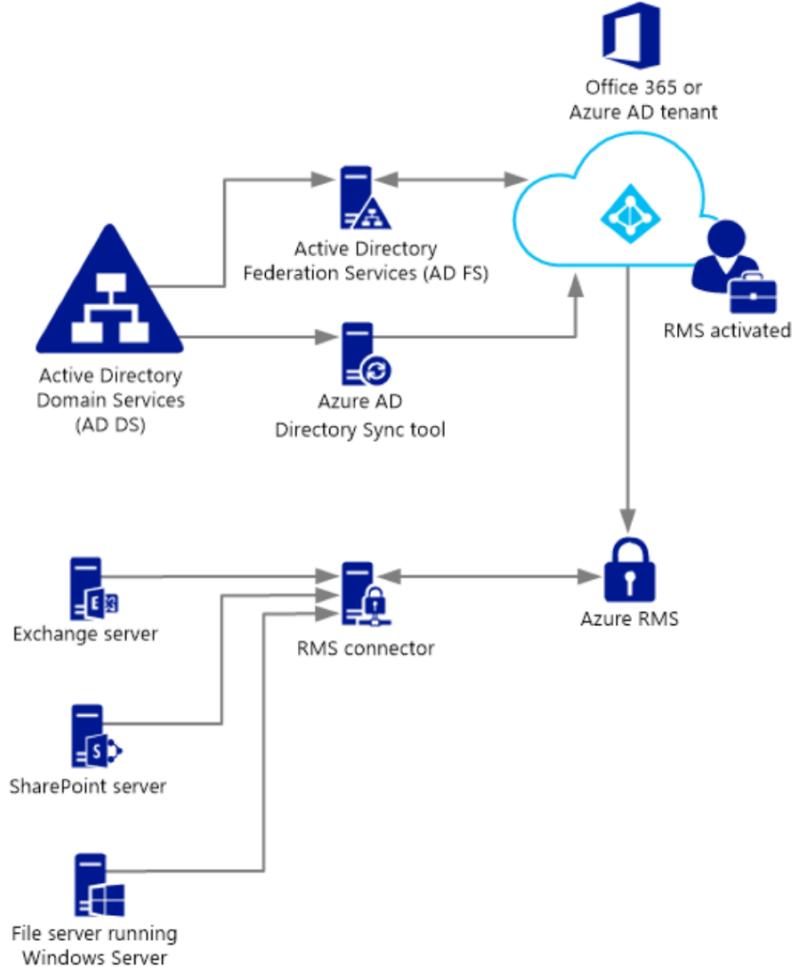
Authorising BYOK: Important!

```
Use-AadrmKeyVaultKey -KeyVaultKeyUrl "https://contosorms-kv.vault.azure.net/keys/contosorms-byok/aaaabbbbcccc111122223333"
```

- In the example, "**aaaabbbbcccc111122223333**" is the version of the key to use
- If you do not specify the version, the current version of the key is used without warning and the command appears to work
- However, if your key in Key Vault is later updated (renewed), the ARM service will stop working for your tenant, even if you run the **Use-AadrmKeyVaultKey** command again
- Make sure that you specify the key version, in addition to the key name when you run this command
- You can use the Azure Key Vault cmd, **Get-AzureKeyVaultKey**, to get the version number of the current key. For example `Get-AzureKeyVaultKey -VaultName 'contosorms-kv' -KeyName 'contosorms-byok'`
- Finally, if ARM service is activated, run **Set-AadrmKeyProperties** to tell AIP to use this key as the active tenant key for the Azure Rights Management service. If you do not do this step, Azure Information Protection will continue to use the default Microsoft-managed key, that was automatically created for your tenant.

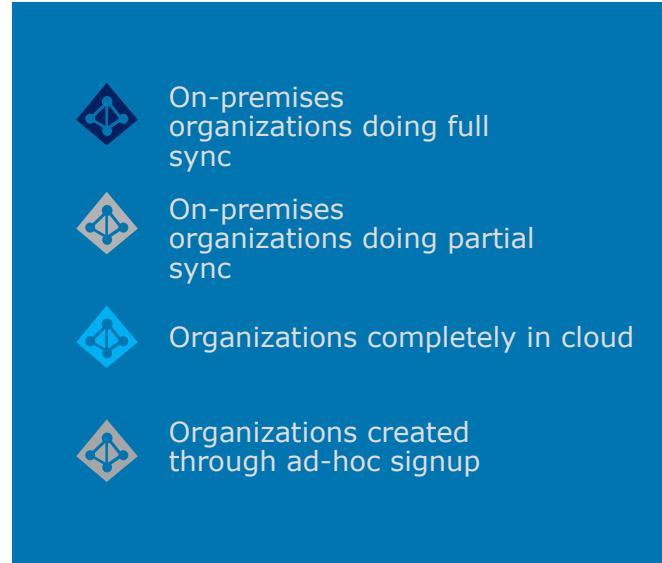
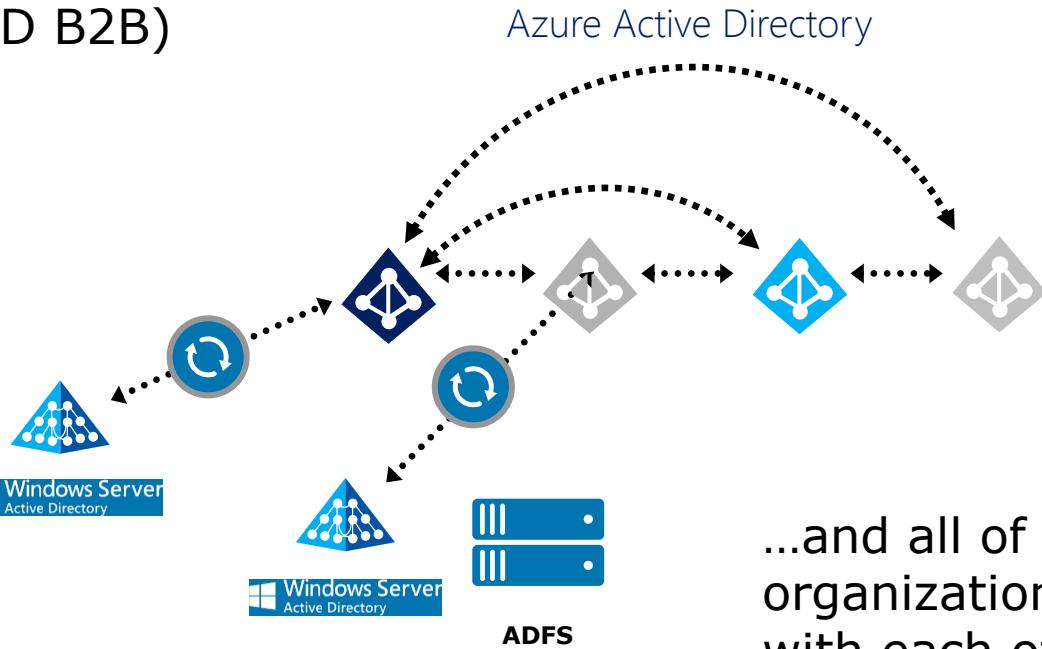
Host Your Own Key (HYOK)

- This relay component functions between on-prem servers (Exchange, SP, FCI)
- Installed on prem on Windows Servers or Virtual Machines
- Supports Hybrid scenarios both (on-prem and on-line mailboxes)



How AIP influences B2B Sharing

Using Azure AD for authentication
Via E-mail or Templates
with external users
(AD B2B)



...and all of these
organizations can interact
with each other.

Auditing / SEIM

Event Viewer

File Action View Help

Custom Views

Windows Logs

- Application
- Security
- Setup
- System
- Forwarded Events

Applications and Services Logs

- Azure Information Protection
- Hardware Events
- Internet Explorer
- Key Management Service

Microsoft

- Microsoft Office Alerts
- Windows PowerShell

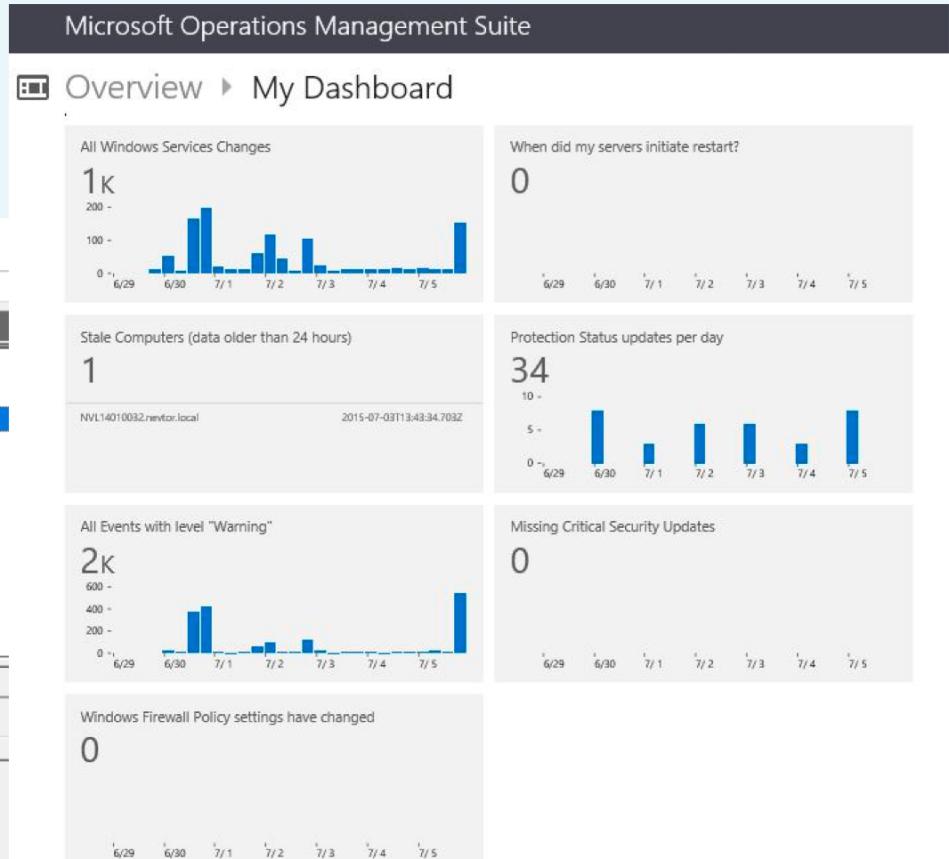
Subscriptions

Azure Information Protection Number of events: 15

Level	Date and Time
Information	18/01/2017 10:58:36
Information	18/01/2017 10:58:30
Information	18/01/2017 10:56:25
Information	18/01/2017 10:55:33
Information	18/01/2017 10:50:22
Information	18/01/2017 09:41:16
Information	18/01/2017 09:37:00
Information	18/01/2017 09:28:06
Information	17/01/2017 15:39:01
Information	17/01/2017 15:38:36
Information	17/01/2017 15:38:32

Event 102, Azure Information Protection

General	Details
Client Version: 1.3.98.0	
User Name: HANDD1\janny	
File Location: RE: HANDD.msg	
Action: Set Label (lower)	
Action Source: Manual	
Label Before Action: Confidential	
Label After Action: Public	
Protection Before Action: Unprotected	
Protection After Action: Unprotected	



Azure Incoming Features

Incoming! The Microsoft Attack Simulator

Office 365 | Security & Compliance

The screenshot shows the Microsoft Attack Simulator interface within the Office 365 Security & Compliance center. On the left, a sidebar lists various security features: Home, Alerts, Classifications, Data loss prevention, Data governance, Threat management (selected), Dashboard, Threat explorer, Attack simulator (highlighted with a red box), Incidents, Campaigns, Mail filtering, Anti-malware, Dkim, Safe attachments, Safe links, and Quarantine.

The main area displays three attack scenarios:

- Display Name - Spear Phishing Account Breach**
Phishing is a generic term for a broad suite of attacks classed as a social engineering style attack. This test is focused on Spear Phishing – a more targeted attack, aimed at a specific group of individuals or an organization. Typically, a customized attack with some reconnaissance performed and using a Display Name that will generate trust in the recipient.
Test bar: Attack Completed [View Report](#) [Schedule Attack](#) [Attack Details](#)
- Brute Force Password Attack Account Breach**
A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate many consecutive guesses as to the value of the desired data.
Test bar: Attack Completed [View Report](#) [Schedule Attack](#) [Attack Details](#)
- Password Spray Attack Account Breach**

At the top right, a callout box says "Simulate attacks to test your defenses" with the subtext "Run realistic phishing, spear phishing and other attack scenarios to identify and find vulnerable users before it impacts your bottom line."



Incoming! Microsoft Compliance Manager

The screenshot shows the Microsoft Compliance Manager interface on a browser window titled "Service Trust Preview" at "localhost:3000/RiskAndCompliance#". The top navigation bar includes links for Microsoft, Service Trust, Documents, Compliance Manager (which is underlined), and Settings. A user account "user1@servicetrustint.onmicrosoft.com" is also visible.

The main area is titled "Compliance Manager" and features several cards representing different compliance frameworks:

- Office 365 GDPR**: Status: Pending (indicated by a blue circle with a white question mark). Actions button. Created 9/14/2017, Modified 9/14/2017. Customer Controls: 90 of 159. Microsoft Controls: 140 of 140.
- Azure ISO 27001:2013 and DPA**: Status: Pending (blue circle with a white question mark). Actions button. Created 9/14/2017, Modified 9/14/2017. Customer Controls: 150 of 229. Microsoft Controls: 359 of 359.
- Dynamics 365 ISO 27001:2013**: Status: Passed (green circle with a checkmark). Actions button. Created 9/14/2017, Modified 9/14/2017. Customer Controls: 174 of 174. Microsoft Controls: 269 of 269.
- Azure FedRAMP Rev4**: Status: Failed (red circle with a minus sign). Actions button. Created 9/14/2017, Modified 9/14/2017. Customer Controls: 8 of 365. Microsoft Controls: 695 of 695.
- Office 365 ISO 27018:2014 and FFIEC**: Status: Pending (blue circle with a white question mark). Actions button. Created 9/14/2017, Modified 9/14/2017. Customer Controls: 5 of 109. Microsoft Controls: 271 of 271.
- Dynamics 365 FFIEC**: Status: Pending (blue circle with a white question mark). Actions button. Created 9/14/2017, Modified 9/14/2017. Customer Controls: 5 of 97. Microsoft Controls: 230 of 230.

Below the cards are buttons for "Review Frameworks", "Action Items", "Check Service Compliance", "Show Archived" (unchecked), "+ Add Framework", and "Filter Products".



Session Review

- Cybercrime Motivation Circa 2018
- Data Leakage: The great security dilemma
- Introducing Azure Information protection
- File Classification Explained
- AIP / ADRMS Architecture
- Rights Management Explained
- The Crypto Secret Recipe
- BYOK & HYOK Solutions
- Review

Andy Malone

(Scotland, UK)

- Thanks for Attending
- Meet the Author event @NIC
- Purchase your signed copy at the Glasspaper Booth
- Author off the Sc-Fi Thrillers
- “The Seventh Day” & Shadows Rising”



Resources

Slides and demos from the conference will be available at
github.com/nordicinfrastructureconference/2018 (bit.ly/2y7JhA3)