NIC

Future Edition

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 Shadows Rising is a race against time thriller, packed with rich historical references entwined into a tense story that will leave you breathless and on the edge of your seat ...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

DARK NEBULA PUBLISHING

Tinker, Tailor, Hacker, Spy!

Azure Information Protection inside out!

Andy Malone

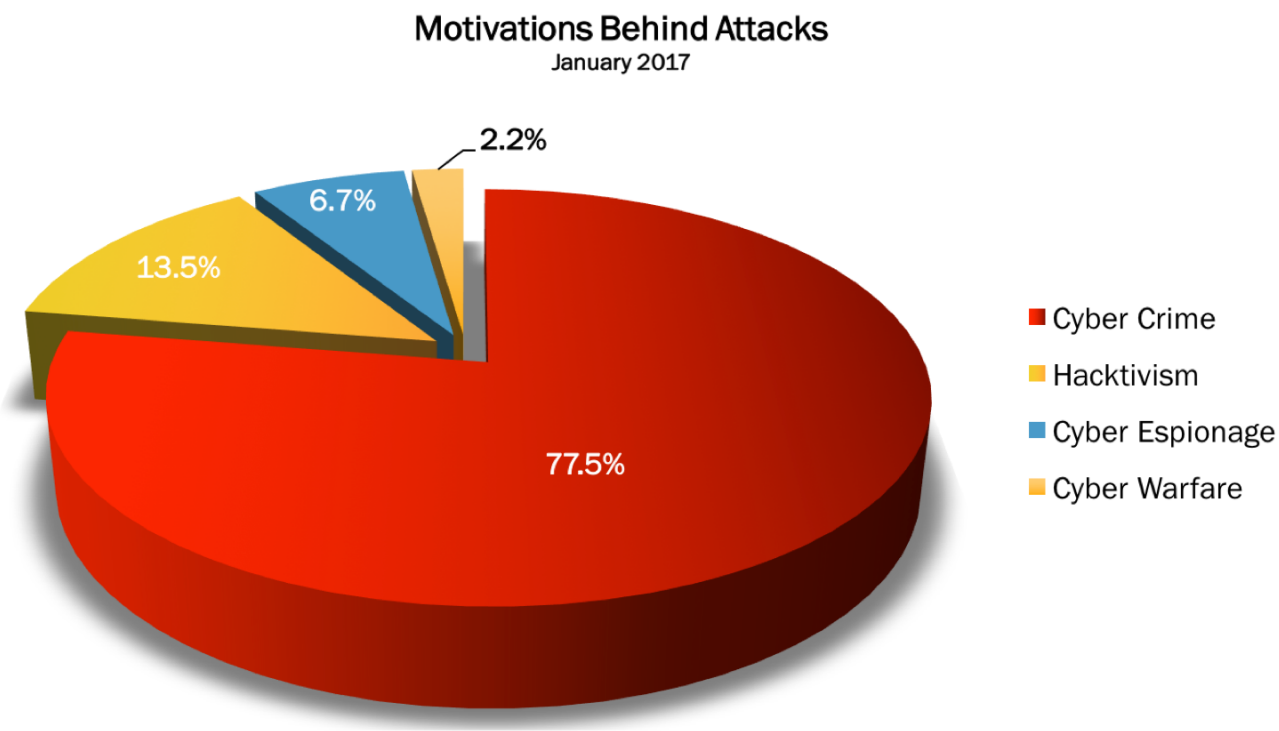
(Scotland, UK)

- 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



hackmageddon.com

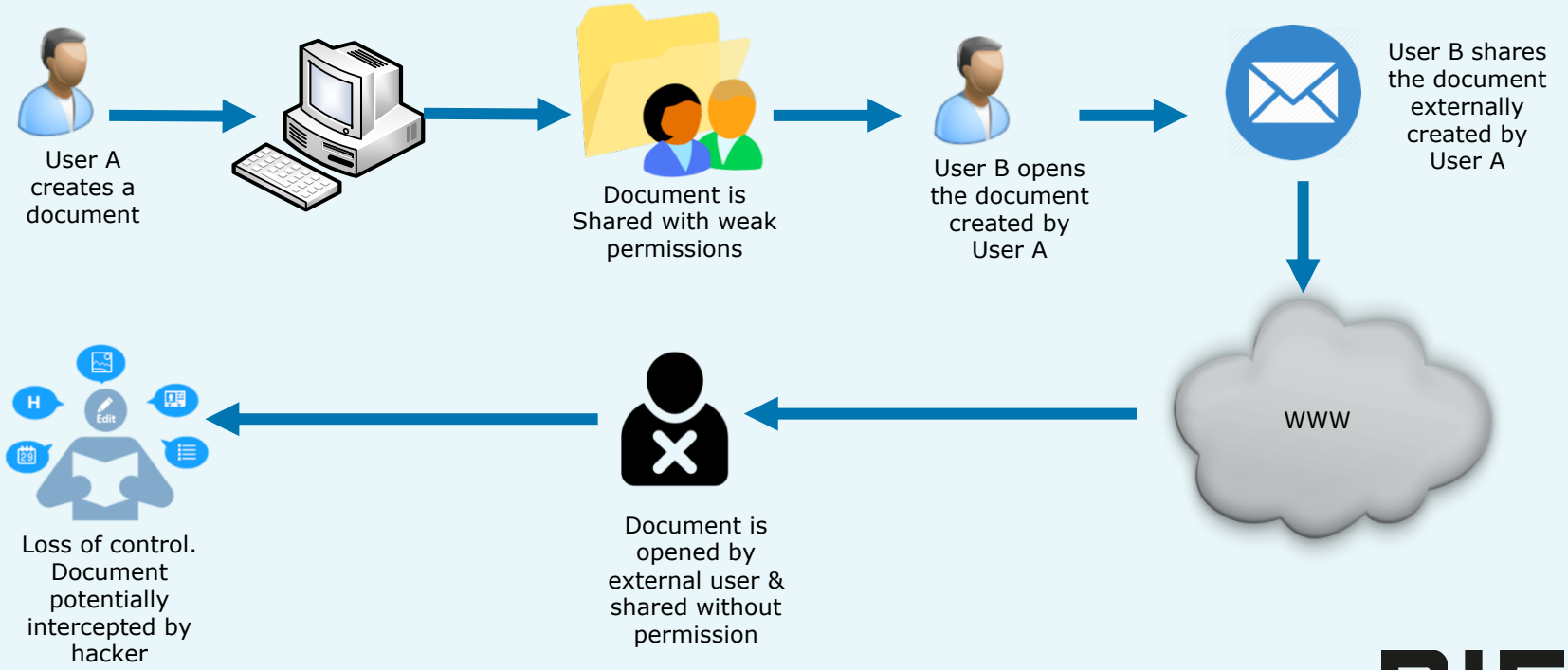
Fraud targeting senior executives is a "key threat", said Europol

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.

The Problem: Traditional File Sharing



The Problem: Traditional File Sharing

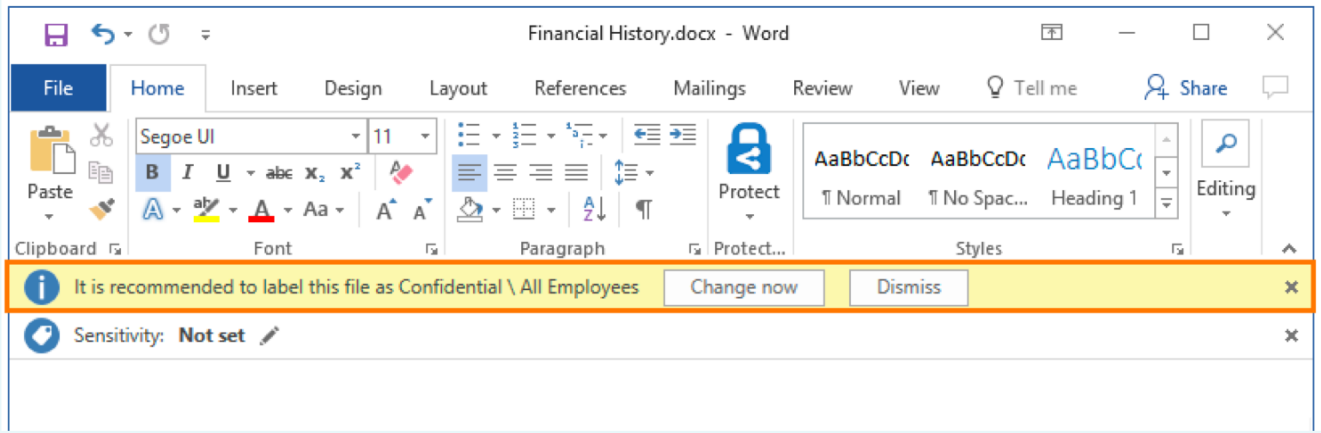
- Prevents Permissions Bleed
- Once data is outside organization, its beyond the realm of your control
- Anyone can plagiarise
- Content easily copied
- Potential Copyright Infringement Issues
- Plausible Deniability Reins
- Lack of Compliance

Demo

FOCA: The Dangers of poor file security

The Solution: Azure Information Protection?

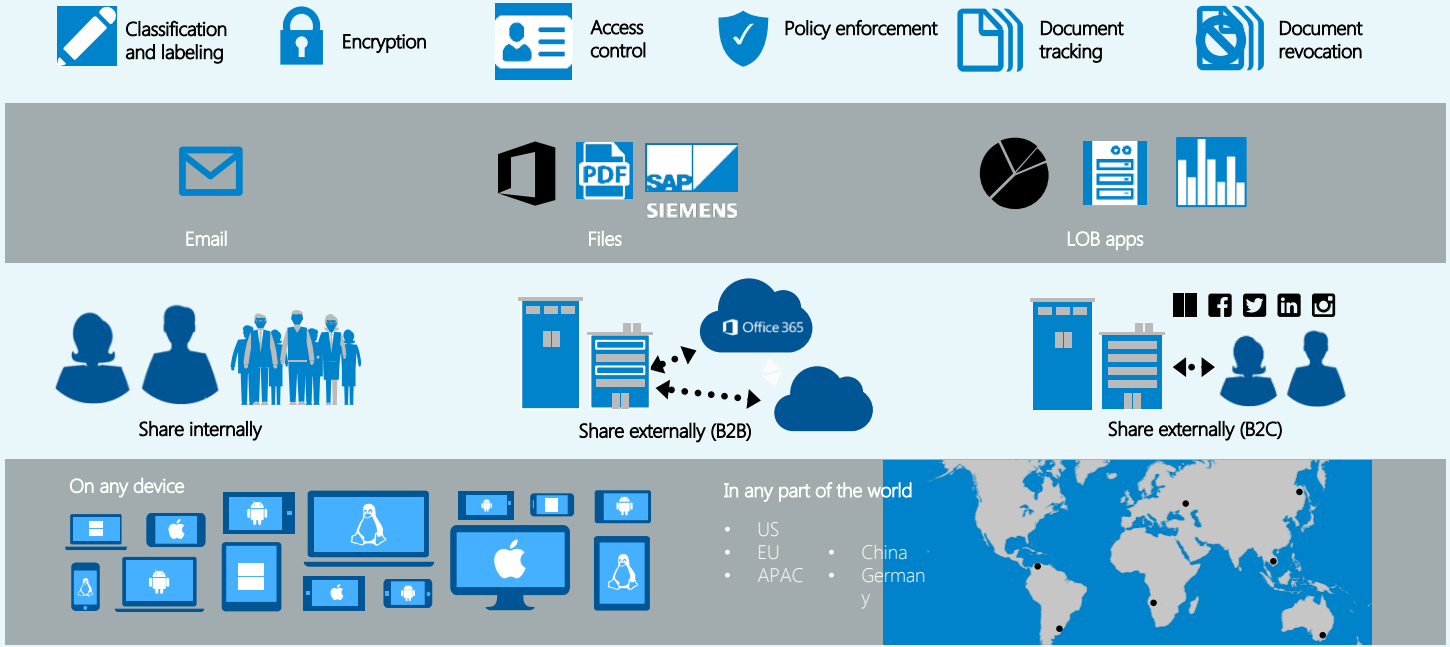
- Azure Information Protection is Microsoft's cloud-based solution that helps an organization to classify, label, and protect its documents and emails.
- This can be done automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations.



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



Azure information Protection Components

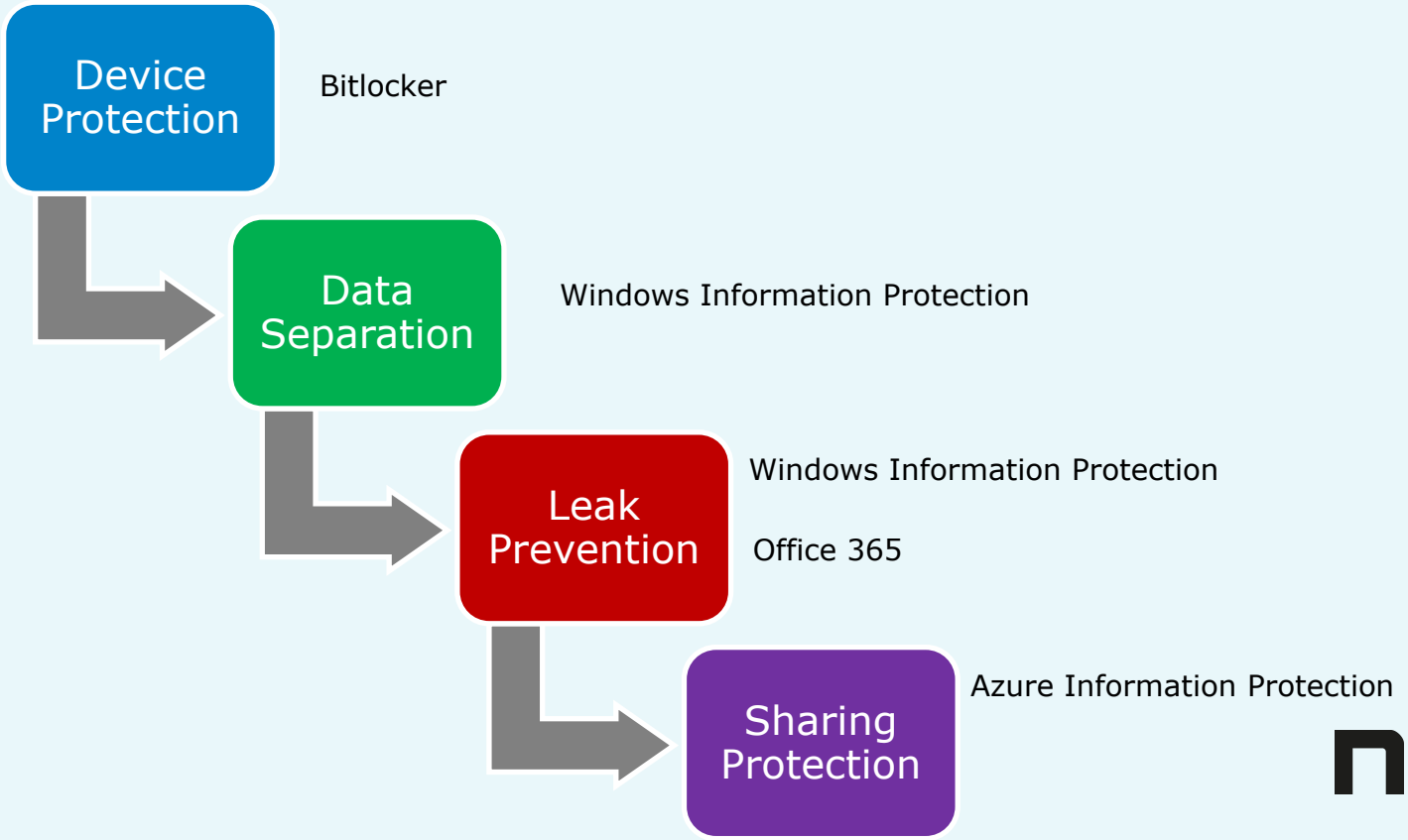
- Identity & Authentication Services provided by Microsoft Azure Active Directory Services

- 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

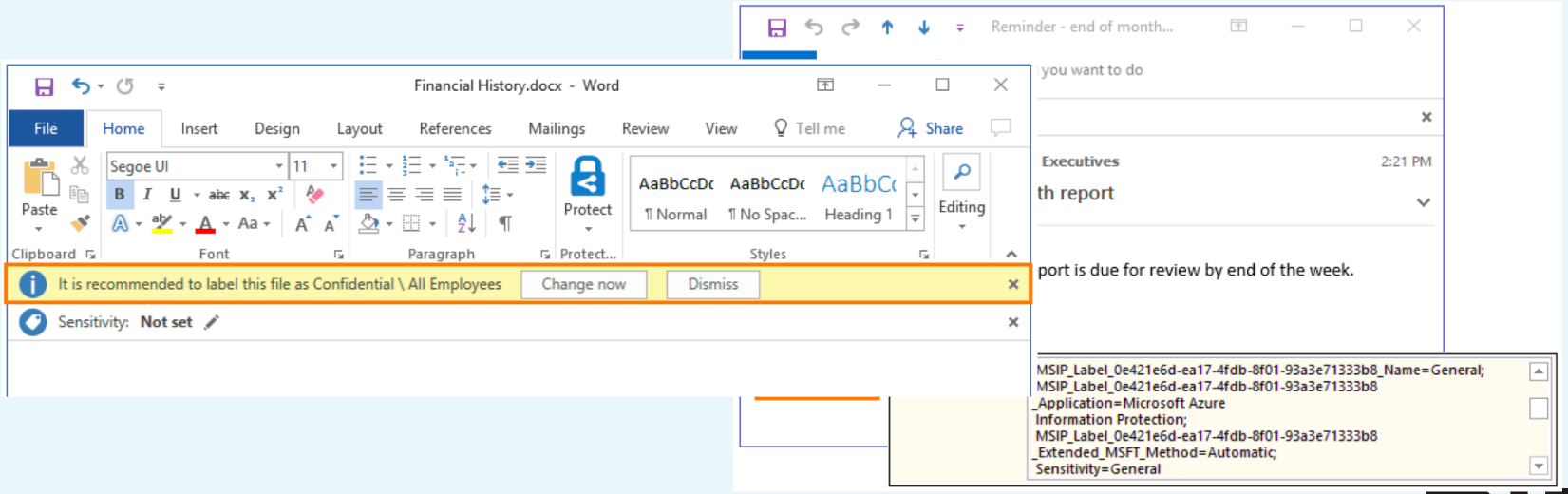
Azure Information Protection Requirements

- **For classification, labelling, and protection**, you must have an Azure Information Protection plan
  - Office 365 “3” plan an 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 ion Azure
- User Accounts must authenticate with a verified UPN
- Apple & Android Apps require certificate-based authentication (CBA)

So How does it Work?
File Classification

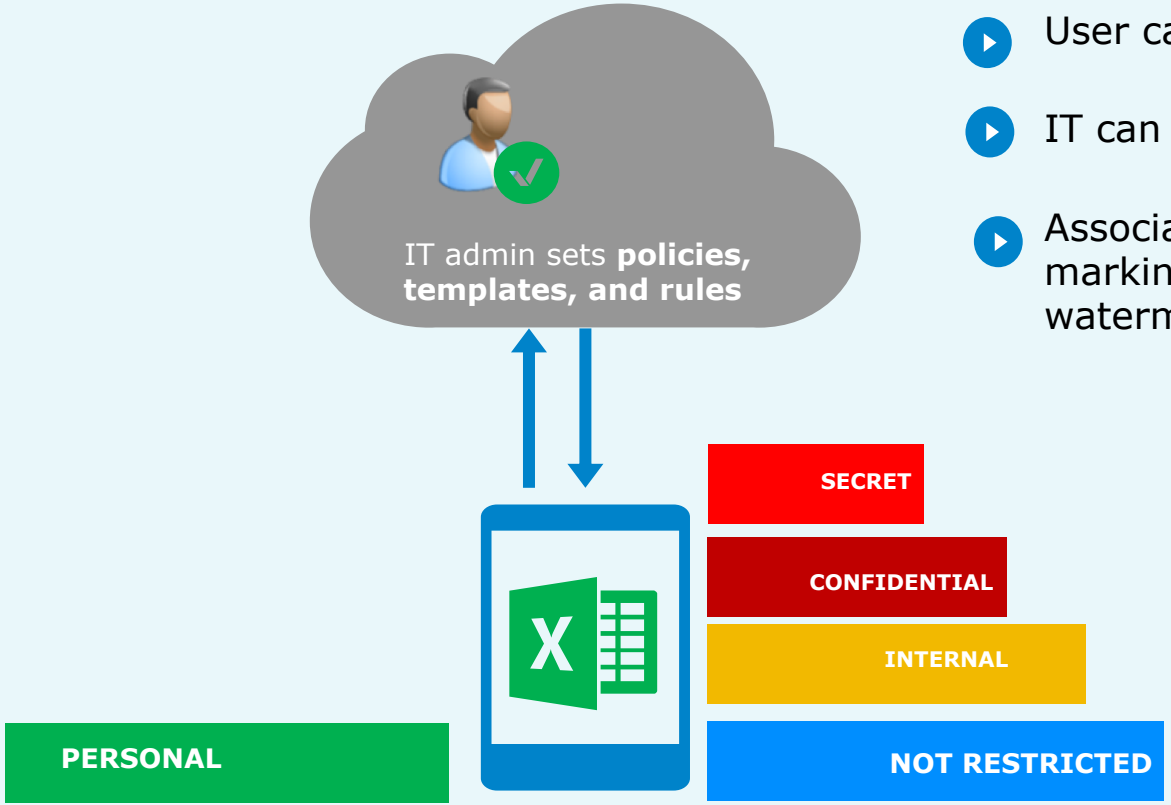
File Classification – What does it do?

- 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

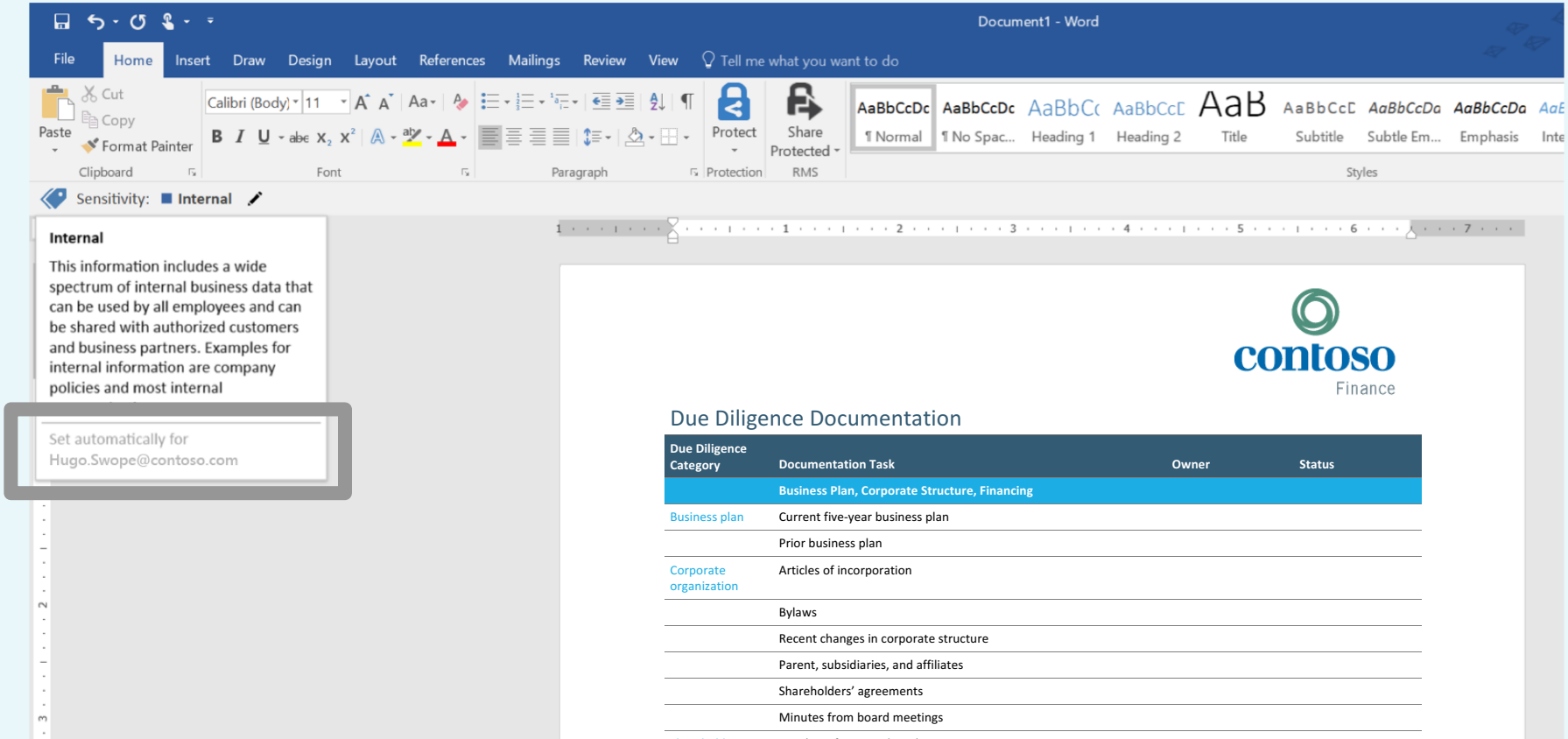
File classification based on sensitivity



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

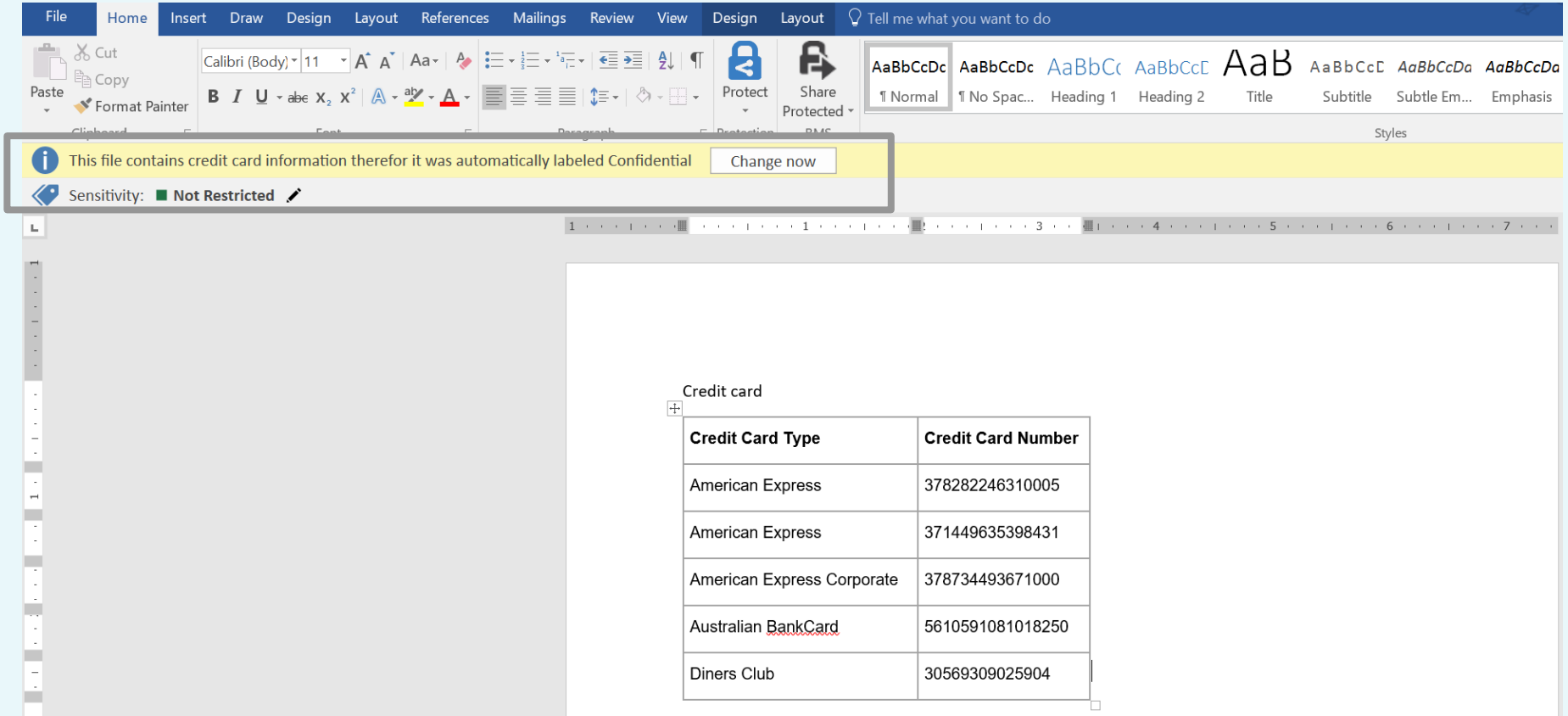
How Classification Works

Automated Classification



How Classification Works

Recommended Classification

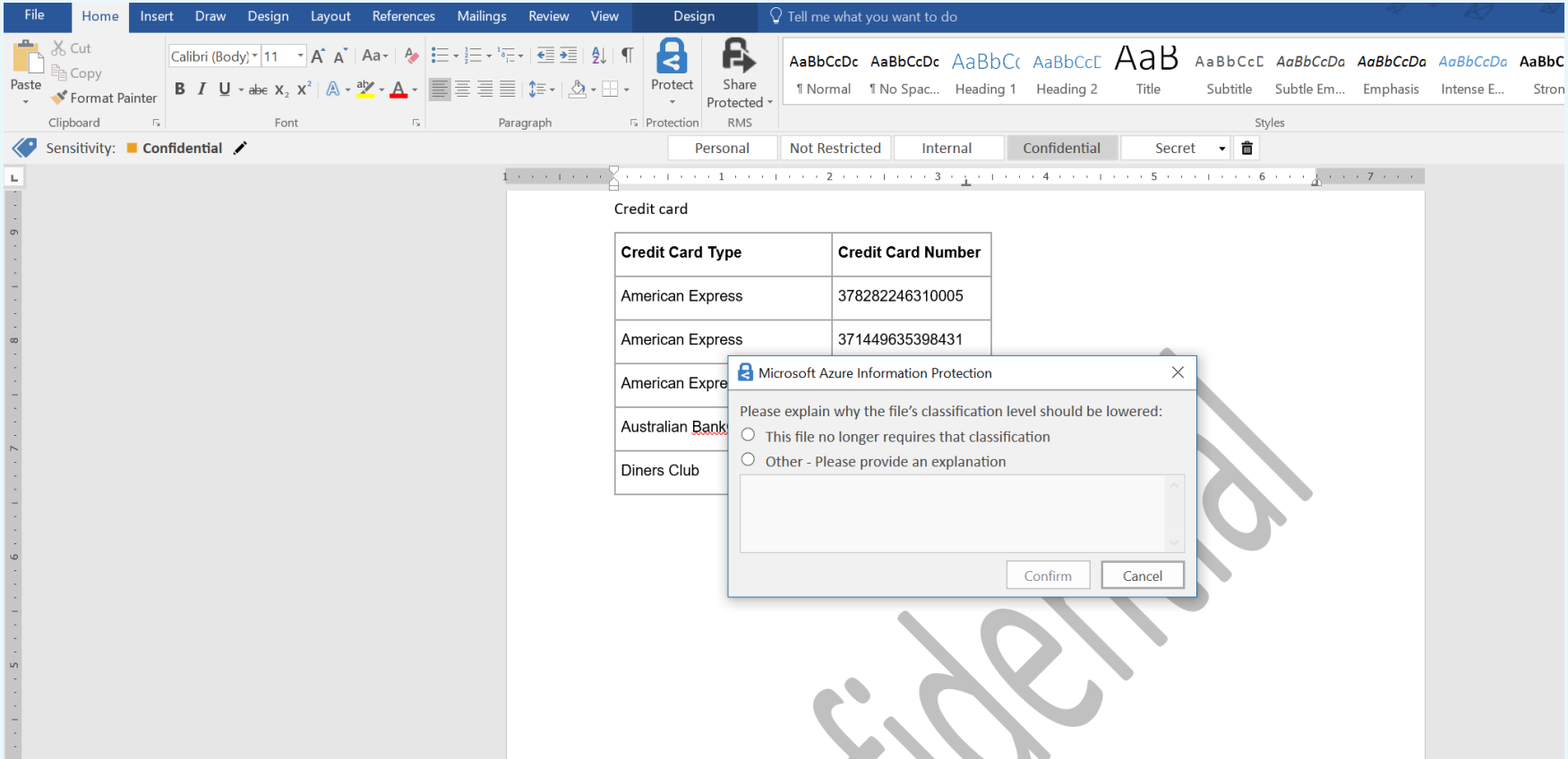


Credit card

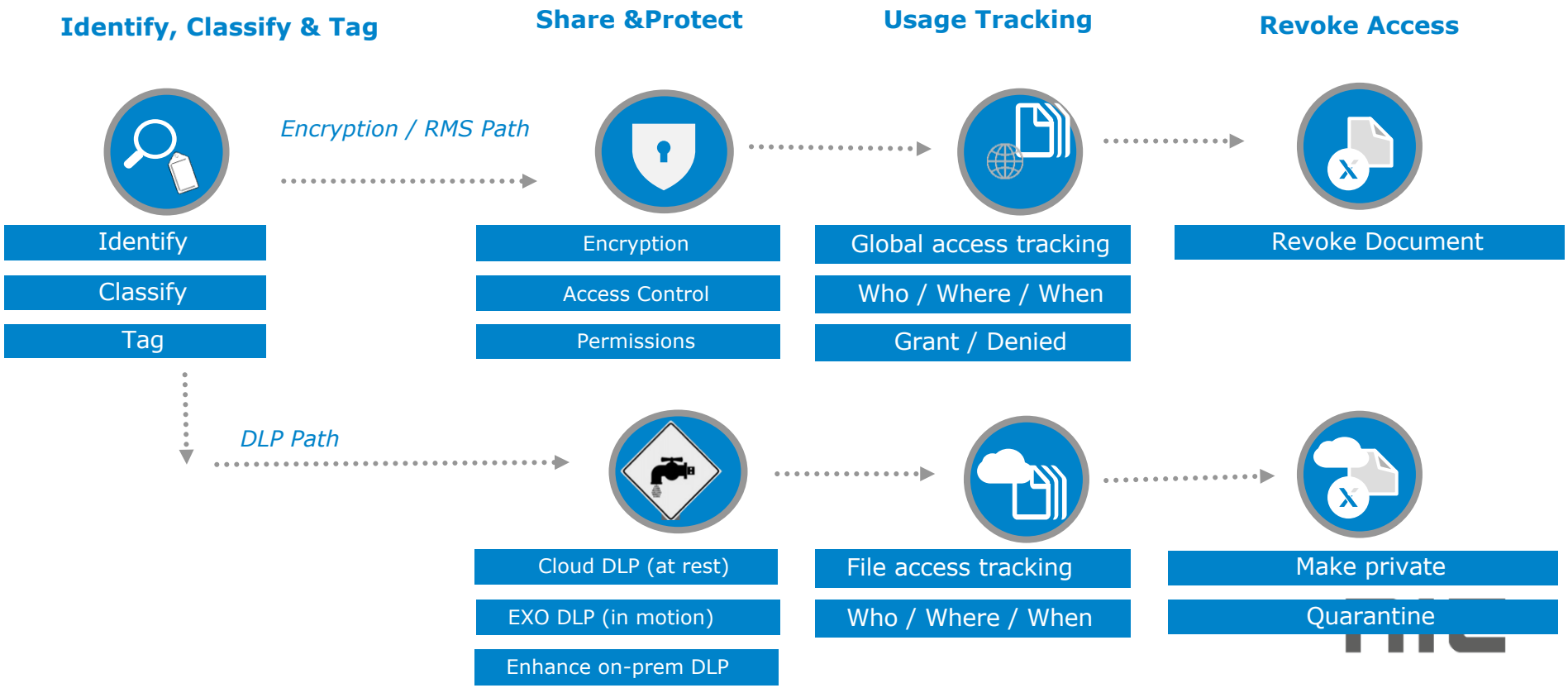
Credit Card Type	Credit Card Number
American Express	378282246310005
American Express	371449635398431
American Express Corporate	378734493671000
Australian BankCard	5610591081018250
Diners Club	30569309025904

How Classification Works

Reclassification & Justification



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**;

Get-AIPFileStatus

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. Tennent Key: Managed by Microsoft
    2. Tennent 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

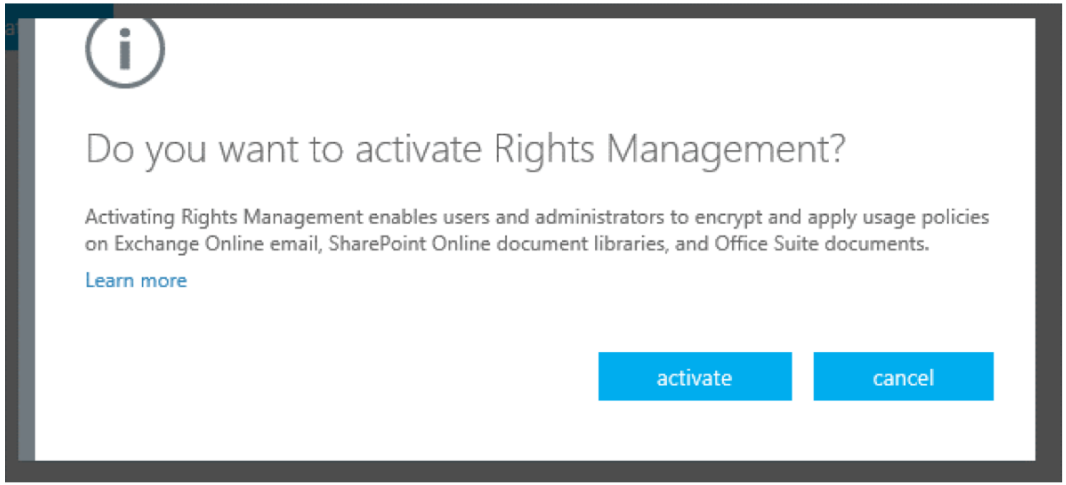
You can configure advanced features for Rights Management using Microsoft Azure.

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



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 cmandlets**

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

- **Connecting to Active Directory Rights Management**

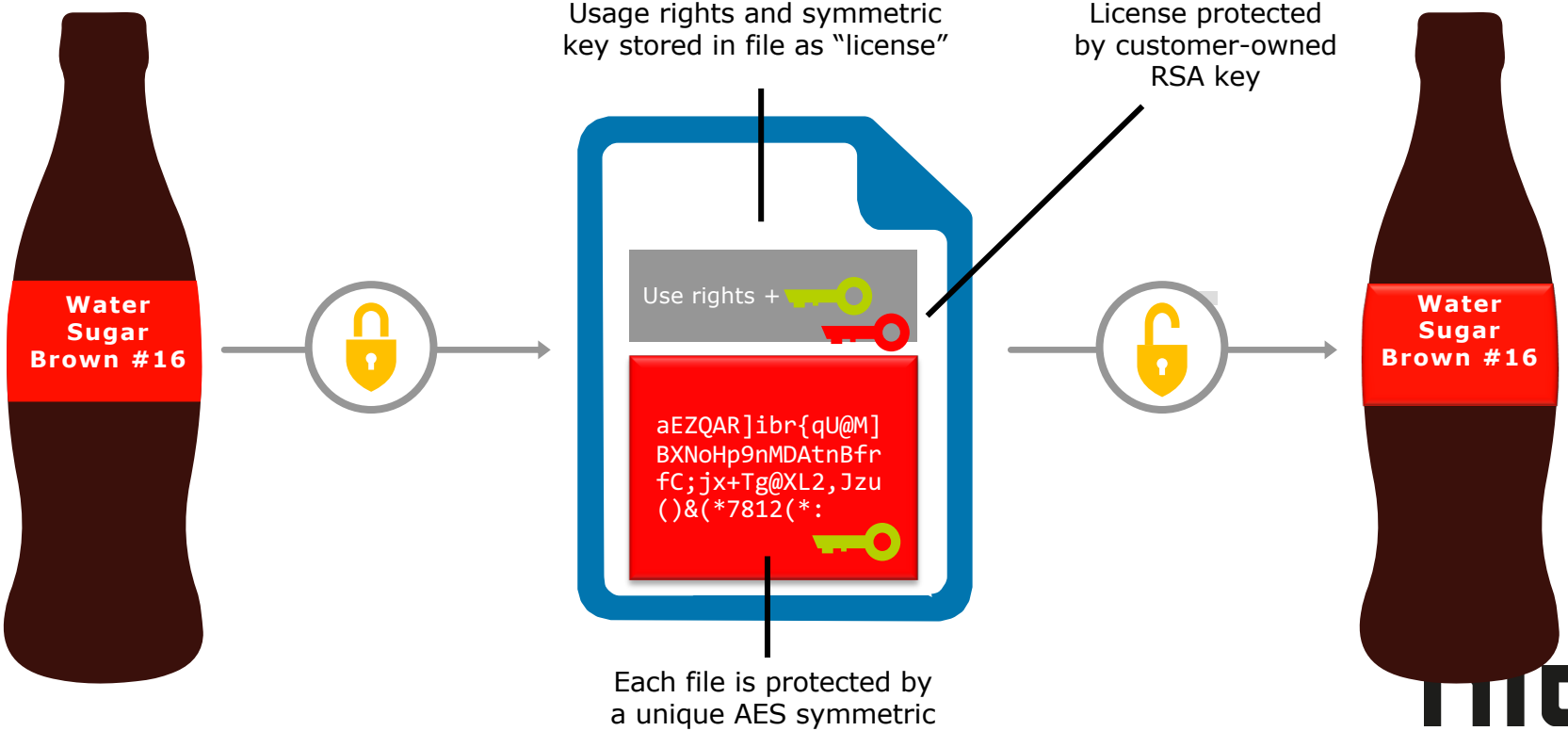
```
PS C:\> Import-Module aadrm
PS C:\> $UserCredential = Get-Credential
PS C:\> Connect-AadrmService -Credential $UserCredential
```

```
Get-Command -Module AADRM
```

```
Get-Help <cmdlet_name>
```

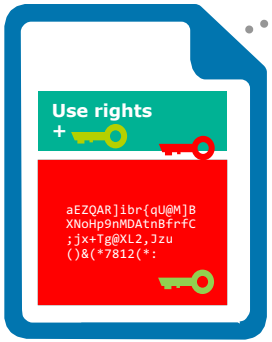
The Secret Cryptographic recipe underneath Azure Information Protection

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

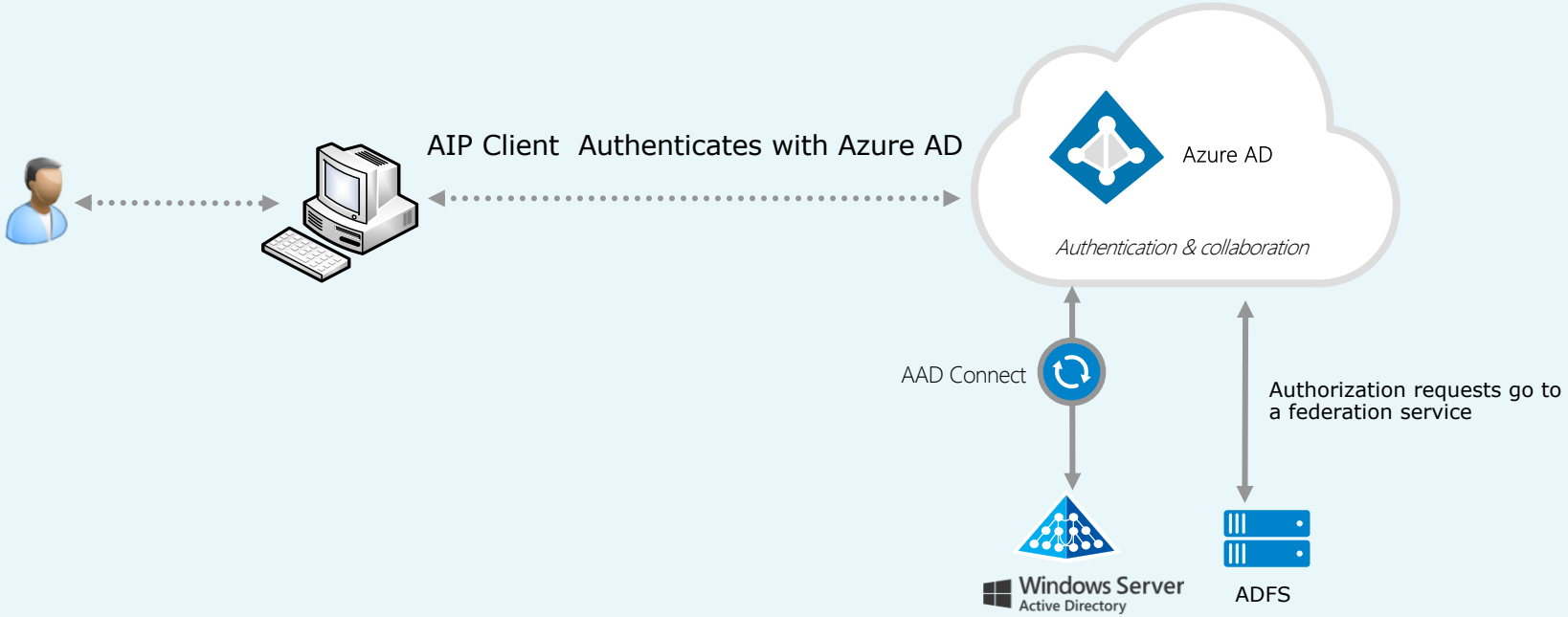
Azure RMS never sees the file content, only the license

Rights Management Active Directory Key Vault

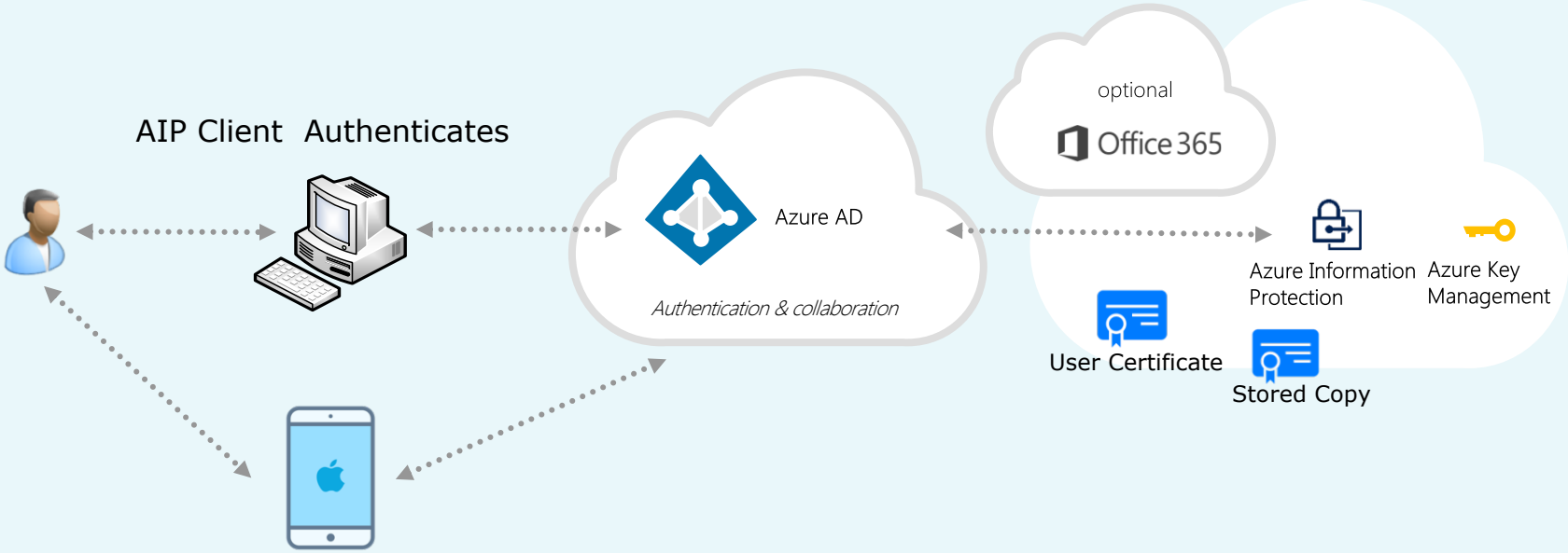
Cryptographic controls used by Azure RMS: Algorithms and key lengths

CRYPTOGRAPHIC CONTROLS	USE IN AZURE RMS
Algorithm: AES Key length: 128 bits and 256 bits [1]	Documentation protection
Algorithm: RSA Key length: 2048 bits	Key protection
SHA-256	Certificate signing

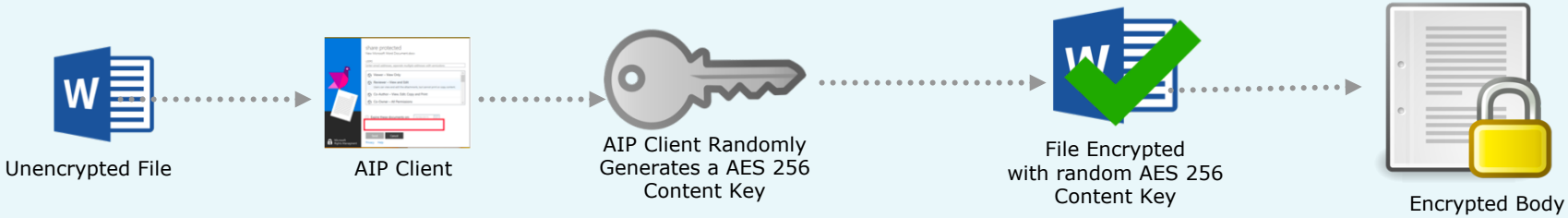
Initialing the User Environment



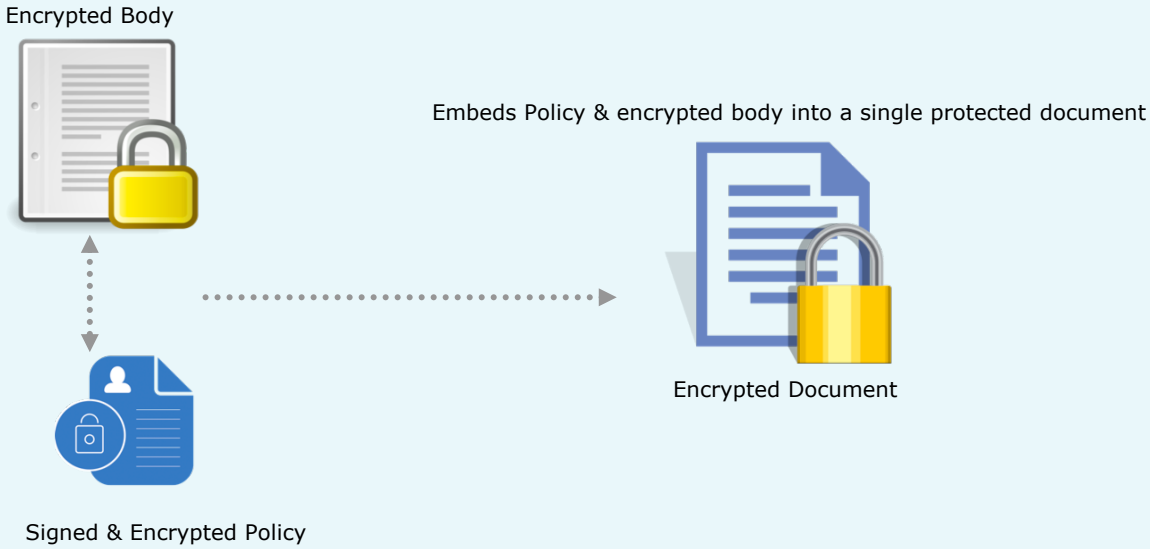
Initialing the User Environment



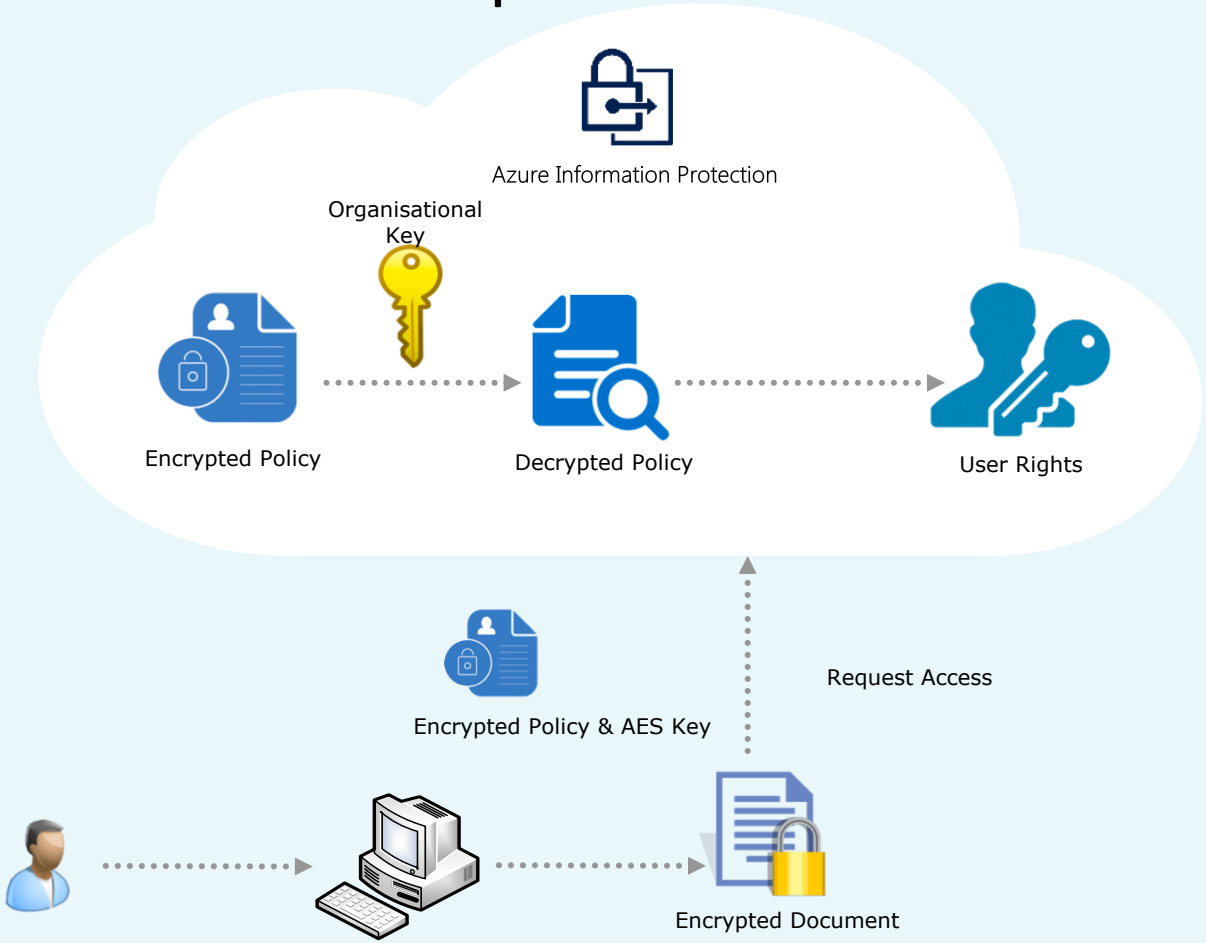
Content Protection



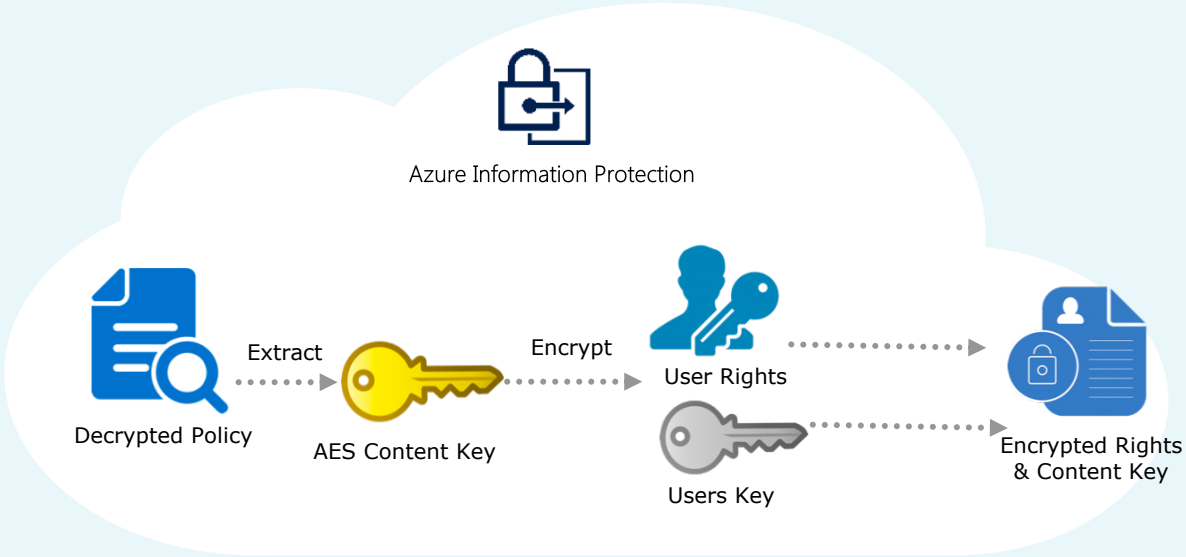
Content Protection



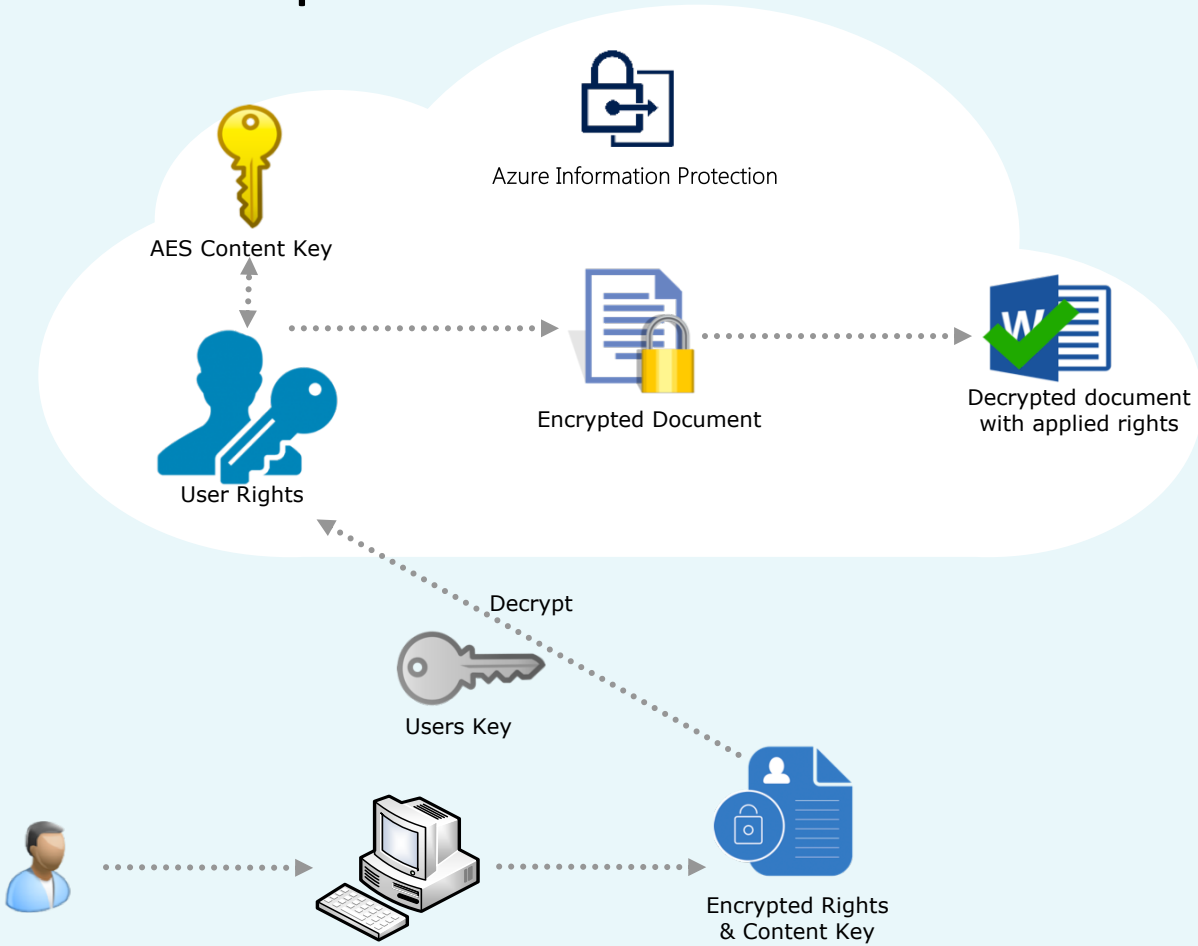
Content Consumption



Content Consumption



Content Consumption



What about mobile & other connectivity options?

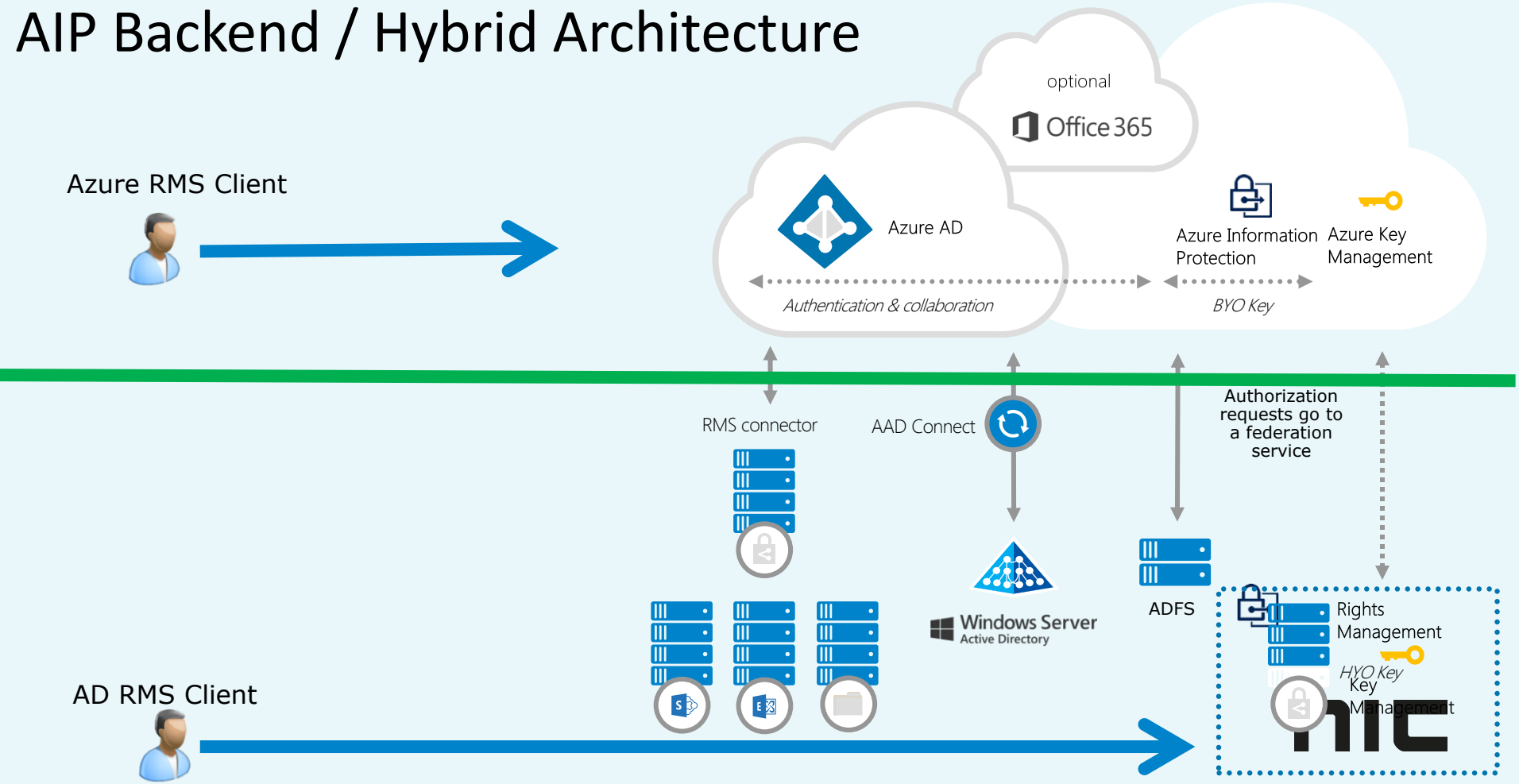
- Mobile devices such as iPhone, Android – No registration process – get publication license and consumption license over TLS
- RMS Connector – Same flow but RMS connector acts as a relay between the on-prem services (e.g. Exchange, SharePoint) and Azure RMS.
- Generic protection (.pfile) – Same flow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

Demo

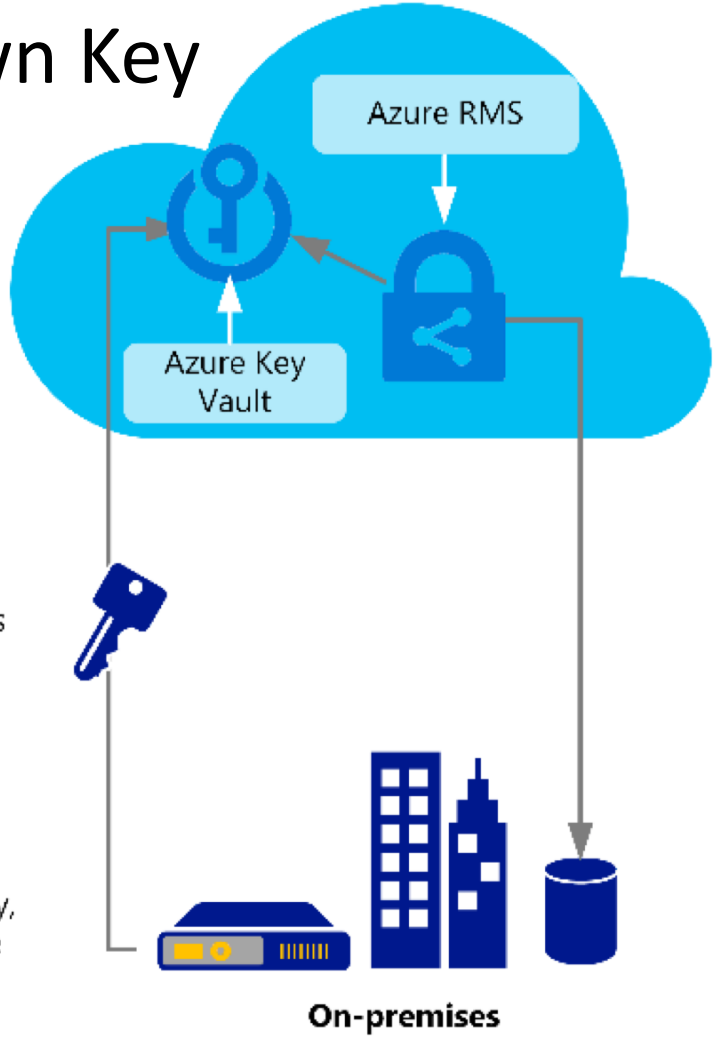
Information Protection / Rights Management In Operation

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

AIP Backend / Hybrid Architecture



Bring Your Own Key



3. Your key stays protected by Azure Key Vault; Microsoft (and people on the Internet) cannot see your tenant key in the cloud.

2. Securely transfer your own tenant key to Microsoft HSMs in the Azure Key Vault region or instance that you choose.

1. You generate your tenant key, keep the master copy, secure it, and back it up.

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)

```
Login-AzureRmAccount
```

```
(Get-Module aadrm -ListAvailable).Version
```

```
LicensingIntranetDistributionPointUrl : https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/_wmcs/licer
```

Azure region or instance	Recommended location for your key vault
rms.**na**.aadrm.com	**North Central US** or **East US**
rms.**eu**.aadrm.com	**North Europe** or **West Europe**
rms.**ap**.aadrm.com	**East Asia** or **Southeast Asia**
rms.**sa**.aadrm.com	**West US** or **East US**
rms.**govus**.aadrm.com	**Central US** or **East US 2**

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"
```

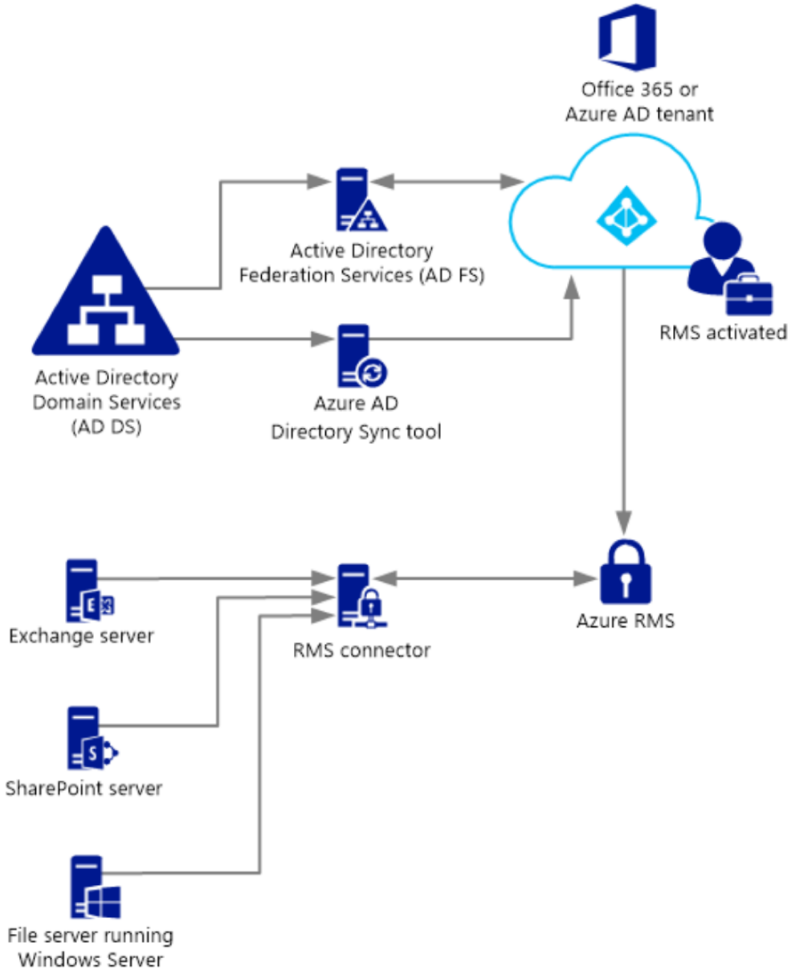
- In the example, "**aaaabbbbcccc111122223333**" is the version of the key to use
- If you do not specify the version, the current version of the key is used without warning and the command appears to work
- **However**, if your key in Key Vault is later updated (renewed), the ARM service will stop working 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)

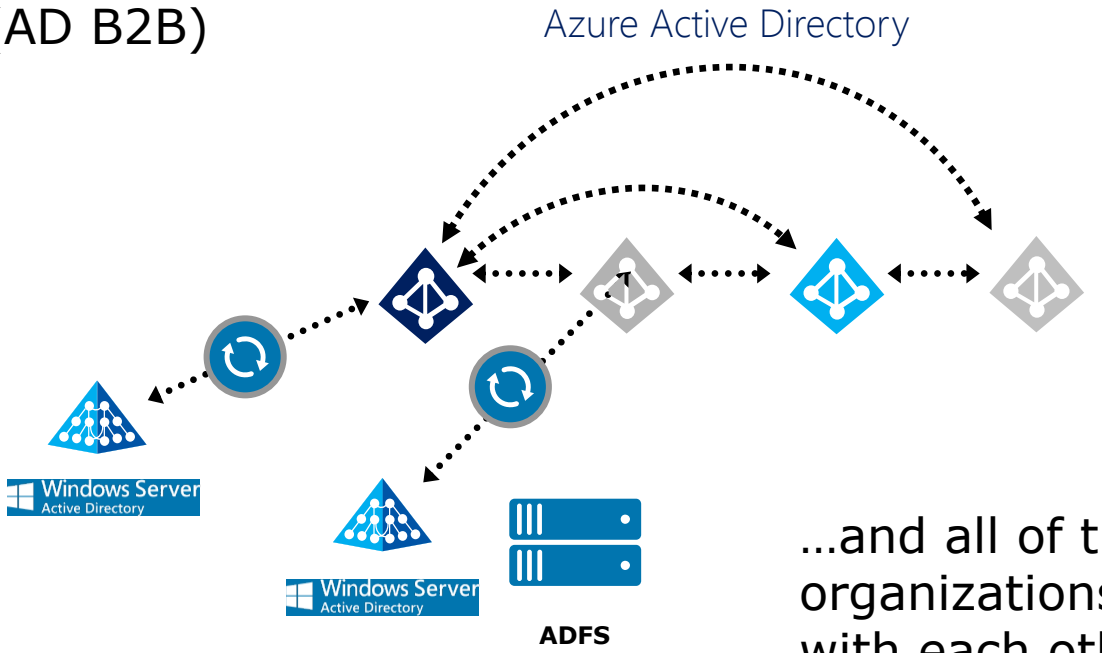
- This relay component functions between on-prem servers (Exchange, SP, FCI)
- Installed on prem on Windows Servers or Virtual Machines
- Supports Hybrid scenarios both (on-prem and on-line mailboxes)



https://docs.microsoft.com/en-us/azure/key-vault/key-vault-hsm-protected-keys

How AIP influences B2B Sharing

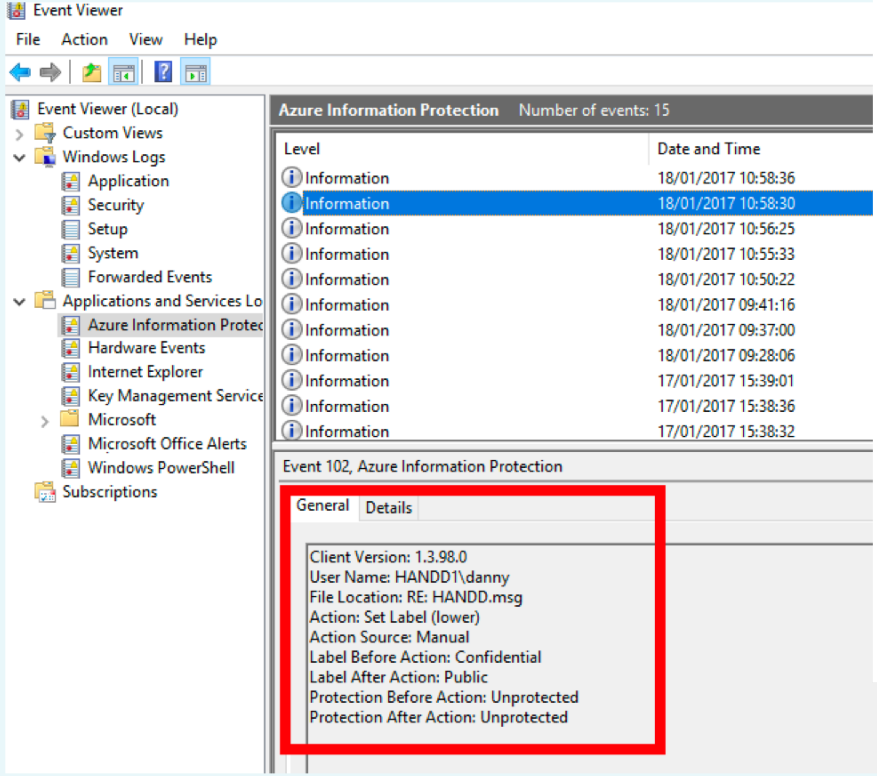
Using Azure AD for authentication
Via E-mail or Templates
with external users
(AD B2B)

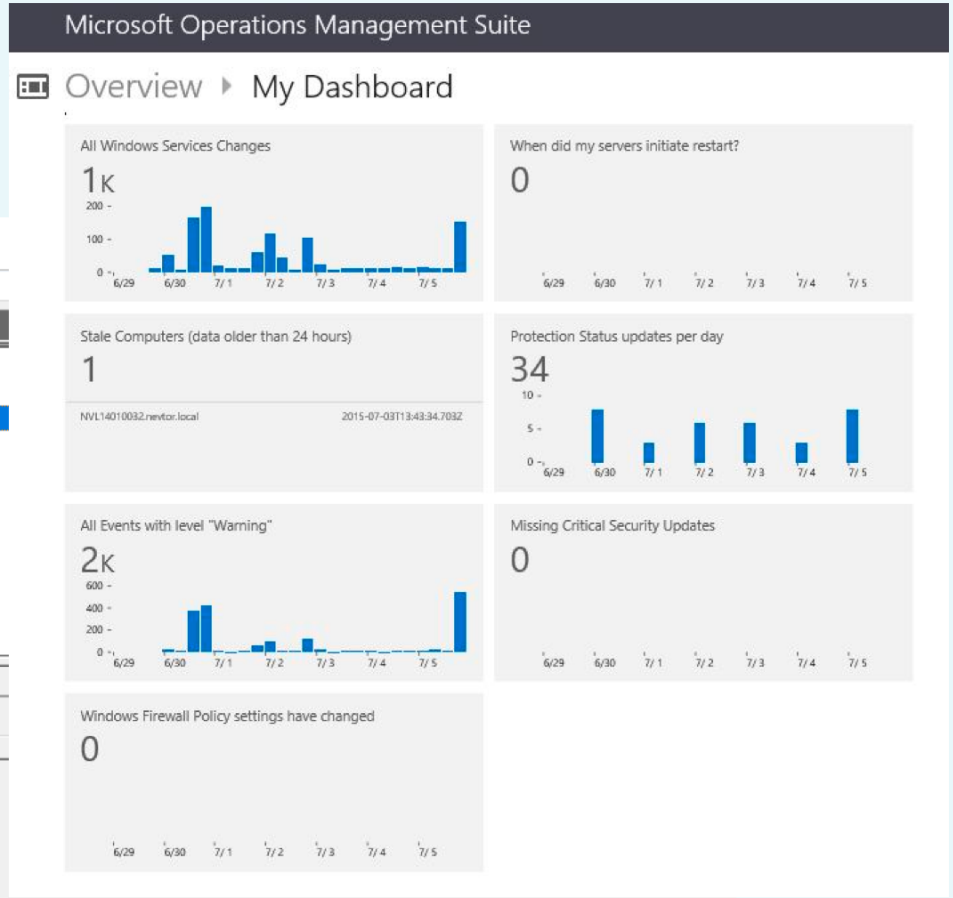


- On-premises organizations doing full sync
- On-premises organizations doing partial sync
- Organizations completely in cloud
- Organizations created through ad-hoc signup

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

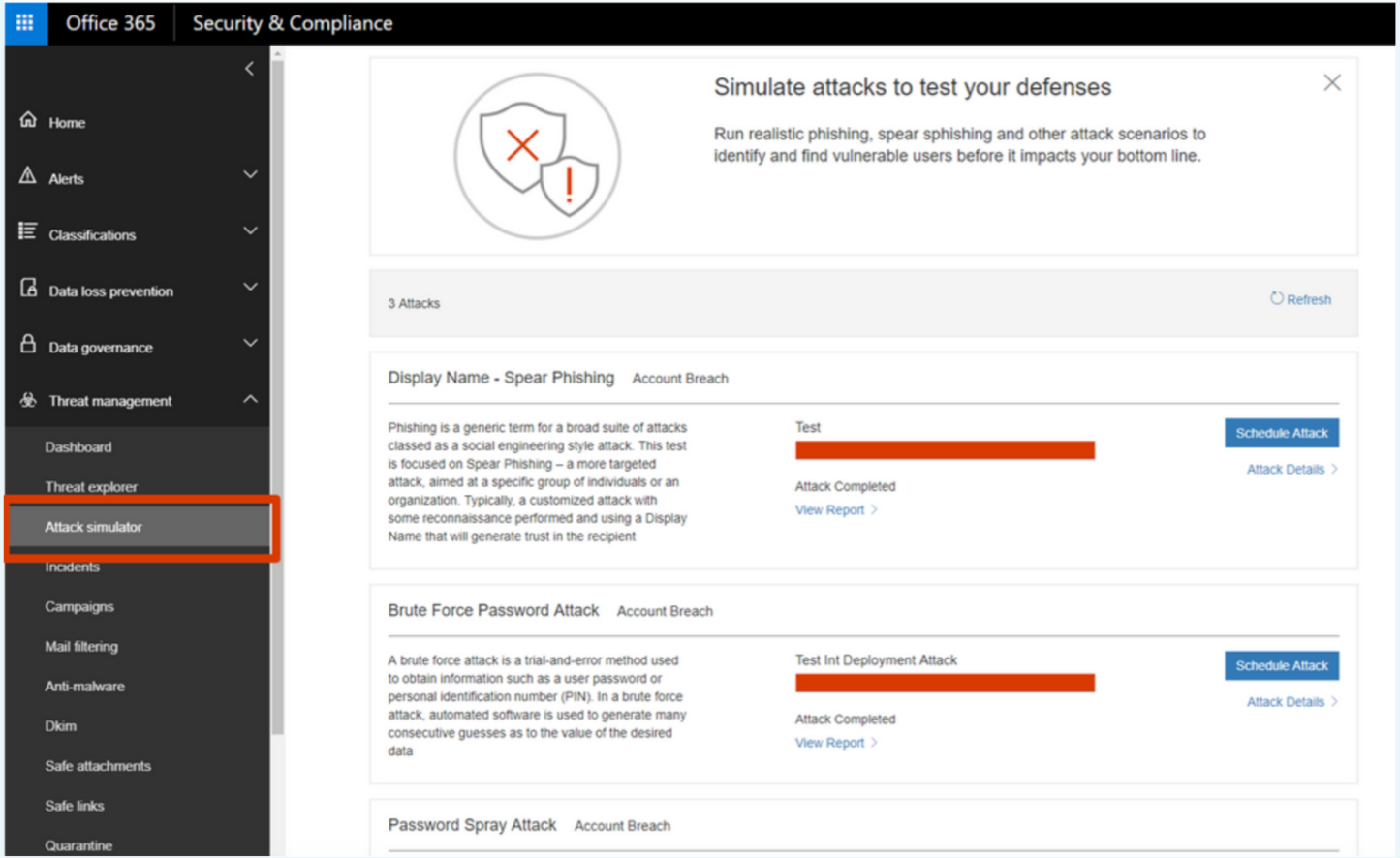
Auditing / SEIM



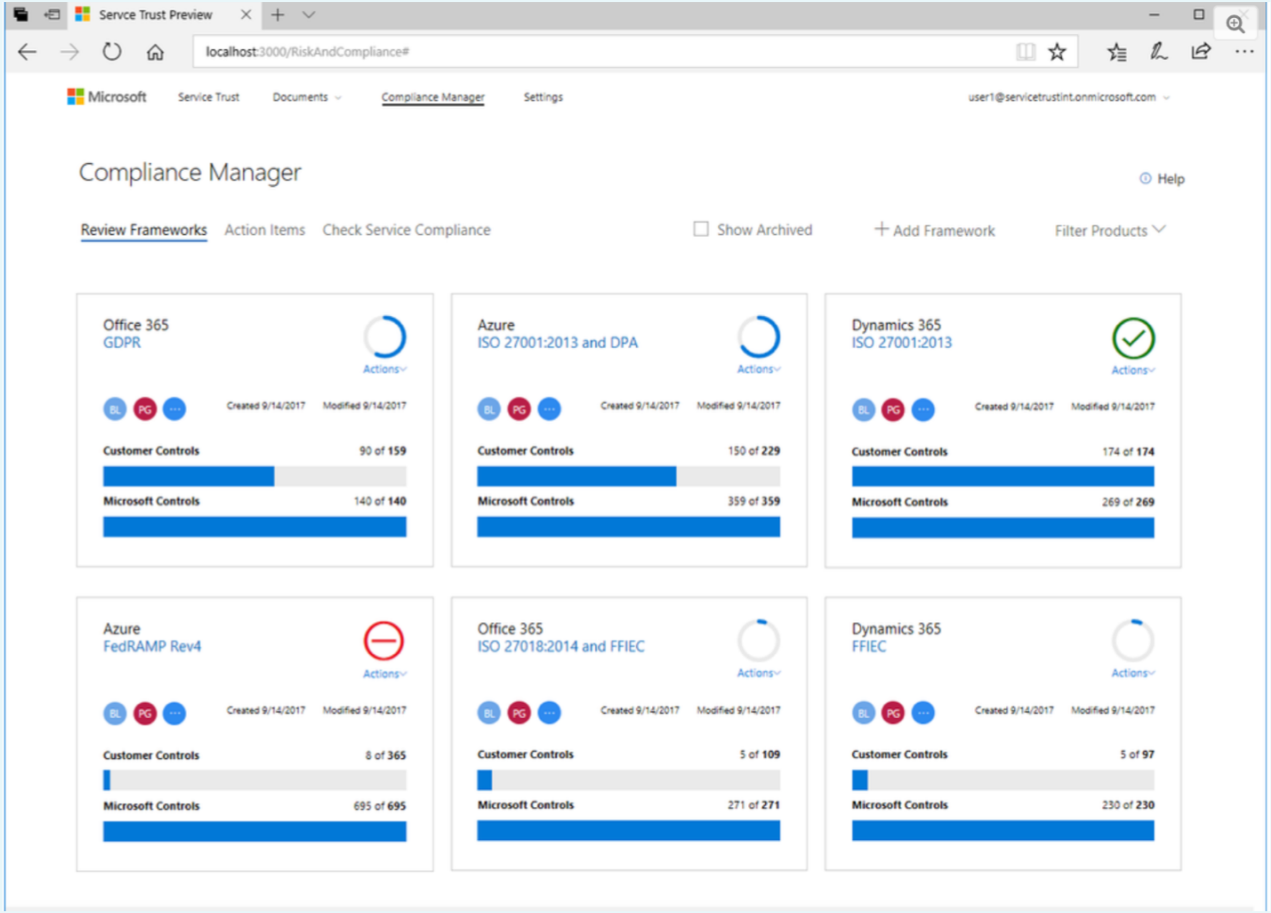


Azure Incoming Features

Incoming! The Microsoft Attack Simulator



Incoming! Microsoft Compliance Manager



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)