

#IMBC7

Office 365 Security

@directorcia

<http://about.me/ciaops>

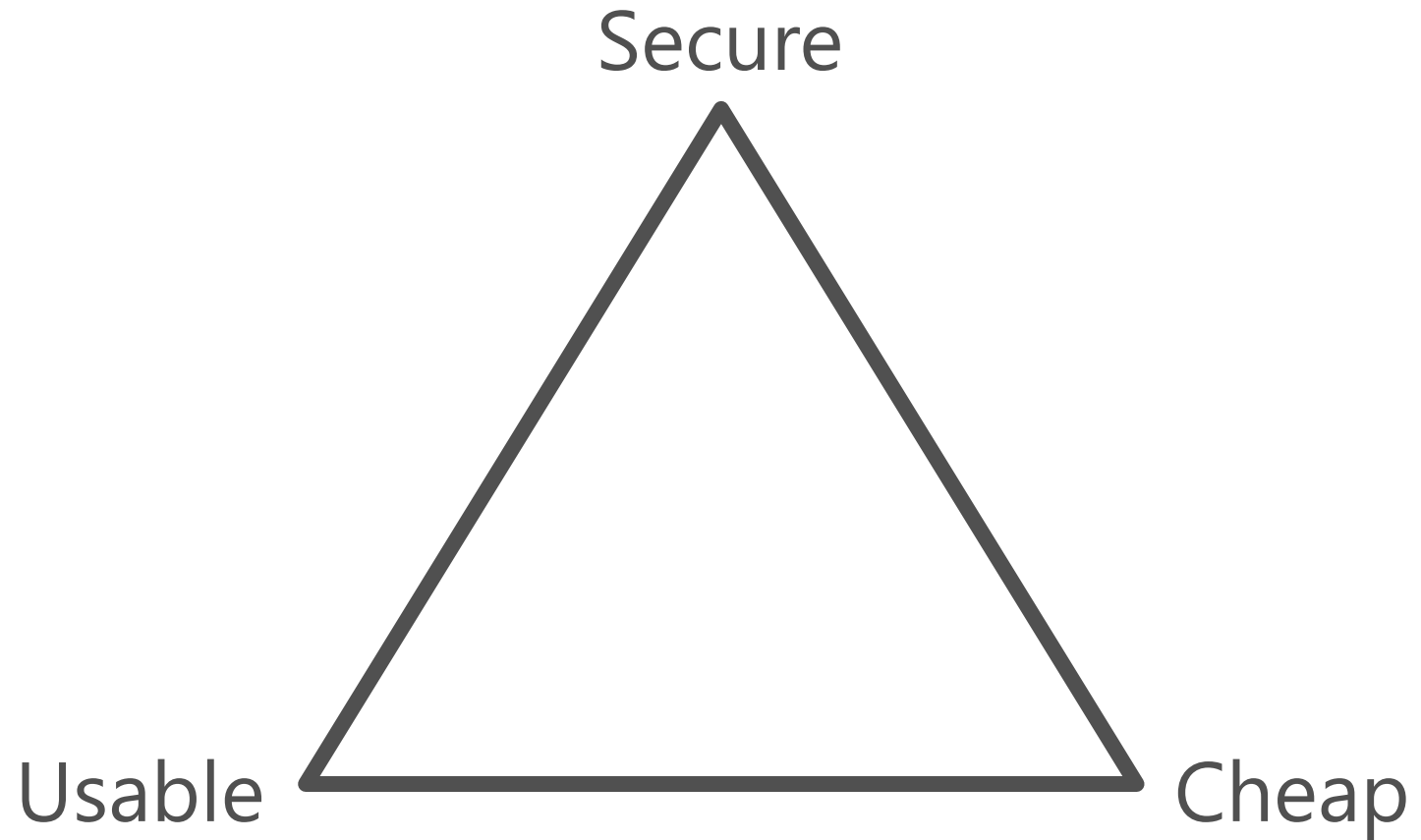
Agenda

- Landscape
- Office 365 Protection
- What you should do
- Some Office 365 security components
- Take aways

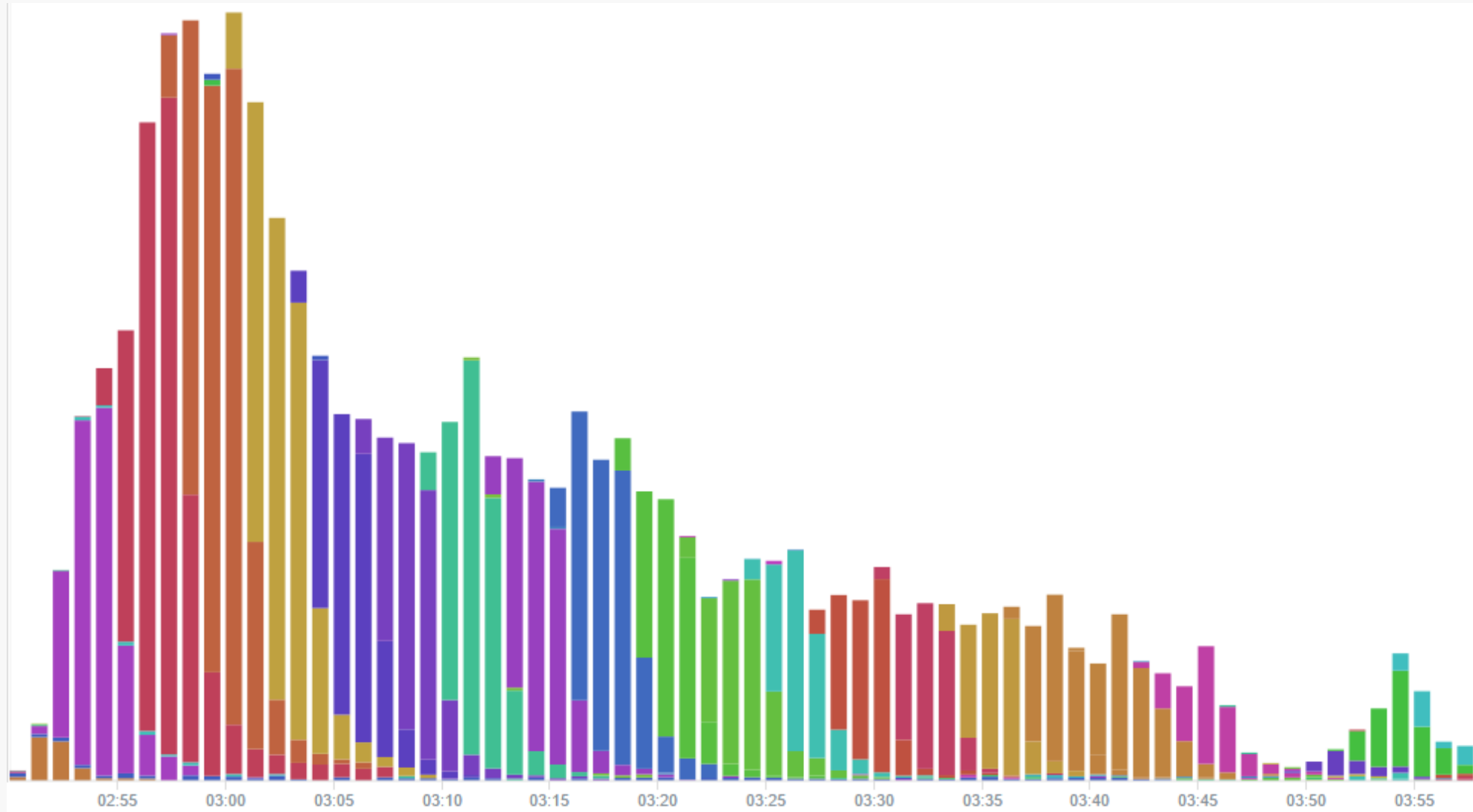


Landscape

The Security Dilemma

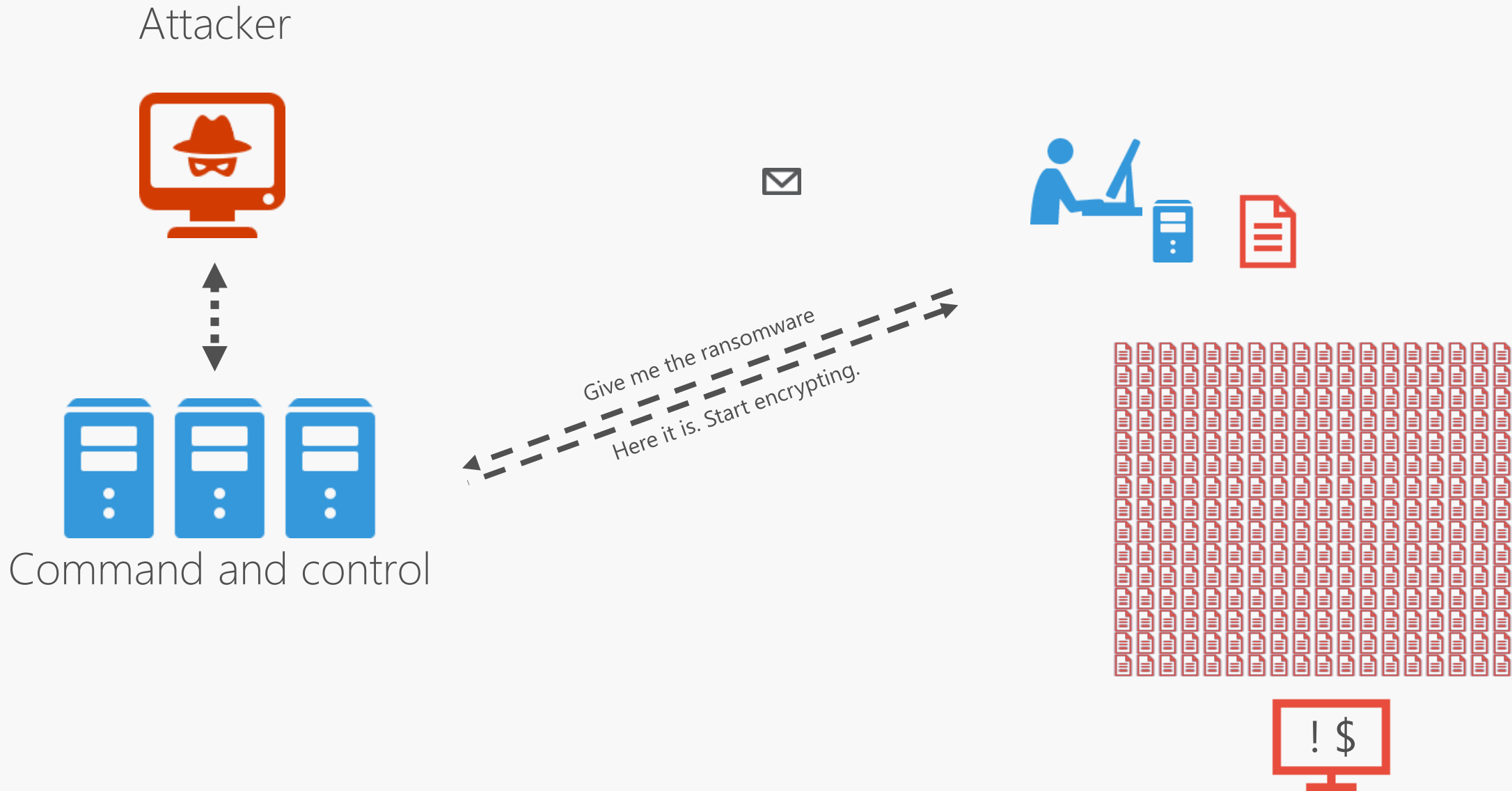


Behind the attack – Cryptolocker Distribution



Attack morphs over time to evade detection

Behind the attack – Cryptolocker infection





Behind the scenes

Office 365 Protection

Edge Block

AV Scanners

Reputation
Blocking

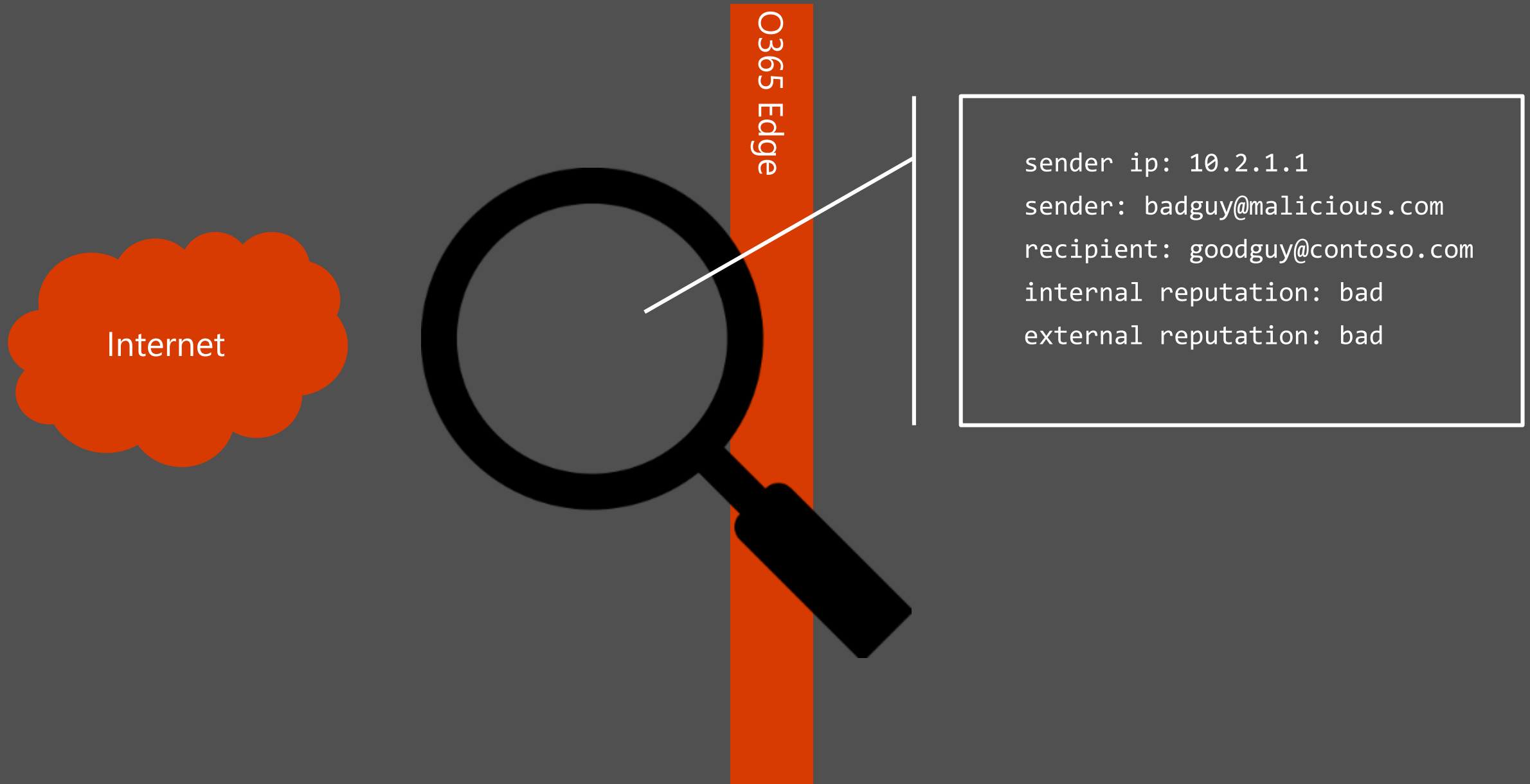
Heuristic
Clustering

ATP Safe
Attachments

Antispam
Phish
Spoof

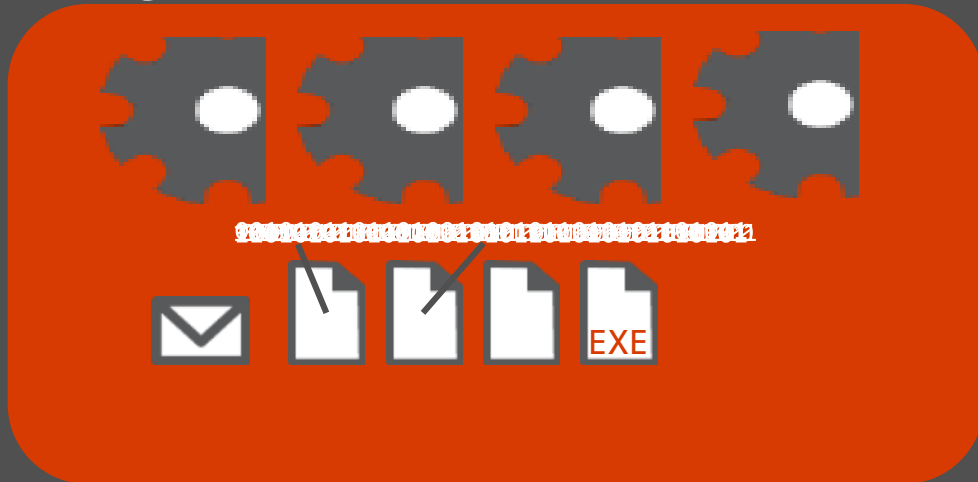
ATP Safe
Links

Preventing attacks

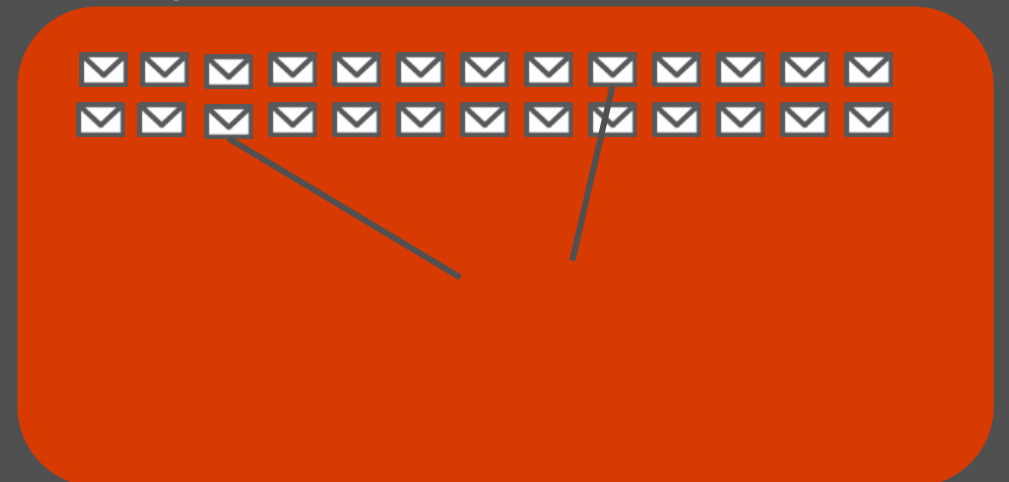


Preventing attacks

Signature AV Scans



Reputation Block



Preventing attacks

Heuristic Clustering



ATP Safe Attachments

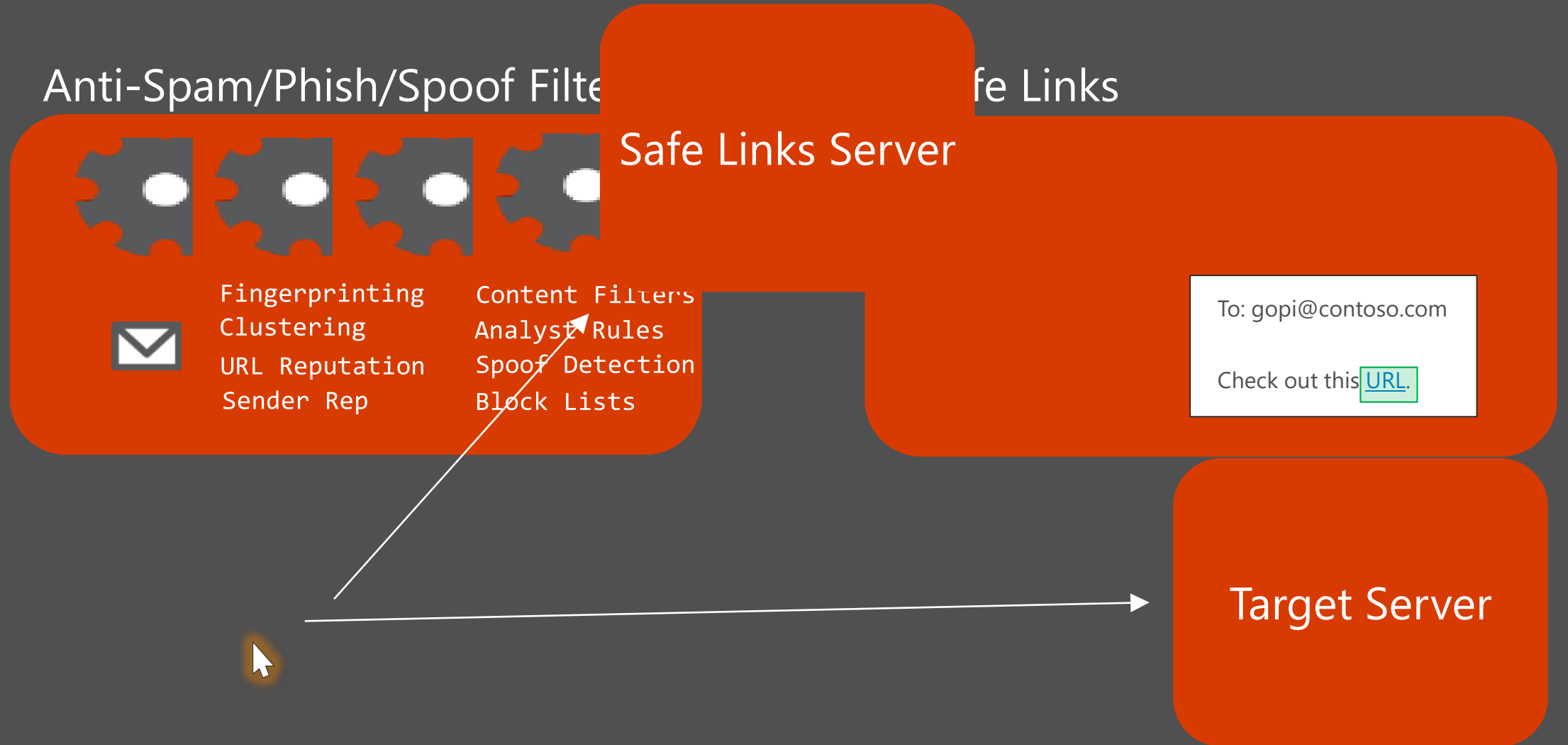


Sandbox

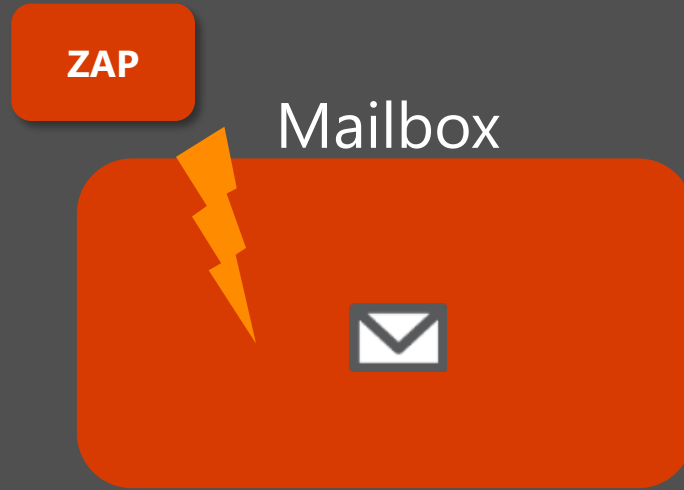
memory scan
obfuscation
evasion
encryption

registry
network
C2 server
file I/O

Preventing attacks

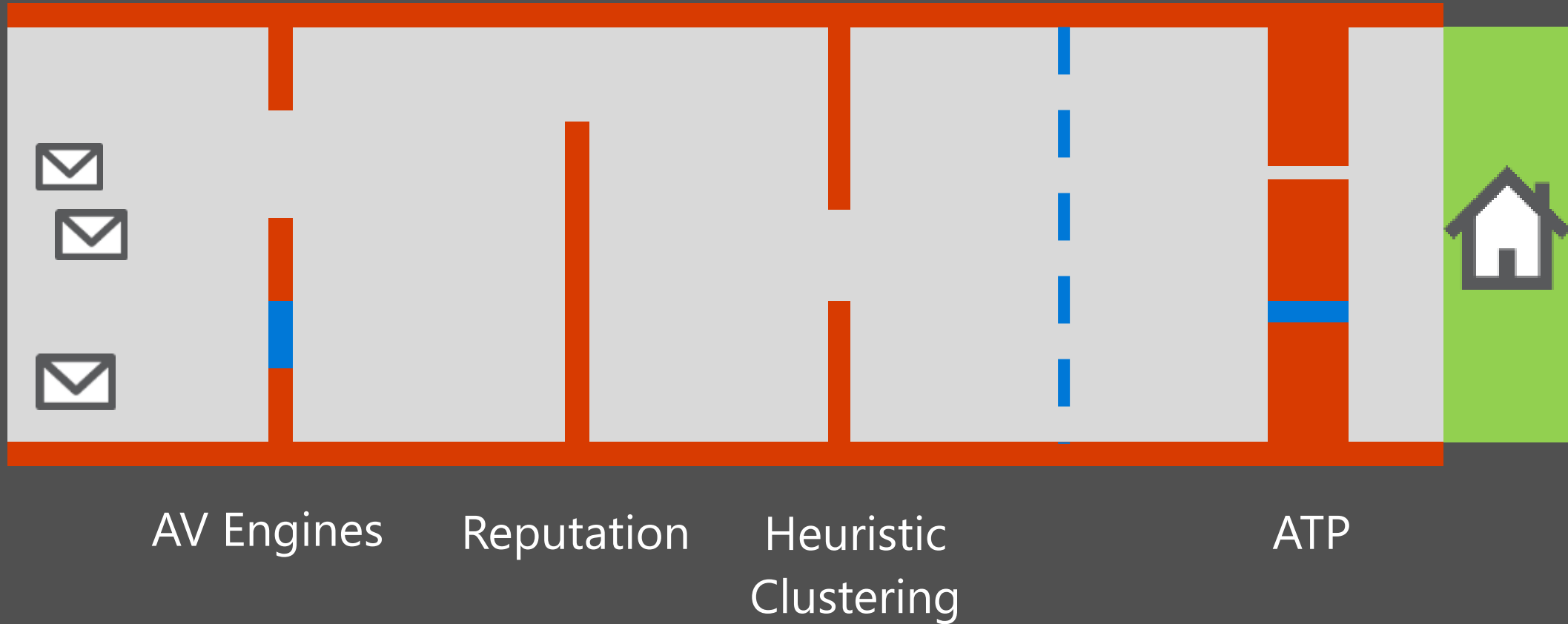


Preventing attacks



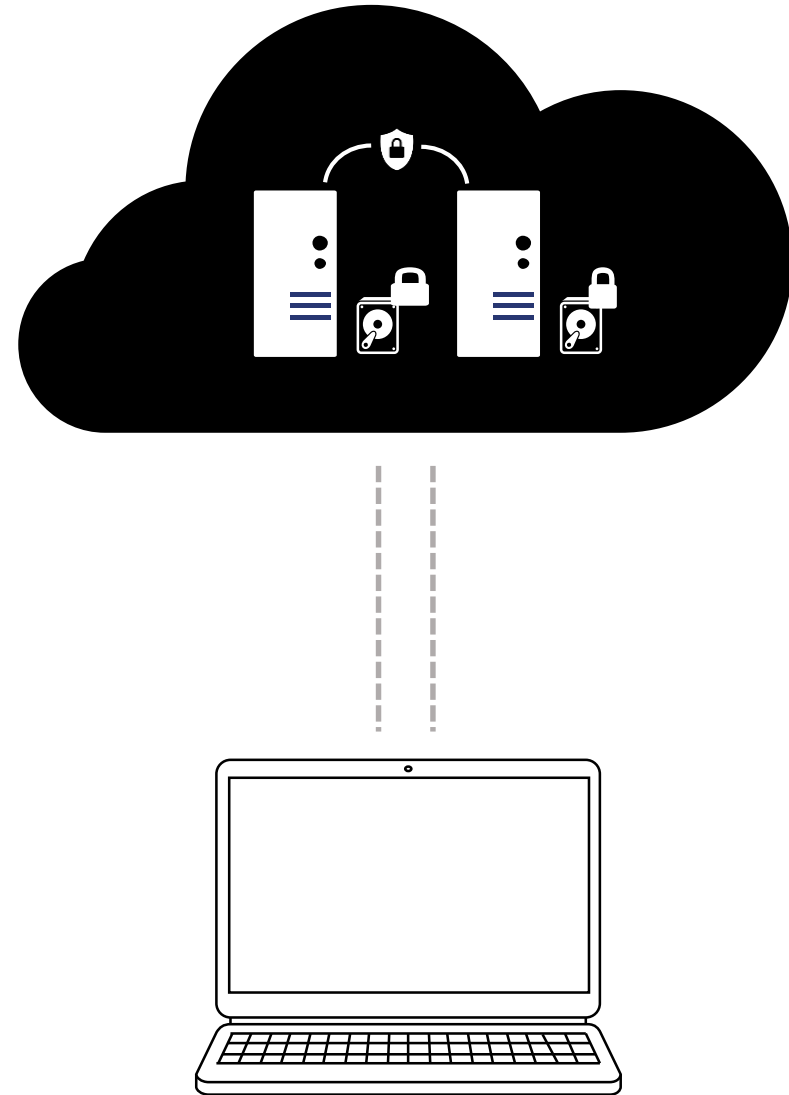
Defense in depth

Anti-Malware Pipeline

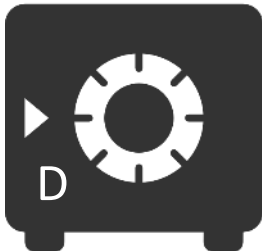
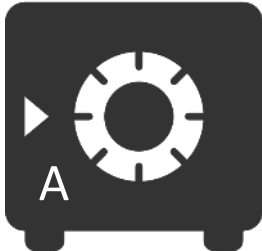


Default Encryption

- **Data in transit**
 - Strong SSL/TLS cipher suite
 - Perfect Forward Secrecy
 - Datacenter-to-datacenter encryption
- **Data at rest**
 - BitLocker disk encryption
 - Per-file encryption for customer content

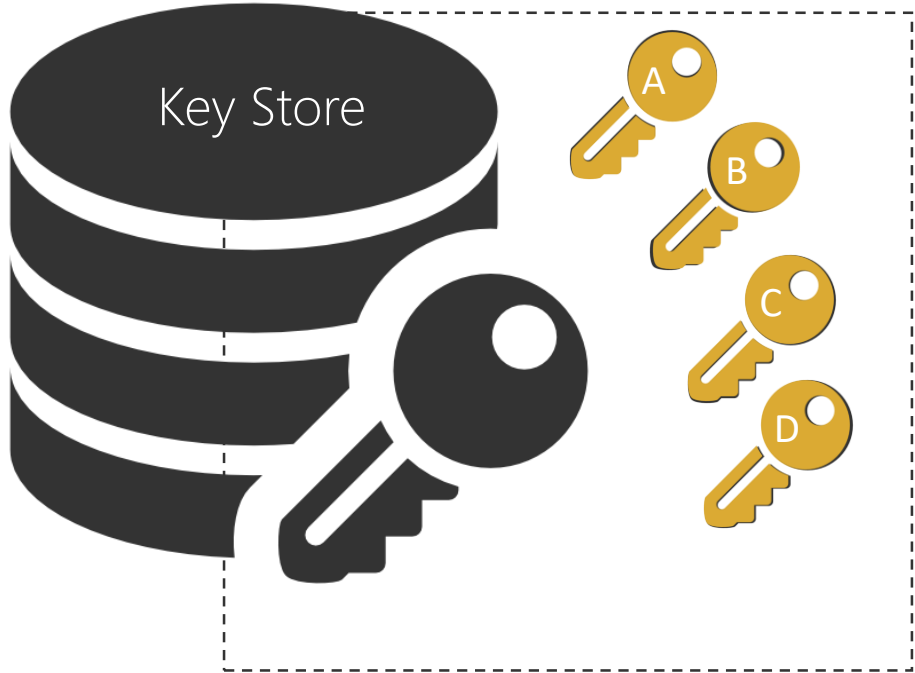
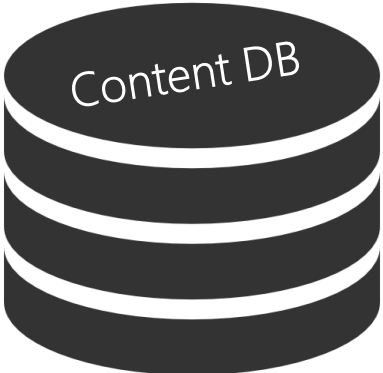


Encryption at rest with Per-file Encryption

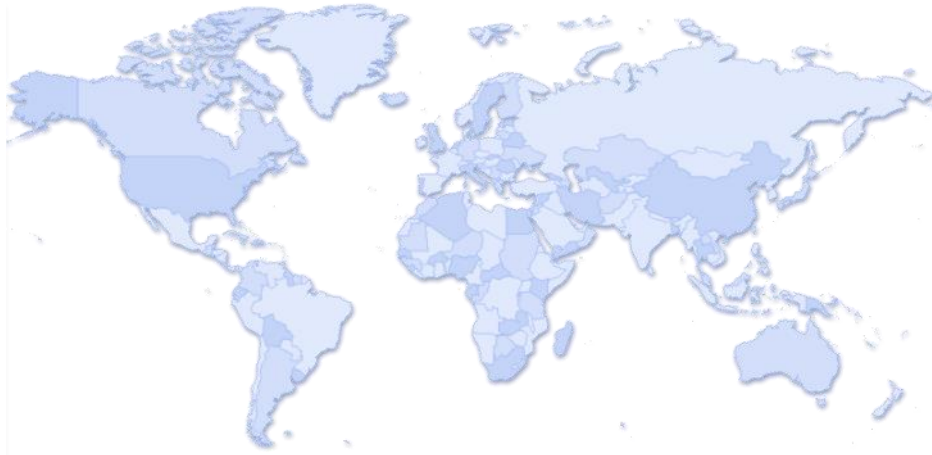


crypto

```
001010101010  
101010110011  
001010101010  
101010110011  
001010101010  
101010110011  
001010101010  
101010110011
```



Standards & Certifications



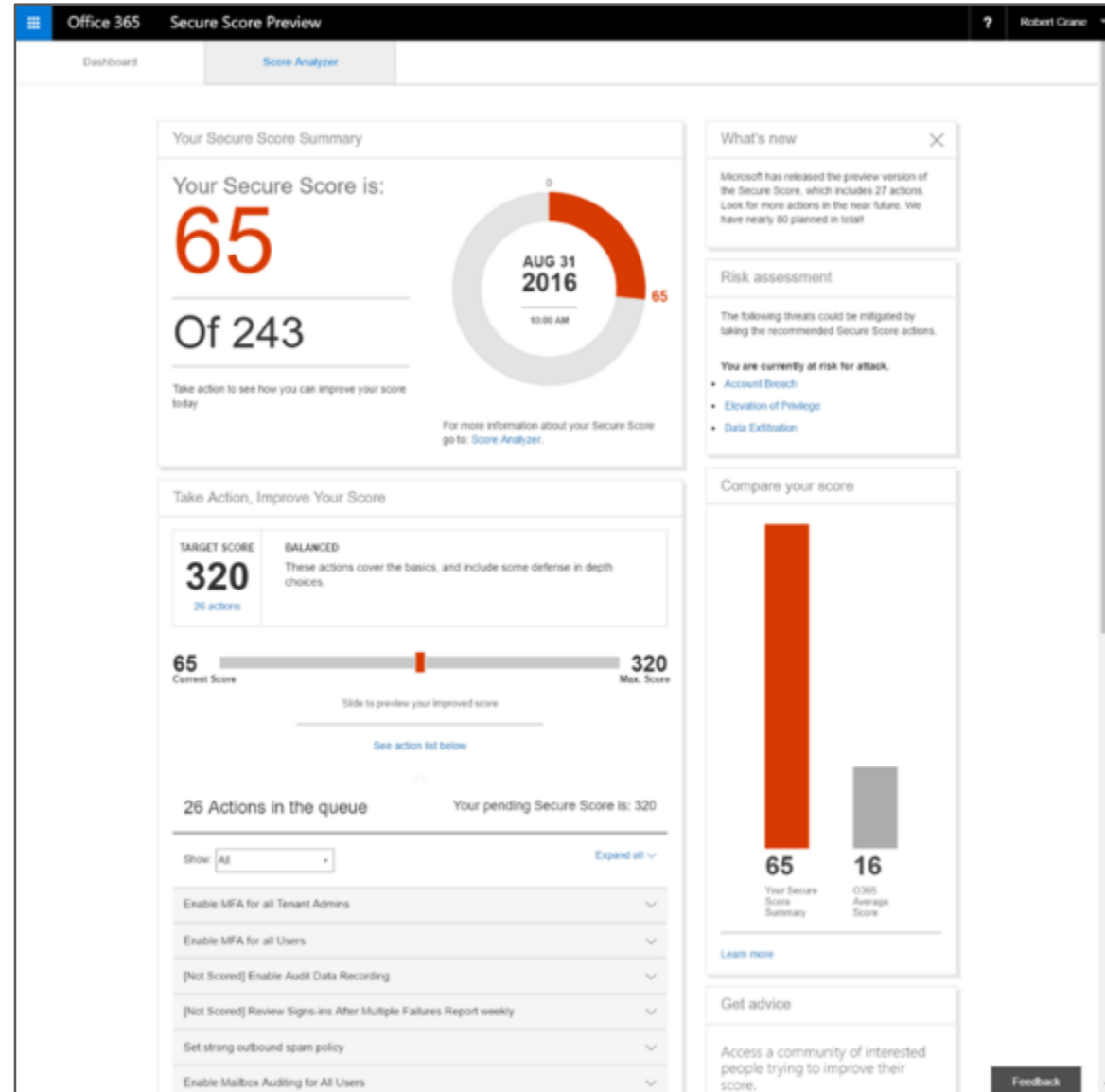
Standards Certifications	Market	Region
SSAE/SOC	Finance	Global
ISO 27001:2013	Global	Global
ISO 27018	Global	Global
EUMC	Europe	Europe
FERPA	Education	U.S.
FedRAMP/FISMA	Government	U.S.
HIPAA	Healthcare	U.S.
HITECH	Healthcare	U.S.
ITAR	Defense	U.S.
HMG IL2	Government	UK
CJIS	Law Enforcement	U.S.
Article 29 ⁺	Europe	Europe
SOC 2	Global	Global



You

should do

Secure Score



- TechNet Library
- Office Products
- Office 365 for administrators
 - ▾ Office 365 Service Descriptions
 - Recent service descriptions changes
 - Office 365 Platform Service Description
 - Office Applications Service Description
 - Office Online Service Description
 - Exchange Online Service Description
 - Exchange Online Protection Service Description
 - Exchange Online Advanced Threat Protection Service Description

Office 365 Service Descriptions

Office 365

Applies to: Office 365

Topic Last Modified: 2016-08-12

Microsoft Office 365 is a cloud-based service that is designed to help meet your organization's needs for robust security, reliability, and user productivity.

The topics in this library provide detailed descriptions of the services and features that are available with Office 365. To compare features across plans, see [Compare Office 365 for Business plans](#) or the relevant service description in the list below.

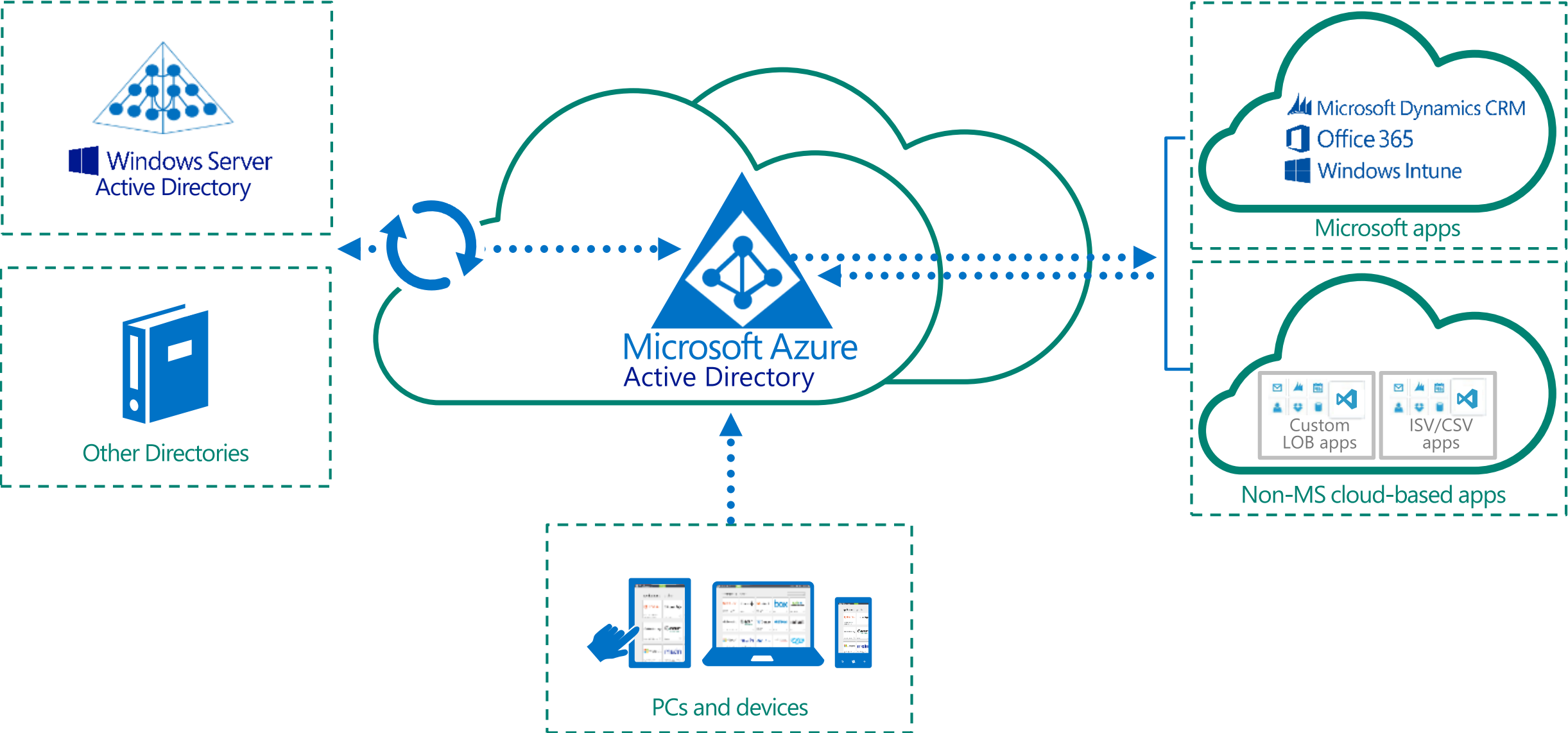
To search for support articles and information, see [Office Support](#).

Note:

If you're looking for the Service Description comparison spreadsheet, it has been retired. The product feature availability tables on each Service Description page have been updated to better help you choose the version of Office 365 that suits your needs.

Microsoft offers the Office 365 Onboarding benefit for eligible services in eligible plans. The Onboarding benefit lets you work remotely with Microsoft specialists to

Azure AD as the control point



Azure Active Directory editions feature comparison + Office 365 IAM features

		Azure Active Directory Free	Azure Active Directory Basic	Azure Active Directory Premium	Office 365 IAM features
Common Features	Directory as a Service	500,000 Object Limit	No Object Limit	No Object Limit	No Object limit for Office 365 user accounts
	User/Group Management (add/update/delete)	Yes	Yes	Yes	Yes
	SSO to pre-integrated SAAS Applications /Custom Apps	10 apps per user	10 apps per user	No Limit	10 apps per user
	User-based access management/provisioning	Yes	Yes	Yes	Yes
	Self-Service Password Change for cloud users	Yes	Yes	Yes	Yes
	Identity Synchronization Tool (Windows Server Active Directory integration, Multi Forest)	Yes	Yes	Yes	Yes
	Security Reports	3 Basic Reports	3 Basic Reports	Advanced Security Reports	3 Basic Reports
Cloud App Discovery*	Yes(Basic)	Yes(Basic)	Yes(Advanced)**	Yes(Basic)	
Premium + Basic Features	Group-based access management/provisioning		Yes	Yes	
	Self-Service Password Reset for cloud users		Yes	Yes	
	Company Branding (Logon Pages/Access Panel customization)		Yes	Yes	
	SLA		Yes	Yes	Yes
Premium Features	Identity Synchronization Tool advanced write-back capabilities * (FY15 Roadmap)			Yes	
	Self-Service Group Management			Yes	
	Self-Service Password Reset/Change with on-premises write-back			Yes	
	Advanced Usage Reporting			Yes	
	Multi-Factor Authentication (Cloud and On-premises (MFA Server))			Yes	Limited Cloud only features for accessing Office 365
	Azure Active Directory Application proxy*			Yes	
	MIM CAL + MIM Server			Yes	
	Administrative Delegation* (FY15 Roadmap)			Yes	

*Features in Preview (Sept 2014) or in the roadmap

** Advanced functionality on Cloud App Discovery is in the roadmap for FY15 H2

10 Apps per user : Every user can have a different set of Apps, up to ten. MS Online apps (e.g. O365) are counted among these 10.

Single Sign On (SSO) Web Portal

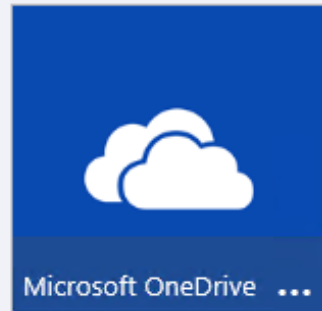
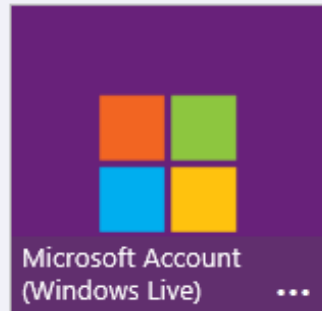
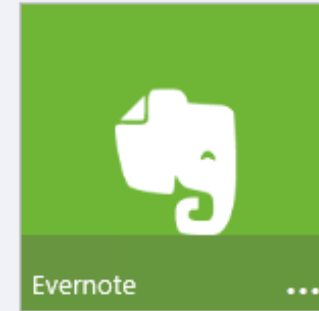
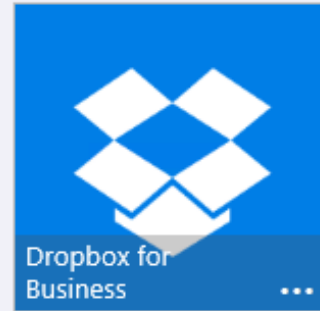
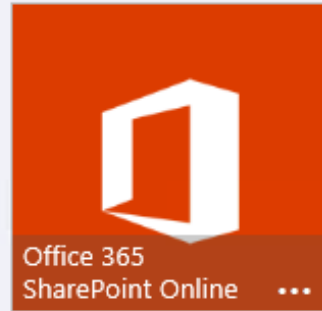
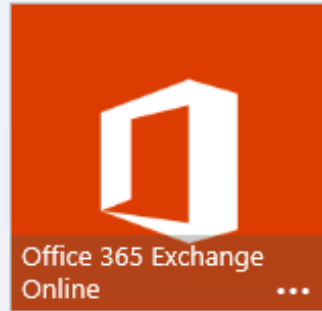
Add an application

Microsoft Azure

lewis.collins@ciaops365.com | CIAOPS |

applications

profile



Showing 7 of 7

Group Management


Microsoft Azure

lewis.collins@kumoalliance.org | Kumo Alliance | ?


applications **groups approvals** profile

You have 1 apps that can't be accessed until you install some software.


[Install Now](#)



Office 365
SharePoint Online ...



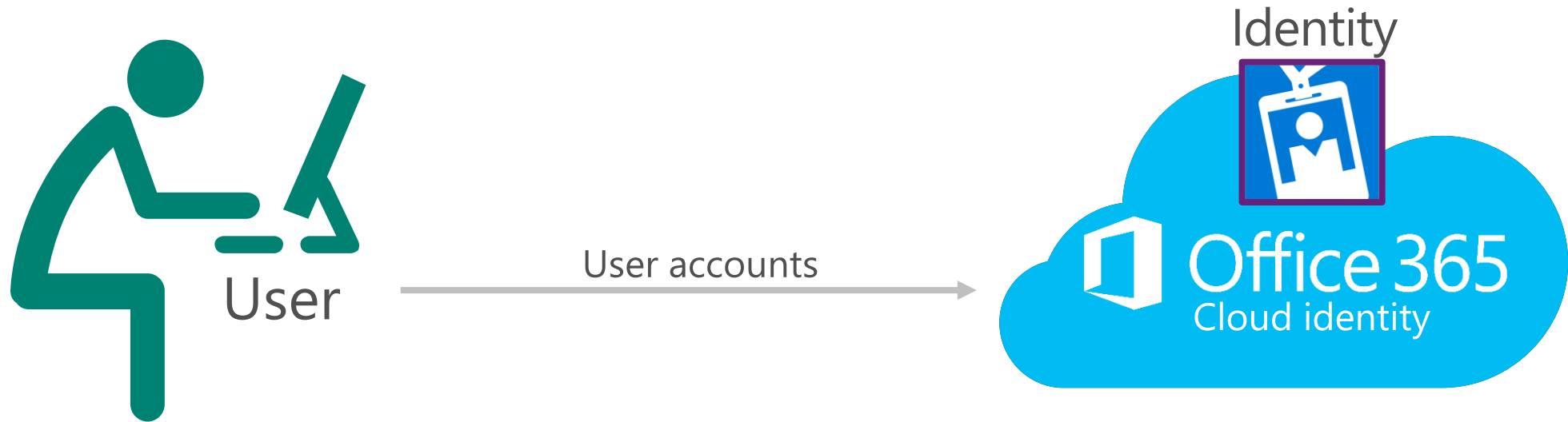
Office 365 Exchange
Online ...



Microsoft OneDrive ...

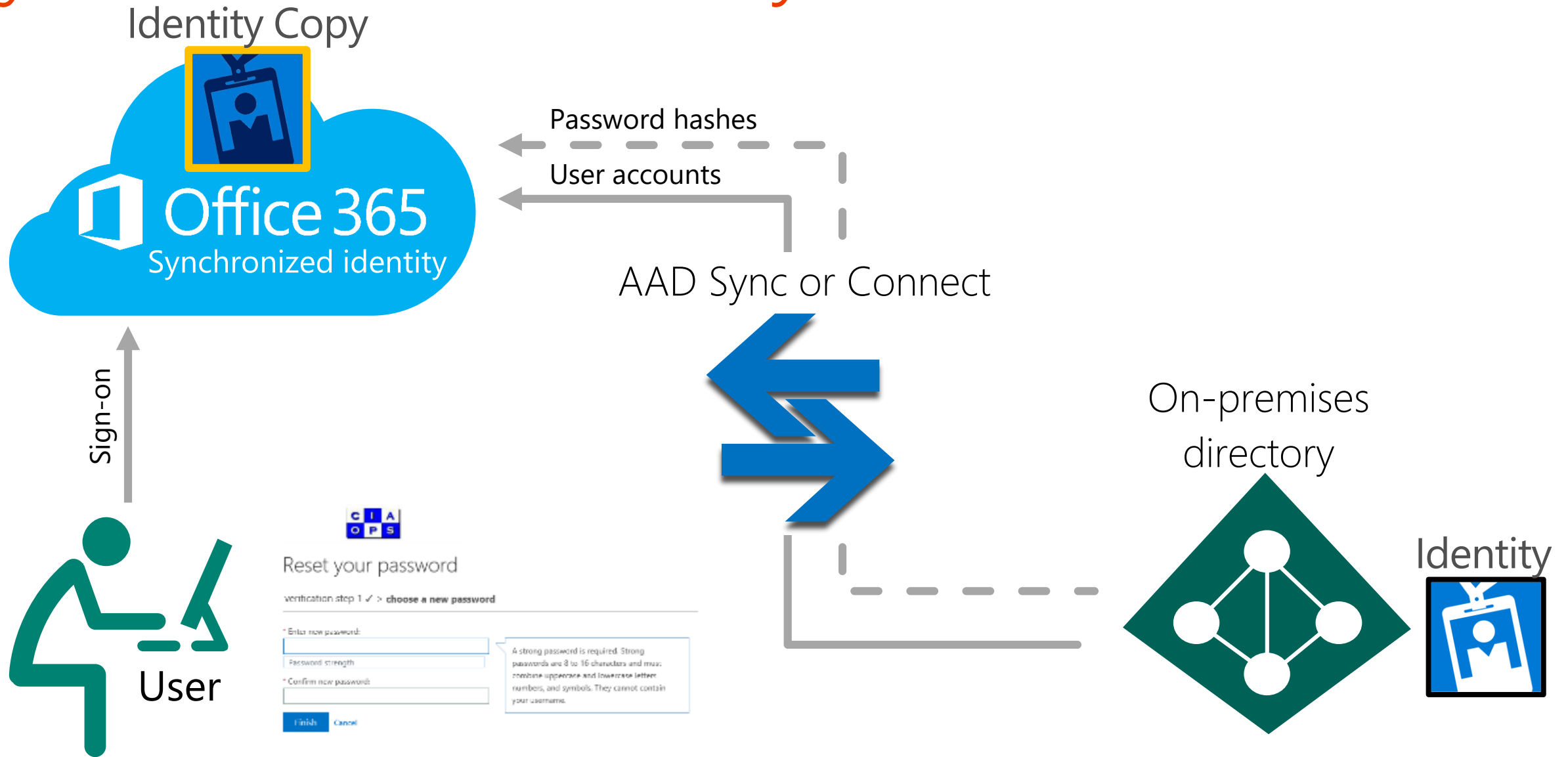
User Password Reset

Cloud identity model



Synchronized Identity Model

 + Azure AD Premium



Security and Compliance Center



- Home
- Alerts
- Permissions
- Classifications
- Data loss prevention
- Data governance
- Threat management
- Search & investigation
- Reports

Home

Customize

Threat management



We understand the importance of keeping your data safe and secure. That's why we provide tools to help you understand and investigate cyber-threats and take action to protect your organization from them.

[Learn more](#)

[+ View quarantine](#)

[+ New spam policy](#)

Search for users

Search for users



What's new

- Enhanced retention
- Enhanced DLP
- Intelligent Import
- [More...](#)

Data governance



It's your data. You own it. So we've developed features that let you take charge of how and when it is stored, used, and retained or removed.

[Learn more about data management](#)

[+ Import data into Office 365](#)

[+ Add a retention policy](#)

[+ Enable extra storage](#)

Search & investigation

Feedback

Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. [Learn more about searching the audit log](#)

Search

 Clear

Activities

User signed in to Teams ▾

Start date

2017-04-01



00:00



End date

2017-05-09



00:00



Users

Show results for all users

Results 150 results found (More items available, scroll down to see more.)

 Filter results

 Export results

Date ▾	IP address	User	Activity
2017-05-08 10:...		admin@ciaops...	User signed in to Te... web (1415/1.0....
2017-05-06 10:...		admin@ciaops...	User signed in to Te... web (1415/1.0....
2017-05-06 10:...		admin@ciaops...	User signed in to Te... web (1415/1.0....
2017-05-06 10:...		admin@ciaops...	User signed in to Te... web (1415/1.0....
2017-05-06 10:...		admin@ciaops...	User signed in to Te... web (1415/1.0....
2017-05-06 09:...		admin@ciaops...	User signed in to Te... web (1415/1.0....

Create a policy to retain what you want and get rid of what you don't.

Name your policy

Settings

Set your locations

Review your settings

Decide if you want to retain content, delete it, or both

Do you want to retain content? [i](#)

Yes, I want to retain it [i](#)

For this long...

Retain the content based on [i](#)

Do you want us to delete it after this time? [i](#)

Yes No

No, just delete content that's older than [i](#)

Need more options?

Use advanced retention settings [i](#)

Back

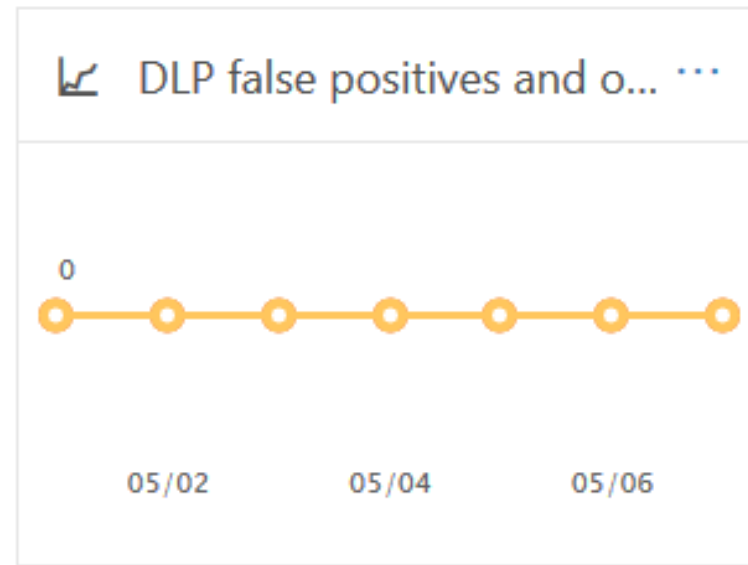
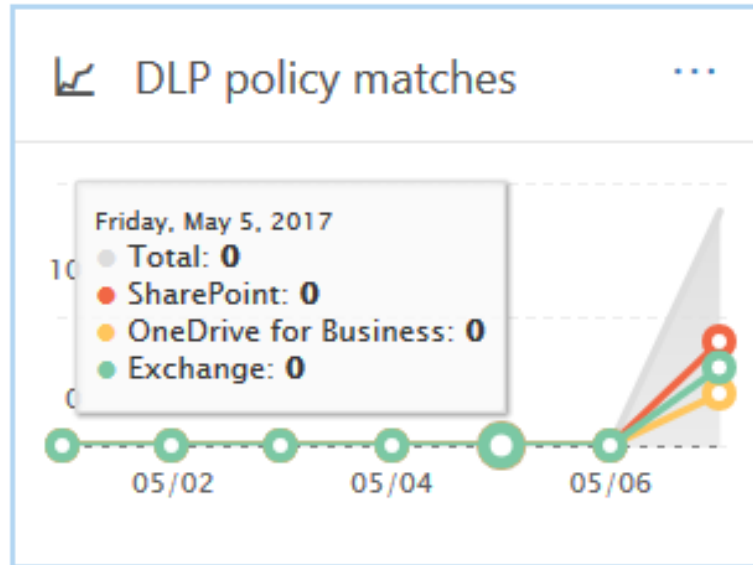
Next

Cancel

Data Loss Prevention (DLP)



Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive information. For example, help make sure information in email and docs isn't shared with the wrong people. [Learn more about DLP](#)

[+ Create a policy](#)[Refresh](#)

<input type="checkbox"/>	Name	Order	Last modified	Status
<input type="checkbox"/>	Credit Card Policy	1	May 7, 2017	On
<input type="checkbox"/>	Australia Financial Data	2	May 7, 2017	On

DLP document fingerprinting

Scan email and attachments to look for patterns that match document templates

Protect sensitive documents from being accidentally shared outside your organization

No coding required; simply upload sample documents to create fingerprints

document fingerprints

You can use document fingerprints to customize sensitive information types in your policies.

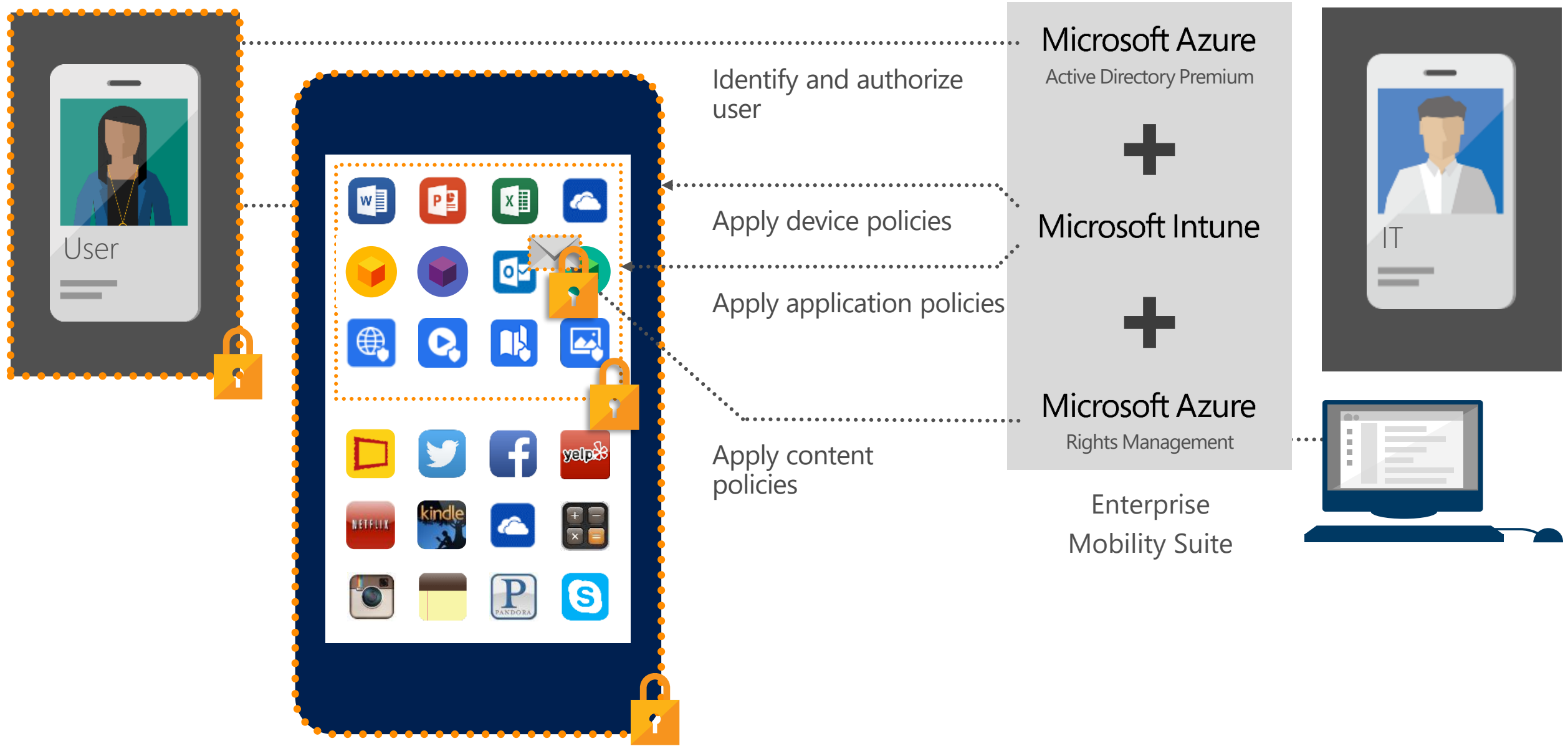
+ ✎ 🗑️ ↺

NAME	
IRS Tax Forms	
Standard Bank Forms	Standard Bank Forms This sensitive information type will detect any of the standard bank forms, like a loan application, account information, etc. Files: Account opening form - Business.pdf Account opening form - Personal.pdf Account opening form - Priority.pdf Auto loan application for business.pdf Auto loan application for salaried individual.pdf Cash Deposit Slip.pdf Cheque Deposit Slip.pdf Credit Card application form.pdf

1 selected of 2 total

Mobile Device Management (MDM)

Multiple layers of data protection

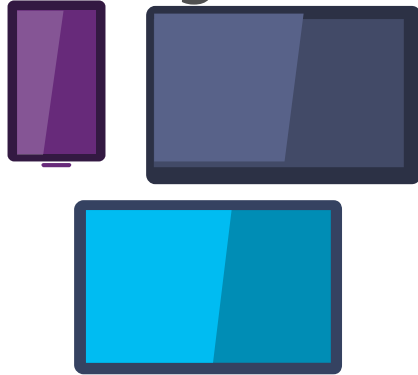


Mobile Device Management

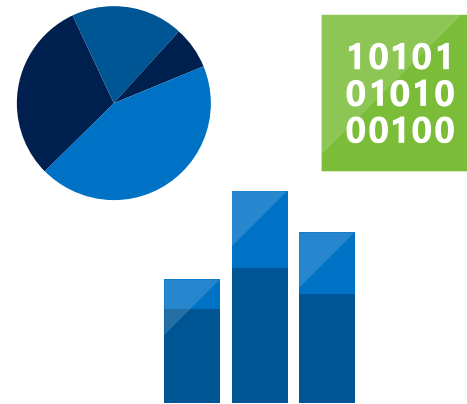
Conditional Access



Device Management



Selective Wipe



Advanced Application Management

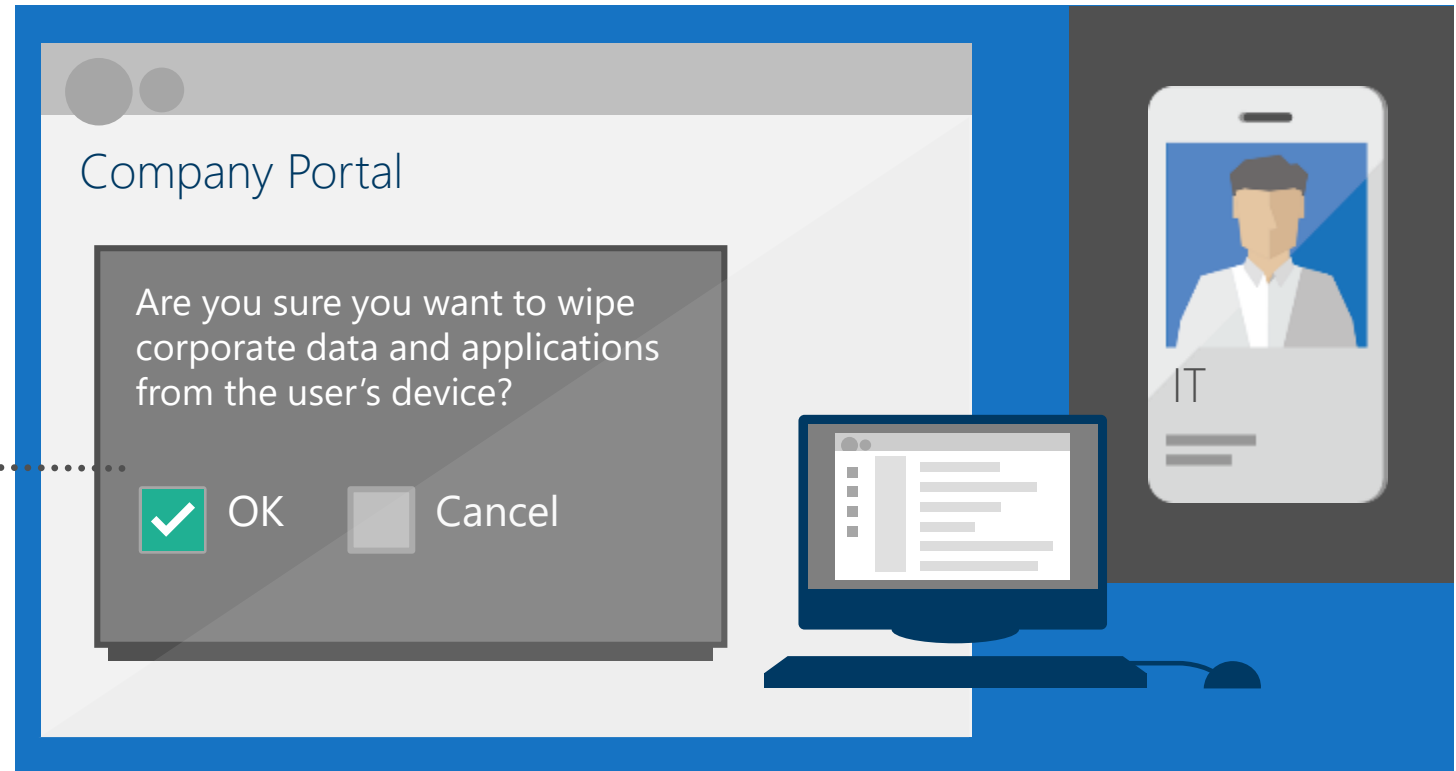
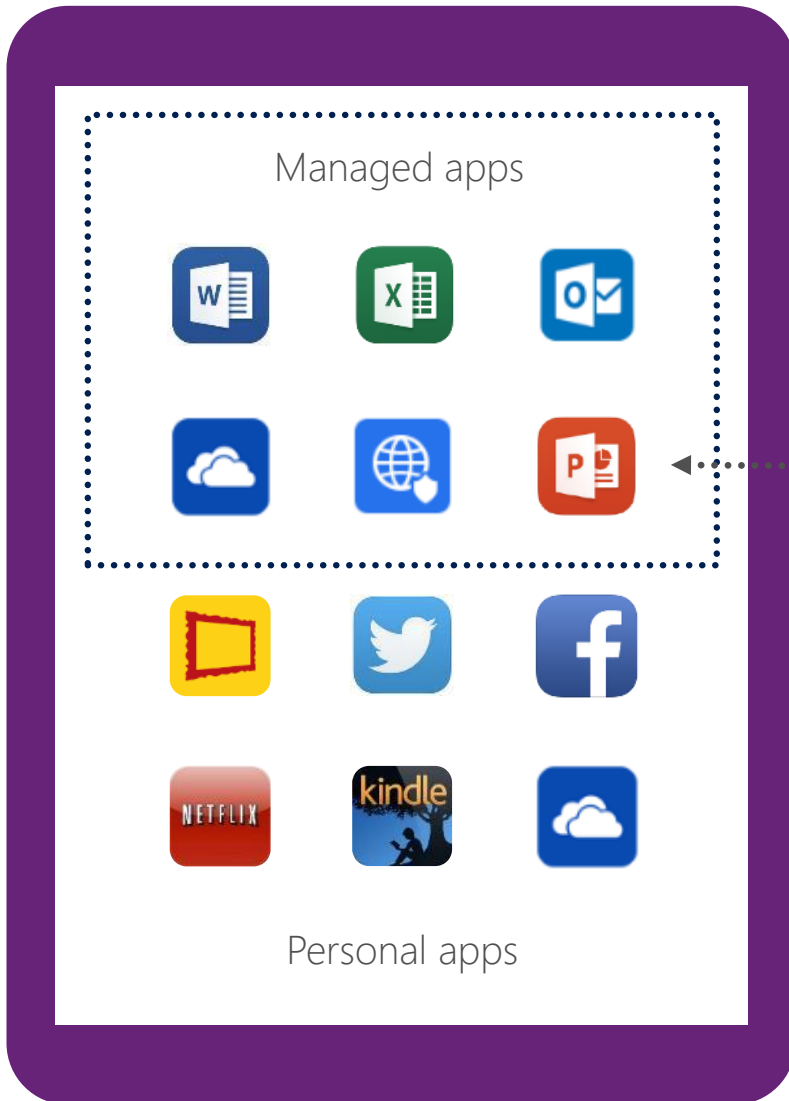


Built-in



Microsoft Intune

Selective wipe



- ▶ Perform selective wipe via self-service company portal or admin console
- ▶ Remove managed apps and data
- ▶ Keep personal apps and data intact

Access requirements

What requirements do you want to have on devices?

- Require a password
- Prevent simple passwords
- Require an alphanumeric password:
Password must include at least character sets
- Minimum password length:
 characters
- Number of sign-in failures before device is wiped
 attempts
- Lock devices if they are inactive for this many minutes:
 minutes
- Password expiration:
 days
- Remember password history and prevent reuse:
Store up to previous passwords

- Require data encryption on devices
- Prevent jail broken or rooted devices from connecting
- Require managing email profile (required for selective wipe on iOS)

If a device doesn't meet the requirements above, then...

- Allow access and report violation
- Block access and report violation

Configurations

What else do you want to configure?

- Require encrypted backup
- Block cloud backup
- Block document synchronization
- Block photo synchronization

- Block screen capture
- Block video conferences on device
- Block sending diagnostic data from devices

- Block access to application store
- Require password when accessing application store

- Block connection with removable storage
- Block Bluetooth connection

The settings above will be configured on users' devices, and violations will be reported



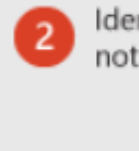
On user's new iPhone 6



In Office 365



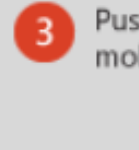
1 Download Office Mobile and sign into Office 365



2 Identify device as not enrolled



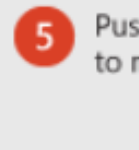
4 Enroll device



3 Push enrollment to mobile device



6 Apply policy to device



5 Push new policy to mobile device



7 Access Office 365 documents in Office Mobile



8 Identify device as compliant



10 View Office 365 documents in Office Mobile



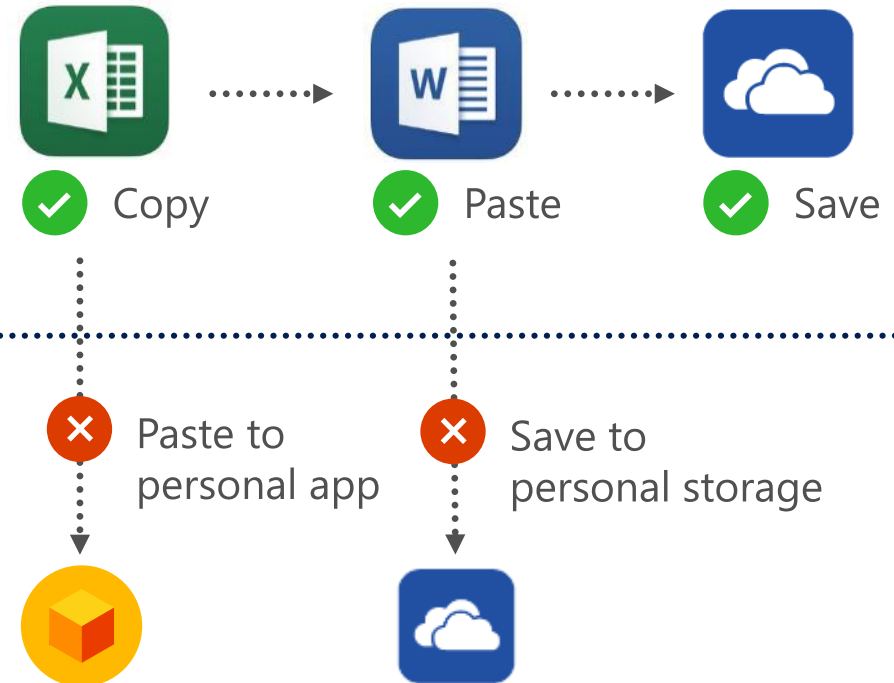
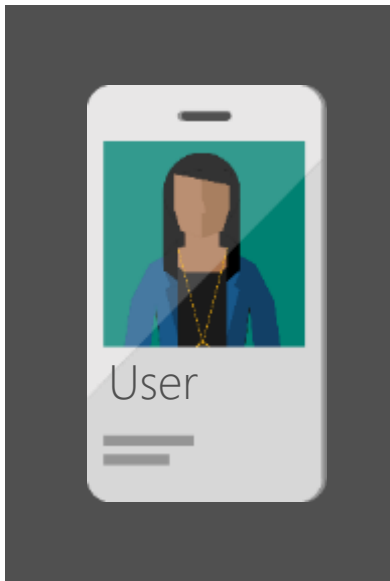
9 Allow device access to Office 365 documents

Feature Comparison with MDM for Office 365



Category	Feature	Exchange ActiveSync	MDM for Office 365	Intune Standalone	Intune + ConfigMgr (Hybrid)
Device configuration	Inventory mobile devices that access corporate applications	●	●	●	●
	Remote factory reset (full device wipe)	●	●	●	●
	Mobile device configuration settings (PIN length, PIN required, lock time, etc.)	●	●	●	●
	Self-service password reset (Office 365 cloud only users)	●	●	●	●
Office 365	Provides reporting on devices that do not meet IT policy		●	●	●
	Group-based policies and reporting (ability to use groups for targeted device configuration)		●	●	●
	Root cert and jailbreak detection		●	●	●
	Remove Office 365 app data from mobile devices while leaving personal data and apps intact (selective wipe)		●	●	●
	Prevent access to corporate email and documents based upon device enrollment and compliance policies		●	●	●
Premium mobile device & app management	Self-service Company Portal for users to enroll their own devices and install corporate apps			●	●
	App deployment (Windows Phone, iOS, Android)			●	●
	Deploy certificates, VPN profiles (including app-specific profiles), email profiles, and Wi-Fi profiles			●	●
	Prevent cut/copy/paste/save as of data from corporate apps to personal apps (mobile application management)			●	●
	Secure content viewing via Managed browser, PDF viewer, Imager viewer, and AV player apps for Intune			●	●
Remote device lock via self-service Company Portal and via admin console			●	●	
PC Management	Client PC management (e.g. Windows 8.1, inventory, antimalware, patch, policies, etc.)			●	●
	PC software management			●	●
	Comprehensive PC management (e.g. Windows Server/Linux/Mac OS X support, virtual desktop and power management, custom reporting, etc.)				●
	OS deployment				●
	Single management console for PCs, Windows Server/Linux/Mac OS X, and mobile devices				●

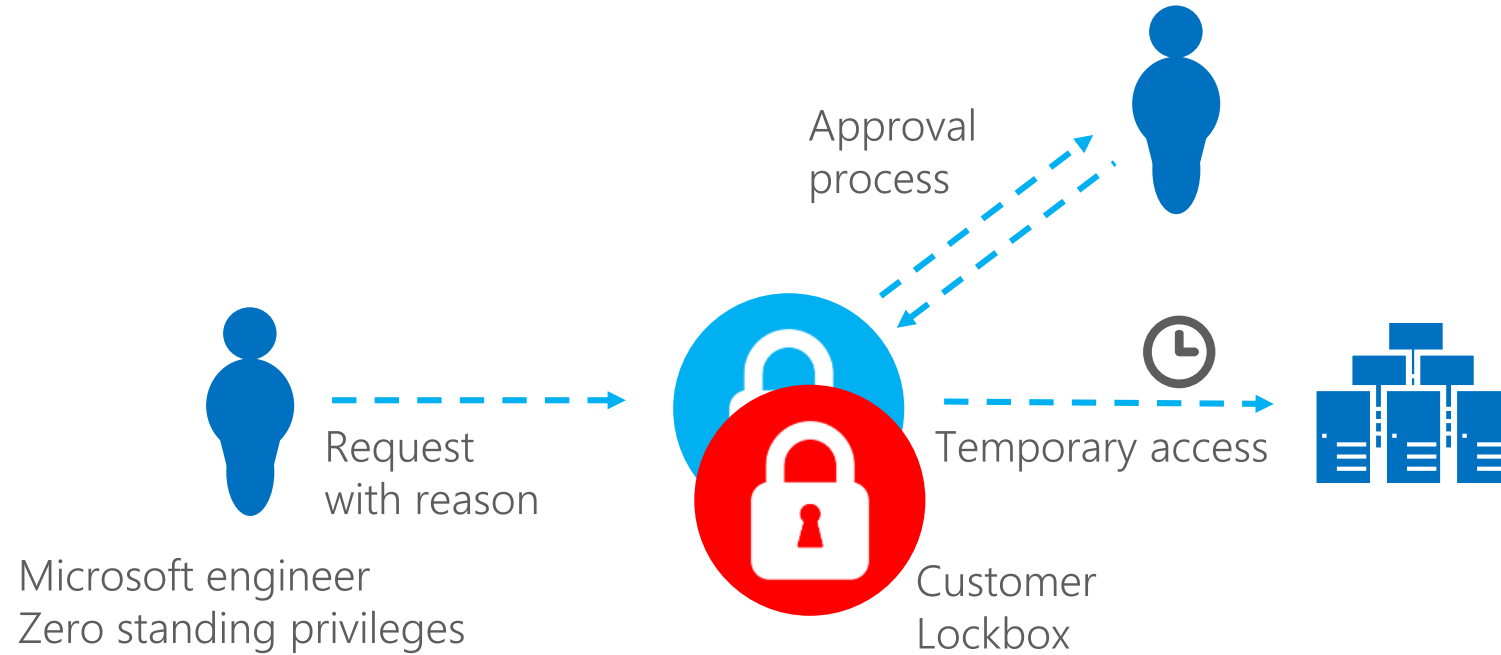
Mobile application management



- ▶ Maximize productivity while preventing leakage of company data by restricting actions such as copy/cut/paste/save in your managed app ecosystem

Customer Lockbox

Just-in-time access



Engineers must have current background check, fingerprinting, security training.
System grants least privilege required to complete task.

Hold and eDiscovery

eDiscovery and In-Place Hold in Office 365 ^{+>E3}

Integrated tools to help you preserve, expire, and discover data

Hold



Keep the data you do want

Data Held In-Place

Customize holds based on filters

Hold across multiple products in a single action

Capture deleted & edited messages

Deletion

Delete the data you don't want

Automated time-based criteria to delete

Set policies at item or folder level – admin or user

Set site level retention policies

Search



Find the data you need

Search across multiple products

De-duplication & search statistics

Case management

Export search results

Advanced Security Protection (ATP)

Office 365 Advanced Security Management | Activity log | Control | Alerts 9

← General Anomaly Detection 2 days ago | 86% Risk score | High severity

Resolution options: claud@acme.com | Dismiss... | Resolve alert...

Description




The user claud@acme.com triggered a suspicious session with a combined risk score of 85.95/100 based on the factors below.

- The IP 109.163.234.2 is an anonymous proxy
- The user claud@acme.com is an administrator
- The ISP 'Voxility S.R.L.'
 - was first used by any user across the organization
 - was first used by any user for administrative activity across the organization
- The administrative action 'Set-Mailbox ForwardingSMTPAddress'
 - was performed for the first time in 82 days
 - was performed only 20 times in the past
- The session contains 3 failed login attempts

It is recommended to confirm the user is familiar with these actions.

Activity log

1 - 8 of 8 activities

Activity	User	App	IP address	Location	Device	Date
 Run command New-Ap...	clau...	Microsoft Exchan...	—	—	?	May 24, 2016, 11:52 ...
 Run command Set-Mai...	clau...	Microsoft Exchan...	—	—	?	May 24, 2016, 11:52 ...
 Run command Set-Mai...	clau...	Microsoft Exchan...	—	—	?	May 24, 2016, 11:52 ...

Creating Activity Policies

Templates for common activities

Rich activity filters

Data Enrichment – Define IP Address Ranges

Repeated activity, Single Event

Can create from Activity Search

Automated Governance Action:

e.g. Suspend User

Policy template

No template

No template

Administrative activity from a non-administrative IP address

User logon from a non-categorized IP address

Mass download by a single user

Multiple failed user log on attempts to an app

Logon from a risky IP address

Log on from an outdated browser

Act on:

Single activity
Every activity that matches the filters

Repeated activity:
Repeated activity by a single user

Minimum repeated activities:

Within timeframe: minutes

Group matched activities per app

Multi-factor Authentication (MFA)

Azure MFA vs MFA for Office 365



	MFA for Office 365/Azure Administrators	Azure Multi-Factor Authentication
Administrators can Enable/Enforce MFA to end-users	Yes	Yes
Use Mobile app (online and OTP) as second authentication factor	Yes	Yes
Use Phone call as second authentication factor	Yes	Yes
Use SMS as second authentication factor	Yes	Yes
Application passwords for non-browser clients (e.g. Outlook, Lync)	Yes	Yes
Default Microsoft greetings during authentication phone calls	Yes	Yes
Suspend MFA from known devices	Yes	Yes
Custom greetings during authentication phone calls		Yes
Fraud alert		Yes
MFA SDK		Yes
Security Reports		Yes
MFA for on-premises applications/ MFA Server.		Yes
One-Time Bypass		Yes
Block/Unblock Users		Yes
Customizable caller ID for authentication phone calls		Yes
Event Confirmation		Yes
Trusted IPs		Yes

Office 365 Rights Management (IRM)

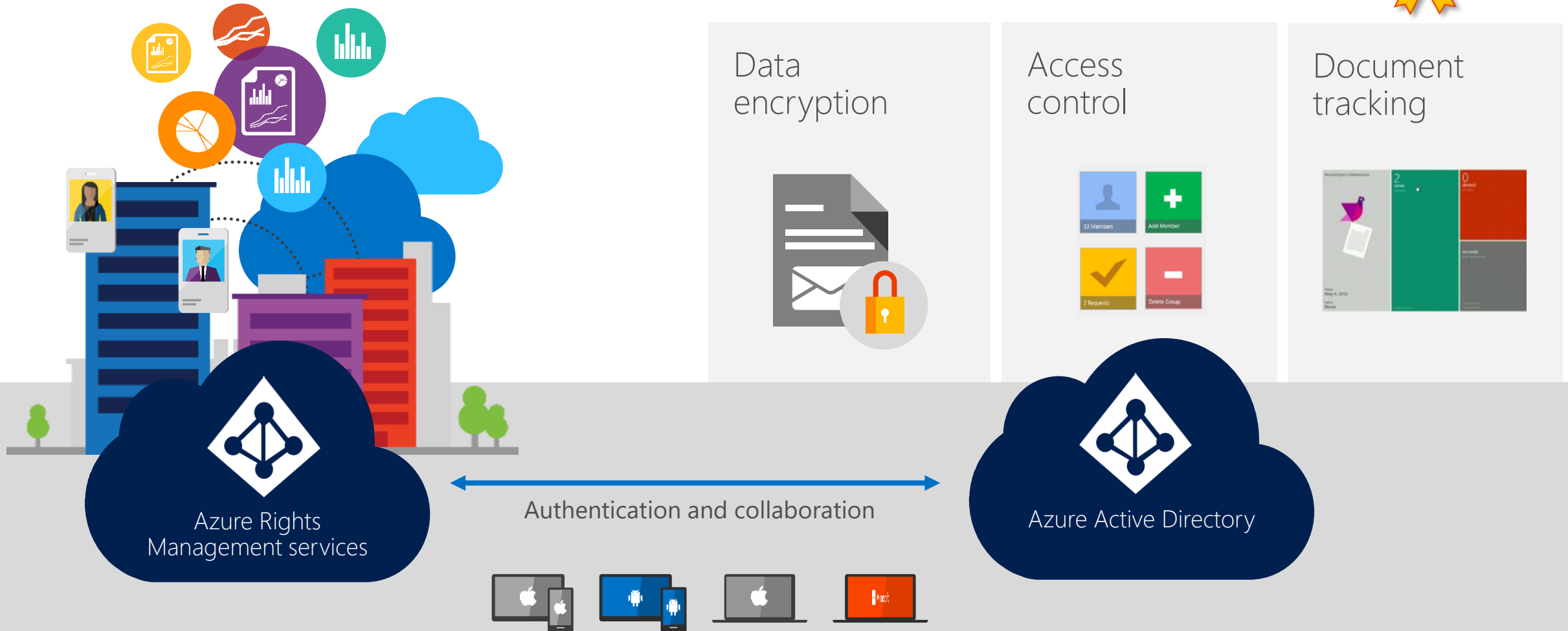
Rights Management



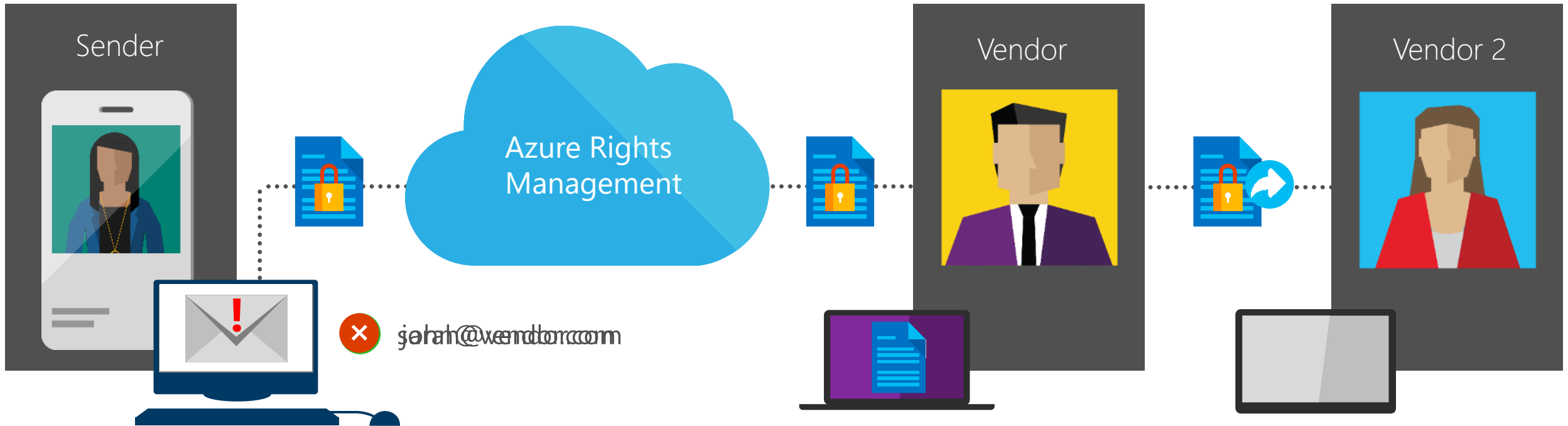
Feature	RMS for Office 365	EMS or Azure RMS Premium
Users can create and consume protected content by using Windows clients and Office applications	●	●
Users can create and consume protected content by using mobile devices	●	●
Integrates with Exchange Online, SharePoint Online, and OneDrive for Business	●	●
Integrates with Exchange Server 2013/Exchange Server 2010 and SharePoint Server 2013/SharePoint Server 2010 on-premises via the RMS connector	●	●
Administrators can create departmental templates	●	●
Organizations can create and manage their own RMS tenant key in a hardware security module (the Bring Your Own Key solution)	●	●
Supports non-Office file formats: Text and image files are natively protected; other files are generically protected	●	●
RMS SDK for all platforms: Windows, Windows Phone, iOS, Mac OSX, and Android	●	●
Integrates with Windows file servers for automatic protection with FCI via the RMS connector		●
Users can track usage of their documents		●
Users can revoke access to their documents		●

Secure collaboration with RMS

Share internally and externally



Secure collaboration with RMS



- Recipient email: john@vendor.com
- Expiration: 5 days
- Email notifications
- Permissions: Read only

john@vendor.com
.....

sarah@vendor.com
.....

Conditional Access

SharePoint admin center

site collections

infopath

user profiles

bcs

term store

records management

search

secure store

apps

sharing

settings

configure hybrid

device access

Restrict access based on device or network location

These settings apply to content in SharePoint, OneDrive and Office 365 groups.

Control access from devices that aren't compliant or joined to a domain

This setting requires Intune and Azure Active Directory premium subscriptions.

To allow limited, web-only access

1. Go to [Microsoft Azure portal](#) and add two policies. [Learn how to set conditional access policies in Azure AD.](#)
 - a. Create a policy for SharePoint that applies to mobile apps and desktop clients, and allows access only from compliant or domain-joined devices.
 - b. Create another policy for SharePoint that applies to web browsers, and select "use app-enforced restrictions."
2. Select the appropriate SharePoint enforced restriction
 - Allow limited access (web-only, without the Download, Print, and Sync commands)

To block access

Go to [Microsoft Azure portal](#) and add a new policy for SharePoint that applies to web browsers, mobile apps, and desktop clients. Configure the policy to allow access only from compliant or domain joined-devices. [Learn how](#)

Control access from apps that don't use modern authentication

The setting applies to third party apps and Office 2010 and earlier.

Allow

Control access based on network location

- Only allow access from specific IP address locations

Allowed IP addresses

Use commas to separate IP addresses and address ranges. For example: 172.160.0.0, 192.168.1.0/16, 2001:4798:80e8:8::290. Make sure you include your current IP address and that IP addresses don't overlap.



Microsoft Operations Management Suite (OMS)



Overview

Feedback



Log Search

My Dashboard

Solutions Gallery

13 GB Usage

AD Assessment

1 Servers Assessed
on Tue Feb 02 2016

3 High Priority Recommendations

5 Low Priority Recommendations

104 Passed Checks



Malware Assessment



0 Servers with Active Threats
33 Servers with Inadequate



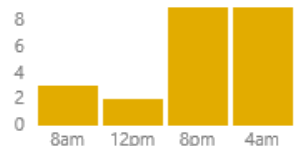
Backup ContosoTier1-backupvault



Alert Management

0 Active critical alerts in the last 24 hours

23 Active warning alerts in the last 24 hours



Automation OMSAutomationdemo

—

Runbooks

—

Jobs in the last 7 days



Capacity Planning



Take aways

- Office 365 has more in built security than people realise
- The more advanced plans provide more security options
- Can extend Office 365 security further with the likes of Azure and Intune
- More security features being added all the time
- Look at building services and revenue from additional security and compliance features
- Azure offers even more security and monitoring opportunities

Resources

- Office 365 Service Descriptions - <https://technet.microsoft.com/en-us/library/office-365-service-descriptions.aspx>
- Office 365 E5 - <https://products.office.com/en-us/business/office-365-enterprise-e5-business-software>
- Office 365 Trust Center - <https://www.microsoft.com/en-us/trustcenter/cloudservices/office365>
- Office 365 Compliance - <https://technet.microsoft.com/en-au/library/office-365-compliance.aspx>
- Customer Lockbox requests - <https://support.office.com/en-us/article/Office-365-Customer-Lockbox-Requests-36f9cdd1-e64c-421b-a7e4-4a54d16440a2>
- Overview of DLP policies - <https://support.office.com/en-us/article/Overview-of-data-loss-prevention-policies-1966b2a7-d1e2-4d92-ab61-42efbb137f5e>

Resources

- Document Tracking - <http://blogs.technet.com/b/rms/archive/2015/05/04/doctracking.aspx>
- Azure RMS Document tracking and revocation - <https://channel9.msdn.com/Series/Information-Protection/Azure-RMS-Document-Tracking-and-Revocation>
- Protect a file that you share by email by using the Rights Management sharing application - [https://technet.microsoft.com/en-us/library/dn574735\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dn574735(v=ws.10).aspx)
- Azure RMS Core Skills - <https://mva.microsoft.com/en-US/training-courses/azure-rights-management-services-core-skills-10500>
- Use Secure files to improve sharing - <https://mva.microsoft.com/en-US/training-courses/use-secure-files-to-improve-sharing-with-customers-and-partners-14042>
- Threat Intelligence for Office 365 - <https://www.youtube.com/watch?v=krFAjlkD66M>

This presentation is at

<https://doc.co/7i2447>

CIAOPS Resources



- Blog – <http://blog.ciaops.com>
- Free SharePoint Training via email – <http://bit.ly/cia-gs-spo>
- Free Office 365, Azure Administration newsletter – <http://bit.ly/cia-o365-tech>
- Free Office 365, Azure video tutorials – <http://www.youtube.com/directorciaops>
- Free documents, presentations, eBooks – <http://docs.com/ciaops>
- Office 365, Azure, Cloud podcast – <http://ciaops.podbean.com>
- Office 365, Azure online training courses – <http://www.ciaopsacademy.com>
- Office 365, Azure eBooks – <http://www.ciaops.com/publications>

[Twitter](#)
@directorcia

[Facebook](#)
<https://www.facebook.com/ciaops>

[Email](#)
director@ciaops.com

[Skype for Business](#)
admin@ciaops365.com