Understanding and Leveraging Microsoft's Enterprise Mobility + Security Suite (EMS)

@spmcdonough on Twitter (for heckling purposes)

Sean P McDonough
Microsoft MVP (Office Development, Office Servers and Services)
National Office 365 Solution Manager
Cardinal Solutions Group

MVP
Microsoft®
Most Valuable Professional

About Cardinal

Founded in 1996
Cincinnati Ohio

350+ FTEs
$50M+ Revenue

Cincinnati
Columbus
Charlotte
Raleigh
Tampa

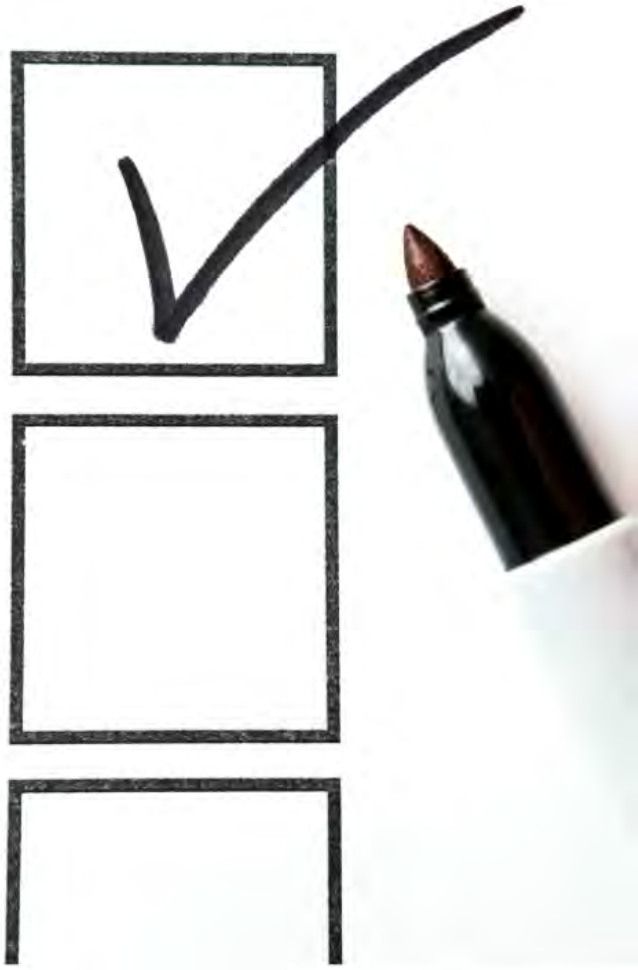
Mobile
Portals & Collab
UXD
Application Dev
WEM
BI

Agile Coaching
Business Analysis
Project Management

cardinal

Our Agenda

- Why I'm Doing This
- An Overview of EMS
- Individual EMS Workloads
- Putting Together Solutions
- Questions & Answers
- References



Why

Let's start with a simple question:

How many of you had heard of EMS prior to this session?

Okay, now how many of you really know what EMS is?

Really know what EMS is.

In my experience, plenty of people have heard of EMS.

Microsoft has been talking about it A LOT

Very few people know exactly what it is or does, though.

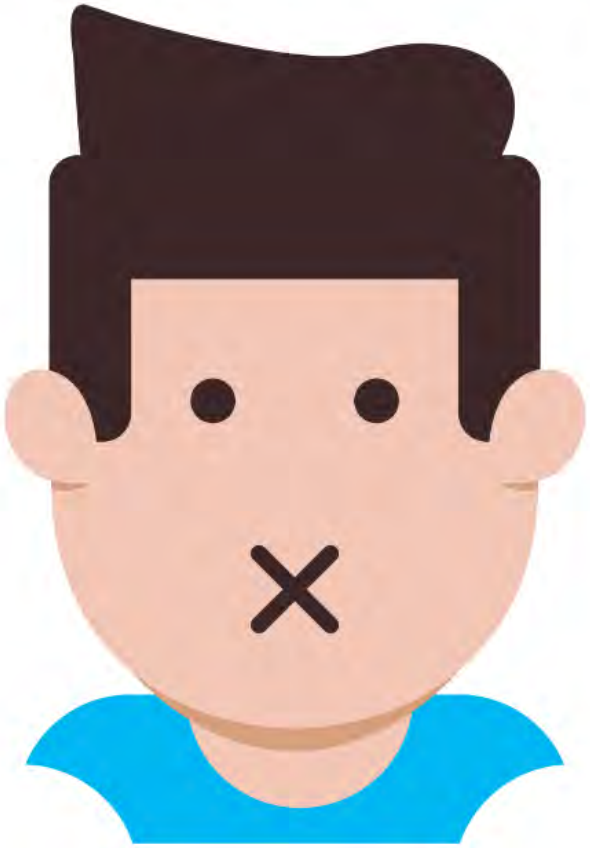
A couple of things

what it is or does, though.

A couple of things complicate the discussion, as well

- There is significant overlap between how EMS is positioned next to Office 365
- The EMS feature set is a fast moving target; it's capabilities keep changing

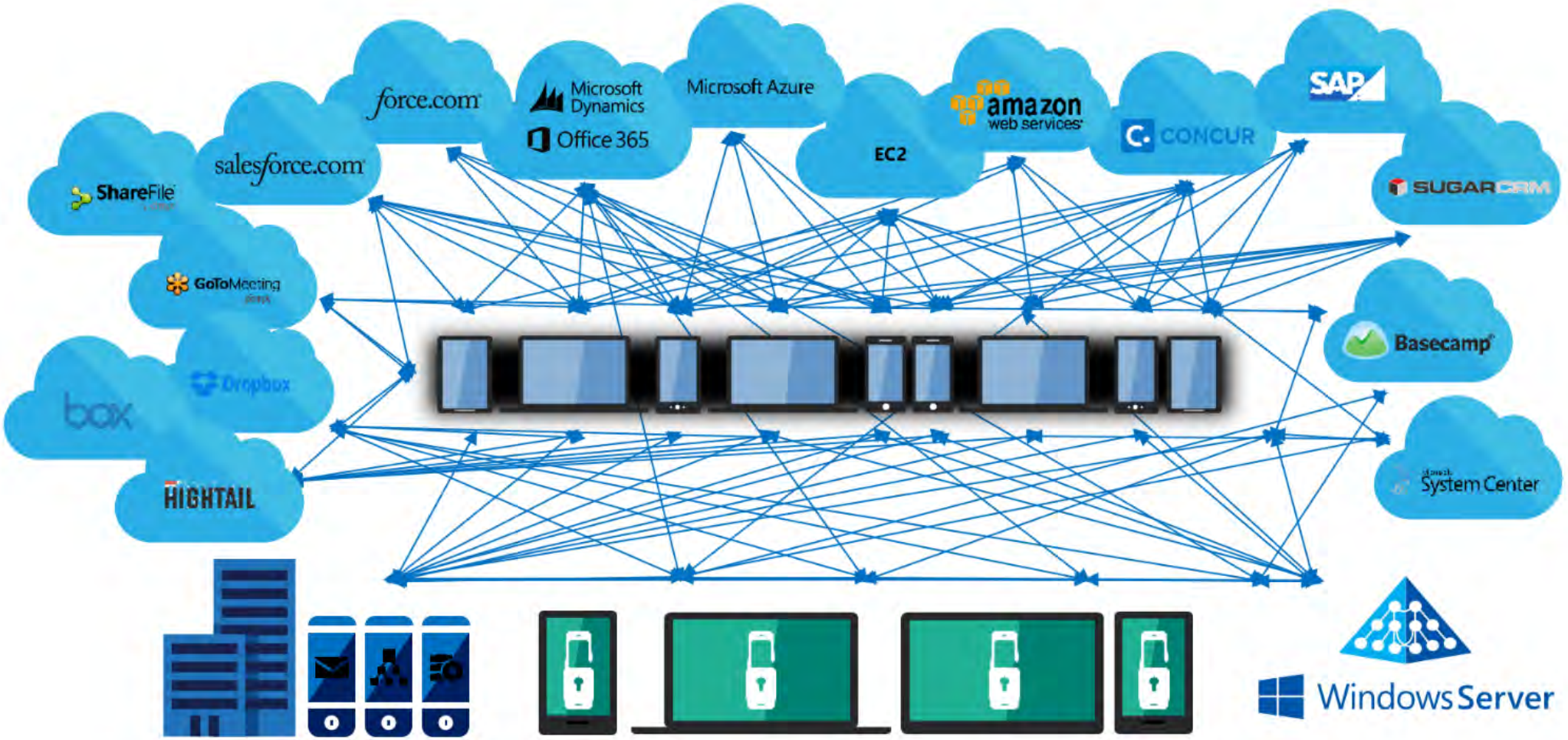
My Goal



To give you real, usable information on how to better leverage Office 365 (which you probably already have) and understand when and where you would need to step-up to EMS

Employees in Large Fi

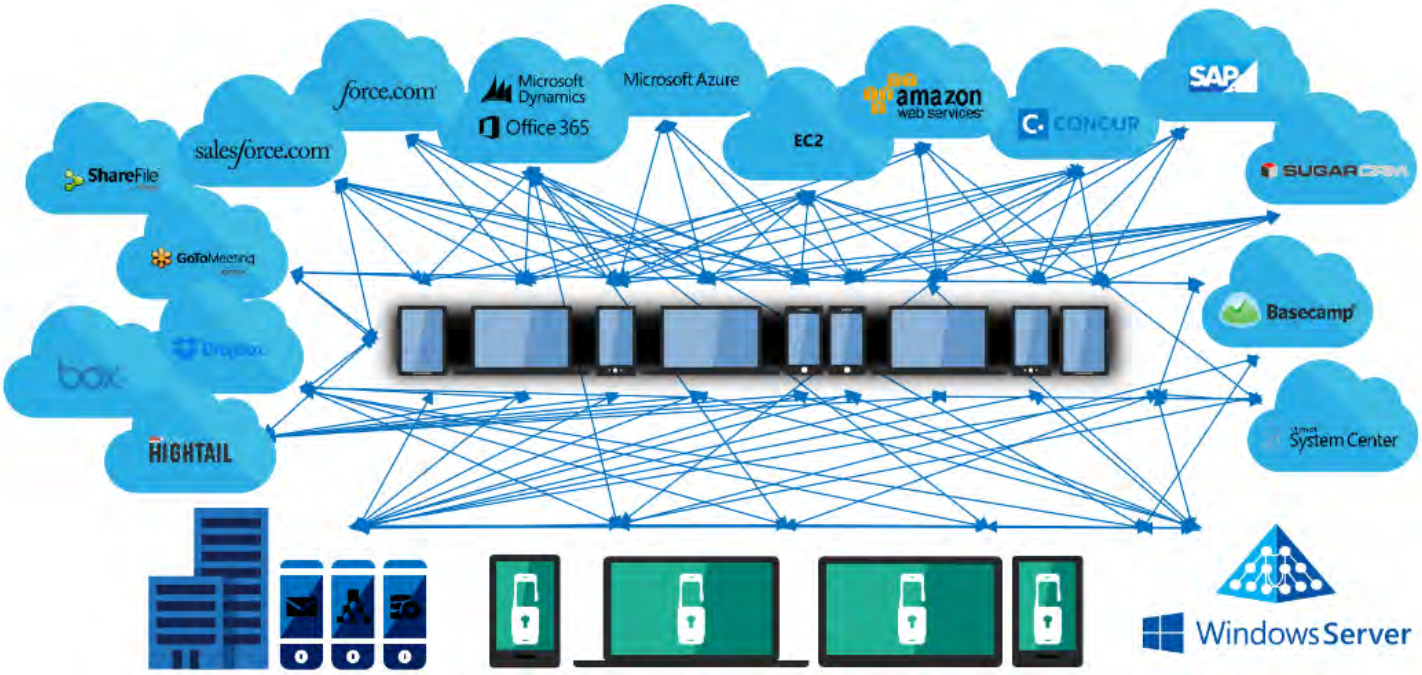
Our modern reality with devices, data, and services



nlighted by this diagram

Employees in Large En

Our modern reality with devices, data, and services



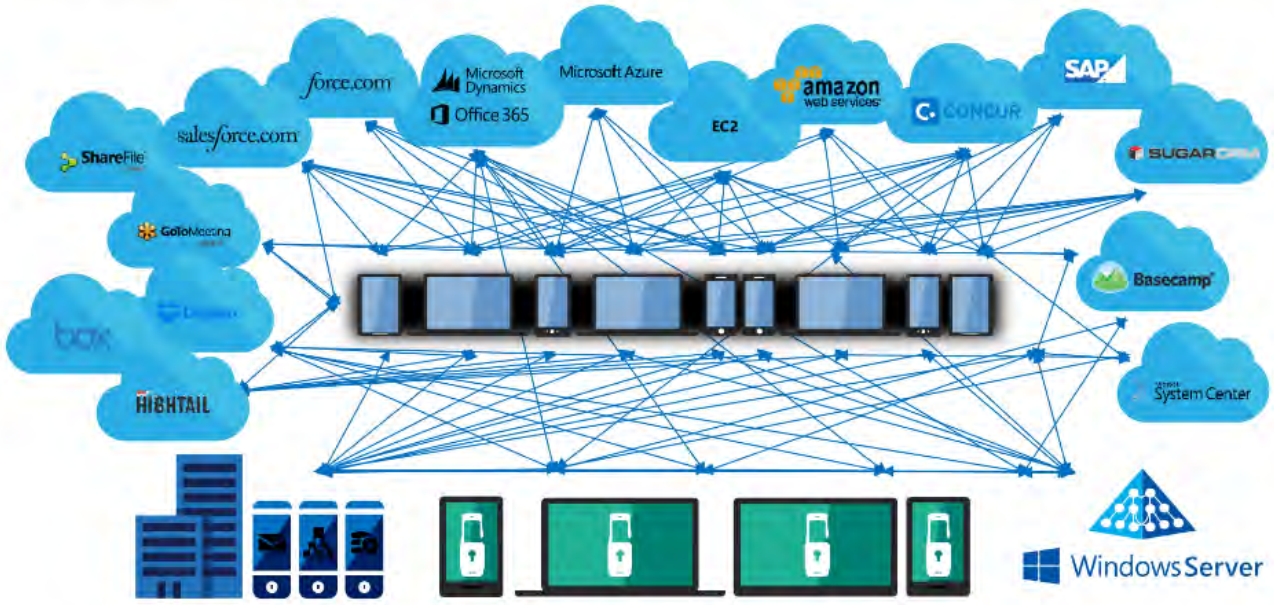
Two truths highlighted by this diagram

- These days, we are hyperconnected across a variety of devices and services
- If you're in IT, security in this type of environment can be an extreme challenge

According to a Gartner study of U.S. Employees in Large Enterprises

- 40% use their personal devices for work purposes
- households average two or more devices
- online banking and purchasing are in the top three activities done on desktop or laptop

Our modern reality with devices, data, and services



nlighted by this diagram

berconnected across a variety of devices and services

Combined with c

terprises

- 40% use their personal devices for work purposes
- households average two or more devices
- online banking and purchasing are in the top three activities done on desktop or laptop

- 80% use non-approved SaaS applications in their jobs
- Nearly 35% of all SaaS applications used in enterprises are not approved
- On average, 15 percent of users have had security, access, or liability events while using SaaS apps

Combined with data from McAfee, the security and related implications are alarming.

Your employees are impacted

laptop

security, access, or liability events while using SaaS apps

Combined with data from McAfee, the security and related implications are alarming.

Your employees are impacted

... but by extension, you are also impacted by

Your business partners

Your customers

Your customers

Bringing this discussion back to EMS

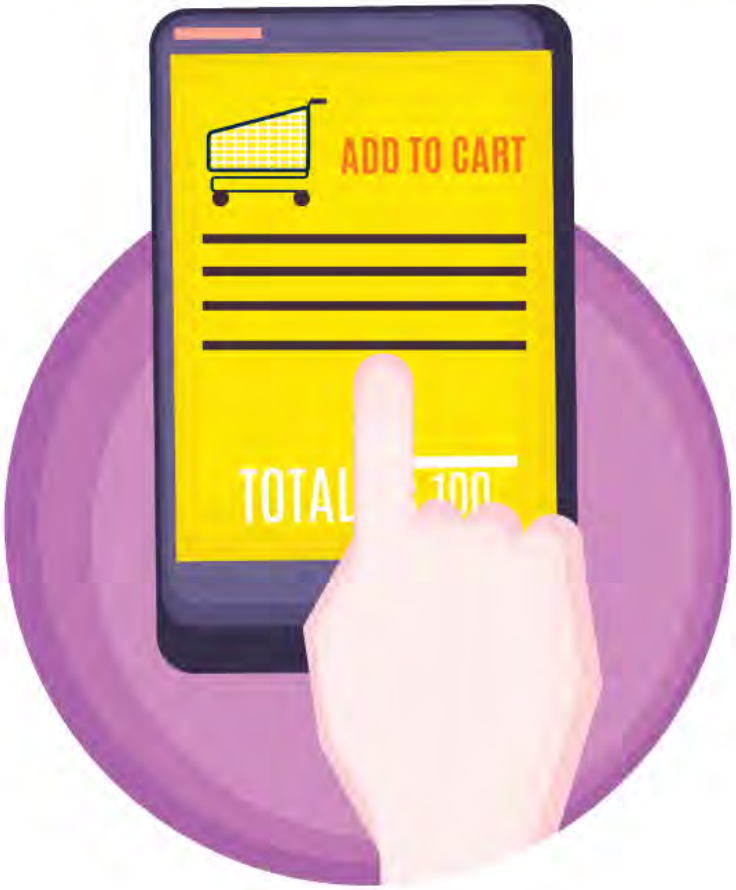
At it's core, EMS is about security

- Enhancing existing identity security
- Strengthening device security
- Protecting data, not just systems
- Extending security to on-premises systems

It's also about convenience

- Extending security to on-premises systems

It's also about convenience



- Can be used to simplify SSO to cloud-based and on-premises systems
- Maximum capability with minimum config
- Natural complement to Office 365

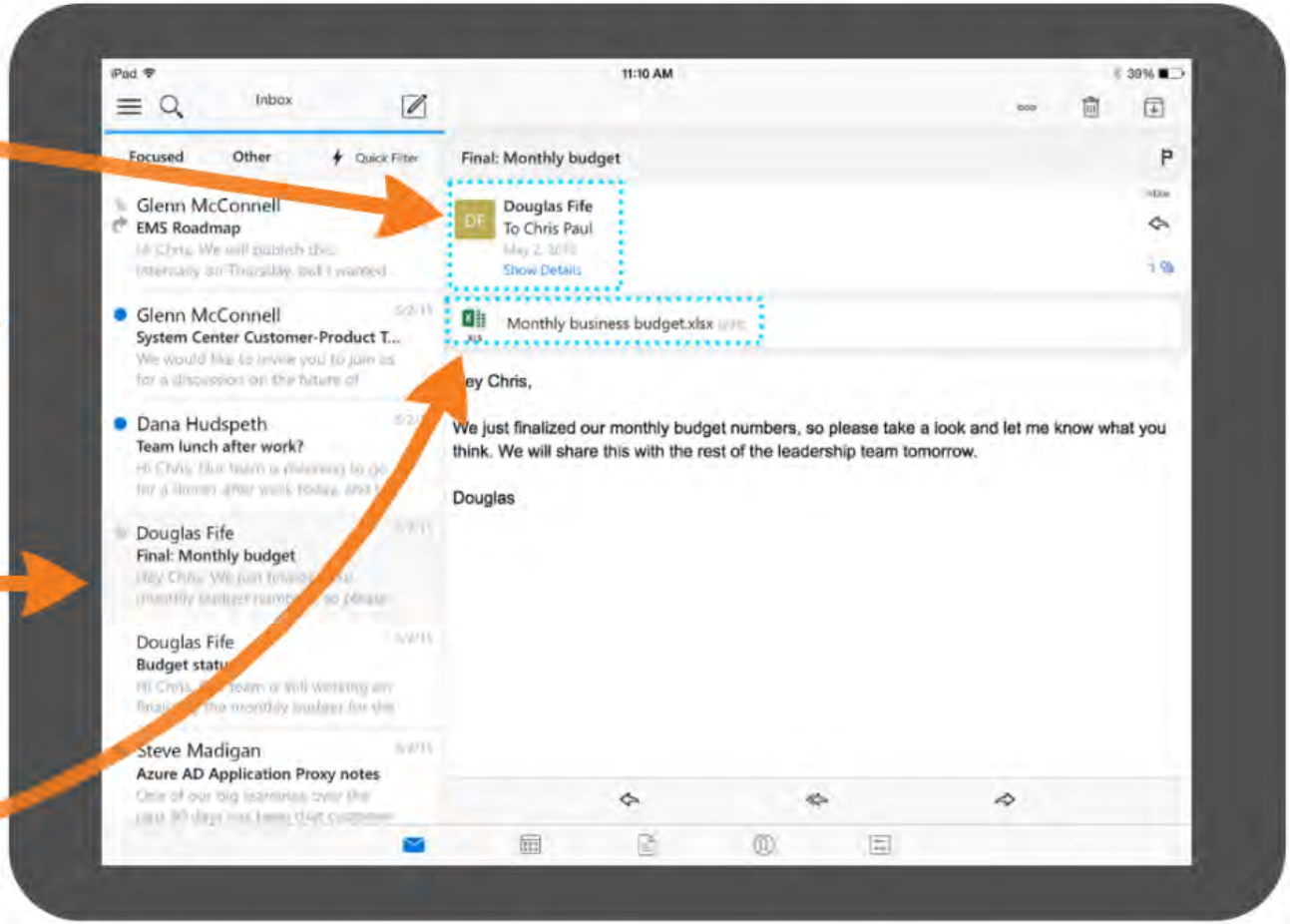
EMS and multi-axis protection

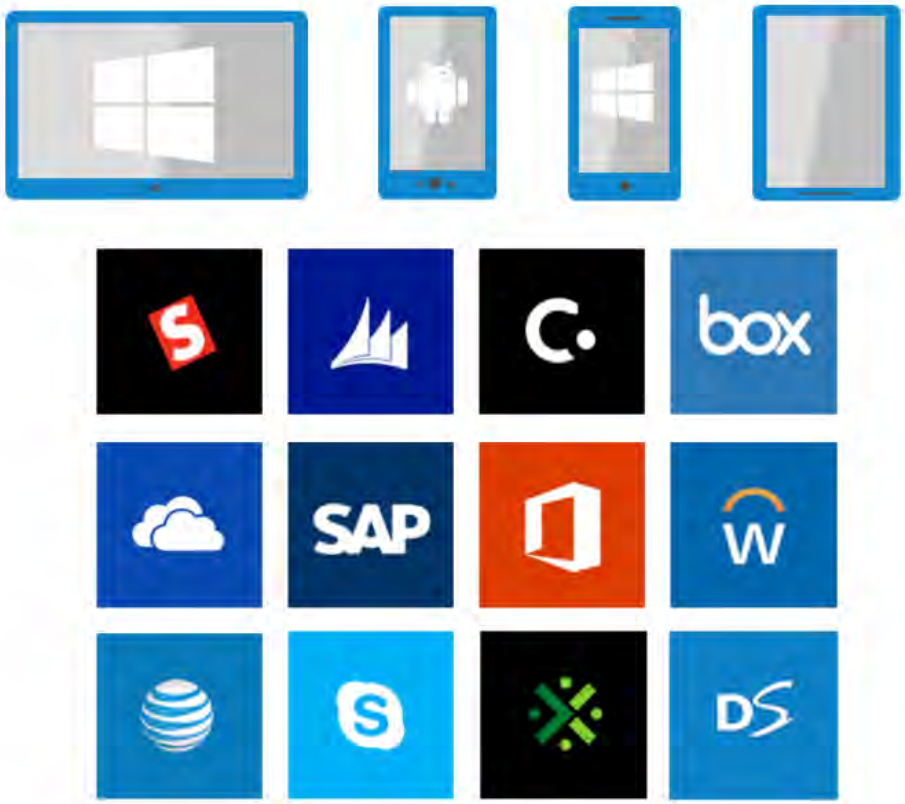
Identity

Device

Application

Data





- iOS, Android, and Windows devices
- thousands of Software as a Service (Saas) apps
- Line-of-business (LOB) apps, RemoteApp

protection that goes cross-platform

At the end of the day, though the best part of EMS is this:

It simply works and complements Office 365 nicely

start by acknowledging that this is something of a trick que

So ... what's in EMS?

Let's start by acknowledging that this is something of a trick question.

So ... what's in EMS?

Azure Active Directory Premium

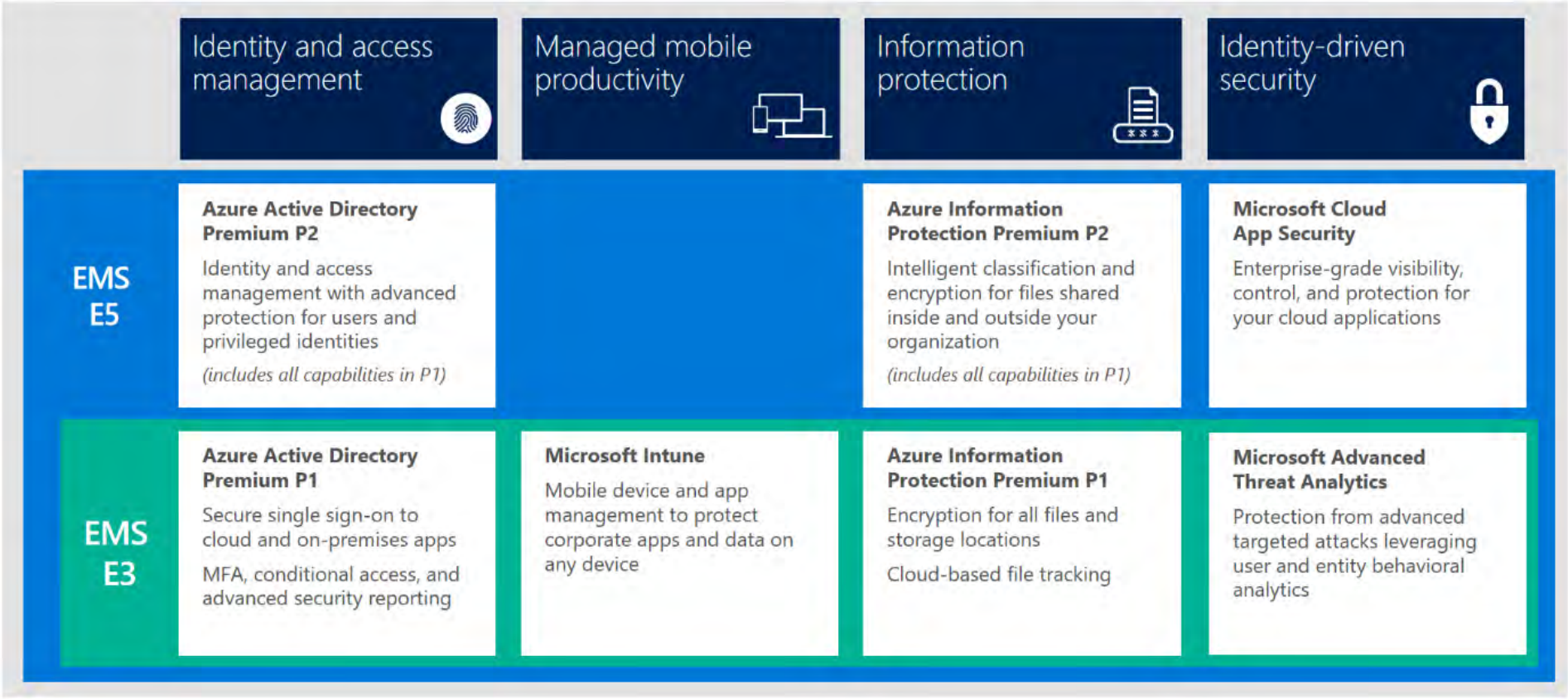
Intune

Azure Rights Management Premium

Advanced Threat Analytics

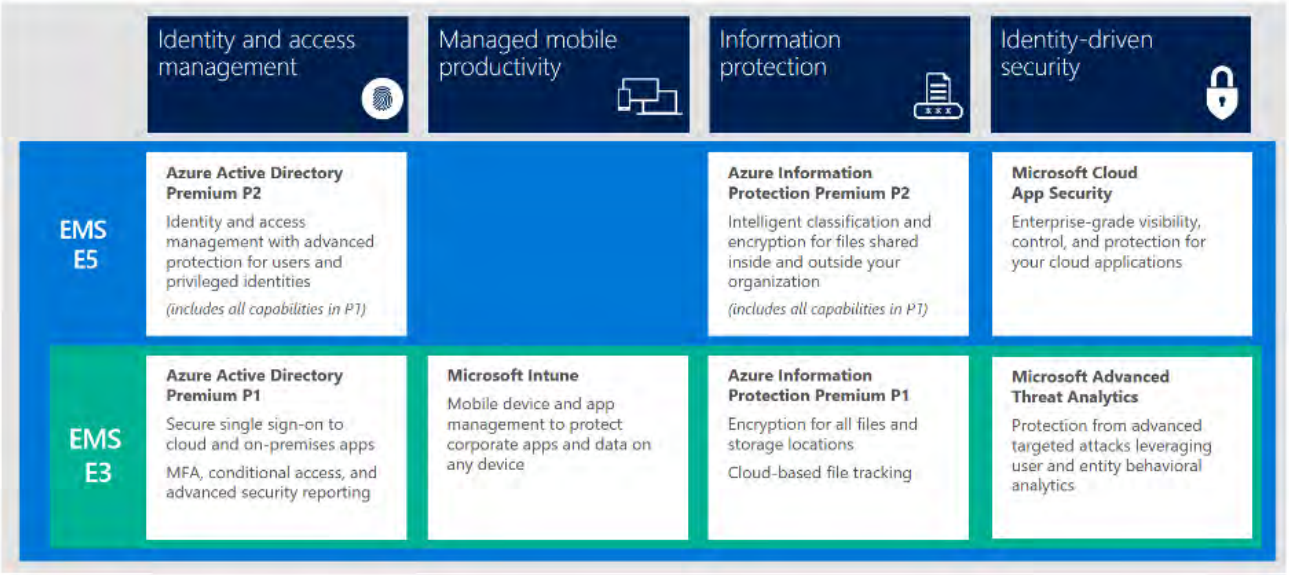
All EMS subscriptions include these four workloads. EMS E5 has some others.

Of course, too many of us were starting to understand the offering, so, Microsoft is pulling a change-up



EMS has become "Enterprise Mobil

f course, too many of us were starting to understand
he offering, so, Microsoft is pulling a change-up



Cliff Notes for the changes that just got here

EMS has become "Enterprise Mobility + Security" rather than "Enterprise Mobility Suite"

- existing EMS capabilities have become EMS E3

An EMS E5 is now available

- E5 includes Cloud App Security, AAD identity protections, and more

Azure Active Directory Premium

Intune

Azure Rights Management Premium

Advanced Threat Analytics

All EMS subscriptions include these four workloads. EMS E5 has some others.

Azure Active Directory: identity controls everything

- Password management
- Password reset
- Group Management

AADConnect to synchronize users

Self-service capabilities

Single sign-on (SSO) to services

Username

Windows Server Active Directory

Other Directories

On-Premises

Azure Active Directory

Cloud Services & Systems

Connector

- All requests originate internally - no "drill in" from the outside

Application Proxy

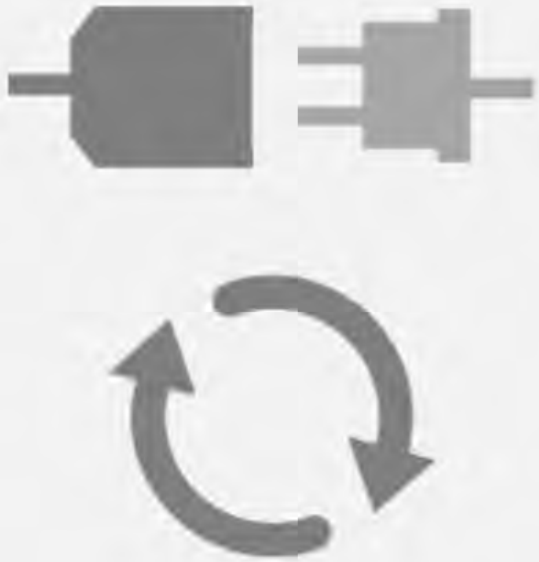
- Microsoft takes care of keeping external entry points up-to-date with security

- Currently there is a gallery of over 2600 SaaS applications preconfigured for your use.
- Many common applications

AADConnect to synchronize users

Windows Server Active Directory

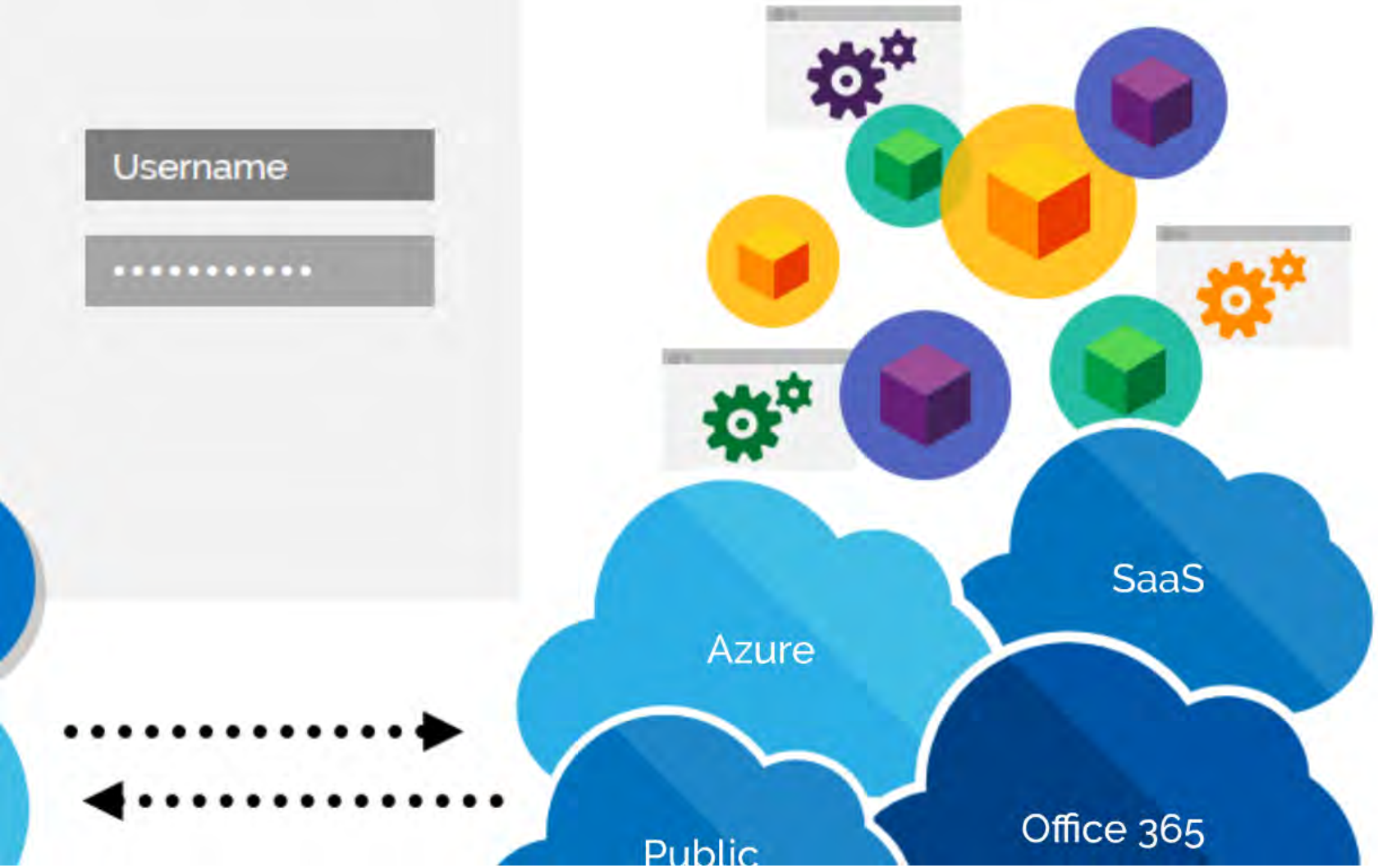
Other Directories



reset

ment

Single sign-on (SSO) to services



APPLICATION GALLERY

Management

Connect to
hronize users

Self-service
capabilities

Single sign-
(SSO) to ser

Azure Active Directory: identity controls everything

- Password management
- Password reset
- Group Management

AADConnect to synchronize users

Self-service capabilities

Single sign-on (SSO) to services

Username

Windows Server Active Directory

Other Directories

On-Premises

Azure Active Directory

Cloud Services & Systems

Connector

- All requests originate internally - no "drill in" from the outside

Application Proxy

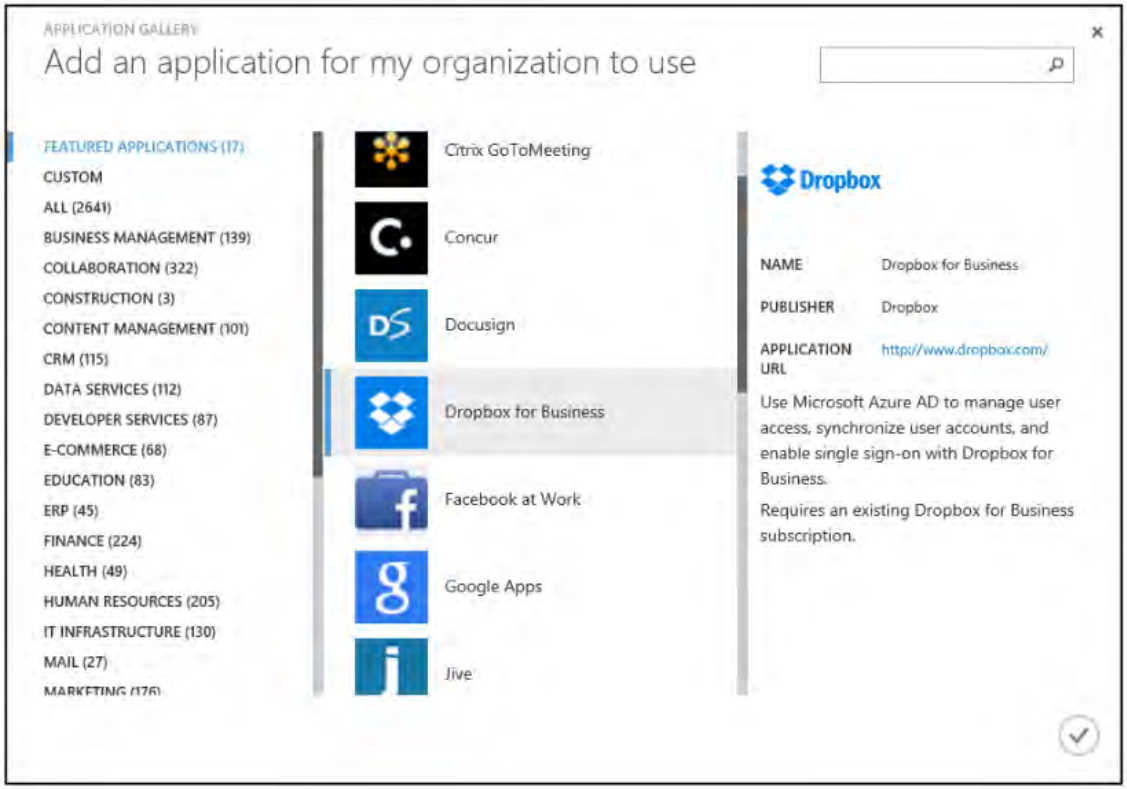
- Microsoft takes care of keeping external entry points up-to-date with security

- Currently there is a gallery of over 2600 SaaS applications preconfigured for your use.
- Many common applications

SSO Application Support

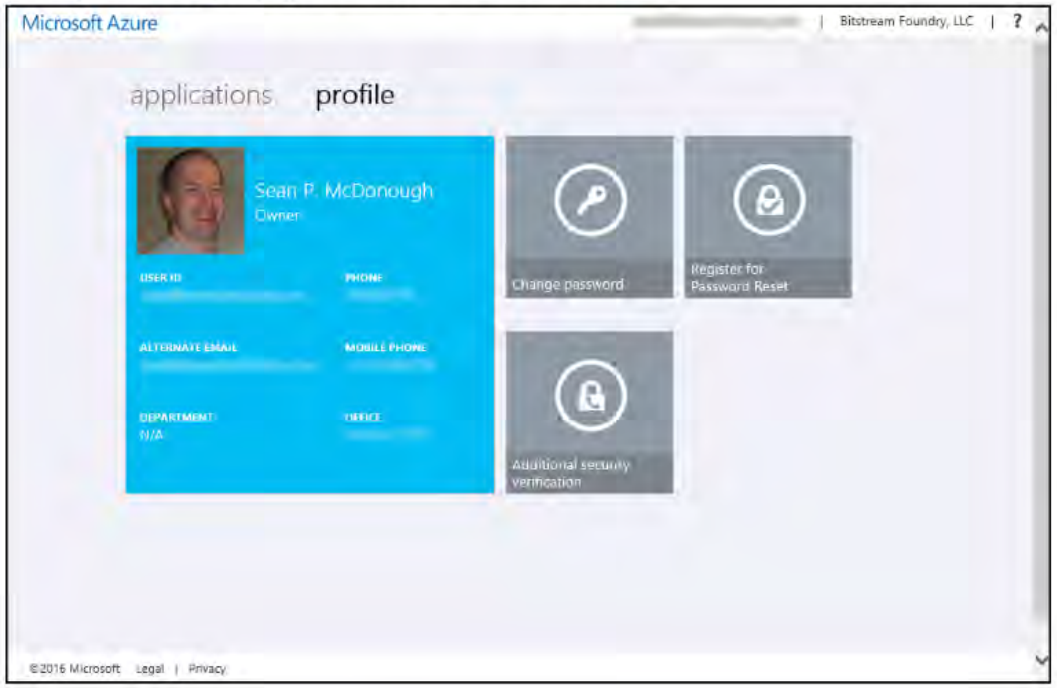
Cloud Services & Systems

- Currently there is a gallery of over 2600 SaaS applications preconfigured for your use.
- Many common applications
  - Salesforce
  - WorkDay
  - Dropbox
  - GoToMeeting
  - Box
  - AvePoint Online
  - Concur
  - Google Apps



tory: Identity C

https://myapps.microsoft.com



- Password management
- Password reset
- Group Management

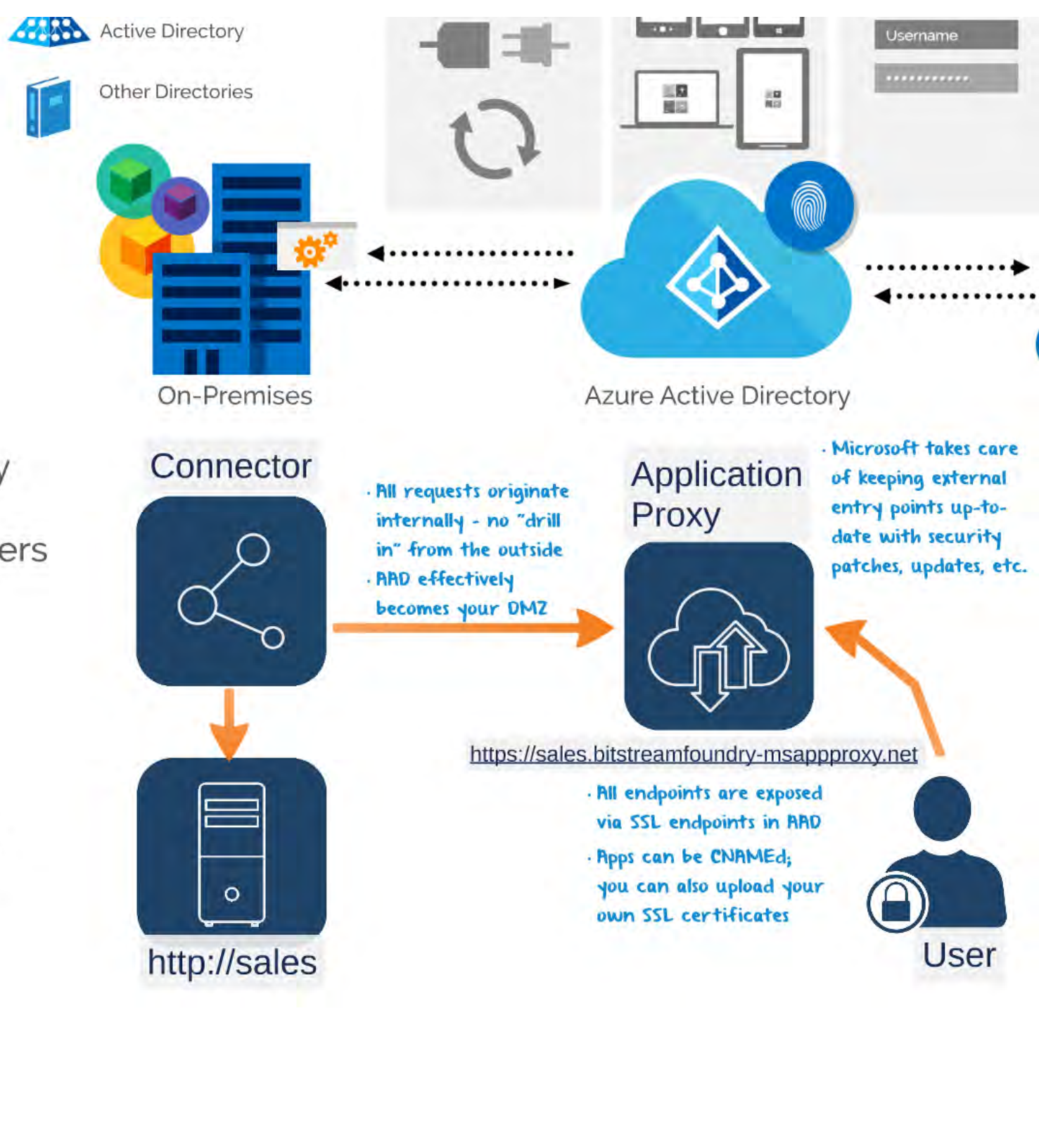
t to users

Self-service capabilities

Singl (SSO)

Exposing on-premises applications (like SharePoint)

- Deploy Azure App Proxy Connector to an on-premises server or servers
- Connector initiates connection to AAD
- Applications are configured in AAD
- Users connect through AAD to get to internal web endpoints



On-Premises

Azure Active Directory

Connector

- All requests originate internally - no "drill in" from the outside
- AAD effectively becomes your DMZ

Application Proxy

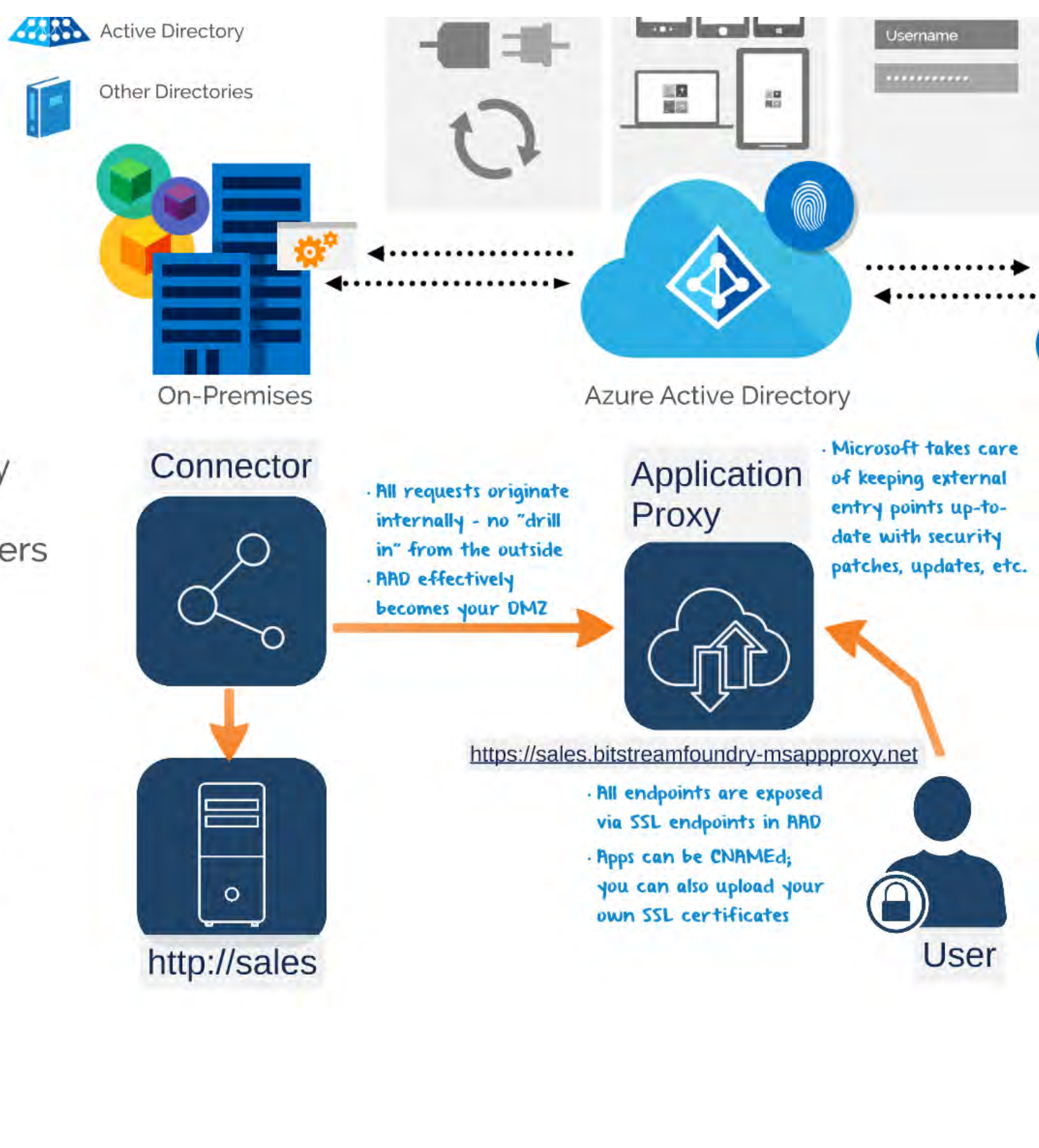
- Microso
of keep
entry p
date w
patches

https://sales.bitstreamfoundry-msappproxy.n

- All endpoints are exposed via SSL endpoints in AAD
- Apps can be CNAMEd;

Exposing on-premises applications (like SharePoint)

- Deploy Azure App Proxy Connector to an on-premises server or servers
- Connector initiates connection to AAD
- Applications are configured in AAD
- Users connect through AAD to get to internal web endpoints



Azure Active Directory

Application Proxy

- Microsoft takes care of keeping external entry points up-to-date with security patches, updates, etc.

/sales.bitstreamfoundry-msappproxy.net

- All endpoints are exposed

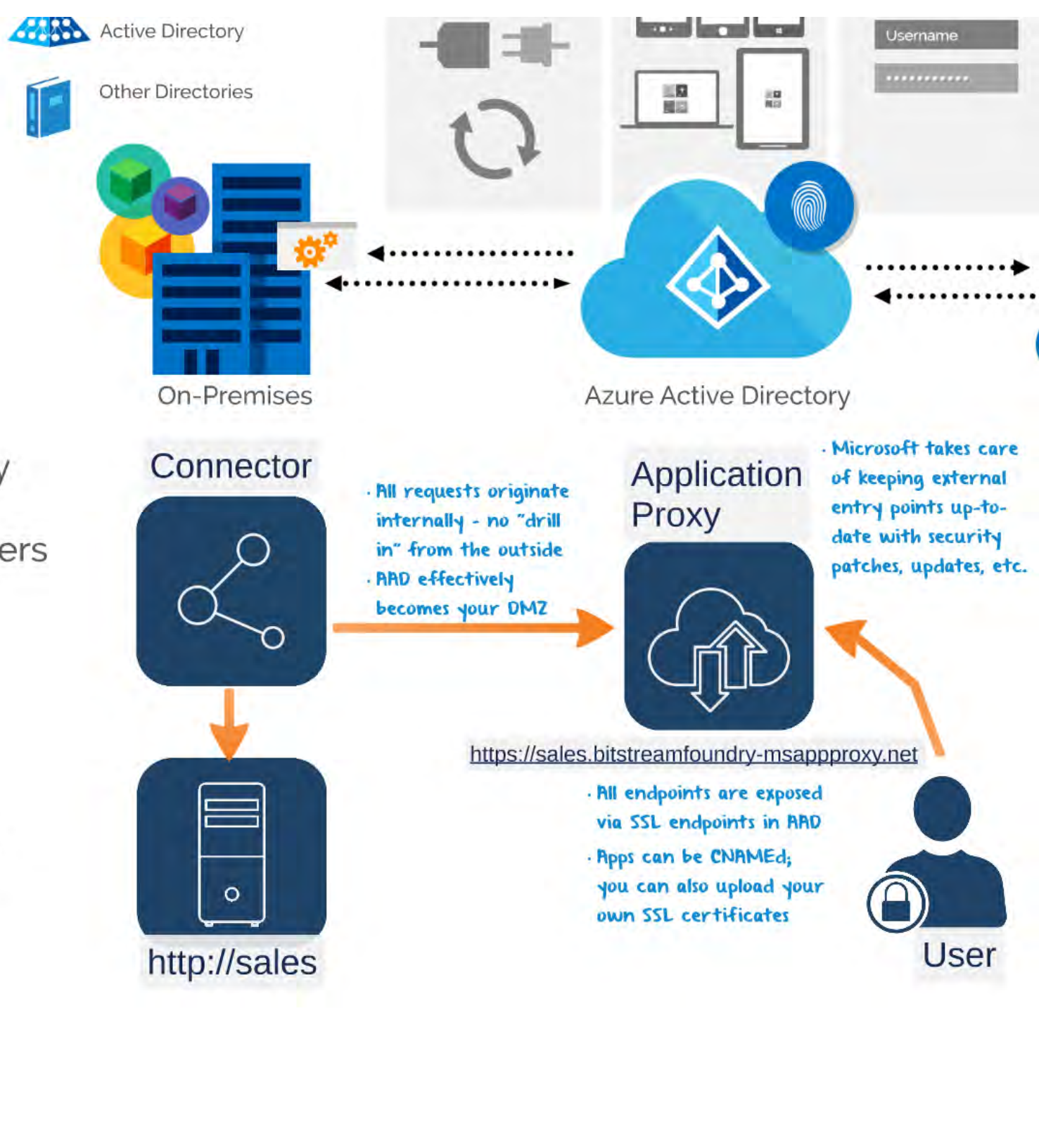
nate
drill
side
MZ

Clou

- Cur
  ove
  pre
- Mar
  - Sa
  - Wo
  - Dr
  - Go

Exposing on-premises applications (like SharePoint)

- Deploy Azure App Proxy Connector to an on-premises server or servers
- Connector initiates connection to AAD
- Applications are configured in AAD
- Users connect through AAD to get to internal web endpoints



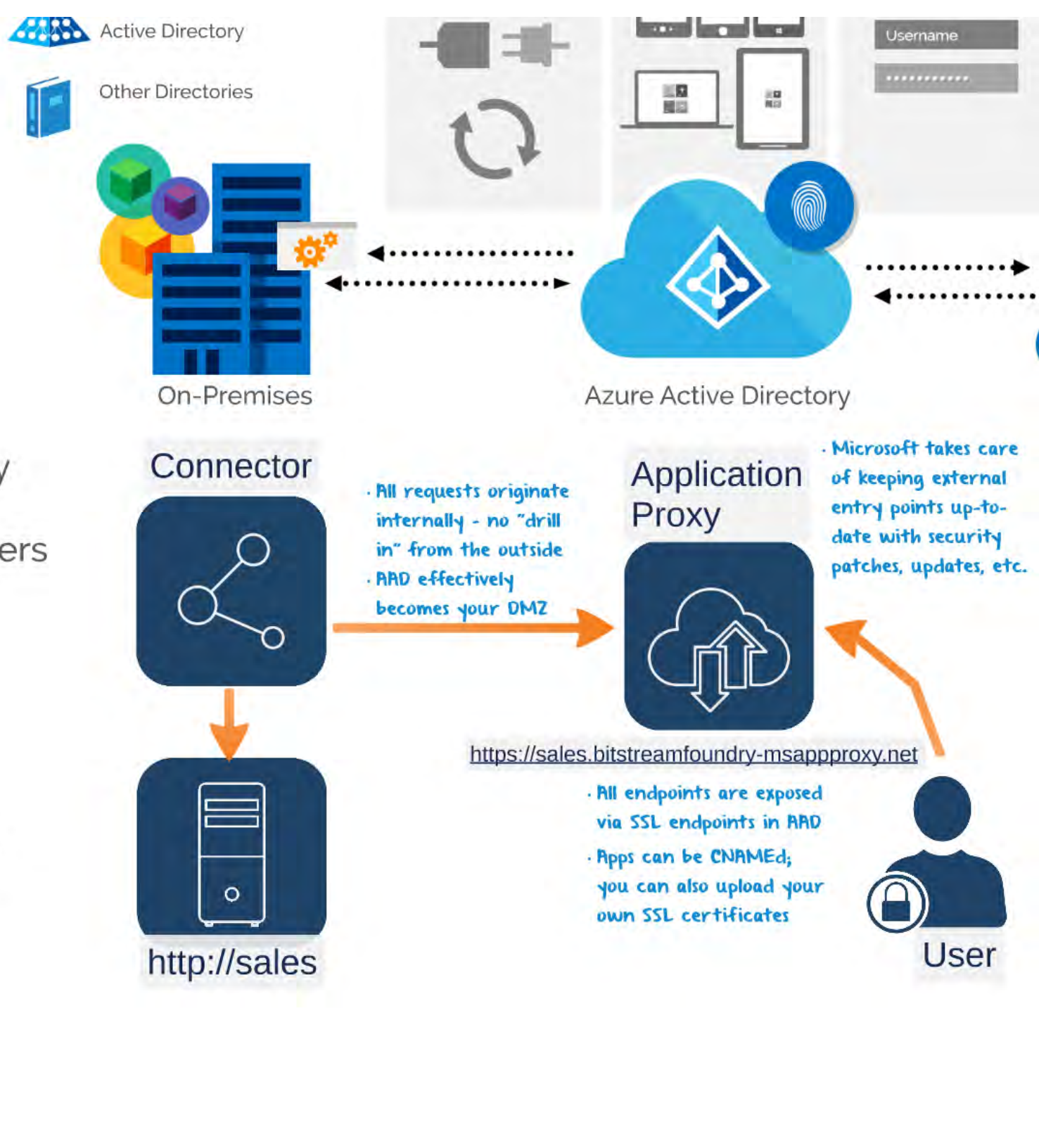
https://sales.bitstreamfoundry-msappproxy.net

- All endpoints are exposed via SSL endpoints in AAD
- Apps can be CNAMEd; you can also upload your own SSL certificates

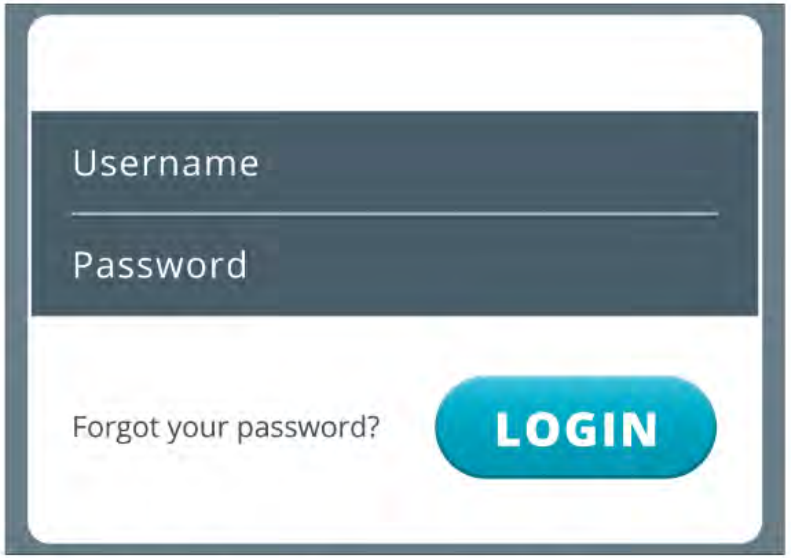
User

Exposing on-premises applications (like SharePoint)

- Deploy Azure App Proxy Connector to an on-premises server or servers
- Connector initiates connection to AAD
- Applications are configured in AAD
- Users connect through AAD to get to internal web endpoints



Multi-Factor Authentication (MFA)

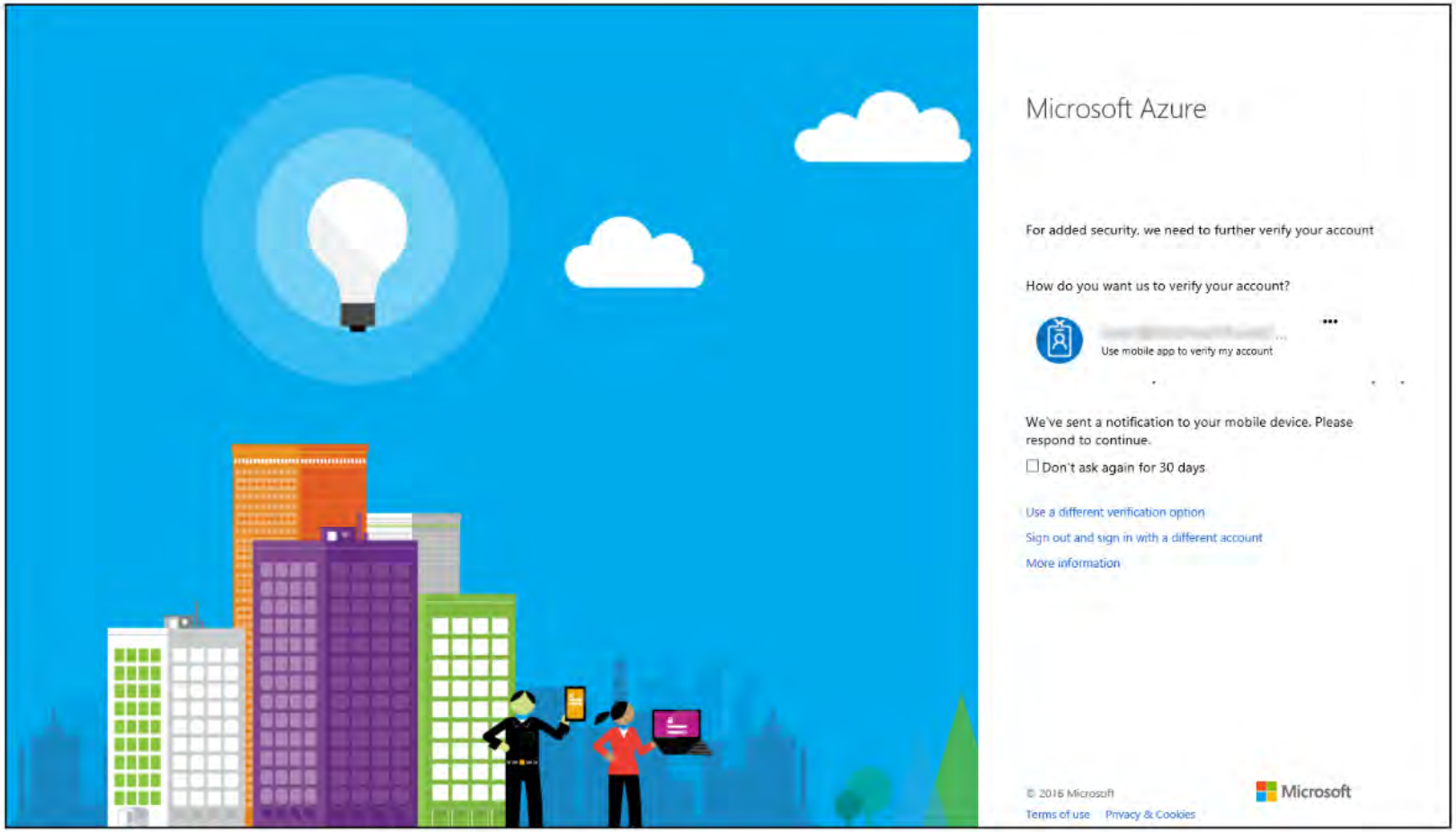


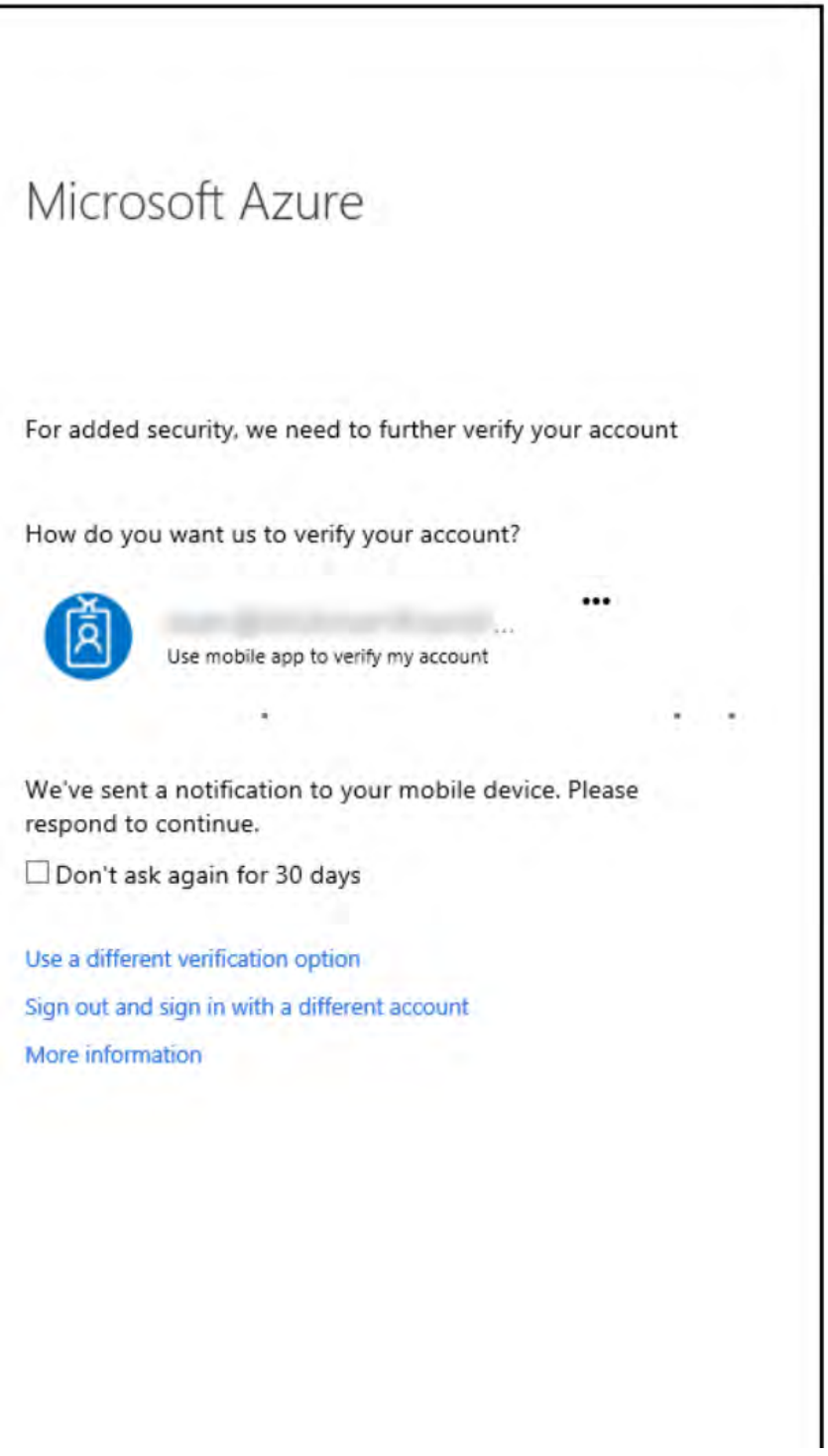
MFA is this ...

... plus something like a fingerprint, SMS message, etc.

When MFA is enabled, the sign-in experience changes a bit

When MFA is enabled, the sign-in experience changes a bit





I've signed in with my username and password, and now I'm being prompted for verification

premises environments)		✓
Service-level agreement (SLA)		✓
Forefront Identity Manager CAL + Forefront Identity Manager Server		✓

Why should I care about MFA?

- bottom line: if your username and password ever become compromised, your account will (probably) still be safe!

Azure Active Directory Version Comparison

	Azure AD (O365)	Azure AD Premium
Directory as a service	✓ Up to 500,000 objects	✓ No limit
User and group management	✓	✓
Single sign-on for pre-integrated SaaS and custom applications	✓ 10 apps per user	✓ No limit
Microsoft Directory Synchronization Tool (Windows Server Active Directory extension)	✓	✓
User-based access management and provisioning	✓	✓
Group-based access management and provisioning		✓
Self-service group management for cloud users		✓
Self-service password change for cloud users	✓	✓
Self-service password reset for cloud users		✓
Security reports	✓	✓
Advanced security reporting (based on machine learning)		✓
Usage reporting		✓
Company branding (logon pages and Access Panel customization)		✓
Multi-factor authentication (all available features on Windows Azure and on-premises environments)		✓
Service-level agreement (SLA)		✓
Forefront Identity Manager CAL + Forefront Identity Manager Server		✓

Why should I care about MFA?

MFA: Office 365 versus EMS

	MFA for O365/Azure Administrators	Windows Azure Multi-Factor Authentication / EMS
Administrators can Enable/Enforce MFA to end-users	✓	✓
Use Mobile app (online and OTP) as second authentication factor	✓	✓
Use Phone call as second authentication factor	✓	✓
Use SMS as second authentication factor	✓	✓
Application passwords for non-browser clients (e.g. Outlook, Lync)	✓	✓
Default Microsoft greetings during authentication phone calls	✓	✓
Custom greetings during authentication phone calls		✓
Fraud alert		✓
MFA SDK		✓
Security Reports		✓
MFA for on-premises applications/ MFA Server.		✓
One-Time Bypass		✓
Block/Unblock Users		✓
Customizable caller ID for authentication phone calls		✓
Event Confirmation		✓

Azure Active Directory Premium

Intune

Azure Rights Management Premium

Advanced Threat Analytics

All EMS subscriptions include these four workloads. EMS E5 has some others.

Intune: Mobile Device Management (MDM)

MDM Comparison between Office 365 and EMS

FREQUENTLY ASKED QUESTION

What is mobile device management?

- applying policies to require PINs, lock

What is mobile device management?

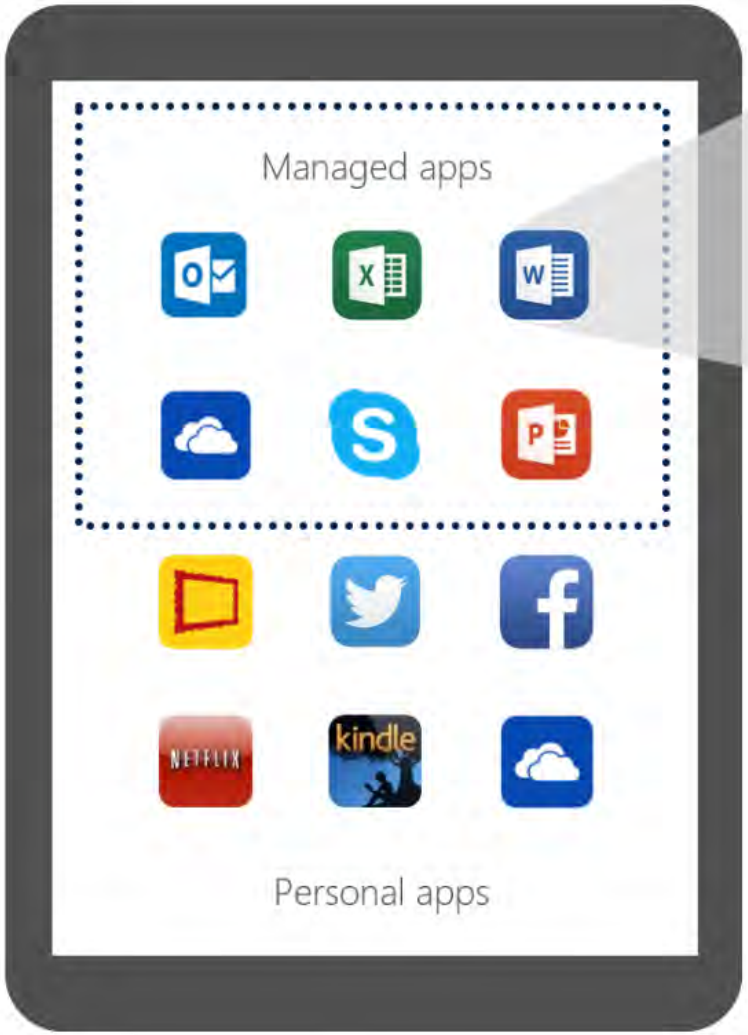
- applying policies to require PINs, lock devices after a period of time, etc.
- deploying and controlling corporate applications for business use
- having the ability to completely or selectively wipe lost or stolen devices
- configuring specific settings for VPN, wi-fi, email, certificates, and more

So, how does Intune "control" my device and protect corporate data?

- You begin by installing the Intune Company Portal from Google Play or the iTunes store.
- You sign into your cloud tenant from the Company Portal to link your device to your Intune configuration.
- Intune pulls down compliance policies, configuration polices, and other policy items.
- During this enrollment process, applications may also be installed. Apps can be installed later, as well. These are "managed apps."

Intune administrators control who

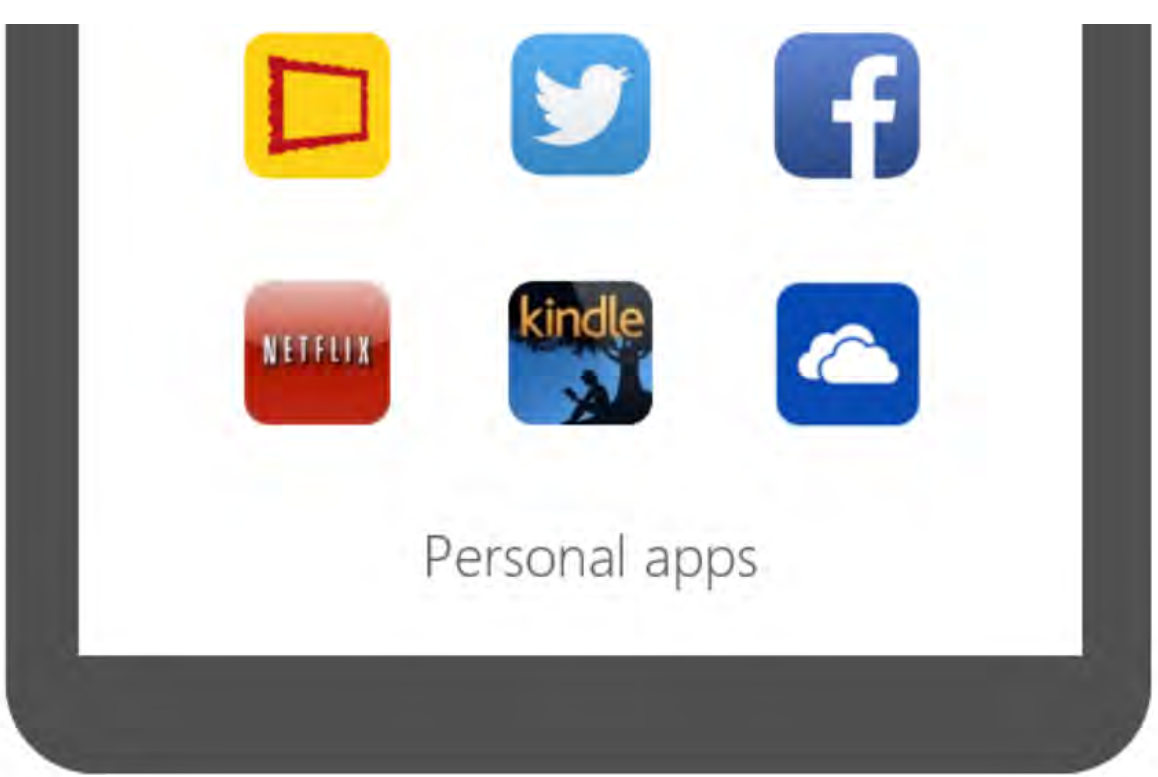
integration can safely span the persona
and managed data boundary



Dual-mode app with native Intune integration

- managed apps are special because they (and their data) live in a sandbox
- the sandbox is like a logical container for control of data flow and policy management

ne enrollment will not "mess

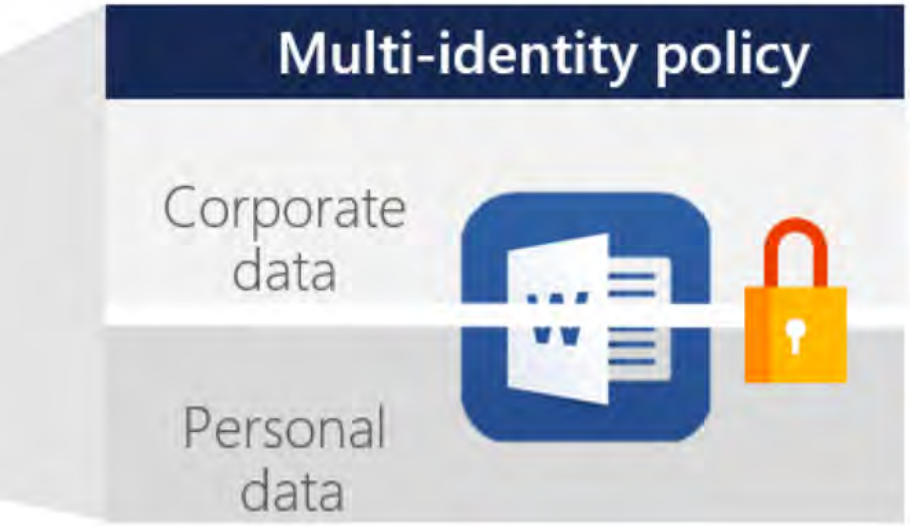


beca
live i

- the s
cont
flow

Intune enrollment will not "mess with" personal apps and data

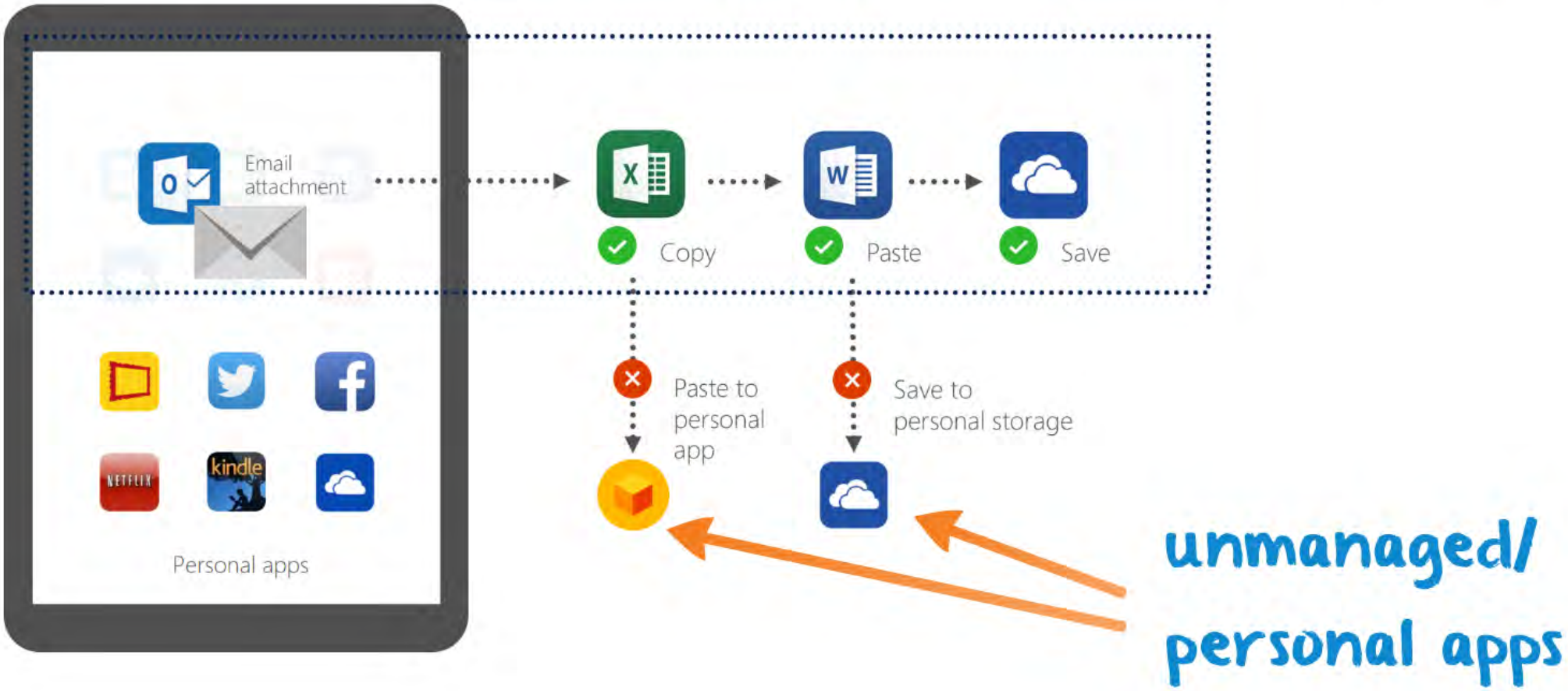
Apps that were written with Intune SDK integration can safely span the personal and managed data boundary



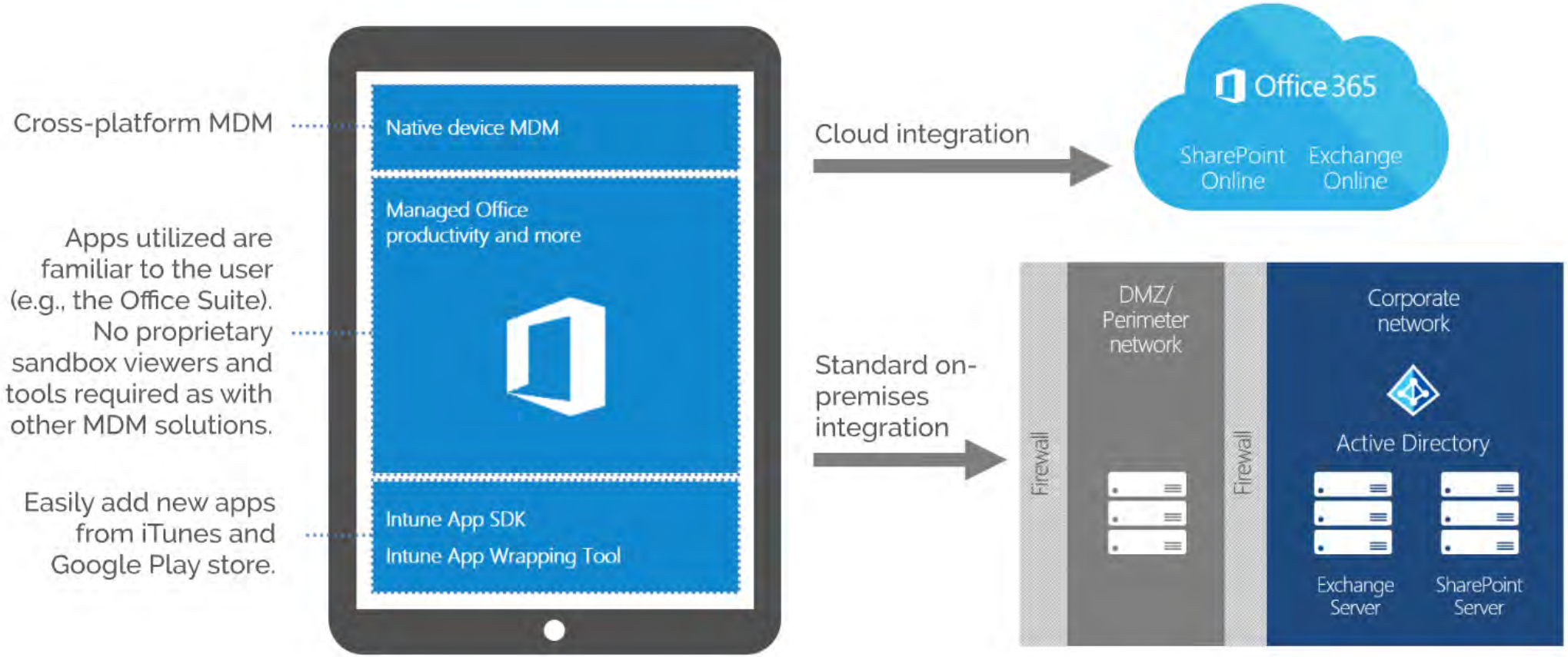
Dual-mode app with native Intune integration

- managed apps are special

Intune administrators control whether or not data can flow across managed/personal boundaries



Intune: Under the Hood



Intune versus other MDM solutions

- I believe in honest assessments
- Intune is not the market leader; Airwatch is the king
- "Organizations that should consider Intune are those that want to extend the Office 365 services to mobile devices and ConfigMgr customers that value client management and EMM integration over best-of-breed EMM functionality."

Figure 1. Magic Quadrant for Enterprise Mobility Management Suites

Source: Gartner (June 2015)

MDM Comparison between Office 365 and EMS

Category	Feature	Exchange ActiveSync	MDM for Office 365	Microsoft Intune (cloud only)	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 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, Image 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. Group Policy, login scripts, BitLocker management, virtual desktop and power management, custom reporting, etc.)				●
	Windows Server/Linux/UNIX/Mac OS X support				●
	OS deployment and imaging				●

Figure 1. Magic

Intune versus other

Azure Active Directory Premium

Intune

Azure Rights Management Premium

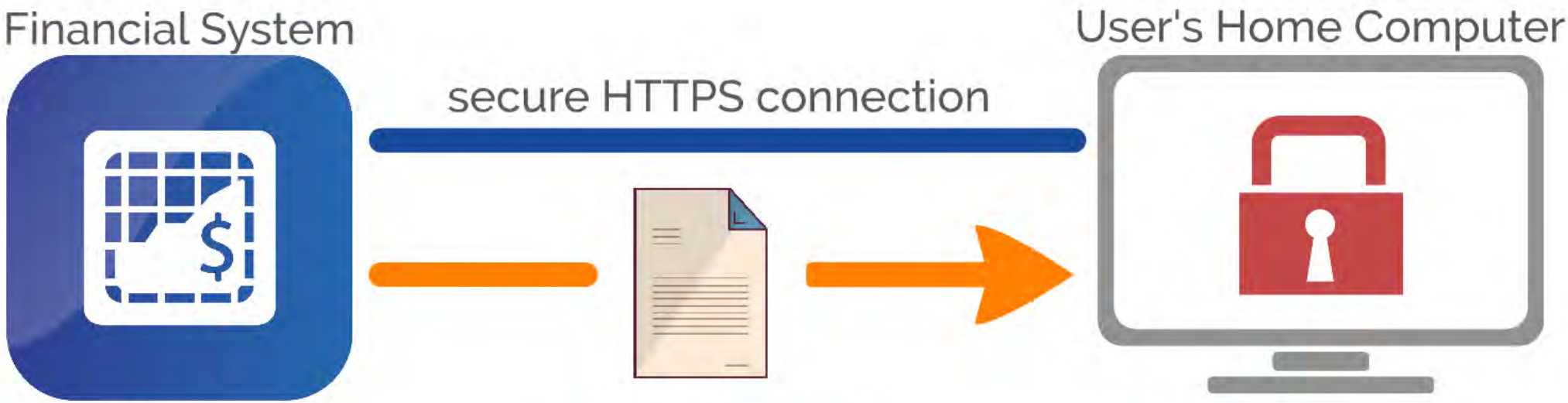
Advanced Threat Analytics

All EMS subscriptions include these four workloads. EMS E5 has some others.

Let's start with a simple question

What problem does RMS (Rights Management Service) solve?

Consider the following example where a user is accessing a corporate financial application



Once the data is on the user's

em

User

secure HTTPS connection

user downloads financial data

py

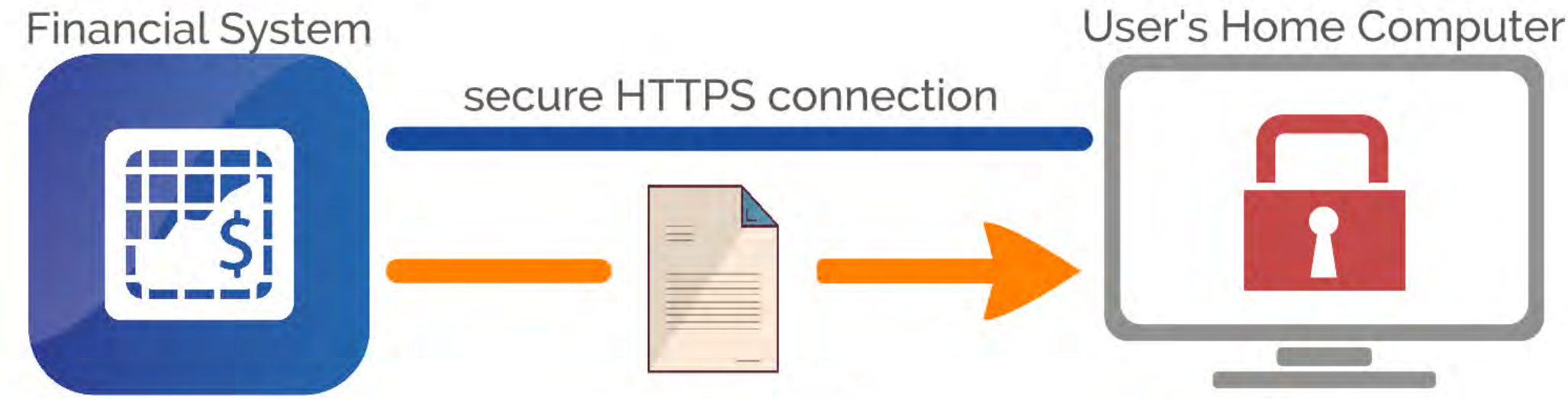
CLs, &

sms

no

co

is accessing a corporate financial application



Once the data is on the user's system, what is securing that data?

If you answered "the user's adherence to corporate policies regarding data usage and system security," then you're trying to apply a protection strategy I call ...

Abstract.docx - Word

This is where RM

If you answered "the user's adherence to corporate policies regarding data usage and system security," then you're trying to apply a protection strategy I call ...

s is where RMS comes in

This usually doesn't cut it in the real world

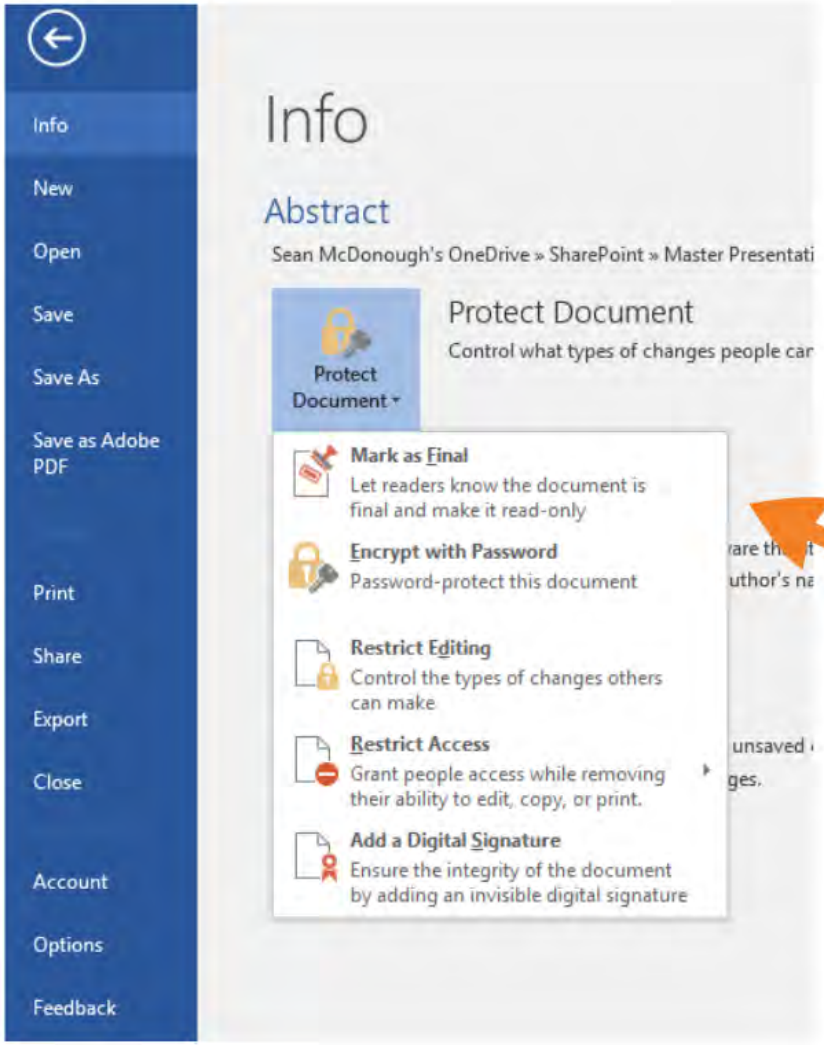
Users will not protect data the way that they should (or that you want them to)

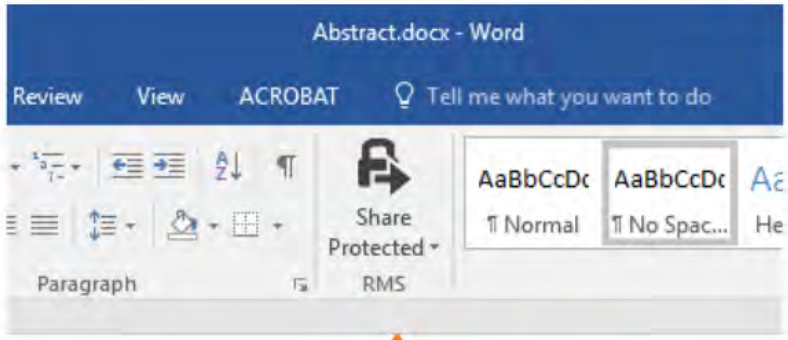
MS comes in

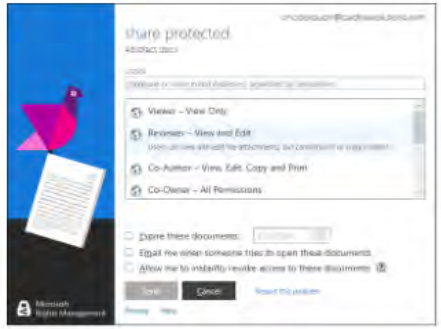
This is where RMS comes in

- With RMS, documents are protected with encryption
- Regardless of where a document resides, it is safe
- Authors determine "who" can do "what" with a document

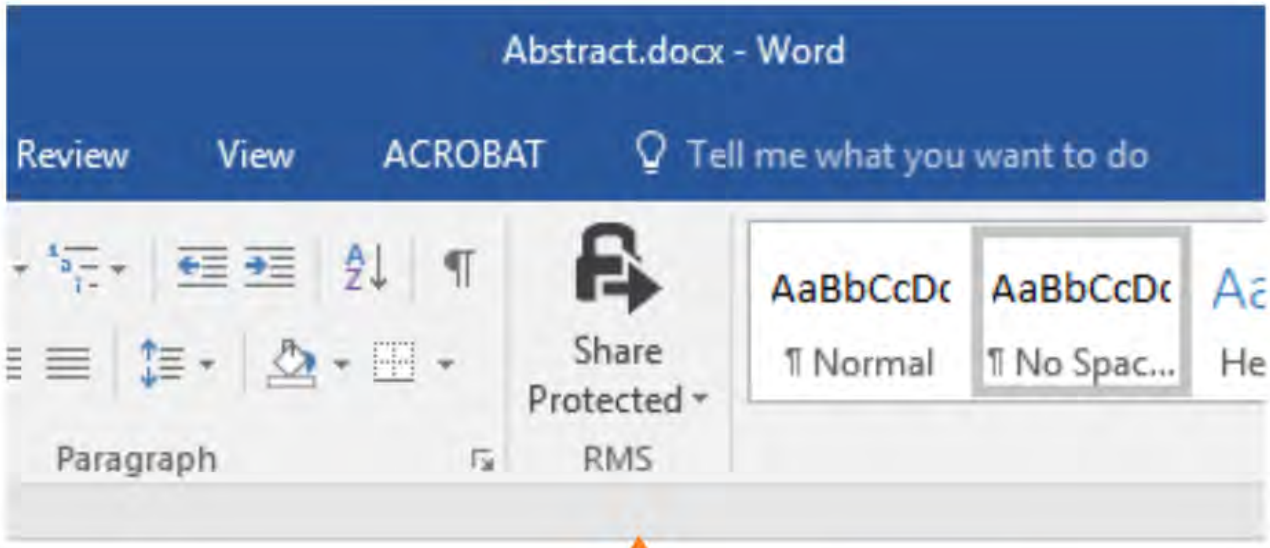
securing that data?

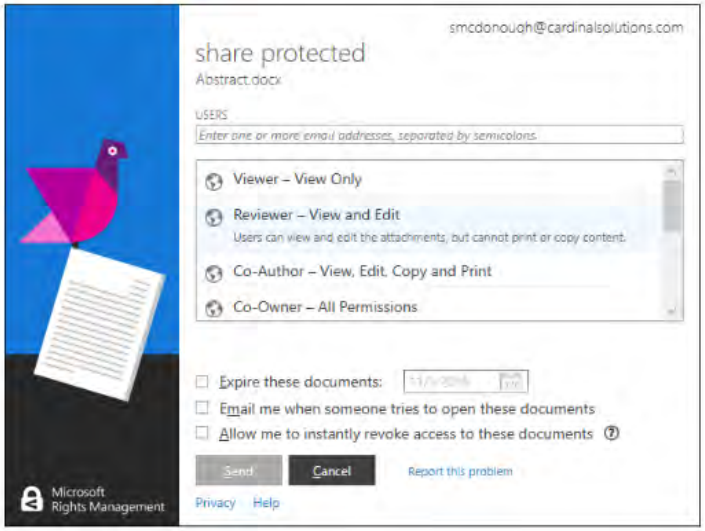






Protecting documents is easy


Abstract.docx - Word
Review
View
ACROBAT
Tell me what you want to do
AaBbCcDc
¶ Normal
AaBbCcDc
¶ No Spac...
Share Protected
Paragraph
RMS


smcdonough@cardinalsolutions.com
share protected
Abstract.docx
USERS
Enter one or more email addresses, separated by semicolons.
Viewer – View Only
Reviewer – View and Edit
Users can view and edit the attachments, but cannot print or copy content.
Co-Author – View, Edit, Copy and Print
Co-Owner – All Permissions
Expire these documents:
Email me when someone tries to open these documents
Allow me to instantly revoke access to these documents
Send
Cancel
Report this problem
Microsoft Rights Management
Privacy
Help

Protecting

Microsoft Rights Management

smcdonough@cardinalsolutions.com

share protected

Abstract.docx

USERS

Enter one or more email addresses, separated by semicolons.

- Viewer – View Only
- Reviewer – View and Edit
  Users can view and edit the attachments, but cannot print or copy content.
- Co-Author – View, Edit, Copy and Print
- Co-Owner – All Permissions

☐ Expire these documents: 11/3/2016

☐ Email me when someone tries to open these documents

☐ Allow me to instantly revoke access to these documents

Send Cancel Report this problem

Privacy Help

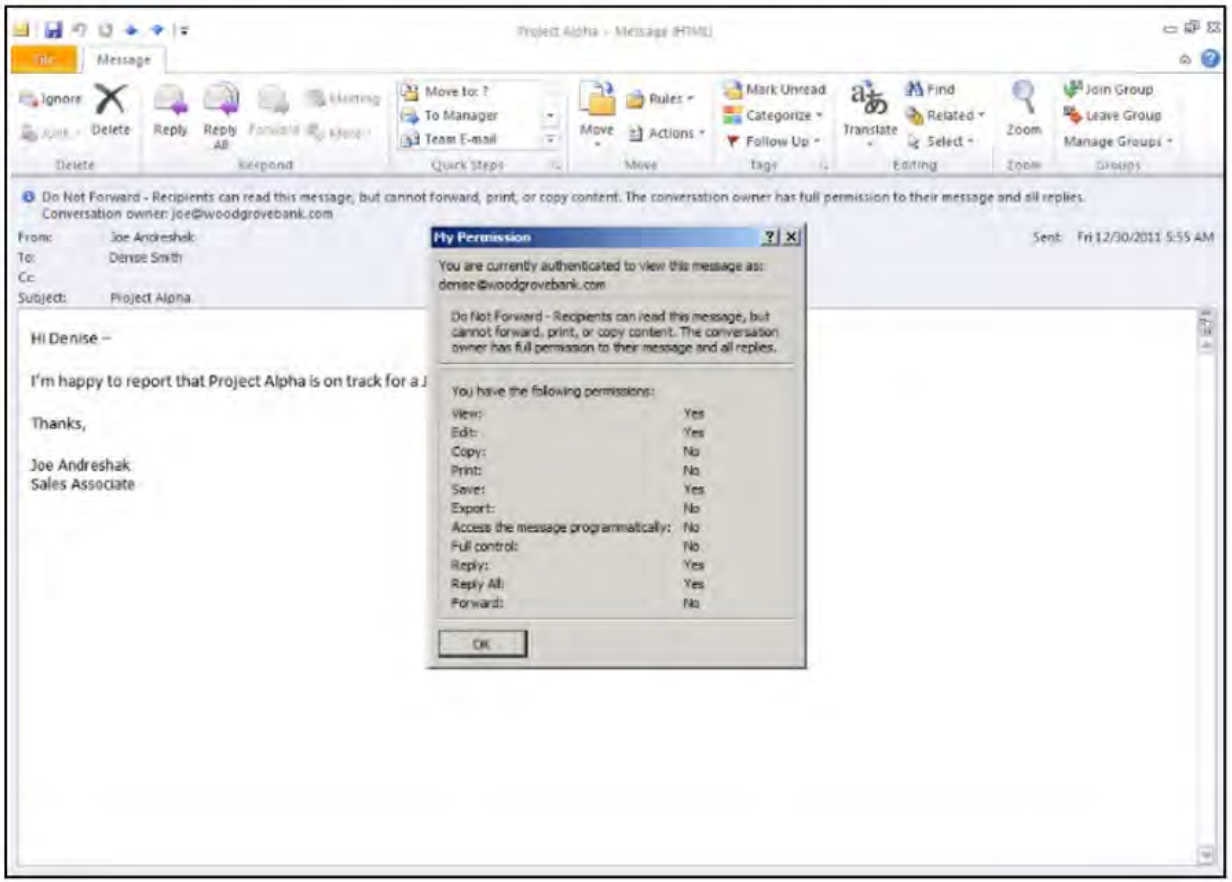
system, what

Behind the scenes, Office is working with Azure RMS (in the cloud) to manage certificates and keys

Have any of you ever worked with PGP?

Managing public and private keys for asymmetric encryption is heavy lifting. Azure RMS does this for you. You simply create and apply policies for document usage

Policies can also be auto-applied



- for example, automatically encrypt any email and/or attachments containing SSNs
- RMS is a natural complement to digital loss prevention (DLP) policies

The only big RMS "add" with EMS E3

An on-premises connector that can be used to apply RMS to non-Office files (via Windows Server 2012 R2 File Classification Infrastructure)

	RMS for O365	Azure RMS (EMS)
Consume & Create RMS content with company ID	✓	✓
Protection for content stored in O365	✓	✓
Protection for content stored in on prem Office (Exchange, Sharepoint via RMS Connector)	✓	✓
Bring your own Key (Hybrid protection)	✓	✓
RMS protection for non office files	✓	✓
RMS SDK	✓	✓
RMS On Prem Connector for on-premises Windows Server file shares (via RMS FCI Connector)		✓

Azure Active Directory Premium

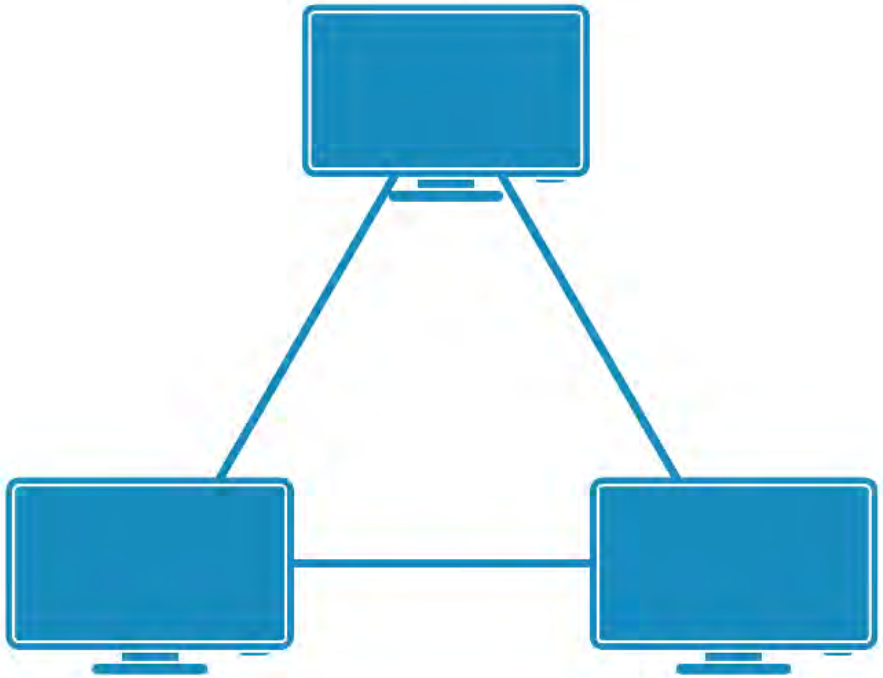
Intune

Azure Rights Management Premium

Advanced Threat Analytics

All EMS subscriptions include these four workloads. EMS E5 has some others.

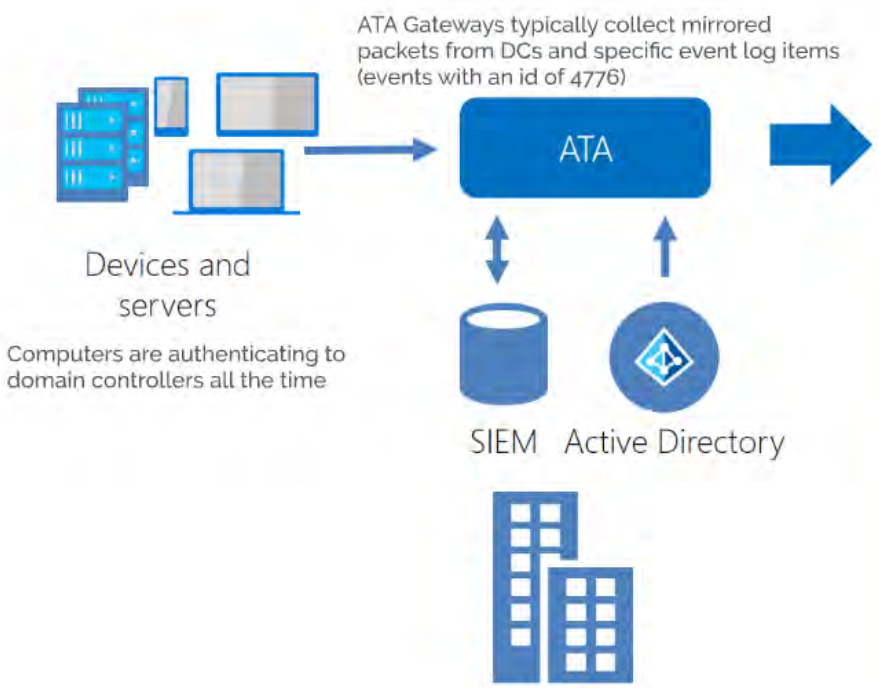
What is Advanced Threat Analytics?



- ATA does analysis of your on-premises authentication traffic
- It looks for anomalies and "weird behavior" using machine learning
- When attacks or compromises are found, you are alerted by ATA

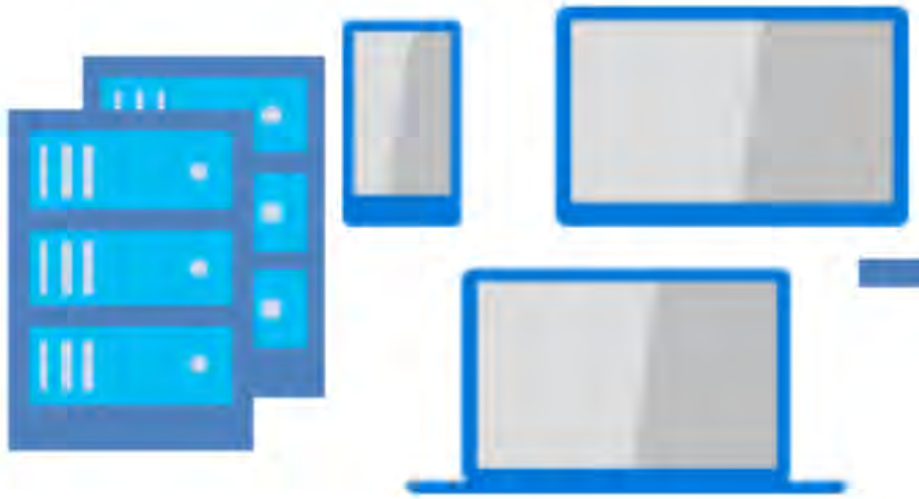
What can ATA

The ATA "Big Picture"



Packets and log information are sent to ATA Centers for analysis. Machine learning does the heavy lifting to find "needles in the haystack" that indicate potential security issues

ATA Gatewa
packets fron
(events with

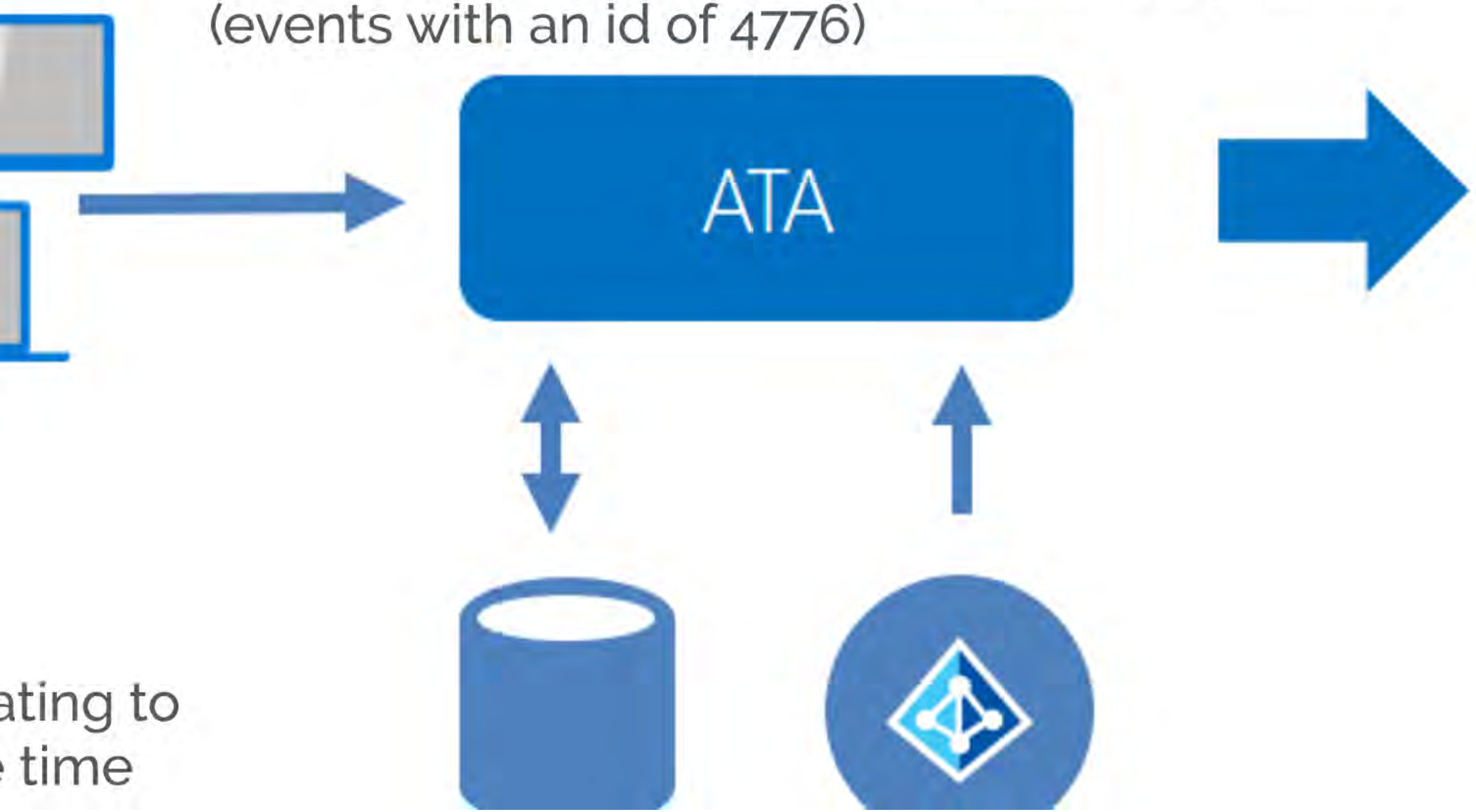


Devices and servers

Computers are authenticating to domain controllers all the time

S

ATA Gateways typically collect mirrored packets from DCs and specific event log items (events with an id of 4776)



ating to
time

Packets and log information are sent to ATA Centers for analysis. Machine learning does the heavy lifting to find "needles in the haystack" that indicate potential security issues

Behavioral Analytics

Forensics for known attacks and issues

Advanced Threat Analytics

Profile normal entity behavior

Search for known security attacks &

Detect suspicious

What can ATA detect?

As it turns out, ATA can detect quite a bit

Note: behavioral analytics are available once 30 days' of data is acquired

Malicious attacks

ATA detects known malicious attacks almost as instantly as they occur.

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Malicious replications
- Reconnaissance
- Brute Force
- Remote execution

Abnormal behavior

Behavioral analytics leverage Machine Learning to uncover questionable activities and abnormal behavior.

- Anomalous logins
- Unknown threats
- Password sharing
- Lateral movement

Security issues and risks

ATA identifies known security issues using world-class security researchers' work.

- Broken trust
- Weak protocols
- Known protocol vulnerabilities

Azure Active Directory Premium

Intune

Azure Rights Management Premium

Advanced Threat Analytics

All EMS subscriptions include these four workloads. EMS E5 has some others.

To Sum It Up

- at it's core, EMS is about enhancing security
- EMS complements Office 365's capabilities well, but EMS doesn't require Office 365
- If you have Office 365, it's worth seeing what you already have before jumping into EMS
- Microsoft is continuously adding to EMS

Office 365 versus EMS

	Identity and access management	Managed mobile productivity	Information protection	Identity-driven security
Enterprise Mobility + Security	**Azure AD for O365+** • Advanced security reports • Single sign-on for all apps • Advanced MFA • Self-service group management & password reset & write back to on-premises, • Dynamic Groups, Group based licensing assignment	**MDM for O365+** • PC management • Mobile app management (prevent cut/copy/paste/save as from corporate apps to personal apps) • Secure content viewers • Certificate provisioning • System Center integration	**RMS for O365+** • Automated intelligent classification and labeling of data • Tracking and notifications for shared documents • Protection for on-premises Windows Server file shares	**Cloud App Security** • Visibility and control for all cloud apps **Advanced Threat Analytics** • Identify advanced threats in on premises identities **Azure AD Premium P2** • Risk based conditional access
Office 365	**Basic identity mgmt. via Azure AD for O365:** • Single sign-on for O365 • Basic multi-factor authentication (MFA) for O365	**Basic mobile device management via MDM for O365** • Device settings management • Selective wipe • Built into O365 management console	**RMS protection via RMS for O365** • Protection for content stored in Office (on-premises or O365) • Access to RMS SDK • Bring your own key	**Advanced Security Management** • Insights into suspicious activity in Office 365

References

- Release for User Survey Analysis: Gartner Consumer Insights - People at Work and Play in 2014

  http://www.gartner.com/newsroom/id/2881217

- McAfee Finds Eighty Percent of Employees User Unapproved Apps at work

  http://newsroom.mcafee.com/press-release/mcafee-finds-eighty-percent-employees-use-unapproved-apps-work

- **Introducing Enterprise Mobility + Security**

  https://blogs.technet.microsoft.com/enterprisemobility/2016/07/07/introducing-enterprise-mobility-security/

- **Enterprise Mobility**

  https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility

- **Gartner Magic Quadrant for Enterprise Mobility Management 2016**

  http://www.air-watch.com/lp/gartner-magic-quadrant-for-enterprise-mobility-management-2016/

Sean P. McDonough

SharePoint & Office 365
Gearhead, Tinkerer, and
Microsoft MVP

Twitter: @spmcdonough

Blog: http://SharePointInterface.com

About: http://about.me/spmcdonough