Microsoft:
What's new and cool FY16

Matt Hickey

Principal ATS

Microsoft

January 2016

What's new and cool?

- "The New Microsoft" – Cloud First, Mobile First
- Office 365 for Education Update
- Exchange Online Advanced Threat Protection (ATP)
- Microsoft Advanced Threat Analytics (ATA)
- Enterprise Mobility Suite (EMS)
  - Azure Active Directory Premium
  - Windows Intune
  - Windows Rights Management Services
- Operations Management Suite (OMS)
- Microsoft Azure
- Windows Azure Remote App
- Microsoft Identity Manager
- PowerBI

Mobile First
Cloud First

Mobility Social Cloud Big data
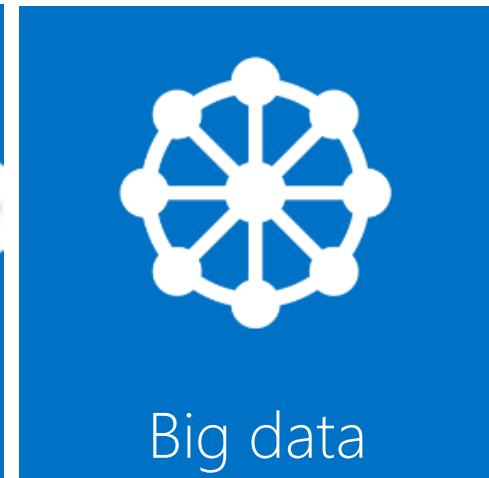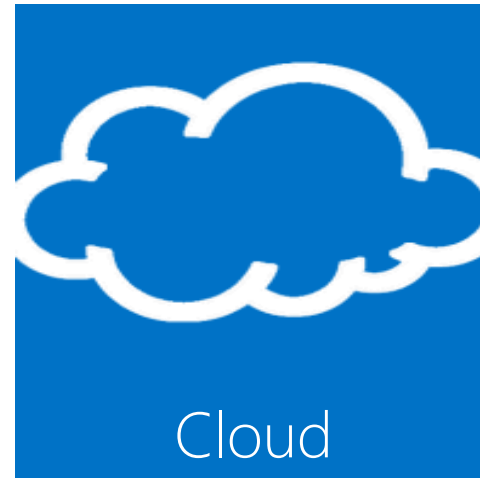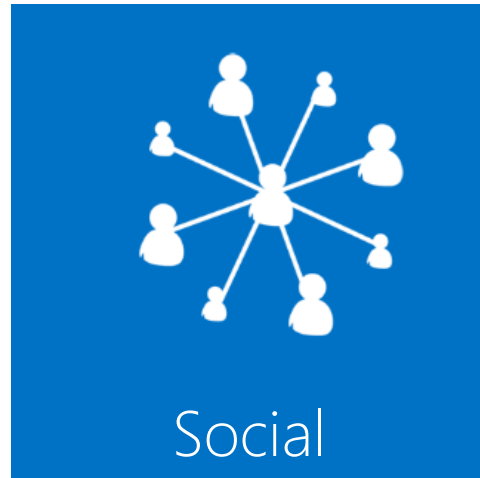
"Everything we do in the world going forward is about ubiquitous computing and ambient intelligence. It is an amazing opportunity."
- **Satya Nadella**

Office 365

			Office 365 Plan E1	Office 365 Plan E3	Office 365 Plan E4
Standard Services	**Exchange Online**	Email, Calendar, Contacts	●	●	●
	Skype for business	IM, Presence, Web Conference	●	●	●
	SharePoint Online and OneDrive	Team sites, Video, storage, sharing	●	●	●
	Yammer	Enterprise Social	●	●	●
	eDiscovery Search	One tool for eMail and Documents	●	●	●
Office	**Office Online**	Edit Office documents in a browser	●	●	●
	Project Online	Manage projects	●	●	●
	Office 365 ProPlus	Office Pro Plus or Office 2011 for Mac, Office for iPad	*	●	●
Advanced Services	**Rights Management Services**	Encrypt eMail, Documents		●	●
	eDiscovery Hold/Export , DLP	Advanced compliance – Legal tools		●	●
	Analytics, PowerPivot, Visio services	Data Analysis		●	●
	Voicemail support	Unified Messaging in Inbox		●	●
	Full Voice with PSTN	Replace PSTN			●
	Price per user/month (Faculty / Student)		FREE	US$ 4.50* / 2.50*	US$ 3.00* / 6.00*

Office 365

			Office 365 Education	
Standard Services	**Exchange Online**	Email, Calendar, Contacts	●	
	Skype for business	IM, Presence, Web Conference	●	
	SharePoint Online and OneDrive	Team sites, Video, storage, sharing	●	
	Yammer	Enterprise Social	●	
	eDiscovery Search	One tool for eMail and Documents	●	
Office	**Office Online**	Edit Office documents in a browser	●	FREE
	Project Online	Manage projects	●	
Advanced Services	**eDiscovery Hold/Export , DLP***	Advanced compliance – Legal tools	●	
	Analytics, PowerPivot, Visio services	Data Analysis	●	
	Voicemail support*	Unified Messaging in Inbox	●	
Additional Services	**Rights Management Services**	Encrypt eMail, Documents	●	
	Office 365 ProPlus	Up to 5 installs on PC or Mac + mobile devices	US$ 1.50** / 2.00**	incl. w/ benefit*
	Full Voice with PSTN	Replace PSTN	US$ .50** / 1.50**	

*ProPlus license included for students at no additional cost when **Office is purchased for faculty and staff**

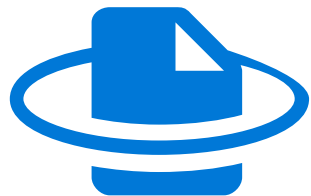**ERP per user/month (Student / Faculty)

***These services will be included after initial launch

Exchange Online Advanced Threat Protection

Protection against unknown malware/virus

- Behavioral analysis with machine learning
- Admin alerts
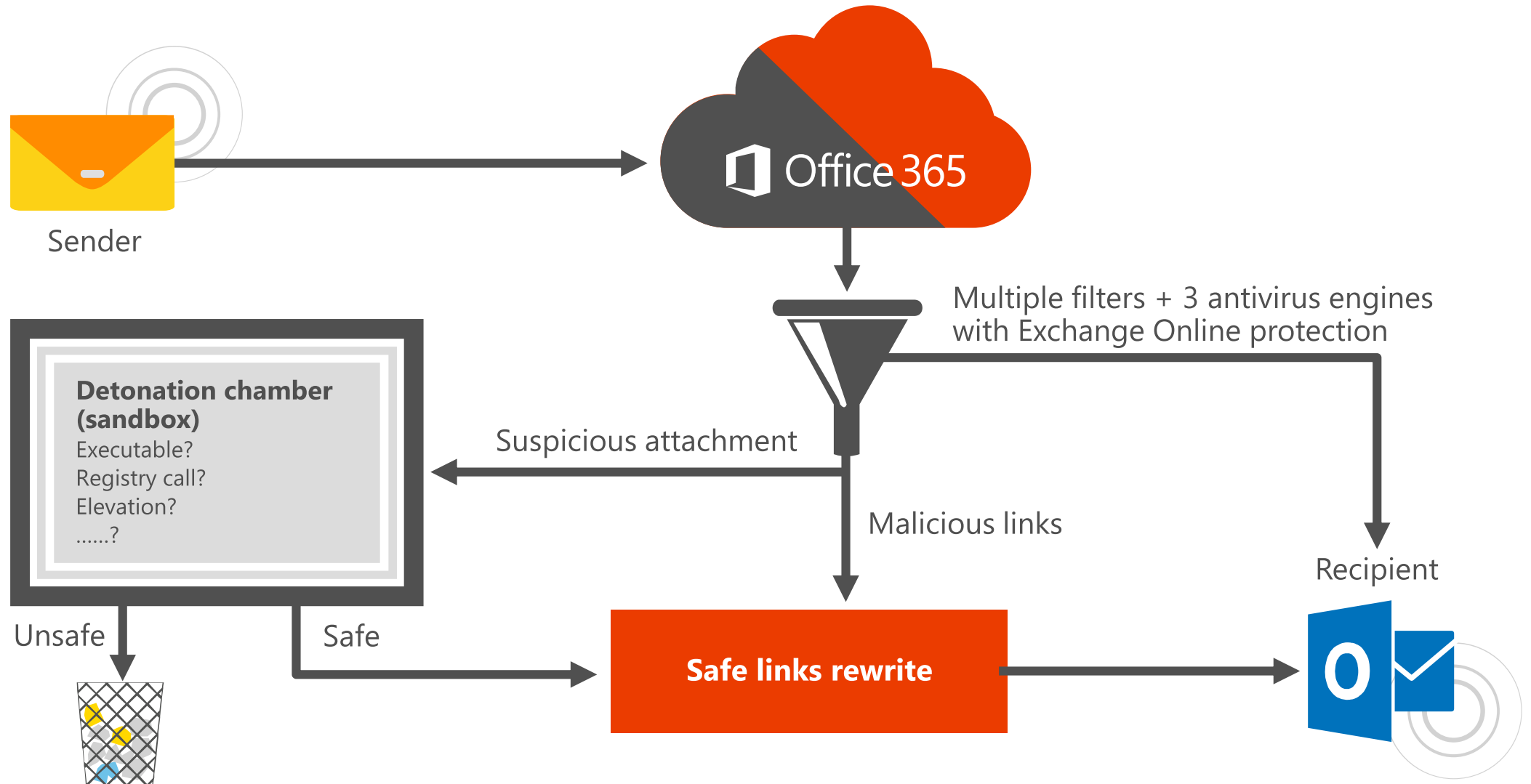
Time of click protection

- Real time protection against Malicious URLs
- Growing URL coverage

Rich reporting and tracing

- Built-in URL trace
- Reports for advanced threats

http://www.gartner.com/technology/reprints.do?id=1-2IXWNX2&ct=150702&st=sb

Exchange Online Advanced Threat Protection

Sender

Office 365

Multiple filters + 3 antivirus engines with Exchange Online protection

Detonation chamber (sandbox)
Executable?
Registry call?
Elevation?
......?

Suspicious attachment

Malicious links
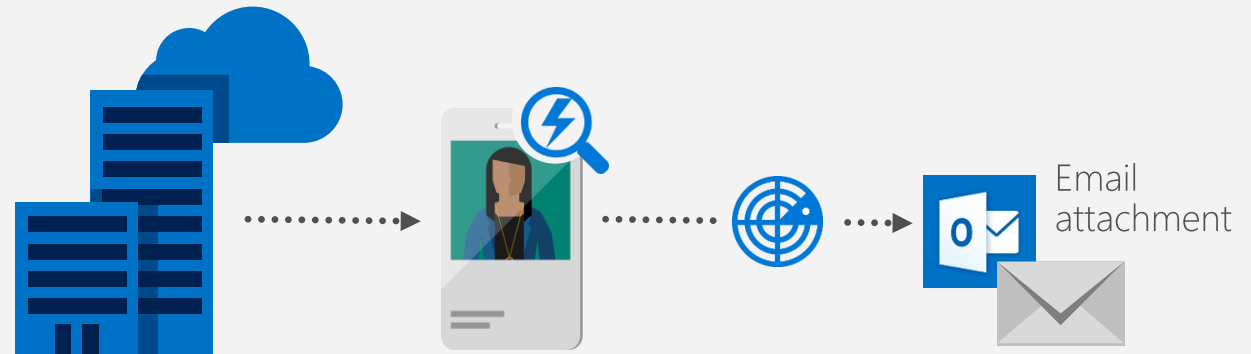
Unsafe

Safe

Safe links rewrite

Recipient

Microsoft Advanced Threat Analytics

An on-premises platform to identify advanced security attacks *before* they cause damage

Comparison:

- **Credit card** companies monitor cardholders' behavior.

- If there is any abnormal activity, they will notify the cardholder to verify charge.

Microsoft Advanced Threat Analytics brings this concept to IT and users of a particular organization
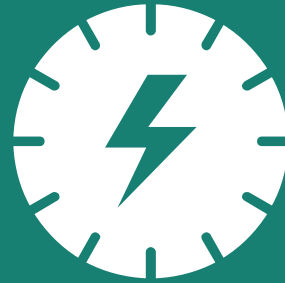

Email attachment

Microsoft Advanced Threat Analytics

An on-premises platform to identify advanced security attacks *before* they cause damage

Behavioral Analytics + Detection for known attacks and issues = Advanced Threat Detection

How Microsoft Advanced Threat Analytics works

Security issues and risks

- Broken trust
- Weak protocols
- Known protocol vulnerabilities

Malicious attacks

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Skeleton key malware
- Reconnaissance
- BruteForce

Abnormal Behavior

- Anomalous logins
- Remote execution
- Suspicious activity
- Unknown threats
- Password sharing
- Lateral movement

12:48 PM
Thursday
March 26, 2015

Computers' Broken Trust Relationship
The trust relationship between CLIENT1 and the domain is broken.
- Group policy is not applied (security violation)
- Users cannot log into the computers.

Note   Email   Export to Excel   Open

CLIENT1
daf::1

DC2
192.168.0.201

12:54 PM
Thursday
March 26, 2015

Identity Theft Using Pass-the-Hash Attack
CLIENT2's hash was stolen from CLIENT2 and used from CLIENT1.

Note   Email   Export to Excel   Open

CLIENT2
192.168.0.2

NTLM hash:B89E5C724F95F41C136038CBBCF2288F

CLIENT1
daf::1

2 Domain controllers

5:21 AM › 12:21 PM
Thursday
March 26, 2015

Suspicion of Identity Theft Based on Abnormal Authentication or Resource Access Behavior
Wayne Hatton exhibited abnormal behavior based on the following activities:
- Performed interactive login from 4 abnormal workstations.
- Requested access to 4 abnormal resources.
- Exceeded the normal amount of working hours.

Note   Email   Export to Excel   Details   Open

Wayne Hatton
Senior head of void

2 Normal computers   +   4 Abnormal computers

Accessed

3 Normal resources   +   4 Abnormal resources

Microsoft Enterprise Mobility Suite

Hybrid identity	Microsoft Azure Active Directory Premium		
	security reports, and audit reports, multi-factor authentication	Self-service password reset and group management	Connection between Active Directory and Azure Active Directory

Mobile device management	Windows Intune		
	Mobile device settings management	Mobile application management	Selective wipe

Access & Information protection	Microsoft Azure Rights Management service		
	Information protection	Connection to on-premises assets	Bring your own key

Identity

3rd party apps

Windows Azure Active Directory

Windows Server Active Directory
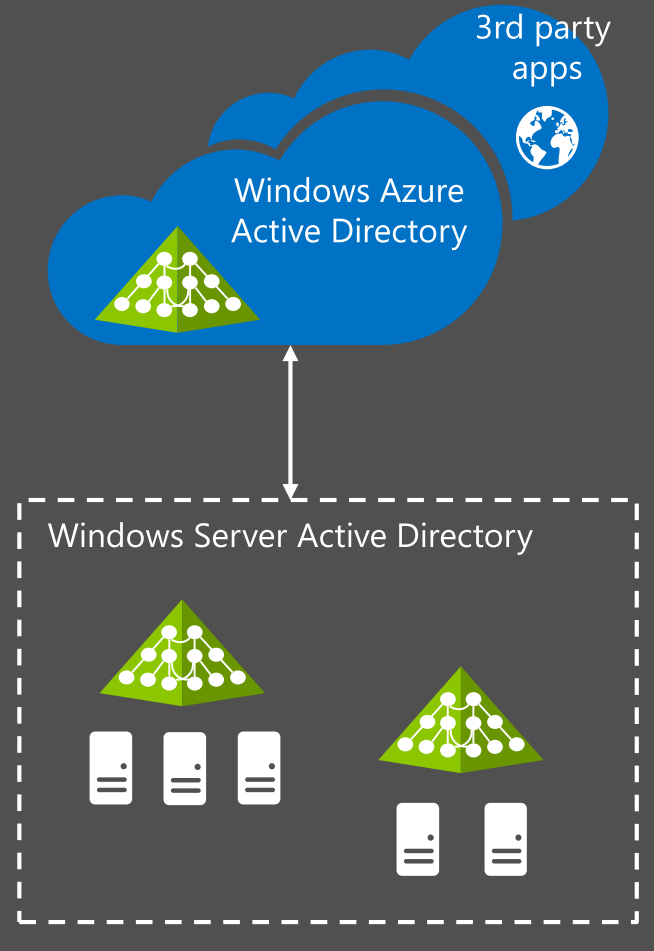
Azure Active Directory Premium

Cloud based IDM providing federation, directory services, device registration, user provisioning, application access control & data protection.

- On-premises and cloud Active Directory managed as one
- Self Service Password reset and group management
- Multifactor authentication
- Branded Logon page
- SSO to 1200+ SaaS applications
- Advanced Security Reports

https://www.microsoft.com/en-us/server-cloud/products/azure-active-directory/

Information Protection

Microsoft Azure
Rights Management
service

Windows
Office

Windows Server
File Services

Microsoft Azure Rights Management Service

- Digital Rights Management for files

- Centralize School information for compliance and data protection

- Provide policy-based access control for applications and data

- Integrates with Exchange and SharePoint

- Automatically identify and classify data based on content with automatic encryption

- More securely share documents with colleagues and business partners

Device Management

Windows Intune

Windows RT, Windows Phone 8 iOS, Android

Windows PCs (x86/64, Intel SoC), Windows to Go Windows Embedded

Mac OS X

Microsoft Intune

Manage staff or student machines

- Windows Updates
- Forefront Antivirus/Antimalware
- HW/SW Inventory
- Software distribution

Manage Mobile Devices

- Agent for Windows Phone, iOS, Android, Windows, Windows RT
- Security policies
- Software distribution – side load apps
- Selective wipe, remote lock, remote password reset

www.microsoft.com/intune

Operations Management Suite (OMS)

Simplified guest and workload management anywhere *(on-premises or in the cloud)*

HYPER-V LINUX WINDOWS
VMware LINUX WINDOWS
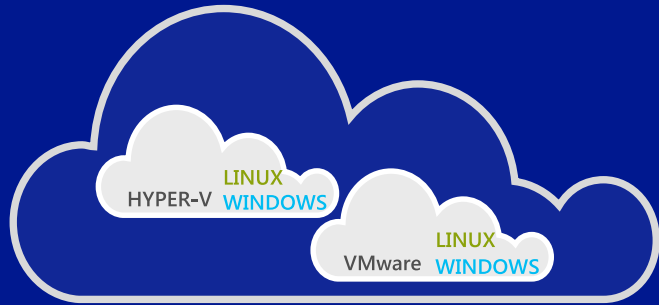
Public Cloud
AZURE or AWS

HYPER-V LINUX WINDOWS
VMware LINUX WINDOWS
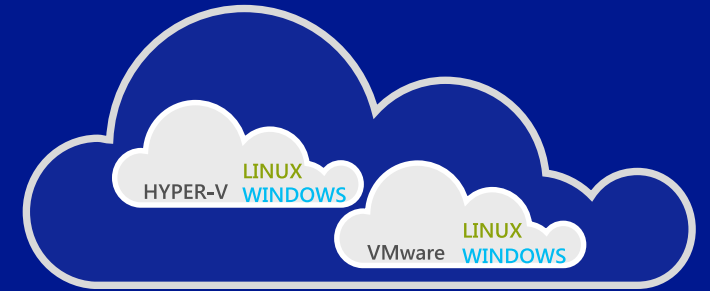
Private or Hosted Third Party Cloud
Rackspace etc.,

Microsoft
Operations Management Suite

HYPER-V LINUX WINDOWS
VMWare LINUX WINDOWS

WINDOWS LINUX

ON-PREMISES WITH SYSTEM CENTER

Operations Management Suite Capabilities

Log analytics

- Effortless log collection
- Integrated fast search and queries with custom dashboard

Backup & Recovery

- Integrated cloud backup
- Seamless disaster recovery and workload migration
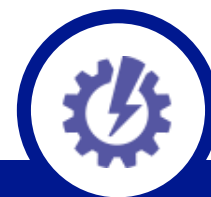
IT Automation

- Hybrid runbook worker
- Graphical workbook authoring and automation DSC

Security & Compliance

- Malware assessment
- Security posture and system update assessment

With OMS capabilities customers can...

| *Spot problems fast* | *Protect data easily* | *Automate tasks quick* | *Recognize threat early* |

extending System Center capabilities, as an all-in-one management solution!

Microsoft Operations Management Suite   Data Plan: Free   OpInsightsDemo

Overview

Log Search

My Dashboard

Solutions Gallery

2.7 GB
Servers and Usage

AD Assessment

4
Servers Assessed

3 ❗
High Priority
Recommendations

6 ℹ️
Low Priority
Recommendations

72 ✅
Passed Checks

Malware Assessment

35%
NEEDS ATTENTION

1
Servers with Active Threats

38
Servers with Inadequate
Protection

Capacity Planning

23.6 %
Available Cores

62.3 %
Available Memory

42.5 %
Available Storage

Backup

ITPRodBackup

13
Servers backed up

3 TB
Backup data

Alert Management

0
Active critical alerts
in the last 24 hours

4
Active warning alerts
in the last 24 hours

1pm 5pm 9pm 1am 5am 9am
3
2
1
0
1pm 5pm 9pm 1am 5am 9am

Automation

ITAutomation

9
Runbooks

15
Jobs in the last 7 days

Change Tracking

20
Software changes in
the last 24 hours

40
20
0
4/26 4/28 4/30 5/2

6
Windows service
changes in the last 24
hours (excludes Status)

10
5
4/26 4/28 4/30 5/2

Security and Audit

95 ↘1
Active Computers in the last
24 hours

64 ↗1
Accounts Authenticated in
the last 24 hours

Feedback ?

Azure Education Workloads and Scenarios

Azure RemoteApp

Microsoft Azure

Remote App

1 Applications execute on Azure Platform (Memory/CPU/Disk space consumed here)...
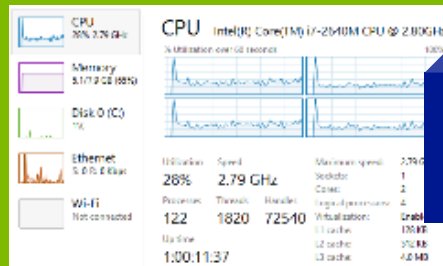
3 User running RemoteApp client sees application open in a standard App window (Memory/CPU/Disk space **NOT** consumed here)...

Click to add title
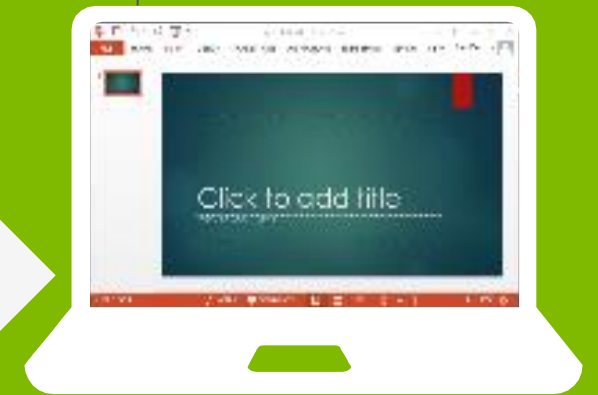
2 Individual application user interface is sent over the network connection

Applications Centrally Managed on Azure
Massive scale & elasticity (VMs spawn based on demand)
Applications *appear* to be running locally @ the client
Apps run on Windows, Mac OSX, iOS and Android

Identity Management

Microsoft Identity Manager 2016

▶ Just in time privilege elevation

▶ Self-service unlock

▶ Virtual Smartcard Management

▶ Flexible workflow and org-based approvals

▶ Mobile Access Scenarios

▶ Bridge to Azure Active Directory

  ▶ SSPR

  ▶ Multifactor Authentication

  ▶ Phone verification

  ▶ Self-service group management

http://www.microsoft.com/en-us/server-cloud/products/microsoft-identity-manager/
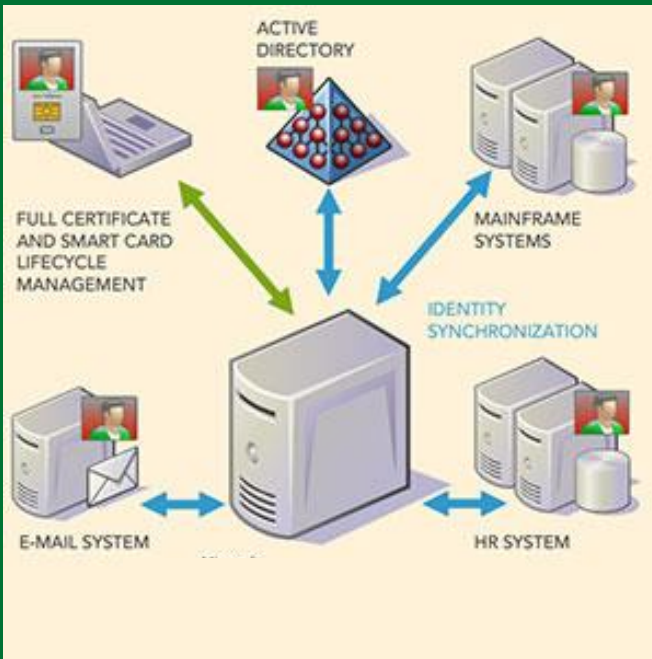
Power BI: experience your data
Any data, any way, anywhere

MICROSOFT CLOUD

Microsoft Azure   Office 365

Microsoft Dynamics

NON-MICROSOFT CLOUD

Acumatica   Marketo   salesforce   GitHub

comSCORE   intuit QuickBooks   twilio

ON-PREMISE DATA

hadoop   SAP   Microsoft SQL Server

ORACLE   TERADATA   IBM

Stream Analytics

Intelligent Apps

45,000
organizations
500,000
unique users
185
countries

What to Use When and Why
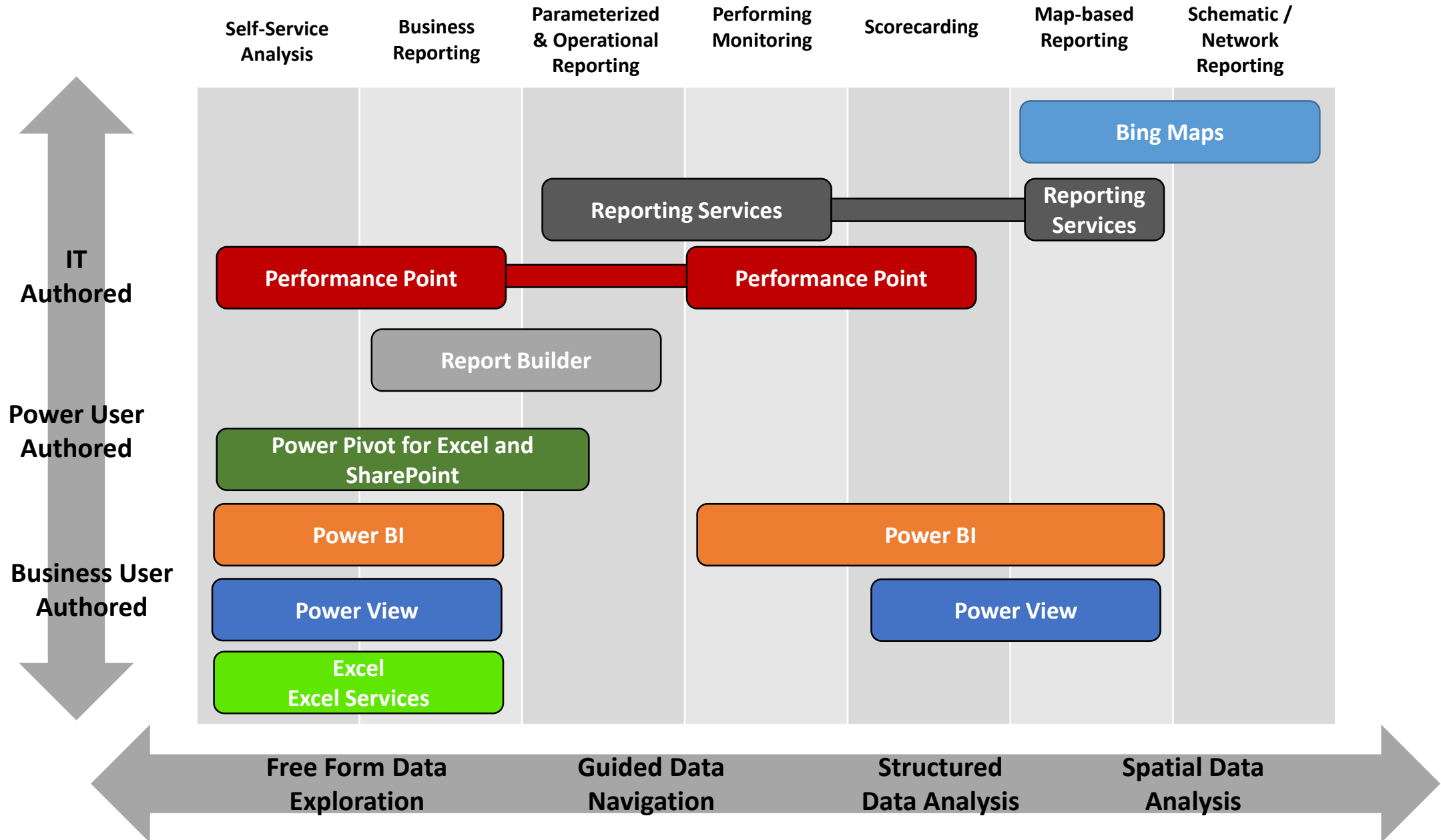
Microsoft®

System Center Licensing Changes

Server Licensing

1. System Center Standard Edition Server Management License (allows you to manage 2 VMs)

2. System Center Datacenter Server Management License (allows you to manage unlimited   VMs per physical

- Configuration Manager +
- Data Protection Manager ++
- Endpoint Protection +
- Operations Manager ++
- Orchestrator ++
- Service Manager ++
- Virtual Machine Manager ++

+ Included with Core Server Platform Agreement
++ Included with Enterprise Server Platform Agreement

Client Licensing

1. Configuration Manager Client Management License
    – Configuration Manager *
    – Virtual Machine Manager *
2. Endpoint Protection Subscription
    – Endpoint Protection *
3. Client Management Suite
    – Data Protection Manager **
    – Operations Manager **
    – Orchestrator **
    – Service Manager **

* Part of CORE CAL Suite
** Part of ECAL Suite

Client Access License Suites FY16

CAL Suites

Exchange Online Archive *NEW!*	Exchange Enterprise CAL w/ Services *NEW!*	Exchange Enterprise CAL	Exchange Standard CAL
Online archiving for Email **ECAL**	DLP – Data Loss Prevention **ECAL**	In place hold and retention management, eDiscovery **ECAL**	Email, calendar, contacts **CORE**
SharePoint Enterprise CAL	**SharePoint Enterprise CAL** *NEW!*	**SharePoint Standard CAL**	**Lync Standard CAL**
Access services, Infopatch forms services **ECAL**	BI: Power View, PerformancePoint Services, Excel Services, and Visio Services **ECAL**	Class sites, team sites, document libraries, App catalog and marketplace. **CORE**	Skype Presence/IM Interoperability **CORE**
Skype Enterprise CAL	**System Center CML**	**System Center Configuration Manager** *NEW!*	**Windows Server**
Skype multi-view video, *NEW!* Skype Web App meetings, Enhanced note taking **ECAL**	Ops Manager Service Manager Data Protection Manager **ECAL**	Antivirus, Software/OS distribution, Patching, remote control, etc. **CORE**	File and Print, Active Directory, etc. **CORE**

Azure AD Premium Multi-Factor Authentication

		Azure AD Free	Azure AD Basic	Azure AD Premium
		$0	(ED TBD, < $0.10)	ED pricing $0.50
Common Features	Directory as a Service	up to 500K Objects	No Object Limit	No Object Limit
	User/Group Management	Yes	Yes	Yes
	SSO to pre-integrated SAAS Applications /Custom Apps	10 apps per user	10 apps per user	No Limit
	User-Based access management/provisioning	Yes	Yes	Yes
	Self-Service Password Change for cloud users	Yes	Yes	Yes
	Identity Synchronization Tool (WSAD Extension, Multi Forest, 3rd party*)	Yes	Yes	Yes
	Security Reports	3 Basic Reports	3 Basic Reports	Advanced Security Reports
	Cloud App Discovery*	Yes (Basic)	Yes(Basic)	Yes(Advanced)**
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
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
	MFA (Cloud and On-premises (MFA Server))			Yes
	Azure AD Application proxy*			Yes
	MIM CAL + MIM Server			Yes
	Administrative Delegation* (FY15 Roadmap)			Yes

Data Privacy

Compliant and certified with worldwide privacy standards

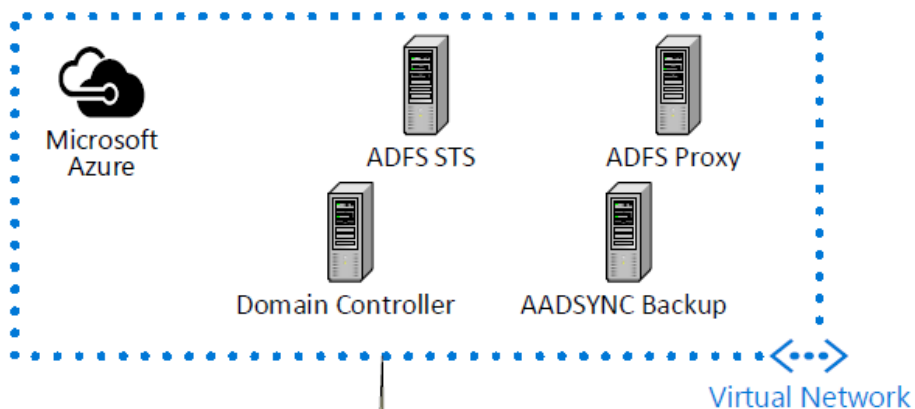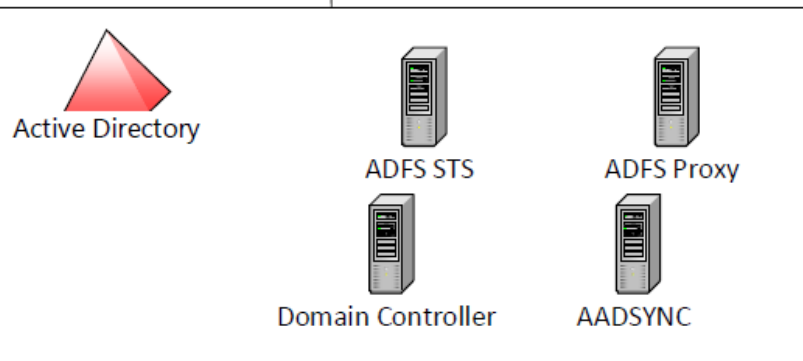|	Microsoft Azure
ISO/IEC 27018	✔
SAS 70/ SSAE / SOC 1 / SOC 2	✔ (Type II)
FedRAMP	✔
HIPAA BAA	✔
EU-Model Clauses / Safe Harbor	✔
UK G-Cloud/IL2	✔
PCI DSS	✔
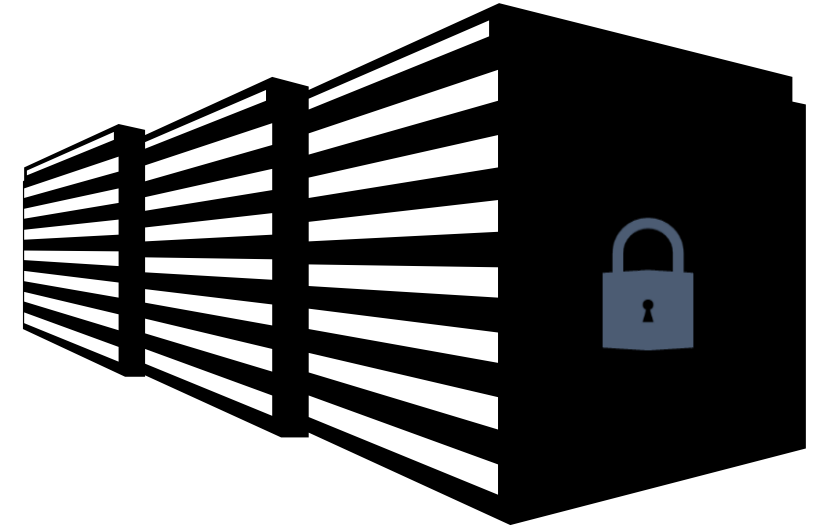
More certification information is available at the Azure Trust Center.

Hosting Active Directory and ADFS Infrastructure in Microsoft Azure

Microsoft Azure

ADFS STS

ADFS Proxy

Domain Controller

AADSYNC Backup

Virtual Network

SSL VPN or ExpressRoute connection To Azure

Active Directory

ADFS STS

ADFS Proxy

Domain Controller

AADSYNC

On Premises Netwo

Benefits:
-Putting DCs and ADFS in Azure provide authentication redundancy. If your local AD is down, users can still authenticate to O365 for critical services like Email
Tips:
-Windows Server 2012 or later is required if running DCs in Server Virtualization
-Configure AD Sites link costs appropriately
-Azure DNS doesn't support AD, you need you own DNS presence in Azure
-Place the AD DIT/SYSVOL on non-cached data drive
Resources:
-Deploy AD DS or AD FS and Office 365 with single sign-on and Azure Virtual Machines
https://technet.microsoft.com/en-us/library/dn509513.aspx
-TUTORIAL: Install a Replica Active Directory Domain Controller in Azure Virtual Networks -
http://azure.microsoft.com/en-us/documentation/articles/virtual-networks-install-replica-active-directory-domain-controller
-TUTORIAL: Install a new Active Directory forest on an Azure virtual network -
http://azure.microsoft.com/en-us/documentation/articles/active-directory-new-forest-virtual-machine/
 -Documentation: Guidelines for Deploying Windows Server Active Directory on Azure Virtual Machines - http://msdn.microsoft.com/library/azure/jj156090.aspx
-White paper: Office 365 Adapter - Deploying Office 365 single sign-on using Azure Virtual Machines - http://technet.microsoft.com/en-us/library/dn509539.aspx

Sample Bill of materials - best bet is to run Azure IaaS estimator on a actual on premises serve				
	Hourly Rate	Monthly Rate	# Servers	Extended
A3 Windows VMs - Domain Controllers 500GB Dat	$ 0.2618	$ 194.78	1	$194.78
A3 Windows VMs ADFS STS 100GB Data	$ 0.2618	$ 194.78	1	$194.78
A3 Windows VMs ADFS PROXY 100GB Data	$ 0.2618	$ 194.78	1	$194.78
A2 Windows VMs AADSYNC backup 100GB Data	$ 0.1309	$ 97.39	1	$ 97.39
				$681.73
	Per Unit	# Units	Monthly Cost	
Storage, Locally Redundant, per GB	$ 0.0511	800	$ 40.88	
Site to Site VPN, per Hour	$ 0.0360	744	$ 26.78	
Storage Transactions, per 100M IOPS	$ 3.6000	10	$ 36.00	
Data Egress, for # of GB transferred out	$ 0.0870	100	$ 8.70	
			$ 112.36	
			$ 794.09	

Backup School Data in Microsoft Azure

Microsoft Azure

Storage blob · Storage blob · Virtual machine backup · Virtual machine backup

Storage blob

Storage blob · Virtual machine backup · Virtual machine backup

Azure Backups – Virtual Machines and Volumes

Azure Backup Service
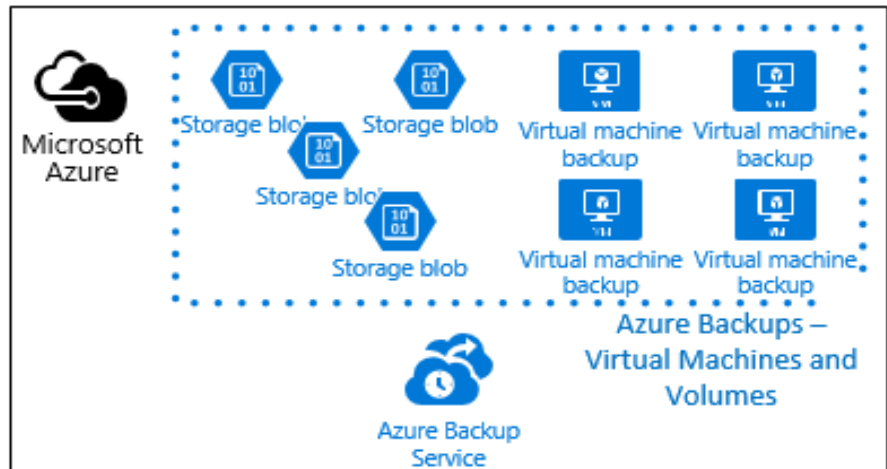
Azure Backup Vault (Geo-replicated)

Data Encrypted in transit

Active Directory

School File Server · Admin App Server

District Web Server · Special Ed Server
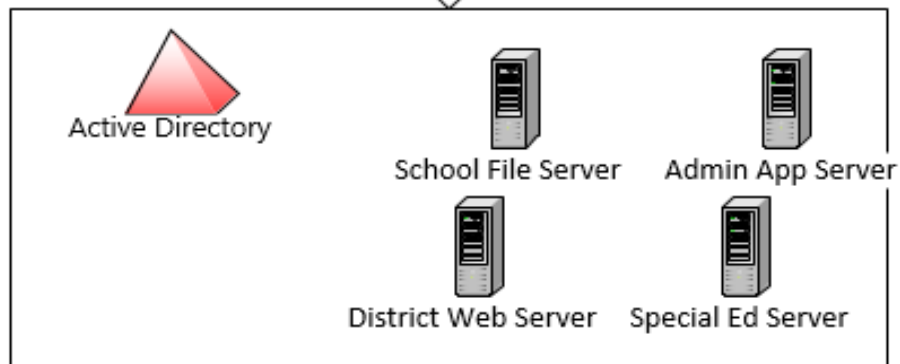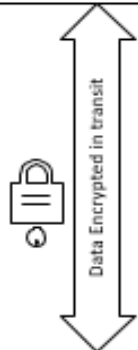
On Premises Network

Benefits:
-Azure backup is a compelling alternative to tape backups with significant cost savings, shorter recovery time and up to 99 years of retention.
-Backing up clients or servers to Azure is secure over the wire and at rest. Backups are stored in geo-replicated storage which maintains 6 copies of you data across two Azure datacenters.

Tips:
-Azure backup can back up physical servers and virtual machines both in the cloud and on premises.
-Use Data Protection Manager for multi-server or complex application workloads (E.g. Exchange, SharePoint, etc.)
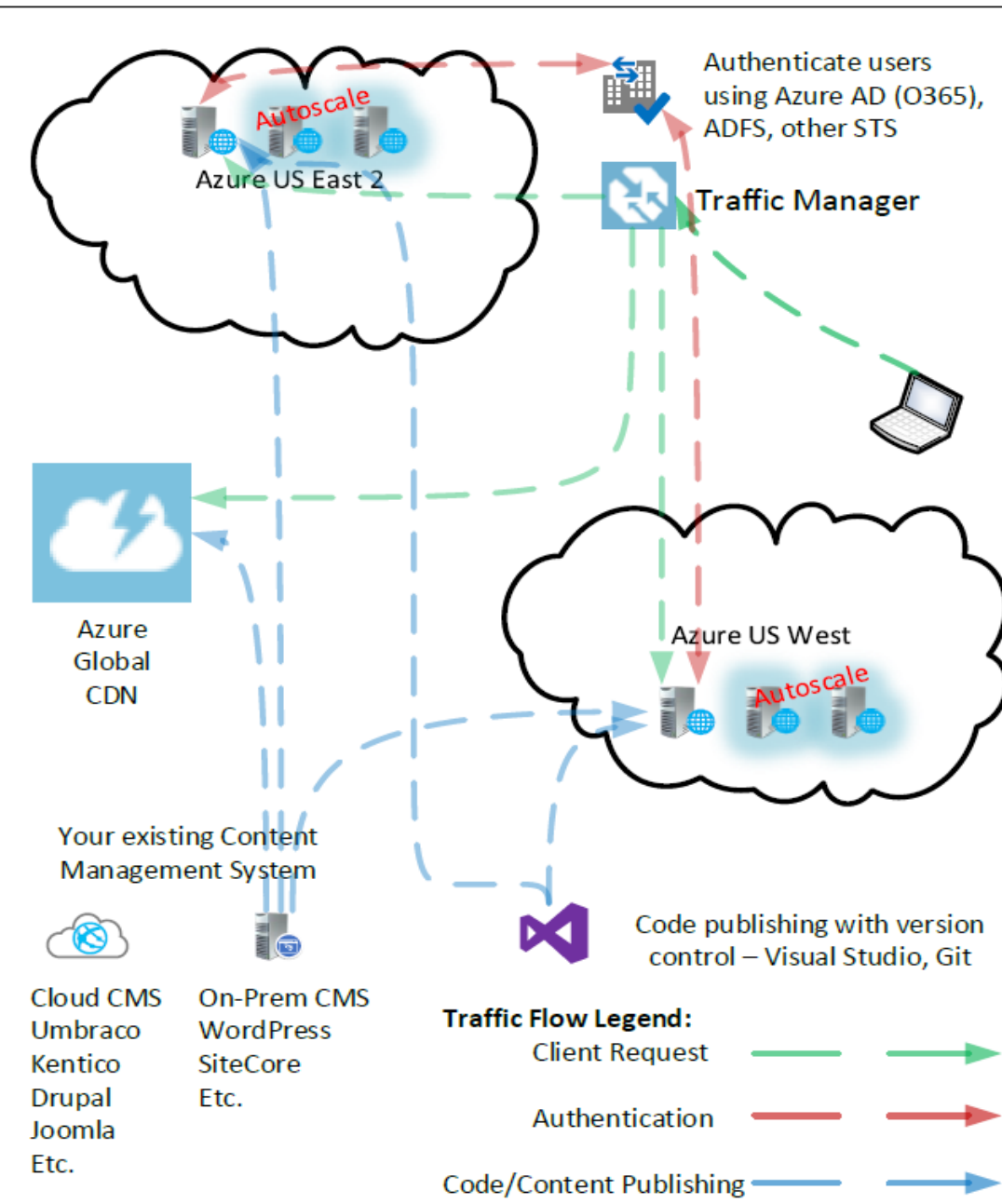
Resources:
- Blog with new Edu pricing - http://azure.microsoft.com/blog/2015/03/31/azure-backup-announcing-new-pricing-model-for-tco-reduction/
-Intro to Azure Backup - http://azure.microsoft.com/en-us/documentation/articles/backup-introduction-to-azure-backup/
-Back up Windows Servers - http://azure.microsoft.com/en-us/documentation/articles/backup-configure-vault/
-Back up Azure VMs with Azure backup – http://azure.microsoft.com/en-us/documentation/articles/backup-azure-vms/
-Azure Backup FAQ - http://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-faq/
-Azure Backup Forums - http://go.microsoft.com/fwlink/p/?linkid=290933&clcid=0x409

Sample Bill of materials - 4 Servers - 1 Large (900GB), 2 Med (400GB/ea), 1 Small (40GB)				
	Monthly Rate	Quantity	Extended	
Cost per protected VM instance				
Small Instance (up to 50GB)	$ 5.00	1	$ 5.00	
Med (51 to 500GB)	$ 10.00	2	$ 20.00	
Large (over 500GB - $10/mo per 500GB)	$ 10.00	2	$ 20.00	
Total			$ 45.00	
	# Units	Cost per GB	Cost	
Locally Redundant Storage (File Setrver)	900	0.024	$ 21.60	
Geo Redunant Storage (App, Web and Special Ed)	840	0.048	$ 40.32	
Total			$ 61.92	
Total Monthly Cost			$ 106.92	
This is a sample only. Data storage costs might grow over time				

Your Public Web Site in Azure App Service

Authenticate users using Azure AD (O365), ADFS, other STS

Azure US East 2

Autoscale

Traffic Manager

Azure Global CDN

Azure US West

Autoscale

Your existing Content Management System

Code publishing with version control – Visual Studio, Git

Cloud CMS
Umbraco
Kentico
Drupal
Joomla
Etc.

On-Prem CMS
WordPress
SiteCore
Etc.

Traffic Flow Legend:
Client Request →
Authentication →
Code/Content Publishing →

Benefits:
- You don't have to patch/upgrade OS, IIS, Java, .Net, etc.
- Multi-Geography, out of region infrastructure with lower maintenance/management overhead.
- Easy auto-scaling to handle peak loads (start/end of semester/year, athletic events, commencement, etc.)
- Integrate Azure Content Delivery Network (CDN) for audio, video, photos, etc.
- Cross-platform: ASP.Net, Java, Node.js, .Net, WordPress, C#, Python, PHP, HTML5
- User Auth – supports Azure AD (O365) as well as on-premises ADFS & other STS as well as multi-factor
- Secure – ISO, SOCS, PCI compliant
- Backups support built-in (consumes Azure Storage for backup retention)

Tips:
- Identify existing Content Management Service (CMS) – likely can publish to Azure Web Sites
- CDN raises performance for heavy media but adds some complexity – assess cost/benefit to your website
- Work with your CMS/Devs to agree on target URL's for Traffic Manager Health Probes

Resources:
- App Service pricing details - http://azure.microsoft.com/en-us/pricing/details/app-service/
- Use Azure CDN in Azure App Service - http://azure.microsoft.com/en-us/documentation/articles/cdn-websites-with-cdn

Sample Bill of materials - 2 Web Servers	Monthly Rate	Quantity	Extended
Cost per Web App Worker Instance (VM)			
B1 (Basic Plan, 1 Core, 1.75GB RAM, 10GB Storage)	$ 56.00	0	$ -
S1 (Standard Plan, 1 Core, 1.75GB RAM, 50GB Storage)	$ 74.00	2	$ 148.00
S2 (Standard Plan, 2 Core, 3.5GB RAM, 50GB Storage)	$ 149.00	0	$ -
P2 (Premium Plan, 2 Core, 3.5GB RAM, 500GB Storage)	$ 149.00	0	$ -
Cost for additional services			
Data Egress 500GB/Month	$ 59.40	1	$ 59.40
SNI SSL (qty. 5 incl. Standard & above, modern browser)	$ 9.00	0	$ -
IP SSL (qty. 1 incl. Standard & above, all browsers)	$ 39.00	0	$ -
Azure CDN 1TB	$ 89.00	1	$ 89.00
Block Blob Storage, LRS (for backups) 100GB	$ 2.40	2	$ 4.80
Total Monthly Cost			**$ 301.20**

Cost Savings Opportunity

- Consolidation
- Buy new PCs with lowest cost OS (e.g. Windows 7 Home)
- System Center Endpoint Protection to replace Symantec
- Bitlocker for device encryption to replace Safeboot
- Windows Intune for PC and Mobile device management
- Hyper-V Server Virtualization to replace VMWare
- Skype for Video or Audio Conferencing and VOIP
- Exchange Unified Messaging to replace aging Voice Mail System
- Azure for Backup, Disaster Recovery and Infrastructure as a Service (IaaS)
- Azure and StorSimple Storage vs expensive SANs
- Azure Remote App to serve up applications remotely and replace VDI
- OneDrive for file storage/sync with enterprise security and privacy
- Office 365 Professional Plus Benefit