

MODERN WORKPLACE



Frank van Leeuwen
Product owner / Architect
Frank.van.leeuwen@centric.eu

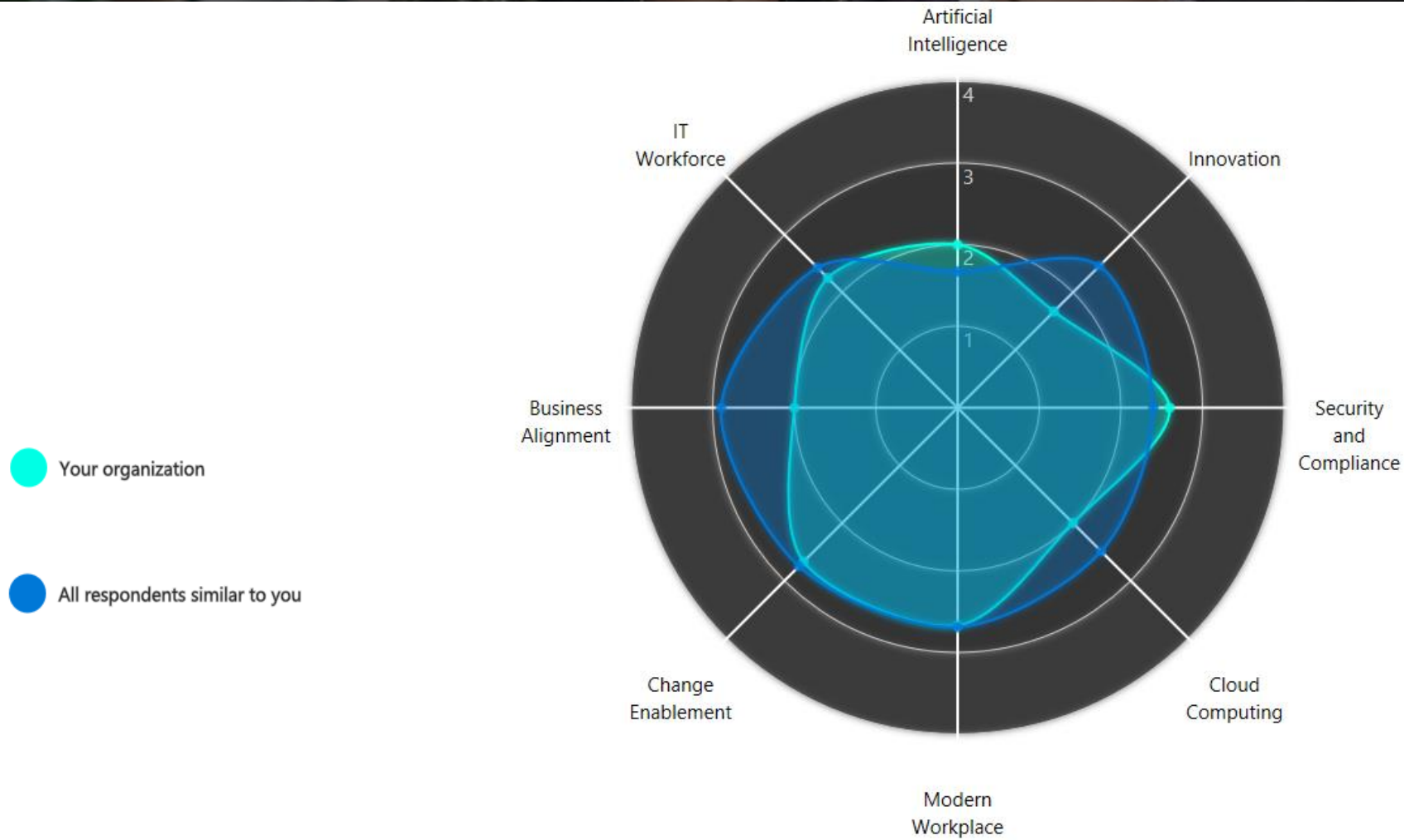
centric
tech
event

What do we mean by the modern workplace



IT Maturity Assessment

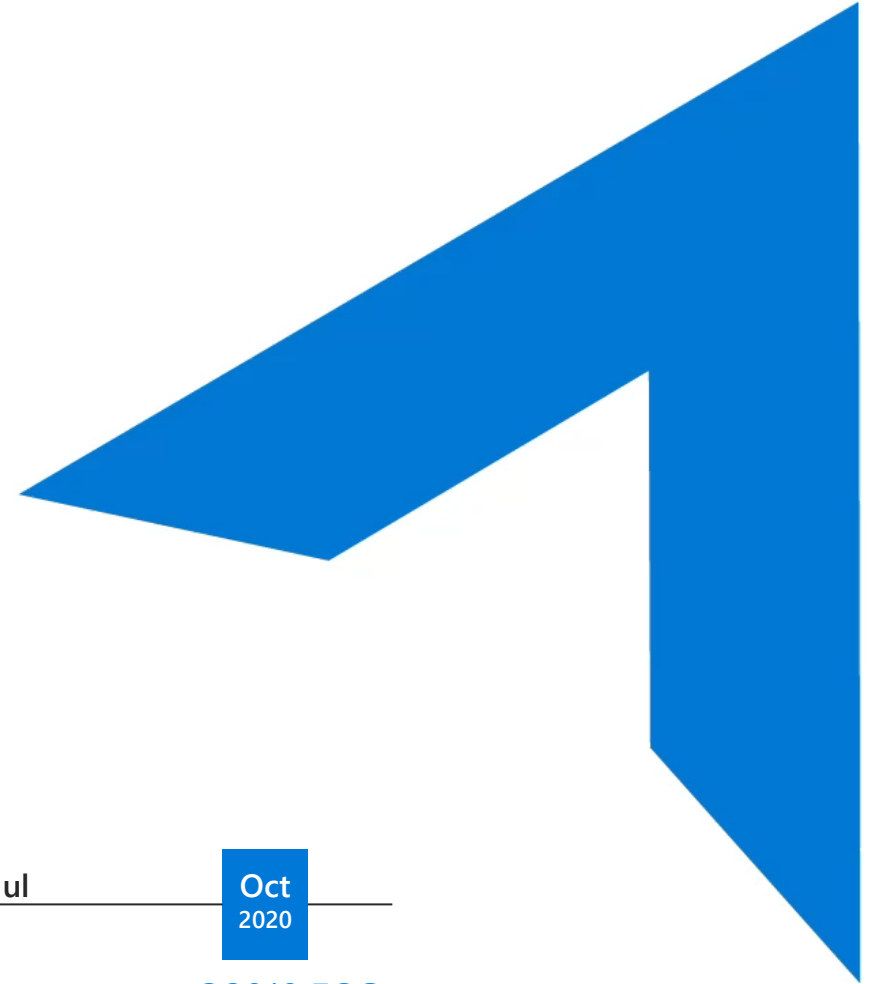
Results



What's top of mind for IT pros?



Now is the time to shift



Learn more at microsoft365.com/shift

Microsoft 365

Users

Simplicity
Flexibility
Mobility



IT

Manageability
Security
Compliance

Built for teamwork

Unlock creativity

Integrated for simplicity

Intelligent security

Windows 10 Enterprise

Office 365 ProPlus

Enterprise Mobility +
Security

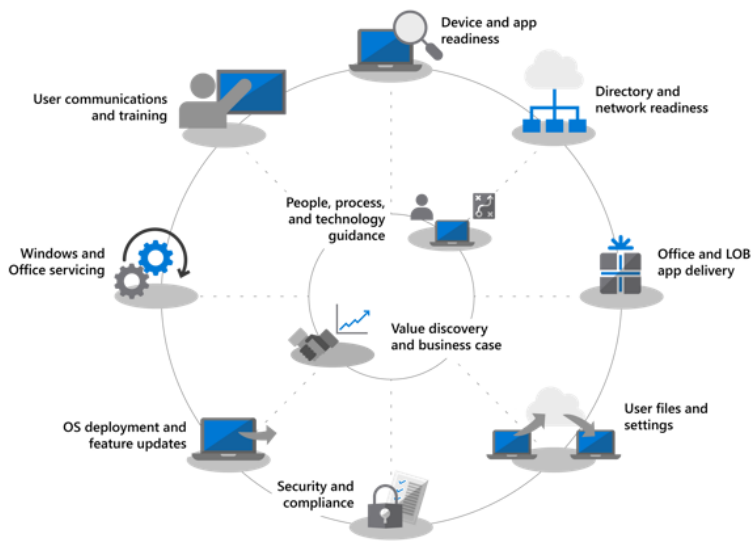
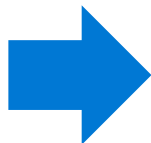
	Standaard	Hybrid	Modern	Future
Workplace				
Network				
Authenticatie				
Applications				
Storage				
Settings				
Security				
Access				
Printing				

Steps for successful implementation



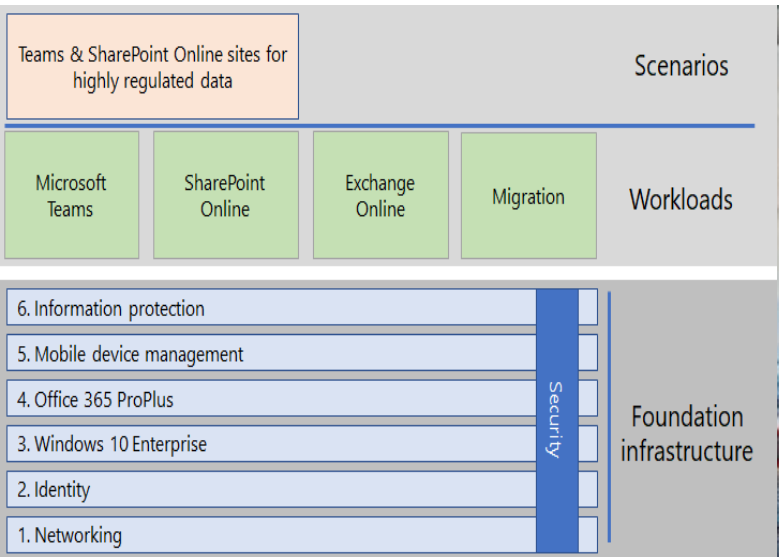
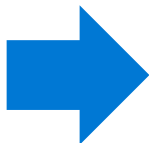
Microsoft Desktop Assessment

1



Desktop deployment Center

2



Microsoft 365 Enterprise deployment guide

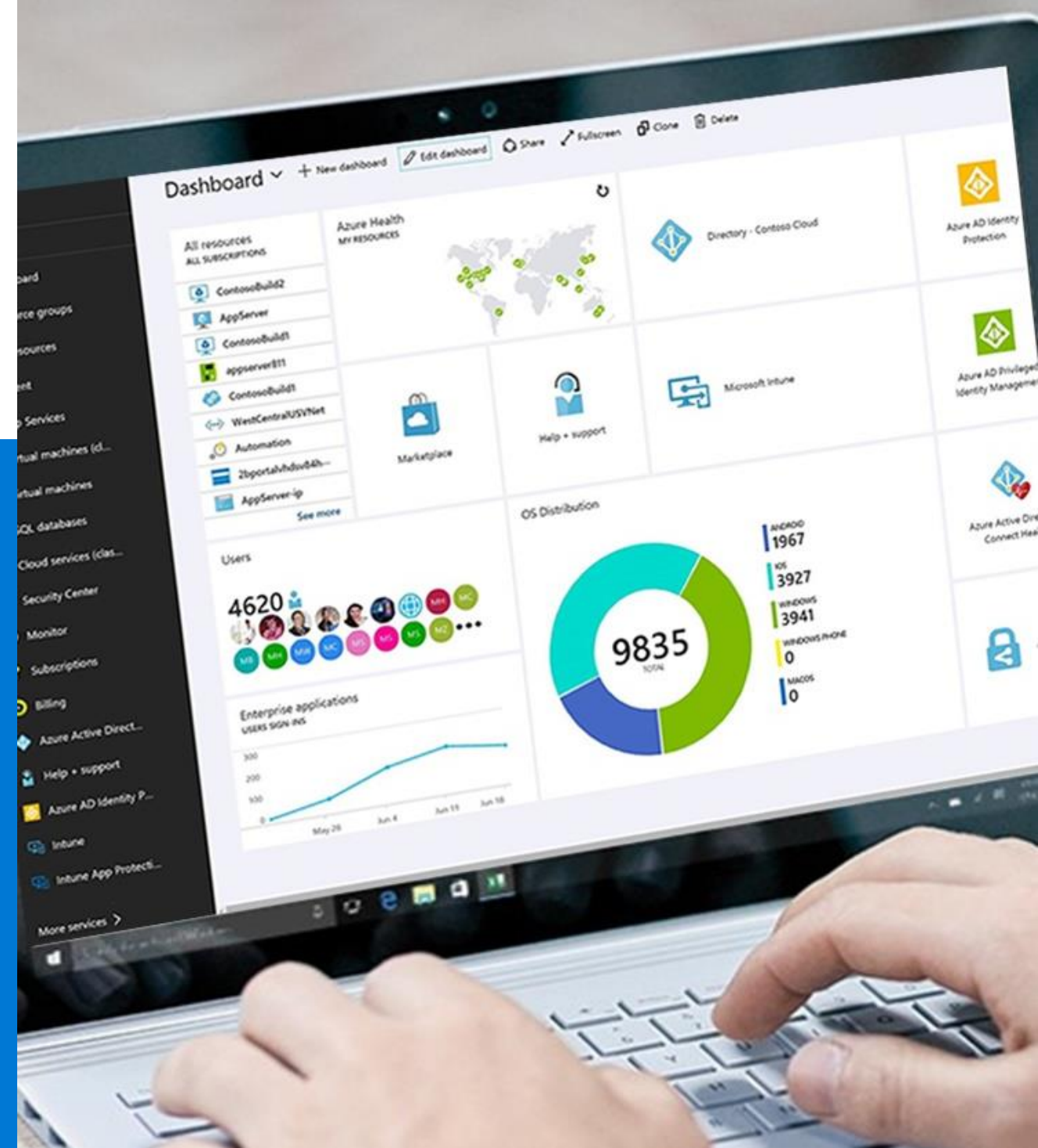
3

Modern Desktop Assessment

Type

1

- Introduction Modern desktop and Windows Analytics
- Implementing Windows analytics and Office Readiness Toolkit
- Analysing and create report impact EOS
- Present Findings and recommendations



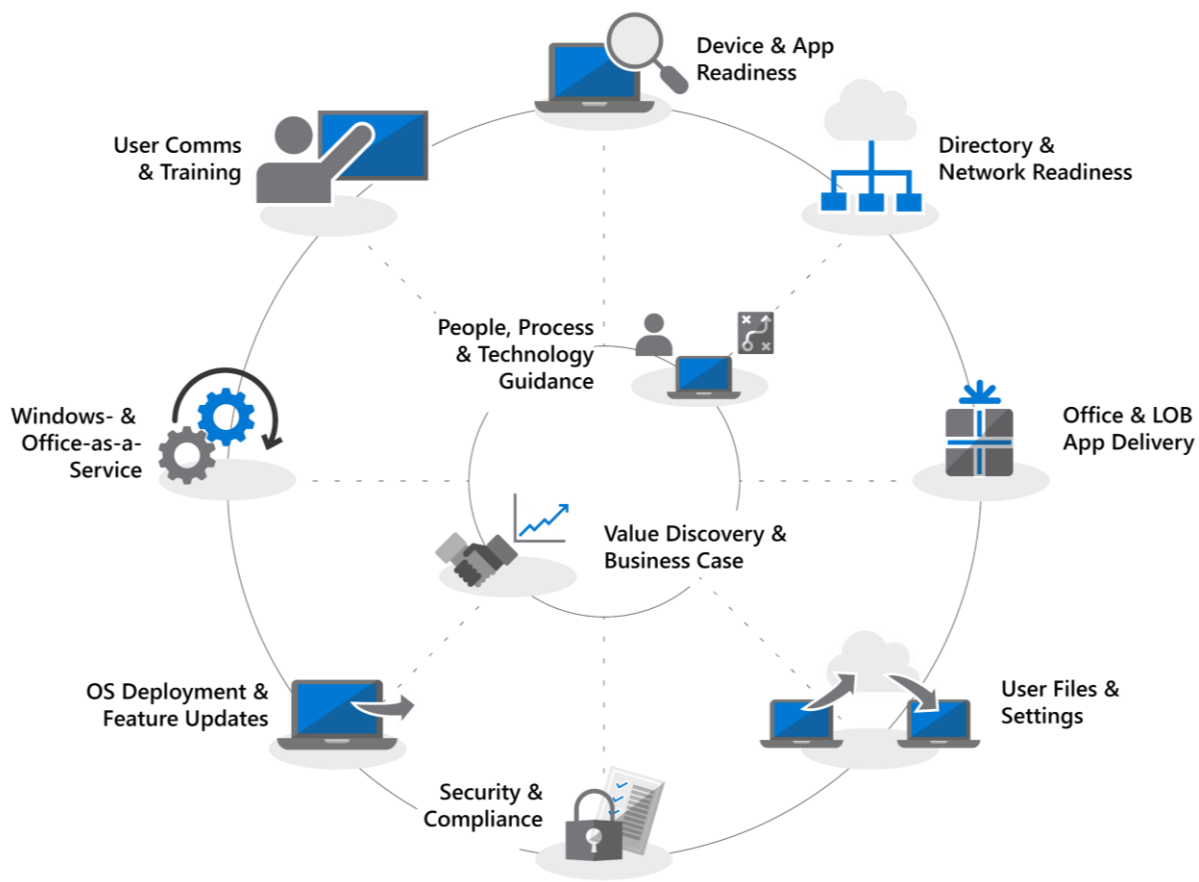
Modern Desktop Assessment

Type

2

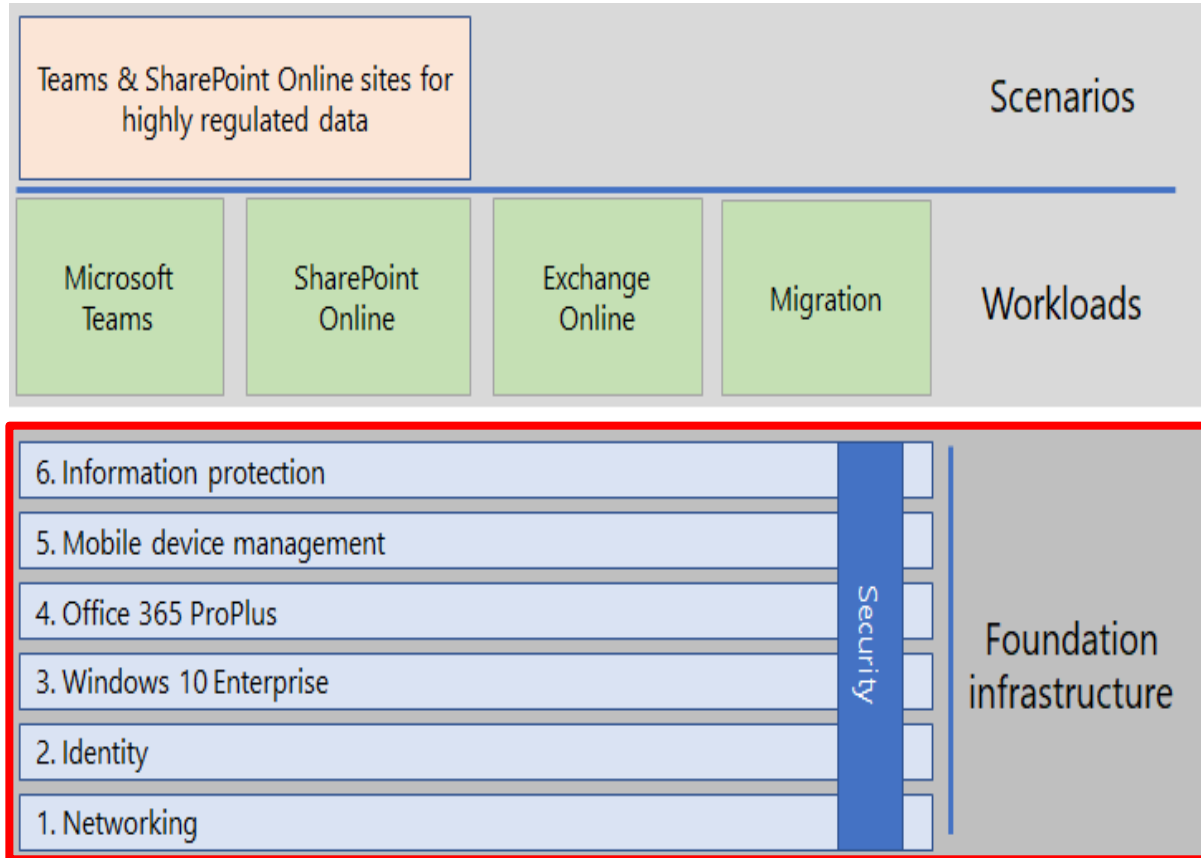
- Introduce assessment goals to customer
- Discuss in depth Modern desktop deployment (Wheel)
- Questionnaire of current environment
- Analysing discovered data including impact EOS / organization
- Present Findings and recommendations





'How to shift' to a modern desktop

Core steps and processes for large-scale deployment of Windows 10 and Office 365 ProPlus



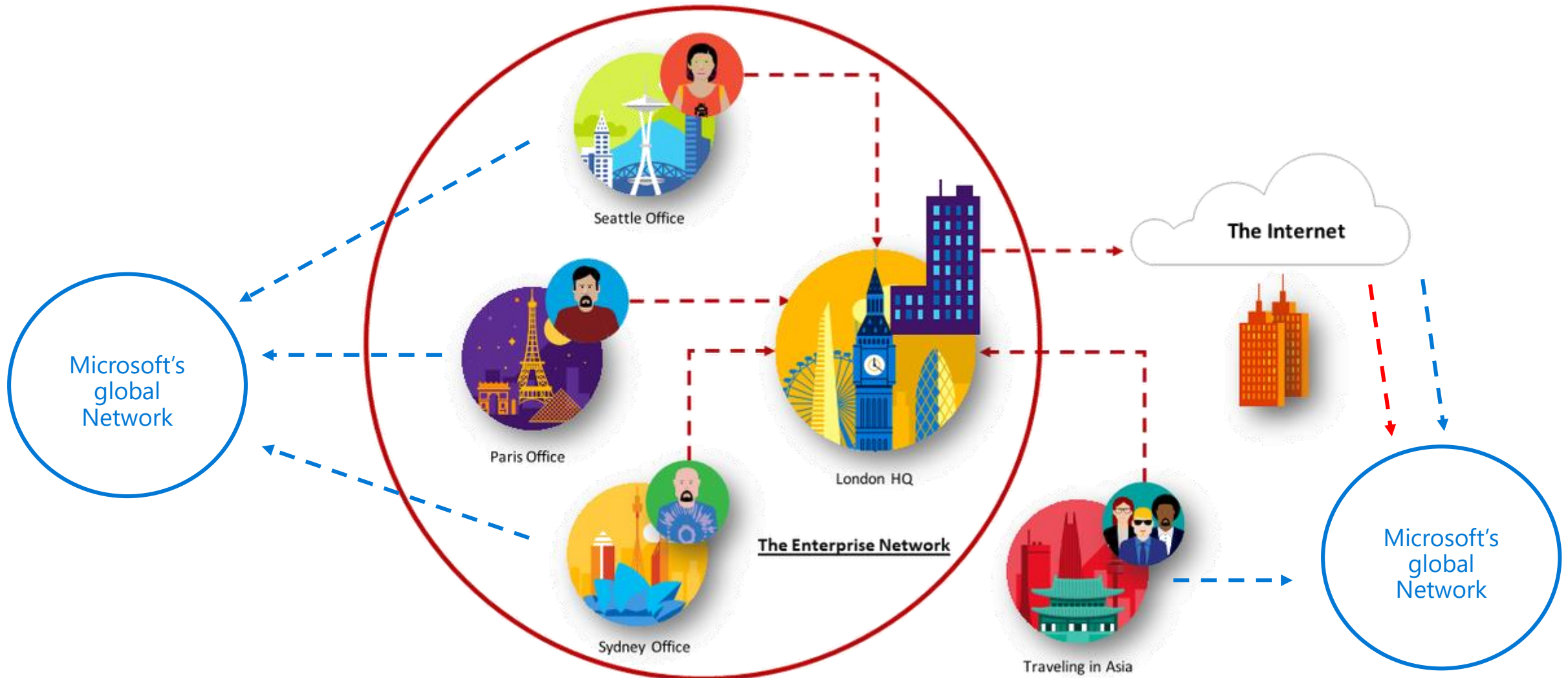
Deploy Microsoft 365 Enterprise

Build a firm IT foundation upon which 365 applications and services can unlock creativity and teamwork in a secure environment

Networking

Prepare you network for Microsoft 365

6. Information protection	
5. Mobile device management	
4. Office 365 ProPlus	
3. Windows 10 Enterprise	
2. Identity	
1. Networking	



Networking

Prepare you network for Microsoft 365

1. < Latency
2. < Round Trip Time



Networking

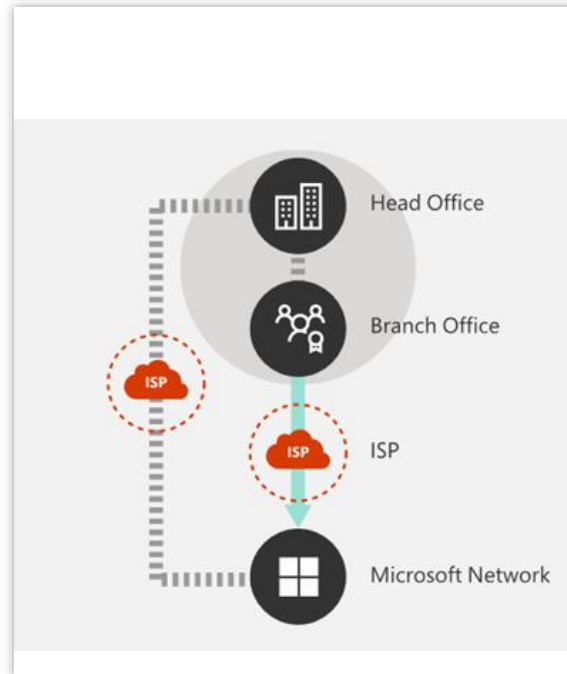
Prepare you network for Microsoft 365

6. Information protection	
5. Mobile device management	
4. Office 365 ProPlus	
3. Windows 10 Enterprise	
2. Identity	
1. Networking	Security



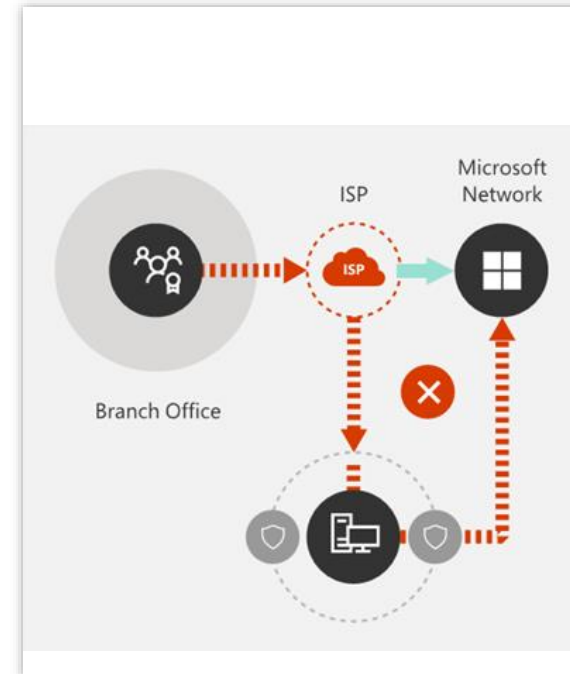
Differentiate traffic

Identify and differentiate Office 365 traffic using Microsoft published endpoints data; Optimize, Allow and Default. new web service publishes Office 365



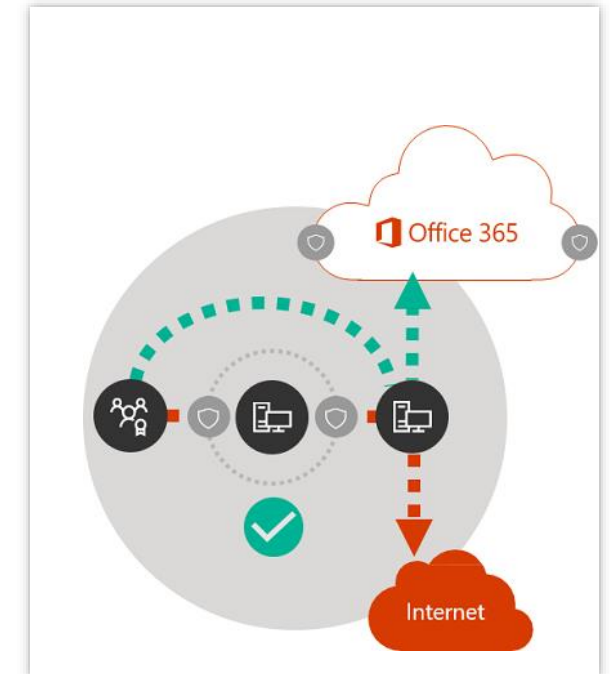
Egress connections

Egress Office 365 data connections as close to the user as practical with matching DNS resolution



Optimize route length

Avoid network hairpins and optimize connectivity directly into the nearest entry point into Microsoft's network

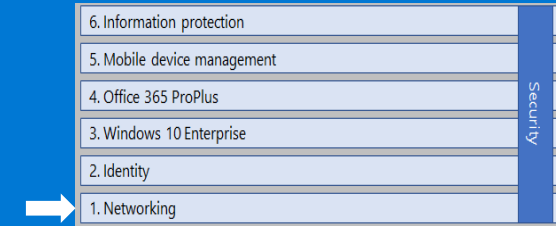


Assess network security

Assess bypassing proxies, traffic inspection devices and duplicate security which is available in Office 365

Networking

Prepare you network for Microsoft 365

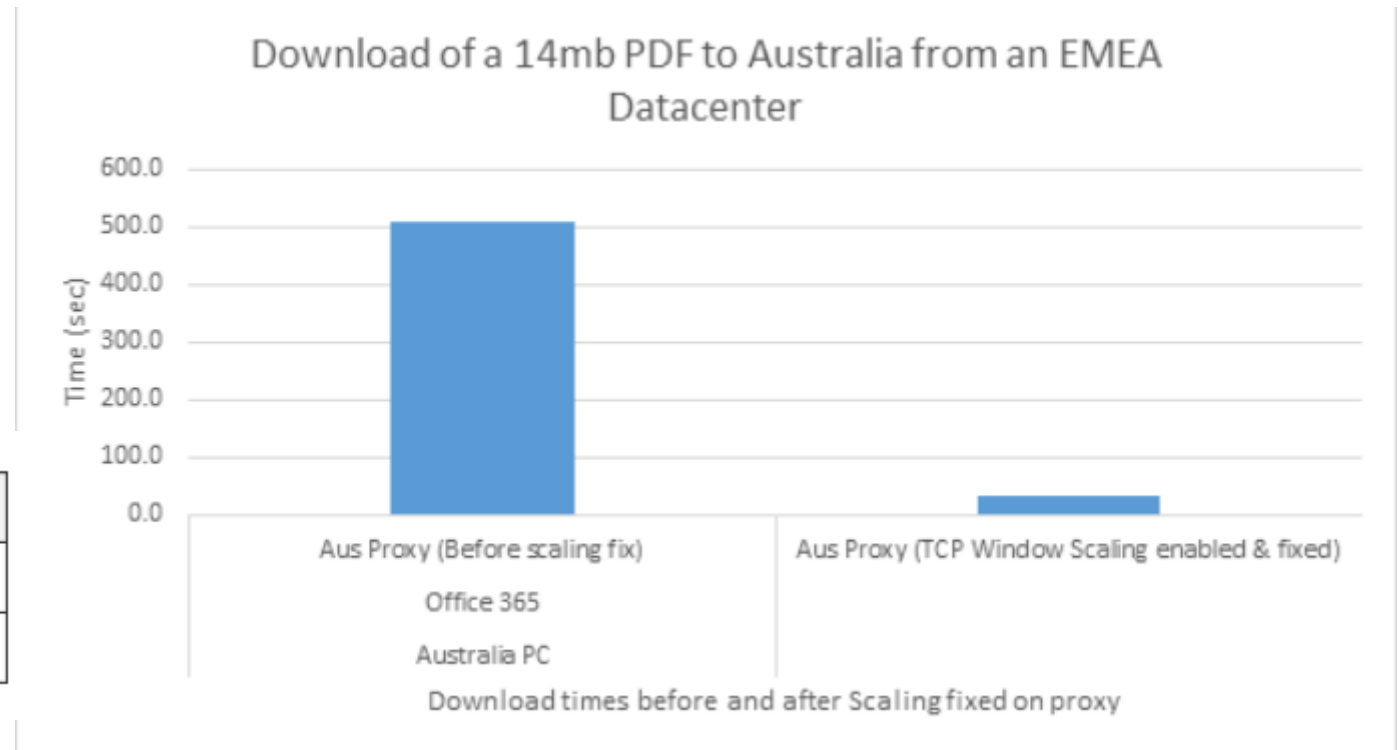


• Office 365 service performance

```
C:\Users>netsh int tcp show global
Querying active state...

TCP Global Parameters
-----
Receive-Side Scaling State      : enabled
Chimney Offload State          : disabled
Receive Window Auto-Tuning Level : normal
Add-On Congestion Control Provider : default
ECN Capability                  : disabled
RFC 1323 Timestamps            : disabled
Initial RTO                     : 3000
Receive Segment Coalescing State : enabled
Non Sack Rtt Resiliency         : disabled
Max SYN Retransmissions        : 2
Fast Open                       : enabled
Fast Open Fallback              : enabled
Pacing Profile                  : off
```

TCP Window Scaling enabled?	Maximum TCP receive buffer (Bytes)
No	65535 (64k)
Yes	1073725440 (1gb)



Identity

6. Information protection	
5. Mobile device management	
4. Office 365 ProPlus	
3. Windows 10 Enterprise	
2. Identity	
1. Networking	

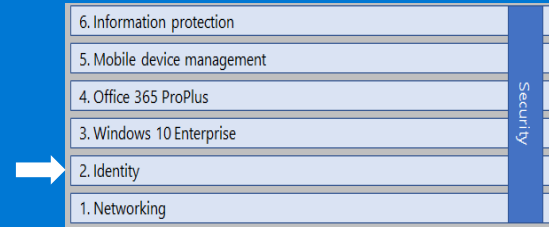
Security

- Plan for ADDS and Azure groups
 - Use groups for easier management
- Secure your privileged identities
 - Configure secure user authentication
- Configure hybrid identity
- Plan your identity infrastructure



Identity

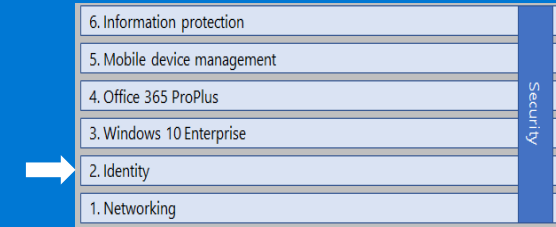
Plan for ADDS and Azure groups



- Use group-based licensing
- Use dynamically based groups (such as department, device)
- Automatically provision protect access (MFA / Conditional access)

Identity

Secure your privileged identities



- Create dedicated global administrator accounts
 - Use strong password
 - Use Multi-Factor Authentication
 - Use a conditional access policy
 - Protecting administrator accounts
- Perform day to day administration by assigning [specific administrator roles](#)
 - Global administrator
 - Exchange administrator
 - SharePoint administrator
 - Security administrator
 - Conditional access administrator

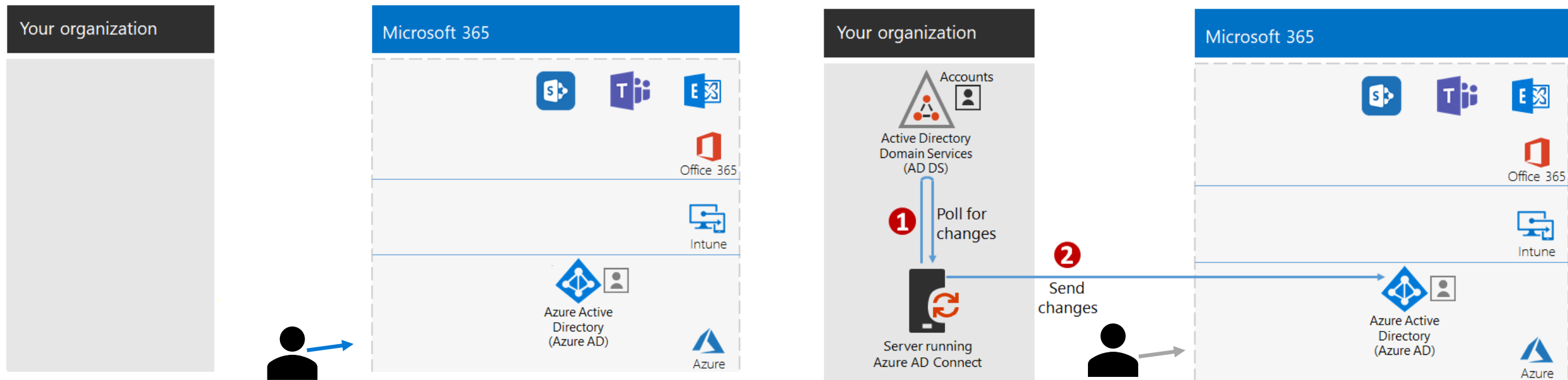
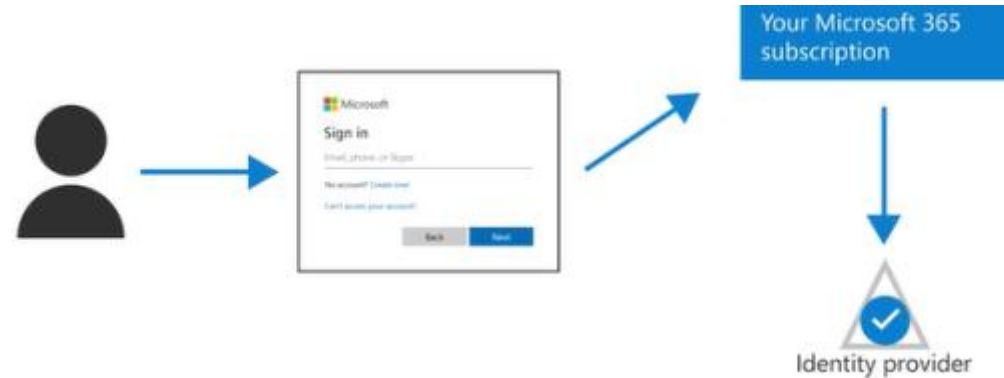
Identity

Configure hybrid identity

6. Information protection

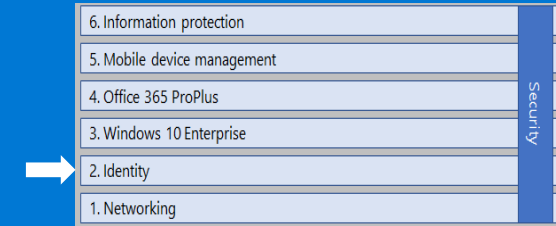
1. Hybrid identity
2. Pass-through Auth.

- Users & Device
 - Cloud-only identity
 - Hybrid identity



Identity

Plan your identity infrastructure



- [Before you synchronize cleanup you AD DS](#)
 - Unique email address “proxyAddresses” attribute
 - Remove any duplicate values in the “proxyAddresses”
 - Ensure a valid and unique value for “userPrincipalName” Attribute. AD DS UPN = Azure AD UPN
- Directory object and attribute preparation
- Prepare the userPrincipalName attribute
 - UPNs in Azure Active Directory and your AD DS match and are using a valid domain namespace.

- **sAMAccountName**
 - Maximum number of characters: 20
 - The attribute value must be unique within the directory.
 - Invalid characters: [\ " | , / : < > + = ; ? *]
 - If a user has an invalid **sAMAccountName** attribute but has a valid **userPrincipalName** attribute, the user account is created in Office 365.
 - If both **sAMAccountName** and **userPrincipalName** are invalid, the on-premises Active Directory **userPrincipalName** attribute must be updated.

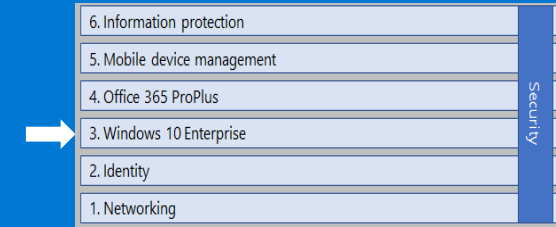
IdFix DirSync Error Remediation Tool

Language: **English**

Download

IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Office 365. IdFix is intended for the Active Directory administrators responsible for DirSync with the Office 365 service.

Windows 10



What's different compared to the last big desktop deployment?



Directory services are moving to the cloud as the fabric for connecting to cloud-based services across apps and services



In-place upgrades are viable and recommended for applying new versions of Windows



UEFI replaces the traditional BIOS and is needed along with 64-bit for many of the modern security and protection capabilities in Windows



Microsoft Intune can manage Windows 10 policies, your connected apps and be configured for co-management with ConfigMgr



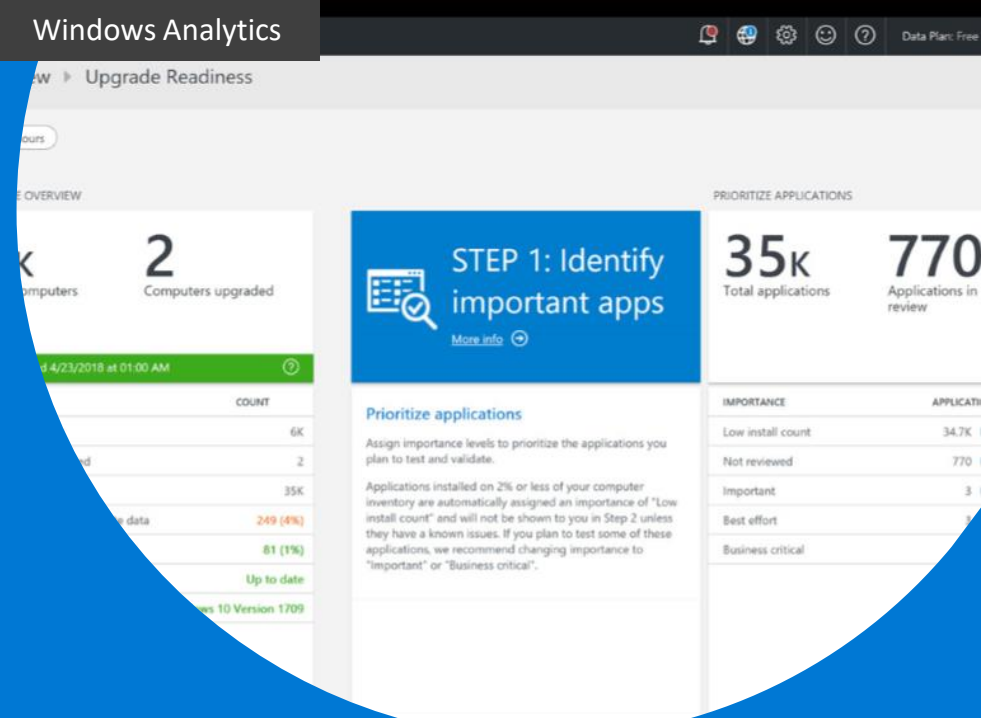
Office 365 ProPlus is the preferred option of Office desktop apps and uses a new package type called Click-to-Run



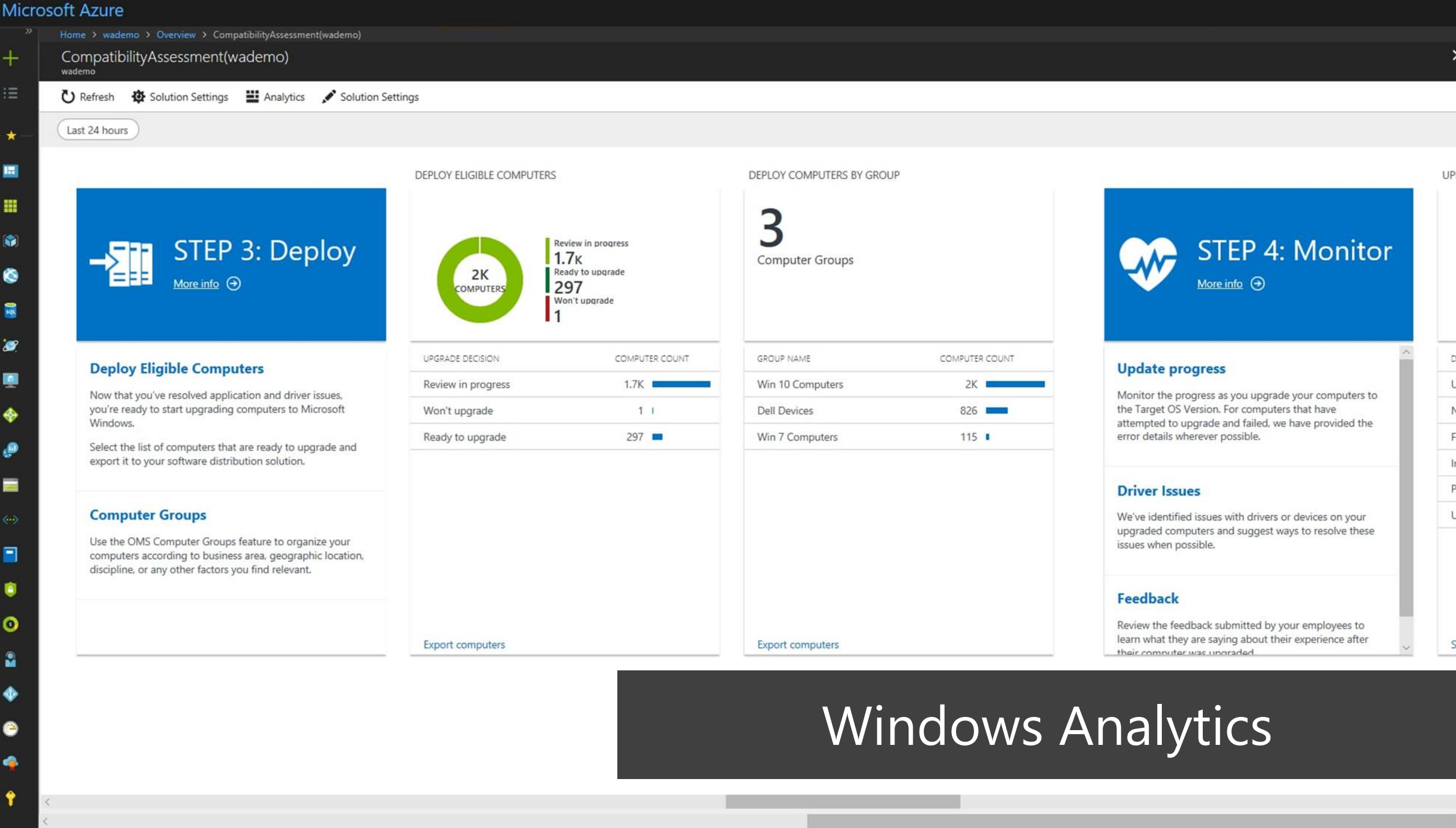
Office 365 ProPlus and Windows 10 are now use semi-annual feature updates and cumulative monthly updates

Device and App Readiness

- Inventory devices and apps under management
- Prioritize devices and apps based on counts and importance
- Windows Analytics Upgrade Readiness helps assess apps and devices against known compatibility status
- Work through hardware and app inventory and use info to target devices ready for deployment
- Engage with Desktop App Assure if incompatible apps are found
- Continue triaging and expanding target devices until deployment is complete
- Implement required fixes for browser-based apps







22

Unique add-ins

100%

Adopted Or Supported add-ins

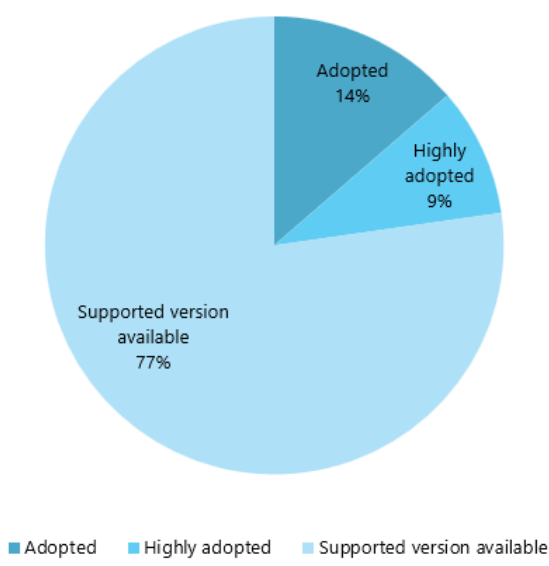
17

Add-ins supported by software provider

0

Add-ins to assess

Overview of add-in readiness for Office 365 ProPlus



■ Adopted ■ Highly adopted ■ Supported version available

[How should I interpret this add-in readiness information?](#)

- 17 Supported version available
- 2 Highly adopted
- 3 Adopted

Which version of Office 365 ProPlus do you plan to deploy?
64-bit

Select which information to display in the report

Office Apps:

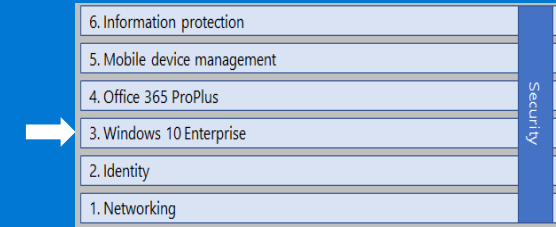
- ☒ Access
- ☒ Excel
- ☒ Outlook
- ☒ PowerPoint
- ☒ Project
- ☒ Publisher
- ☒ Visio
- ☒ Word

Add-ins installed with Office Yes

Readiness Toolkit for Office

Windows 10

Device states in Azure AD



- Cloud deployment and management

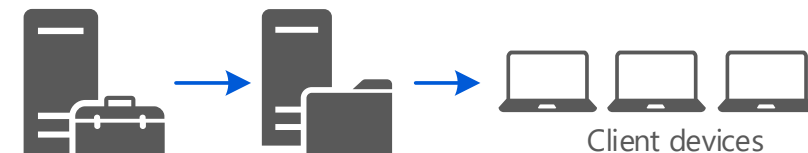
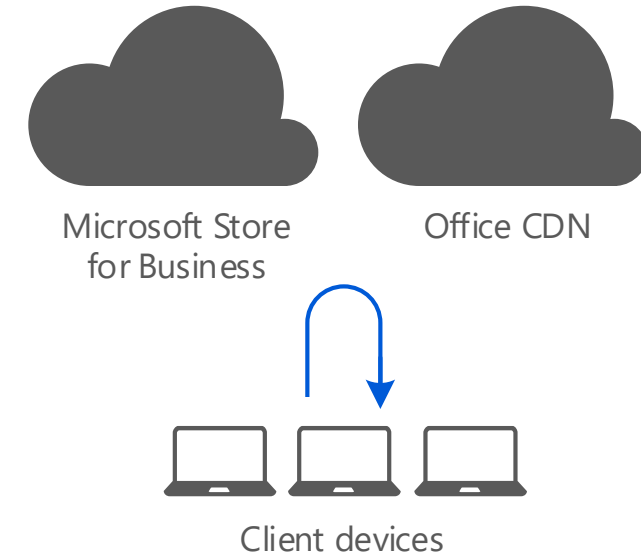
- AutoPilot
- Intune

- SCCM Co-Management

- Central environment

Considerations

- Bare-metal installation
- Bios / Driver updates
- Application update
- Windows defender



Microsoft 365 admin center

Create profile - Microso

+

▼

←

→

↺

🏠

https://devicemanagement.microsoft.com/?ref=AdminCenter#blade/Microsoft_Intune_Enrollment/EnrollmentMenu/windowsEnrollment

📖

☆

⌵

🔍

🔗

⋮

Microsoft 365 Device Management

🔔

⚙️

?

FrankvanLeeuwen@T...
CENTRIC

👤

⏪

Dashboard

Device enrollment - Windows enrollment

Windows Autopilot deployment profiles

Create profile

Dashboard

All services

FAVORITES

Device enrollment

Device compliance

Conditional Access

Security Baselines

Device configuration

Devices

Desktop Analytics

Software updates

Client apps

Users

Groups

Roles

Troubleshoot

Tenant status

Create profile

Windows PC

1 Basics

2 Out-of-box experience (OOBE)

3 Scope tags

4 Assignments

5 Review + create

* Name

Demo_TechEvent

✓

Description

Demo TechEvent

✓

By default, this profile can only be applied to Autopilot devices synced from the Autopilot service. [Learn more](#)

Convert all targeted devices to Autopilot ⓘ

No

Yes

Previous

Next

https://devicemanagement.microsoft.com/?ref=AdminCenter#blade/Microsoft_Intune_Devices/DeviceEntryBlade

🏠

Configure hybrid Azure AD joined devices

Microsoft 365 admin center

Create profile - Microso

https://devicemanagement.microsoft.com/?ref=AdminCenter#blade/Microsoft_Intune_Enrollment/EnrollmentMenu/windowsEnrollment

Microsoft 365 Device Management

FrankvanLeeuwen@T...
CENTRIC

Dashboard

All services

FAVORITES

Device enrollment

Device compliance

Conditional Access

Security Baselines

Device configuration

Devices

Desktop Analytics

Software updates

Client apps

Users

Groups

Roles

Troubleshoot

Tenant status

Dashboard > Device enrollment > Windows enrollment > Windows Autopilot deployment profiles > Create profile

Create profile

Windows PC

Basics

Configure the profile

Deployment mode

Join to Azure AD as

Microsoft Software License Terms

Important information about hiding license terms

Privacy settings

The default value for diagnostic logging

Hide change account options

User account type

Allow White Glove OOB

Apply device name template

Previous

Next

Deployment mode controls if a user needs to provide credentials in order to provision the device.

User-Driven

Select directory service devices will join

Azure AD joined

Hybrid Azure AD joined

Show

Hide

Enable pressing Windows key 5 times to run OOB without user authentication to enroll device and provision all system-context apps and settings. User-context apps and settings will be delivered when the user signs in.

No

Yes

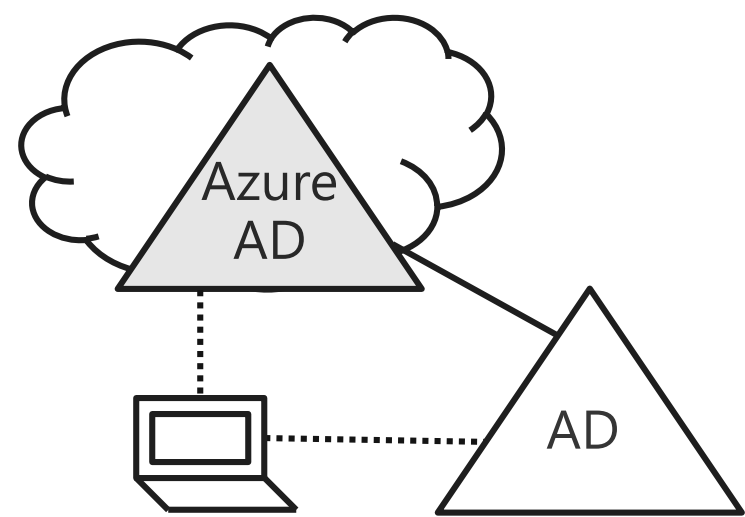
No

Yes

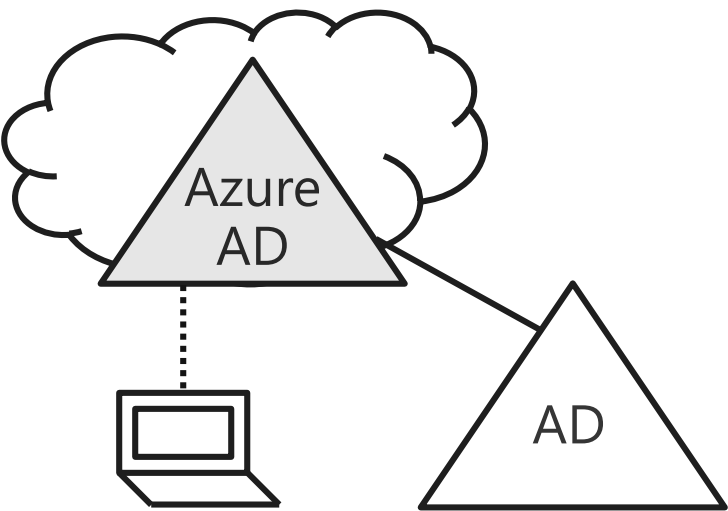
Windows 10

Device states in Azure AD

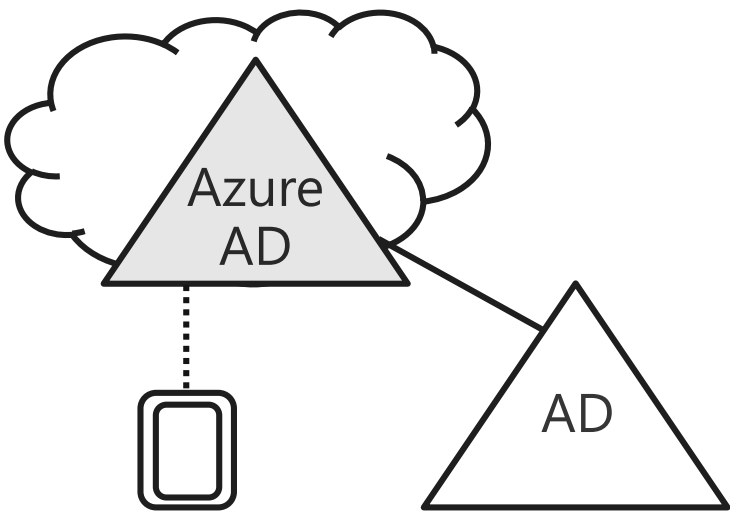
6. Information protection	Security
5. Mobile device management	
4. Office 365 ProPlus	
3. Windows 10 Enterprise	
2. Identity	
1. Networking	



Hybrid Azure AD joined



Azure AD joined

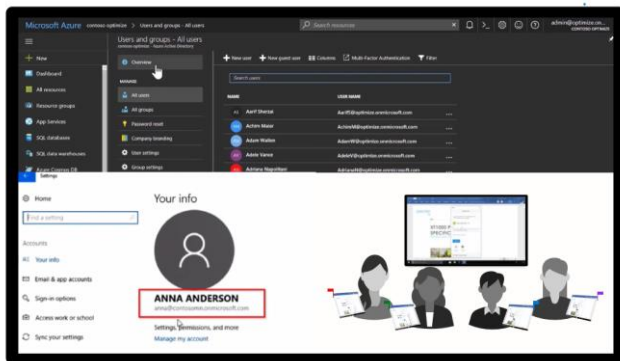


Azure AD registered

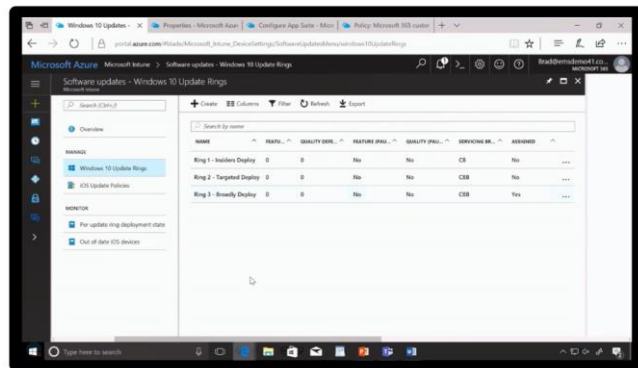
Modern

Hybrid

Future

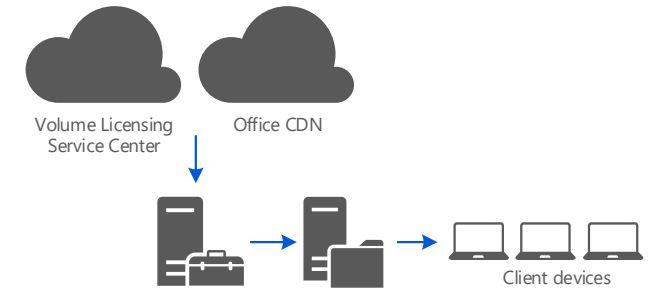


Azure Active Directory, Azure AD Join and co-authoring enabled by Office 365 ProPlus sign-in

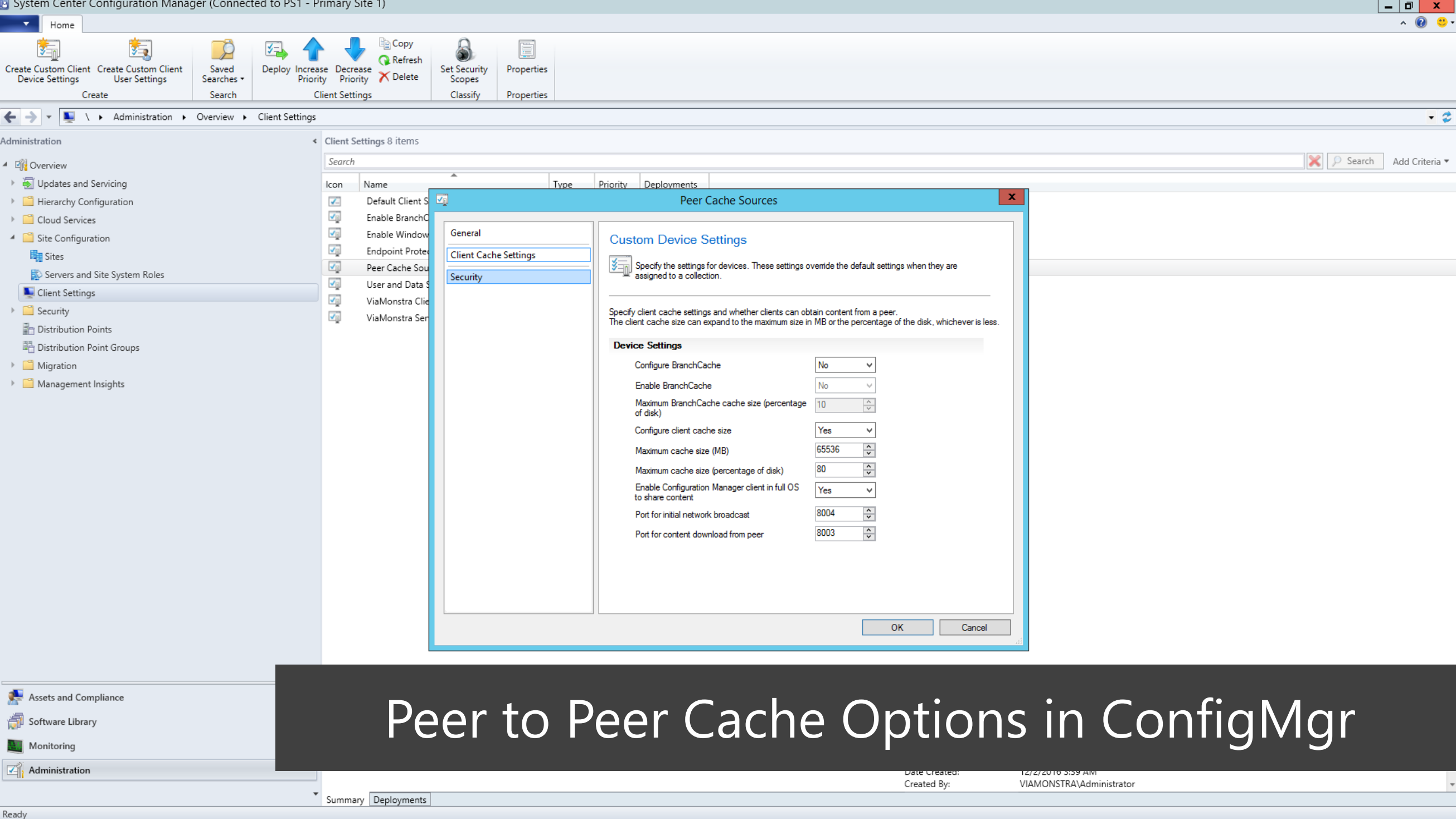


Deployment rings used to validate updates and upgrades before broad deployment

Directory and Network Readiness

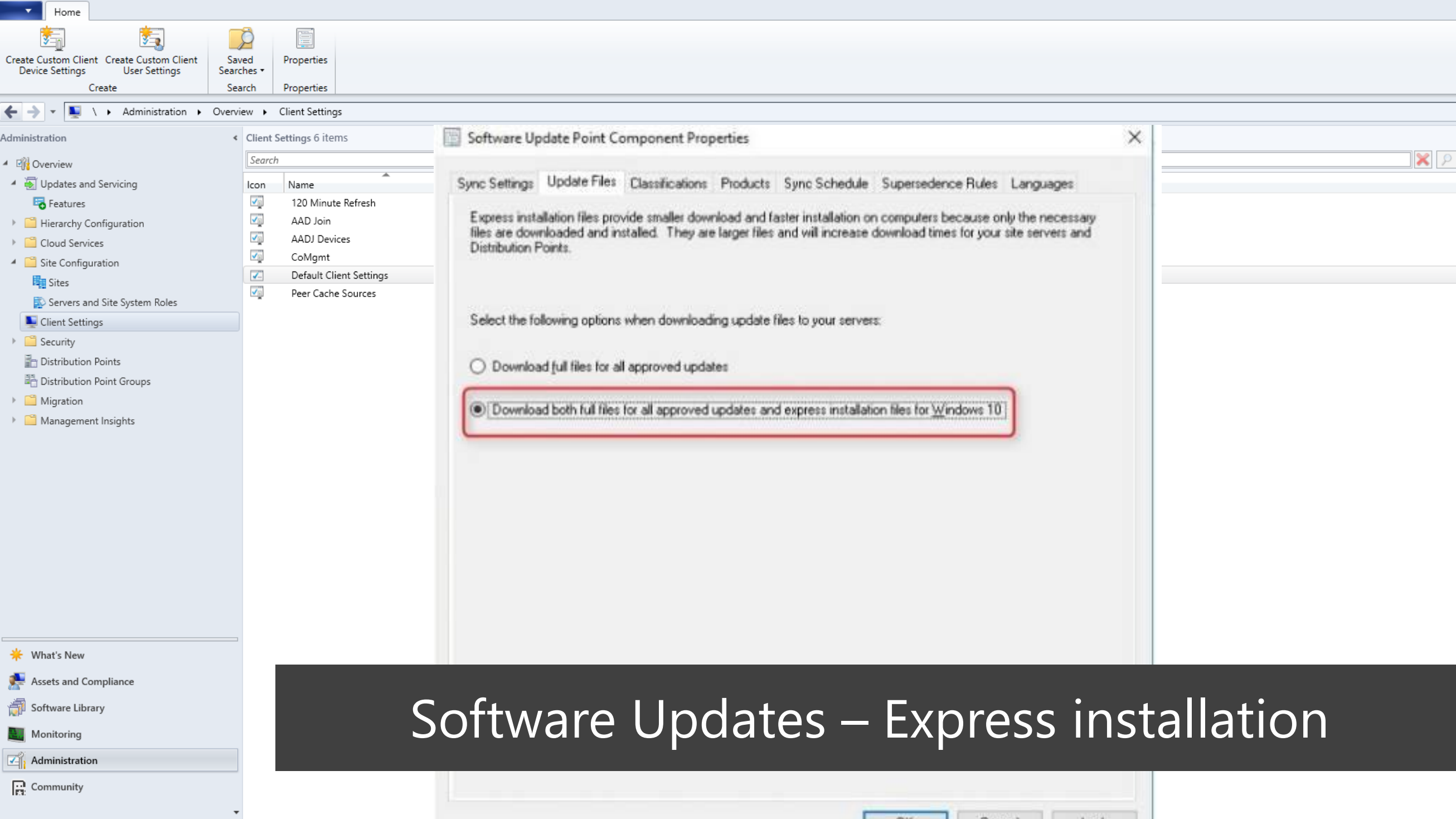


- Azure Active Directory deployed for targeted users + user licensing configured for Office 365 ProPlus
- Network bandwidth requirements calculated for OS, apps, drivers, language packs and user state
- Delivery Optimization, P2P caching, LEDBAT and compression controls configured to control bandwidth
- Plan Office-related networking considerations: OneDrive Known Folder Move, Outlook Data Files, etc.
- Deployment rings and group phases planned based on readiness and network capacity

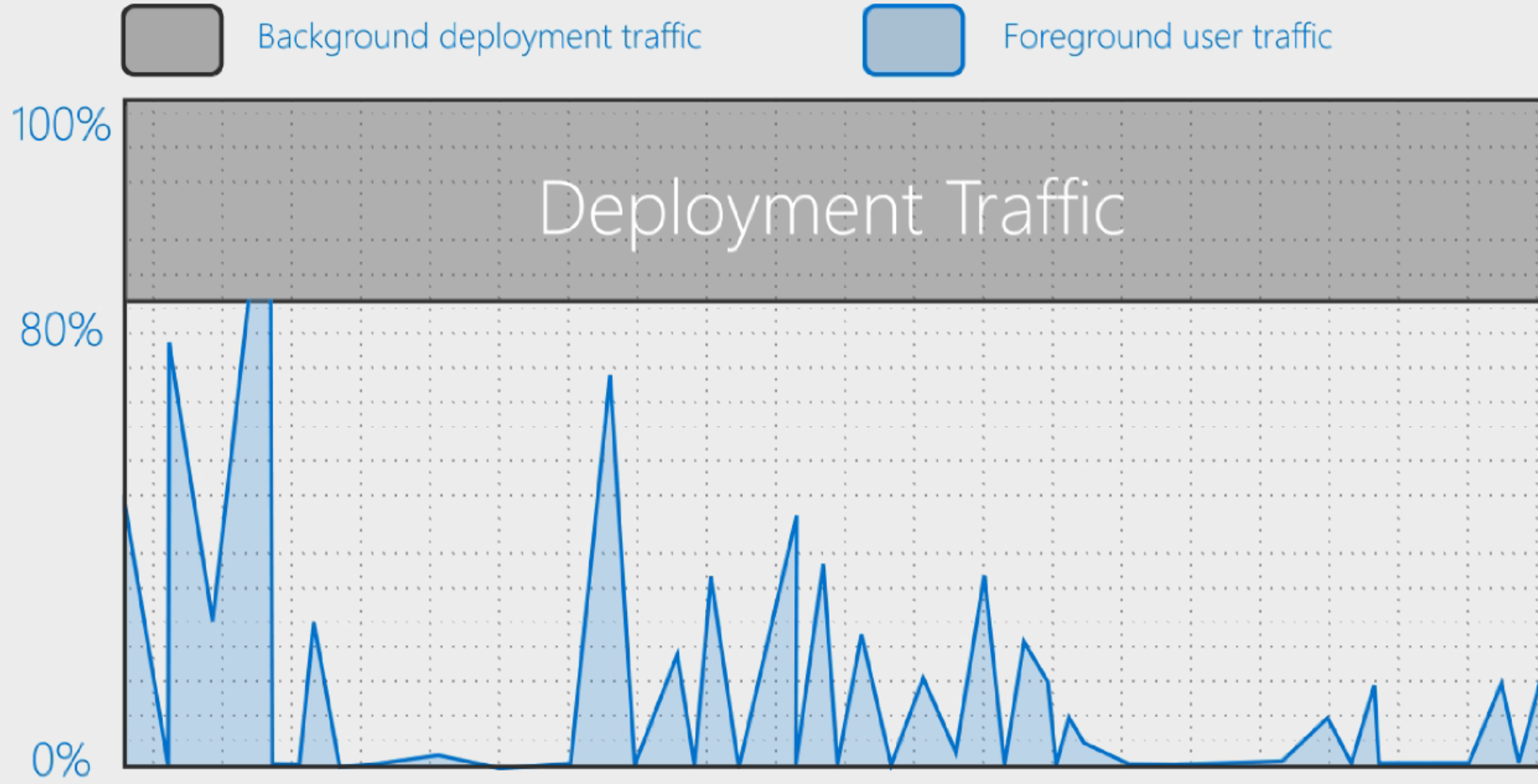


Peer to Peer Cache Options in ConfigMgr

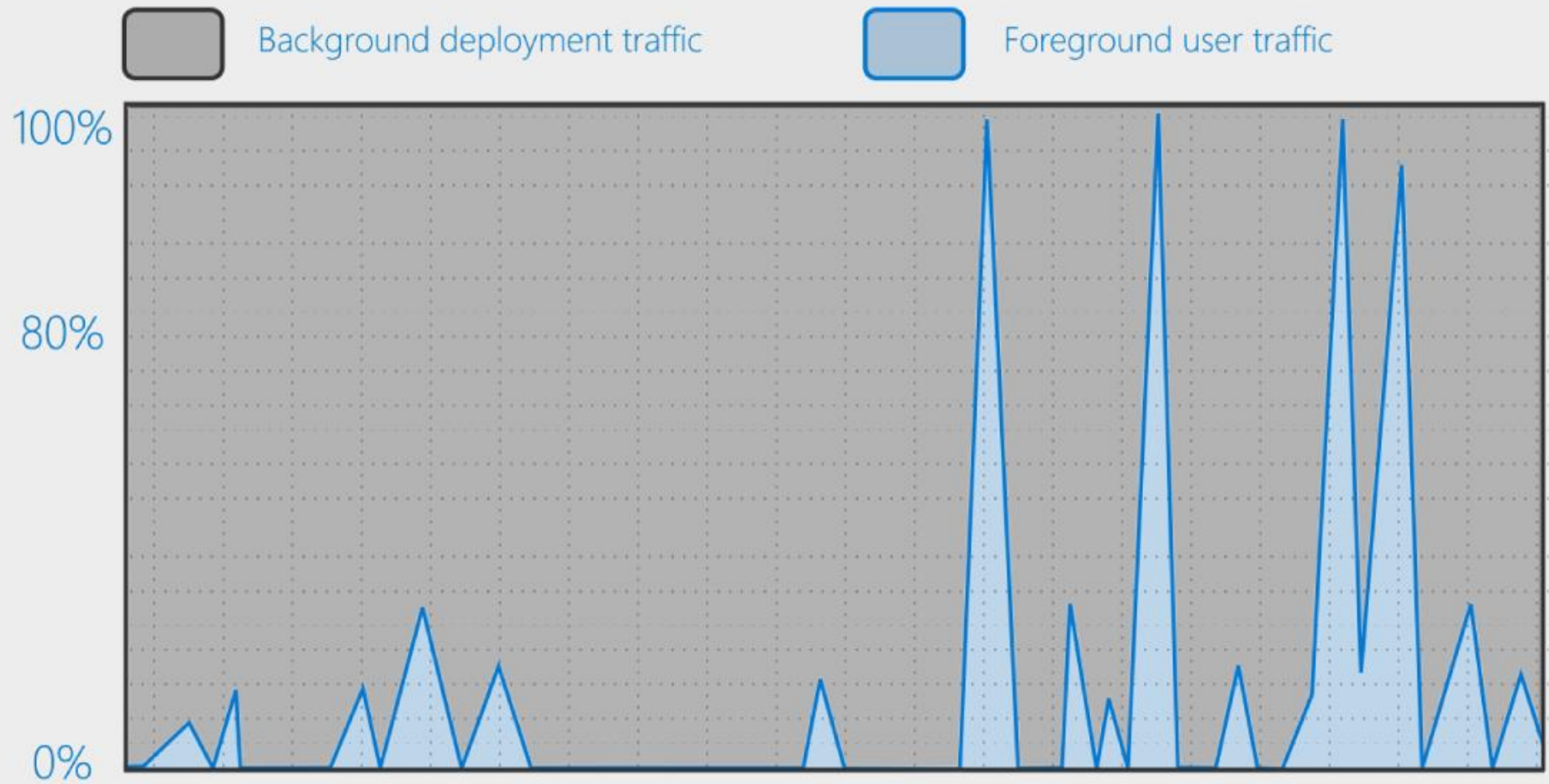
Date Created: 12/27/2016 3:59 AM
Created By: VIAMONSTRA\Administrator



Software Updates – Express installation



Classic Network Throttling



Windows Low Extra Delay Background (LED BAT)

TP-DP.SCCMDOM.COM Properties

Pull Distribution Point Security

General PXE Multicast Group Relationships Content Content Validation Boundary Groups Schedule Rate Limits

A distribution point contains source files for clients to download.

☐ Enable and configure BranchCache for this distribution point

☐ Adjust the download speed to use the unused network bandwidth (Windows LEDBAT)

Description:

Specify how client computers or mobile devices communicate with this distribution point.

☐ HTTP Does not support mobile devices or Mac computers.

☐ Allow clients to connect anonymously

☒ HTTPS Requires computers to have a valid PKI client certificate.

If you manage Mac computers or have mobile devices that are enrolled by Configuration Manager, select an option that allows Internet client connections.

☐ Allow mobile devices to connect to this distribution point

Create a self-signed certificate or import a PKI client certificate.

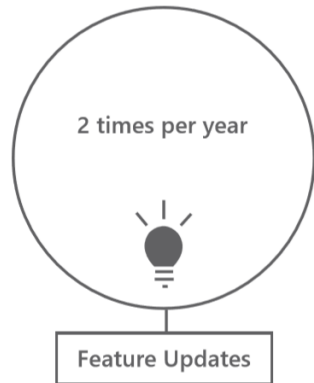
☐ Create self-signed certificate

Set expiration date:

Use the application or package properties to choose how content is copied to this distribution point.

OK Cancel Apply

Enabling LEDBAT In ConfigMgr



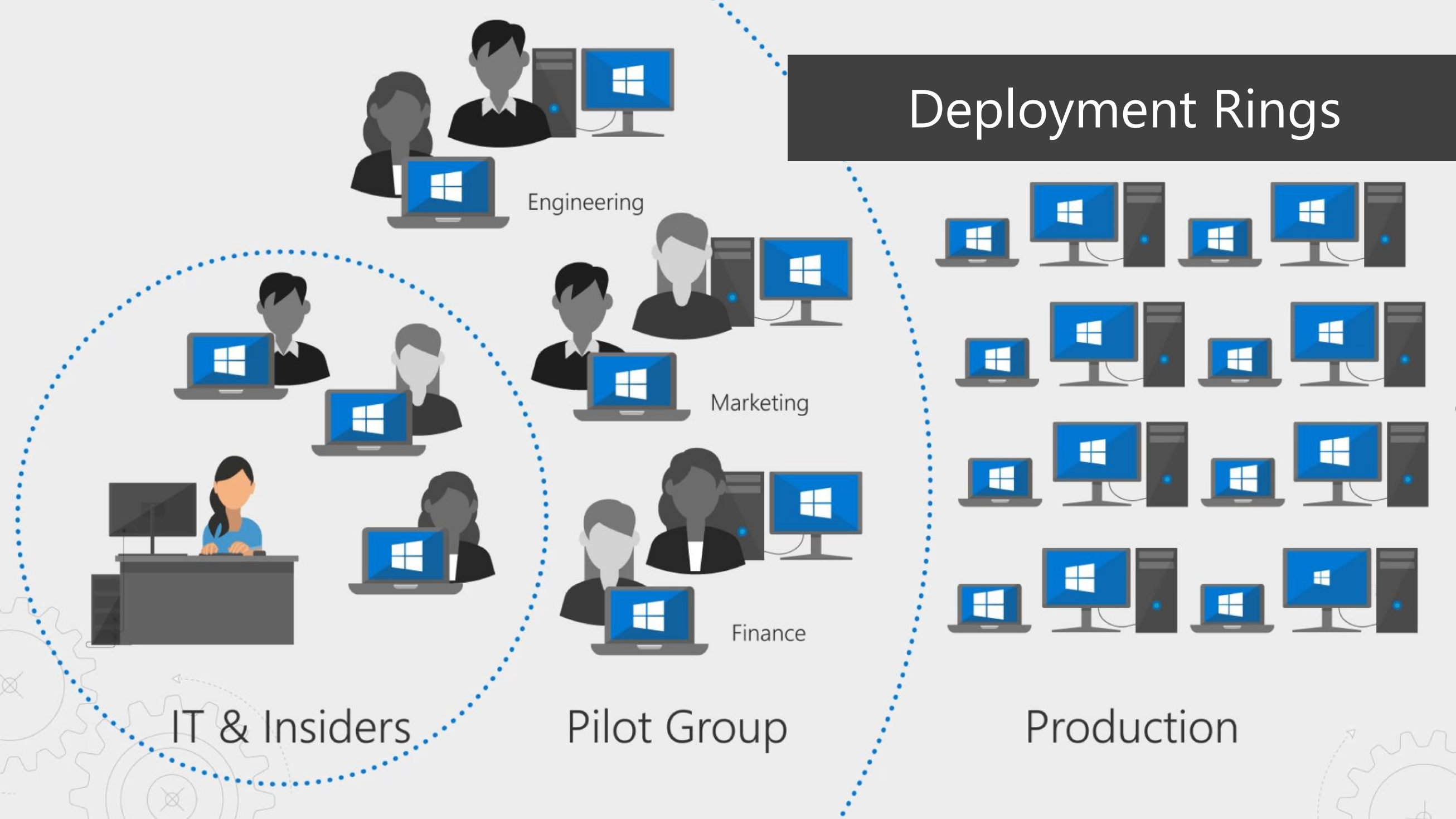
Monthly & Cumulative



Windows- & Office-as-a-Service

- Prepare for semi-annual feature updates to Office and Windows
- Establish Insider team and process to evaluate new Windows and monthly Office updates
- Prepare for updates to software distribution and update management tools as needed
- Operationalize semi-annual deployment processes

Deployment Rings

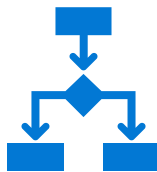
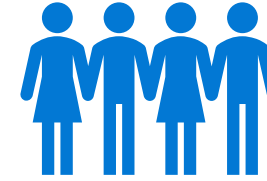
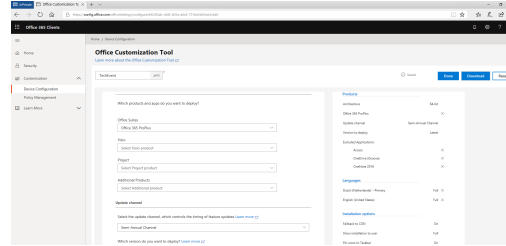


Office 365 ProPlus

Microsoft 365 Enterprise

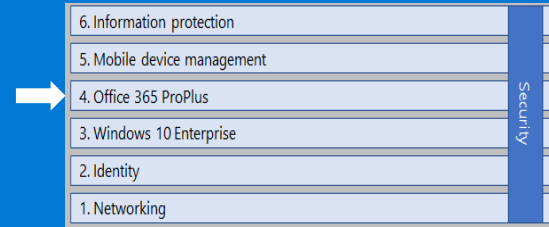
6. Information protection	Security
5. Mobile device management	
4. Office 365 ProPlus	
3. Windows 10 Enterprise	
2. Identity	
1. Networking	

- Impact of Office 365 on the end users
- Office Customization tool
- What should you take in consideration



Office 365 ProPlus

Microsoft 365 Enterprise



InPrivate Office Customization Tool

https://config.office.com/officeSettings/configure/bf20f3ab-cfd8-405a-a8c6-731be5b65ee3/edit

Office 365 Clients

Home / Device Configuration

Office Customization Tool

[Learn more about the Office Customization Tool](#)

TechEvent .xml ✓ Saved Done Download Reset

Which products and apps do you want to deploy?

Office Suites

Office 365 ProPlus

Visio

Select Visio product

Project

Select Project product

Additional Products

Select Additional product

Update channel

Select the update channel, which controls the timing of feature updates [Learn more](#)

Products

Architecture	64-bit
Office 365 ProPlus	X
Update channel	Semi-Annual Channel
Version to deploy	Latest
Excluded Applications:	
Access	X
OneDrive (Groove)	X
OneNote 2016	X

Languages

Dutch (Netherlands) --Primary	Full X
English (United States)	Full X

Installation options

Office 365 ProPlus

Considerations

6. Information protection	
5. Mobile device management	
4. Office 365 ProPlus	
3. Windows 10 Enterprise	
2. Identity	
1. Networking	

Table 4 Outlook with Exchange Online, Outlook in Online Mode (No Cache File)			
Function	Online Mode On-Premises Exchange (Baseline)	Online Mode Exchange Online	Percent Increase/Decrease from baseline

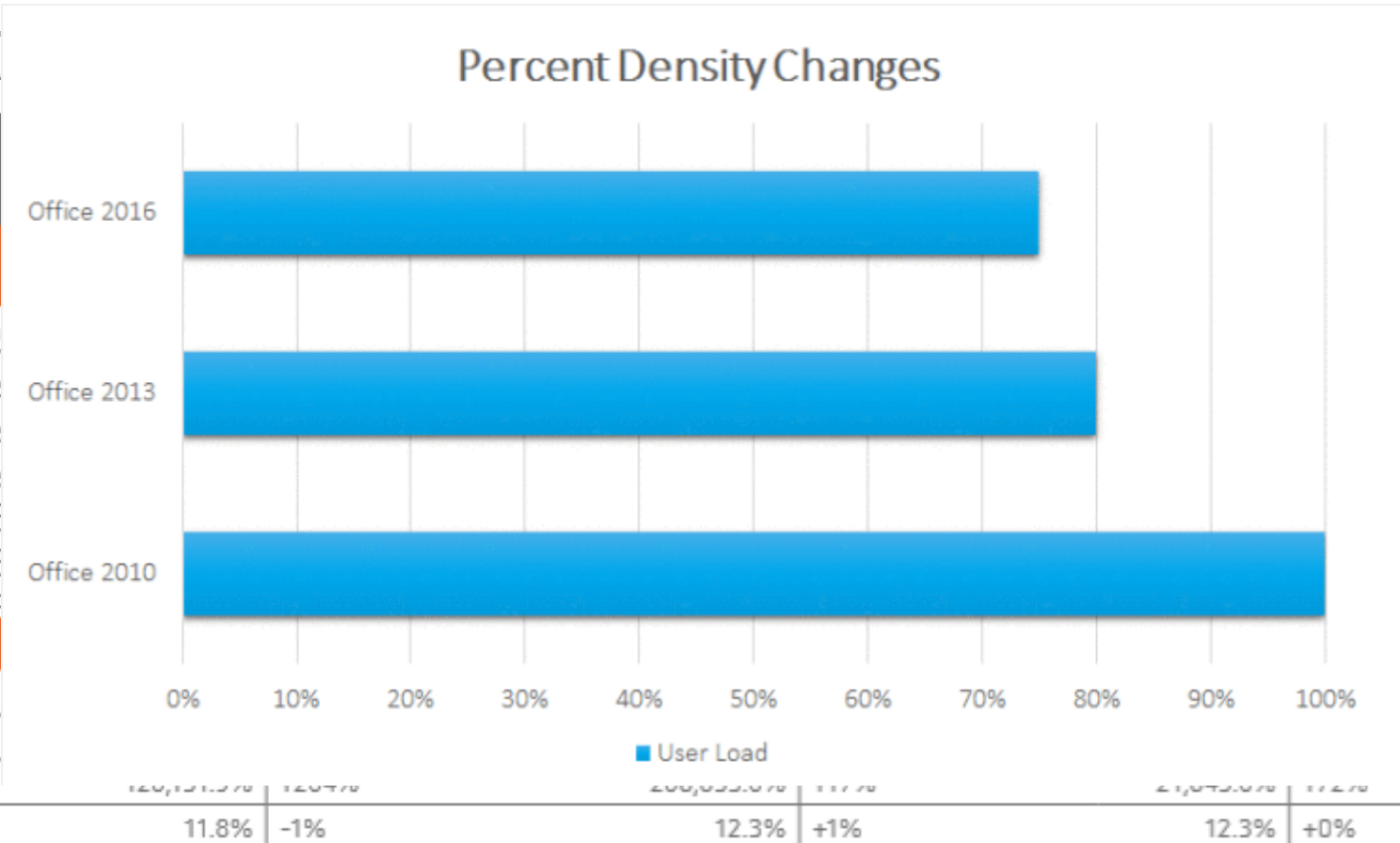
Outlook 2016 start time (preview pane fully loaded)	
Mail display time, 1 MB inline image	
Mail display time, 3 MB inline image	
Mail display time, 6 MB inline image	
Mail send time, local 1 MB attachment	
Mail send time, local 3 MB attachment	
Mail send time, local 5 MB attachment	

Table 5

Function	Outlook Start
Avg CPU	19.3%
Logical Disk	3.1%
Network Bps	36,337.7%
Memory	12.5%

Function	Outlook Start
Outlook 2016 start	
Mail display time	
Mail display time	
Mail display time	
Mail send time, local	
Mail send time, local	
Mail send time, local	

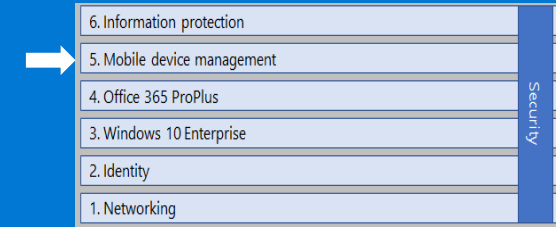
Function	Outlook Start
Avg CPU	
Logical Disk	
Network Bps	
Memory	



Fat client device

Mobile device mangement

Microsoft 365 Enterprise



Windows 10 Enterprise

- Problem check
- Compliance
- Configuration
- App deployment
- Windows update Ring
- Identity threat alerts
- Microsoft Secure Score

Bi-Annually

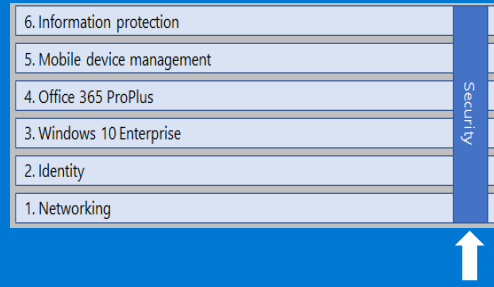
- Update required Windows OS version
- Review new capabilities in Intune
- Review new capabilities in Azure Active directory

Device Management

- Device Configuration Profiles
- App Deployment Policies
- Compliance Policies
- Conditional Access Policies
- Enrollment or Registration
- App Protection Policies

Security

Microsoft 365 Enterprise




- Identity and Access management
 - Protect users identities and control access to valuable resources based on user risk level
- Information Protection
 - Ensure documents and Emails are seen only by authorized
- Threat protection
 - Protect against advanced threats and recover quickly when attacked
- Security management
 - Gain visibility and control over security tools

Security

Microsoft 365 Enterprise

6. Information protection	Security
5. Mobile device management	
4. Office 365 ProPlus	
3. Windows 10 Enterprise	
2. Identity	
1. Networking	



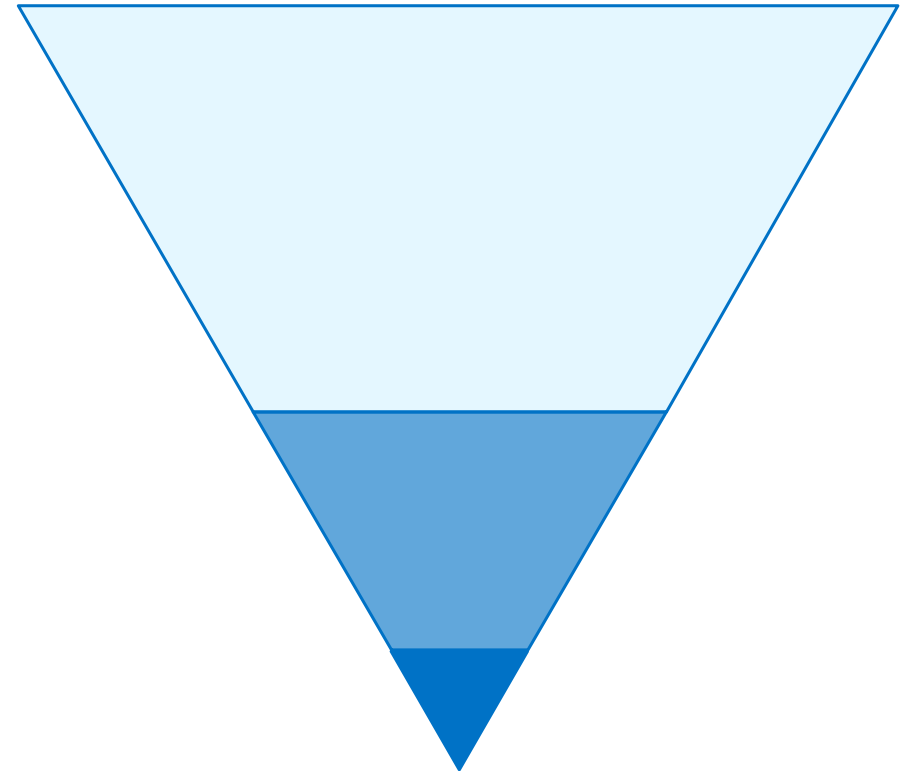
Three tiers of protection for data, identities, and devices

- ① Baseline protection**

Microsoft recommends you establish a minimum standard for protecting data, as well as the identities and devices that access your data. Microsoft provides strong default protection that meets the needs of many organizations. Some organizations require additional capabilities to meet their baseline requirements.
- ② Increased protection**

Some customers have a subset of data that must be protected at higher levels. You can apply increased protection to specific data sets in your Office 365 environment. Microsoft recommends protecting identities and devices that access sensitive data with comparable levels of security.
- ③ Protection for highly regulated environments**

Some organizations may have a very small amount of data that is highly classified, trade secret, or regulated data. Microsoft provides capabilities to help organizations meet these requirements, including added protection for identities and devices.




Security


Microsoft 365 Enterprise


6. Information protection	Security
5. Mobile device management	
4. Office 365 ProPlus	
3. Windows 10 Enterprise	
2. Identity	
1. Networking	


Baseline protection	Sensitive data protection	Highly regulated or classified data
Data protection Find more information about these capabilities here: File Protection Solutions in Office 365 .	Default file encryption	Classification, labeling, and protection
		Bring Your Own Key (BYOK) with Azure Information Protection and SharePoint Online


Baseline protection
Identity and device protection Identity and device capabilities work together to secure access to your data. This document includes more information about these capabilities plus additional recommendations.

**User attributes**
Group membership

**Devices**
Domain Joined
compliant
Platform type
(Windows, iOS, Android)

**Application**
Per app policy
Type of client
(Web, Rich, mobile)

**Location**
IP Range

**Risk**
Session risk
User risk

 ALLOW

 ENFORCE MFA

 BLOCK



Cloud and
On-premises
applications

Enterprise Mobility + Security



Identity and access management



Identity Driven Security



Managed Mobile Productivity



Information Protection

Azure Active Directory Premium P1

Eenmalige aanmelding tot cloud en onpremise applicaties.
Voorwaardelijke basistoegang
beveiliging en selfservice password
reset

Microsoft Advanced Threat Analytics

Identificeren van verdachte
activiteiten & geavanceerde aanvallen
op onpremise Active Directory

Microsoft Intune

Mobiele apparaat en app beheer om
zakelijke apps en gegevens te
beschermen.

Azure Information Protection Premium P1

Labeling, classificatie en bescherming
voor bestanden en opslagplaatsen.
Cloud based file tracking en controle
over toegangsrechten

Azure Active Directory Premium P2

Geavanceerde, op risico gebaseerde
identiteitsbescherming met
waarschuwingen, analyse en herstel.
Voor beheerders gecontroleerde
toegang (Least Privilege)

Microsoft Cloud App Security

Gecontroleerd aanbieden van SaaS
applicaties. Realtime controle &
inzicht op toegang en het gebruik van
SaaS toepassingen en Shadow-IT.

Azure Information Protection Premium P2

Intelligente (automatische)
classificatie & encryptie voor
bestanden binnen en buiten de
organisatie. Tevens mogelijkheid
eigen encryptiesleutel in te zetten.

EMS E5

EMS E3

Windows 10 Enterprise



The most trusted platform

Windows Information Protection
Prevent accidental leaks by separating personal and business data.

Windows Hello for Business
Enterprise grade biometric and companion device login

Credential Guard
Protects user access tokens in a hardware-isolated container

AppLocker
Block unwanted and inappropriate apps from running

Device Guard
Device locked down to only run fully trusted apps

Advanced Threat Protection
Behavior-based, attack detection
Build-in threat intelligence
Forensic investigation and mitigation
Advanced Windows Security & Compliance Reporting



More productive

Azure Active Directory Join
Streamline IT process by harnessing the power of the cloud

MDM enablement
Manage all of your devices with the simplicity of MDM

Windows Store for Business, Private Catalog
Create a curated store experience for employee self-service

Application Virtualization (App-V)
Simplify app delivery and management

Cortana Management
Create, personalize and manage Cortana profiles through Azure Active Directory



More personal

User Experience Virtualization
OS and app settings synchornized across Windows instances

Granular UX Control
Enterprise control over user experience



The most versatile devices

Windows 10 for Industry Devices
Turn any inexpensive, off-the-shelf device, into an embedded, handheld, or kiosk experience


WINDOWS 10 E5

WINDOWS 10 E3

Security

Microsoft 365 Enterprise

6. Information protection	Security
5. Mobile device management	
4. Office 365 ProPlus	
3. Windows 10 Enterprise	
2. Identity	
1. Networking	

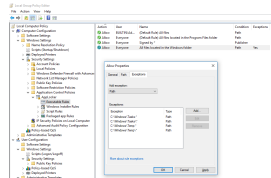


Windows 10 Enterprise

With AppLocker Whitelisting you can secure your system. The most imported directories are;

- C:\Windows Allow
- C:\Programfiles Allow
- C:\Users
- C:\Programdata

Don't allow specific applications!!

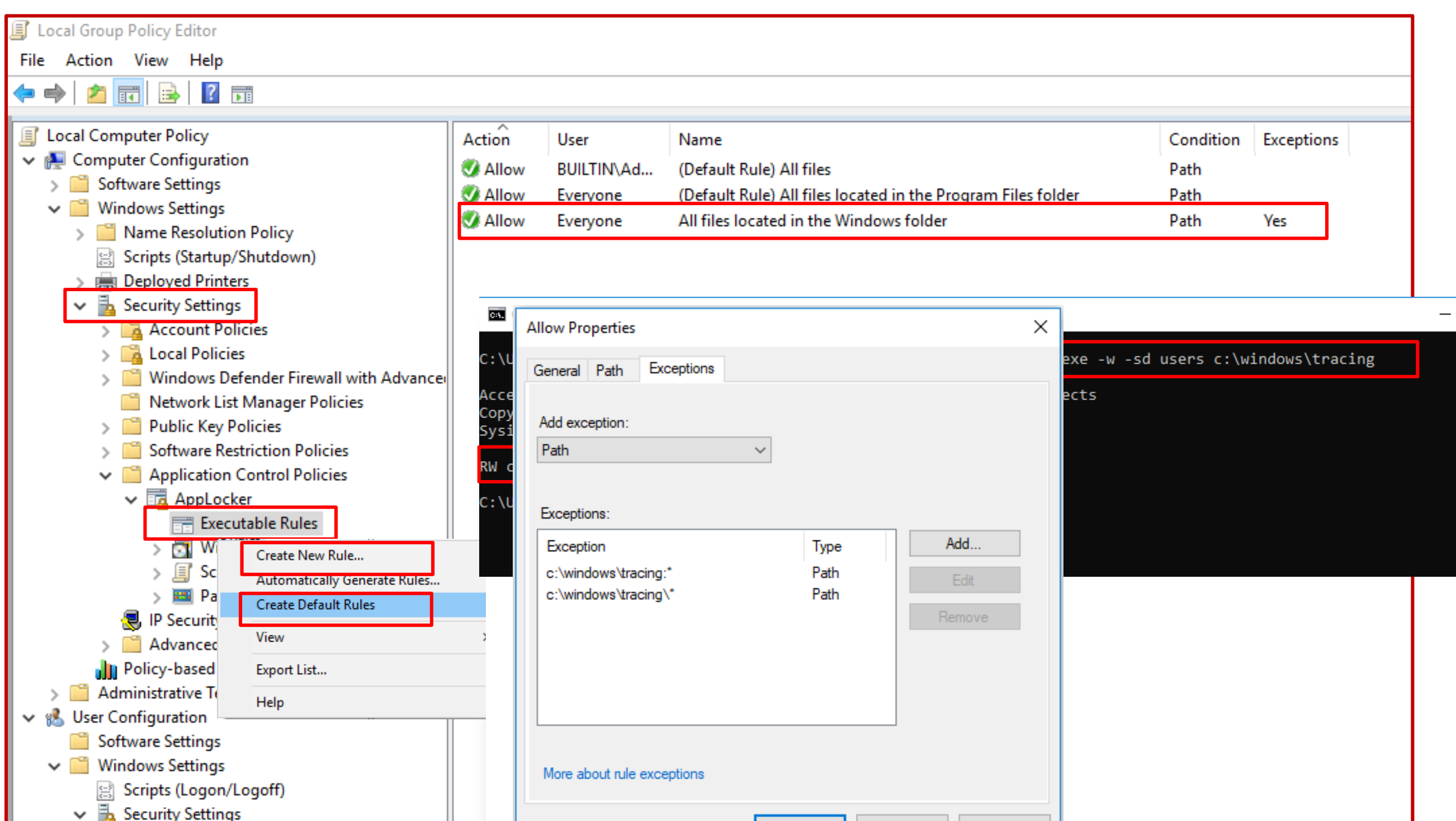


- Microsoft Baseline
- Windows Defender
- Bitlocker
- Applocker
- Biometric authentication
- Windows Information Protection (BYOD)

- Office 365 Threat Intelligence
- Azure Information Protection (AIP)
- Data Loss Prevention policies
- Exchange Online Protection (EOP)

Enterprise Mobility + Security

- Microsoft Intune device-based conditional access policies
- Advanced Threat Analytics
- Azure Multi-Factor Authentication



Action	User	Name	Condition	Exceptions
Allow	BUILTIN\Administrators	(Default Rule) All files	Path	
Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path	
Allow	Everyone	All files located in the Windows folder	Path	Yes

Allow Properties

General Path Exceptions

Add exception:

Path

Exceptions:

Exception	Type
c:\windows\tracing.*	Path
c:\windows\tracing*	Path

Add...

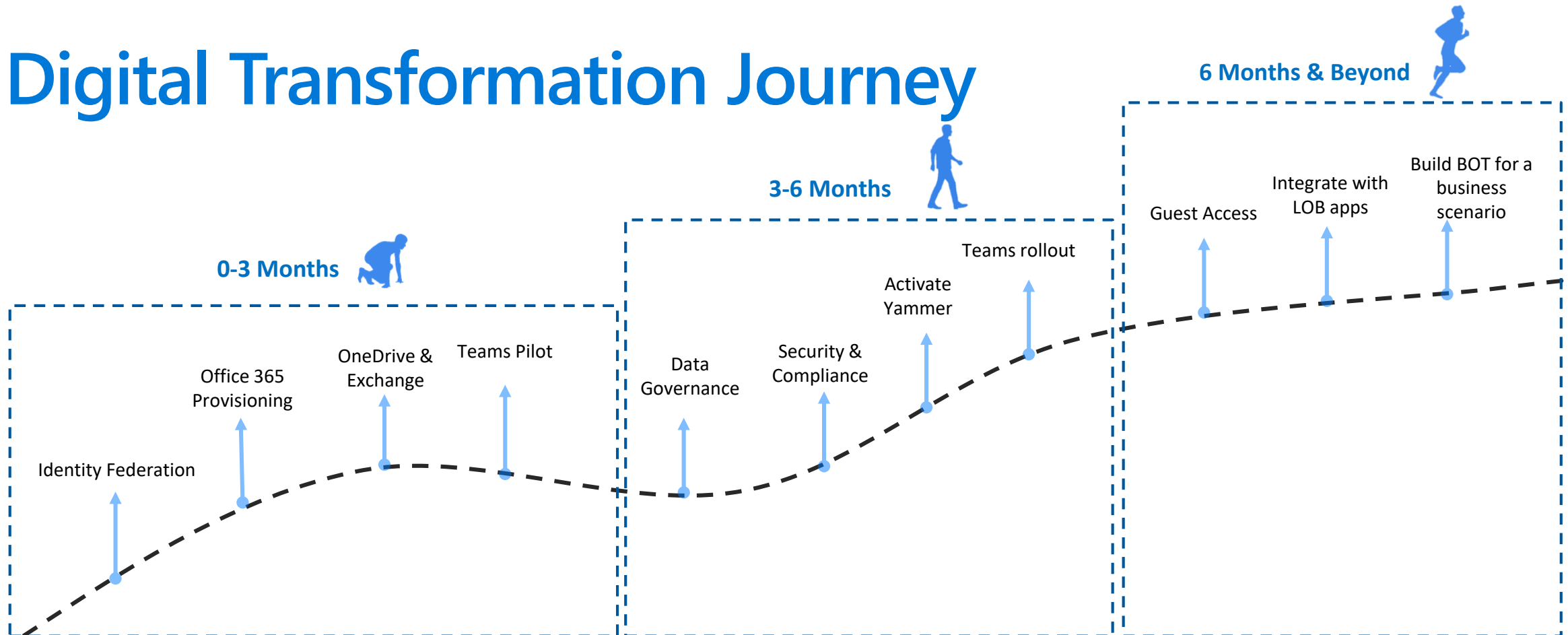
Edit

Remove

[More about rule exceptions](#)

```
cmd.exe -w -sd users c:\windows\tracing
```

Digital Transformation Journey



Adoption & Change Management

Managed Collaboration Service: Office 365 Governance

Managed Security Service: Microsoft 365 Device Security & Information Protection

Managed Collaboration Service

Yammer Network Moderation, Integration of Microsoft Teams and LoB Apps

Now is the time to shift

Learn more at microsoft365.com/shift



Sources

Links

Microsoft Desktop Assessment

- <https://www.microsoft.com/microsoft-365/partners/moderndesktopassessment>

Deploy Microsoft 365 Enterprise

- <https://docs.microsoft.com/en-us/microsoft-365/enterprise/deploy-microsoft-365-enterprise>

Foundation infrastructuur

- <https://docs.microsoft.com/en-us/microsoft-365/enterprise/deploy-foundation-infrastructure>

Desktop Deployment Center

- <https://docs.microsoft.com/en-us/microsoft-365/enterprise/desktop-deployment-center-home>
- <https://blogs.technet.microsoft.com/swisspfe/2018/01/25/branch-cache-vs-peer-cache/>

Office 365 IP Address and URL Web service

- <https://docs.microsoft.com/en-gb/office365/enterprise/office-365-ip-web-service>

Citrix

https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/deployment-guide-office-365-for-xenapp-and-xendesktop.pdf

<https://virtualfeller.com/2016/04/27/microsoft-office-2016-impact-on-xendesktop-scalability/>

AppManageEvent

https://www.youtube.com/watch?v=yjSwSxE_r6w

<https://github.com/api0cradle/UltimateAppLockerByPassList>

Modern Workplace door Frank van Leeuwen

Geef jouw feedback!

Gebruik je mobiel

Ga naar bit.ly/ct19modern

Of start dit op met de QR code;



Windows 10 commercial edition comparison

With enhanced security, more tools for IT and end user productivity features

1. Windows Hello for Business with biometric authentication requires specialized hardware, such as a fingerprint reader, illuminated IR sensor, or other biometric sensors, depending on the authentication method.
2. Requires TPM 1.2 or greater for TPM-based key protection.
3. Windows Information Protection requires either MDM or System Center Configuration Manager to manage settings. Sold separately.
4. Requires Azure AD for automatic MDM enrollment. Requires Microsoft Intune for Blocking Status page. Sold separately.
5. Requires Microsoft Intune or third-party MDM service. Sold separately.
6. Not all MDM capabilities are available in the Home SKU. MDM requires an MDM product such as Microsoft Intune or other third-party solutions, sold separately.
7. Requires Azure AD for identity management. Sold separately.
8. Requires Azure AD and Microsoft Intune, sold separately.
9. Available in select markets. Functionality and apps may vary by region and device.
10. Requires Bing for business to search across company resources and portals. Requires Office 365 subscription, sold separately, to search across OneDrive for Business and SharePoint locations.
11. Shows up to 30 days of past activities done on table and mobile phone when users are signed into their Microsoft accounts.
12. Available in select markets; experience may vary by region and device.
13. Requires Office 365 subscription. Sold separately.
14. Touch-based capabilities require a touch capable device. Pen accessory sold separately.
15. Users must link their mobile phone to their PC in PC settings, install the appropriate app for their device, and follow the setup prompts.
16. Touch capable device required. Pen accessory sold separately.
17. Remix 3D catalog available in select markets. Experience may vary by region and device.

	Home	Pro	Pro for Workstations	Enterprise E3	Enterprise E5
Intelligent security Advanced security, powered by cloud intelligence, that proactively protects your business.					
Attack surface reduction					
Next-generation protection					
Endpoint detection and response					
Automatic investigation and remediation					
Security posture					
Cross-platform extensibility and integration					
Multifactor authentication and biometrics ¹					
Credential protection					
Full-volume encryption ²					
Data loss prevention ³					
Simplified updates Tools and insights IT can trust to simplify deployment and updates, freeing resources to drive more business value.					
Windows Analytics Upgrade Readiness					
Windows Analytics Update Compliance					
Windows Analytics Device Health					
Windows as a service					
Windows Update for Business					
Flexible management Comprehensive endpoint management that supports traditional, cloud, or hybrid IT on your terms.					
Windows Autopilot ⁴					
Single or multi app kiosk mode ⁵					
Mobile device management (MDM) ⁶					
Windows 10 Subscription Activation ⁷					
Hybrid Azure AD Join ⁸					
Mobile Application Management (MAM)					
Microsoft Store for Business ⁹					
Manage user experiences					
Enhanced productivity An intuitive experience with built-in features that help employees collaborate and work efficiently.					
Enterprise search ¹⁰					
Windows Timeline ¹¹					
Microsoft Edge					
Cortana ¹²					
Office 365 on Windows ¹³					
Microsoft Whiteboard ¹⁴					
OneNote					
Continue on PC ¹⁵					
Windows Ink ¹⁶					
3D in Windows 10 ¹⁷					

Office 365 Commercial Plan Comparison

Office 365 Commercial Plan Comparison		Business ¹			Enterprise ²				
		Business	Business Essentials	Business Premium	ProPlus	F1	E1	E3	E5
Standard Services	Estimated retail price per user per month \$USD (with annual commitment)	\$8.30	\$5	\$12.5	\$12	\$4	\$8	\$20	\$35
	Install Office on up to 5 PCs/Macs + 5 tablets + 5 smartphones per user	Business ³		Business ³	ProPlus ⁴			ProPlus ⁴	ProPlus ⁴
	Access to Office apps and documents from all major smartphones and iPad	●		●	●			●	●
	OneDrive for Business – personal online document storage	1 TB	1 TB	1 TB	1 TB	2 GB ⁹	1 TB	1-5+ TB ⁸	1-5+ TB ⁸
	Office Mobile Apps – Create/edit rights for commercial use of Office Mobile apps ¹⁴	●	● ¹⁸	●	●	● ¹⁸	● ¹⁸	●	●
	Office Online – Create/edit rights for online versions of core Office apps	●	●	●	●	●	●	●	●
	Sway for Office 365 ⁵	●	●	●	●	●	●	●	●
	To-Do – Personal task management app		●	●		●	●	●	●
	PowerApps and Flow		●	●		● ¹¹	●	●	●
	Team collaboration & internal portals (SharePoint), Internal social networking (Yammer)		●	●		● ¹⁵	●	●	●
	Email - 50 GB email, contacts, shared calendars (Exchange)		●	●		2 GB ¹³	●	● ¹⁶	● ¹⁶
	Skype for Business, Microsoft Teams – Conferencing, meetings, IM/presence, chat-centered workspace		●	●		● ¹⁰	●	●	●
	Shift scheduling, content sharing, and workgroup messaging			●		●	●	●	●
	Microsoft Bookings			●				●	●
	Outlook Customer Manager, Invoicing, Business center, Listings, Connections & MileIQ			● ¹⁷					
	Microsoft Stream					● ¹²	●	●	●
Advanced Services	On-premises Active Directory synchronization for single sign on	●	●	●	●	●	●	●	●
	Mobile Device Management (MDM) for Office 365 ⁶	●	●	●	●	●	●	●	●
	Access to equivalent on-premise servers (Exchange, SharePoint, Skype for Business)						●	●	●
	Legal compliance & archiving needs for email – archiving, eDiscovery, mailbox hold							●	●
	Information protection – message encryption, rights management, data loss prevention							●	●
	Enterprise Voice w/Skype for Business (on-prem only) ⁷								●
	Office 365 Cloud App Security, Advanced Compliance, Advanced Threat Protection, Threat Intelligence								●
	Threat Intelligence								●
	Data analytics and visualization (Power BI Pro), personal productivity analytics (MyAnalytics)								●
Phone System, Audio Conferencing								●	

See speaker notes section for footnotes