Microsoft

Microsoft 365

Building a Security Practice

Workshop 2: Managing & Securing Devices with Intune

Mark Layton – Design Sales Engineer

Quotes about phones and tablets from IT managers

“People have their own phones and are **putting all kind of crazy stuff** on the phone.”

— Bob, Property management, 150 employees

“Phones: They are **easy to steal easy to lose**, and have ton of information. So we need to protect them.”

— Matthew, Accounting firm, 175 employees

“If they leave phone sitting somewhere [without a PIN] **anyone can pick it up and access their business email**”

— David, Printing, 45 employees

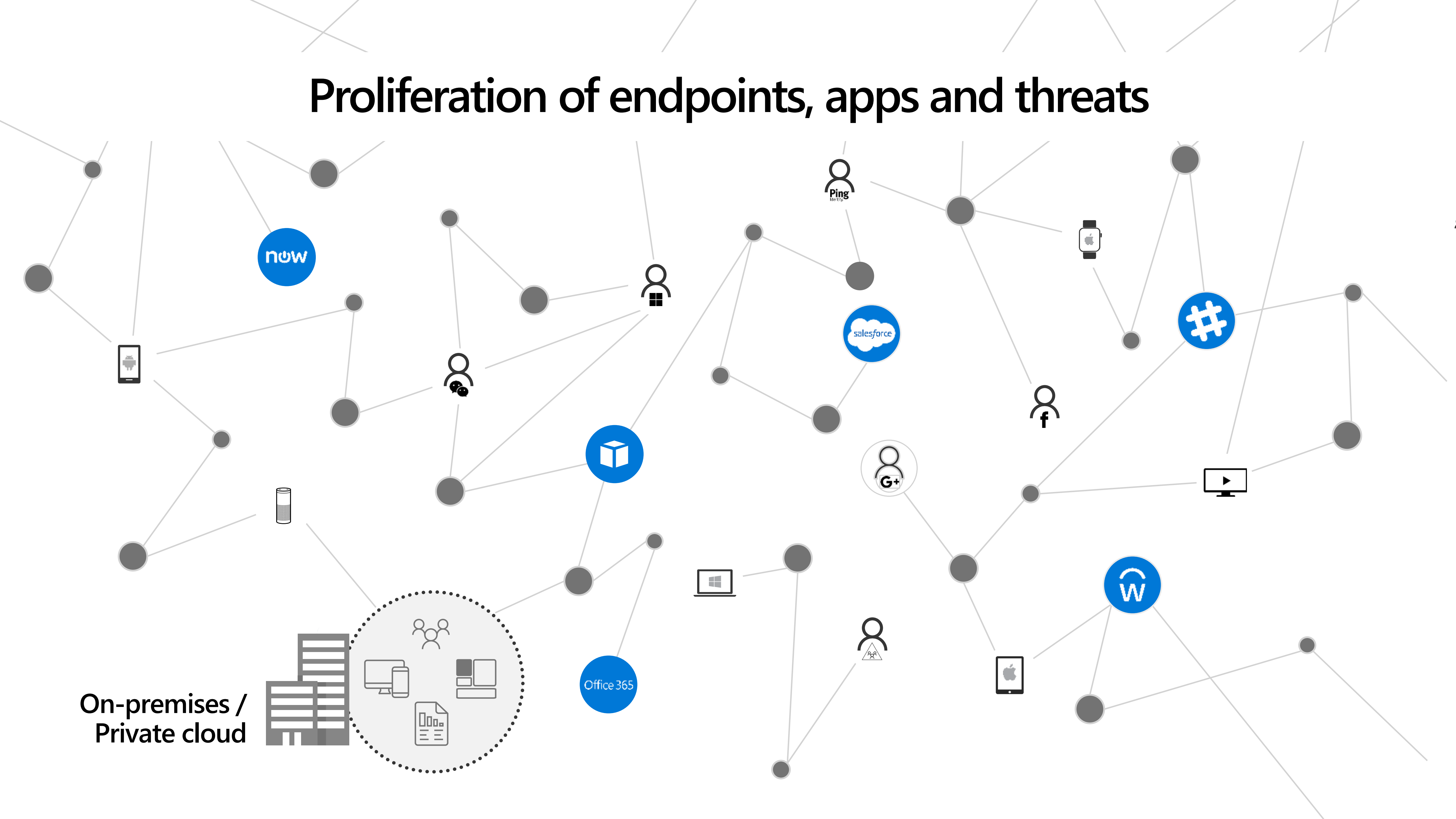
“**Our lawyers wrote up a policy that said we can't wipe phones;**.”

—Vincento, Aviation Consulting, 180 employees

Technology needs are evolving in the modern workplace

Fragmented	→	Integrated
Closed Perimeter	→	Cloud
Less Regulated	→	More Regulated
Manual	→	Automated
Insourced	→	Managed

Proliferation of endpoints, apps and threats



IT challenges of the modern workplace

How do you empower users while
protecting your most important assets?

Employee goals

Collaborate

Easy access

Work
anywhere

IT goals

Protect data

Manage access

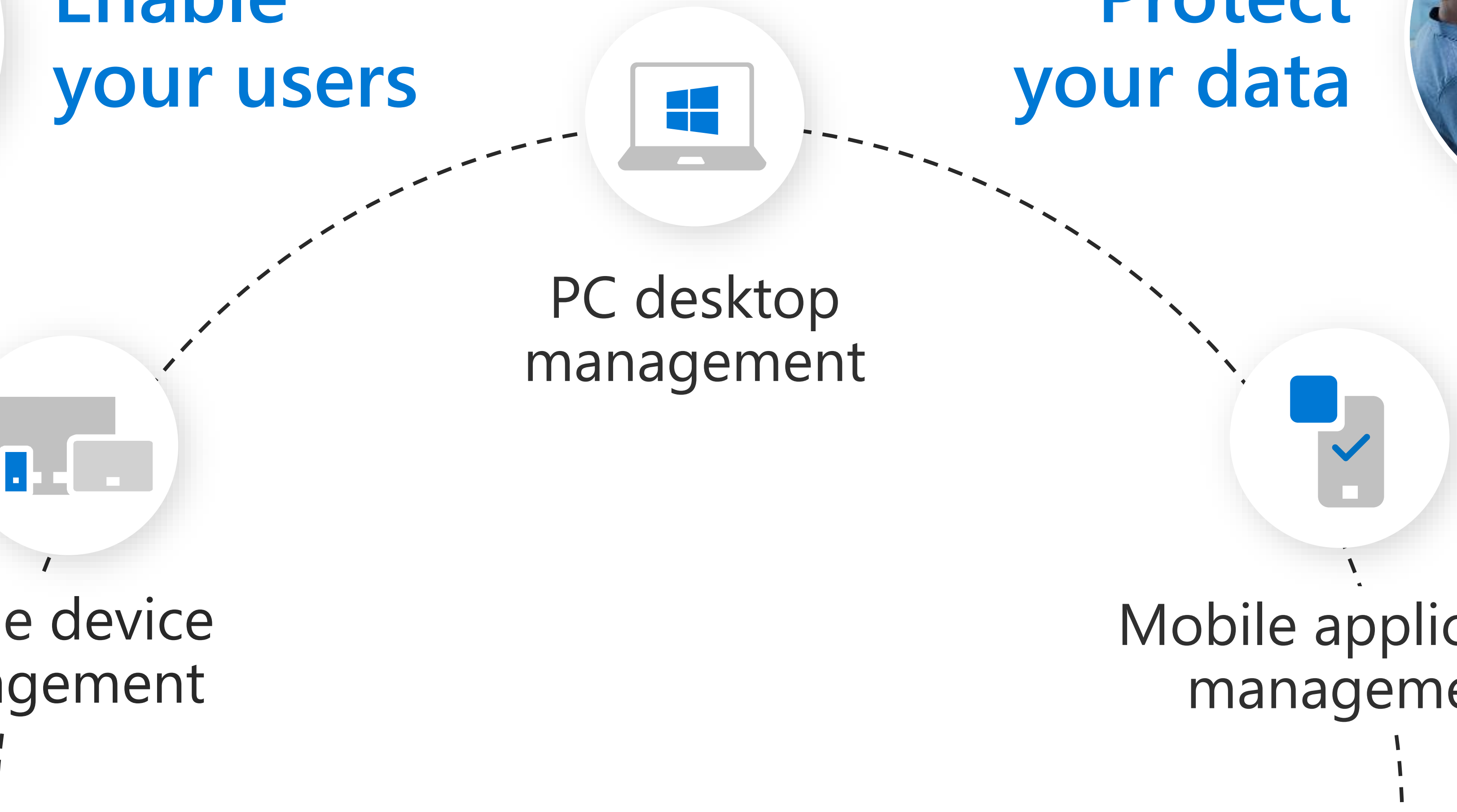
Stay
innovative

Transformative device management and security

Microsoft Flexible Device Management

Enable your users

Protect your data



PC desktop management

Mobile device management

Mobile application management

Why choose Microsoft?

Most complete

Transform how you manage iOS, Android, macOS, and Windows devices, powered by the Microsoft intelligent cloud

Most secure

Apply conditional access and security controls for all apps and data, on corporate and personal devices

Fastest time to value

Maximize user productivity with fast roll-out of new services and out-of-box integration with Microsoft architecture and apps

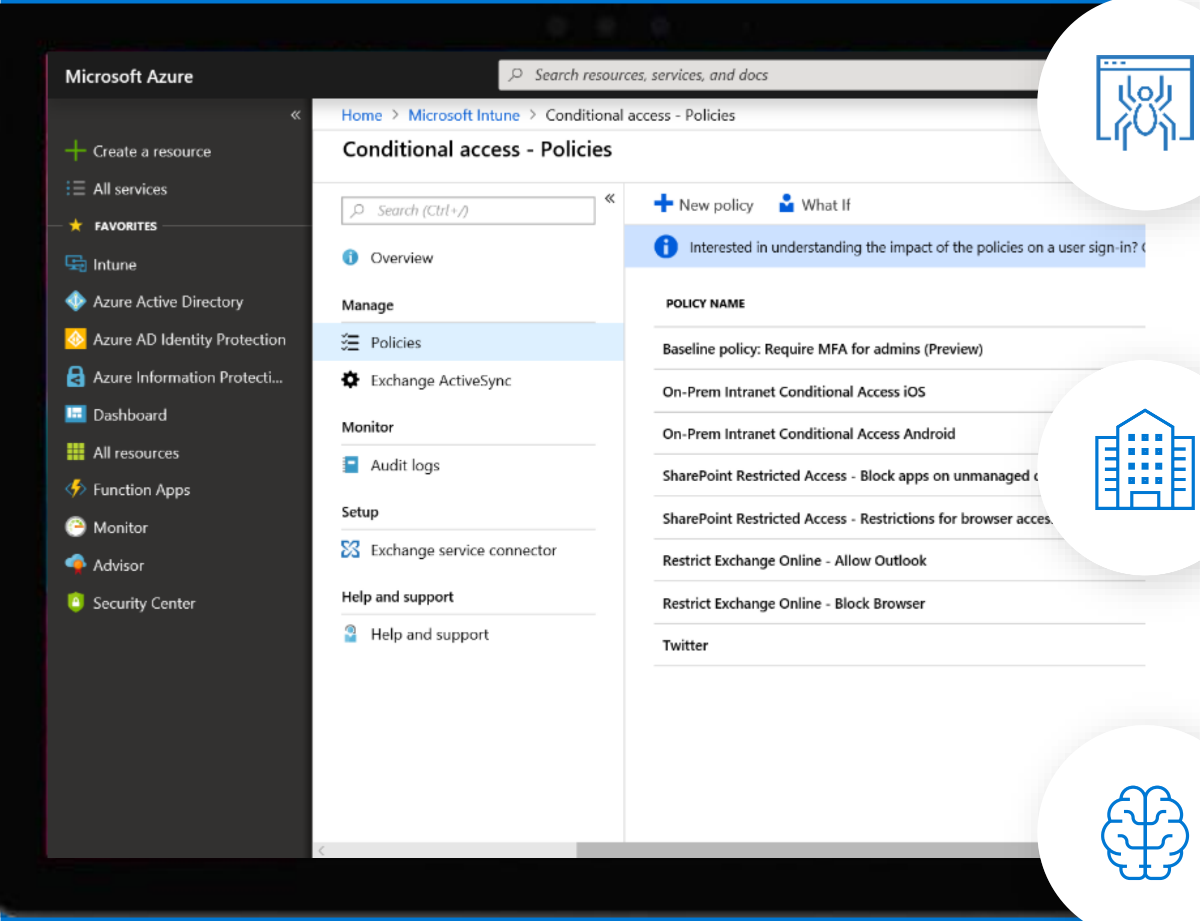
Transform IT delivery and device management

Zero-touch IT provisioning for all devices using Windows Autopilot, Apple Business Manager, or Android Enterprise

App lifecycle management for in-house (LOB) apps, public store apps, and traditional Win32 apps

Depth of **configuration and security controls** across any device

Secure apps and data in the modern workplace



Interested in understanding the impact of the policies on a user sign-in?

POLICY NAME
Baseline policy: Require MFA for admins (Preview)
On-Prem Intranet Conditional Access iOS
On-Prem Intranet Conditional Access Android
SharePoint Restricted Access - Block apps on unmanaged
SharePoint Restricted Access - Restrictions for browser acces
Restrict Exchange Online - Allow Outlook
Restrict Exchange Online - Block Browser
Twitter

Respond to internal and external threats with **real-time risk-analysis** before access to company data

Protect corporate data before, during and after they are shared, even outside the company

Extensive **visibility and intelligent cloud-powered insights** to improve end-to-end security posture

Maximize user productivity

Deliver native **app experiences** that work and feel natural on any platform

Simplify **access to resources** employees need with single sign-on, for faster service roll-out

Enable Office apps that users love on mobile devices, without compromising data security

Securing the devices that connect to your data

Phones Tablets Laptops Desktops

iOS and Android devices

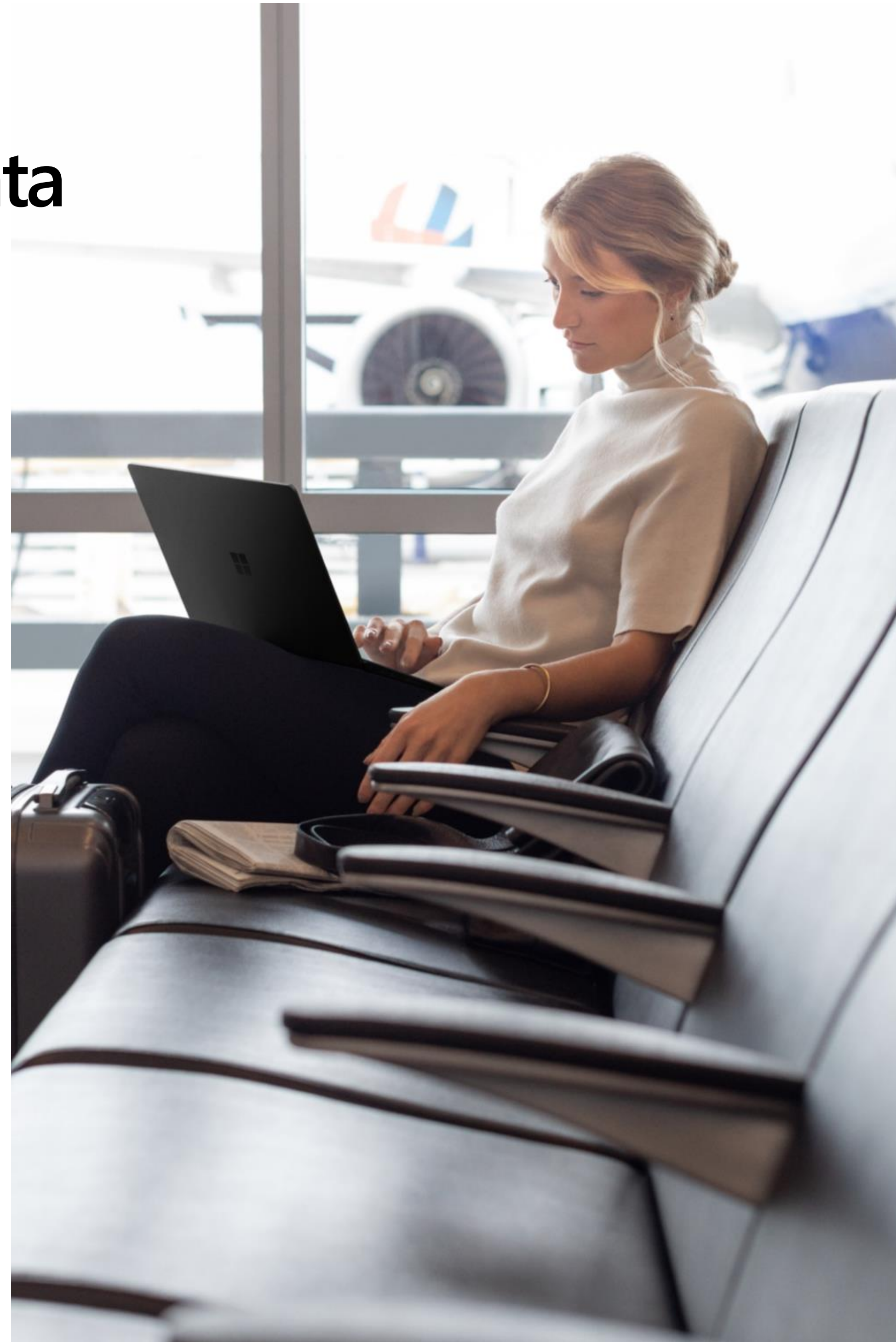
Windows PCs

Comprehensive device management solution

Includes the full capabilities of Microsoft Intune

Ensures devices and apps are compliant with your organization's security requirements

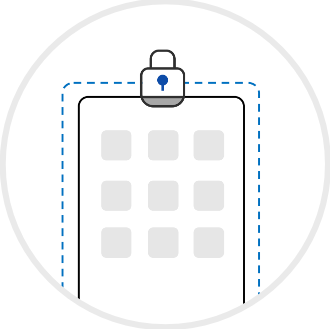
Includes policies that help keep your organization data safe



Protect your data on virtually any device with Intune

Mobile **Device** Management (MDM)

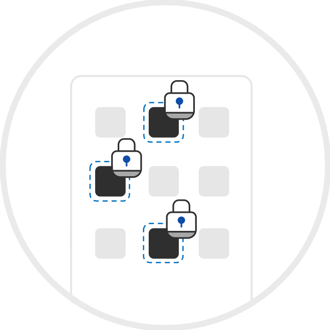
Conditional Access:
Restrict access to managed and compliant devices



- Enroll devices for management
- Provision settings, certs, profiles
- Report & measure device compliance
- Remove corporate data from devices

Mobile **Application** Management (MAM)

Conditional Access:
Restrict which apps can be used to access email or files



- Publish mobile apps to users
- Configure and update apps
- Report app inventory & usage
- Secure & remove corporate data within mobile apps

Require key security features on mobile devices

The problem:

Mobile devices provide productivity benefits, but they can be difficult to secure company data on.

The solution:

Easily enforce use of key security features with Intune Mobile Application Management:

- Deny access to jailbroken or rooted devices
- Prevent users from pasting data to unsecured apps

Remove company data when employee leaves company

The problem:

When an employee loses a device, or leaves the company, your data is still on their device.

Completely wiping the device will delete the employee's personal files such as photos and text messages

The solution:

Remotely delete company data from a device without impacting personal files personal information intact.

Device data/app options in Endpoint Manager (Intune)

Method	Usage	Intune Management	Azure AD Enrollment
Retire/Delete	Get rid of outdated devices	Removed	Removed
Wipe (Keep enrollment)	Reset device to default, remove Apps Keep user’s data/files	Keep, Re-apply policies	Keep
Wipe	Lost stolen device, device handover, Return to OOBE	Removed	Removed
Fresh Start (Keep enrollment)	Reset device to Signature Edition, Remove Apps, Keep user’s data/files update to latest Windows version	Keep	Keep
Fresh Start	Reset device to latest Windows Signature Edition	Removed	Keep
Autopilot Reset	Reuse a device and remove previous user’s profile/data.	Keep	Keep

Microsoft

SYNNEX CORPORATION

Manage Windows devices

The problem:

There are several security actions that can be enabled for Windows devices, but it is cumbersome to enable these capabilities on a per-computer basis.

The solution:

Microsoft 365 Business Premium offers centralized management of Windows 10 devices so you can easily manage a consistent set of security options.

Too many apps available; many not secure

The problem:

There are over 1.5 million apps available on Apple's app store and over 600k on Google Play, with more are added every day. You will want to ensure that only a select group of secure apps access company data.

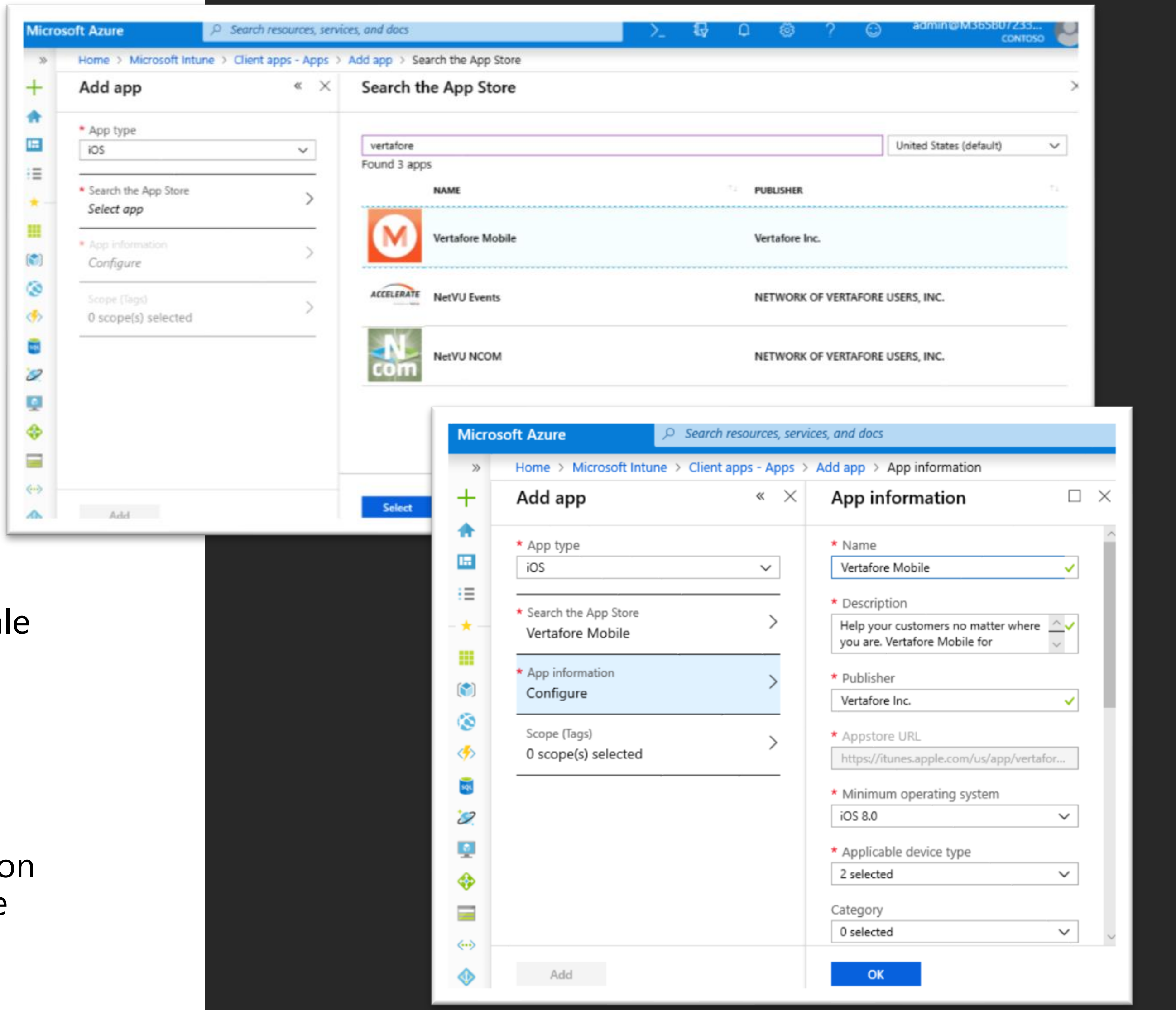
The solution:

Control which apps can be installed on company-issued mobile devices.

Take-home demo instructions

Control which apps can be installed

1. Sign in to the [Azure portal]
2. Select **All services** > **Intune**
   Intune is located in the **Monitoring + Management** section
3. In the **Intune** pane, select **Client apps**
4. In the **Client apps** workload pane, under **Manage**, select **Apps**
5. In the **Apps** pane, select **Add**
6. In the **App type** list, under the **Store app** types, select **iOS**
7. Select **Search the App Store**
8. In the **Search the App Store** pane, select the App Store country locale
9. In the **Search** box, type the name (or part of the name) of the app
   Intune searches the store and returns a list of relevant results
10. In the results list, select the app you want, and then select **Select**
11. In the **Add app** pane, select **App information** to configure the app
12. In the **App information** pane, add the app information. Depending on the app you have chosen, some of the values in this pane might have been automatically filled in
13. Select **OK**
14. Select **Add**



Microsoft Azure
Search resources, services, and docs
admin@M365B07233...
CONTOSO
Home > Microsoft Intune > Client apps - Apps > Add app > Search the App Store
Add app
Search the App Store
Add
Select
Microsoft Azure
Search resources, services, and docs
Home > Microsoft Intune > Client apps - Apps > Add app > App information
Add app
App information
Add
OK

Add app

* App type: iOS

* Search the App Store: Select app

* App information: Configure

Scope (Tags): 0 scope(s) selected

Search the App Store

vertafore — United States (default)

Found 3 apps

NAME	PUBLISHER
Vertafore Mobile	Vertafore Inc.
NetVU Events	NETWORK OF VERTAFORE USERS, INC.
NetVU NCOM	NETWORK OF VERTAFORE USERS, INC.

Add app

* App type: iOS

* Search the App Store: Vertafore Mobile

* App information: Configure

Scope (Tags): 0 scope(s) selected

App information

* Name: Vertafore Mobile

* Description: Help your customers no matter where you are. Vertafore Mobile for

* Publisher: Vertafore Inc.

* Appstore URL: https://itunes.apple.com/us/app/vertafor...

* Minimum operating system: iOS 8.0

* Applicable device type: 2 selected

Category: 0 selected

Recap

The growing use of various types of devices presents opportunities and challenges

With Microsoft 365 Business Premium, you get a comprehensive solution for managing phones, tablets, and laptops:

- Protect company data on personal devices through mobile application management
- Fully control company owned mobile devices through mobile device management
- Enforce policies for Windows 10 PCs to keep them secure and up-to-date

Demo

Endpoint Manager (Intune)

Microsoft

End of – **Building a Security Practice Workshop 2: Managing & Securing Devices with Intune – Windows, iOS, MacOS & Android**

For more information, contact **msftcsp@synnex.com**

SYNNEX CORPORATION