

© Copyright Microsoft Corporation. All rights reserved.

FOR USE ONLY AS PART OF MICROSOFT VIRTUAL TRAINING DAYS PROGRAM. THESE MATERIALS ARE NOT AUTHORIZED FOR DISTRIBUTION, REPRODUCTION OR OTHER USE BY NON-MICROSOFT PARTIES.



Microsoft 365 Virtual Training Day: Managing Windows and Surface Devices



Device Enrollment

Module Agenda



Managing Device Authentication



Device Enrollment using Microsoft Endpoint Configuration Manager

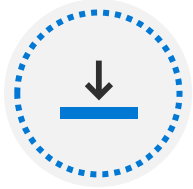


Device Enrollment using Microsoft Intune

Lesson 1: Managing Device Authentication



Lesson Introduction



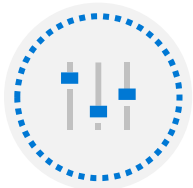
Azure AD join



Azure AD join prerequisites, limitations and benefits



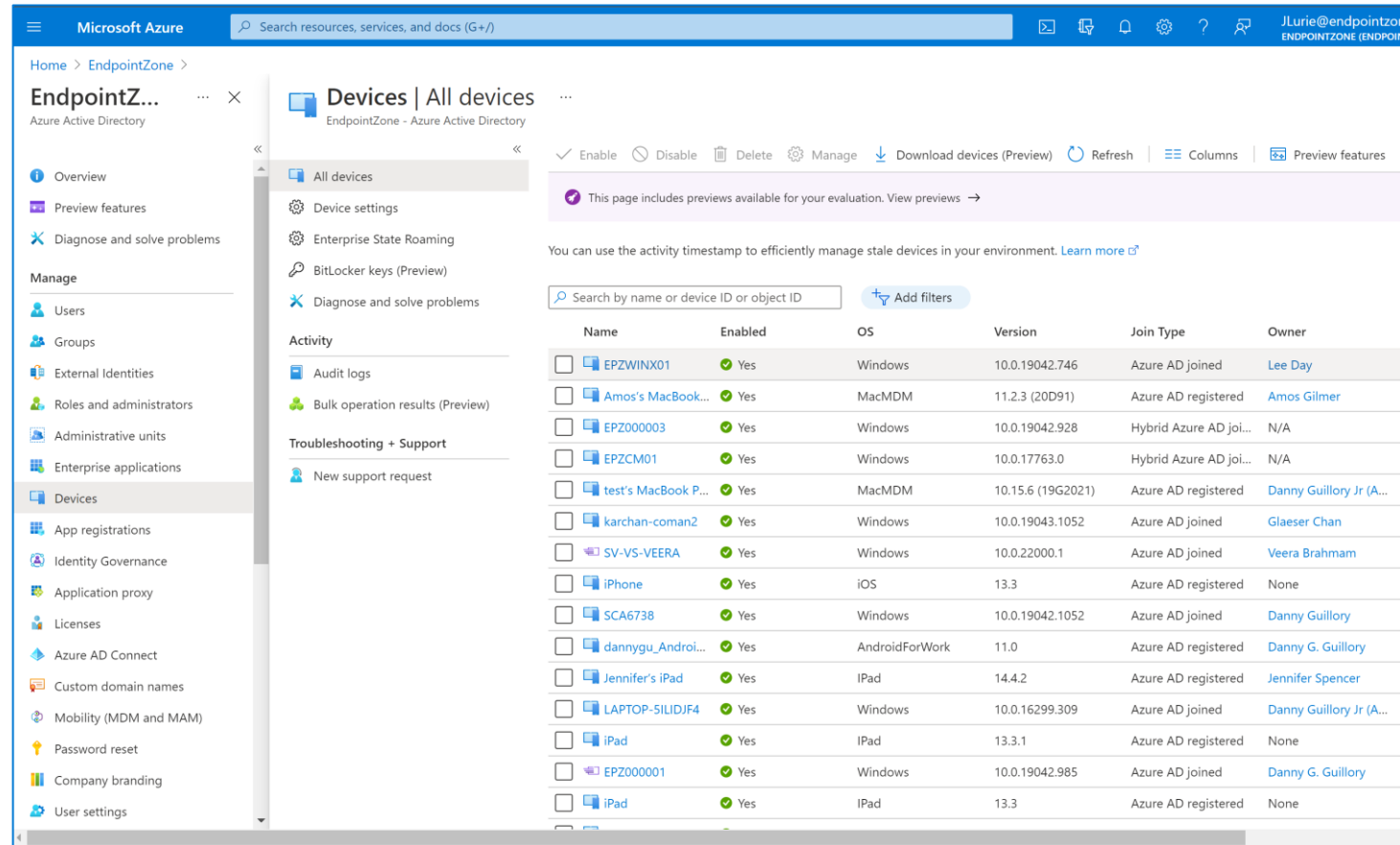
Joining devices to Azure AD



Managing devices joined to Azure AD

Azure AD Join Overview

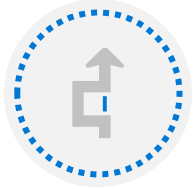
- Windows 10 can join Azure AD
- Typical scenarios:
 - Applications and resources are mostly in the cloud
 - Separate temporary accounts
 - Enable users to join their device to the corporate environment
- Join devices during initial setup or later
- Hybrid Azure AD join automatically registers your on-premises domain-joined devices with Azure AD



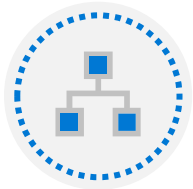
The screenshot shows the Microsoft Azure portal interface for managing devices. The left sidebar contains navigation options like Overview, Preview features, Diagnose and solve problems, Manage (Users, Groups, External Identities, Roles and administrators, Administrative units, Enterprise applications), Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, and User settings. The main content area is titled 'Devices | All devices' and includes a search bar, a table of devices, and various management actions like Enable, Disable, Delete, and Manage. A table of devices is displayed below, with columns for Name, Enabled, OS, Version, Join Type, and Owner.

| Name | Enabled | OS | Version | Join Type | Owner |
|---------------------|---------|----------------|-------------------|------------------------|-------------------------|
| EPZWIX01 | Yes | Windows | 10.0.19042.746 | Azure AD joined | Lee Day |
| Amos's MacBook... | Yes | MacMDM | 11.2.3 (20D91) | Azure AD registered | Amos Gilmer |
| EPZ000003 | Yes | Windows | 10.0.19042.928 | Hybrid Azure AD joi... | N/A |
| EPZCM01 | Yes | Windows | 10.0.17763.0 | Hybrid Azure AD joi... | N/A |
| test's MacBook P... | Yes | MacMDM | 10.15.6 (19G2021) | Azure AD registered | Danny Guillory Jr (A... |
| karchan-coman2 | Yes | Windows | 10.0.19043.1052 | Azure AD joined | Glaeser Chan |
| SV-VS-VEERA | Yes | Windows | 10.0.22000.1 | Azure AD joined | Veera Brahmam |
| iPhone | Yes | iOS | 13.3 | Azure AD registered | None |
| SCA6738 | Yes | Windows | 10.0.19042.1052 | Azure AD joined | Danny Guillory |
| dannygu_Androi... | Yes | AndroidForWork | 11.0 | Azure AD registered | Danny G. Guillory |
| Jennifer's iPad | Yes | iPad | 14.4.2 | Azure AD registered | Jennifer Spencer |
| LAPTOP-SILIDJF4 | Yes | Windows | 10.0.16299.309 | Azure AD joined | Danny Guillory Jr (A... |
| iPad | Yes | iPad | 13.3.1 | Azure AD registered | None |
| EPZ000001 | Yes | Windows | 10.0.19042.985 | Azure AD joined | Danny G. Guillory |
| iPad | Yes | iPad | 13.3 | Azure AD registered | None |

Azure AD Join Prerequisites, Differences, and Benefits



Multitenancy is very difficult to implement with AD DS



Azure AD is not a part of the core infrastructure



Azure AD has different management capabilities than AD DS

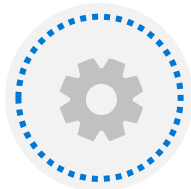


Azure AD is multitenant by design

Joining Devices to Azure AD



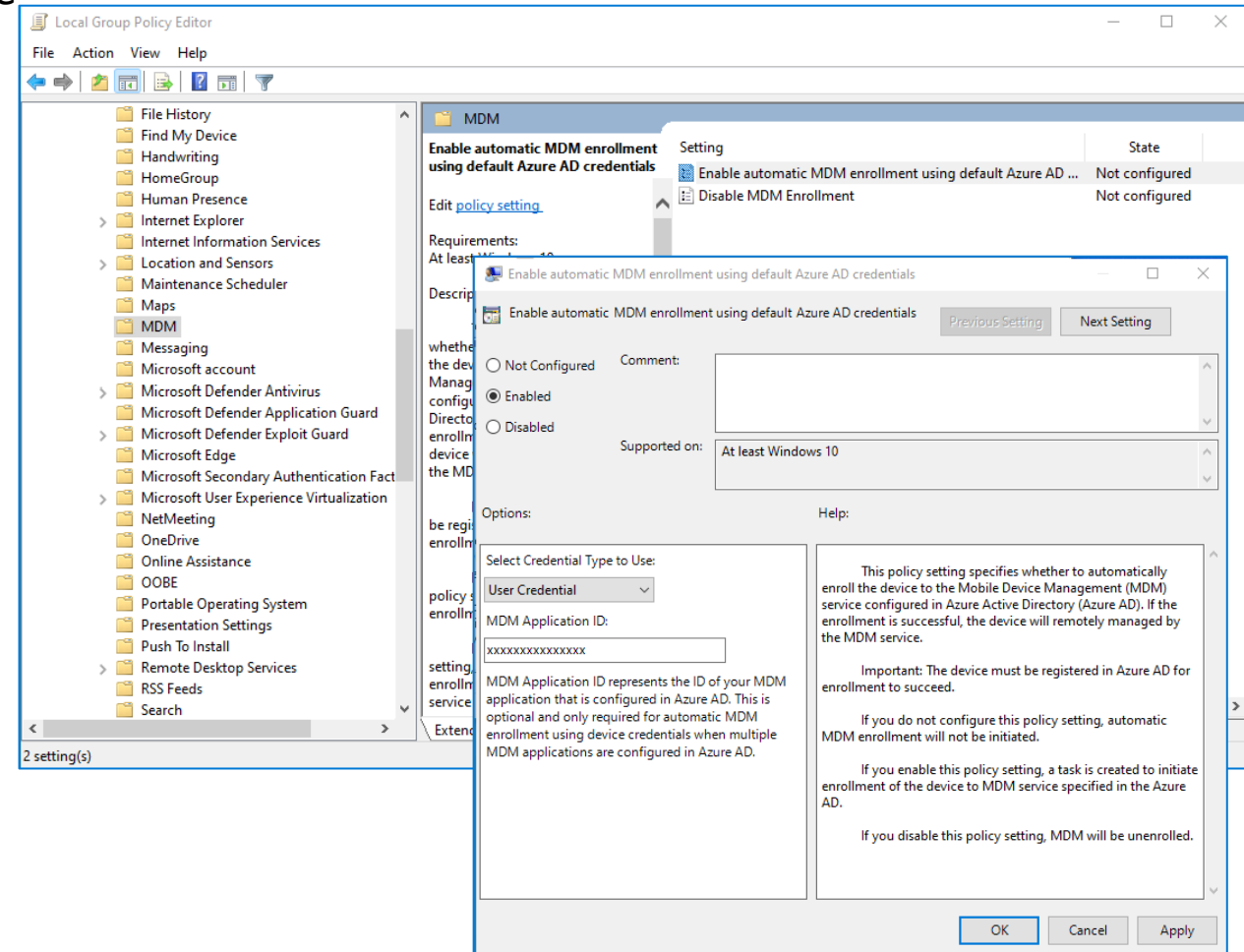
Joining a device to Azure AD is a simple procedure



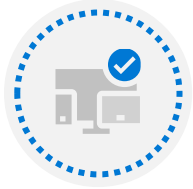
You can join to Azure AD during Windows 10 installation, or you can do it later, at any time by using Settings pane, a script, or a number of management tools



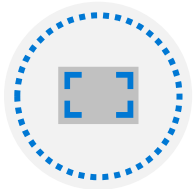
You need Azure AD credentials to join device to Azure AD



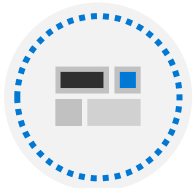
Managing Devices Joined to Azure AD



Group Policy manages devices that join on-premises AD DS



Group Policy is not always available or supported for devices that join Azure AD



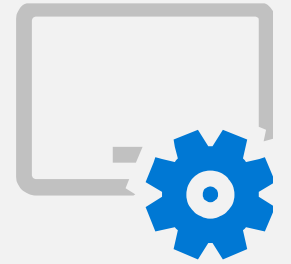
Azure AD supports integration with mobile device management (MDM) services such as Intune



When integration between Intune and Azure AD is configured, a device that joins Azure AD automatically enrolls with Intune (additional licensing may be required)

DEMO: Enroll a Windows 10 device automatically

Lesson 2: Device Enrollment using Microsoft Endpoint Configuration Manager



Lesson Introduction



Introduction to Microsoft Endpoint Manager



Deploying the Microsoft Endpoint Configuration Manager Client



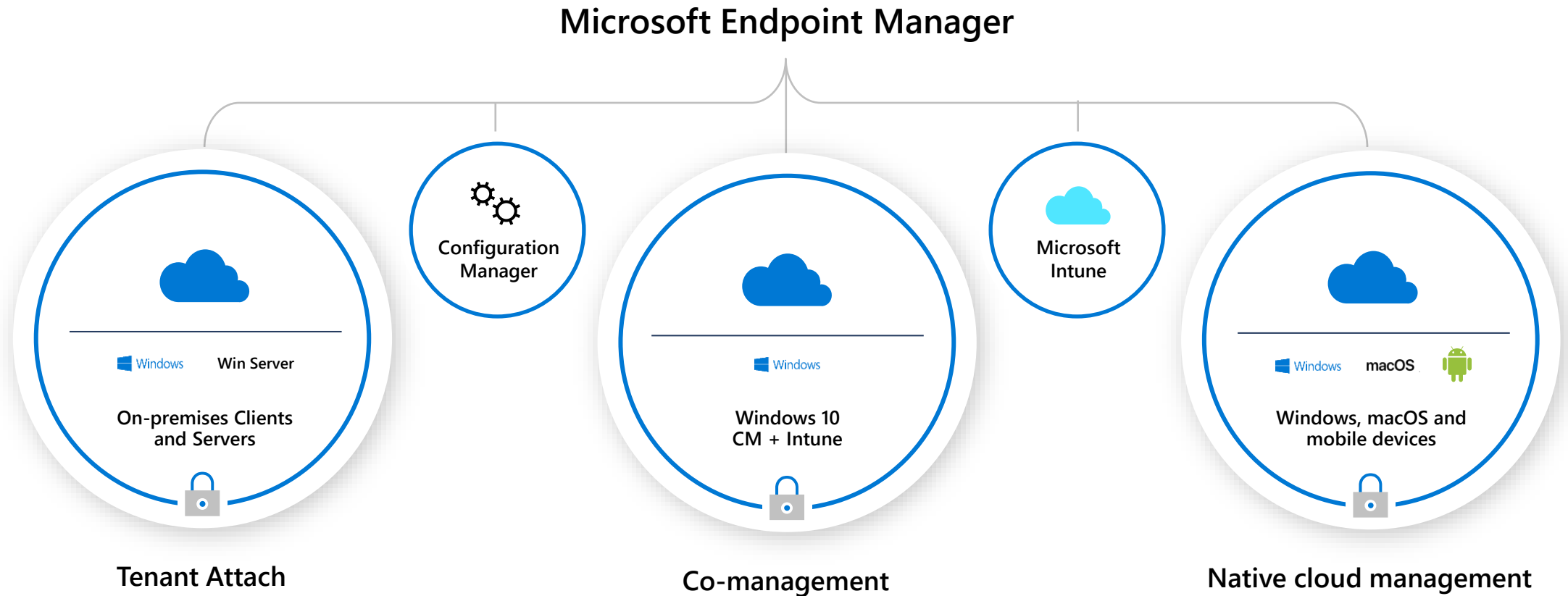
Monitoring the Microsoft Endpoint Configuration Manager Client



Managing the Microsoft Endpoint Configuration Manager Client

Microsoft Endpoint Manager

Manage on-prem endpoints in the cloud at your own pace



Why Deploy the Configuration Manager Client?

Benefits for IT administrators

Track software present on the device

Access inventory information in relation to hardware

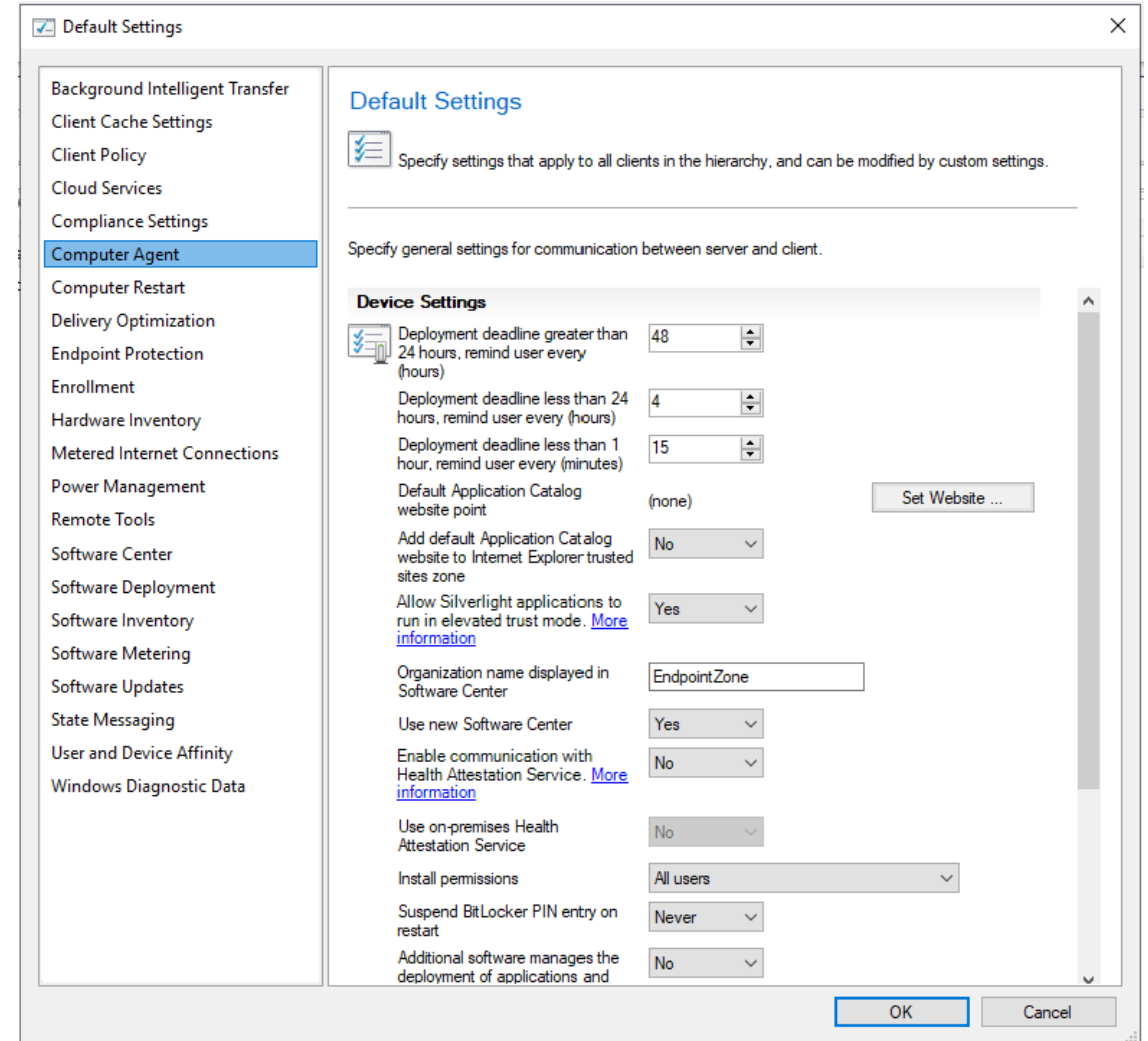
Update the device with Quality and Feature updates

Manage and deploy the OS and LoB applications

Benefits for end users

Browse a feature rich self-service catalogue of software that empowers the user to choose software to install

Configure working hours to ensure interruptions are minimized



Client Deployment Options



Client push

Deploys the Configuration Manager client directly from the Configuration Manager console

Device discovery (Active Directory LDAP integration)

Copies the files to the source computer and initiates the install automatically

Initial copy process may increase network traffic



Manual deployment

Deploys the Configuration Manager client installation source files and a script file containing the install parameters

Executes from the ccmsetup.exe file or from the MSI that is part of the client files

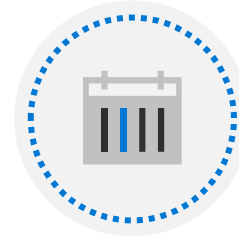
Can be time consuming as a delivery mechanism



OS deployment

When installing and setting up Windows 10 using a task sequence, slip-stream the Configuration Manager client into the Windows setup and provide it with the necessary installation parameters

Must be installed when a device is built for the first time (or rebuilt)



Microsoft Intune

Intune drives Configuration Manager client installation and registers the device with the Cloud Management Gateway

Manage each respective workload from either Intune or Configuration Manager after installation

Monitoring the Microsoft Endpoint Configuration Manager Client



Client online status. Online (connected to its assigned management point) or offline.



Client activity. Active (it has communicated with Configuration Manager in the past seven days) or inactive.



Primary User. The primary user of this device, calculated over a 60-day period of the most frequent logins.



Operating System Build. See the OS version of a device without having to connect to or perform any remote management.



Client check. State of the periodic evaluation that the Configuration Manager client runs on the device. The evaluation checks the device and can remediate some of the problems it finds.

Managing with Microsoft Endpoint Configuration Manager

When the Configuration Manager client installs

- Assigns device to a site
- Adds device to query-based Collections
- Scans device for inventory and uploads inventory data
- Scans for compliance, pushes required software, etc.

Collections

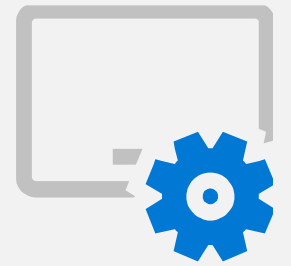
- Represent devices or users that have some commonality
- Perform tasks, such as target a deployment or run a report

Other management options

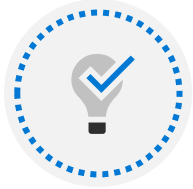
- Start Resource Explorer
- Start Policy Retrieval
- Add to a collection
- Client Settings RSOP

DEMO: Enroll a Windows 10 device using Configuration Manager

Lesson 3: Device Enrollment using Microsoft Intune



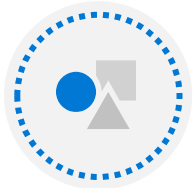
Lesson Introduction



Activating and deploying MDM services

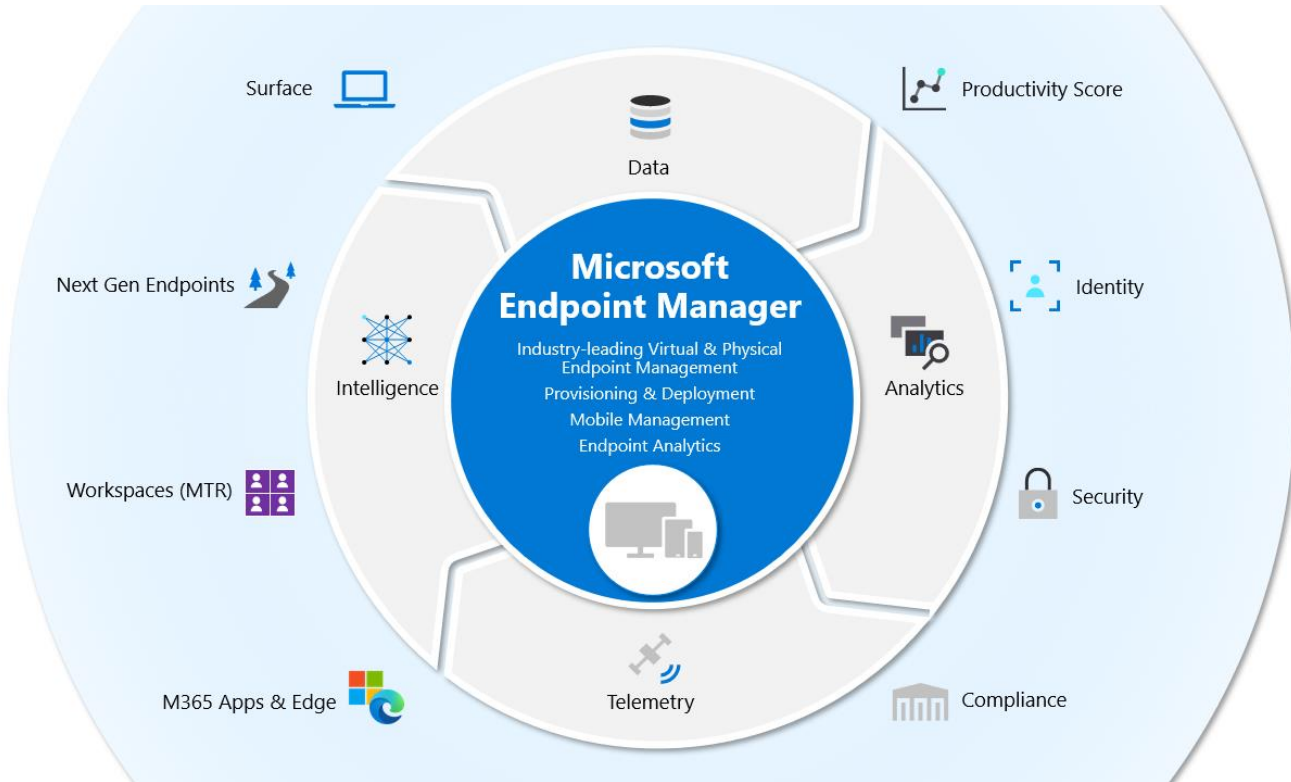







Managing Corporate Enrollment Policy



Enrolling Windows to Intune

Managing devices with Microsoft Intune



-  Enroll/Unenroll devices
-  Remote tasks
-  Application Management
-  Inventory and Analytics
-  Device security and management

One consistent set of MDM capabilities across Mobile, Desktop, and IoT

Enabling Mobile Device Management

Enable Intune as the MDM Authority

Get an Apple MDM push certificate

Sign up for Apple Business if you intend to use Apple's Device Enrollment Program

Choose MDM Authority

Mobile Device Management Authority

Choose whether Intune or Configuration Manager is your mobile device management authority.

Choose Intune as your MDM authority to manage mobile devices with Microsoft Intune only.

Choose Configuration Manager as your MDM authority to manage mobile devices with System Center Configuration Manager and Microsoft Intune.

Mobile devices cannot be managed if an MDM authority is not chosen.

Learn more about [choosing your MDM Authority](#).

Intune MDM Authority

Configuration Manager MDM Authority

None

Considerations for Device Enrollment

- Determine enrollment method
 - Group Policy
 - Joining Azure AD
 - Manually (Settings, Provision Package, Company Portal App)
- Determine devices allowed and restrictions
- Determine if enrollment is optional or mandatory

The screenshot shows the 'Create restriction' page in the Microsoft Endpoint Manager admin center. The page is titled 'Create restriction' and is part of the 'Enroll devices' workflow. It has a breadcrumb trail: Home > Devices > Enroll devices > Create restriction. The page is divided into several tabs: Basics, Platform settings (selected), Scope tags, Assignments, and Review + create. Below the tabs, there is a section for 'Device type restriction' with a description: 'Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. Learn more.' Below this is a table with columns: Type, Platform, versions, Personally owned, and Device manufacturer. The table lists five device types: Android Enterprise (work profile), Android device administrator, iOS/iPadOS, macOS, and Windows (MDM). Each row has 'Allow' and 'Block' buttons for the Platform and Personally owned columns, and a text input field for the Device manufacturer column. The 'Block' buttons are highlighted in purple. The 'Restriction not supported' text is shown in the Device manufacturer column for iOS/iPadOS, macOS, and Windows (MDM).

| Type | Platform | versions | Personally owned | Device manufacturer |
|-----------------------------------|-------------|---------------------------------|------------------|---------------------------|
| Android Enterprise (work profile) | Allow Block | Allow min/max range: Min Max | Allow Block | Manufacturer name here |
| Android device administrator | Allow Block | Allow min/max range: Min Max | Allow Block | Manufacturer name here |
| iOS/iPadOS | Allow Block | Allow min/max range: Min Max | Allow Block | Restriction not supported |
| macOS | Allow Block | Restriction not supported | Allow Block | Restriction not supported |
| Windows (MDM) | Allow Block | Allow min/max range: Min Max | Allow Block | Restriction not supported |

Managing Corporate Enrollment Policy

- Your initial Azure AD domain will follow the model:
 - your-domain.onmicrosoft.com
- Add one or more of your custom domain names, i.e. Contoso.com (recommended)
- Add custom domain names in the Microsoft 365 management portal
- Configure Automatic MDM enrollment (recommended) OR
- Create CNAME records to simplify enrollment and device registration when not licensed for Azure AD Premium

The screenshot displays the Microsoft Endpoint Manager admin center interface. The left-hand navigation pane includes sections for Home, Dashboard, All services, FAVORITES, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Tenant admin | Customization' and features a search bar and a list of configuration options. The 'Configuration' section includes settings for device enrollment, privacy statements, and push notifications. The 'Microsoft Managed Desktop' section includes settings for tenant enrollment. The 'Help and support' section includes a link to help and support. The 'Scope tags' section includes a 'Default' tag. The 'Policies' section includes a note about creating and assigning customization policies. The URL bar at the bottom shows 'https://endpoint.microsoft.com/#'.

| Configuration | Value |
|---|--------------------------|
| Device enrollment | Available, with prompts |
| Privacy statement URL | http://www.microsoft.com |
| Privacy message about what support can't see or do (iOS/iPadOS) | Default |
| Privacy message about what support can see or do (iOS/iPadOS) | Default |
| Send a push notification to users when their device ownership type changes from personal to corporate (Android and iOS/iPadOS only) | No |
| Azure AD Enterprise Applications | Show |
| Office Online Applications | Show |
| Hide remove button on corporate Windows devices | Yes |
| Hide reset button on corporate Windows devices | No |
| Hide remove button on corporate iOS/iPadOS devices | No |
| Hide reset button on corporate iOS/iPadOS devices | No |

Enrolling Windows Devices in Intune

Many ways to enroll Windows 10 devices in Microsoft Intune:

- Add work or school account
- Modern app sign-in (user driven)
- Enroll in MDM only (user driven)
- Azure AD join (Out of Box Experience (OOBE))
- Azure AD join (autopilot – User-driven deployment mode)
- Enroll in MDM only (Device Enrollment Manager)
- Azure AD device registration + automatic enrollment Group Policy Object
- Configuration Manager co-management
- Azure AD join (bulk enrollment using provisioning package)

DEMO: Enrolling devices in Intune

Resources

[Security, Compliance and Identity Blog](#)

[Azure Active Directory documentation](#)

[Join the Microsoft Endpoint Manager Community](#)

[Microsoft Endpoint Manager Blog](#)

[Microsoft Endpoint Manager documentation](#)

[Microsoft Intune documentation](#)

[Configuration Manager Blog](#)

[Microsoft Endpoint Configuration Manager Documentation](#)

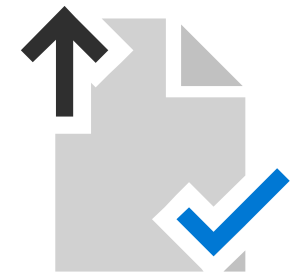
[Microsoft Endpoint Manager Learning Path](#)

[Configuration Manager Learning Paths](#)



Application Management

Lesson 1: Deploying and Updating Applications



Lesson Introduction



Adding applications to Intune



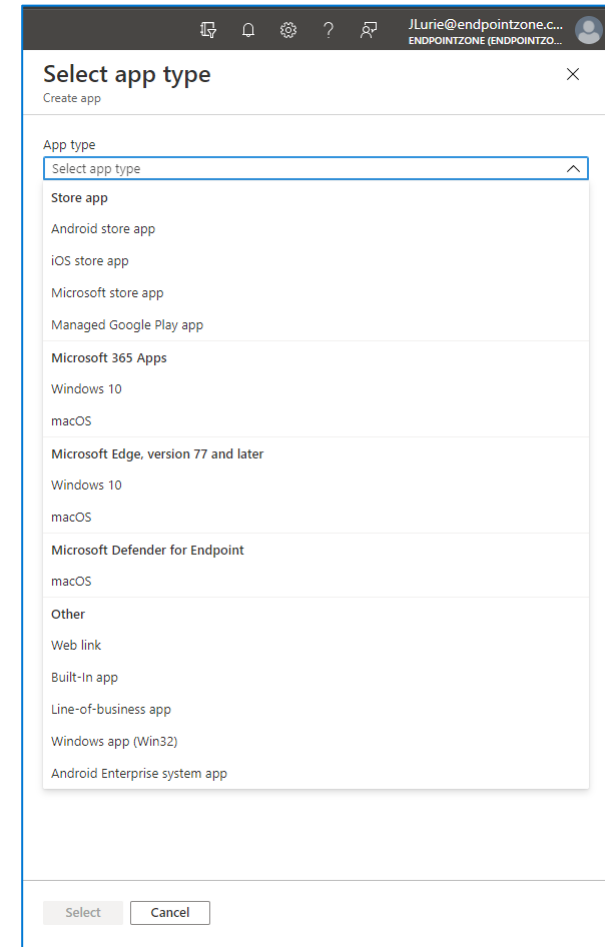
Deploying Applications with Configuration Manager

Adding Apps to Intune

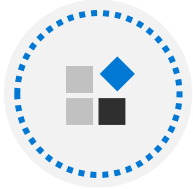
Apps must be added to Intune before you can deploy or manage them.

Apps Supported:

- Apps from the various stores (Apple and Google)
- Apps for Windows 10 from Windows Store or an app catalog
- Microsoft 365 Apps
- Web Links
- Built-in Apps (i.e. OneDrive and Edge)
- LOB Apps
- Win32 Apps



Managing Win32 apps with Intune



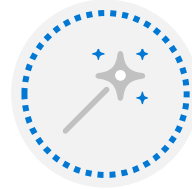
Devices must be joined to Azure AD



Max size 8GB per app



32/64-bit supported



Win32 Content Prep Tool used to create .intunewin file



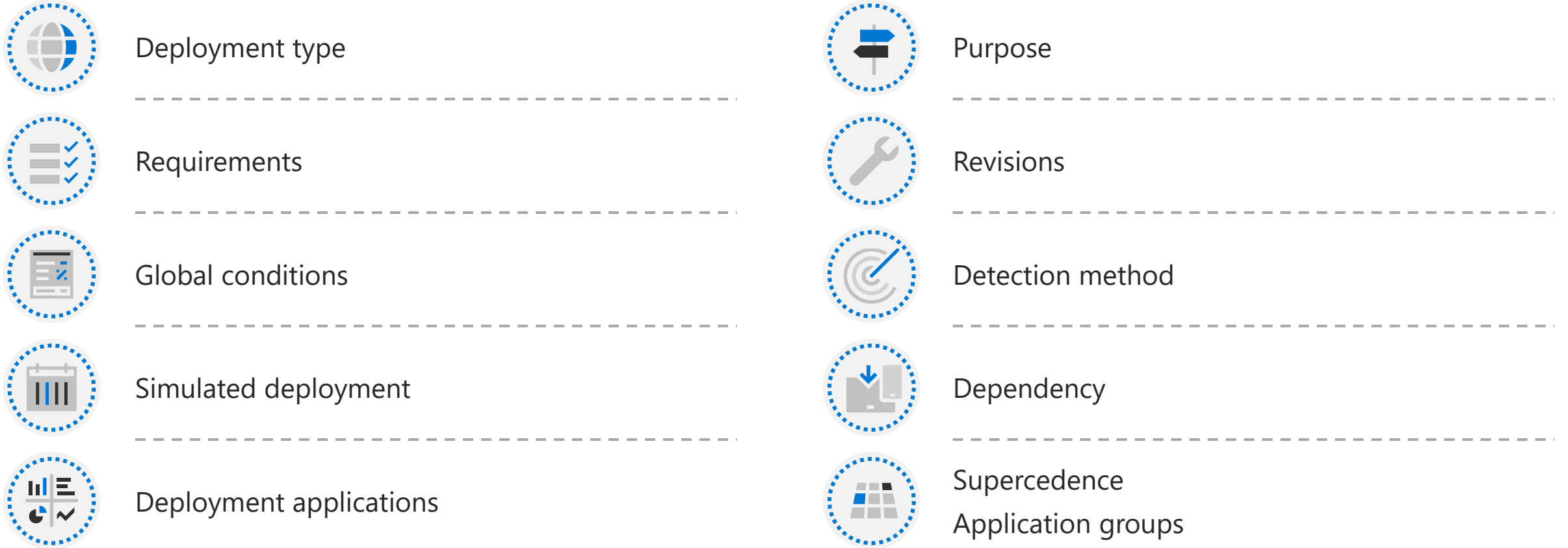
Add App to Intune

- App info and requirements
- Install/uninstall commands
- Rules for existing config and apps
- App return codes

DEMO: Deploying Windows applications with Intune

Deploying Applications with Configuration Manager

Elements of the application model



Creating an Application in Configuration Manager

To create an application:

1. In the Configuration Manager console, choose **Software Library** > **Application Management** > **Applications**. Select **Users and groups**, and then select **All users**.
2. On the **Home** tab, in the **Create** group, choose **Create Application**.
3. On the **General** page of the **Create Application Wizard**, choose **Automatically detect information about this application from installation files**.
 1. **Type**: Choose **Windows Installer (*.msi file)**.
 2. **Location**: Type the location (or choose Browse to select the location) of the installation file Contoso.msi.
4. On the **General Information** page, you can supply further information about the application.
5. In the **Installation program** field, specify the full command line that will be used to install the application on PCs.
6. Choose **Next**. On the **Summary** page, confirm your application settings and then complete the wizard.

Specify information about this application

| | |
|----------------------------|---|
| Name: | <input type="text" value="Contoso Application"/> |
| Administrator comments: | <input type="text"/> |
| Publisher: | <input type="text" value="Contoso"/> |
| Software version: | <input type="text" value="1"/> |
| Optional reference: | <input type="text"/> |
| Administrative categories: | <input type="text"/> <input type="button" value="Select..."/> |

Specify the installation program for this application and the required installation rights.

| | |
|--|---|
| Installation program: | <input contoso.msi"="" q"="" type="text" value="msiexec /i "/> <input type="button" value="Browse..."/> |
| <input type="checkbox"/> Run installation program as 32-bit process on 64-bit clients. | |
| Install behavior: | <input type="text" value="Install for system if resource is device; otherwise install for user"/> |

Choosing an Endpoint Manager Solution for Deploying an Application

| Application Type | Configuration Manager | Microsoft Intune |
|--------------------------|-----------------------|------------------|
| .MSI | Yes | Yes |
| .IntuneWin | No | Yes |
| Office C2R | Yes | Yes |
| APPX/MSIX | Yes | Yes |
| Store Apps | Yes | Yes |
| M365 Apps for Enterprise | No | Yes |
| Appv | Yes | No |

DEMO: Deploy a Windows 10 app using Configuration Manager

Resources

[Microsoft Intune documentation](#)

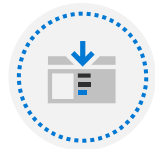


Deployment Using Microsoft Endpoint Manager (Segment 1 of 2)

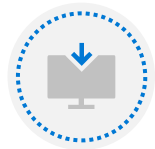
Module Agenda



Assessing Deployment Readiness



On-Premises Deployment Tools and Strategies



Deploying New Devices Using Autopilot

Lesson 1: Assessing Deployment Readiness



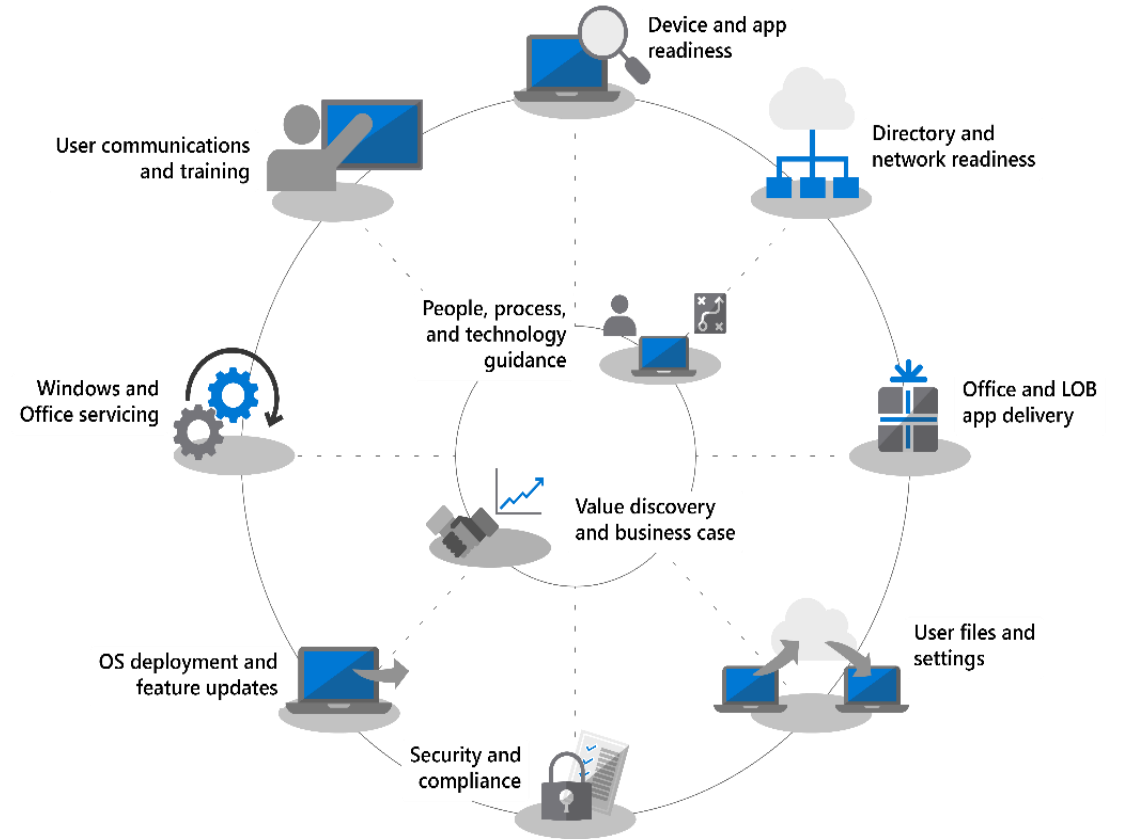
Lesson Introduction



Guidelines for an effective enterprise desktop deployment

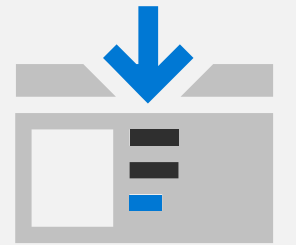
Deployment Guidelines

- Take inventory and establish infrastructure map
- Identify devices to retire
- Strategy for supporting complex application installs
- Determine opportunities for virtualization
- Establish data migration process
- Establish method for backing up data on devices where applicable
- Establish a deployment plan describing the complete process
- Create a training and post-deployment plan



**DEMO: Review the Windows and Office
Deployment Lab Kit (aka.ms/DeploymentLabKit)**

Lesson 2: On-Premises Deployment Tools and Strategies



Lesson Introduction



Traditional Deployment



Deploying Windows 10 using Configuration Manager



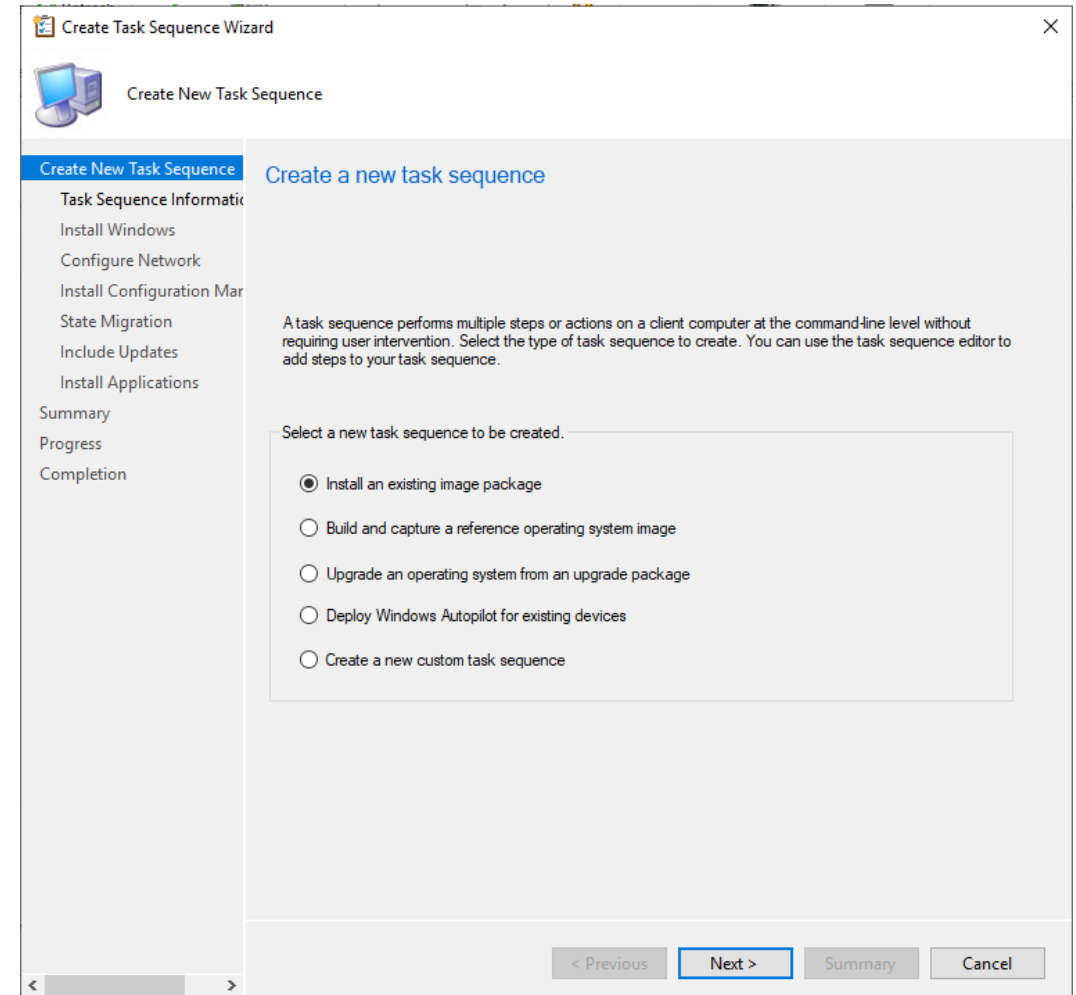
Planning In-Place Upgrades

Traditional Deployment

| Default Image | Custom Image |
|---|--|
| <ul style="list-style-type: none">• No need to create an image | <ul style="list-style-type: none">• Image must be created and maintained |
| <ul style="list-style-type: none">• Applications and settings must be applied separately | <ul style="list-style-type: none">• Applications and Settings can be included in custom image |
| <ul style="list-style-type: none">• One image per architecture (x86/x64) can be used for the organization | <ul style="list-style-type: none">• The configuration and application requirements (and sometimes hardware) of each group within an organization can typically require several images to be created and maintained |
| <ul style="list-style-type: none">• Updates to applications do not require the image to be re-built | <ul style="list-style-type: none">• Updates to applications cause images to become stale, requiring images to be updated or re-created frequently |
| <ul style="list-style-type: none">• Overall deployment time is typically slower, as configurations must be applied, and applications installed after the OS image is deployed | <ul style="list-style-type: none">• Overall deployment time is typically faster with the configurations and applications included in the image |
| <ul style="list-style-type: none">• Some applications can be difficult to automate the installation | <ul style="list-style-type: none">• When applications are installed on the reference machine, they are typically easier to deploy when included with the image |

Deploying Windows 10 using Configuration Manager: Introduction

- **Role of Configuration Manager in a modern desktop journey**
 - With modern management tools, such as Intune and Autopilot, and the innovative changes to Configuration Manager, it can now act as a bridge between how things were done, and how things can be done in a more modern and agile way
- **Building on the foundations of MDT**
 - Access to a wider expanse of task sequence variables with which to utilize during OS deployment
 - MDT Rules engine offers a raft of in-built options to aid OS deployment
 - The ability to install Windows features without the knowledge of code
 - Log file collection out of a template task sequence wizard



DEMO: Examine the Configuration Manager admin console

Deploying Windows 10 using Configuration Manager: Introduction

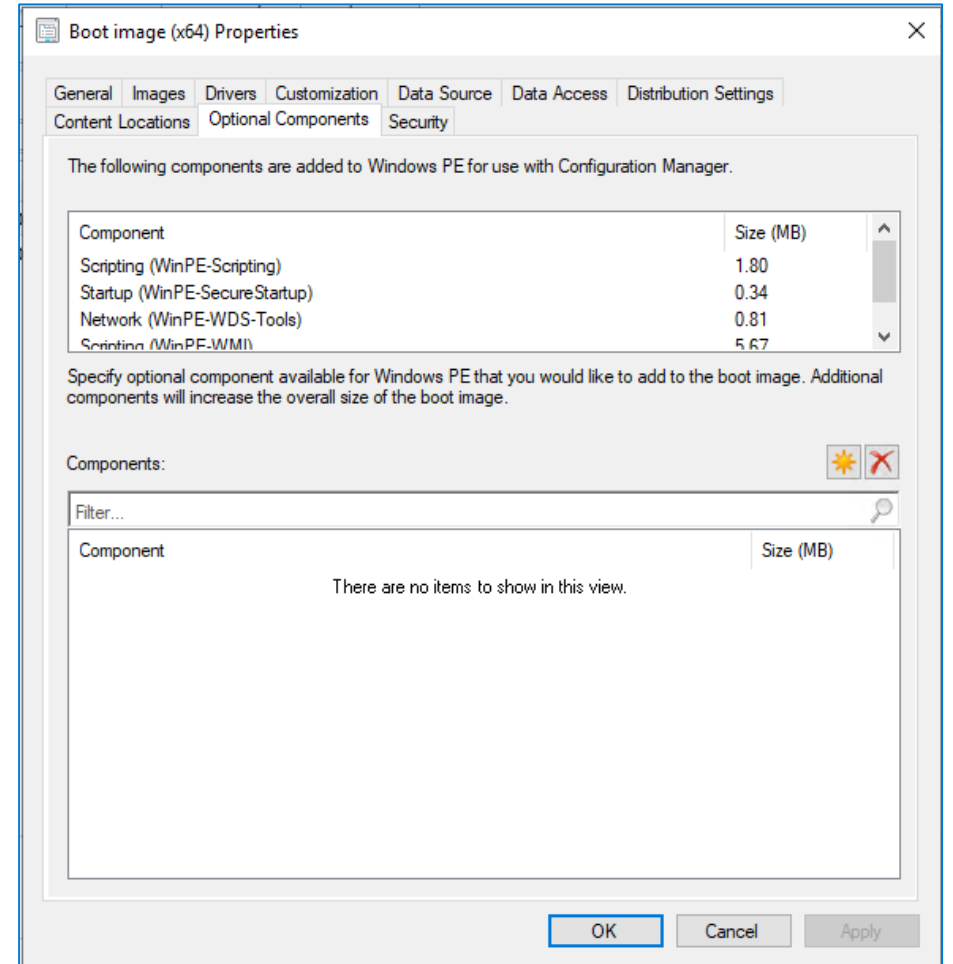
Exploring Configuration Manager

- OS Deployment
- Application Management
- Update Management
- Servicing Management
- Device Inventory (CMDB)
- Basic License Tracking
- Self Service Software Catalogue
- Cloud Management capability
- Real Time query and reporting
- Enterprise Scalability
- Azure AD Integration
- Proactive cadence adoption through Desktop Analytics
- Remote Control
- User Settings Capture and Restore

Deploying Windows 10 using Configuration Manager: Introduction

Exploring the Deployment Components Configuration Manager

- **Boot images**
 - The Windows Preinstallation Environment (Windows PE) images that are used to start a Windows 10 deployment
 - Start boot images from a CD or DVD, an ISO file, a USB device, or over the network using a Pre-Boot Execution Environment (PXE) server
 - Two default boot images: One to support x86 platforms and the other to support x64 platforms
- **Considerations for customizing boot images**



Deploying Windows 10 using Configuration Manager: Introduction

Exploring the Deployment Components Configuration Manager

OS images

Stored in the Windows Imaging (WIM) file format

A compressed collection of reference files and folders that are required to successfully install and configure an operating system on a computer

You must select an operating system image for all operating system deployment scenarios

Operating system upgrade packages

The source setup files for an operating system

You can also use this package to deliver a vanilla image down onto a device

Import operating system upgrade packages to Configuration Manager from a DVD or mounted ISO file

Device drivers

You can install device drivers on destination computers without including them in the operating system image that is being deployed

Configuration Manager provides a driver catalog in the Software Library workspace, consisting of two nodes: Drivers and Driver Packages

Software updates

Provide a set of tools and resources that can help manage the task of tracking and applying software updates to client computers

Configuration Manager builds on the basic offerings of MDT and provides a management plane that can segregate updates by type or OS, and work with existing processes for release management

Task sequences

Configuration Manager uses task sequences to provide schedule-based deployments that can be fully automated and require no user interaction (zero-touch installation or ZTI)

Automate components in Configuration Manager (software update packages, the application model, and Cloud Management Gateway)

Deploying Windows 10 using Configuration Manager: Managing & Monitoring

Methods for Composing a Windows 10 Deployment using Configuration Manager

Task sequences

Like MDT task sequences, but can draw on other elements within it, such as applications created packages and scripts

Integrate the Configuration Manager task sequence engine with the MDT binaries for greater flexibility

Scenarios for using a task sequence

Deployment collections

After creating the task sequence, you can target it at a deployment collection to allow the successful delivery

Prevents unintended delivery of an OS.

Target **unknown computers** to present any new device acquired with an ability to launch a created task sequence

Deploying Windows 10 using Configuration Manager: Managing & Monitoring

Troubleshooting a Windows 10 Deployment using Configuration Manager

Reporting

With a reporting services point configured in Configuration Manager, you can access to a set of tools and resources that help you use the advanced reporting capabilities of SQL Server Reporting Services (SSRS) and Power BI Report Server

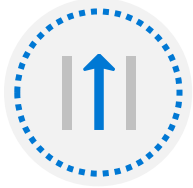
Log files

Configuration Manager produces numerous log files on both the client and server side to aid with troubleshooting

Examples:

- Ccmsetup.log
- SMSTS.log
- AppEnforce.log
- Execmgr.log

Planning In-Place Upgrades



Recommended path to Windows 10



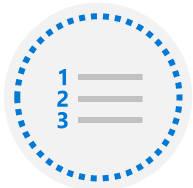
Preserves all data, settings, apps, and drivers



Can be rolled back at any point



Leverages Windows setup

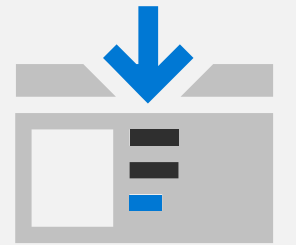


Use task sequences leveraging either MDT or Configuration Manager

Considerations for in-place upgrades

| Scenario | In-Place Upgrade | Fresh Installation |
|--|------------------|--------------------|
| Move from 32-bit operating system to 64-bit (e.g. Windows 7 32-bit to Windows 10 64-bit) | No | Yes |
| Move from one version of Windows to a lower target version (e.g. Windows 10, version 21H1 to version 1909) | No | Yes |
| Existing device meets minimum hardware specifications (including free disk space) | Yes | Yes |
| Existing apps are compatible with the target version | Yes | Yes |
| Existing OS language is the same as the target version | Yes | Yes |
| Intend to multi-boot/dual boot operating systems | No | Yes |
| Intend to use the standard install.wim | No | Yes |
| Requires creating and maintaining operating system images (or a clean ISO file which then needs to be updated with apps, drivers, and settings) | No | Yes |

Lesson 3: Modern Deployment Using Windows Autopilot



Lesson introduction



Modern Deployment using Autopilot



Requirements for Windows Autopilot



Preparing Device IDs for Autopilot



Device Registration and OOB Customization

Modern Deployment using Windows Autopilot

- No images, drivers, or infrastructure
- Customize the out-of-box-experience
- New devices typically have Windows 10 installed
- Device refresh

The screenshot displays the Microsoft Endpoint Manager admin center interface. The left-hand navigation pane includes options like Home, Dashboard, All services, FAVORITES, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Create profile' for a 'Windows PC' and is currently on the '2 Out-of-box experience (OOBE)' step. The page contains several configuration options with radio buttons and dropdown menus:

- Deployment mode: User-Driven
- Join to Azure AD as: Azure AD joined
- Microsoft Software License Terms: Hide
- Privacy settings: Hide
- Hide change account options: Hide
- User account type: Standard
- Allow White Glove OOBE: No
- Language (Region): Operating system default
- Automatically configure keyboard: Yes
- Apply device name template: No

At the bottom of the page, there are 'Previous' and 'Next' navigation buttons.

Modern Deployment using Windows Autopilot

Comparing Autopilot with Traditional Methods

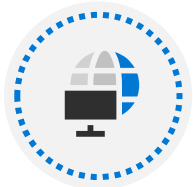
| | Traditional deployment | Modern deployment |
|--|---|--|
| Deploys Windows 10 images | Yes | No |
| Can be used with any preinstalled operating system | Yes | No |
| Requires a previous Windows 10 installation | No | Yes |
| Uses an on-premises infrastructure | Yes | No |
| Tools for preparing the deployment | Windows ADK, Windows Deployment Services, Microsoft Deployment Toolkit (MDT), and Configuration Manager | Windows Configuration Designer and Windows Autopilot |

Requirements for Windows Autopilot



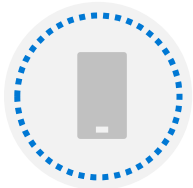
Devices must have Windows 10 preinstalled:

- Windows 10 Pro, Enterprise, or Education



Devices must have internet connectivity:

- Windows Autopilot is a cloud service



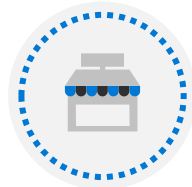
Intune or other mobile device management service (optional):

- For managing deployed Windows 10 devices



Devices must be registered to the organization:

- Device-specific information uploaded to the cloud



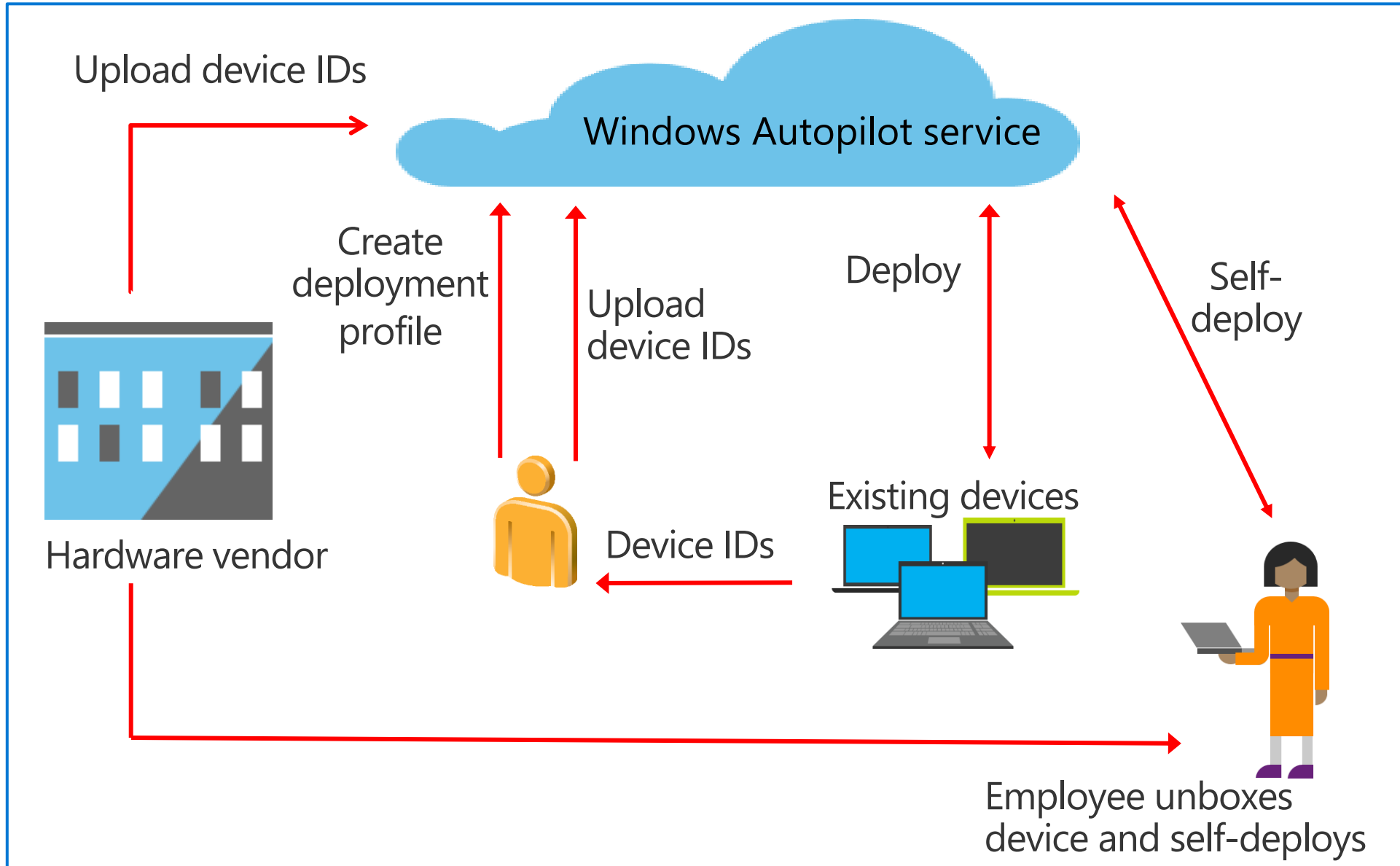
Organization must be using Azure AD:

- It must also use Microsoft Store for Business or Intune



Access to required URLs

Preparing Device IDs for Autopilot



Device Registration and OOB E Customization

Step 1 Create a Windows Autopilot deployment file

A required profile that specifies the settings to apply to the devices

You can create and use multiple deployment profiles with Windows Autopilot, but can only use a single profile to deploy each device

Step 2 Apply a deployment profile

Until you apply the deployment profile, Windows Autopilot doesn't manage the OOB E setup phase on the device

Windows Autopilot takes control of the OOB E setup phase on the devices to which you apply the profile

Module Three Resources

[Windows Autopilot Documentation](#)

[Join the Windows Community](#)

[Windows IT Pro Blog](#)

[Windows technical documentation](#)

[Windows Learning Paths](#)

Deployment Using Microsoft Endpoint Manager (Segment 2 of 2)

Module Agenda

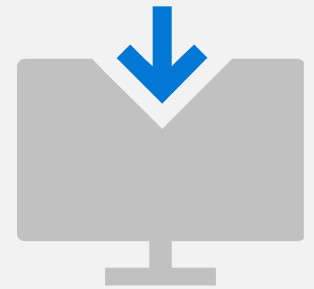


Deploying New Devices Using Autopilot



Dynamic Deployment Methods

Lesson 1: Deploying New Devices Using Autopilot



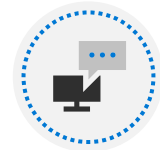
Lesson introduction



Demo Windows Autopilot



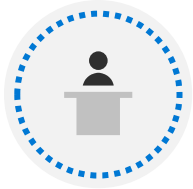
Autopilot Scenarios



Troubleshooting Windows 10 Autopilot

DEMO: Create and apply an Autopilot deployment profile

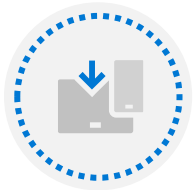
Autopilot Scenarios



Windows Autopilot user-driven mode



Windows Autopilot Self-Deploying mode



Autopilot for Existing Devices

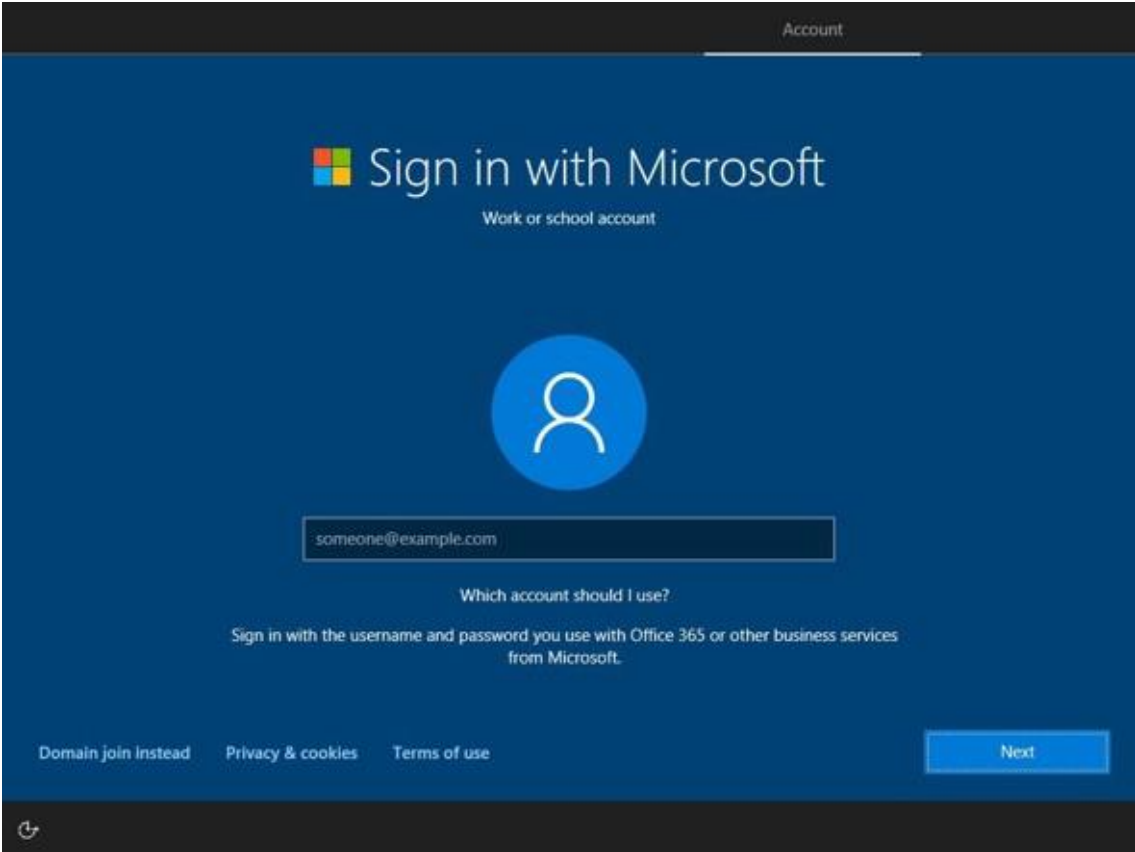


Windows Autopilot for pre-provisioned deployment



Windows Autopilot Reset

Comparing the default and Autopilot OOBExperience

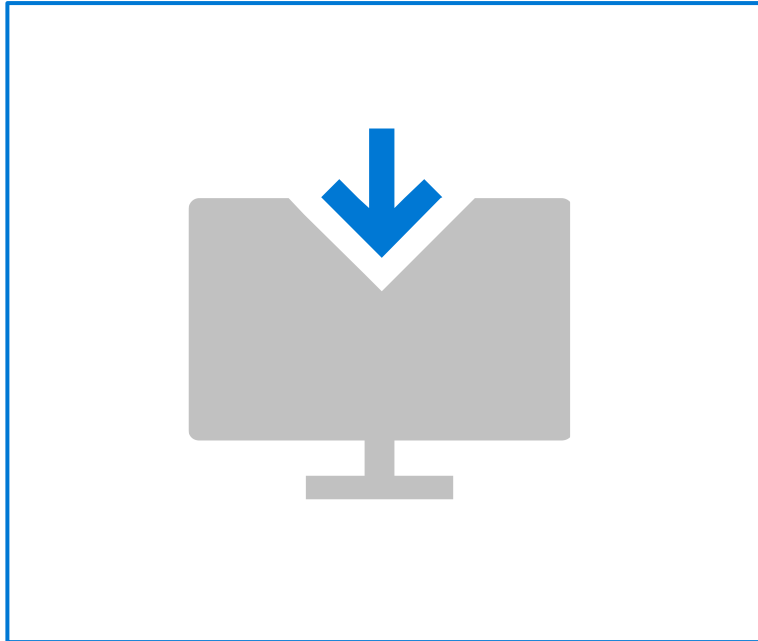


Default OOBExSetup phase



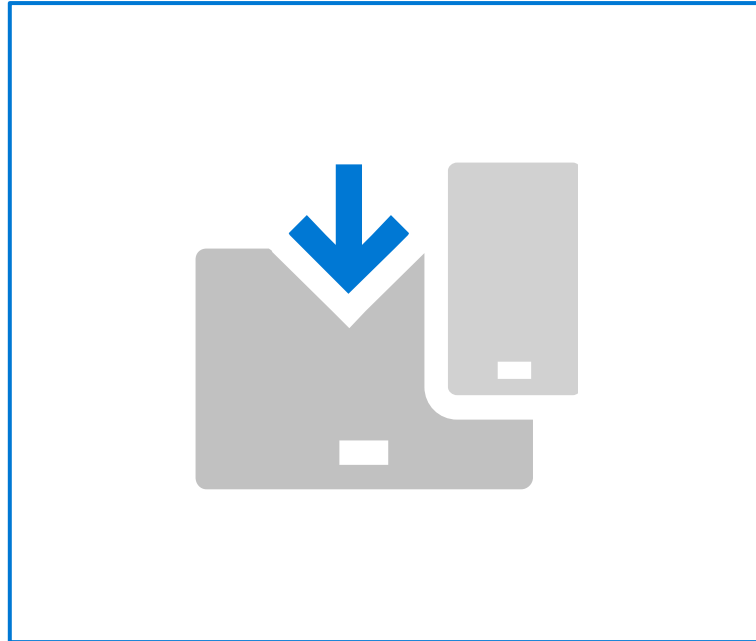
OOBExSetup phase with Windows Autopilot

Dynamic provisioning methods



Subscription activation

Change the edition of Windows 10



Mobile Device Management

Auto-enroll existing Windows 10 devices to apply configuration policies and applications installed



Provisioning packages

Apply configuration settings to a Windows 10 devices using either removable media or downloaded directly to the device

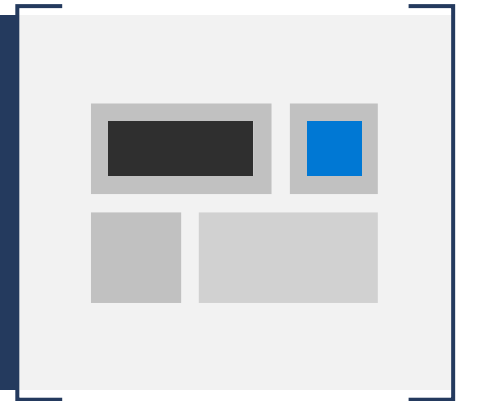
DEMO: Review Subscription Activation and Provisioning Packages

Troubleshooting Windows 10 Autopilot

When troubleshooting Windows Autopilot, the key things to understand are:

| | |
|------------------------|--|
| Autopilot flow | <ol style="list-style-type: none">1. Network connection established2. Autopilot profile downloaded3. User is authenticated (user-driven deployment mode only)4. Azure AD join occurs5. Auto MDM enrollment6. Settings applied |
| Profile download | <ol style="list-style-type: none">1. Ensure user connected device to the internet2. Ensure profile exists and is assigned<ol style="list-style-type: none">1. If a blank profile downloaded, check Microsoft Endpoint Manager admin center and assign a profile2. New profile can be downloaded by rebooting the device3. Ensure only one profile is assigned to the device |
| Key actions to perform | <ol style="list-style-type: none">1. Review Azure AD and Microsoft Intune for proper licensing and profile and user assignments2. Look for Azure AD join issues and MDM enrollment issues3. Gather troubleshooting logs mdmdiagnosticstool.exe -area Autopilot -cab <path> |

Lesson 2: Dynamic Deployment Methods



Lesson Introduction



Azure AD Join with Automatic MDM Enrollment

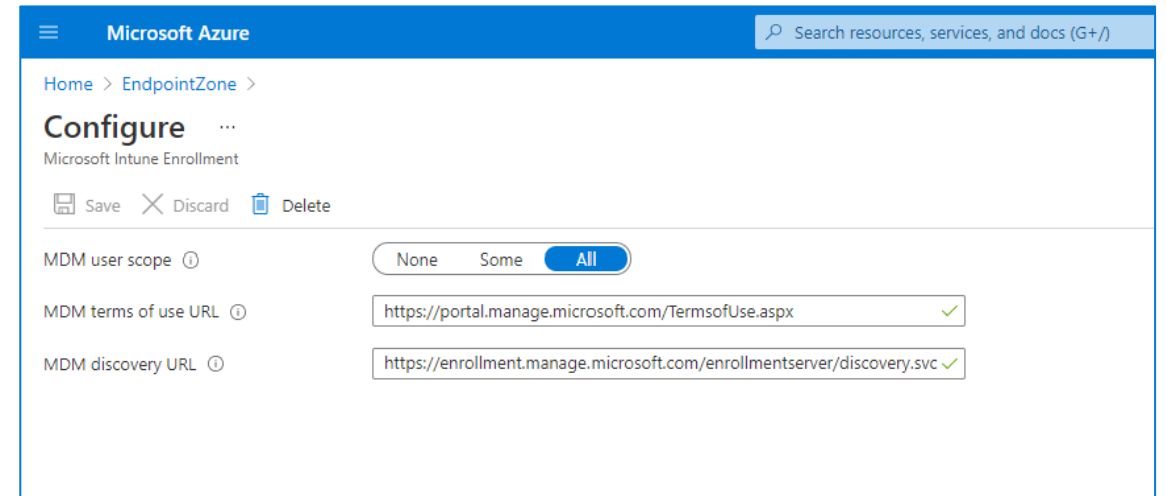
Azure AD Join with Automatic MDM Enrollment

What it is

- Registers devices in Azure AD and auto-enrolls them into Intune
- Simplifies provisioning of devices
- Applies to BYOD/CYOD scenarios

Using Azure AD/MDM, you can:

- Join devices to Azure AD automatically
- Auto-enroll your users' devices into MDM services
- Configure the joined devices by using MDM policies

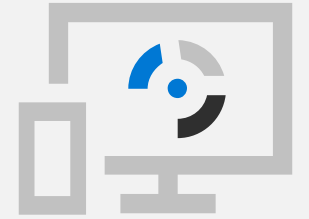


The screenshot displays the Microsoft Azure portal interface for configuring Microsoft Intune Enrollment. The page title is "Configure" and the subtitle is "Microsoft Intune Enrollment". At the top, there are navigation options: "Home > EndpointZone >". Below the title, there are three action buttons: "Save", "Discard", and "Delete". The configuration settings are as follows:

| Setting | Value |
|----------------------|---|
| MDM user scope | None Some All |
| MDM terms of use URL | https://portal.manage.microsoft.com/TermsOfUse.aspx ✓ |
| MDM discovery URL | https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc ✓ |

DEMO: Automatic Azure AD Join with MDM Enrollment

Lesson 3: Planning a Transition to Modern Management



Lesson Introduction



Co-Management – A Practical Path to Modern Management



Prerequisites for Co-Management



Modern Management Considerations



Modern Management Upgrade or Migration



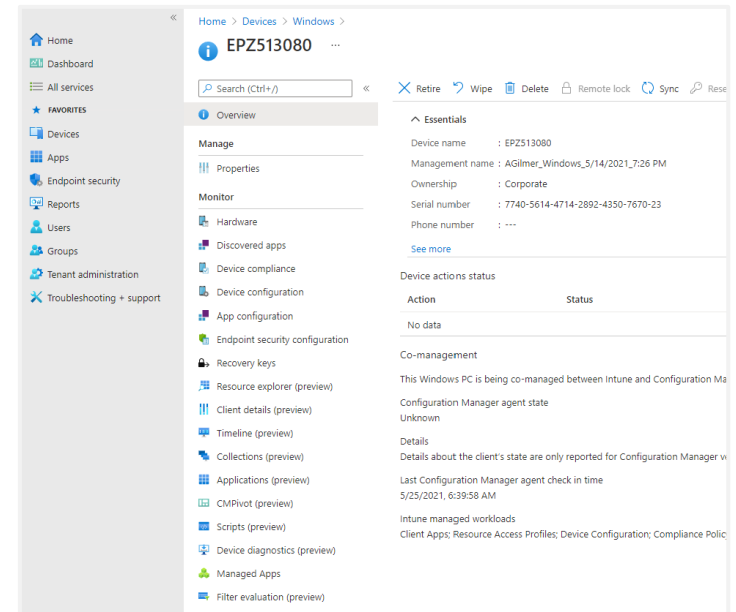
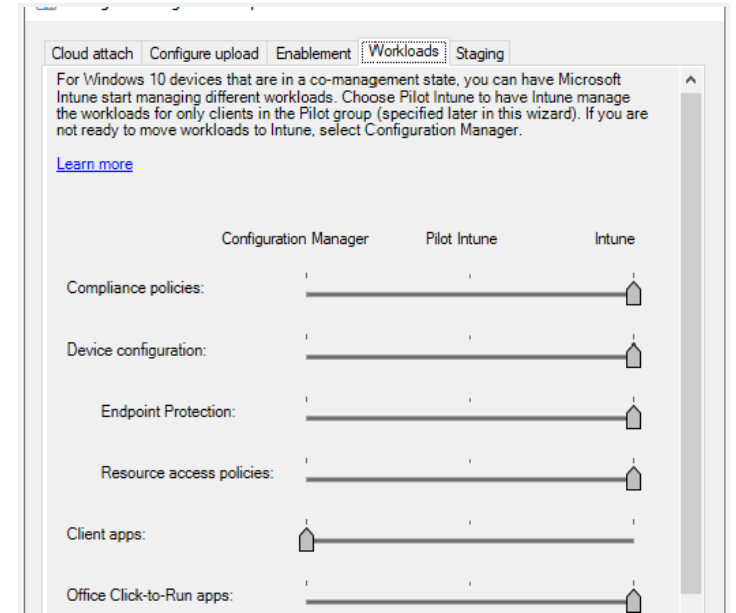
The Modern Transition: Migrating Data



The Modern Transition: New Devices with Intune

Co-management: a practical path to modern management

- Simplifies the transition to modern management
- Benefits of modern management from day one
- Devices managed using both on-premises Configuration Manager and Intune
- Even when not connected to on-premises environment, devices can be managed by Intune



Prerequisites for Co-Management



Devices must be hybrid Azure AD joined



Latest Azure AD connect must be installed and configured to sync computer accounts to Azure AD



Intune MDM must be setup and automatic enrollment configured



All users must have Enterprise Mobility + Security (EMS) or Intune license assigned



Windows 10, version 1709 or later must be used



Azure AD automatic enrollment enabled

Planning Co-Management

Transitioning Workloads to Intune

- **Resource access policies**
 - Email profile
 - Wi-Fi profile
 - VPN profile
- **Certificate profile**
- **Windows Update policies**
- **Device Configuration**
- **Microsoft 365 Select-to-Run apps**
- **Endpoint Protection**
 - Windows Defender Application Guard
 - Windows Defender Firewall
 - Windows Defender SmartScreen
 - Windows Encryption
 - Windows Defender Exploit Guard
 - Windows Defender Application Control
 - Windows Defender Security Center
 - Windows Defender Advanced Threat Protection
 - Windows Information Protection
 - BitLocker

DEMO: Configuring Co-Management

Modern Management Considerations

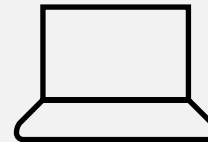
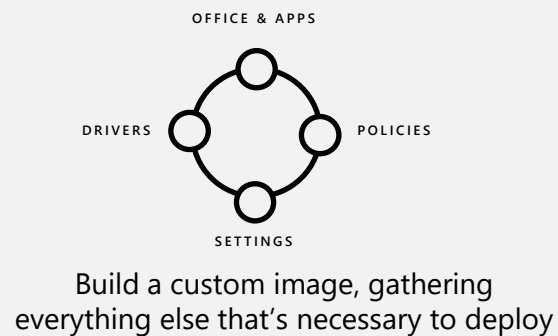
Modern Transition Considerations

| | MDT | Configuration Manager | Windows Autopilot |
|---|--|--|--|
| Require the creation golden images | Yes | Yes | No |
| Ability to rebuilt or reset the device | Yes | Yes | Yes |
| Ability to perform a bare-metal build | Yes | Yes | No |
| Can be used with any preinstalled operating system | Yes It will wipe the preinstalled operating system | Yes It will wipe the preinstalled operating system | Yes |
| Installation of applications when device is being built | Yes | Yes | Yes |
| Deployment of applications post build | No | Yes | Yes |
| Migration of user data (USMT) | Yes | Yes | No Recommend to use OneDrive Known Folders |
| Perform an in-place upgrade | No | Yes | No Deployment only |

Using Imaging with Modern Methods

Scenarios that may require you to use imaging with modern management

- A device cannot boot into Windows, resulting in the need for a bare-metal build
- Bare-metal deployments
- Client storage drive replacements
- A device is procured with a newer version of Windows 10 than has been standardized in your company



Deploy image to a new computer

The Modern Transition: Upgrade and Migration

Migrating user state and data

Migrating user data

- Device replacement
- Device is being upgraded from an older OS to Windows 10 and an in-place upgrade is not possible (e.g. 32-bit Windows to 64-bit Windows)
- A clean installation is needed

Migration scenarios

- Side-by-side: source and destination computer are different
- Wipe-and-load (refresh migration): source and destination computer are the same

Migrating user data the traditional way

Using USMT with Configuration Manager



Create a USMT Package from Configuration Manager

Create a custom USMT package or use the default package

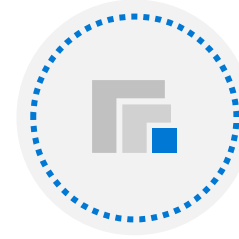


Setup a State Migration Point (Configuration Manager Site System Role)

Acts as a file share to store data

Stores a unique hash:

- Device that allows data to be captured
- Device upgraded
- Relevant data to be restored

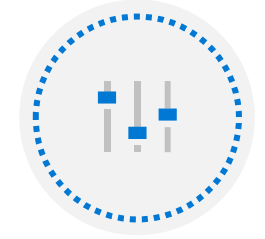


Task Sequence

Can include USMT

Occurs in the task sequence when:

- Capturing settings
- Reinstating the settings for a user depending on selected options



Use USMT Templates for Migration

xml templates that control data that is collected in a user's profile:

- MigApp.xml
- MigDocs.xml
- MigUser.xml
- ConfigMgr.xml

Migrating user data the modern way

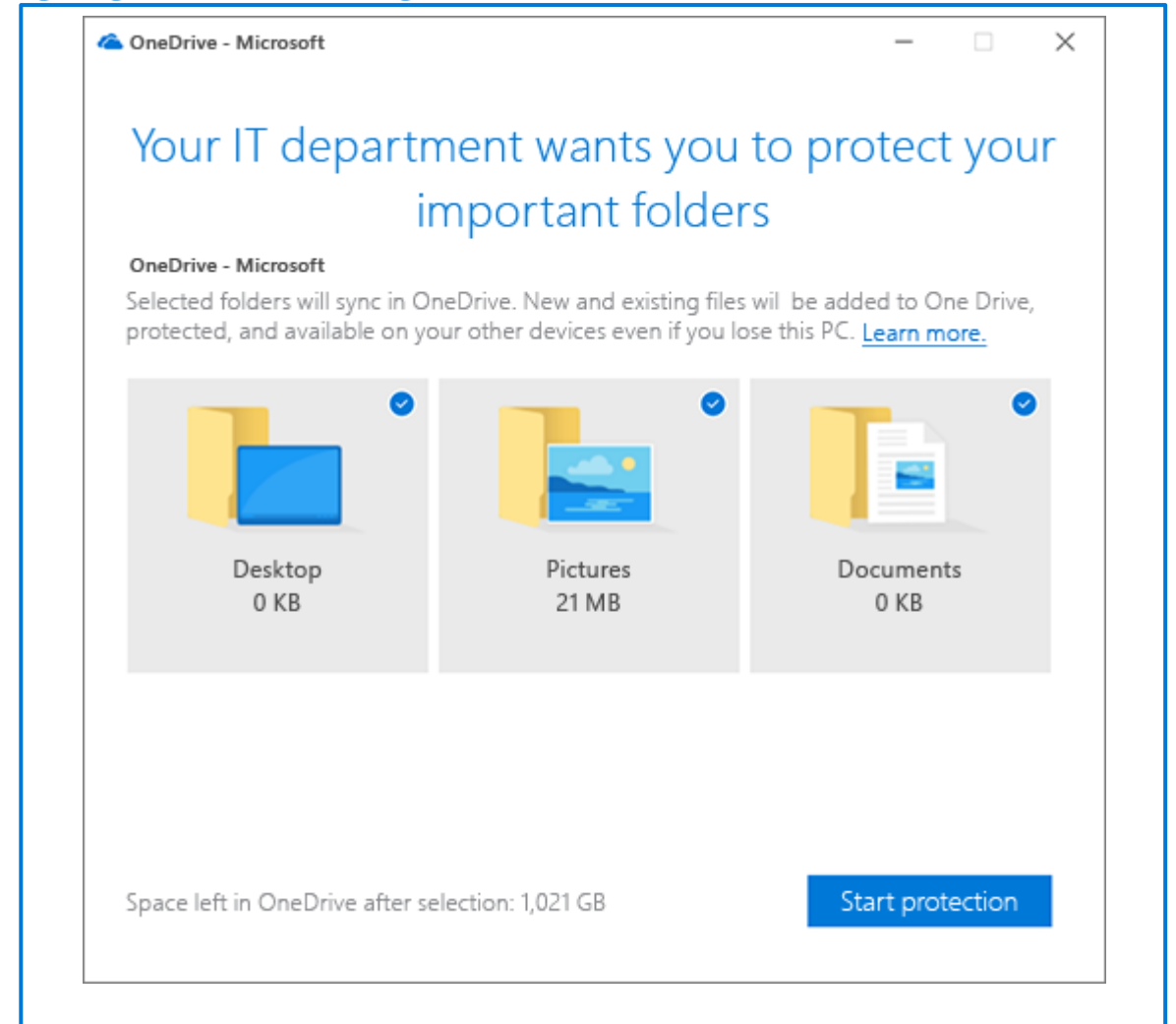
Known Folder Move - A Modern Alternative to Managing User Settings

Automatically migrate user files to OneDrive

Prompt or Silent operation

Be mindful of bandwidth when implementing

Can't use KFM if using Folder Redirection or unsupported file types



The Modern Transition: Upgrade and Migration

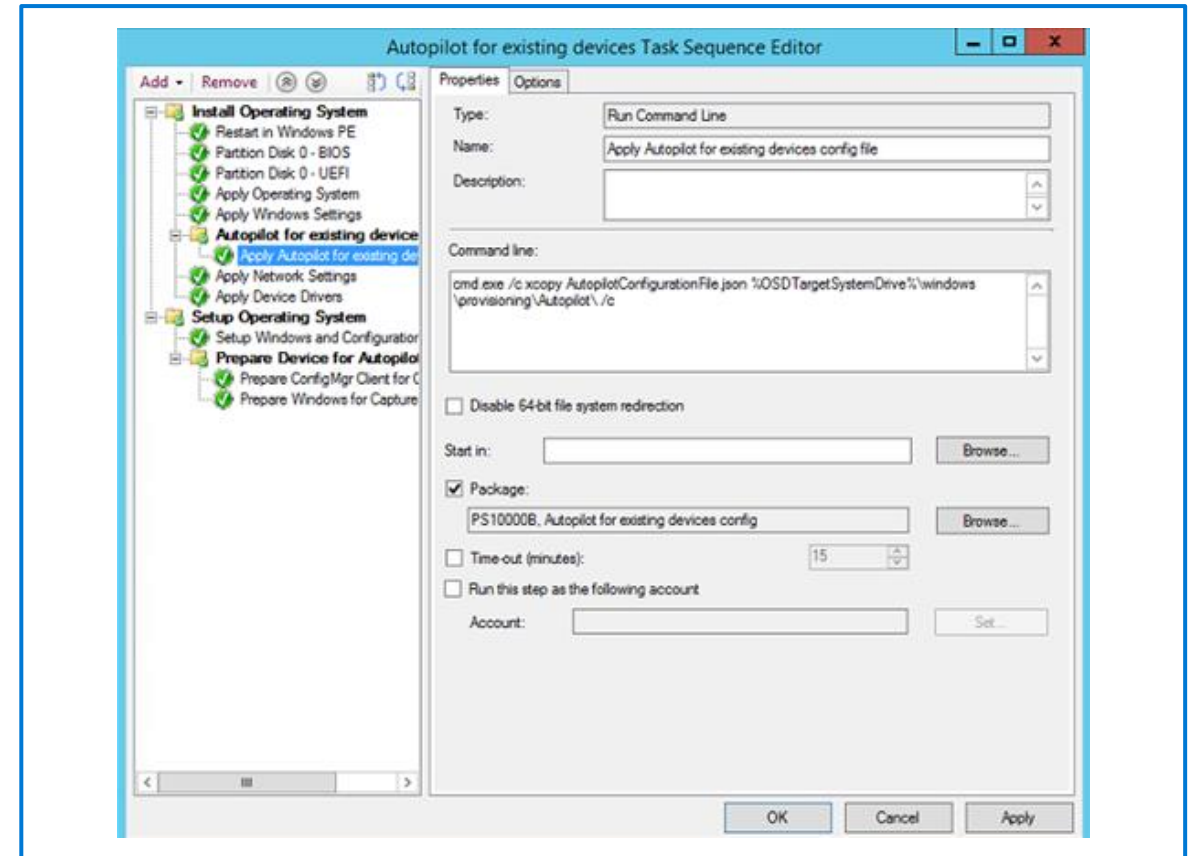
Considerations for Migrations

| In-Place upgrade | Migration |
|---|---------------------------------------|
| Preserves the environment | Provides a standardized environment |
| Doesn't need to reinstall apps or transfer data | You can control what migrates |
| Upgrade can be rolled back if needed | Cleans up the environment |
| Only certain upgrade paths are possible | You must reinstall the apps |
| You must use the in-place Windows 10 image | You can use a custom Windows 10 image |

In-Place Upgrades

Adapt modern desktop deployment with Windows Autopilot for an existing, legacy device

Transform a traditional domain joined endpoint into an Azure AD managed device and perform a rebuild, all within the same piece of automation



The Modern Transition: Workload Migration

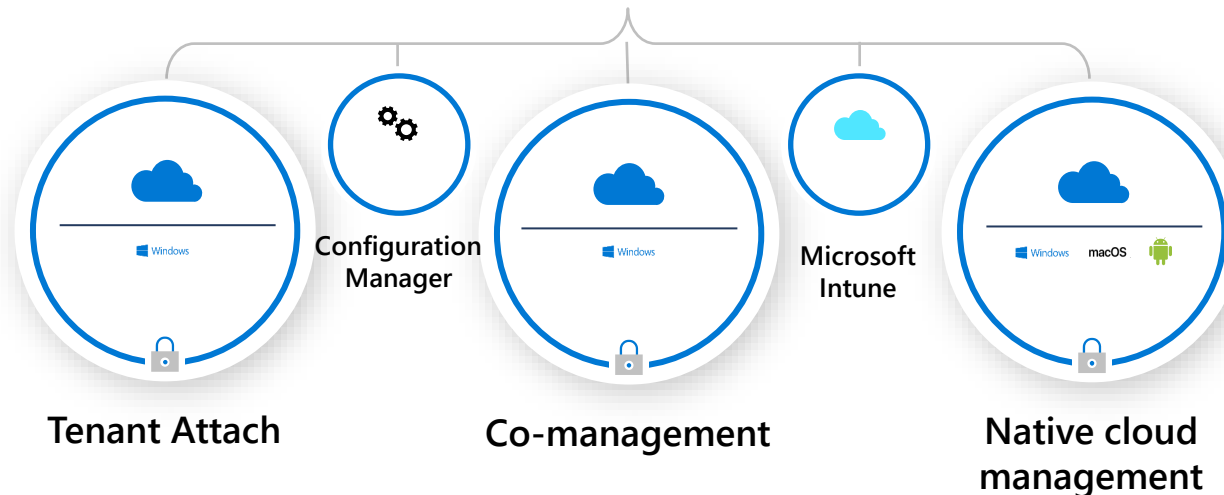
Migrating client management to Intune

Start moving to cloud-management

- Simplifies the transition to modern management
- Benefits of modern management from day one
- Devices managed using both Configuration Manager and Intune
- Even when not connected to on-premises environment, devices can be managed by Intune

Smaller or new organizations should start in the cloud

- The OS configuration capabilities provided by Intune meet the needs
- Applications are modern and relatively simple installs
- There is not an excessive amount of existing legacy applications
- The existing configuration management deployment is relatively simple



Resources

[Windows Autopilot Documentation](#)

[Join the Windows Community](#)

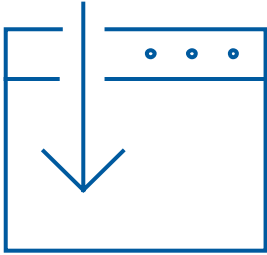
[Windows IT Pro Blog](#)

[Windows technical documentation](#)

[Windows Learning Paths](#)



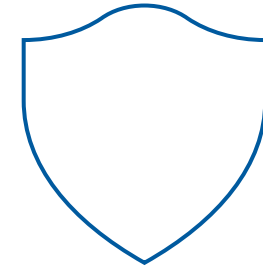
Surface Deployment with Autopilot



**Streamlined
Deployment**

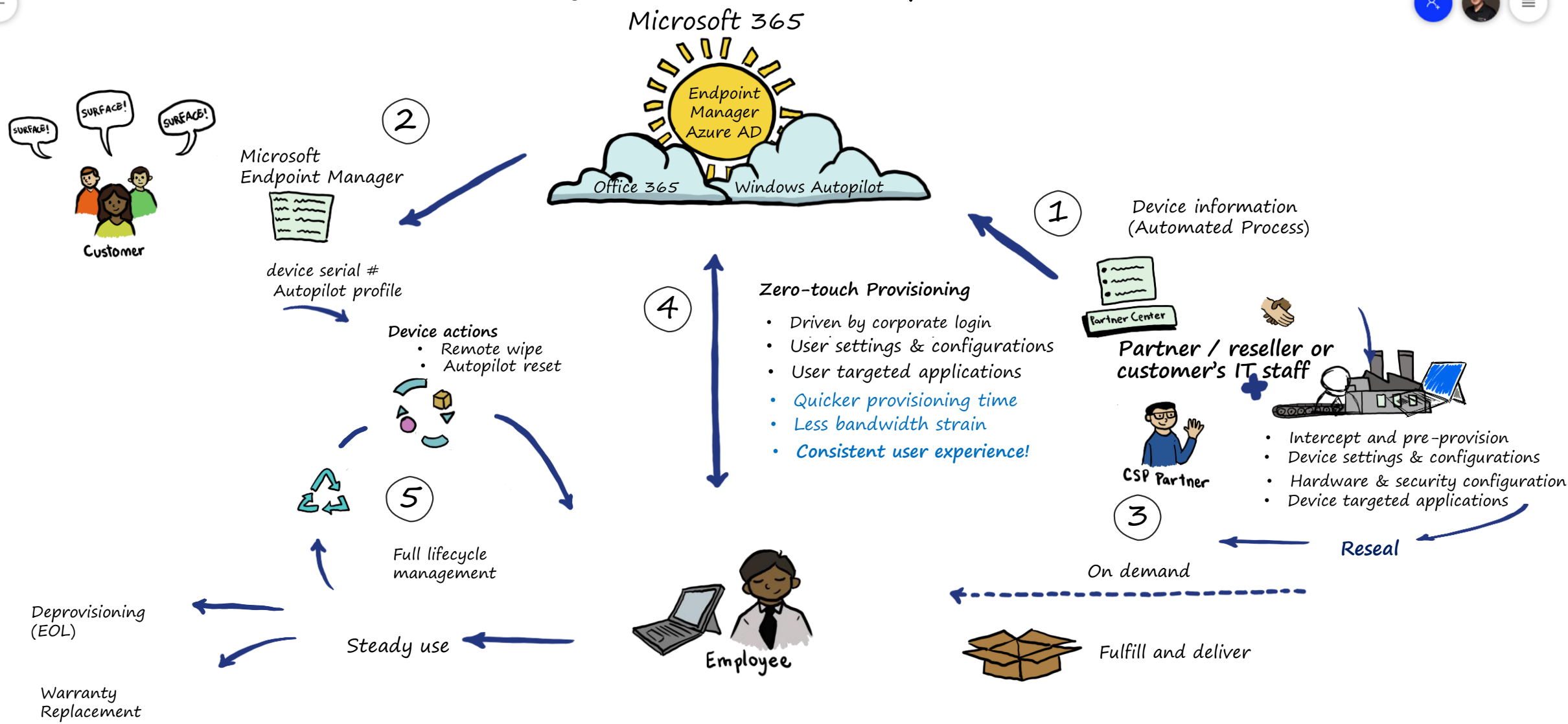
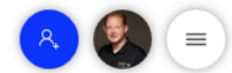


**Complete device
Management**



**Intelligent
Security
+ Secure hardware**

Surface Devices across the lifecycle: Windows Autopilot and White Glove



Windows Autopilot on Surface

End-users are immediately productive with Surface!

- Only OEM to automatically deregister/reregister returned devices
- Partner-channel enabled and ready
- Sales & Support operationalized and mature and free
- Commercial SKU is tuned for fastest Autopilot experience with Office Pro Plus and clean image
- PKID and OS Version number on all Commercial SKUs on latest generation of products



Streamlined deployments

Zero touch deployment through Autopilot

Partner expertise that reduces IT complexity

Lifecycle strategy to remotely replace and reuse

IT saves over **25** minutes per device deployed¹

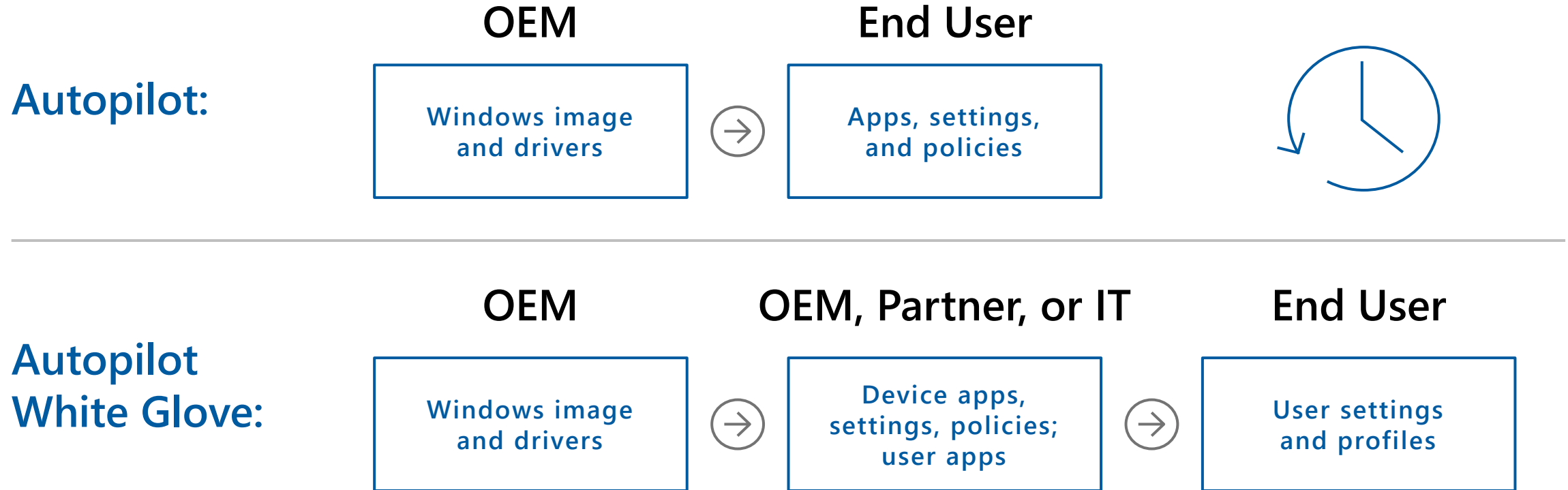
78% agree they have reduced IT time and cost to deploy Surface devices vs. non-Surface devices¹

¹A Forrester Total Economic Impact™ Study:
Maximizing your ROI from Microsoft 365 Enterprise with Microsoft Surface



Windows Autopilot

White Glove



Demo

Autopilot (White Glove) -> Full Productivity



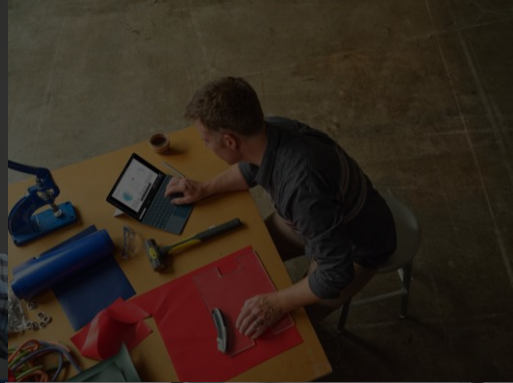
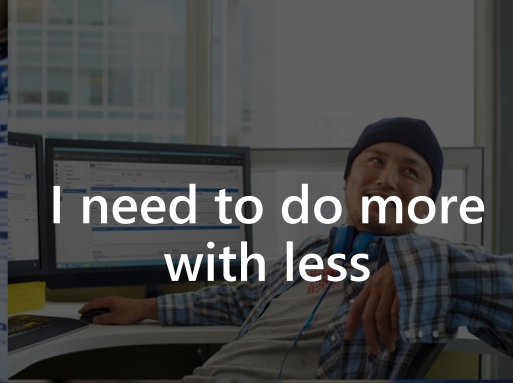
Modern Management on Surface



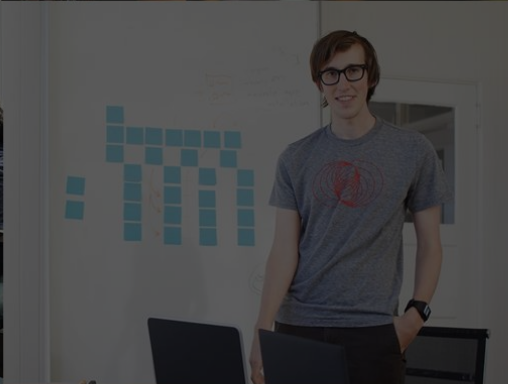
Help my users collaborate remotely



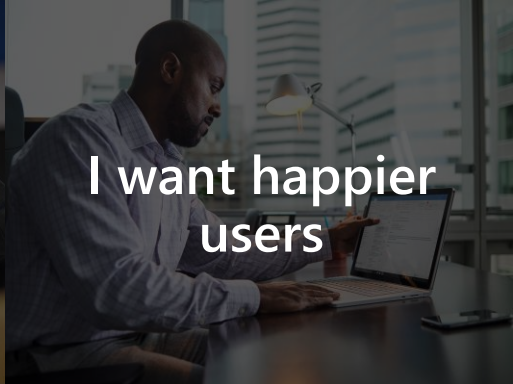
I need to do more with less



Help me stay safe and secure



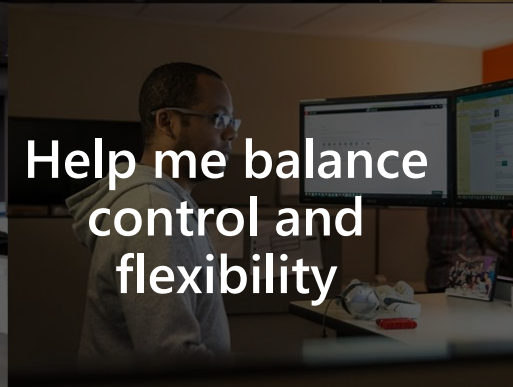
I'm drowning in complexity!



I want happier users



Help me succeed in a hybrid environment



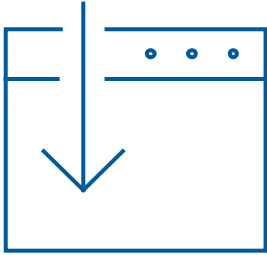
Help me balance control and flexibility





**IT Pros love Microsoft
Surface + M365 because
it reduces cost and
complexity**





**Streamlined
Deployment**



**Complete device
Management**



**Intelligent
Security
+ Secure hardware**

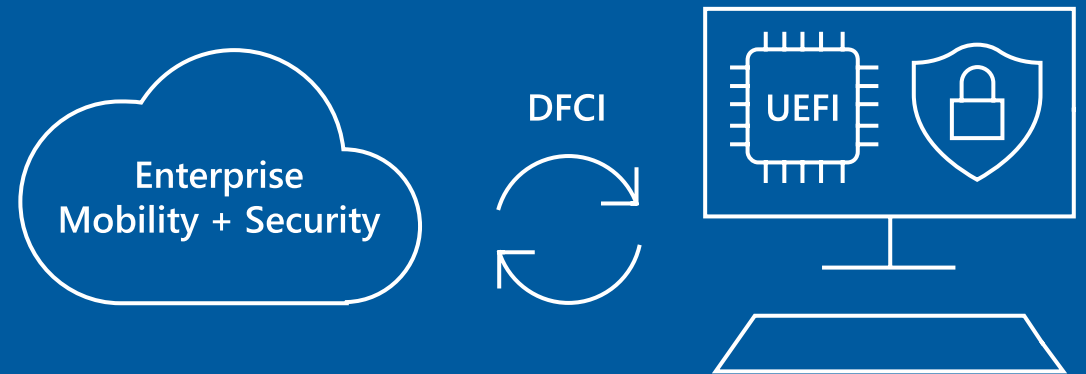
Intune Zero-touch UEFI Management

IT can remotely manage UEFI BIOS settings w/o physical access to the device

Builds on the Surface-team-developed Surface Enterprise Management Mode (SEMM)

Automatically available to devices deployed via Autopilot

Implemented first on Surface

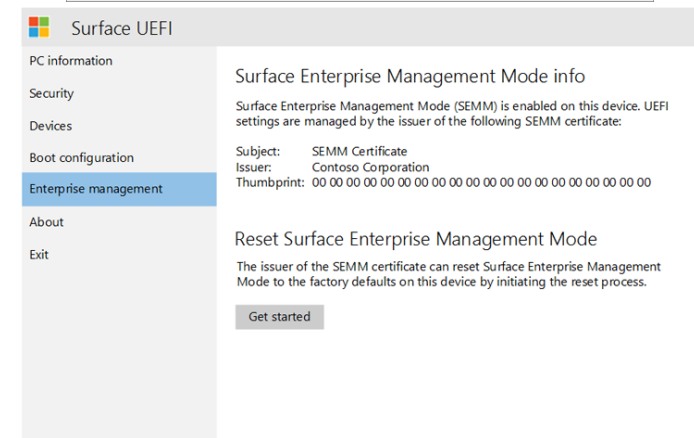
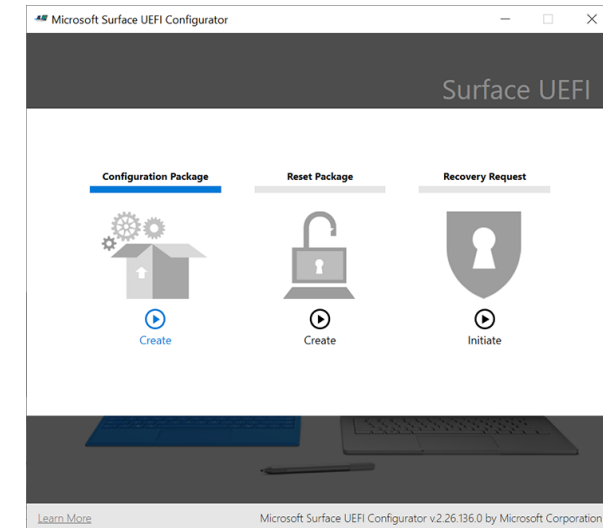


Surface Enterprise Management Mode (SEMM)

Secure and manage firmware settings in your organization

Prepare UEFI settings configurations and install them on a Surface device.

Manage independently or through SEMM module in Microsoft Endpoint Manager Config Mgr (on-prem)

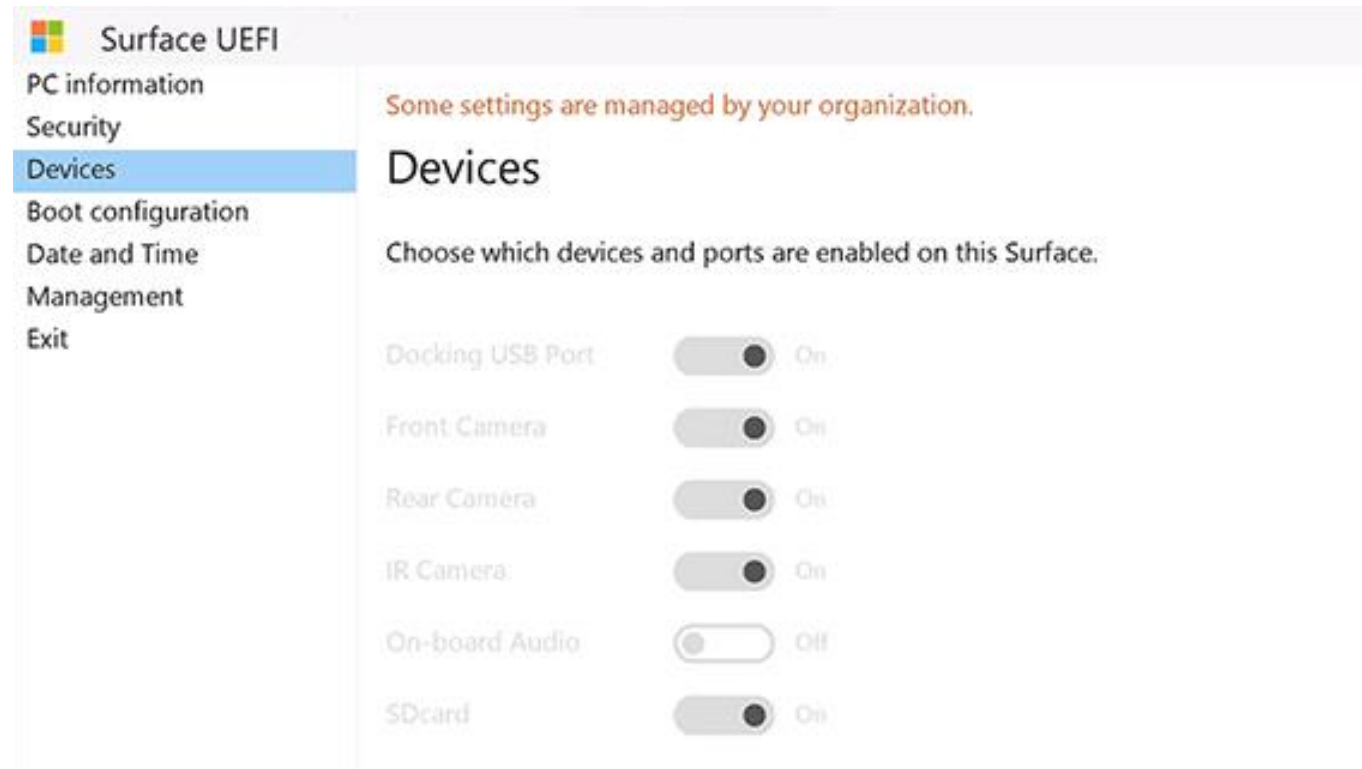


Intune Zero-touch UEFI Management

UEFI Management is locked to Intune only

Granular management of firmware

Pre-boot disablement of firmware to reduce security vulnerabilities or unneeded device capabilities



Modern management

Complete device management from UEFI to Windows

Always up to date—automatically, even while asleep

Purpose built tools for diagnostics and tuning

15% reduction in device and application performance tickets with Surface¹

78% agree that Microsoft Surface reduced the IT time and labor to manage and update Microsoft 365¹

¹A Forrester Total Economic Impact™ Study:
Maximizing your ROI from Microsoft 365 Enterprise with Microsoft Surface



Demo

DFCI – Microsoft Endpoint Manager (Intune) management of Surface Firmware

Device configuration - Profiles

Search (Ctrl+)

Overview

Manage

Profiles

PowerShell scripts

eSIM cellular profiles (preview)

Monitor

Assignment status

Audit logs

Devices with restricted apps

Encryption report

Setup

Certificate connectors

Telecom expense management

Derived Credentials

Help and support

Help and support

+ Create profile Columns Filter Refresh Export

Search by name

| Profile Name | Platform | Profile Type | Assigned | Last Modified | |
|---|----------------------|---------------------|----------|-------------------|-----|
| iOS device restriction to block Game Center | iOS/iPadOS | Device restrictions | Yes | 5/18/19, 10:00 AM | ... |
| Win10-DeviceConfig-Restrictions | Windows 10 and later | Device restrictions | Yes | 5/18/19, 10:00 AM | ... |

Tenant Lockdown

Surface continues to implement Microsoft 365 technologies 1st and Best

Tenant Lockdown—Ensure device remains bound to owning tenant in case of accidental reset or a theft/loss of the device

Reset can only take place when connected to a network with no ability to create a local account

Builds in technologies from Autopilot, Azure AD and the new Intune UEFI Management

Best-in-class security

Defense in depth from silicon to cloud

Built-in Secure Hardware—Fully Enabled

Passwords elimination: Windows Hello for Business

80% reduction in annual security breach costs¹

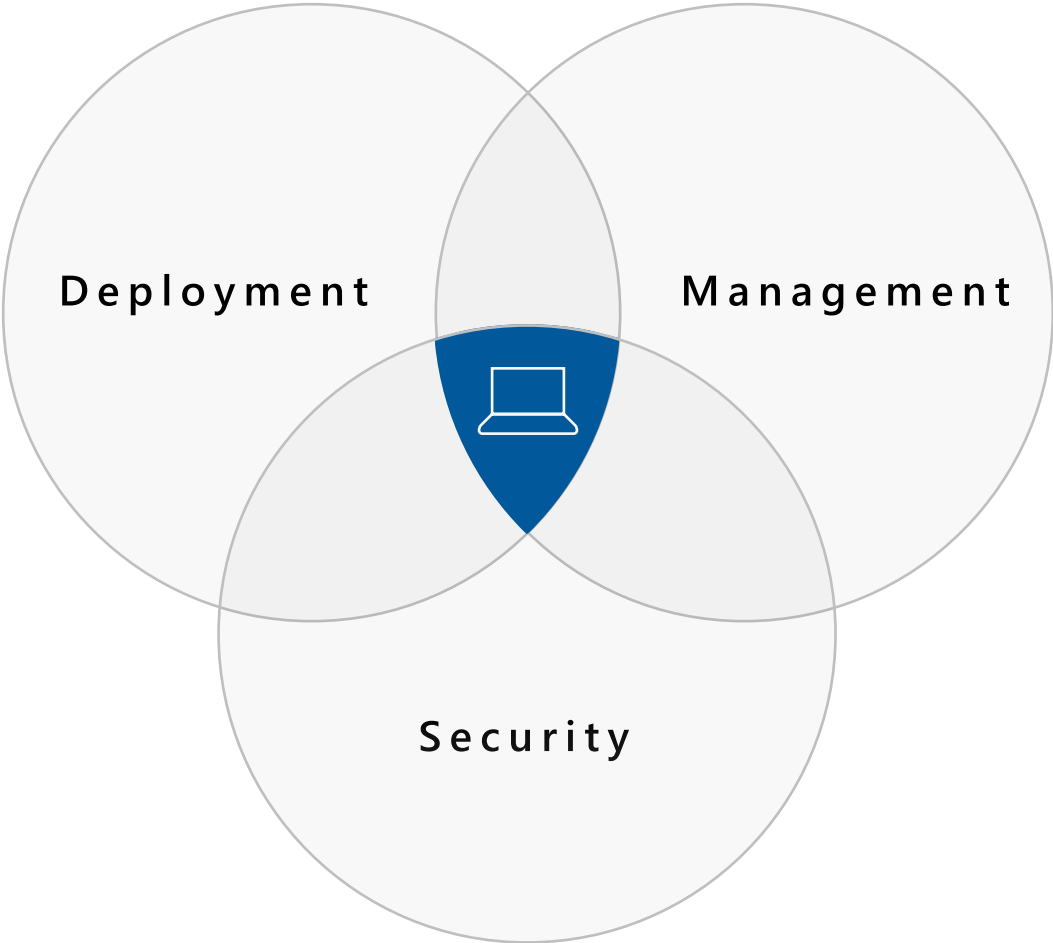
50% reduction in annual security breach volume¹

¹A Forrester Total Economic Impact™ Study:
Maximizing your ROI from Microsoft 365 Enterprise with Microsoft Surface



- Intune Wipe and Retire
- Microsoft Defender 365
- Windows Update for Business
- Conditional Access
- Advanced Windows Security Features
- Windows Hello for Business
- Intune UEFI Management
- BitLocker
- Secure Boot
- SEMM
- UEFI w/TPM 2.0





Removing the barriers

Surface empowers productivity and innovation

Workers realized nearly **five hours**
in weekly productivity gains¹

Business decision making by senior
leadership was accelerated by nearly **21%**¹

76% agree that Microsoft 365-powered Surface
devices have helped improve employee retention¹



¹A Forrester Total Economic Impact™ Study:
Maximizing your ROI from Microsoft 365 Enterprise with Microsoft Surface

Our Surface Family

Studio

The ultimate creative studio

The most immersive and powerful Surface desktop with a 28" fully adjustable touch-screen.



Book

Powerhouse performance

Ultimate performance in a laptop form factor with 13.5" or 15" detachable touchscreen.



Laptop

Style and speed

The perfect everyday laptop is now even faster. Choose from two durable keyboard finishes with 13.5" or 15" touchscreens.



Pro

Ultra-light versatile

The iconic Surface 2-in-1, now even faster and more versatile with USB-A & USB-C.



Go

Portable power

The smallest, most affordable Surface 2-in-1 with a 10" touchscreen. Available with 4G LTE



Hub

Teamwork without boundaries

The revolutionary all-in-one digital whiteboard, meetings platform, and collaborative computing device





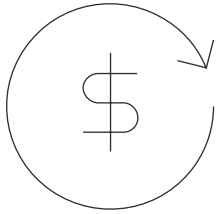
Surface to Chip Cloud Security



Today's workplace needs an integrated security solution

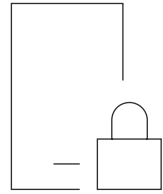
- ✓ Organizations are pivoting to remote work
- ✓ Current network infrastructures were not built with today's security in mind
- ✓ Increasingly sophisticated and targeted attacks, specifically at a firmware level
- ✓ Customers need an added layer of security to ensure comprehensive protection as they adapt to remote work

The increasing costs of data breaches



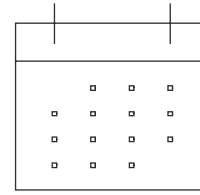
\$3.86M
USD

average total cost of data breach to companies worldwide, +6.4% from 2017 ¹



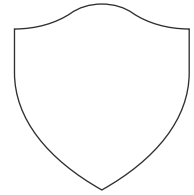
> \$124B
USD

will be spent worldwide for information security in 2019 ²



190
DAYS

average mean time it takes to identify a data breach ¹



\$10B
USD

will be spent globally on security awareness training for employees in 2027 ³

¹NASCIO, Ponemon Institute's 2018 Cost of a Data Breach Study, September 2018. ²Gartner, Gartner Forecasts Worldwide Information Security to Exceed \$124 Billion in 2019, August 2018. ³<https://www.cpomagazine.com/cyber-security/11-eye-opening-cyber-security-statistics-for-2019>, June 2019.

Did you know? Security effects more than just IT

C-Suite & Finance



40%

Three years after an attack, breached companies underperform the index by a margin of over 40%.⁴

Product Development



96%

96% of cybercriminals attack to gather intelligence such as proprietary IP.⁴

HR & Operations



24x

The average cost of downtime is 24 times higher than the average ransom amount.⁴

Legal



**LAWSUITS
& FINES**

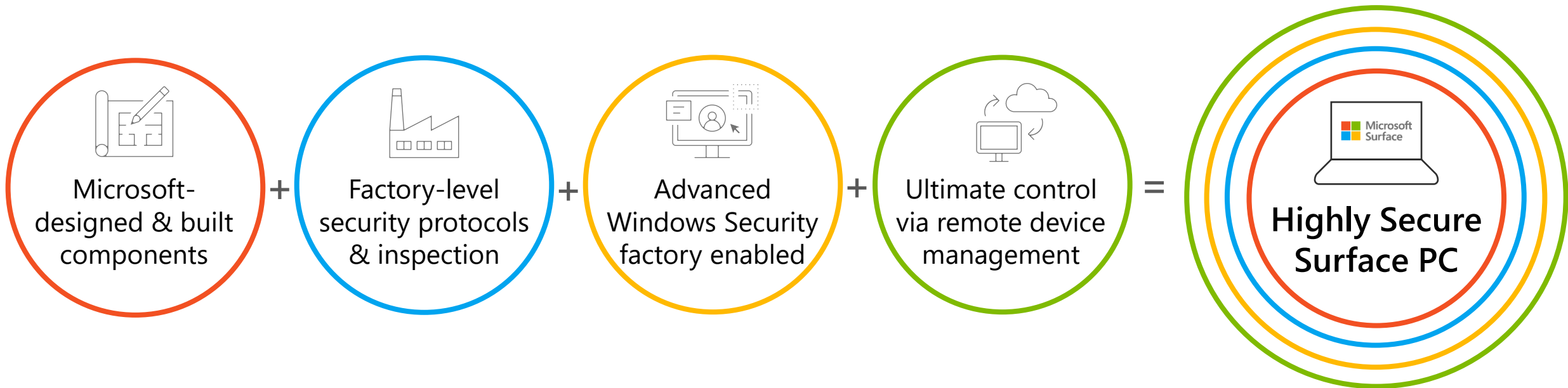
Companies can be sued by customers whose PII has been stolen; and fined by regulatory agencies.¹¹

¹ 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2020] EDITION] – Comparitech, July 2020, <https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/>

² <https://www.blackstratus.com/risk-liability-assessment/>

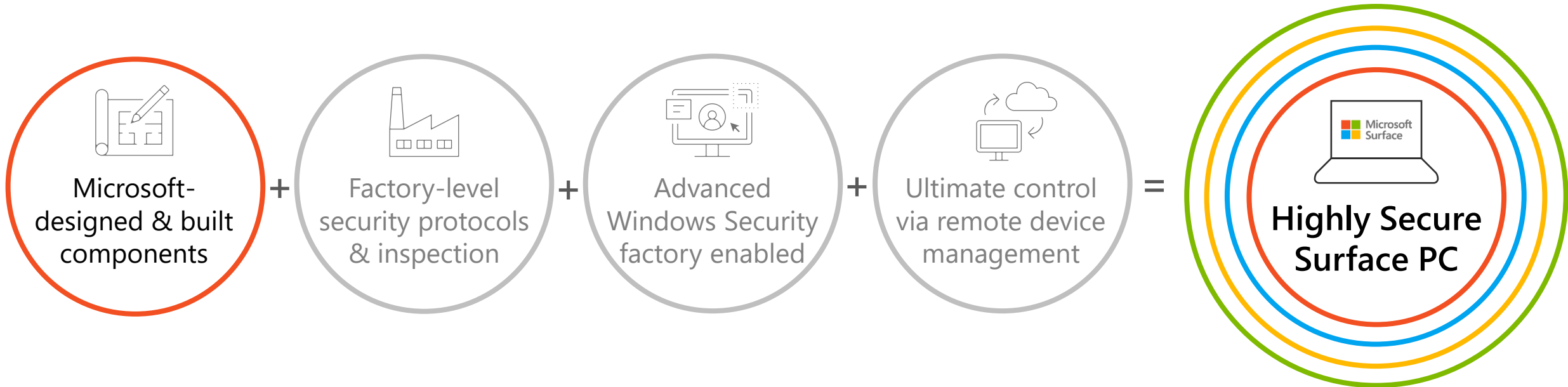
There is a clear need for device protection.

The answer? Layered security with Microsoft Surface.



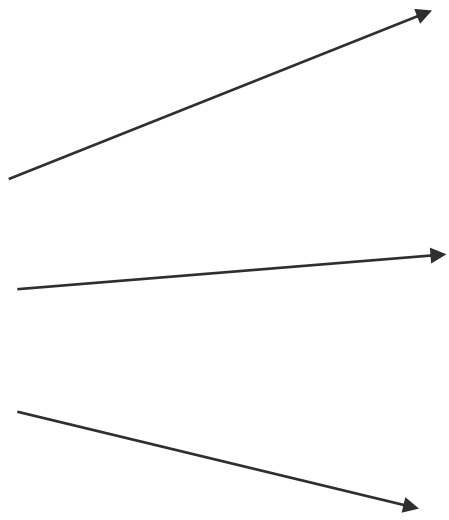
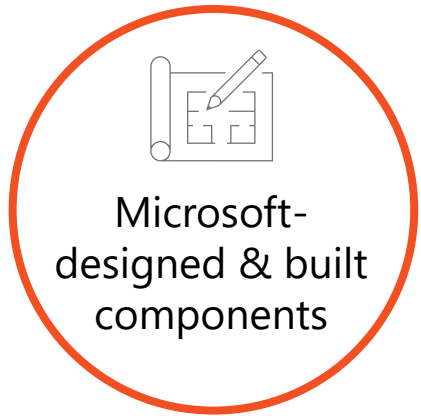
Every layer of Surface from chip to cloud **is developed and maintained by Microsoft**, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Defense in Depth: Layered security with Surface



Every layer of Surface from chip to cloud **is developed and maintained by Microsoft**, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

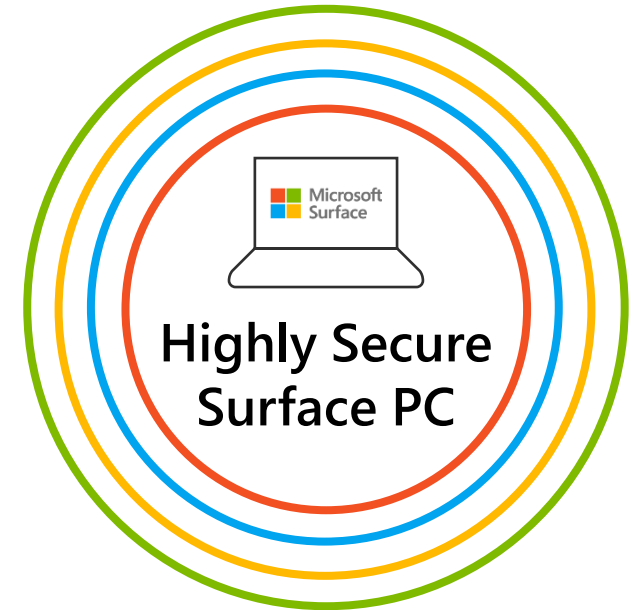
Defense in Depth: Layered security with Surface



Microsoft built UEFI for Boot Security and Firmware Management

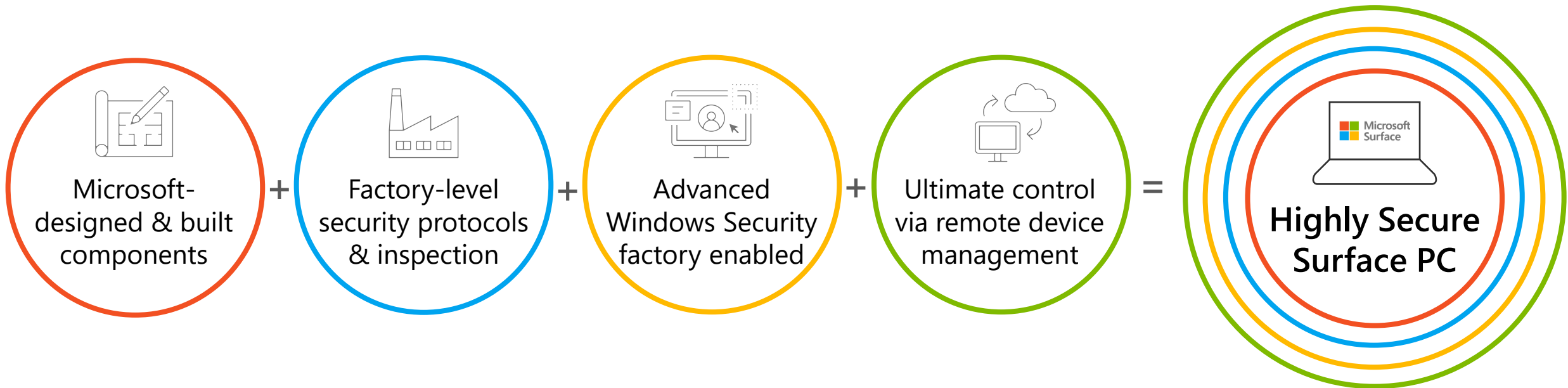
TPM 2.0 Security Processor to ensure data protection

Windows 10 and Microsoft 365 Defender enterprise defense suite, built-in is better than bolt-on



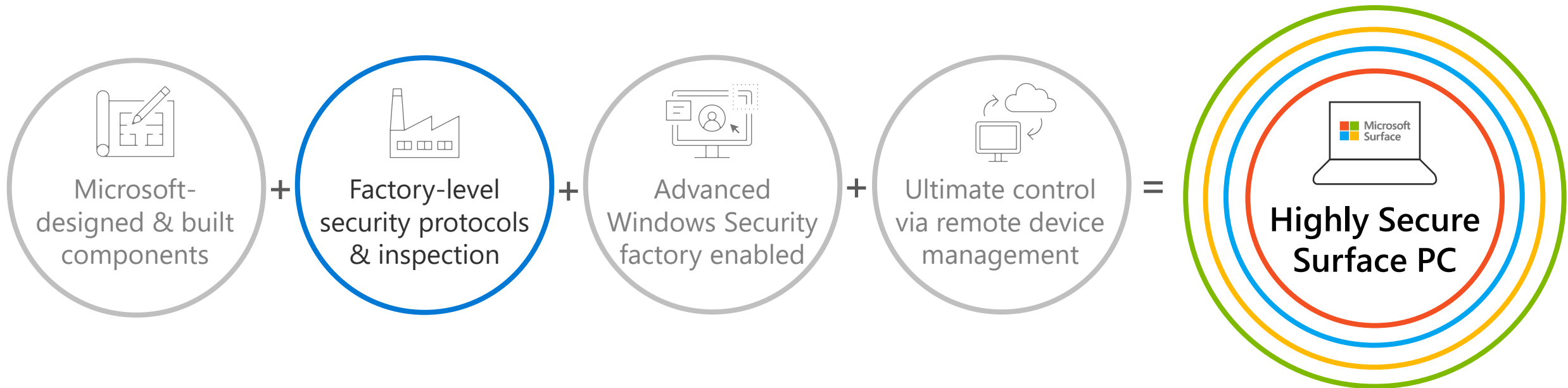
Every layer of Surface from chip to cloud **is developed and maintained by Microsoft**, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Defense in Depth: Layered security with Surface



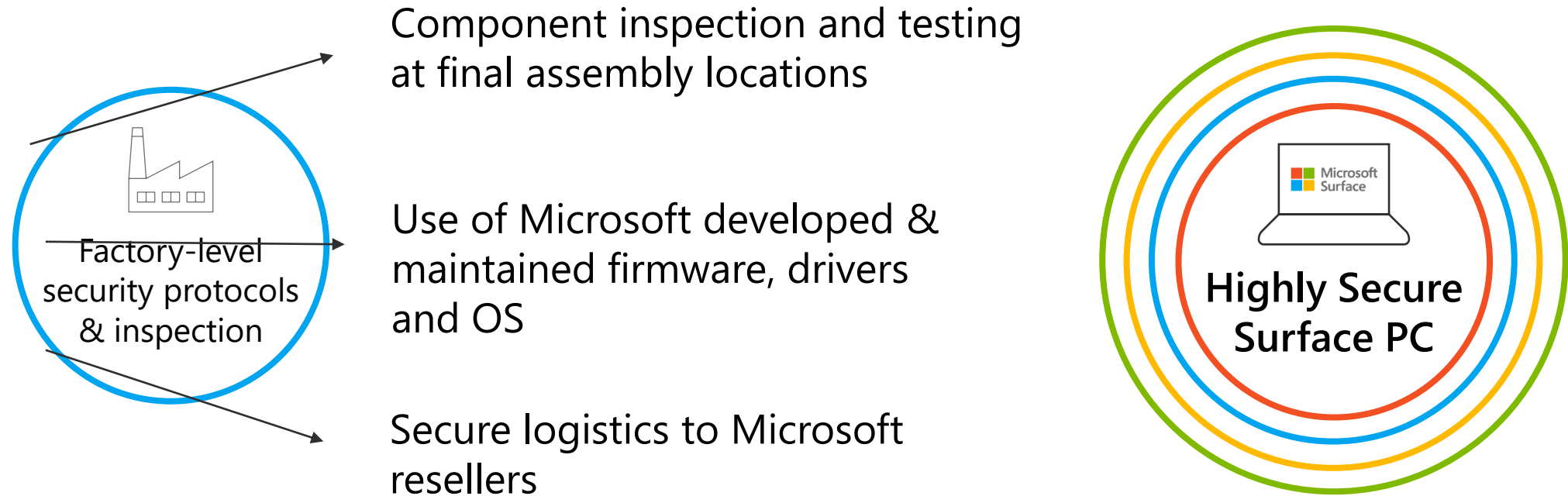
Every layer of Surface from chip to cloud **is developed and maintained by Microsoft**, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Defense in Depth: Layered security with Surface



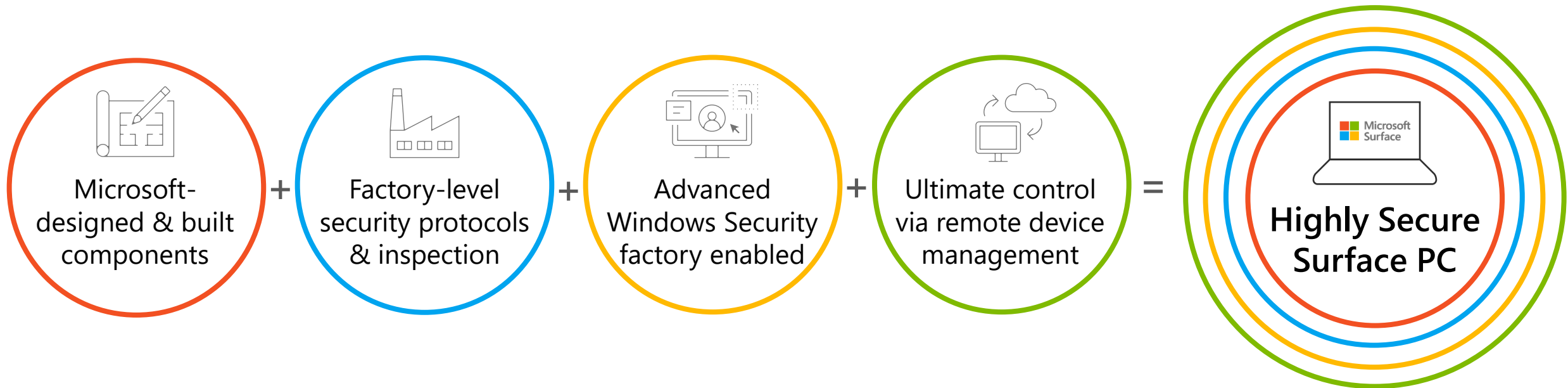
Every layer of Surface from chip to cloud **is developed and maintained by Microsoft**, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Defense in Depth: Layered security with Surface



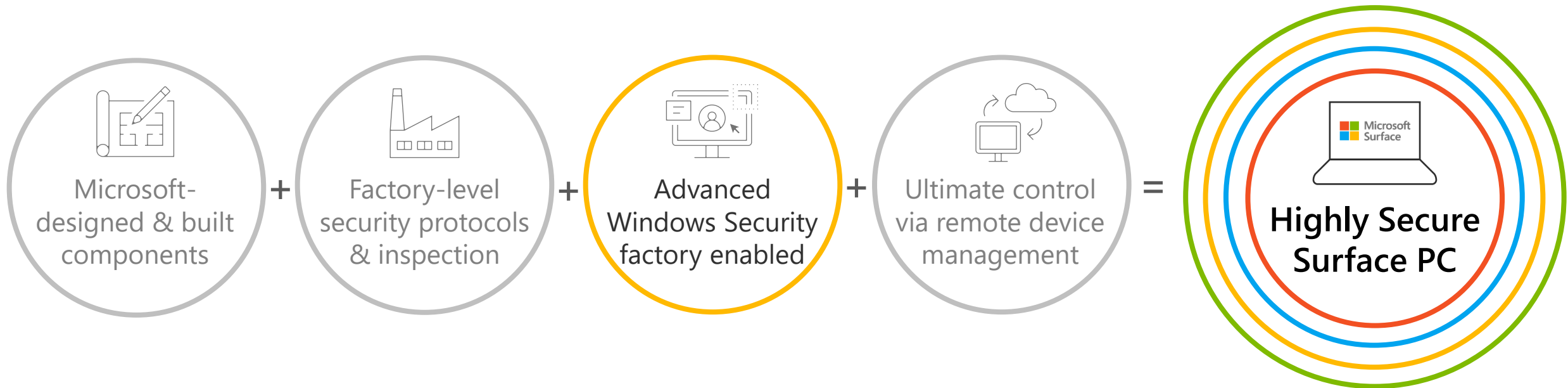
Every layer of Surface from chip to cloud **is developed and maintained by Microsoft**, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Defense in Depth: Layered security with Surface



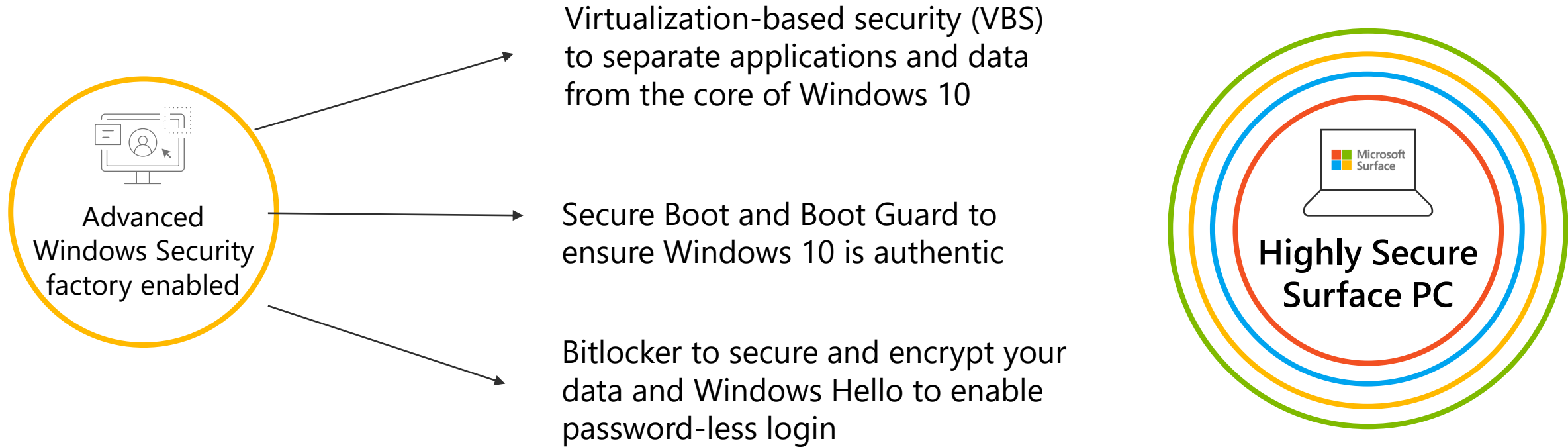
Every layer of Surface from chip to cloud **is developed and maintained by Microsoft**, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Defense in Depth: Layered security with Surface



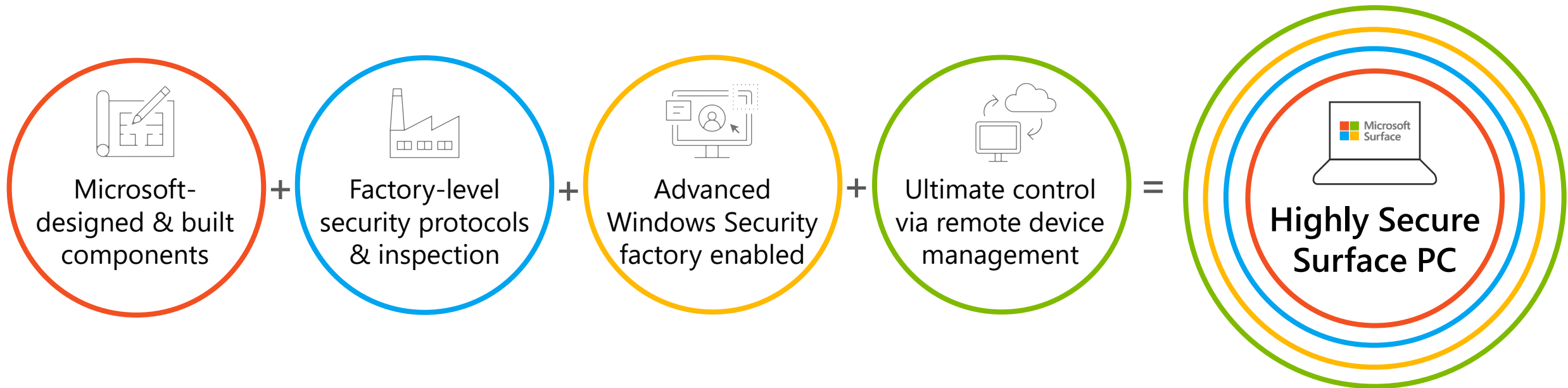
Every layer of Surface from chip to cloud **is developed and maintained by Microsoft**, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Defense in Depth: Layered security with Surface



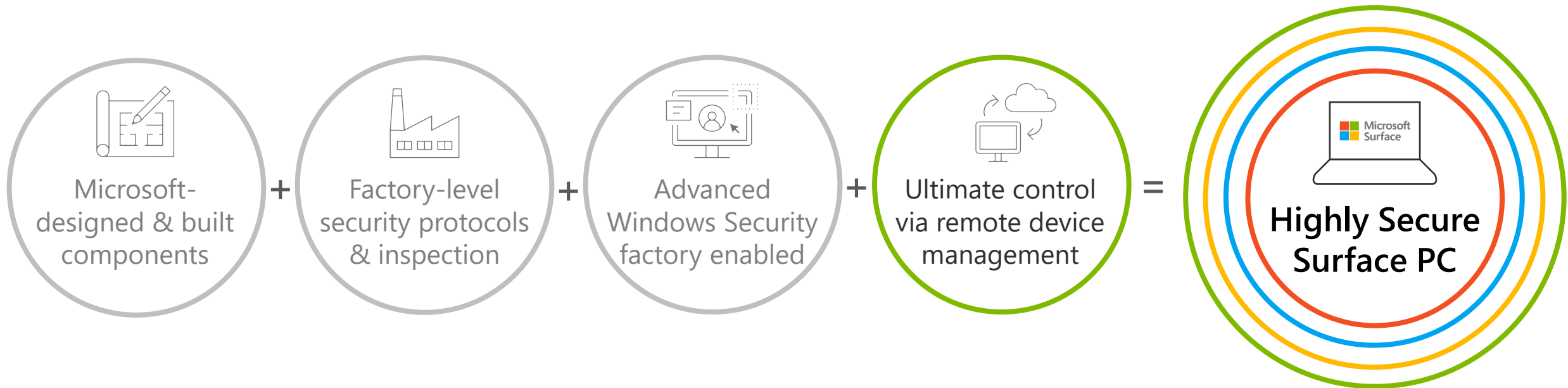
Every layer of Surface from chip to cloud **is developed and maintained by Microsoft**, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Defense in Depth: Layered security with Surface



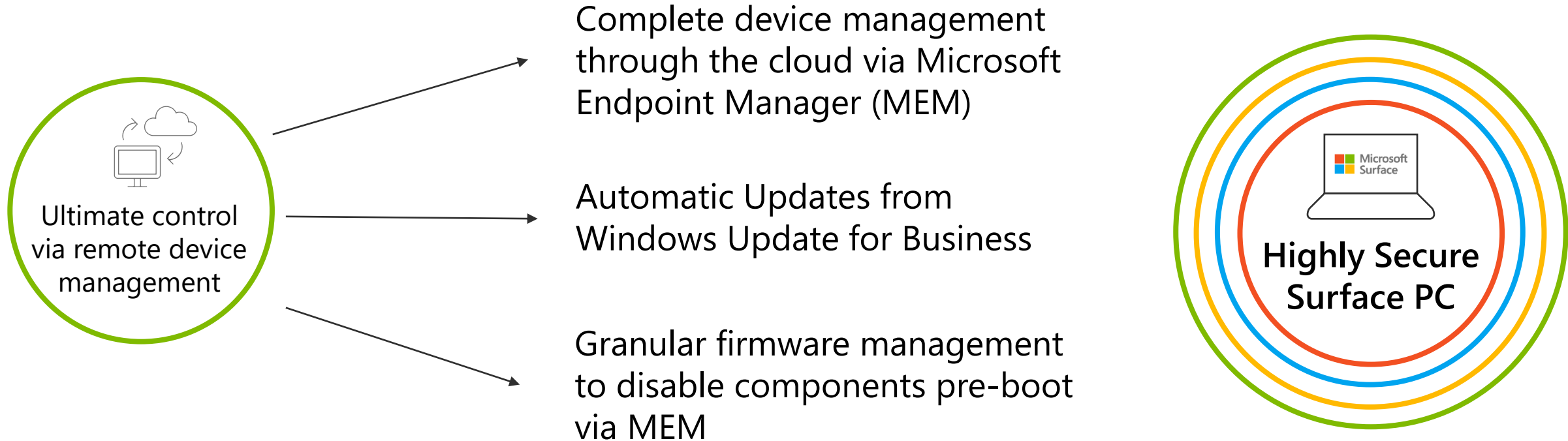
Every layer of Surface from chip to cloud **is developed and maintained by Microsoft**, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Defense in Depth: Layered security with Surface



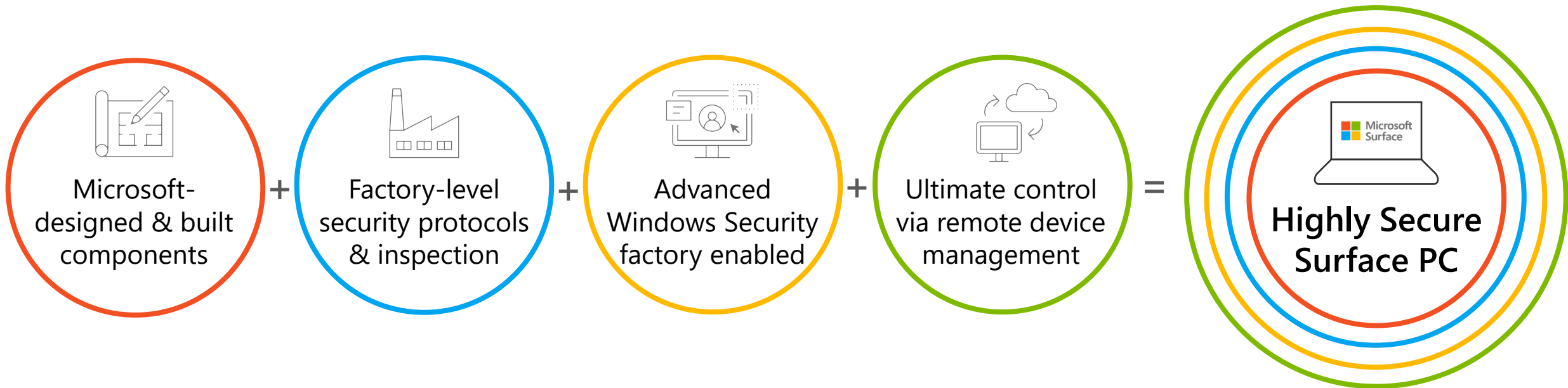
Every layer of Surface from chip to cloud **is developed and maintained by Microsoft**, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Defense in Depth: Layered security with Surface



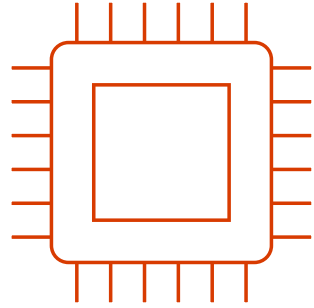
Every layer of Surface from chip to cloud **is developed and maintained by Microsoft**, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Defense in Depth: Layered security with Surface



Every layer of Surface from chip to cloud **is developed and maintained by Microsoft**, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Why firmware defense matters



“ By 2022, 70% of organizations that do not have a firmware upgrade plan in place will be breached due to a firmware vulnerability. ”

- Gartner



Jan 2018

Spectre & Meltdown vulnerability at processor level of all x86, PowerPC and select ARM devices.

Jan 2019

ShadowHammer supply chain attack against ASUS firmware infecting > 1M devices.

Sept 2020

MosaicRegressor is identified as a bootkit that over-writes the UEFI and is used for espionage and data exfiltration.

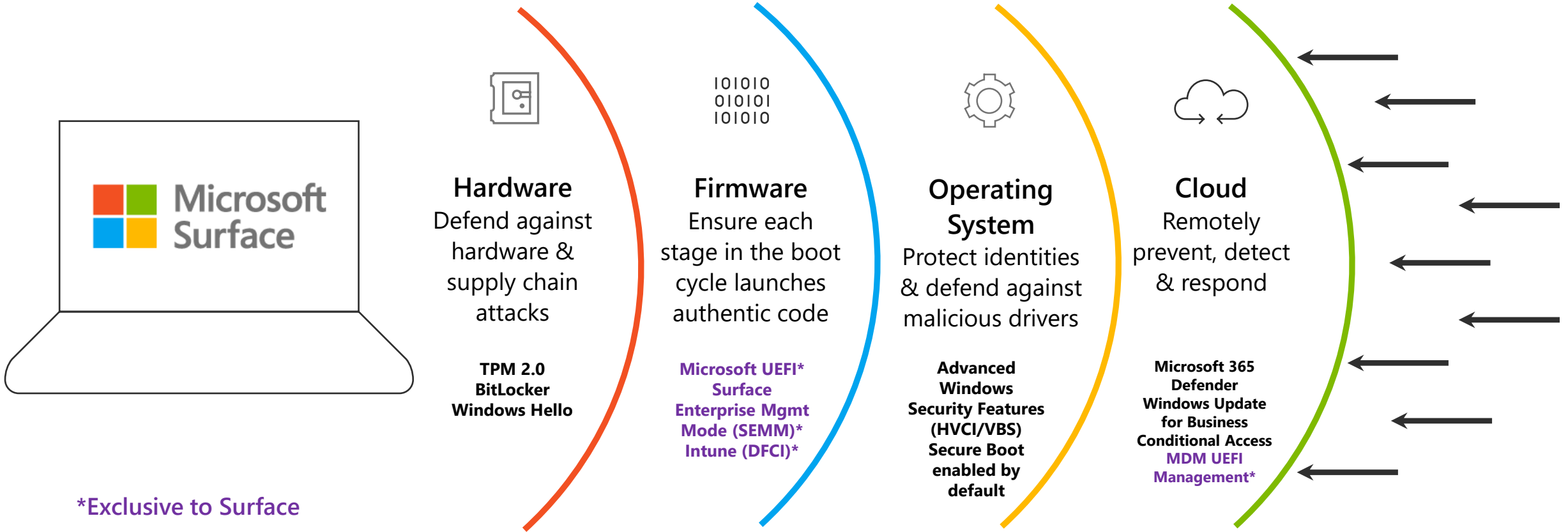
Sept 2020

US National Security Agency (NSA) issues technical report recommending Secure Boot and protections for UEFI/Firmware.

Dec 2020

Trickbot malware begins to target UEFI vulnerabilities to overwrite firmware and takeover OS as a bootkit.

Chip to cloud security is built-in to Surface DNA

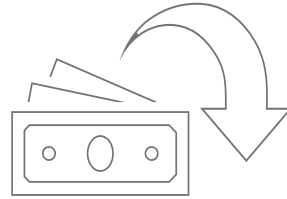


Reduce risk and lower costs with Microsoft 365–powered Surface devices



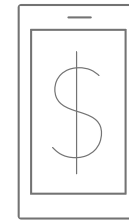
20%↓

reduction
in security breaches
for Surface users



17%↓

reduction
in endpoint security
spend



14%↓

reduction
in mobile device
management spend

Source: A commissioned Total Economic Impact™ study conducted by Forrester Consulting on behalf of Microsoft, July 2020. "Maximizing Your ROI from Microsoft 365 Enterprise With Microsoft Surface."



Surface Secure: the gold standard in endpoint security

- ✓ Windows Enhanced Hardware Security features enabled out of the box to protect against malicious code
- ✓ Complete Cloud-based device management and updates from OS to firmware to reduce IT complexity
- ✓ Security processor protections; BitLocker to secure & encrypt your data and Windows Hello for password-less login
- ✓ Microsoft written, open source UEFI (BIOS) to ensure authenticity of firmware and Windows 10

Microsoft Surface & Secured Core PCs

Different approaches but the same result: best-in-class endpoint security from Microsoft.



| | Surface Devices | Secured Core PCs |
|--|-----------------|------------------|
| Protect with hardware root of trust | ✓ | ✓ |
| Defend against firmware level attack | ✓ | ✓ |
| Prevent access to unverified code | ✓ | ✓ |
| Protect identities from external threats | ✓ | ✓ |

Microsoft Surface & Secured Core PCs

Different approaches but the same result: best-in-class endpoint security from Microsoft.

Protect with hardware root of trust



Surface's Root of Trust checks signatures and measurements at each stage to tightly ensure each stage is secure and authentic before allowing the next phase of boot to proceed.



Partnering with leading PC manufacturers and silicon vendors, secured-core PCs use industry standard hardware root of trust coupled with security capabilities built into today's modern CPUs.

Defend against firmware level attack



Microsoft builds its own firmware from the ground up, rather than relying on 3rd party source code. This allows Microsoft to continuously provides updates, down to the firmware level to protect against the latest threats.



Secured-core PCs use hardware rooted security in the modern CPU to launch the system into a trusted state, preventing advanced malware from tampering with the system and attacking at the firmware level.

Prevent access to unverified code



With Hypervisor Code Integrity (HVCI), Windows 10 devices are protected from running any unverified code. Code running within the trusted computing base runs with integrity and is not subject to exploits or attacks.

Protect identities from external threats



Protect Identities from external threats with Windows Hello². Credential Guard ensures that identity and domain credentials are isolated and protected in a secure environment.

Surface Devices

Secured Core PCs

Surface Security Specifications

| Security Feature | W10 O/S Feature | Surface + OEMs | Surface only | What does it mean? |
|--|-----------------|----------------|------------------|--|
| Custom Built UEFI | | | Yes ¹ | Replaces the standard basic input/output system (BIOS) with new features including faster startup and improved security. The Unified Extensible Firmware Interface (UEFI) — built by Microsoft without third-party involvement — ensures significantly more control over the hardware of a device and speedier react times. ¹ |
| DCFI (Device Firmware Configuration Interface) | | | Yes ² | Delivers cloud-scale remote firmware management with zero-touch device provisioning. Microsoft's own UEFI allows stronger DCFI implementation, enabling organizations to disable hardware elements and remotely lock UEFI using Intune. ¹ |
| Protected DMA Access | | | Yes | Mitigates potential security vulnerabilities associated with using removable SSDs or external storage devices. Newer Surface devices come with DMA Protection enabled by default. |
| Surface Data Eraser | | | Yes | Provides a bootable USB tool to securely wipe data from your Surface devices. |
| SEMM (Surface Enterprise Management Mode) | | | Yes | Enables centralized enterprise engagement of UEFI firmware settings across on-premises, hybrid, and cloud environments. ¹ |
| Removable SSD | | Yes | Yes ³ | Helps organizations protect their data and comply with data retention policies. |
| Physical TPM 2.0 | | Yes | | Uses a physical, discrete TPM 2.0 chip, implementing a secure and sandboxed environment for storing passwords, PIN numbers, and certificates. |
| BitLocker | Yes | Yes | Yes | Combined with physical TPM and UEFI, provides a significantly improved and integrated encryption solution. |

[1] Surface Go and Surface Go 2 use a third party UEFI and do not support DCFI. DCFI is currently available for Surface Laptop Go, Surface Book 3, Surface Laptop 3, Surface Pro 7, and Surface Pro X. [about managing Surface UEFI settings.](#)

[2] DCFI is currently available for Surface Laptop Go, Surface Book 3, Surface Laptop 3, Surface Pro 7, and Surface Pro X. [about managing Surface UEFI settings.](#)

[3] Removable SSD available on Surface Laptop 3, Surface Laptop Go, and Surface Pro X. Hard drive is only removable by skilled technicians following Microsoft instructions. Hard drive replacement may cause damage or safety risk and is not recommended.

Surface Security Specifications *(contd)*

| Security Feature | W10 O/S Feature | Surface + OEMs | Surface only | What does it mean? |
|--------------------------------------|-----------------|----------------|---------------|---|
| Windows Hello for Business | Yes | Yes | Yes | Replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN. |
| Secure Boot | Yes | Yes | Yes | Enabled by UEFI and TPM 2.0, ensures that only code signed, measured, and correctly implemented code can execute on a Surface device. |
| Microsoft Defender with Endpoint | Yes | Yes | Ships Enabled | Provides an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. |
| Windows Defender Credential Guard | Yes | Yes | Ships Enabled | Isolates and hardens key systems and user secrets, making an attack against user credentials much harder to perform. |
| Windows Defender Application Control | Yes | Yes | Ships Enabled | Hardens computers against malware and prevents malicious code. If code is not previously confirmed as secure, it cannot run. |

[1] Surface Go and Surface Go 2 use a third party UEFI and do not support DFCI. DFCI is currently available for Surface Laptop Go, Surface Book 3, Surface Laptop 3, Surface Pro 7, and Surface Pro X. [about managing Surface UEFI settings.](#)

[2] DFCI is currently available for Surface Laptop Go, Surface Book 3, Surface Laptop 3, Surface Pro 7, and Surface Pro X. [about managing Surface UEFI settings.](#)

[3] Removable SSD available on Surface Laptop 3, Surface Laptop Go, and Surface Pro X. Hard drive is only removable by skilled technicians following Microsoft instructions. Hard drive replacement may cause damage or safety risk and is not recommended.

Surface is secured chip-to-cloud

- **Secure from chip-level to cloud management**
 - Silicon, firmware, OS, and cloud service each play a role
- **Defense in depth**
- **Layering of independent defensive sub-components**

CHIP

to

CLOUD

- UEFI w/TPM 2.0
 - SEMM
 - Secure Boot
 - BitLocker
 - MDM UEFI Management
 - Windows Hello
- Advanced Windows Security Features
 - Conditional Access
 - Windows Update for Business
 - Microsoft Defender ATP
 - Intune Wipe and Retire



Securing boot

Security standard to boot only a trusted OS

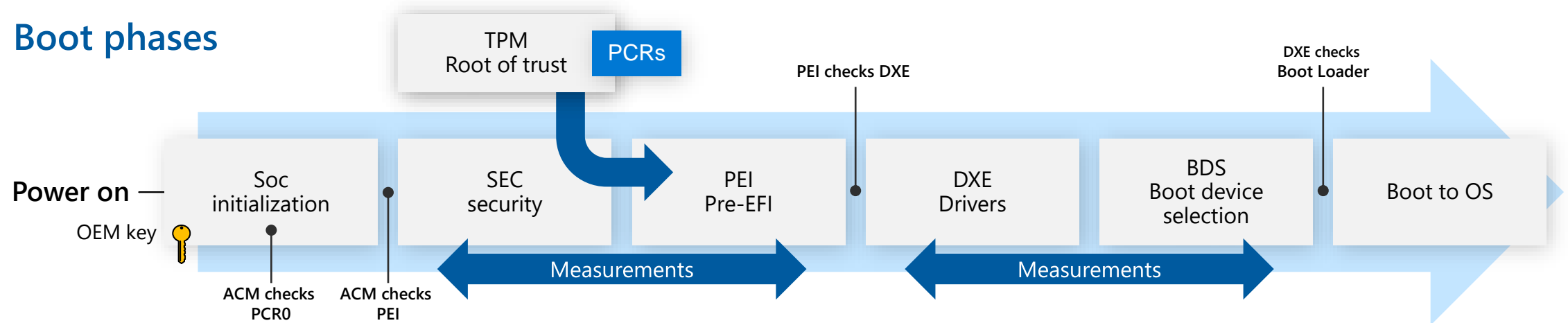
Trust chain

- Root of Trust anchored in HW
- Each stage checks the next
- Boot Guard, Secure Boot

Security components

- SoC security processor—vendor and OEM keys
- TPM 2.0—security processor
 - Crypto engine
 - Keys
 - Measurements
 - VMK (BitLocker)

Boot phases



Surface firmware

Firmware are built by Surface

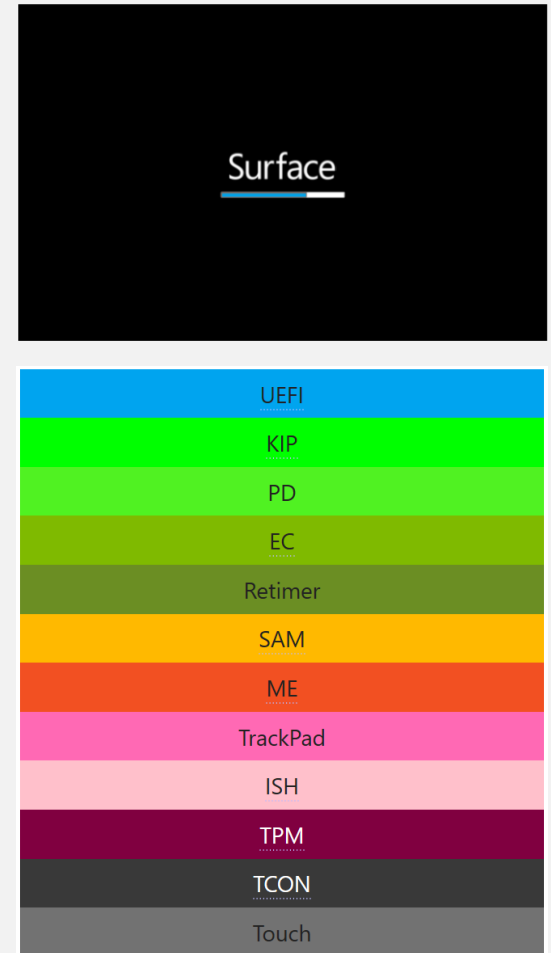
- Surface builds UEFI/controllers/sensors/SoC firmware
- Surface UEFI based from Windows' UEFI Project Mu open source
- Mitigation against supply chain attacks

A-B update mechanism

- Guard against corrupted updates

FW is kept current via Windows Update

- Windows signed drivers wrap Capsule Updates
- Surface signed capsule update
- UEFI applies FW update payload
- Color progress bar indicates which FW is updating



Surface Enterprise Management Mode

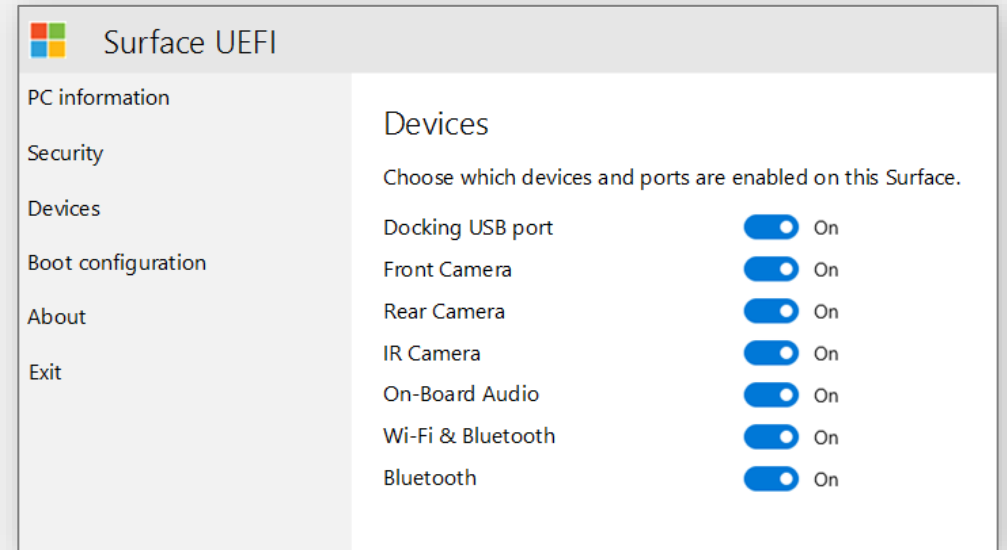
UEFI software tool for volume deployments

Secure and manage UEFI firmware configuration

Standalone tool or integration with SCCM

Manage individual components,
boot order and advanced settings

- Disable and lock devices (no drilling!)
- Lock out UEFI front pages



DFCI/Cloud UEFI Management

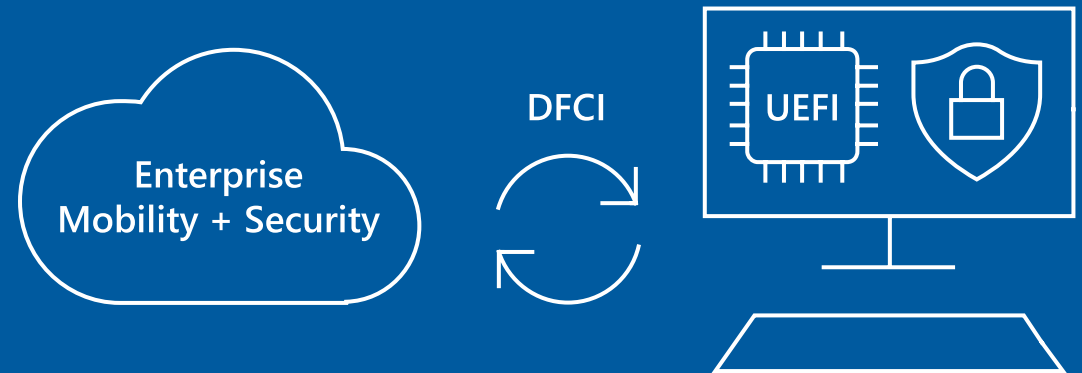
Capabilities of SEMM through Intune/MDM

Cloud-scale remote firmware management with zero-touch device provisioning

Eliminates BIOS passwords, provides control of security settings including boot options and built-in peripherals

Lays the groundwork for advanced security scenarios in the future

Implemented first on Surface



BitLocker

Drive encryption protecting data and OS

Automatic device encryption enabled during OOBЕ when:

- TPM is present
- Secure Boot enabled

Bitlocker Recovery

- When security and/or boot changes have been made

Removable SSD

- DMA remapping protection



Windows Hello for Business

Replaces passwords with strong two-factor authentication on Surface

Trusted authentication

- Facial recognition
- Finger recognition
- Strong on-device PIN

Paired with password or pin stored (encrypted) during OOB

Valid Biometric unlocks TPM key to access pin and allow login



Advanced Windows Security Features

Virtual Secure Mode (VSM)

- Virtualization Based Security (VBS), security enclave on hypervisor

Microsoft Defender Application Control

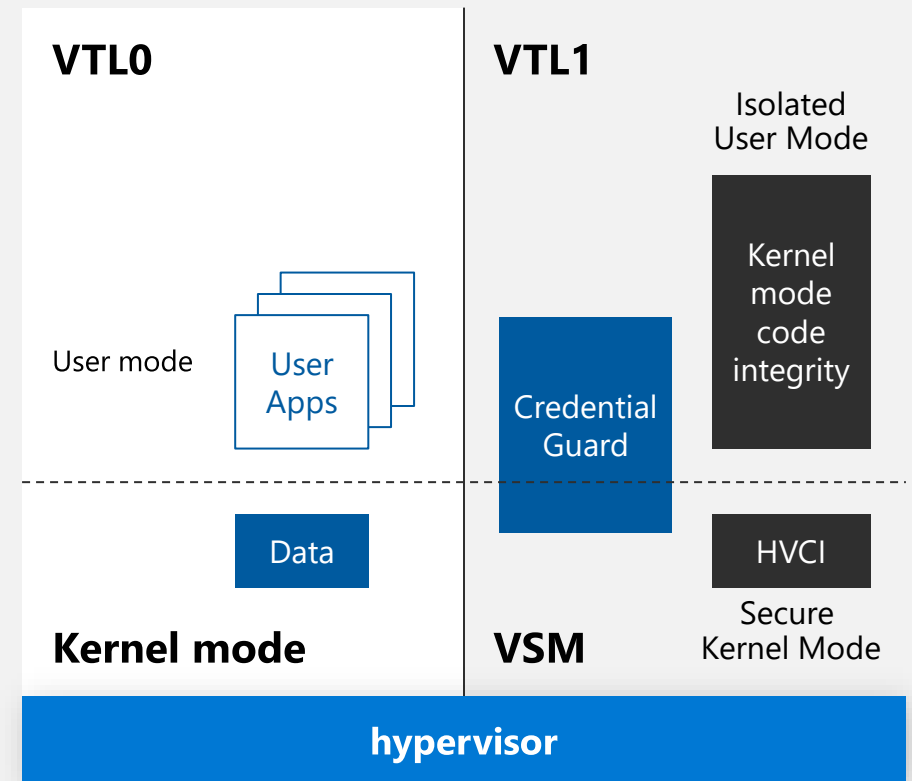
- Harden Surface against Malware

Credential Guard

- Isolate key system and user secrets

Hypervisor Code Integrity (HVCI)

- Protects drivers/apps against code modification
- Ensure Trustlets have valid cert



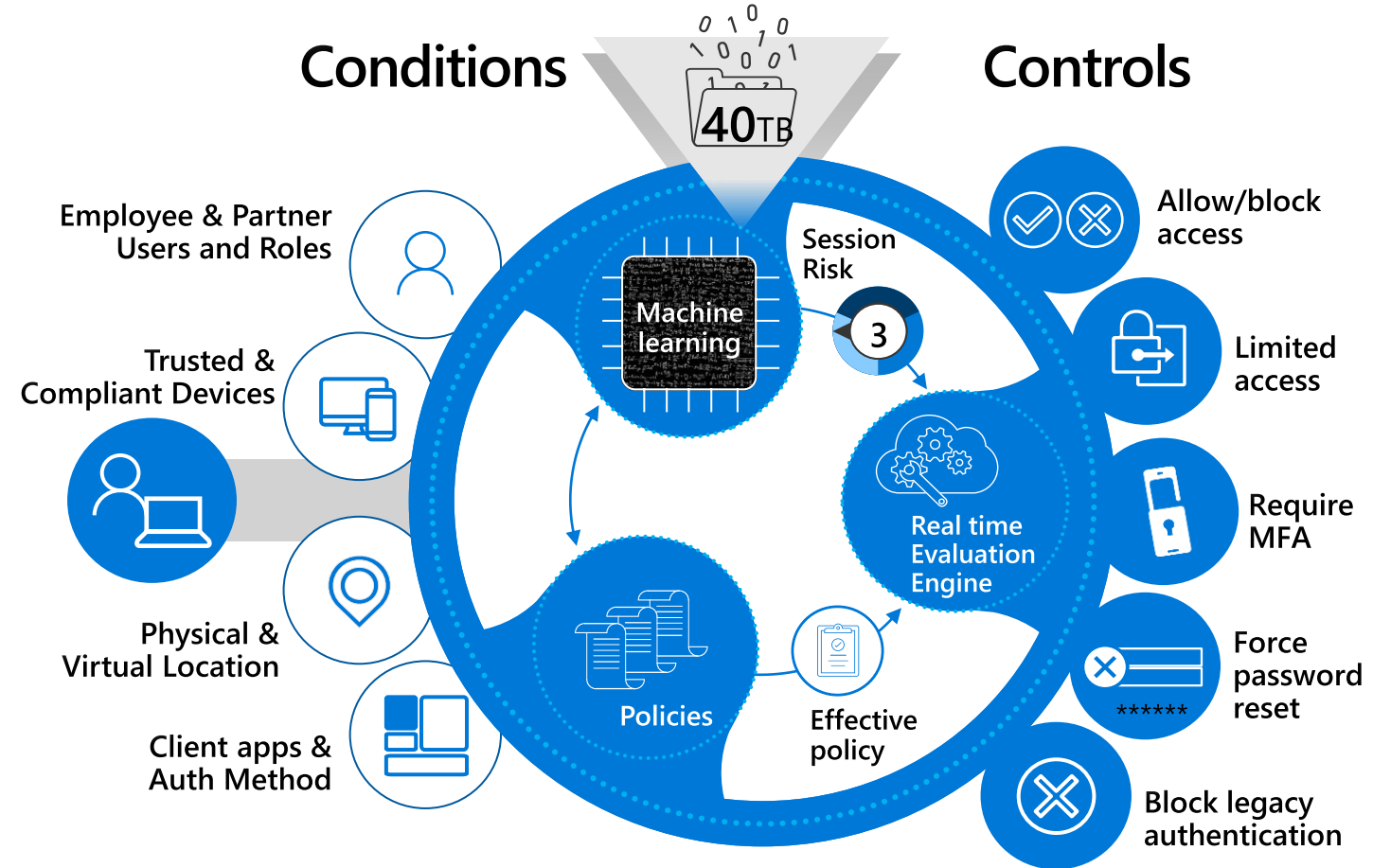
Conditional access

Control access and protect your Surface

Conditional access

- Intune managed policies
- Devices are granted access based on compliance
- Non-Compliant devices are blocked or automatically remediated

Geo-fencing, automated posture-changing and network-based firmware management... maybe!



Microsoft Defender 365

Detect, investigate, and respond to attacks

Agentless, cloud-powered

- Always up to date

Unparalleled optics

- Built into Windows 10 and exchanges data with Microsoft Intelligent Security Graph

Automated security

- Alert to remediation in minutes

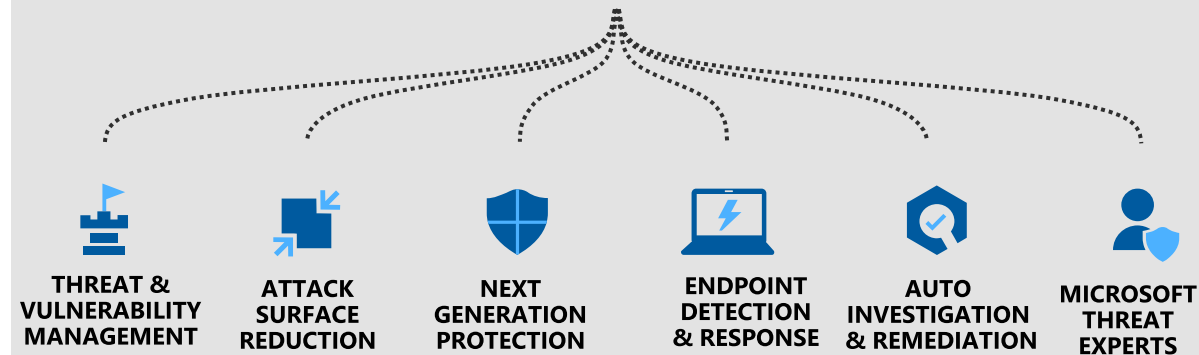
Synchronized defense

- Shared across Microsoft365, device/identity/data



Microsoft Defender ATP

Built-in. Cloud-powered.



Windows Update for Business

Always up to date with latest security defenses

Surface works closely with Windows to
push all updates through Windows Update

Integrates with Configuration Manager,
Intune and WSUS

Utilize deployment rings for testing

Reports via Windows Analytics



Surface Tools for Business

Further protect your Surface

Deployment

- Surface Enterprise Management Mode
- Surface Deployment Accelerator (Scripts: Open Source)

Management

- Surface Dock Firmware Updater (silent)
- Surface Brightness Control
- Surface Diagnostics toolkit for Business

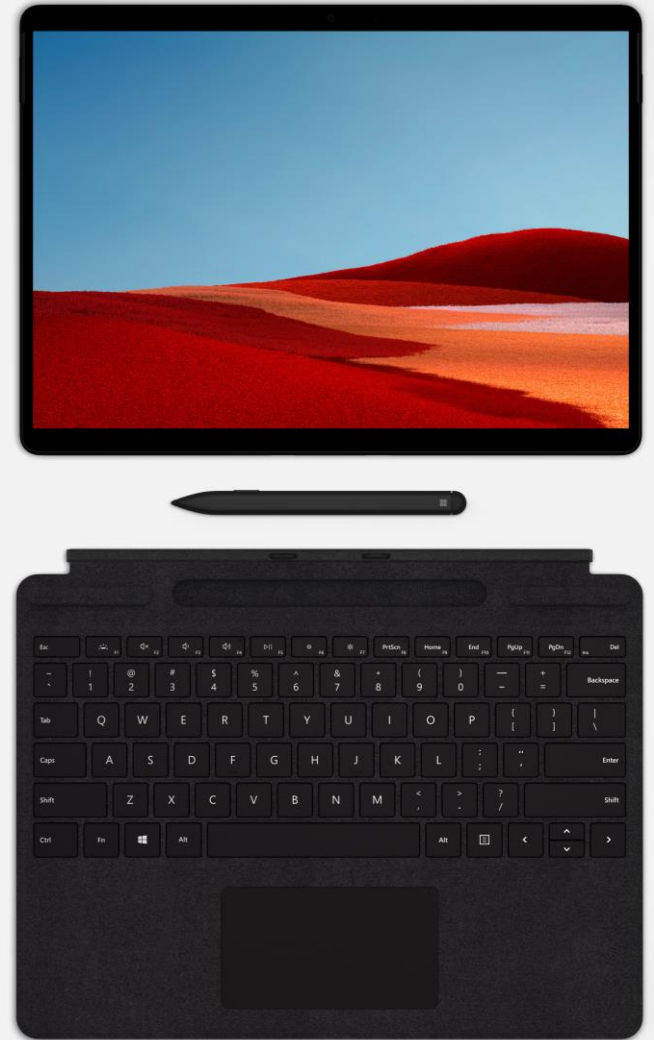
Retirement

- Surface Data Eraser

Download: aka.ms/SurfaceTools

Documentation: aka.ms/SurfaceToolsDocs

Videos: aka.ms/SurfaceToolsVideo



Key takeaways

Built from the ground up for best-in-class security

Surface is secured chip-to-cloud

- Providing best and first security innovations from Surface, Windows, and EMS
- Surface firmware tightly controlled by Microsoft
- Security stays current through automatic updates
- Enterprise management of devices securely through the cloud

CHIP

to

CLOUD

- UEFI w/TPM 2.0
 - SEMM
 - Secure Boot
 - BitLocker
 - MDM UEFI Management
 - Windows Hello
- Advanced Windows Security Features
 - Conditional Access
 - Windows Update for Business
 - Microsoft Defender ATP
 - Intune Wipe and Retire





Thank You