



User experience drives  
modern management  
at Microsoft

# What we'll cover today

- Migration to modern management approach
- Group policy to Mobile Device Management (MDM)
- New device experience
- Managing Windows updates
- What's next
- How Microsoft Surface helps with frictionless devices

# Technology needs are evolving in the modern workplace

## Modern IT

Single device



Multiple devices

Business owned



User and business owned

Corporate network and legacy apps



Cloud managed and  
software as a service (SaaS) apps

Manual



Automated

Reactive



Proactive

High-touch



Self-Service

# Microsoft Endpoint Manager

A cloud-enabled transformative platform for unified and secure endpoint management



  
Microsoft  
Endpoint  
Manager

## Unified admin console

Configuration Manager

Microsoft Intune

Desktop Analytics

Autopilot

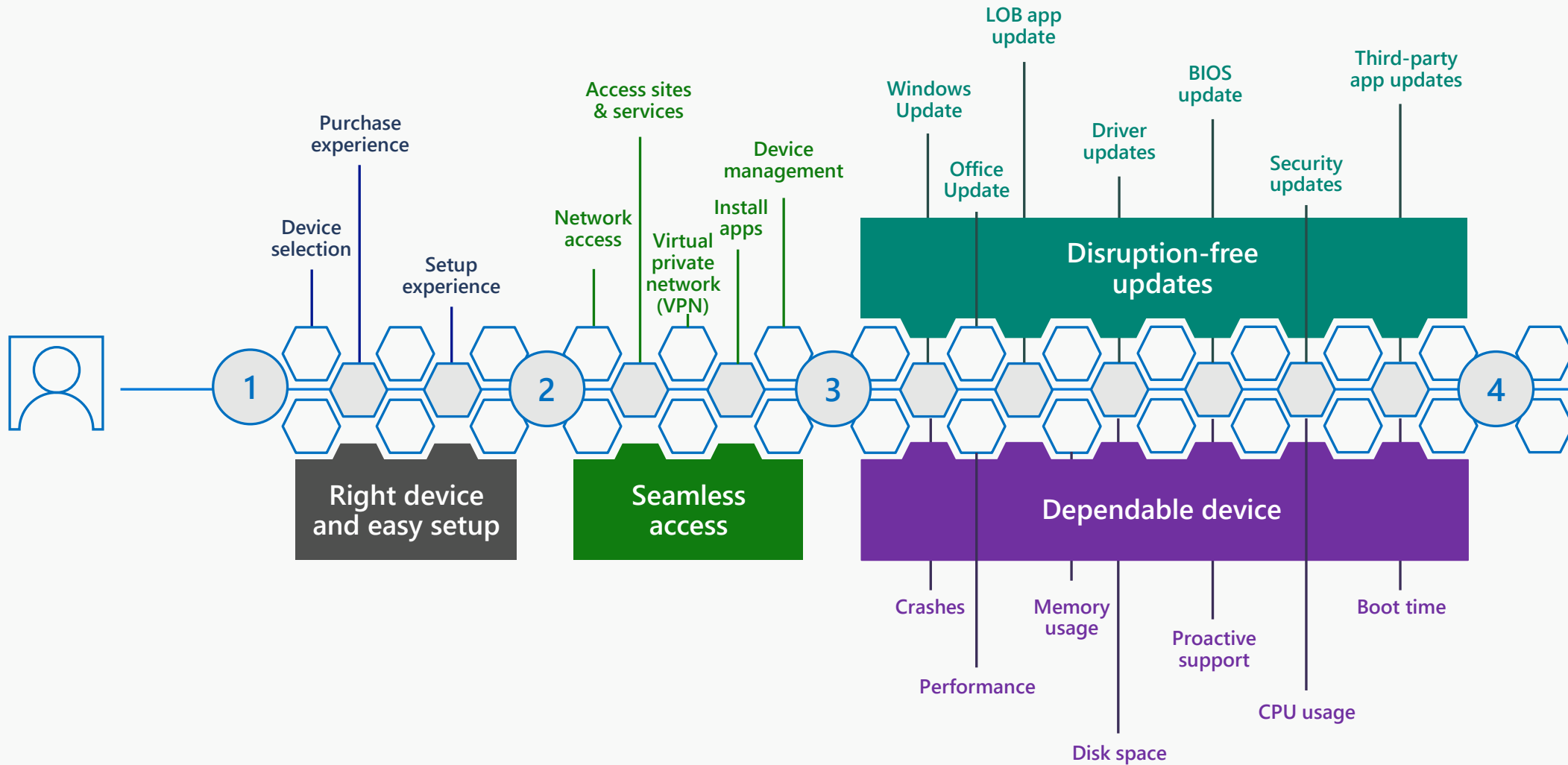
App protection policies

Endpoint analytics

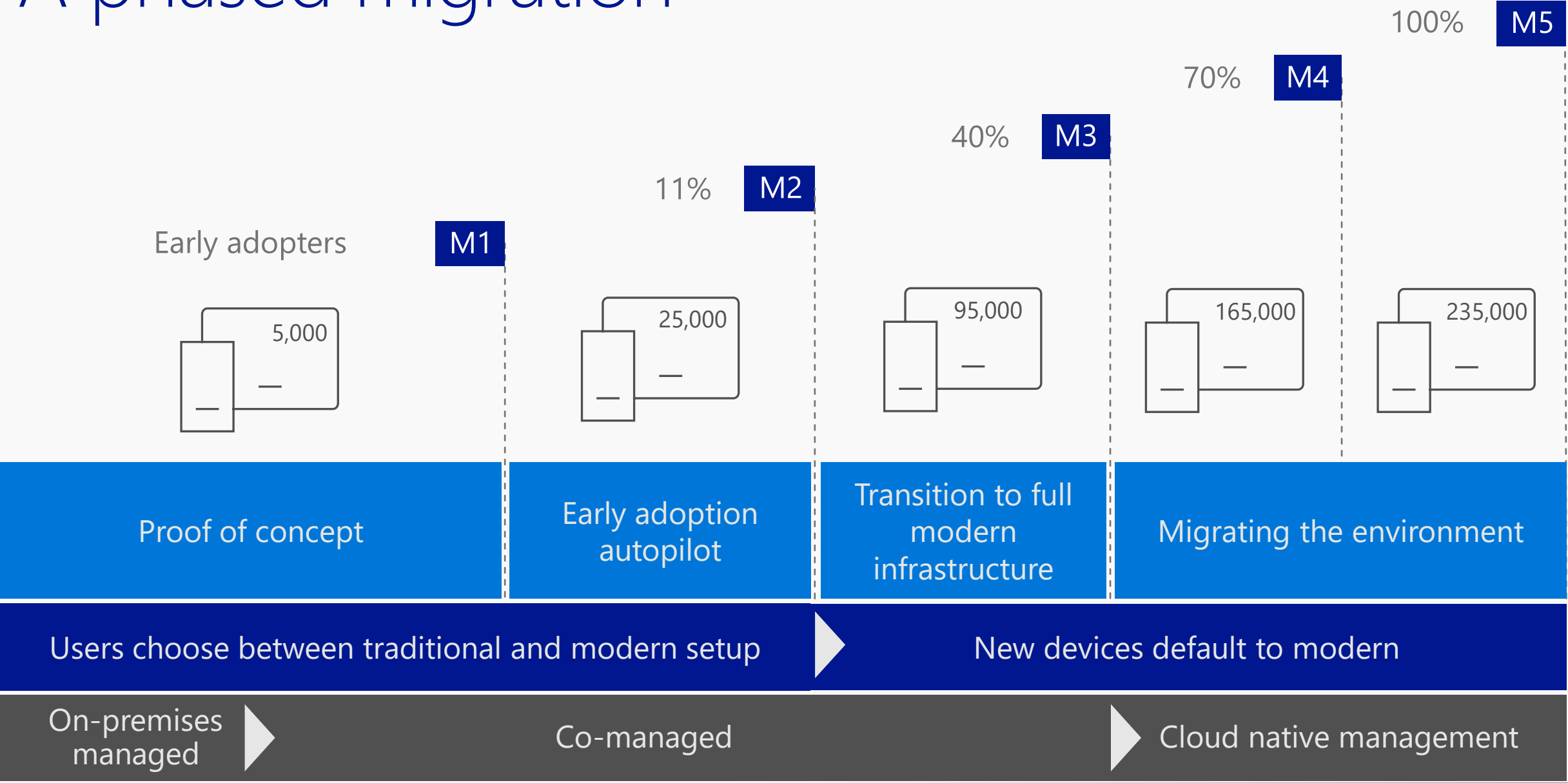
Endpoint security

Other Endpoint-management capabilities in Microsoft 365

# Journey map



# A phased migration




# Moving from group policy to MDM

## Background

- 8 Active Directory domains**
- 1 Organizational unit (OU) per domain with end-user devices**
- 3.5k Group policies across domains**

## Migration process

-  **Inventory group policies**
-  **1 Identify and prioritize required settings**
-  **Map group policies to MDM**
-  **Determine how to target MDM policies**
-  **Deploy MDM policies**

## Benefits

- Single policy solution for managing Windows, Mac, iOS, and Android devices.
- Microsoft Intune provides analytics and reporting on the application of policy.
- Simplified device management by only applying about 120 required settings.

## Lessons learned:

- Don't try and replicate exactly what was done with Group Policy. Take the opportunity to reevaluate and simplify.
- Use tools such as the MDM Migration Analysis Tool (MMAT) and Intune Policy Analytics to help accelerate the mapping process.
- Minimize the use of custom Uniform Resource Identifiers (URIs) to avoid tattooing settings on devices.
- Options for targeting MDM policies to users and devices are not as robust as Group Policy. Look for opportunities to flatten the management structure to reduce targeting complexity.
- Take a proof-of-concept, pilot, broad approach to deploying policies to minimize the impact if policies don't work as expected.

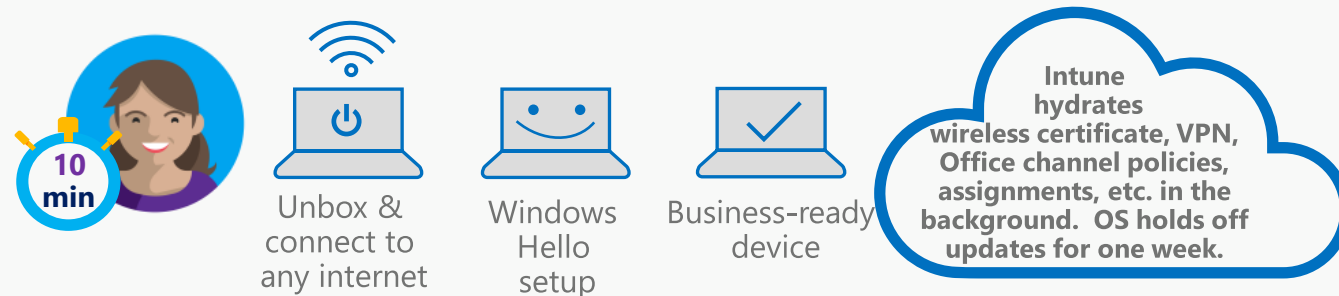
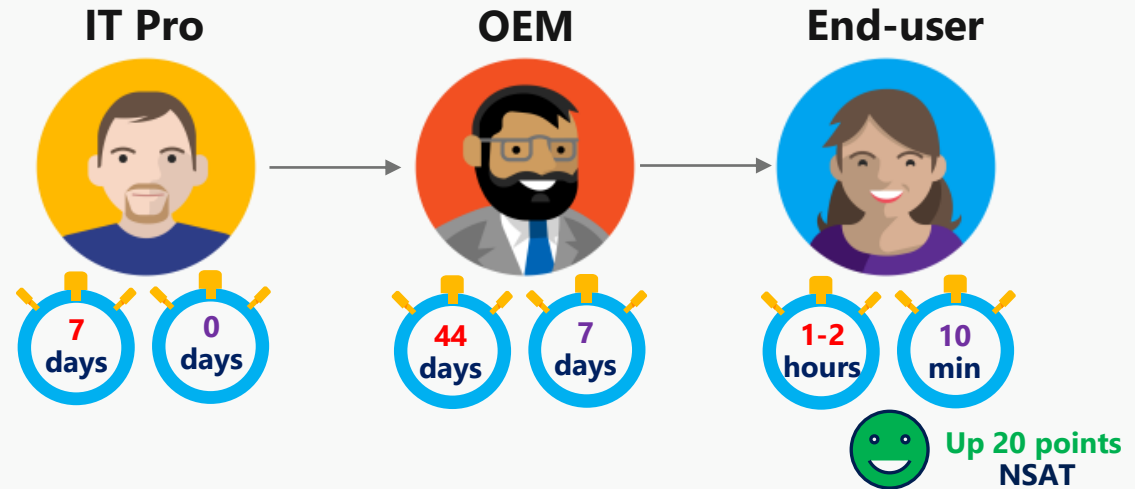
# New device setup experience

## Benefits:

- Set up devices from any internet network.
- Reduce end users' device setup time by 90%.
- Cloud-based and seamless provisioning of new devices.
- Users can access their desktop and start collaborating while certificates, policies, and apps are being silently provisioned on their new device.
- Device manufacturers own and manage the imaging process for enterprise customers.
- Device manufacturers factory process is optimized, resulting in fewer delays and faster shipments and deliveries.
- Autopilot profiles enable IT pros to define and target the setup experience for end users.
- IT pros can focus on data and reporting, maintain their infrastructure, and be more customer focused.

## Microsoft program results:

- **96%** of users experienced 10 minutes **or less** in setup time.
- Net satisfaction (NSAT) score is up **20 Points**.
- Savings of about **\$2 million dollars** in productively hours every year.





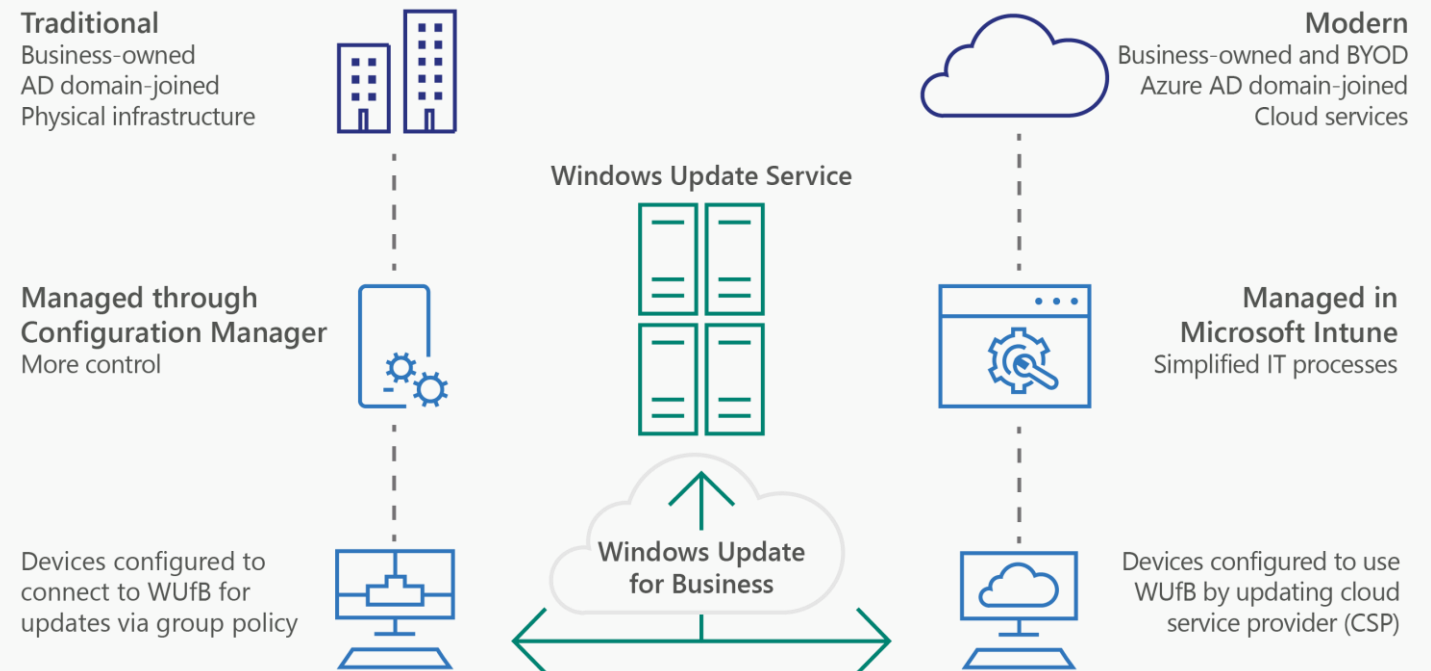
# Windows Update for Business migration

## Benefits:

- Eliminated packaging, replication, testing, and publishing associated with Microsoft System Center Configuration Manager operating system deployment (OSD), saving approximately 200 hours.
- Support for all OS languages and architectures, not just the ones CSEO officially supports.
- Windows Update user experience provides users more control over when updates are installed.
- Reduced bandwidth utilization using Delivery Optimization.
- Single deployment approach for AADJ and Active Directory devices.

## Lessons Learned:

- Compatibility blocks not available to devices using Windows Update for Business. (Fixed in Windows version 1903)
- Some users appreciate the auto-restart experience, but it can result in lost work. (Addressed with Windows version 1903 restart policies.)
- Need to set deferrals for both quality and feature updates. If one is missing, the assumed value is 0.



Case study: [Keeping Windows 10 devices up to date with Microsoft Intune and Windows Update for Business](#)

# IT initiatives toward modern management



**Remote users:** Enable remote users



**Wireless-first:** Disable wired ports



**Internet-first:** Remove corporate networks



**Zero trust:** Never trust, always verify



**Server retirements:** Move services to the cloud



**Co-manage:** Transition from classic to modern with Intune and ConfigMgr

## Modern management

The Enterprise IT infrastructure is cloud-based for identity and device management services





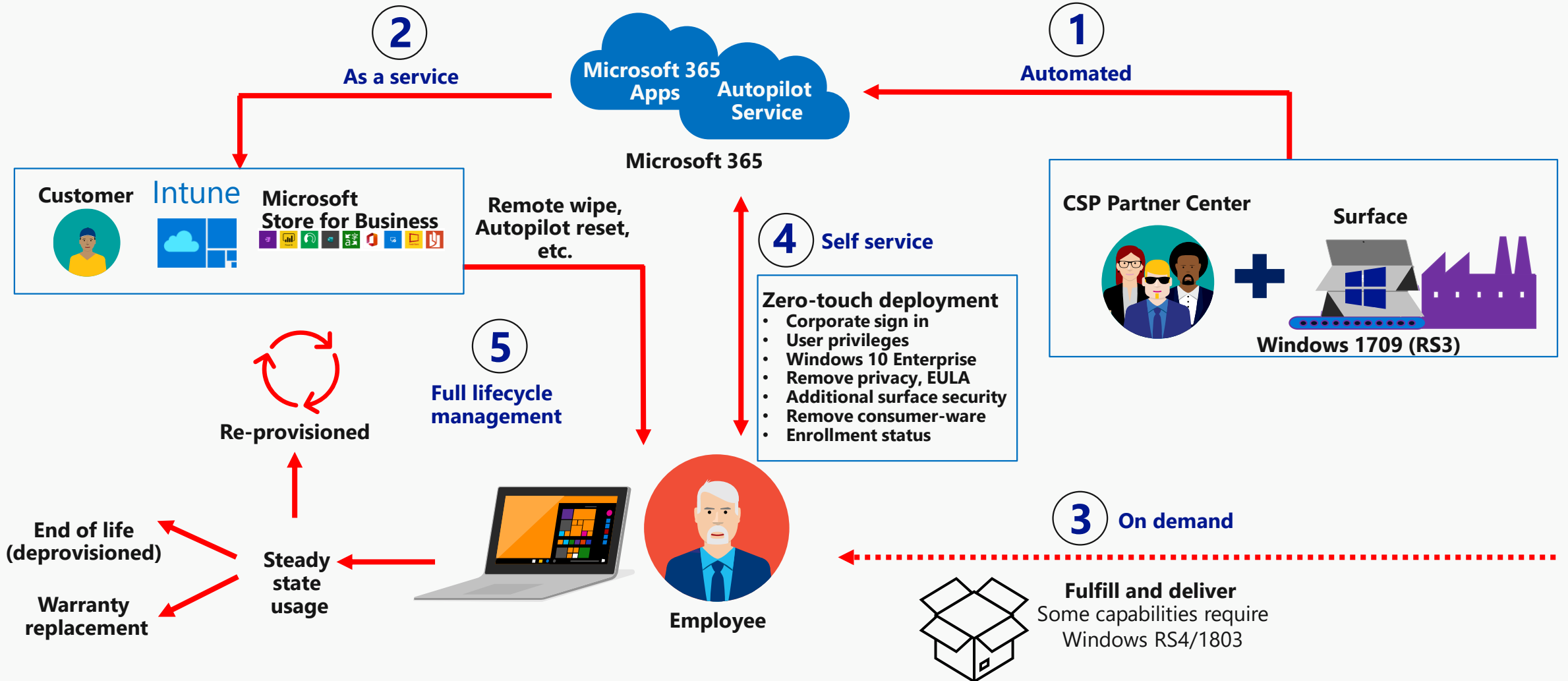
# How Microsoft Surface helps with frictionless devices: a modern management story

Max Sanders

Microsoft Surface Specialist



# Windows Autopilot with Surface: modern device lifecycle management



# Windows Autopilot on Surface

- End users are immediately productive with Surface
- Only OEM will automatically deregister/reregister returned devices
- Partner-channel enabled and ready
- Sales & Support operationalized, and free
- Commercial SKU is tuned for fastest Windows Autopilot experience with Office ProPlus, and a clean image



# Streamlined deployments

Zero-touch deployment through Autopilot

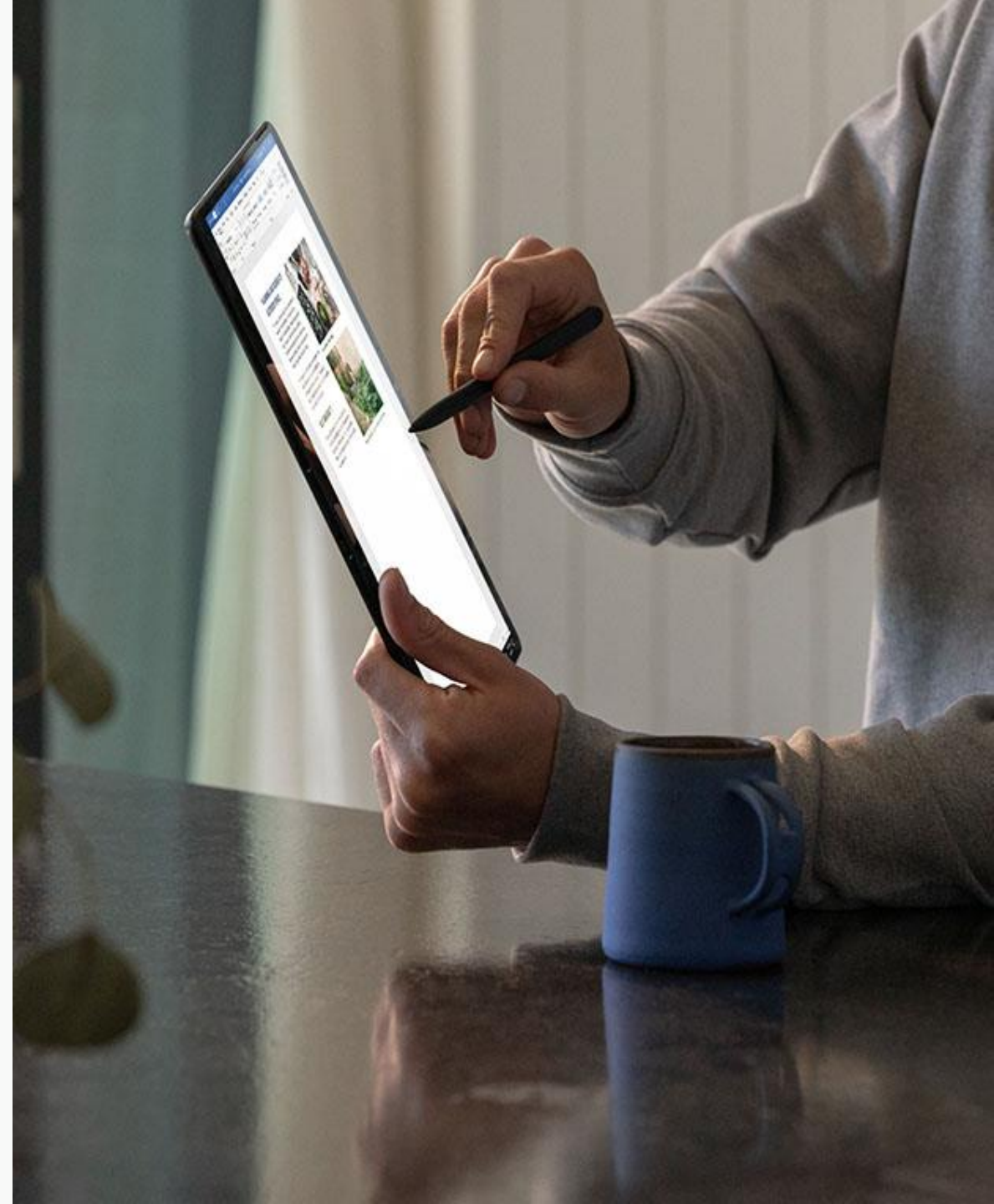
Partner expertise that reduces IT complexity

Lifecycle strategy to remotely replace and reuse

---

IT saves over **25 minutes** per device deployed<sup>1</sup>

**78%** agree they have reduced IT time and costs to deploy Surface devices vs. non-Surface devices<sup>1</sup>



# How far have we come?

## Windows Autopilot scenarios

Available in 1703

---

User-driven mode  
with Azure AD Join

Join device to  
Azure Active Directory  
(Azure AD), enroll  
in Intune/MDM

Available in 1809

---

Self-deploying mode

No need to provide  
credentials, automatically  
joins Azure AD

Available in 1809

---

Self-deploying mode

Join device to Azure AD,  
enroll in Intune/MDM

Available in 1809

---

Windows Autopilot  
for existing devices

Windows 7/8.1  
to Windows 10

ConfigMgr task  
sequence, followed  
by Windows Autopilot  
user-driven mode

New! Hybrid Azure  
AD Join support

Available in 1903

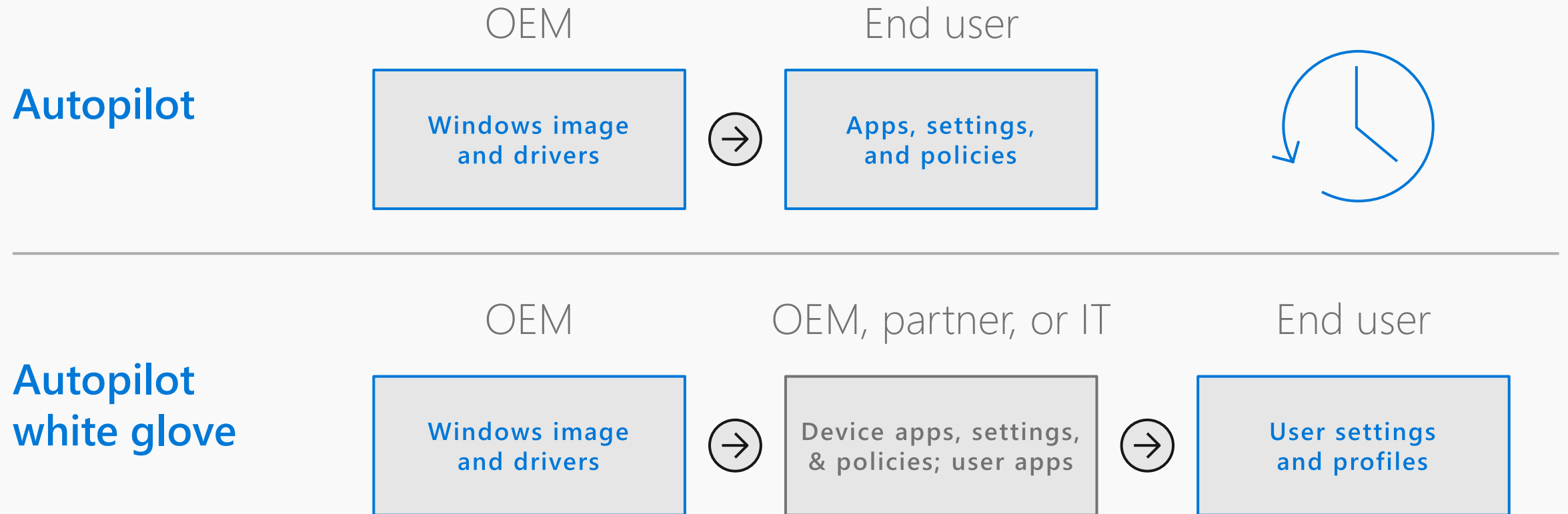
---

Windows Autopilot  
white glove deployment

White glove partners or IT  
staff can pre-provision  
Windows 10 devices to be  
fully configured and  
business-ready for an  
organization or user

# Windows Autopilot

White glove





# Modern management

Complete device management from Unified Extensible Firmware Interface (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 Surface<sup>1</sup>

**78%** agree that Surface reduced the IT time and labor to manage and update Microsoft 365<sup>1</sup>



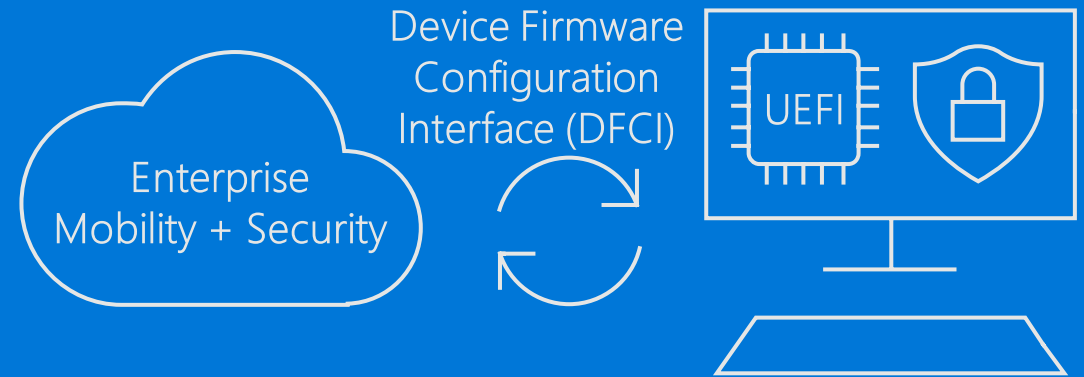
# Intune zero-touch UEFI management

IT can manage UEFI BIOS settings remotely without 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



# 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 cost<sup>1</sup>

**50%** reduction in annual security breach volume<sup>1</sup>

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



- Intune Wipe and Retire
- Windows Defender Advanced Threat Protection (ATP)
- Windows Update for Business
- Conditional Access
- Advanced Windows Security features
- Windows Hello for Business
- Intune UEFI management
- BitLocker Drive Encryption
- Secure boot
- SEMM
- UEFI with Trusted Platform Module (TPM) 2.0

# Tenant lockdown

Surface continues to implement Microsoft 365 technologies first and best

Tenant lockdown: Ensure device remains bound to owning tenant in case of accidental reset or theft/loss of the device

Reset can only occur 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

# Microsoft Surface for Business

Devices they love on the platform you trust



**Innovation that inspires**



**Designed for the future of work**



**Modern security & manageability  
from Microsoft**

# Microsoft IT Showcase

How Microsoft does IT

➔ Visit the website  
[microsoft.com/itshowcase](https://microsoft.com/itshowcase)





Placeholder name

Placeholder title

Core Services Engineering

office:

mobile:

[placeholder-email@microsoft.com](mailto:placeholder-email@microsoft.com)