

Modern Endpoint Management:

Why 'built in' is better than 'bolt on'

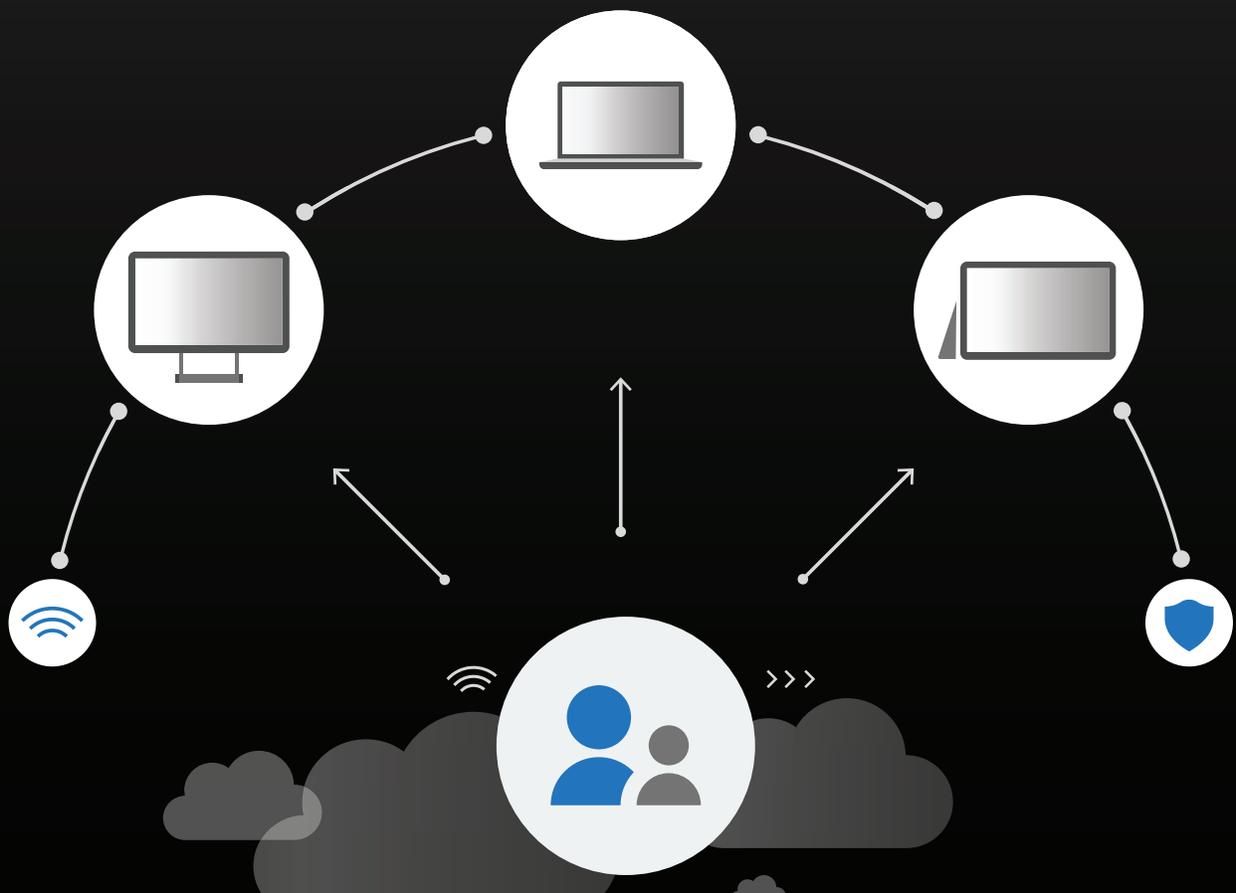


Table of contents

03

Introduction

05

**The modern
management model**

12

Making the transition

04

**The evolution of
mobile management**

08

**A modern desktop,
built for modern
management**

14

Conclusion

Introduction

Managing endpoint devices in today's enterprise is an increasingly complex—and often frustrating—activity. The modern workplace is defined by a diverse mix of desktops, laptops, tablets, and smartphones, spread across a wide variety of locations, used for many different purposes.

This complicated landscape has made it difficult for IT leaders to rein in burgeoning support costs and keep users current with the latest apps and functionality. Perhaps even more importantly, uneven management of endpoint devices increases security risk, because it's impossible to ensure that all devices are up to date with the latest patches and protection. IDG's [2019 Security Priorities Study](#) found that improving protection of confidential and sensitive data is the No. 1 priority for nearly 6 in 10 IT and security professionals. Protecting data ties directly to better device management.

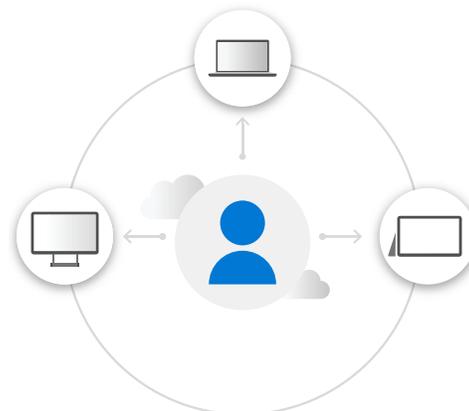
The traditional answer to this challenge—strict policies that limit access to corporate networks,

applications, and data—has given rise to another IT pain point: frustrated users.

Employees have grown accustomed to seamless access to information from their personal devices; they want the same seamless experience at work. IT teams are sympathetic:

In IDG's [2019 Digital Business Study](#), IT leaders said improving worker productivity is a critical component of digital transformation, and IT managers said improved employee productivity is the most important metric for measuring digital business success.

To address these ongoing challenges of the modern enterprise, **IT teams need a modern approach to device management, one that seamlessly integrates all components, from the chip to the cloud.**



The evolution of mobile management

Mobility management is a historical jumble of acronyms, from MDM (mobile device management) and MAM (mobile application management) to EMM (enterprise mobility management) and, more recently, UEM (unified endpoint management). These terms all share a primary goal: provide a comprehensive, yet streamlined, view across endpoint devices to help IT teams more effectively manage policies, applications, and updates.

The need for a more modern endpoint management approach, featuring streamlined policy enforcement, is driving the emergence of UEM. Analyst Jack Gold expects enterprises to embrace UEM to eliminate the overlap between mobile and PC management solutions.

“If you are not viewing endpoint management strategically, and not preparing for the next phase in capabilities, you risk putting your company on a path to reduced productivity, increased threat surface, and higher TCO,” Gold [writes in Computerworld](#).

The cloud plays a critical role in this transition to modern mobile management.



The full benefits of modern management come from wiping the slate clean with a pure form of cloud-based management. It's a built

in model, with tightly integrated functionality from silicon to cloud, versus simply bolting on a series of increasingly complex solutions.

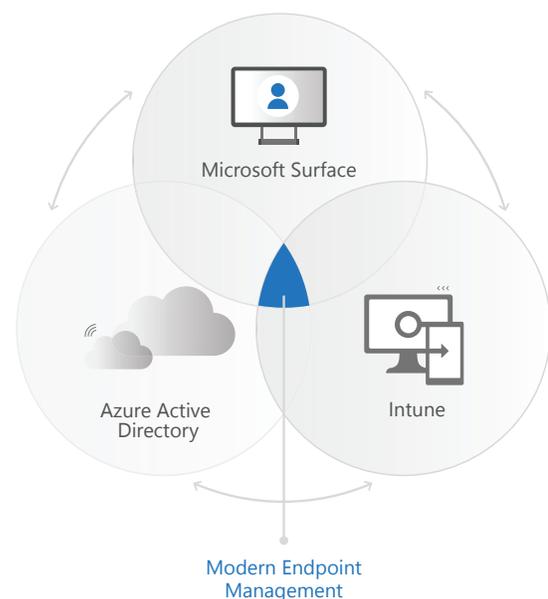
The modern management model

Traditional endpoint management assumes every device IT manages is owned by the organization and is connected to an on-premises network. Group policies lock down how each user operates the device assigned to them.

IT teams often struggle, however, to keep up with growing security threats and the increasing speed with which operating systems and applications change. As a result, they are frequently reactive—fixing problems—instead of proactively adding features and functionality that enhance the user experience instead of inhibiting it. IT may also be hamstrung by confusing or outdated policies that were instituted by previous management, further increasing overall IT complexity.

Users, for their part, are giving IT an earful about what many see as an overly restrictive approach. Today's workforce is accustomed to an established

smartphone/app ecosystem that provides a steady flow of new capabilities and their choice of easy, intuitive devices and apps. They want a seamless start-up experience when they receive a new device and more self-service options for customizing their experience. They also want the technology to adapt to their work style instead of being required to modify their own behavior. In other words, they want the technology to fade into the background while they go about their day.



Microsoft helps IT teams address these challenges through a modern endpoint management approach that leverages three core components: Azure Active Directory, Intune, and Microsoft Surface.

Azure Active Directory

Azure Active Directory helps administrators assign and manage application privileges via existing groups in Active Directory. It includes features such as Conditional Access, which protects services in multiple ways, including multifactor authentication, and can include policies to take appropriate mitigation or remediation actions automatically when a user or sign-in is flagged as risky.

Intune

Intune is the platform for managing Surface and many other modern endpoints, including employee-owned devices. Intune integrates with Azure Active Directory for identity and access control, and Azure Information Protection for data protection. Intune, combined with Windows 10's System

Center Configuration Manager (SCCM), makes it easier for IT administrators to set policies for controlling access to specific apps without controlling the entire physical device. Intune also allows for self-service capabilities, ensuring that users can easily access the apps they need while reducing the burden on IT.

Microsoft Surface

Microsoft Surface devices are designed for modern management, providing the optimal balance of productivity and security while also lowering TCO. A recent Forrester Consulting study found that Surface increased the ROI of Microsoft 365 investments and provided several other benefits, including:

- ✓ Boosting employee productivity.
- ✓ Enhancing workforce creativity and teamwork.
- ✓ Reducing costs and improving IT manageability.
- ✓ Improving security and compliance.

Modern Management: Maximizing ROI

How much do Surface devices add to the business benefit of Microsoft 365? Quite a bit, according to a Forrester Consulting Total Economic Impact™ (TEI) study. The study examined the potential ROI enterprises may realize by implementing Microsoft 365 Enterprise on Microsoft Surface devices. Among the findings, as demonstrated by a 1,500-user composite organization Forrester built for the study:

Security breach remediation costs decreased by 80 percent and the number of annual breaches decreased by 50 percent. Using two-factor authentication, Advanced Threat Analytics, and Surface Enterprise Management Mode (SEMM), the composite organization reduced breach remediation costs by a risk-adjusted present value (PV) of nearly \$1 million over a three-year analysis.

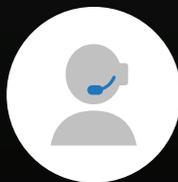
A reduction in several third-party technology costs, devices, infrastructure, and IT support requirements. A wide variety of third-party technology, device, and support

costs were reduced or eliminated using Microsoft 365-powered Surface devices, saving the organization a PV of over \$1.9 million over three years.

Help desk calls for password resets decreased by over 86 percent, while device and application performance-related tickets decreased by 15 percent. The stability of Surface resulted in fewer incidents of crashing and nearly eliminated the number of password-reset help desk tickets from Microsoft 365-powered Surface device users. The total risk-adjusted PV over three years surpassed \$150,000. three years surpassed \$150,000.



Security



Help desk



Costs

Source: Maximizing Your ROI From Microsoft 365 Enterprise With Microsoft Surface

A modern desktop, built for modern management

Surface has been designed with built-in support for simplified modern management of the entire device lifecycle: **before it's deployed, during it's use, and after it's returned to be redeployed or retired.**

Before

Microsoft thinks about Surface management before customers even receive the device. Setting up the device before it has been deployed significantly reduces the IT burden.

A Microsoft Cloud Solution Provider (CSP) will enroll a new device via its serial number into the customer's Azure Active Directory environment. This allows for the creation of device profiles (e.g., applications, policies, and settings) before the device is sent to the customer. A customer can create profiles for different groups (e.g., engineering, marketing, or HR) so that all of the proper settings and applications are available to the user the first time they turn on the device, via Windows Autopilot, with no unnecessary or unwanted bloatware.

Windows Autopilot leverages the OEM-optimized version of Windows 10

that is preinstalled on a device, saving organizations from having to maintain custom images and drivers for every model being used. Instead of reimaging the device, an existing Windows 10 installation can be transformed into a business-ready state, applying settings and policies, installing apps, and even changing the edition of Windows 10 being used (e.g., from Windows 10 Pro to Windows 10 Enterprise) to support advanced features.



During

Microsoft Surface contains sophisticated, mature hardware and firmware designed for comprehensive management, empowering administrators to control even the lowest level of hardware settings without having to touch the machine.

By comparison, managing firmware settings on previous generations of devices was quite difficult. Any configuration and management option involved custom or third-party software, known as a UEFI (Unified Extensible Firmware Interface), provided by the manufacturer. Surface, by comparison, includes a Microsoft-created UEFI, which enables automatic updating of both the operating system and the UEFI/firmware in one action. This approach not only provides streamlined administration, but also greater security.

Managing UEFI firmware settings is done via the Device Firmware Configuration Interface (DFCI), a component of Intune, and an open-source standard Surface

UEFI from Microsoft's Project Mu. With DFCI, Intune asks the Autopilot service to confirm a given customer trying to manage the firmware is the actual owner of the device. After Autopilot confirms the owner, Intune then applies the appropriate settings with no user interaction. On Surface devices, IT admins can also use Surface Enterprise Management Mode (SEMM) to manage the device at the boot level with custom firmware controls. Using SEMM, Intune enables direct management of many Surface device settings, including:

-  Certificates
-  Update settings
-  Bitlocker
-  Device features
-  Email
-  VPN connections
-  Windows security baselines
-  Wi-fi connections

Every Surface component, from firmware to Windows 10 policy settings, can be managed by Intune and updated via Windows Update for Business.

Surface also integrates into the Microsoft 365 security stack to detect vulnerabilities across the globe and automatically protect devices—even while they're asleep. Surface devices implement a Modern Standby low-power state that allows the device to appear asleep, drawing very little power, but also listening for updates via Windows Update for Business and application data streams like email. This allows a Surface on battery power to achieve a long standby battery life while also staying up-to-date on application data, and automatic pushes of security updates even down to the UEFI.

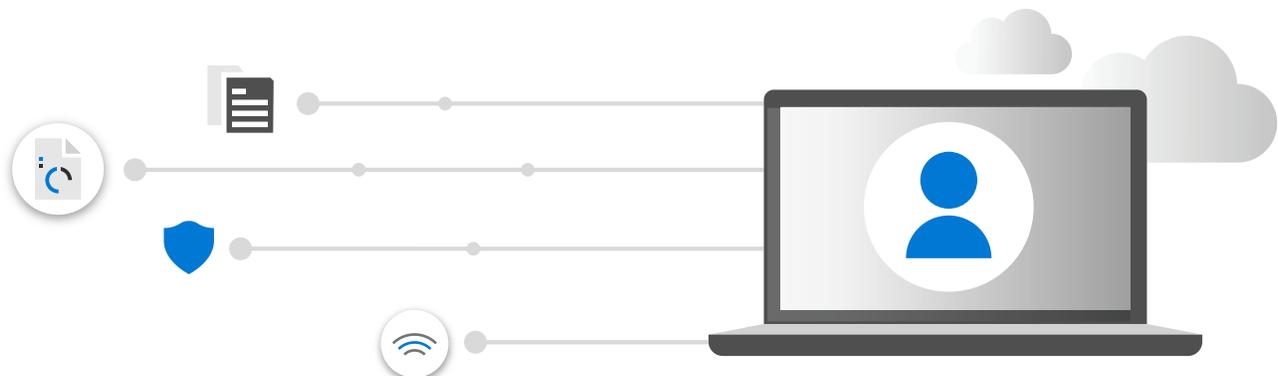
In addition, **Surface includes purpose-built tools for diagnostics and tuning that can automatically fix**

issues, assist with troubleshooting, and optimize functionality from brightness control to battery usage.

The Surface Diagnostic Toolkit for Business (SDT), for example, enables IT administrators to quickly investigate, troubleshoot, and resolve hardware, software, and firmware issues with Surface devices.

Surface devices are tuned to provide the perfect balance between battery life and performance. Windows Power Management mode on Surface is the result of significant research in processor heat and performance measured against the need for all-day battery life.

Finally, integration among Intune, Surface, and Microsoft 365 lets administrators configure custom suites of Office 365 apps, choose how and when those apps are updated, and even decide which apps are mandatory.



During

Endpoint management should extend to when a device is returned to IT to be redeployed or retired, or is lost or stolen. This end-of-life management gives administrators piece of mind that settings and other data on the device won't be exposed to unauthorized users.

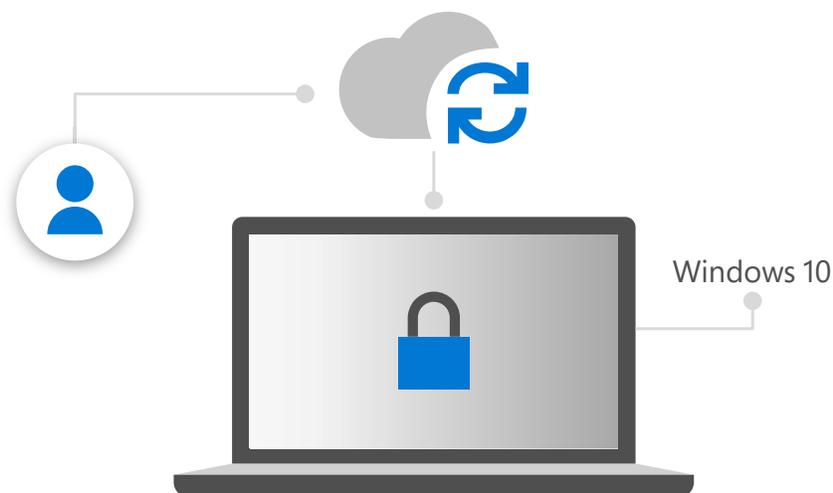
Using Intune, an IT administrator can remotely lock a device, reset passcodes, or wipe the device completely—

protecting data in the event that a device is lost or stolen. After a wipe, the device is reset to the out-of-box experience, at which point proper credentials are once more required for setup.

In addition, using the Fresh Start option in Windows 10, an administrator can remove all applications and install the latest version of Windows.

When an employee leaves the company, IT can reprovision the device remotely via Intune without the need to return the device to a central IT location. The device does not have to be shipped back to be reimaged.

IT can also manage the deprovisioning of remote devices via the Azure Active Directory portal for devices that have been retired or destroyed.



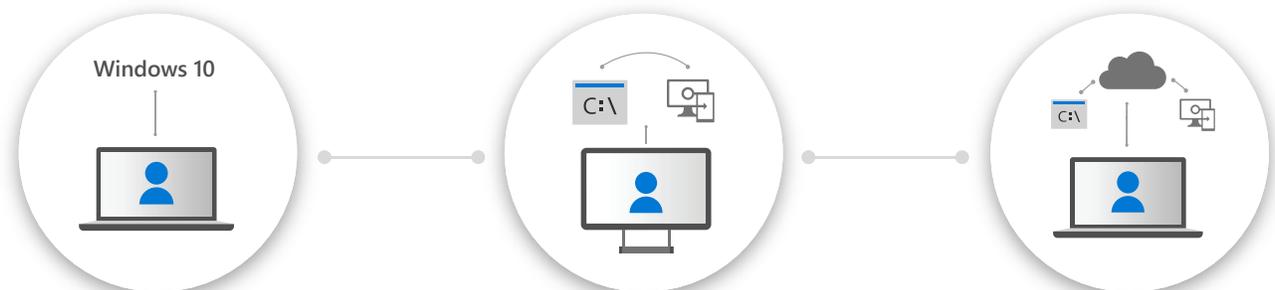
Making the transition

Making the change to modern management isn't always easy. IT teams have already invested time and resources into their infrastructure. Unfortunately, legacy IT processes and hardware continue to be the biggest roadblocks to transitioning to modern management.

Surface makes the transition easier, because it can address IT needs regardless of where the organization is in its modernization journey:

Traditional on-premises management:

On-premises device management provides a lighter-touch approach, using SCCM to manage devices. This option relies on the device management capabilities built into Windows 10 and is not as full-featured as client-based management. On-premises device management requires a Microsoft Intune subscription, which is used solely to track licensing of the devices; Intune is not used to manage or store management information. All management data is stored at your organization using the on-premises Configuration Manager infrastructure.



Hybrid/co-management: Co-management enables IT admins to concurrently manage Surface devices by using both SCCM and Intune. Creating a bridge between Active Directory and Azure Active Directory allows administrators to unlock new cloud-based functionality, such as conditional access.

Co-management provides flexibility to use the technology solution that works best for your organization. IT controls which workloads, if any, to switch from SCCM to Intune. Enrolling existing SCCM clients in co-management provides several immediate benefits:

- ✓ Conditional Access with device compliance.
- ✓ Support for Intune-based remote actions, such as restart, remote control, or factory reset.
- ✓ Centralized visibility of device health.
- ✓ The ability to connect users, devices, and apps with Azure Active Directory.
- ✓ Modern provisioning with Autopilot.

Full cloud-based management: Intune provides a highly scalable, integrated endpoint-management platform that leverages the cloud to help IT teams streamline and automate deployment, provisioning, policy management, app delivery, and updates. A global distributed cloud architecture ensures devices are always up to date, and Intune's app protection policies enable granular control over Microsoft 365 data on endpoint devices. Other benefits of the Intune experience in the Azure portal include:

- ✓ An integrated console for all enterprise mobility and security components.
- ✓ An HTML-based console built on web standards.
- ✓ Microsoft Graph API support to automate many actions.
- ✓ Access to Azure Active Directory groups to provide compatibility across all Azure applications.
- ✓ Support for most modern web browsers.

Conclusion

IT teams face many challenges as businesses become more digital. Managing endpoint devices using outdated tools or processes makes it difficult to keep devices and data safe and users productive and happy. The bolt-on method to endpoint management is no longer sufficient for the modern workplace.

Microsoft has built many innovative management features into Windows 10, but if your device manufacturer doesn't embrace modern management and take advantage of these capabilities, you can't realize the full potential of modern endpoint management.

Microsoft Surface for Business devices offer modern hardware and software that is built to take advantage of the management capabilities of Windows 10.

Every Surface component, from firmware to Windows 10 policy settings, can be managed by Intune and updated via Windows Update for Business. Surface integrates into the Microsoft 365 security stack to detect vulnerabilities across the globe and automatically protect your devices—even while they're asleep. Surface tools can automatically fix issues, assist you with troubleshooting, and optimize functionality from brightness control to battery usage.

To ensure a seamless integration into your business, find Microsoft Surface resellers that can help you deploy and manage Surface devices and software.

[Request a call](#)

