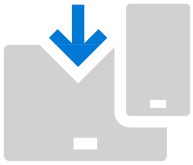
Microsoft Surface

Three ways you can modernise device IT and improve productivity

Table of contents



The business case for modern devices

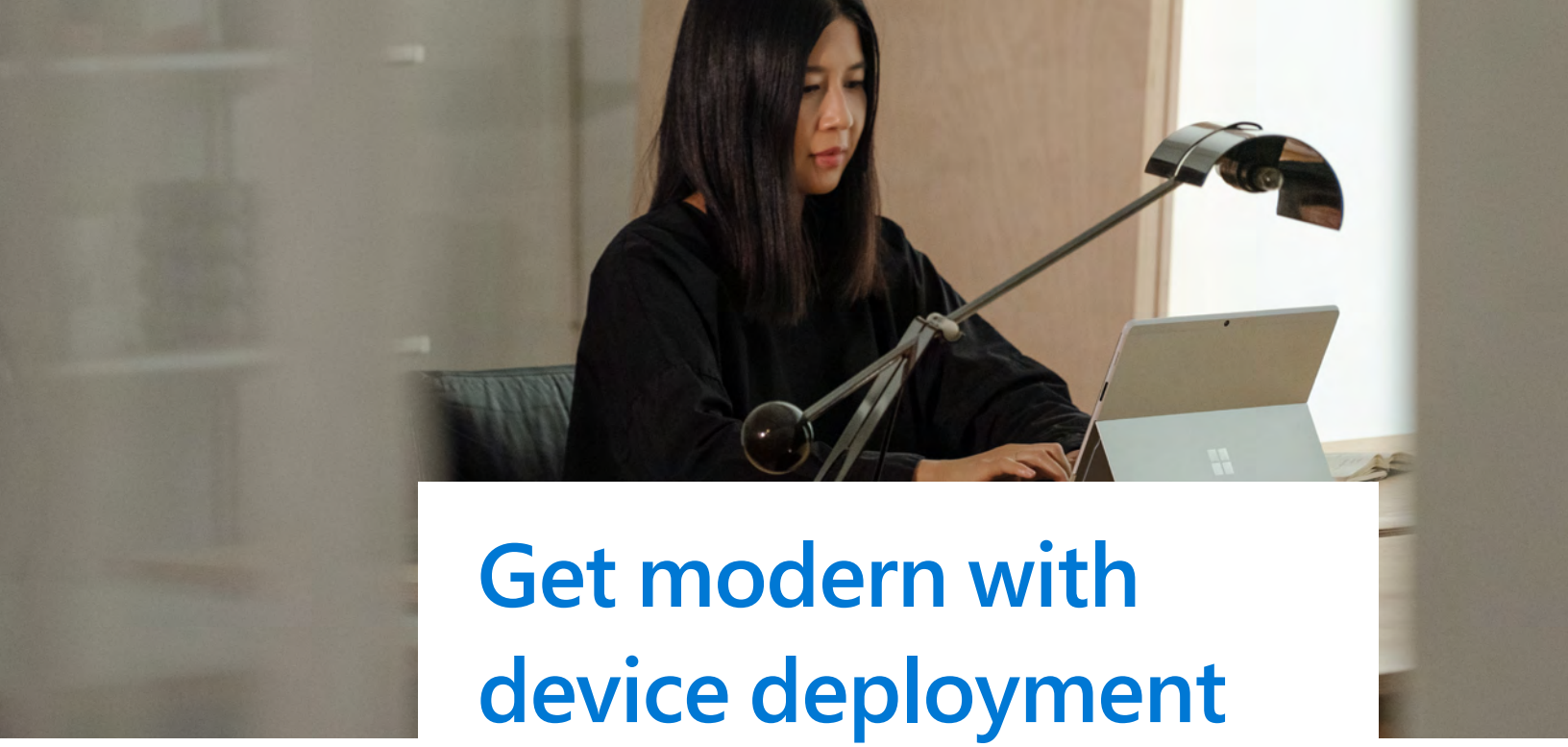
Devices that are easier to deploy, manage and protect can reduce IT costs while making employees more productive, because their devices perform better and are always up to date.

IT staff using Microsoft 365 say that Surface devices can save configuration and deployment time. “We used to spend the better part of a workday getting new devices ready for our end users. With Surface, the end user gets the device immediately and sets it up in 10 to 15 minutes,” said a VP and CISO at an HR services company.[1]

Improvements in device management also free up IT resources. Forrester Consulting found that with adopting Microsoft 365 and Surface, application updates required approximately 3.25 hours less to complete per device, while help desk call times decreased on average by 75%.[1]

Security is a rising cost for most organisations, but Microsoft 365 and Surface can help. “We have seen a 30% to 40% reduction in security incidents needing a person dispatched thanks to using Surface devices with Microsoft 365 E5,” said a CTO at a professional services company.[1]

While the benefits may be obvious, it’s important to make sure that the modern devices you’re considering perform across three key areas: **deployment, management and security.**



Get modern with device deployment

Configuring endpoint devices with the proper applications, profiles and security settings for every employee places heavy demands on IT staff, often driving up total cost of ownership (TCO). Delays and disruptions associated with device configurations and deployments can be equally frustrating to employees who just want to start using their new devices.

Microsoft has pioneered a 'zero-touch' deployment approach with Surface and Windows. Services such as Windows Autopilot and Microsoft Intune use automated provisioning and self-service options to give users a secure, productive experience without the IT team ever touching the computer.

- **Windows Autopilot** lets you set up and preconfigure Windows 10 devices with deployment profiles and application settings for different groups and departments. Deployment polices are applied automatically when the employee powers up the device for the first time. Software, including custom apps, can be pre-installed ahead of delivery.

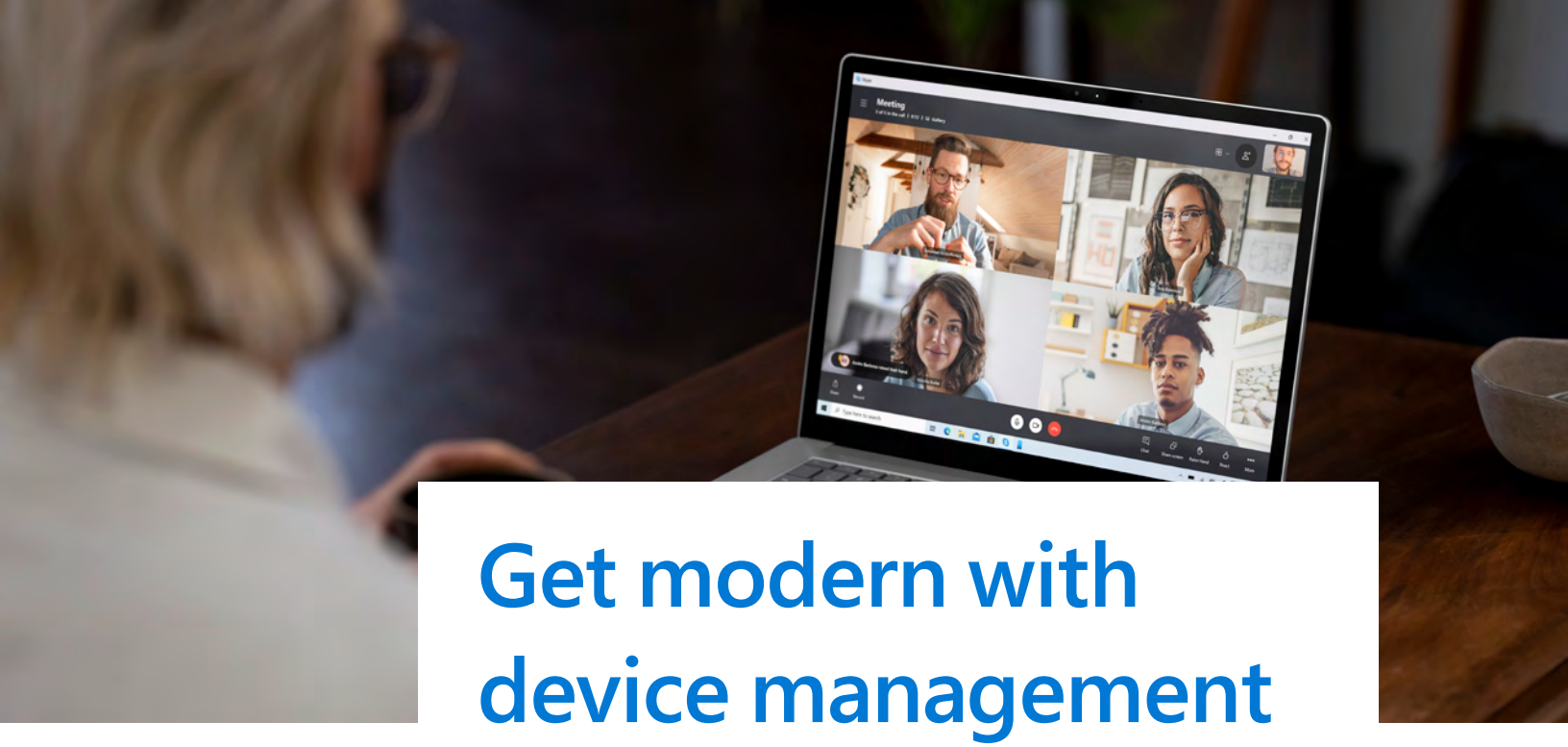
- By signing in with their **Active Directory or Azure AD identity** (which can be verified with multi-factor authentication), the user sees a custom version of the Windows set-up experience that can bypass the EULA, create the computer name or even change the Windows edition automatically, so users can get straight to work.

- **Pre-configured deployment** policies also apply security settings and authentication options such as Windows Hello. In addition, the device can include use policies for activities such as setting up department printers or controlling which websites require extra security through Windows Defender Application Guard.

This automated, self-service approach reduces the time to get a new device up and running from hours to minutes. That's a win-win for IT and users alike.

Looking for more?

Protect your business with Microsoft security and Surface



Get modern with device management

Ongoing management of a large PC estate has long been a pain point for IT, consuming budget and resources just to keep everything current while leaving little time for improvements or innovation. Advances in unified endpoint management tools have relieved some of the strain, but the practice and software have their limits.

Chip-to-cloud security shifts the management emphasis from locking down devices to keeping them up-to-date and functioning at full performance. The same verified identity that enables zero-touch deployment allows secure remote management of every Surface component, from firmware to Windows 10 policy settings, through Intune and Windows Update for Business.

This integration helps IT manage the entire device lifecycle: before the device is deployed, during its use and after it's returned to be redeployed or retired.

- Using **hybrid co-management** that combines Microsoft's cloud-based Intune service with the familiar System Centre Configuration Manager in the new Microsoft Endpoint Manager, IT can easily apply system updates (including anti-malware) and policy updates (including certificates, BitLocker, email, application whitelisting, VPN connections and more) automatically.

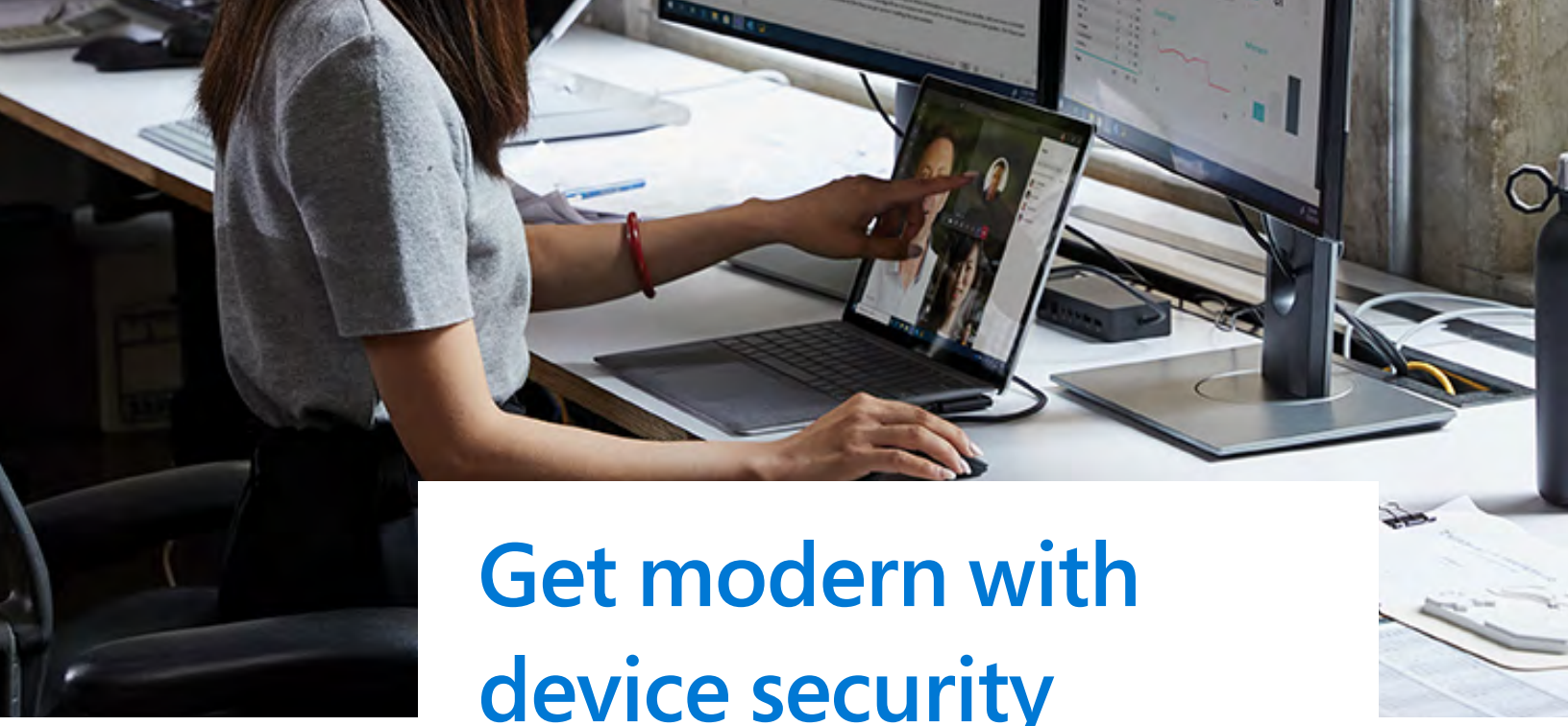
- **Built-in trouble-shooters in Windows 10** fix many common support problems without a help desk call. The Surface Diagnostic Toolkit for Business supplements that with tools to investigate, diagnose and resolve more persistent software, hardware and firmware issues.

- **End-of-life management** – when a device is lost, stolen or returned to be redeployed or retired – ensures that settings or data on the device are not exposed to unauthorised users. Using Intune, administrators can remotely lock or completely wipe a missing device.

- For **devices that are redeployed to a new employee**, Intune also allows remote reprovisioning, instead of having to collect, re-image and return the device. Surface devices can also be de-registered and re-registered through Autopilot without losing the MDM enrolment and the Azure AD join, so when it's sent to a new employee, it's properly provisioned at start-up.

Want more?

[Learn about modern device management solutions with Surface]



Get modern with device security

Traditional endpoint management – with inconsistent configurations and capabilities across different devices – increases security risk, because keeping all devices current with the latest updates and protection is all but impossible.

Embracing modern security with Surface provides a fast track to securing endpoints and the data on them.

- Managing device firmware is a generally inconsistent experience and often involves third-party providers, which makes firmware difficult to monitor and complicated to maintain. By comparison, Microsoft wrote and maintains the UEFI firmware in Surface (with the exception of the Surface Go, which uses a third-party UEFI), and makes it available for inspection through the open source Project Mu.

The UEFI in Surface can be easily managed through Microsoft Endpoint Manager, and critical updates to plug vulnerabilities are pushed to the device automatically through Windows Update for Business.

- Support for biometrics and multi-factor authentication (MFA) can help you move away from vulnerable passwords and credentials that attackers can use to gain access across your corporate network. Employees get a better experience, with better security – without having to remember passwords or carry security dongles.

Modern endpoint security has a long reach, from device firmware up to the cloud. It extends across all phases of the device lifecycle, with an emphasis on user privileges, prompt updates and data encryption. With built-in protection at every layer, Surface implements every standard for a highly secure Windows 10 device.

Key takeaways for modern device management

Microsoft has designed Surface from the chip on up to support modern management across the entire device lifecycle. With Surface, you can:

Reduce IT costs and avoid time-consuming image management

Reduce risk across the organisation without compromising employee experience

Help employees do their best work on devices they love that are easy to manage.

Learn what Surface can do for your business >

Microsoft Surface

[1] 'Maximizing Your ROI From Microsoft 365 Enterprise With Microsoft Surface', a commissioned Total Economic Impact™ study conducted by Forrester Consulting, 2020.