Microsoft Surface

Zero-Touch Device Deployment:

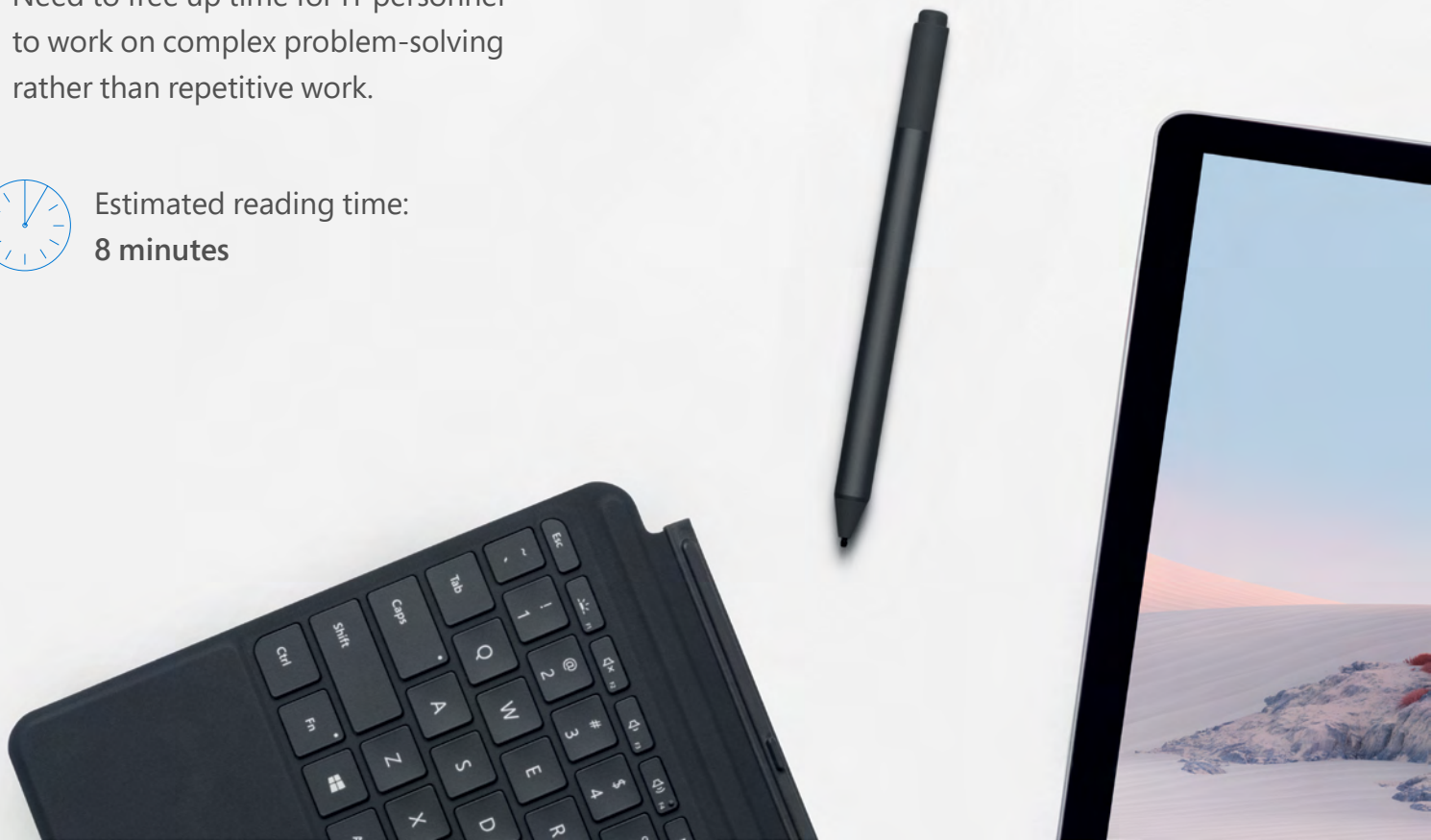
Prioritizing User Experience Through Automated Provisioning and Secured Access at Scale

This information is for you if you...

- Are involved in purchasing and deploying devices within your company.
- Want to understand how automation can help accelerate, simplify, and lower the cost of device deployment and management.
- Want to enhance the experience of your employees and IT departments for device onboarding or replacement regardless of their location.
- Need to free up time for IT personnel to work on complex problem-solving rather than repetitive work.

Estimated reading time:
8 minutes

Contents



1

Introduction

Remote work has become the norm for millions around the world. The trend is almost certain to continue after the end of the COVID-19 pandemic. It's been embraced by many companies as a full-time or part-time option, but the shift to remote work has impacted employees and IT departments with resources already stretched thin. For some organizations, deploying and managing devices has been a cumbersome and time-consuming experience. Manual, error-prone processes for setup, integration, security, and lifecycle management can lead to downtime.

At Microsoft, we believe that using an automated, zero-touch solution is essential to replacing outdated device management processes. Microsoft Surface for Business devices are built and configured for zero-touch deployment. This e-book will explain why zero-touch deployment has become critical to enterprise organizations deploying devices at scale, and demonstrate how it works with Microsoft products and services.

2

Overcoming time, distance, and complexity

Organizations manage increasingly complex device environments, with a mix of corporate-owned and personal computers, laptops, tablets, and smartphones across a variety of platforms. The breadth of devices and platforms used today leads to a lot of onboarding work for IT. This includes imaging hundreds or even thousands of devices with a company's proprietary applications and collaboration tools, and ensuring that critical security features like Windows Hello and BitLocker are installed and ready right out of the box.

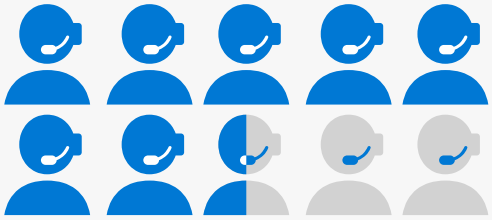
With social distancing during the pandemic, organizations scrambled to equip their employees to work remotely. Some workers used services like Windows Virtual Desktop on Microsoft Azure to add conferencing, email, and messaging. However, many employees were using dated hardware, making them ill-equipped to work remotely with full confidence they were complying with security and governance requirements. According to a report by Fluxon titled, "Evolving Opinions on Working from Home," 50.6 percent of workers said their number one frustration in working from home was technology issues.[1]

[1] "Evolving Opinions on Working From Home," Fluxon Survey, June 2020.

[2] "Employees + Anywhere = The New Digital Workplace," 1E and Vanson Bourne, June 2020.

A 2020 report by 1E and Vanson Bourne looked at the experience of 300 remote workers in the US and found that:

More than half said their devices were performing poorly due to slow-running applications and network issues, crippling their productivity.



A majority cited technical problems that further slowed their work and **nearly 75 percent said they sometimes had to wait up to weeks for their IT problems to be fixed.**[2]

Given that so many of the frustrations encountered by remote workers involve connectivity, access and diagnostics, you must ensure that any solution you expect employees to use is not hampering their ability to be productive."

John Windels,
The Enterprise Experience Blog[3]

The fact is, everyone—from IT to the people they support—was forced into a new way of working, without much time to adapt. That introduced a host of issues, including loss of centralized control, data and access security risks, and inefficient use of resources.

Fortunately, there's a better approach to device deployment and management that not only addresses immediate needs, but lays a strong foundation for meeting future needs while aligning with important initiatives and trends as well, such as consolidating devices, automation, and cloud migration.

[3] "The most frustrating things about working remotely," The Enterprise Experience Blog, April 2020.

3

Zero-touch overview: Using Windows Autopilot

What is Windows Autopilot?

Windows Autopilot is a cloud-based deployment solution that enables companies and their device suppliers to set up and preconfigure Surface for Business devices running Windows 10 and to reset, repurpose, and, if necessary, recover them. It activates features within Microsoft 365, Azure Active Directory, and the mobile device management service Microsoft Intune, to automate the provisioning and management of policies, settings, apps, and software for Surface devices.

Windows Autopilot gives employees the freedom to work from any location while IT still maintains control over device management and security. With Microsoft Endpoint Configuration Manager, IT administrators synchronize and deploy Surface firmware and driver updates within the Configuration Manager client. Integration with Microsoft Intune provides an overview of all managed, co-managed, and partner-managed devices in one place.

Azure Active Directory

An enterprise identity service that provides single sign-on and multi-factor authentication to help protect your users from cybersecurity attacks.

Windows Autopilot

Cloud-based deployment software in Windows 10 that activates features in Microsoft 365 to automate provisioning and management of hardware and software on Surface for Business devices.

Microsoft Intune

Cloud-based mobile device, operating system, and application management tool to deploy and update Surface devices.

City of Lokeren, Belgium

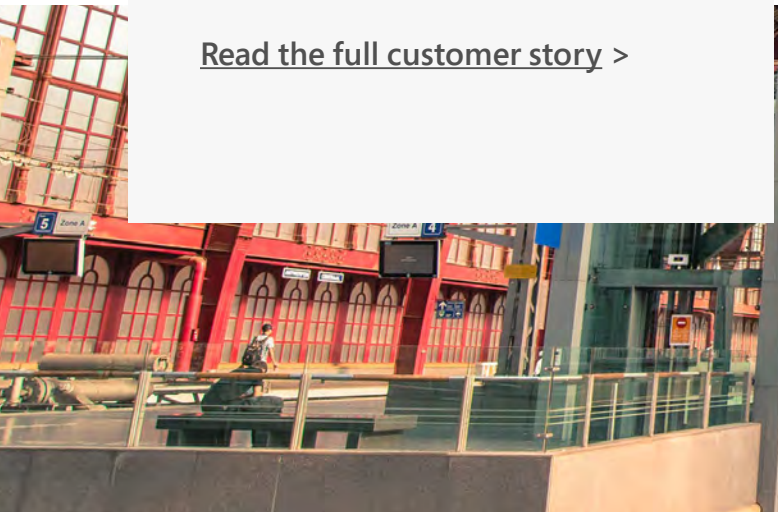
The City of Lokeren, Belgium, wanted to shift from paper to digital documents and enable desk-bound employees to work from anywhere in the city or the world. Using Microsoft Intune and Windows Autopilot, the company configured and managed its Surface Pro and Surface Go devices remotely, giving employees a simple, fast, zero-touch deployment experience. The city quickly customized devices, provisioned applications, and got employees up and running while maintaining end-to-end security and compliance policies. At the same time, Lokeren IT administrators now have firmware-level control over Surface functionality, both on-premises and through the cloud.[4]

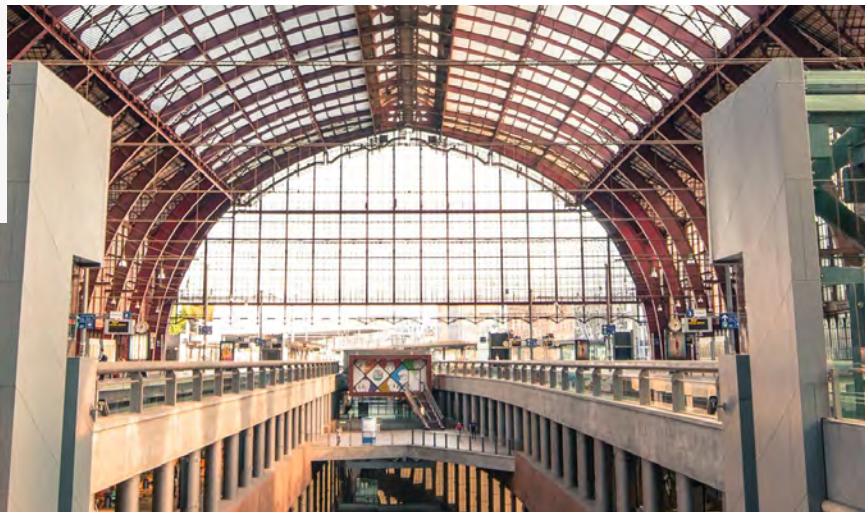
Read the full customer story >

Using Microsoft Intune to manage Windows Autopilot endpoints such as Surface devices, administrators can manage Unified Extensible Firmware Interface (UEFI) BIOS settings after enrollment using the Device Firmware Configuration Interface (DFCI). UEFI management extends modern stack capabilities down to the hardware level while DFCI layer enables seamless management down to the firmware layer with just a few clicks through the cloud.

Zero-touch provisioning has the added benefit of eliminating BIOS passwords and providing more control over security settings, including boot options and built-in peripherals such as 4K cameras, mics, and speakers.

[4] "Belgian city streamlines daily work with Microsoft Surface and Windows Autopilot," Microsoft Customer Story, May 2020.





How zero-touch deployment works

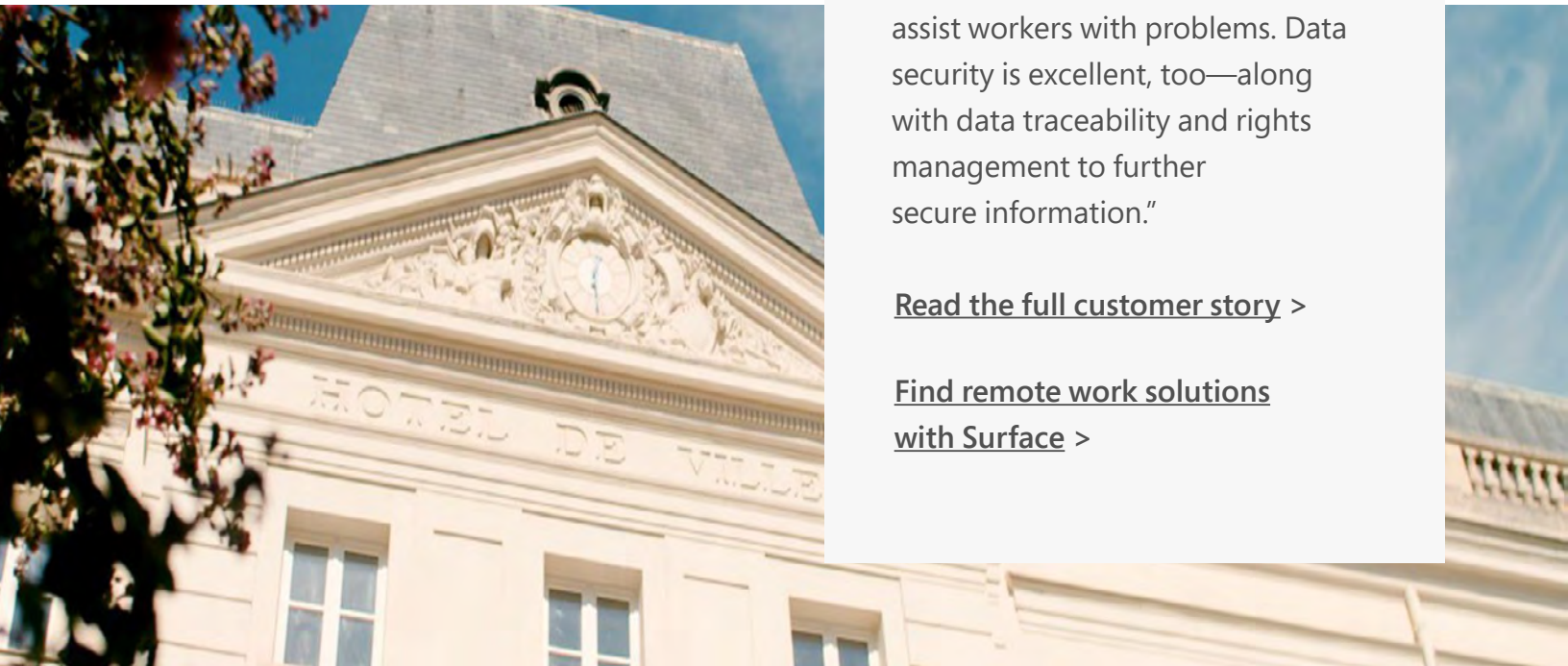
Built for Windows Autopilot, Surface reduces IT complexity and eliminates time-consuming corporate re-imaging by deploying and shipping devices straight to employees' hands, and every Surface device (except Surface Duo and Surface Hub) are enabled for Windows Autopilot when they ship from the factory. Microsoft pairs each Surface device with a cloud service provider (CSP) to enable zero-touch deployment. The electronic data interchange (EDI) number or "hardware hash" of each device is provided by Microsoft to verify its serial number. The device profile is then sent to the Microsoft Partner Center Tool, with access to the customer company's tenant domain. After enabling Windows Autopilot, an IT administrator at the purchaser's company accepts the CSP request to add another device to the company's tenant.

The IT organization can use their Azure Active Directory portal and Microsoft Intune to access serial numbers, product types, and other information to create user roles or department profiles. They can then configure for deployment applications, policies, and settings that load when each device is turned on by a remote employee.

When a Surface device is turned on and connects to a network, it calls Microsoft with its device ID, which is checked against the registration data in Windows Autopilot. If the device has been properly registered, the Microsoft Intune instance on the customer tenant is notified. Microsoft Intune then pushes applications, policies, and settings to the device with no reimaging required. Each application that is deployed is tied to Azure Active Directory. No further setup is required by the user.

It's simple, fast, and delivers device provisioning and management automation at scale.

[5]"City of Issy-les-Moulineaux creates a flexible, adaptive workplace with Surface and Microsoft 365," Microsoft Customer Story, January 2021.



French city of Issy-les-Moulineaux

The French city of Issy-les-Moulineaux wanted a flexible workplace accessible by officials and offsite field workers that would allow them to work in multiple locations across the city. The city chose Microsoft Surface devices with Microsoft 365 providing Microsoft Office applications, intelligent cloud services, and world-class security.[5]

"It's very easy to manage machines remotely with Windows Autopilot," says Jean-Paul Poggioli, the city's IT manager. "We can lock them down to protect data if a device is stolen or remotely access the device to assist workers with problems. Data security is excellent, too—along with data traceability and rights management to further secure information."

Read the full customer story >

Find remote work solutions with Surface >

Flexible options for deployment and lifecycle management with Microsoft 365

Surface devices are preconfigured for Windows Autopilot straight from the factory. Devices can also be deployed and managed using on-premises tools like Systems Center Configuration Manager (SCCM). Hybrid deployments in Active Directory and Azure Active Directory, with co-management by SCCM and Microsoft Intune, are also possible. Another deployment option is Windows Autopilot for pre-provisioned deployment, which you can use to configure devices before they are sent to end users.

Once Surface devices are deployed, they are enrolled in the Microsoft automated lifecycle management service.

Bridgewater Associates

Asset management company Bridgewater Associates needed to support an increasingly mobile workforce while keeping highly sensitive information accessible and secure. The company has fully automated its Surface device provisioning and management with Windows Autopilot.[6] Anthony Golia, Bridgewater's head of productivity and endpoint engineering, reported that the deployment process for employees was simple and completely self-service.

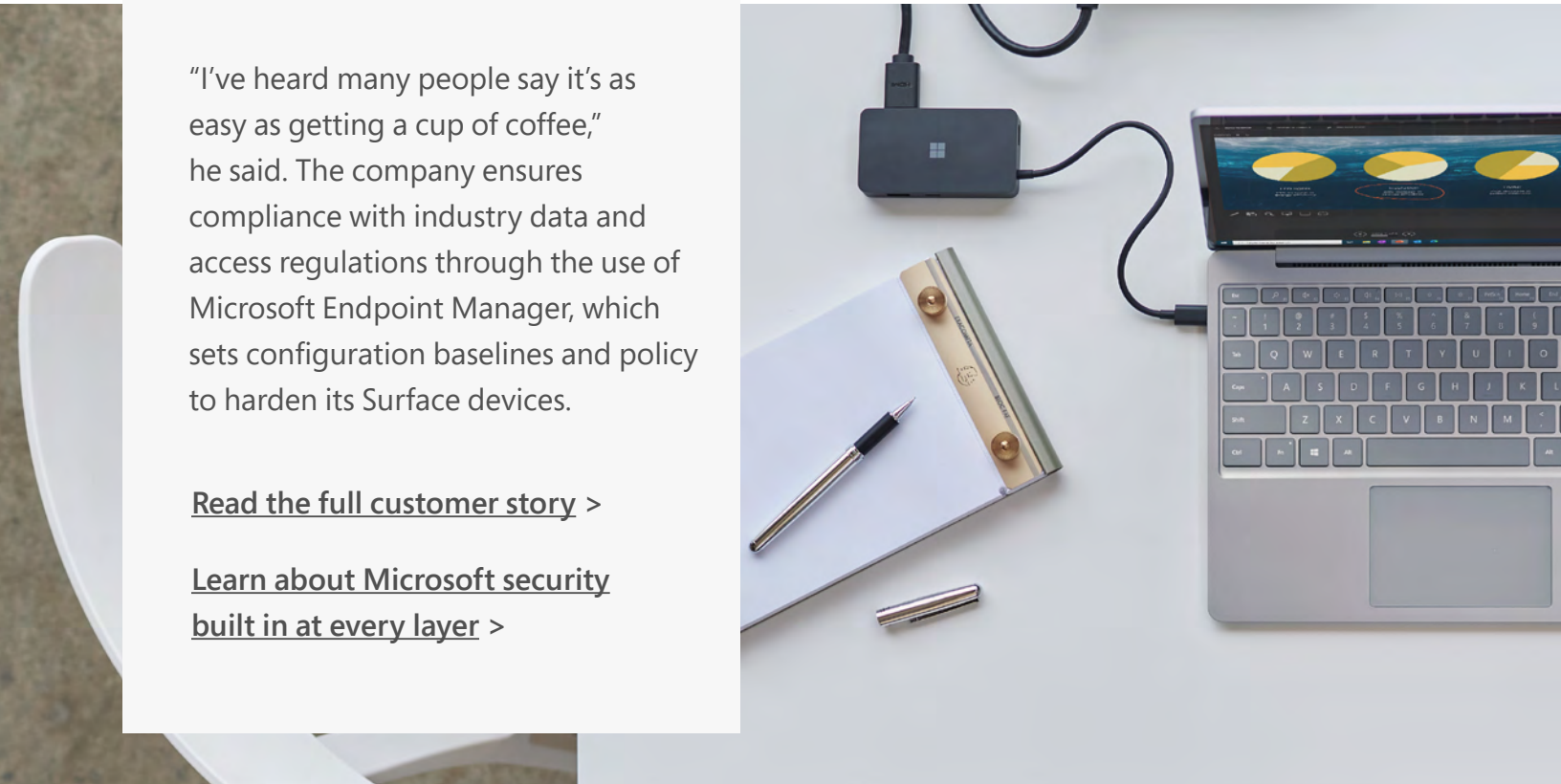
"I've heard many people say it's as easy as getting a cup of coffee," he said. The company ensures compliance with industry data and access regulations through the use of Microsoft Endpoint Manager, which sets configuration baselines and policy to harden its Surface devices.

Read the full customer story >

Learn about Microsoft security built in at every layer >

Modifications and confirmation changes from the organization are automatically pushed to the device. Features like Windows Update for Business, Microsoft Defender Advanced Threat Detection, and the Microsoft Intelligent Security Graph help ensure that every device is up-to-date, secure, and managed.

[6] "Bridgewater invests in secure remote work with a Zero Trust security model using Microsoft 365," Microsoft Customer Story, August 2020.



4

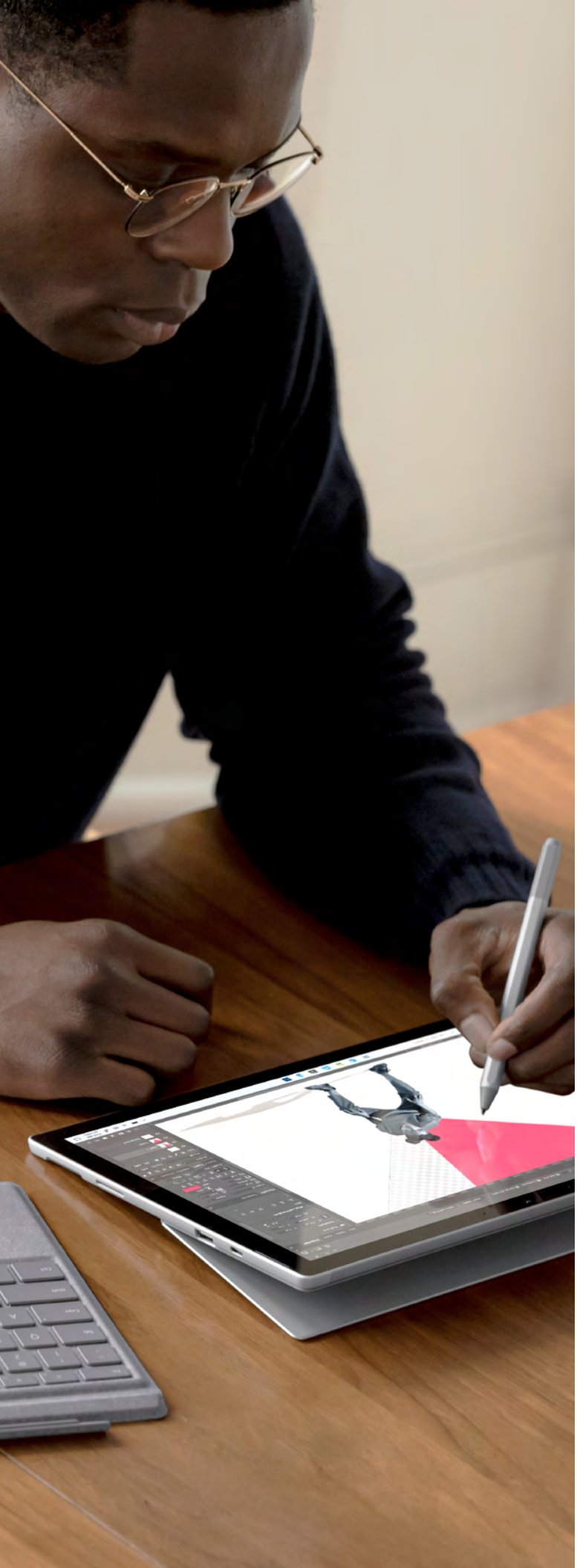
Surface devices: Built and configured for zero-touch

The world of work has already evolved and IT departments are being challenged to innovate and champion new and better ways of operating. That's why zero-touch using Windows Autopilot has gone from a compelling option to the smartest approach for device deployment.

Employees like Windows Autopilot because it's built in (instead of "bolted on") to their Surface devices and they can get up and running fast and hassle-free. Zero-touch deployment with Surface lets them minimize downtime and maximize productivity. IT departments like it because it frees them from time-consuming hardware, software and management tasks that can be prone to error. A zero-touch deployment strategy gives them more time to work on more strategic initiatives.

In addition, Surface devices are built for security from the chip to the cloud. Using Trusted Platform Module (TPM) 2.0 chips integrated with system hardware and firmware, each Surface for Business device monitors cryptographic keys and hashes to make them tamper resistant.

Zero-touch deployment and management provide ongoing benefits to every person within an organization enrolling or using Surface devices. Wherever employees work, Surface delivers the right remote working tools to help them stay productive while helping IT teams ensure security and maintain control.



Microsoft Surface

Explore how Surface for Business makes it easier to manage and secure your devices.

Learn more >