



Welcome to Microsoft 365 & Surface

The modern workplace is evolving.



Microsoft 365 and Surface deliver the experiences employees love, the protection organisations demand, and flexibility for teams to work their way. Encourage productivity, engagement, and collaboration with Surface for Business.



9hours

According to Forrester Research, Microsoft 365-powered Surface devices give users up to 5 hours in weekly productivity gains with up to 9 hours saved per week for highly mobile workers ¹

112%

ROI on Microsoft 365 with Surface ¹

75%

agree Microsoft 365-powered Surface devices help improve employee satisfaction and retention ¹

[1] Source: Forrester Consulting, "A Forrester Total Economic Impact™ Study: Maximizing Your ROI From Microsoft 365 Enterprise With Microsoft Surface," commissioned by Microsoft, 2018.

Productivity Cloud & Surface

Devices they love on the
platform you trust.

Create

- Experience industry-leading typing comfort
- Dictate with your voice
- Draw and write using Microsoft Ink

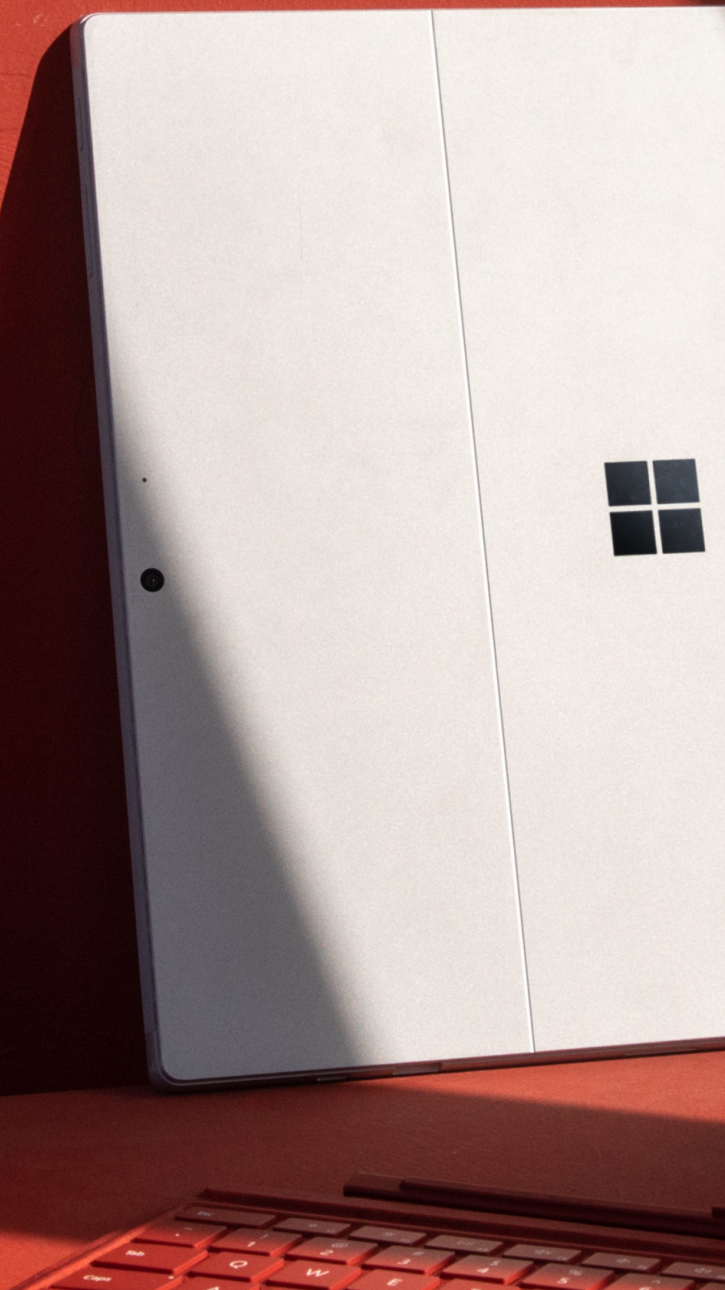
Communicate

- Distraction-free Focused Inbox
- Add live captions
- Translation tools

Collaborate

- Collaborate with Microsoft Teams
- Co-author Office documents
- Share ideas with Microsoft Whiteboard

All supported by secure
device management.



Total Security

From chip to cloud, Microsoft 365 and Surface helps organizations stay protected.

Security by design

With both hardware and software designed, built, and tested together by Microsoft, users can be confident they're productive and protected by leading technologies from chip to cloud.

Keeping Windows up to date ensures that you stay ahead of new security threats. Windows 10 has been engineered from the ground up to be more secure and utilise the latest hardware capabilities to improve security.

Every Microsoft 365 component, from firmware to Windows 10 is delivered by Microsoft. With a purpose-built UEFI and Windows Update for Business that responds to evolving threats, end-to-end protection is secure and simplified.¹

DMA (direct memory access) via USB, prioritising security.

Device encryption lets you protect the data on your Surface so it can only be accessed by authorized individuals. All Surface devices feature a Trusted Platform Module (TPM) that make it fast and easy to encrypt your data.

Optimised experiences

Microsoft 365 and Surface is a unified platform delivering every Windows security feature*. All Surface portfolio devices ship with a custom-built camera, designed for Windows Hello.

Windows Defender is built in and needs no extra agents to be deployed, simplifying management and optimising device start up.

The true out-of-the-box experience. Autopilot and MMD enable zero-touch deployment and management, wherever users are.

*Subject to licensing and enablement

[1] Surface Go uses third party UEFI.

[2] Surface Laptop 3 and Surface Pro X only. Hard drive is not user removable. Hard drive is only removable by skilled technician following Microsoft provided instructions.

Modern management

Remove power to the components so the OS doesn't know it exists. IT administrators can disable hardware elements at a firmware level such as mics, USB ports, SD card slots, cameras, and Bluetooth which removes power to the peripheral.

Device Firmware Configuration Interface (DFCI) enables IT managers to manage UEFI via Microsoft Intune, for simple remote management.

Windows Defender Credential Guard uses virtualization-based security so that only privileged system software can access them. By enabling Windows Defender Credential Guard, you get hardware security, virtualization-based security, and better protection against advanced persistent threats.

Surface designed with physical security in mind without compromising on build quality. Removable drives² means greater control over data retention.



Total Security

Security Feature	W10 O/S Feature	Device Feature	Surface feature	What does it mean?
SEMM (Surface Enterprise Management Mode)		Yes	Yes	Feature of Surface devices with Surface UEFI that allows you to secure and manage firmware settings within your organization. ¹
Conditional Access	M365 E5			Optimised user experience by granting access based on use of Windows Hello as multi-factor authentication built into Surface.
Protected DMA Access		Yes	Yes	We placed a boot mask over PCI-E port during boot so it is inaccessible, we remove power to entire device if the SSD is ever removed and during boot all of RAM is zero'd out by UEFI.
Windows Defender Credential Guard	Yes			Isolate and harden key systems and user secrets. This makes an attack against user credentials much harder to perform.
Windows Defender Application Control	Yes			Harden computers against malware and prevent malicious code. This stops code that has not been previously ratified as secure from running.
Device encryption	Yes			Implementing BitLocker, and managing that through a TPM chip.
Purpose Built UEFI w/TPM 2.0		Yes	Yes All Current	Microsoft's unique Unified Extensible Firmware Interface (UEFI) is built by Microsoft, delivers automatic updates, and is consistent, minimizing risk and maximizing your control. ¹
Device Firmware Configuration Interface (DCFI)		Yes	Yes All Current	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.
Removable SSD ²		Yes	Laptop 3 & Pro X	Confidence around data retention on serviced devices.
Surface Data Eraser		Yes	Yes	Written in partnership with the US security services, this tool allows you to fully wipe and erase a Surface. US DoD approved.
Microsoft Defender Advanced Threat Protection (ATP)	Yes			Providing evergreen and updated malware protection, digital forensics (to identify the attack after the event). Running the agents in a separate memory space (discussed in the next point) reduces the risk of the Defender code itself being compromised.
Windows Hello	Yes		Optimised	Hello process designed and tested for Surface. Surface camera specifically designed for Hello.
Physical TPM 2.0		Yes		By using a physical TPM 2.0 chip in most of the Surface range, rather than a virtualised environment inside firmware, we have a more secure and sandboxed environment for storing passwords, PIN numbers and certificates.
Secure Boot	Yes		Optimised	Enabled by UEFI and TPM 2.0. Only code signed, measured, and correctly implemented can execute on a Surface device.
BitLocker	Yes		Optimised	Our physical TPM and the UEFI control allows a significantly improved and integrated encryption solution.

[1] Surface Go uses a third party UEFI.

[2] Surface Laptop 3 and Surface Pro X only. Hard drive is not user removable. Hard drive is only removable by skilled technician following Microsoft provided instructions.

Find out more

Get Modern

- Seamless Deployment & Management
- Enhancing employee productivity
- Built-in for everyone

Firstline

- Connect your Firstline to drive productivity through Microsoft Teams
- Drive cultural changes with Surface & Teams
- Streamline business practices with Power Apps

Microsoft Teams

- Accelerate Teams adoption with Surface Hub 2S
- Drive cultural change with Surface & Teams
- Connect your Firstline to drive productivity through Microsoft Teams

