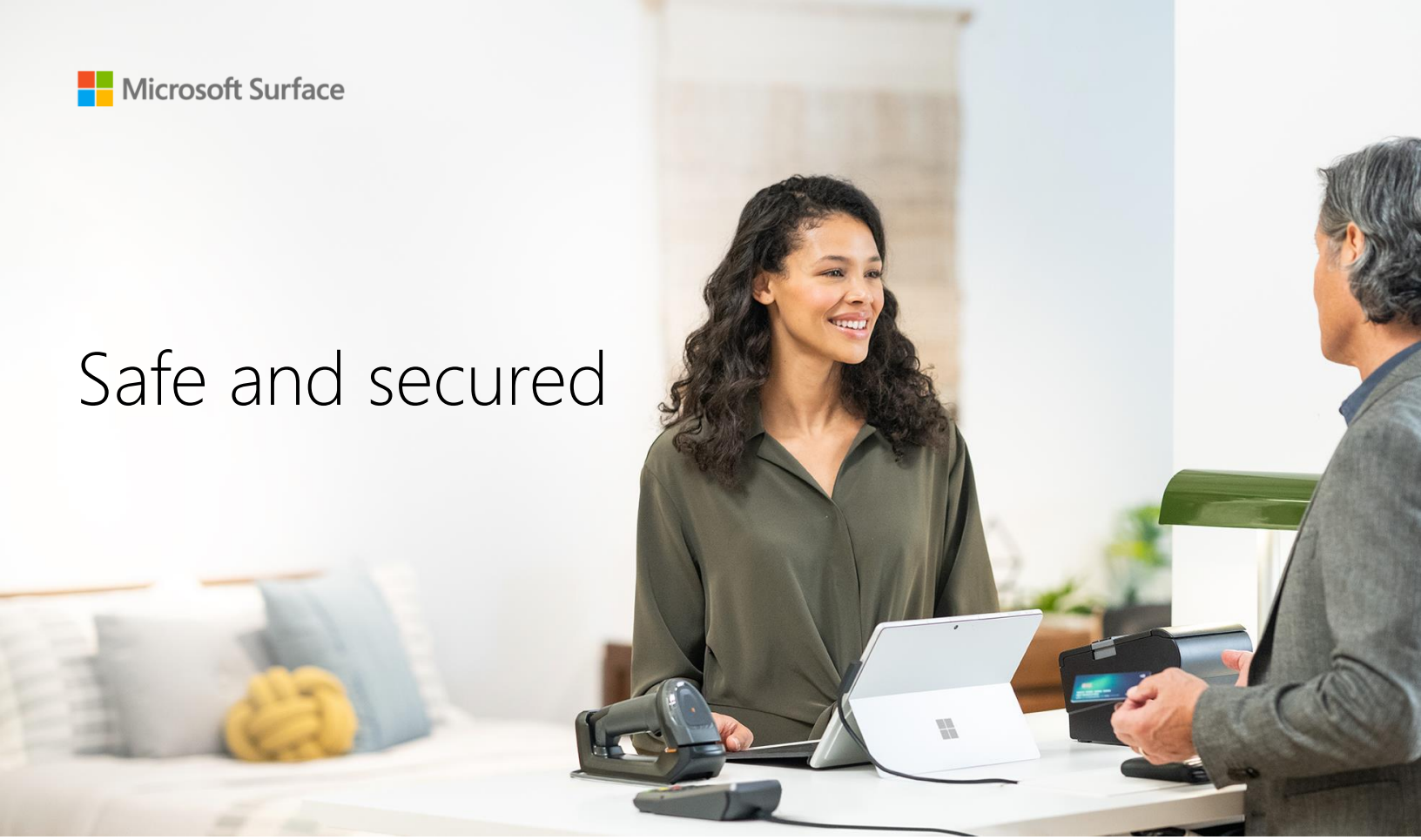
Microsoft Surface

Safe and secured



When your team is protected, they can focus on moving the business forward.

The world is changing—fast. Security threats continue to escalate in scale and sophistication as businesses shift to modern work environments with geographically distributed devices.

Without the protection of secured offices and internal networks, your devices are the front line between your data and digital attackers. IT endpoint security isn't enough on its own, so modern devices need to defend themselves against evolving threats.

Surface combines the best of Microsoft hardware and software to prevent zero-data exploits, protect encryption keys, stop firmware attacks, and secure your data.

With Microsoft Surface, world-class security is simple.

Built for peace of mind

Whatever the size of your business, Surface gives you built-in security that's ready for modern work at any scale.

We created Surface with industry-leading protection across hardware, firmware, software, applications, and identity. As a result, devices designed by Microsoft provide uncompromising chip-to-cloud security that delivers proactive protection and peace of mind.

Surface's hybrid features implement Zero Trust cloud services, so you can rely on your tamper-proof processor and CPU chips to track device health. That means your technology ecosystem works together to isolate threats before they get out of control, and you can move forward with confidence.

Microsoft Surface

The control you need

By bringing powerful security features together across every layer of hardware and software, you can keep control in your hands long after deployment.

Combined with Windows and Microsoft 365*, Surface adapts your business to the ever-changing world of defensive security through intelligent features and automatic updates.

At the same time, you have the power to configure and manage firmware remotely, update security, and gain insights through Surface Management Portal.

From conceptual design to a team member's first Hello, Surface reduces complexity, elevates trust, and gives you the control you need, wherever and however work gets done.

Key Features of Microsoft Surface

- Trusted Platform Module (TPM) 2.0 protects and controls authentication.
- BitLocker encryption is enabled by default.
- Microsoft's Unified Extensible Firmware Interface (UEFI)[1] unlocks remote firmware configuration and control on most Surface devices.
- Windows Hello for Business uses industry-leading biometrics to give device owners instant and secure access without the need for passwords.
- Microsoft Defender and Advanced Threat Protection leverage cloud-based telemetry to defend against real-time global threats.
- Strong, two-factor authentication protects your employees and devices.
- Removable SSDs[2] come standard on most Surface devices, so you don't have to worry about your most sensitive data.
- Microsoft Intune* admin center lets you control devices down to the firmware layer[3] through the cloud with just a few clicks.

*Software license required for some features. Sold separately.
[1]Surface Go and Surface Go 2 use a third-party UEFI and do not support DFCI. For details on Microsoft protection for Surface Go and Go 2, visit https://www.microsoft.com/en-us/surface/business/surface-go-2.
[2]Available service options for SSD replacement may vary by device and/or market. See https://www.microsoft.com/en-us/download/100440 for details. Devices returned to Microsoft with a missing SSD may be subject to an SSD replacement fee unless the user is enrolled in the Drive (SSD) Retention offer. Opening and/or repairing your device can present electric shock, fire and personal injury risk and other hazards. Use caution if undertaking do it-yourself repairs. Device damage caused during repair will not be covered under Microsoft's Hardware Warranty or protection plans.
[3]Firmware level management is not available on Surface Go.