Microsoft Surface

From Chip to Cloud: Endpoint Security for the Modern Workplace

Modern endpoint security has a long reach, from the device firmware, up to the cloud, and across all phases of the device lifecycle.

Every layer of a Surface device, from the hardened firmware that is adopted from a Microsoft open-source UEFI, to the operating system, is maintained by Microsoft. Get the highest level of security and control, from chip to cloud, with protection from Microsoft.

Inside the endpoint

Each Microsoft Surface contains sophisticated hardware and firmware designed to secure the device and the software that runs on it. Administrators can control even the lowest level of hardware settings without having to touch the machine.

- The **Trusted Platform Module** (TPM) makes encrypting data fast and easy, enabling access only to authorized individuals.
- The **Unified Extensible Firmware Interface** (UEFI) is maintained by Microsoft,[1] so that from the time the power button is pressed to the time that the operating system boots, organizations can avoid a critical vulnerability point and be assured that the latest UEFI updates are pushed out.

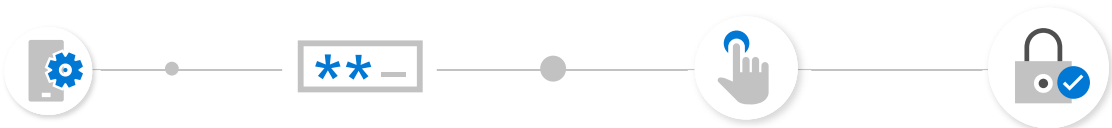
[1] Surface Go and Surface Go 2 use a third-party UEFI and do not support DFCI. DFCI is currently available for Surface Book 3, Surface Laptop 3, Surface Pro 7, and Surface Pro X. Find out more about managing Surface UEFI settings.

Windows Update for Business and Microsoft System Center Configuration Manager (SCCM) make it easy to manage software updates and get them out to users as quickly as possible.

Access to the endpoint device

Passwords are still the primary protection for many devices. However, they're not the most secure approach to authentication. New technologies significantly reduce the need for passwords—even enabling you to remove passwords from your identity directory entirely.

- **Windows Hello** biometric authentication eliminates the need for passwords. Employees may forget a password or reveal it in a phishing attack, or lose a hardware token, but Windows Hello never forgets a face, or a fingerprint. Microsoft's Windows Hello is certified as FIDO-2 compliant.[2]
- **Microsoft 365 Conditional Access** provides users access to data and resources only when a device meets specific criteria, like user location, time of day, or other factors you choose.
- The **Microsoft Authenticator** phone app leverages multifactor authentication to provide users with easy, secure access to online accounts.



[2] FIDO (Fast IDentity Online) standards are defined by the FIDO Alliance.

Deployment, redeployment, retirement

Microsoft tools allow IT to automate robust security practices across each phase. Keep every Surface device secure through its lifecycle, from its first deployment to its last, and until you're ready to upgrade.

- **Windows Autopilot** offers zero-touch deployment, which enables you to reduce IT complexity and eliminate time-consuming corporate re-imaging by shipping and deploying straight to users.
- **Microsoft Endpoint Manager** allows you to manage the device down to the firmware layer through the cloud. Surface is the only manufacturer to have Device Firmware Configuration Interface (DFCI) enabled for modern cloud-based device management.[3]
- With **Microsoft InTune**, IT can wipe a device clean, either because it was lost or stolen or to assign it to a different user. Then the device can be reset to the out-of-the-box experience, at which point proper credentials are required for set-up.

Microsoft Surface

Ready to get started?

The IT industry has learned the hard way that there's no substitute for defense in depth. In an age of rising security threats, businesses need protection across multiple layers. Surface continues to innovate to meet the evolving needs of customers, helping your business stay secure and maintain control, from chip to cloud, with protection from Microsoft. With built-in protection at every layer of the device, you can be confident that you have the best, most streamlined implementation of Microsoft's security stack.

Learn more about Surface by signing up for weekly emails.

Find a reseller ›

[3] Surface Go and Surface Go 2 use a third-party UEFI and do not support DFCI. DFCI is currently available for Surface Book 3, Surface Laptop 3, Surface Pro 7, and Surface Pro X. Find out more about managing Surface UEFI settings.