Microsoft Surface

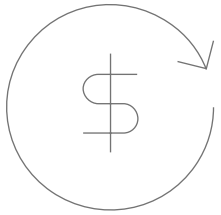
Microsoft Surface Security |

Built-in, fully integrated, chip to cloud protection

Today's workplace needs an integrated security solution

- ✓ Organizations are pivoting to remote work
- ✓ Current network infrastructures were not built with today's security in mind
- ✓ Increasingly sophisticated and targeted attacks, specifically at a firmware level
- ✓ Customers need an added layer of security to ensure comprehensive protection as they adapt to remote work

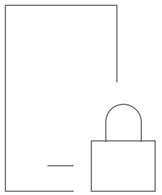
The increasing costs of data breaches



$3.86M

USD

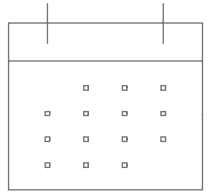
average total cost of data breach to companies worldwide, +6.4% from 2017 [1]



$123B

USD

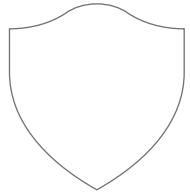
was spent worldwide for information security in 2020 [2]



190

DAYS

average mean time it takes to identify a data breach [1]



$10B

USD

will be spent globally on security awareness training for employees in 2027 [3]

[1]NASCIO, Ponemon Institute's 2018 Cost of a Data Breach Study, September 2018. . [2]Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020, June 17, 2020 [3]https://www.cpomagazine.com/cyber-security/11-eye-opening-cyber-security-statistics-for-2019, June 2019.

Did you know? Security effects more than just IT

C-Suite & Finance

40%

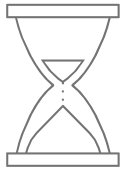
Three years after an attack, breached companies underperform the index by a margin of over 40%. [4]

Product Development

96%

96% of cybercriminals attack to gather intelligence such as proprietary IP. [4]

HR & Operations



24x

The average cost of downtime is 24 times higher than the average ransom amount. [4]

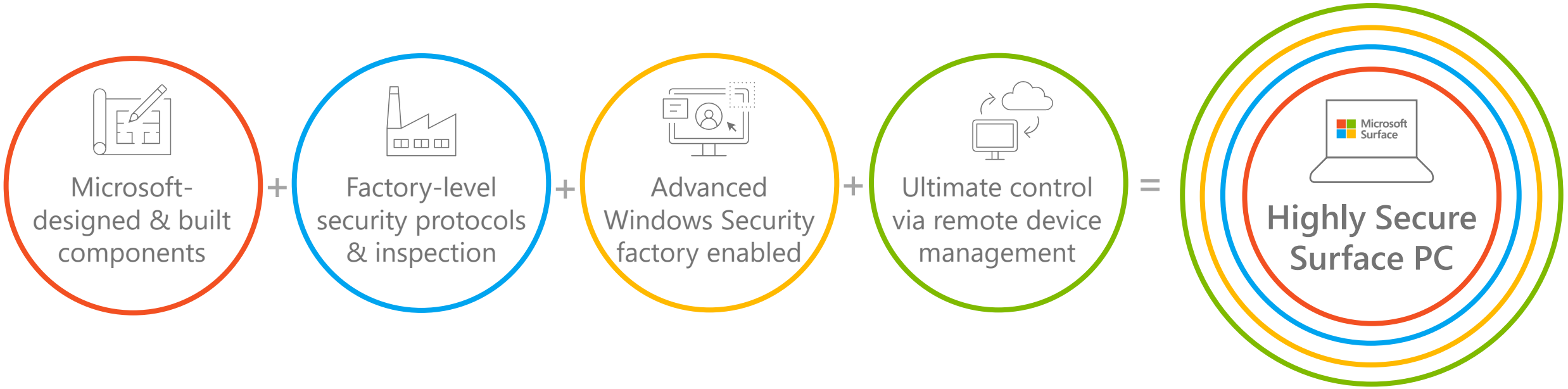
Legal

LAWSUITS & FINES

Companies can be sued by customers whose PII has been stolen; and fined by regulatory agencies. [11]

[1] 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2020] EDITION] – Comparitech, July 2020, https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
[2] https://www.blackstratus.com/risk-liability-assessment/

There is a clear need for device protection.
The answer? Layered security with Microsoft Surface.



Every layer of Surface from chip to cloud is developed and maintained by Microsoft, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

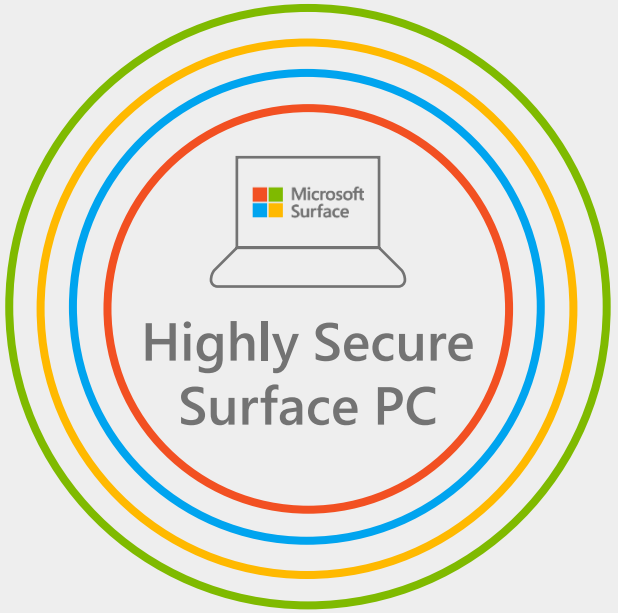
Click each circle to expand

Microsoft-designed & built components

Microsoft built UEFI for Boot Security and Firmware Management

TPM 2.0 Security Processor to ensure data protection

Windows 10 and Microsoft 365 Defender enterprise defense suite, built-in is better than bolt-on



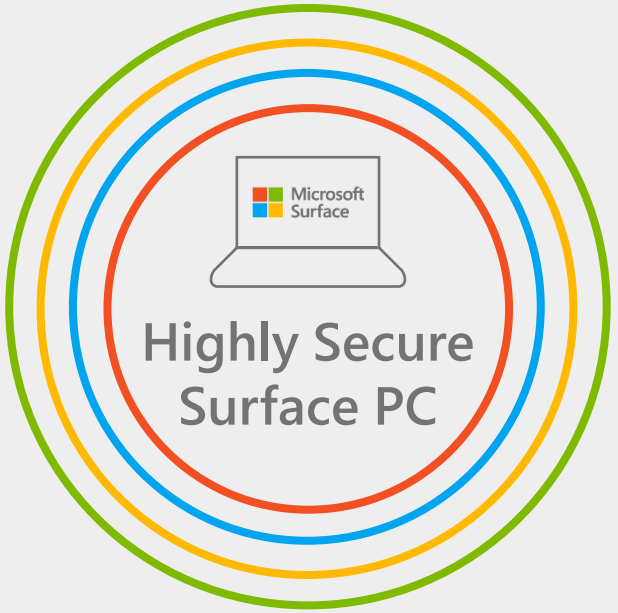
Every layer of Surface from chip to cloud is developed and maintained by Microsoft, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Factory-level security protocols & inspection

Component inspection and testing at final assembly locations

Use of Microsoft developed & maintained firmware, drivers and OS

Secure logistics to Microsoft resellers



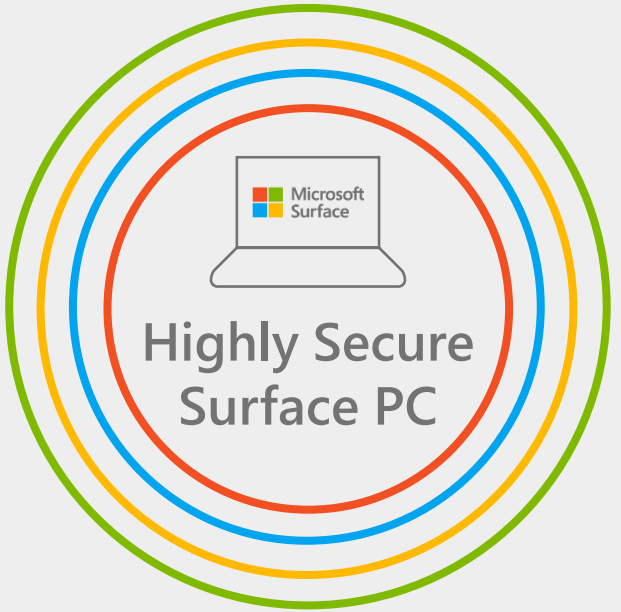
Every layer of Surface from chip to cloud is developed and maintained by Microsoft, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Advanced Windows Security factory enabled

Virtualization-based security (VBS) to separate applications and data from the core of Windows 10

Secure Boot and Boot Guard to ensure Windows 10 is authentic

Bitlocker to secure and encrypt your data and Windows Hello to enable password-less login



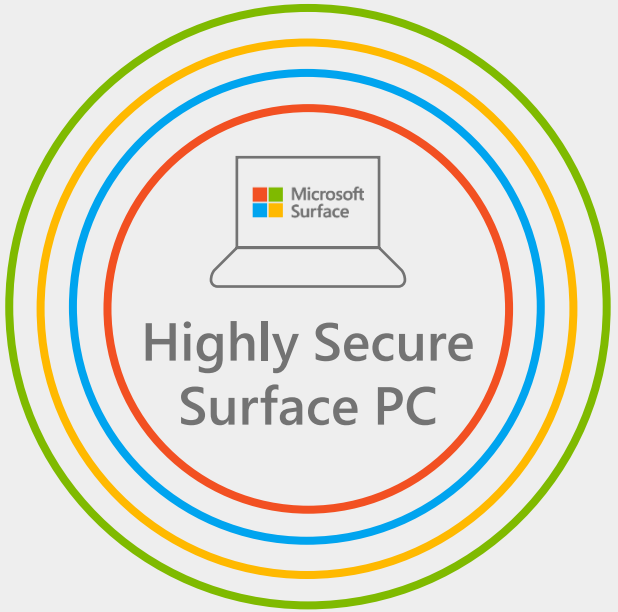
Every layer of Surface from chip to cloud is developed and maintained by Microsoft, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Ultimate control via remote device management

Complete device management through the cloud via Microsoft Endpoint Manager (MEM)

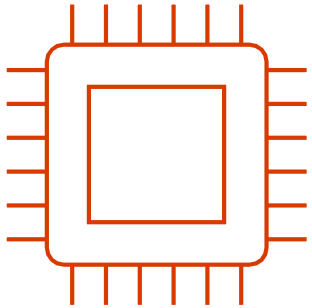
Automatic Updates from Windows Update for Business

Granular firmware management to disable components pre-boot via MEM



Every layer of Surface from chip to cloud is developed and maintained by Microsoft, giving you ultimate control, proactive protection, and peace of mind wherever and however work gets done.

Why firmware defense matters



Does your organization have a firmware defense strategy in place?

Jan 2018

Spectre & Meltdown vulnerability at processor level of all x86, PowerPC and select ARM devices.

Jan 2019

ShadowHammer supply chain attack against ASUS firmware infecting > 1M devices.

Sept 2020

MosaicRegressor is identified as a bootkit that over-writes the UEFI and is used for espionage and data exfiltration.

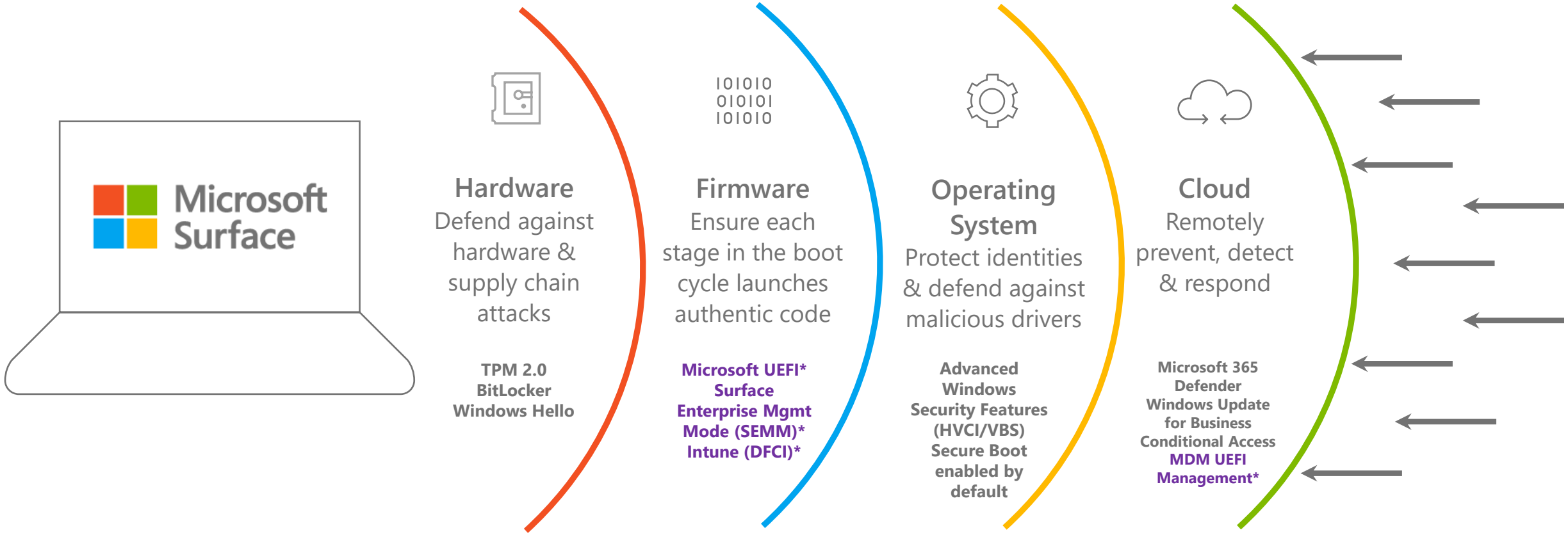
Sept 2020

US National Security Agency (NSA) issues technical report recommending Secure Boot and protections for UEFI/Firmware.

Dec 2020

Trickbot malware begins to target UEFI vulnerabilities to overwrite firmware and takeover OS as a bootkit.

Chip to cloud security is built-in to Surface DNA



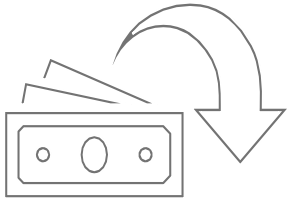
*Exclusive to Surface

Reduce risk and lower costs with Microsoft 365–powered Surface devices

20% ↓

reduction

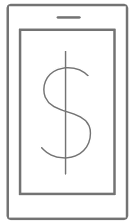
in security breaches for Surface users



17% ↓

reduction

in endpoint security spend



14% ↓

reduction

in mobile device management spend

***Source**: A commissioned Total Economic Impact™ study conducted by Forrester Consulting on behalf of Microsoft, July 2020. "Maximizing Your ROI from Microsoft 365 Enterprise With Microsoft Surface."*

Surface Secure: the gold standard in endpoint security

- ✓ Windows Enhanced Hardware Security features enabled out of the box to protect against malicious code
- ✓ Complete Cloud-based device management and updates from OS to firmware to reduce IT complexity
- ✓ Security processor protections; BitLocker to secure & encrypt your data and Windows Hello for password-less login
- ✓ Microsoft written, open source UEFI (BIOS) to ensure authenticity of firmware and Windows 10

Microsoft Surface & Secured Core PCs

Different approaches but the same result: best-in-class endpoint security from Microsoft.

	Surface Devices	Secured Core PCs
Protect with hardware root of trust	✓	✓
Defend against firmware level attack	✓	✓
Prevent access to unverified code	✓	✓
Protect identities from external threats	✓	✓

Microsoft Surface & Secured Core PCs

Different approaches but the same result: best-in-class endpoint security from Microsoft.

	Protect with hardware root of trust	Defend against firmware level attack	Prevent access to unverified code	Protect identities from external threats
Surface Devices	☑ Surface's Root of Trust checks signatures and measurements at each stage to tightly ensure each stage is secure and authentic before allowing the next phase of boot to proceed.	☑ Microsoft builds its own firmware from the ground up, rather than relying on 3rd party source code. This allows Microsoft to continuously provides updates, down to the firmware level to protect against the latest threats.	☑ With Hypervisor Code Integrity (HVCI), Windows 10 devices are protected from running any unverified code. Code running within the trusted computing base runs with integrity and is not subject to exploits or attacks.	☑ Protect Identities from external threats with Windows Hello[2]. Credential Guard ensures that identity and domain credentials are isolated and protected in a secure environment.
Secured Core PCs	☑ Partnering with leading PC manufacturers and silicon vendors, secured-core PCs use industry standard hardware root of trust coupled with security capabilities built into today's modern CPUs.	☑ Secured-core PCs use hardware rooted security in the modern CPU to launch the system into a trusted state, preventing advanced malware from tampering with the system and attacking at the firmware level.		

Surface Security Specifications

Security Feature	W10 O/S Feature	Surface + OEMs	Surface only	What does it mean?
Custom Built UEFI			Yes [1]	Replaces the standard basic input/output system (BIOS) with new features including faster startup and improved security. The Unified Extensible Firmware Interface (UEFI) — built by Microsoft without third-party involvement — ensures significantly more control over the hardware of a device and speedier react times. [1]
DCFI (Device Firmware Configuration Interface)			Yes [2]	Delivers cloud-scale remote firmware management with zero-touch device provisioning. Microsoft's own UEFI allows stronger DCFI implementation, enabling organizations to disable hardware elements and remotely lock UEFI using Intune. [1]
Protected DMA Access			Yes	Mitigates potential security vulnerabilities associated with using removable SSDs or external storage devices. Newer Surface devices come with DMA Protection enabled by default.
Surface Data Eraser			Yes	Provides a bootable USB tool to securely wipe data from your Surface devices.
SEMM (Surface Enterprise Management Mode)			Yes	Enables centralized enterprise engagement of UEFI firmware settings across on-premises, hybrid, and cloud environments.[1]
Removable SSD		Yes	Yes [3]	Helps organizations protect their data and comply with data retention policies.
Physical TPM 2.0		Yes		Uses a physical, discrete TPM 2.0 chip, implementing a secure and sandboxed environment for storing passwords, PIN numbers, and certificates.
BitLocker	Yes	Yes	Yes	Combined with physical TPM and UEFI, provides a significantly improved and integrated encryption solution.

[1] Surface Go and Surface Go 2 use a third party UEFI and do not support DFCI. DFCI is currently available for Surface Laptop Go, Surface Book 3, Surface Laptop 3, Surface Pro 7, and Surface Pro X. about managing Surface UEFI settings.
[2] DFCI is currently available for Surface Laptop Go, Surface Book 3, Surface Laptop 3, Surface Pro 7, and Surface Pro X. about managing Surface UEFI settings.
[3] Removable SSD available on Surface Laptop 3, Surface Laptop Go, and Surface Pro X. Hard drive is only removable by skilled technicians following Microsoft instructions. Hard drive replacement may cause damage or safety risk and is not recommended.

Surface Security Specifications *(contd)*

Security Feature	W10 O/S Feature	Surface + OEMs	Surface only	What does it mean?
Windows Hello for Business	Yes	Yes	Yes	Replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.
Secure Boot	Yes	Yes	Yes	Enabled by UEFI and TPM 2.0, ensures that only code signed, measured, and correctly implemented code can execute on a Surface device.
Microsoft Defender with Endpoint	Yes	Yes	Ships Enabled	Provides an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.
Windows Defender Credential Guard	Yes	Yes	Ships Enabled	Isolates and hardens key systems and user secrets, making an attack against user credentials much harder to perform.
Windows Defender Application Control	Yes	Yes	Ships Enabled	Hardens computers against malware and prevents malicious code. If code is not previously confirmed as secure, it cannot run.

[1] Surface Go and Surface Go 2 use a third party UEFI and do not support DFCI. DFCI is currently available for Surface Laptop Go, Surface Book 3, Surface Laptop 3, Surface Pro 7, and Surface Pro X. about managing Surface UEFI settings.
[2] DFCI is currently available for Surface Laptop Go, Surface Book 3, Surface Laptop 3, Surface Pro 7, and Surface Pro X. about managing Surface UEFI settings.
[3] Removable SSD available on Surface Laptop 3, Surface Laptop Go, and Surface Pro X. Hard drive is only removable by skilled technicians following Microsoft instructions. Hard drive replacement may cause damage or safety risk and is not recommended.