Microsoft Surface

Call guide:
How to sell Surface as part of a more complete security solution

Modern security is quickly evolving. Previously, the company network lived behind a firewall, but with an increasingly mobile workforce, devices have become the frontline for endpoint security. While safeguarding data has always been a priority, the growing financial and reputational risks of a data breach are increasingly high. It is predicted that 64% of organizations will experience at least one endpoint attack that will compromise their data assets or IT infrastructure.[1]

A 2018 Forrester Total Economic Impact™ study on the use of Microsoft 365 Enterprise and Microsoft Surface saw an 80% reduction in security breach costs, and a 50% reduction in annual security breach volume over three years.[2] With the right device, you can take advantage of all of the security measures built into Windows 10 and Microsoft 365.

This guide will cover all the key points that will help you explain how Microsoft Surface forms an essential part of the Microsoft security solution.

Why IT pros love Surface and Microsoft 365

IT staff are often slowed down by manual or time-consuming processes. Delivering cloud-based IT solutions and collaboration tools enables organizations to boost productivity and save time and money.

As a device and security solution, Surface can help organizations meet their security needs while delivering greater flexibility and productivity to their employees. With Intune and Windows Autopilot, IT staff can save time spent readying, deploying, and managing devices, while employees gain productivity from immediate access to the applications and resources they need to successfully do their job.

Some IT departments are committed to legacy solutions

It's important to note that organizations may have existing security solutions that they trust and are not yet ready to replace. By introducing Surface and Microsoft 365 together, you can position the two as a comprehensive solution that empowers employees to work how they want, with the peace of mind that company data, applications, and systems remain more secure behind an always up-to-date layer of security.

Please review this guide as you prepare to sell Surface as part of a security solution.

1. Introduction: Why should I sell Surface as part of a security solution?

For customers

The following are just a few reasons why customers like Surface as part of a security solution:

Surface is designed with technology that simplifies device management for IT staff.

IT staff also love it because it helps complete the security job.

It makes defense in depth, from chip to cloud, and accessible to every kind of organization.

For you

By selling Surface as an endpoint security solution, you can to establish yourself with customers as a long-term partner, creating lasting value for both parties.

- Sellers can position themselves as long-term trusted partners, not just one-time device resellers.
- Surface + Microsoft 365 gives customers the best of Microsoft and gives sellers the opportunity to have more valuable conversations with customers, along with longer-term relationships, which deliver more reliable, regular revenue over time.
- Combined with a software as a service model, partners can position themselves as a one-stop IT solutions shop.
- Overall deal value can increase when Surface, Windows 10, and Microsoft 365 are sold together.

2. The productivity and security opportunity for customers

Surface helps IT staff save time deploying devices with cloud-based tools such as Windows Autopilot and Intune. Some productivity gains include:

- Zero-touch device deployment: Employees can start using their Surface right out of the box.
- 9 hours saved on common tasks by mobile workers.[2]
- 112% ROI on Microsoft 365 with Surface.[2]
- 78% of customers reduced IT time and labor to configure and deploy Surface devices.[2]
- 2.5 hours saved by IT per app provisioning request.[2]
- 25 minutes saved configuring each device.[2]

3. Target organizations are undergoing significant changes

As modern organizations race to keep up with evolving cybersecurity threats and compliance requirements, Microsoft Surface can help organizations with:

- Growth and change in the organization.
- Growing interest in cyber and broader operational resilience.
- Accelerating trends in remote work, more flexible workforces, and multiple locations.
- The growing financial impact of breaches—the average cost of a breach is $8.19M (Forbes).[3]
- Excessive or poorly integrated solutions that decline as new technology arises.

4. How Surface delivers productivity and high security

Surface helps organizations better meet their security needs while delivering greater flexibility and productivity to its employees. Windows Autopilot and Intune help IT staff save time deploying devices and users gain immediate access to the apps and resources they need to do their job:

- 15% reduction in device and application performance tickets is achieved with Surface.[2]
- 76% of organizations that use Surface devices agree that Microsoft 365–powered Surface devices have helped improve employee retention.[2]
- Surface helps achieve nearly 5 hours in weekly productivity gains for workers.[2]
- Microsoft Unified Extensible Firmware Interface (UEFI) for Surface allows automatic security updates through Windows Update for Business.[4]
- Cloud-based accessibility makes it possible to manage devices with just a few clicks.
- Cloud-based accessibility also enables zero-touch device management.
- Features such as Windows Hello enable modern authentication methods, including biometrics.

Case study: KMD cuts deployment from 24 hours to 10 minutes

As an example of customer success, KMD, a global IT and software services company, recently invested in Surface to support the needs of its increasingly global workforce. They were able to:

- Launch a choose-your-own-device (CYOD) program, where many employees elected to switch to Surface Pro devices.
- Upgrade from the Microsoft 365 E3 licensing tier to E5 to take advantage of deeper security features that ensure compliance with Europe's General Data Protection Regulation (GDPR).
- With AutoPilot and Windows 10, devices now take just minutes to get up and running, and no longer involve restoring from a full back up manually.

Critical security features: quick guide

Surface devices are designed with security features, from chip to cloud. Some of the business-critical security features include the following:

Customer objective	Where Surface and Windows features can help	Definition	Objection handling and key talking points
Can I secure devices from malware attacks?	Surface includes a No DMA Access feature prevents malware entering internal memory through external peripherals, such as a USB stick.	Surface includes a No DMA Access feature that prevents malware from entering internal memory through external peripherals, such as a USB stick.	What about malware that is shared digitally? *Surface devices that run Microsoft 365 are automatically updated with the latest threat intelligence, which includes known malware attacks. See also Windows Defender Device Guard.*
How can I secure users' credentials?	Windows Defender Credential Guard isolates and hardens key systems and data, helping prevent attacks against user credentials.	A virtualization-based isolation technology that prevents attackers from stealing credentials that could be used for pass-the-hash attacks.	How can I securely store sensitive data including credentials and passwords? *Windows Defender Device Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them.*
How can I secure my organization from malicious files such as malware?	Windows Defender Device Guard hardens devices against malware and prevents malicious code. If code isn't previously confirmed secure, it won't run.	A combination of enterprise-related hardware, firmware, and software security features that, when configured together, will lock down a device so that it can only run trusted applications.	Even with the best security, a user may download a malicious file. Then what? *Windows Defender Device Guard disallows malicious files to run if code isn't proven to be secure.*
Can I encrypt the data hosted on or shared from a device?	Yes, by implementing BitLocker and managing that through a TPM chip, you can encrypt sensitive data.	BitLocker is a full-volume encryption feature.	Device security is great, but my organization shares a lot of sensitive data. *Bitlocker when combined with a TPM chip allows data to be encrypted and stored securely.*
What level of control do I have over my organization's devices?	Without third-party involvement, you have significantly more control over a device's hardware, in addition to faster uptake times.	Surface Enterprise Management Mode (SEMM), along with unique UEFI from Microsoft, allows you to remotely manage a device's firmware components.	Many new threats target specific components of a device's firmware, such as its camera or speakers. SEMM can support your efforts to defend against these and other potential attacks.

Can I manage a device's hardware and firmware features?	Microsoft UEFI allows for stronger Device Configuration Firmware Interface (DCFI) implementation. Organizations can disable hardware elements, such as USB ports and cameras, and remotely lock UEFI, using Intune.	DCFI securely enables zero-touch remote configuration of these settings built upon Intune and authorized by Windows Autopilot. It can also configure and lock hardware security features before launching the OS.	Remote working is the new normal—are you sure your IT team has high visibility and control over every device (and its security) in your estate?
Can I scrub a device at the end of its life cycle?	Surface Data Eraser enables a full wipe to erase a Surface device. Intune can remotely wipe a device if it is lost or stolen.	Surface devices enrolled in Intune can be located, locked, and remotely wiped in the event that they are lost or stolen.	Some of the data my organization manages is sensitive. How can I ensure that data is secure at the end of a device's life cycle? *Surface Data Eraser and Microsoft Intune allow you to clean all data from a device's hard drive before it is re-imaged and repurposed.*
Will I need to manually update devices?	Microsoft Defender Advanced Threat Protection (ATP) provides evergreen and updated malware protection and digital forensics.	Microsoft ATP is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.	A secure device is great, but what about the rest of my environment? *Windows Defender ATP protects, detects, and responds to threats across your organization's entire environment by reducing the size of your threat surface.*
How can I secure developer environments?	Using the physical Trusted Platform Module (TPM) 2.0 chip, rather than a virtualized environment, inside firmware creates a more secure sandbox.	This physical security component is designed to help generate, store, and limit the use of cryptographic keys.	Some of your users may need higher levels of security, particularly in developer environments. When TPM chips are provisioned, these users benefit from devices that are effectively tamper resistant, and malicious software is unable to tamper with the security functions of the TPM.

[1] Ponemon Institute, *2018 State of Endpoint Security Risk*, October 2018.

[2] A commissioned Forrester Consulting Total Economic Impact™ Study: *Maximizing Your ROI from Microsoft 365 Enterprise with Microsoft Surface*, May 2018.

[3] Forbes, *Your Mobile Phone Is Your Identity. How Do You Protect It?*, August 2019.

[4] The new firmware UEFI interface is used on Surface Pro 4, Surface Pro (5th Gen), Surface Pro (5th Gen) with LTE Advanced, Surface Pro 6, Surface Laptop (1st Gen), Surface Laptop 2, Surface Studio (1st Gen), Surface Studio 2, Surface Book, Surface Book 2. Surface Go, and Surface Go with LTE Advanced. For Surface Pro, Surface Pro 2, Surface Pro 3, and Surface 3, we continue to support standard BIOS.