Microsoft

Roll out new tech like a pro

4 tips for implementing a successful and secure hardware solution

Navigate new device implementation like a pro

Making big IT decisions that affect your department, and organization as a whole, brings up many concerns. When you've been tasked with updating the company's hardware, consider devices that best protect your organization's data with no additional stress.

In this eBook, we will describe four tips to ensure the process is as pain-free for your IT team and end users as possible.

1. Integrate seamlessly
2. Ensure cutting-edge security
3. Be compliant without adding complexity
4. Get tangible hardware control

Rolling out new tech to your company presents a lot of questions:

- What new hardware is needed?
- How does the new hardware integrate with what we already use?
- How much time will a transition take?
- How does the new hardware stack up security-wise?
- Do the benefits of the new tech outweigh the time and resources it will take to implement?

Surface can help you address each tip while protecting company data and easing management complexity.

TIP 01:

Choose devices that... **Integrate seamlessly**

While software is often available from device to device, worrying if you'll lose time or productivity during a hardware transition shouldn't hold you back. Ensure you have access to the best tools and that your devices are up-to-date.

In a world where every minute impacts your bottom line, new device implementation, integration, and deployment should be seamless to avoid unnecessary risk and save valuable time.

Surface is built to take full advantage of the available security features of Windows 10. For example, virtualization-based security provides a safety bubble around your security solutions protecting them from malicious software. The unified updating platform of Windows Update ensures seamless distribution of driver and firmware updates right alongside your Windows updates to keep your system secured on every level.

Confidently integrate with advanced security features

When you're tasked to modernize technology across your company, choose devices that takes full advantage of all the security solutions available. Get everyone up and running without creating additional threats to your organization.

Surface seamlessly integrates with a comprehensive set of Windows security features.

Windows Defender Antivirus

is a built-in antimalware solution that provides security and management for desktops, laptops, and servers.

Cloud-delivered protection detects and blocks new malware in seconds, without waiting hours for a definition update. You can even customize which information is shared with the cloud and how aggressively new files are blocked.

Always-on scanning uses real-time protection, behavior monitoring, and heuristics to identify suspicious or malicious malware activities. These methods can detect activities, like unusual changes to existing files, modifications or additions of automatic startup registry keys and startup locations, or other adjustments to the file system or structure.

Dedicated protection updates based on machine-learning, human and automated big-data analysis, and in-depth threat resistance research ensures that Windows Defender Antivirus stays up-to-date with the latest protection available.

AppLocker

helps prevent malware from gaining access to company devices. Control which apps and files users can run, including executable files, scripts, Windows Installer files, dynamic-link libraries, packaged apps, and packaged app installers. This reduces administrative overhead by eliminating unapproved apps—and the resulting help desk calls.

Protect against unwanted software by adding apps to a list of exclusions or creating rules that only allow licensed software to be downloaded to devices.

Keep track of which apps have access to company information with app inventory management.

Customize policies
by creating specific rules for an individual or group.

Work Folders

stores files, allowing access from almost any device—even when working offline. Not only does this increase security protection by allowing you to centrally store files on a company server, but you can also enable specific user-device policies, such as encryption and lock screen passwords.

Cost saving meets seamless integration

Another common point of discussion when upgrading your company's tech is cost. Sure, upgrades can be costly, but attacks can cost even more in the long run. Choose a premium device, like Microsoft Surface Pro, which is highly mobile, user friendly, and built for Windows 10.

According to data from Gartner, migrating to a Windows 10 device costs

$155 to $242

per system as compared to

$256 to $445

for non-Windows 10 devices.[1]

Surface provides easy, secure deployment for everyone on your team.

TIP 02:

Choose devices that... **Ensure cutting-edge security**

Malware evolves at a breakneck pace and it can be difficult for your IT team to stay up-to-date while providing the best device security possible. With bring-your-own-device policies and a growing mobile workforce, there are more devices for your IT team to manage, often without additional resources.

According to research from the Ponemon Institute, 67% of respondents are unable to detect which employees use insecure mobile devices.[2] Surface enables mobility without creating additional security risks.

With extra protection at the hardware layer, Surface has cutting-edge security features. These let you control hardware configuration and OS processes within device firmware, which is thoughtfully designed to protect data in even the most regulated industries.

Surface protects the user

Are your company's credentials at risk?
Login credentials for websites, computers, and networks are often the first layer of security defense. Unfortunately, without the proper security tools behind the network and hardware, they are an easy point of entry for attacks.

90%

of login traffic on web and mobile applications can be attributed to stolen credential attacks.[3]

3.3 billion

credentials were reported stolen in 2016.[3]

Windows Hello for Business

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.

Because Surface stores this biometric identification data on the device itself, the information doesn't roam and isn't sent to external devices or servers—thus eliminating an attack opportunity.

Advanced mobile device security
has advanced biometrics and login capabilities via facial and fingerprint recognition, as well as dual-factor authentication, your first line of defense against threats.

Hardware control and identity verification
built into Surface hardware is an enterprise-grade identity verification mechanism. It uses a camera specially configured for near-infrared imaging to authenticate and unlock Windows devices.

This camera allows the Surface to conduct:

- Facial recognition
- Single sign-on verification to unlock Microsoft Passport
- Enterprise-grade authentication
- Consistent imaging in diverse lighting conditions

The problem with passwords

End users often repeat or cycle through passwords. A whopping **35% of users** have weak passwords and the remaining **65%** can be cracked, according to Preempt.[4] And according to Microsoft, **63% of breaches** involve weak or stolen passwords.[5] Tracking, managing, and remembering strong passwords is exceedingly difficult, but enterprise security shouldn't be compromised just because of human error.

Windows Hello addresses the following problems with passwords:

- Strong passwords can be difficult to remember, and users often reuse passwords on multiple sites.
- Server breaches can expose symmetric network credentials/passwords.
- Passwords are subject to replay attacks.
- Users can inadvertently expose their passwords due to phishing attacks.

Microsoft Passport + Windows Hello
Windows Hello for Business recognizes users and uniquely identifies and authenticates Windows access on each device. What the user does not see is that Windows Hello releases a stored credential that is used as the second authentication factor by Microsoft Passport.

TIP 03:

Choose devices that... **Support compliance without adding network complexity**

A lot of businesses need to follow strict compliance standards, from healthcare's HIPAA regulations to banking and education standards. In the past, you often had to turn to third-party applications to achieve the required high-level compliance with standard hardware—leading to higher levels of complexity for your IT team to navigate.

According to a Verizon report, 80% of businesses failed their interim compliance assessments for meeting Payment Card Industry (PCI) security standards.[6] These mistakes can be costly for your organization; PCI compliance violations can result in fines of $5,000–$100,000 per month.[7]

Surface has built-in features that can help your organization meet government-level compliance standards.

Built-in peace of mind

Devices that come with capabilities to meet government-level compliance standards reduce the demand on your IT department and provide peace of mind. Surface is specifically designed to meet this level of security.

- A top technique for attackers is gaining access through device browsers. Microsoft Edge has been designed to systematically disrupt phishing, malware, and hacking attacks. This allows employees to still browse the web as needed to complete their work, but protects your organization against threats.
- Microsoft Intelligence Security Graph and the human expertise behind it provides an additional layer of security for your organization's data with IOCs powered by sensors and unique optics.

Compliant enough for the NSA

The NSA recently added Windows 10 and Surface to the Commercial Solutions for Classified Programs.[8] According to the listing, Windows 10, as well as Surface devices, when used in a layered solution, can meet the highest security requirements for use in classified environments.

Surface Data Eraser

boots from a USB stick and allows you to perform a secure wipe of all data from a compatible Surface device. If you're locked out of a device or need to wipe one for whatever reason, you're able to do so securely and safely. This reduces the amount of time it takes to wipe a device, whether reclaiming it from a former employee or sending it out for repairs.

Microsoft BitLocker Administration and Management

provides enterprise management capabilities, simplifies deployment and key recovery, provides centralized compliance monitoring and reporting, and minimizes the costs associated with provisioning and supporting encrypted drives.

TIP 04:

Choose devices that... **Allow tangible hardware control**

In today's tech space, every IT professional is on the front line of the organization's cybersecurity.

This doesn't mean they're only protecting your organization against phishing scams or malware from your Internet browsers. Built-in peripherals, such as a camera, USB ports, and microphones leave your important information open to threats if not properly protected and monitored.

Even the most tech-savvy employees can fall victim to an attack. According to a study conducted by the University of Illinois, the University of Michigan, and Elie Bursztein, 48% of people who picked up a dropped USB drive plugged it into their computer.[9] It may not cross a user's mind that this seemingly innocent act could be malicious, but it can leave your organization open to serious security threats.

By adding Surface to your toolbox to properly protect against—and react to—threats, you can better protect your company's data.

Cloud control protects against peripheral threats and allows you to actively monitor peripheral security and either proactively disable their use or react efficiently if a breach is detected. Windows Defender combines sensors built into the operating system with powerful cloud security, adding an additional protection to peripheral threats on devices themselves. The security analytics cloud detects attacks that have made it past all other defenses, using both behavioral and machine learning detections over new and historical information to identify attacks.

Protecting your organization's hardware is seamless with Surface devices, which you can manage and monitor from virtually anywhere.

Surface Enterprise Management Mode (SEMM) enables customers to manage firmware settings for their Surface devices including disabling HW such as USB ports, cameras etc.

Confidently implement a secure hardware solution

Making tech decisions for your organization is challenging, and without the right tools, organizations are at risk for costly security breaches. That's why you must choose devices that integrate seamlessly, ensure up-to-date security, come with built-in features to help your organization meet government-level compliance standards, and have tangible hardware control. Select a solution that can cover all your bases.

Surface is designed to address each tip, and more. Implement today.

See which Surface products are right for your business.

→

Sources:

1. "Making Critical Deployment Choices for Windows 10 Success," 2016, Gartner
2. "The Cost of Insecure Mobile Devices in the Workplace," 2014, Ponemon
3. "2017 Credential Spill Report," 2017, Shape Security
4. "35% of Users Have Weak Passwords; the Other 65% can be Cracked," 2017, Preempt
5. "Designed to be the most secure Windows yet," Microsoft
6. "PCI Compliance Report," 2015, Verizon
7. "PCI Noncompliance Consequences," 2017, Payment Card Industry Data Security Standard (PCI DSS)
8. "Commercial Solutions for Classified Program," NSA
9. "Users Really Do Plug in USB Drives They Find," 2015, University of Illinois, the University of Michigan, and Elie Bursztein via Elie.com

Microsoft
Surface