Microsoft Surface

A Modern Blueprint for Endpoint Protection

Ask yourself:

Imagine that a senior employee's laptop is stolen. It could be industrial espionage. Are the security precautions you have in place today sufficient to stop the thief from extracting valuable information or credentials from the laptop?

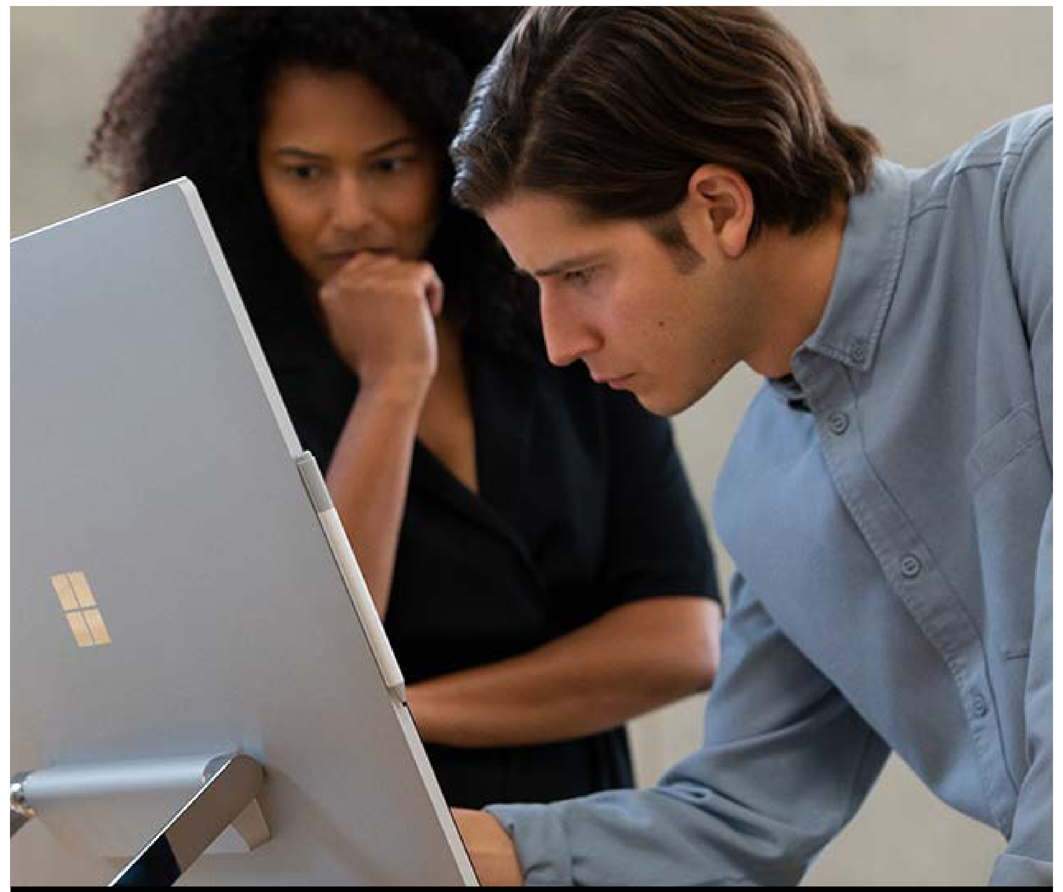
Digital transformation and the changing workplace are shining a light on two intersecting trends: the variety and volume of endpoint devices, and the need to secure data and systems wherever they reside. No surprise, then, that improving security is a top driver of IT investments in the year ahead, rising steadily in importance over the last three years[1].

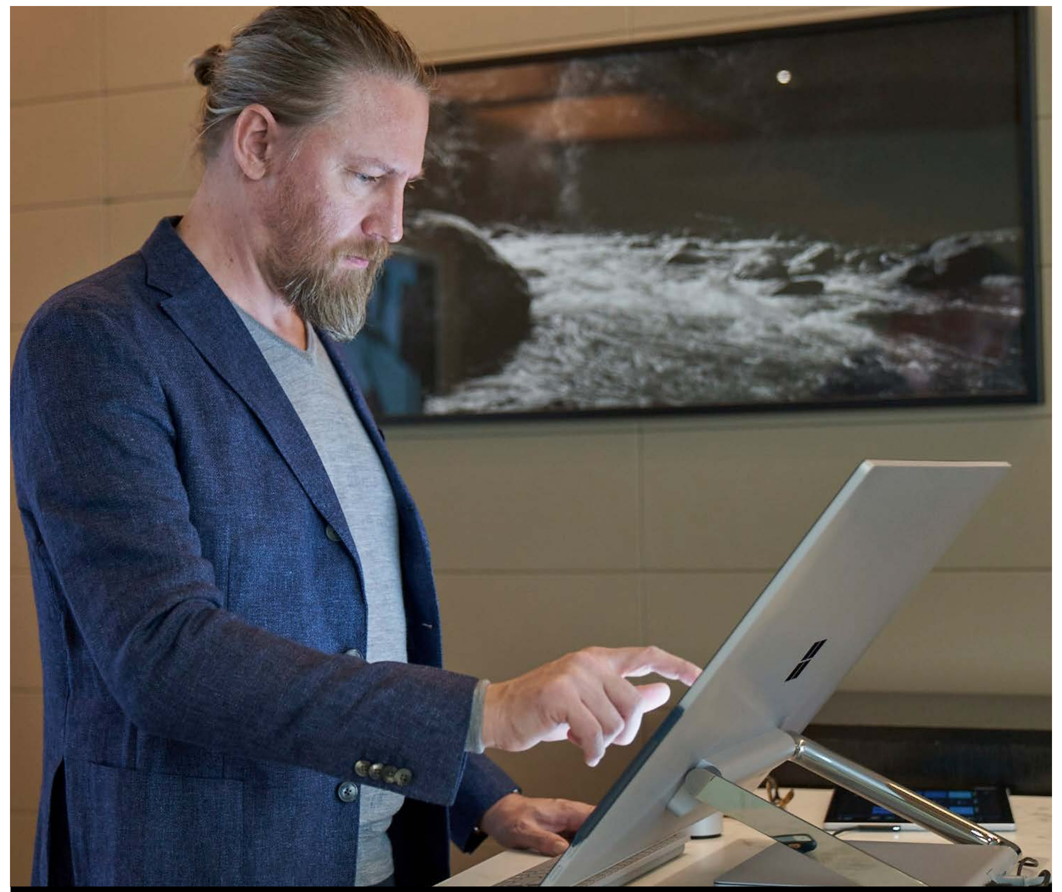
Securing endpoints and the data they contain is becoming more urgent, yet just 27% of organizations in IDG's 2019 Digital Business survey say they've completed a strategy for data protection[2]. Organizations that are lagging are likely to fall further behind as the volume and scope of endpoint devices continue to grow.

As security becomes table stakes for digital business, IT and security teams are working more closely than ever to identify threats and vulnerabilities proactively across the entire IT architecture. Nearly two-thirds (64%) of respondents in the State of the CIO survey say security is tightly integrated with IT strategy, a figure expected to jump to 82% in three year[3].

This collaboration is likely to impact all technology purchasing decisions, including desktops, laptops, and other endpoint devices, which present some of the most vulnerable entry points to bad actors. Security teams understand the need to modernize endpoint security methods, moving beyond traditional methods such as firewalls or antivirus software. Modern endpoint security has a long reach, from the device firmware up to the cloud, across all phases of the device lifecycle, with an emphasis on user privileges, prompt updates, and encryption of data in transit and at rest. In this e-book, we provide an overview of the key components of an endpoint security strategy: the device itself, access to the device, and device deployment and management.

Table of contents





What is an endpoint?

Mobile devices running iOS and Android are obviously an enormous presence in business today, but their capabilities and vulnerabilities are still a fraction of those of desktop and laptop computers. The management and security of mobile devices generally is handled separately from desktops and laptops, but there is clearly a movement toward consolidation.

Traditional Windows administration is done using Microsoft System Center Configuration Manager (SCCM) or a similar third-party system running on-premises. But new products, including Microsoft Intune, adopt the Mobile Device Management (MDM) model of moving this function into the cloud. The benefits for deployment and management generally are clear, and described in greater detail in this e-book.

?
1
2
3
...

Inside the endpoint device

Modern Windows-based devices, such as Microsoft Surface, contain sophisticated, mature hardware and firmware designed for securing the device and the software that runs on it. An optimal security strategy takes advantage of these features and empowers administrators to control even the lowest level of hardware settings without having to touch the machine.

TPM and UEFI

The two most important device components are the Trusted Platform Module (TPM) and the Unified Extensible Firmware Interface (UEFI).

TPM is a crypto-processor that is resistant both to physical tampering and the efforts of malicious software to change or interfere with it. TPM can generate, store, and control the use of cryptographic keys. It comes with a unique, embedded, and unchangeable RSA key that provides strong device authentication.

UEFI is a standard for a much more sophisticated version of what we used to call BIOS (Basic Input/Output System), the ROM in the PC used for booting and certain hardware access. **The UEFI is a mini-operating system itself, whose job is to load the operating system.** An implementation of UEFI, conforming to the specification, is delivered by the device manufacturer. But UEFI is itself extensible (the E in UEFI) by the manufacturer and the operating system.

? 1 2 3 ...

Like all other modern technology, TPM and UEFI are updated from time to time. Because they are so important to the security of the system, it is essential that the manufacturer provide the means for applying updates and that administrators have the ability to distribute these updates.

Most manufacturers buy a UEFI from a third-party vendor, which provides updates to the manufacturer, which in turn distributes these updates to customers. The UEFI in Surface devices, by comparison, was written by Microsoft, so updates to it are pushed to the customer automatically through Windows Update for Business rather than having to be manually pulled by IT and packaged for delivery to users. This makes updates not only more timely, but also more likely to be applied.

The importance of quick UEFI updates became clear following a spate of speculative execution side-channel attack vulnerabilities, including Meltdown and Spectre, two chip-level flaws discovered in early 2018 that could allow attackers to access data previously considered completely protected. A variety of updates to operating systems, web browsers, and compilers followed, but updates to the UEFI were crucial to mitigating the threats.

By the numbers

5B Number of threats detected on devices monthly.

Source: Microsoft Security Blog, "The evolution of Microsoft Threat Protection, June update," June 2019.

Key takeaway:

Make sure your endpoint devices can be managed and updated down to the UEFI level efficiently to mitigate a critical vulnerability point.

?
1
2
3
...

Secure, Trusted, and Measured Boot

When a PC with UEFI and TPM boots up, it first verifies that the bootloader was digitally signed with a trusted certificate from among those stored in the TPM. This process is called Secure Boot, and it is designed to prohibit unauthorized software from running at boot time.

A manufacturer will typically preload the TPM with their own certificates, that of the UEFI author, and those provided by Microsoft. An administrator can load other certificates if they wish to run other trusted operating systems. Certified-for-Windows PCs must have Secure Boot enabled by default. They must trust Microsoft's certificate, and allow the user to configure the system to trust other bootloaders and to disable Secure Boot completely. After Secure Boot, Trusted Boot takes over. The bootloader verifies the digital signature of the Windows 10 kernel before loading it. Windows 10 then verifies all parts of the Windows startup process.

These measures provide substantial protection against boot-stage malware, mostly called bootkits and rootkits, and tampering with boot software. One example of this type of threat is the LOJAX malware, a UEFI rootkit found in the wild in 2017[5].

Boot-stage protections don't stop there. **Attackers may also attempt to compromise a device with malicious software designed to launch in the early stages of Windows boot.** One example of this is ZeroAccess, a Windows driver-level rootkit that used encrypted NTFS alternate data streams for storage[5].

To counter this threat, Measured Boot is a process that can run before the loading of an anti-malware product, providing further assurance that the boot process hasn't been compromised.

During startup, the UEFI stores a hash of all the software loaded before the anti-malware software in the TPM. After startup, Windows starts a remote attestation client, and a remote attestation server sends the client a unique key. The TPM uses this key to sign the log recorded by the UEFI, including the hash it created. The remote attestation client then sends the signed log, possibly with other security information, to the server. Software on the server, or working with it, can analyze the logs for suspicious behavior.

At this point, the operating system and other security products can monitor other software that loads before and after the user signs in. Multiple protections of the boot process using different methods is not an overreaction, as we know from LOJAX.

A successful infection by this malware would not necessarily be blocked by Secure Boot, but other measures, such as a hardware root of trust enforced by the CPU, would be.

?
1
2
3
...

By the numbers

391.1M Total shipments for PC devices in 2019, including desktops, notebooks, workstations, and tablets.

Source: IDC press release, "Personal Computing Device Shipments Forecast to Continue Their Slow Decline with a Five-Year Compound Annual Growth Rate of -1.2%, According to IDC," March 2019.

Key takeaway:

Advanced malware that runs before the OS boots is a real threat and can be difficult to remove. Best practices and the latest in security technology, like that found in Microsoft Surface devices, can prevent it from infecting in the first place.

The Importance of software updates

Updating operating system and application software is obviously a crucial part of any well-designed plan for endpoint security. Windows Update for Business and Microsoft System Center Configuration Manager (SCCM) let you manage this process while getting updates to users as quickly as possible.

The same considerations mean that you should make a practice of retiring old and insecure products, such as old versions of Windows and Office, and replace them with modern versions that are automatically kept secure and up to date.

?
1
2
3
...

Access to the endpoint device

?
1
2
3
...

For most organizations, the primary protection for employee devices (and their email and other accounts) is a password. It has been clear for a long time, however, that passwords are not the best solution to the problem of authentication. Millions of username and password combinations have been stolen from websites. Your users are probably using some of them on your network, creating easy points of entry for attackers.

New technologies make it possible for passwords to be required rarely, if at all. Eventually, you should be able to remove passwords from your identity directory entirely – eliminating a significant vulnerability.

Authentication is stronger when it involves more than one authentication factor, and in particular, more than one type of factor.

Multifactor authentication dramatically reduces the risk of many forms of attack, including phishing, a common method for attackers to gain initial entry to a network.

A variety of other established methods provide strong authentication without the limitations of passwords. These include biometrics, smart cards, and authenticator apps.

The classic factor types are:

Something you know:
Usually a password.

Something you have:
Can be a digital certificate, smart card, or some other hardware token.

Something you are:
A biometric, generally a fingerprint or facial recognition.

? 1 2 3 ...

Biometrics

Biometric authentication products are growing in both availability and sophistication. Windows 10, for example, includes Windows Hello for Business, which authenticates the user with a biometric or a PIN. These credentialsare tied to the device and stored in the TPM.

This means that, in order to access a device protected by Windows Hello for Business, you must have the actual device and either the PIN or biometric. It also means that you need different PINs for different devices, but it limits the damage that can come from a compromised PIN. It also means that if you can't use a biometric (e.g., you have a bandage on the finger you use for fingerprint recognition) you can just use the PIN. Note that Microsoft stores no biometric data in the cloud.

By the numbers

$11.2B Value of the global endpoint security market in 2018, with 9.9% annual growth projected through 2024

Source: Mordor Intelligence, "Endpoint Security Market - Growth, Trends, and Forecasts (2019 - 2024)," undated.

Key takeaway:

Biometrics are a strong form of authentication. You may forget a password or lose a hardware token, but you always have your face with you.

?
1
2
3
...

Smart cards and FIDO devices

The strongest form of "something you have" authentication is a cryptographic hardware token. These inexpensive devices contain crypto-processors that can sign data digitally with a secure private key, which can then be validated by the system with the corresponding public key. Smart cards are credit-card-sized tokens that the user inserts into a special reader.

A laptop or other device protected in this way cannot be used without the hardware token. This approach would mitigate concerns that arise when a laptop with unencrypted data is lost or stolen.

It's possible to use a digital certificate stored on a portable device, like a USB key, as an authentication factor, but the state of the art in this space is in small hardware devices using the Client to Authenticator Protocols (CTAP) (formerly Universal 2nd Factor or U2F) standard to connect to the system via USB, and the FIDO2 authentication standard. FIDO ("Fast IDentity Online") standards are defined by the FIDO Alliance, an industry association whose mission is to develop authentication standards as a more secure alternative to passwords.

Many companies supply FIDO-certified products. Some of them incorporate a fingerprint reader, thus allowing for easy "something you are" to go with the key's "something you have." Microsoft's Windows Hello and Windows Hello for Business are certified as FIDO2-compliant.

By the numbers

64% Percentage of organizations experiencing one or more endpoint attacks that successfully compromised data assets and/or IT infrastructure.

Source: Ponemon Institute, "The 2018 State of Endpoint Security Risk," October 2018.

Key takeaway:

FIDO devices require the user to have the device with them, but they are the cutting edge of inexpensive authentication.

?
1
2
3
...

Smartphone-based authentication

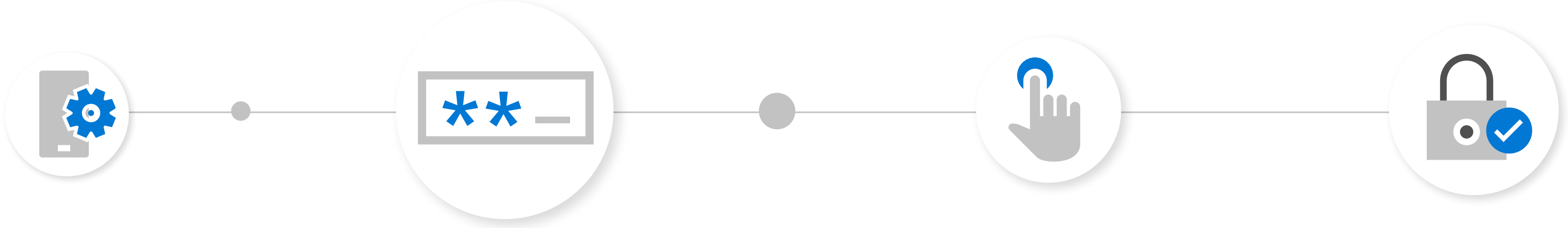
Another solution is to use a smartphone as an authentication factor. The best way to do this is to use an authenticator app, such as Microsoft Authenticator. When the login process asks for an authentication code, the user goes to the authenticator app and looks up the code for the service they are logging into.

An older and less-secure alternative is to have the service send a validation code via SMS text message to the user's phone, which they then enter into the service they are logging into.

A hardware token has additional physical and cryptographic safeguards that make it the most secure complement to biometrics, but any second factor added to authentication will add significant protection to the resources behind the login. Authentication factors can prevent many of the common phishing schemes used to access payroll or other systems.

Key takeaway:

Virtually everyone has a smartphone that can be used for authentication, although these methods are not generally as reliable for authentication as biometrics.



Deployment, redeployment, retirement

?
1
2
3
...

Zero-touch device deployment

Endpoint security continues throughout the device lifecycle. Deploying and managing hardware devices used to require that IT develop and maintain system images for every device type they supported. Then, for each individual system, a technician in-house or at the device maker had to wipe the hard drive and apply the proper operating system image to it before sending it on to the user, ensuring that the approved software and policies were set on it.

Intelligent cloud services make this time-consuming step unnecessary. **Windows AutoPilot, for example, automates all stages of the device lifecycle, both for IT and users. The device can go straight from the manufacturer to the customer and the security process begins when you purchase new equipment.** The hardware vendor sends a file containing the hardware IDs of the new equipment. IT uploads these IDs into the Windows AutoPilot deployment service using an Active Directory administrator account and claims ownership of those devices for the organization. After the first such operation, the hardware vendor can perform this step on your behalf.

Next, the IT administrator creates a deployment profile in AutoPilot and assigns it to the devices. You can create a default profile and profiles for groups and individuals. This profile customizes each person’s setup experience, including whether they are allowed a local administrator account. At this point, you can ship the device directly from the hardware vendor to the user.

?
1
2
3
...

By the numbers

$440 Average cost per compromised endpoint due to the loss of IT and user productivity and theft of information assets.

Source: Ponemon Institute, “The 2018 State of Endpoint Security Risk,” October 2018.

Key takeaway:

Maintaining system images is a burden for IT regardless of security concerns. Cloud-based deployment speeds the process while enhancing device security.

Self-service setup

When the user turns the device on and goes online, the setup begins. **Windows AutoPilot recognizes that the device belongs to your organization and delivers the setup experience created for it.** The user logs in with their organization email address and whatever other authentication factors the company requires, automatically enrolling in Mobile Device Management.

At this point, the device is set up with Microsoft Intune for management, and Intune begins to push policies and software to the device. Many of the typical questions, such as those having to do with configuration and registration, are bypassed because the deployment profile has answered them already. With just a few clicks, the device is ready to use and IT has not had to lay a finger on it.

After a conventional “out of box” experience, the user is signed in as a local administrator. Using Windows AutoPilot, by comparison, allows the user to set up the device and be logged in with a standard account, which automatically removes many avenues of attack on the system.

?
1
2
3
...

Streamlined, yet secure setup

If the hardware allows it, as with Microsoft Surface devices, IT can enable or disable individual features as part of the setup. This includes the cameras, Micro SD card, Bluetooth, LTE, whether the computer can boot off of a USB device, and many more. **In Microsoft Surface devices, this capability is called Surface Enterprise Management Mode (SEMM).** This approach minimizes the impact of remote-access trojans and other methods that enable attackers to take control of device components.

Using Microsoft Intune, IT also can wipe a device clean, either because it was lost or stolen or to assign it to a different user. After the wipe, it is reset to the out-of-box experience, at which point proper credentials are once more required for set-up.

Key takeaway:

All phases of the product lifecycle are opportunities to strengthen endpoint security. The best tools, like Microsoft AutoPilot and SEMM, allow IT to automate robust security practices across each phase.

Summary

The IT industry has learned the hard way that there's no substitute for defense-in-depth. There should be no one thing that can go wrong that results in the compromise of a system or important data. Better still, there should be no two things that can go wrong, and so on.

?
1
2
3
...

Secure from chip to cloud

Even the most secure enterprises can be penetrated, but by the same token, even the most talented and resourceful hackers can be defeated. The way to do this is to put impediments in their way at every step.

At the endpoint, you do this by managing the device thoroughly from the beginning of the lifecycle, removing privileges not needed by the user, applying updates to all levels of software promptly, and encrypting data both in transit and at rest.

Modern endpoint systems and the software for managing them make such control practical, without the need to restrict users' ability to get their work done. Microsoft Surface and management systems like AutoPilot are examples of the state of the art in such technologies.

Nothing connected to the Internet is impregnable, but modern tools and best practices enable businesses of any size to provide a high level of protection, both from sophisticated attackers and user error.

Ensure your devices are secure

Let's revisit the thought exercise we proposed at the beginning of this e-book.

- **Are the hard drives on your laptops encrypted at the device level using keys in the TPM?**
- **Does signing in to the device require multiple factors?**
- **Is the thief prevented from booting a new operating system from a USB drive?**
- **Is he prevented from going into the UEFI settings and changing them?**

You never want to assume that it's impossible to hack the device, but with these steps, you've made it a much less attractive target for bad actors.

?
1
2
3
...

Ready to get started?

In an age of rising security threats, businesses need protection across multiple layers. From chip to cloud, Surface considers the most secure device capabilities available and continues to innovate to meet the evolving needs of customers. With built-in protection at every layer, Surface implements every standard for a highly secure Windows 10 device. With Surface, you can be confident that you have the best, most streamlined implementation of Microsoft's security stack.

Find a reseller >

Sources
[1] 2019 State of the CIO study, CIO.com
[2] 2019 Digital Business Survey, IDG
[3] 2019 State of the CIO study, CIO.com
[4] ESET Research, September 2018
[5] ZeroAccess botnet, Wikipedia