Introduction to Windows 10

SECURITY

by Onuora Amobi

Legal Notice

While all attempts have been made to verify information provided in this publication, neither the author nor the publisher assumes any responsibility for errors, omissions or contradictory interpretation of the subject matter herein.

This publication is not intended to be used as a source of binding technical, technological, legal or accounting advice.

Please remember that the information contained may be subject to varying state and/or local laws or regulations that may apply to the user's particular practice.

The purchaser or reader of this publication assumes responsibility for the use of these materials and information.

Adherence to all applicable laws and regulations, both federal, state, and local, governing professional licensing, business practices, advertising and any other aspects of doing business in the US or any other jurisdiction is the sole responsibility of the purchaser or reader.

Nnigma Inc. assumes no responsibility or liability whatsoever on behalf of any purchaser or reader of these materials.

Table of Contents

Introduction to Windows 10 Security

Security has always been an issue for computer users. However, over the last couple of decades, security threats have become much worse.

While you may think you have the best security system possible on your PC it is likely that you probably don't. Why? Because the landscape of cyber-threats is changing too fast for ordinary security software to keep up with.

Heck, you could buy a new security system for your computer right now and within 72 hours; it would require a security update.

Cyber threats are becoming more complex and attackers more cunning. Viruses and malware for example, have gained new abilities to hide and remain undetected.

Cyber-attacks are more sophisticated and highly targeted compared with years ago when hackers could only hope for indiscriminate and unfocused damage.

In the early days, we had Script Kiddies, which were aimed at causing mischief rather than damage.

Today criminal gangs conduct crimes such as click fraud and ID theft, conducted purely for illicit profit. We also have activists and the Internet terror groups whose sole aim is to cause as much disruption and damage as they can, as well as steal identities.

In the midst of this very treacherous landscape, Microsoft has taken up the challenge of keeping computer users safe. With Windows 10, the software company is introducing unprecedented levels of security safeguards into the very fabric of the Operating System.

I wrote this book because I wanted to take a brief look behind the curtain to see what types of security were embedded in Windows 10.

Here's what I found.

Microsoft and the FIDO Alliance

The FIDO (Fast Identity Online) Alliance was launched in 2012 as a way of addressing the lack of interoperability between strong authentication devices and the problems users have in remembering multiple usernames and passwords.

PayPal and Lenovo, two of the biggest names in the industry, were founding members of FIDO. In just over a year after launch, many more big names had joined the alliance, including Google, Blackberry, Visa, SecureKeys and of course, Microsoft.

So, how does the FIDO Alliance factor into Windows 10?

To get to that, we need to go back a step or two, to talk about why Microsoft opted to join the Alliance.

Security problems on our devices are getting worse, partly because of the significant jump in malicious attacks and partly because of user behaviour.

You see, it often comes down to passwords. Computer users often get sloppy and lax, and share their passwords with others.

That isn't the only problem, though; the next part of the puzzle involves the websites we visit. The issue is not that they are unsafe because most of them are safe. It's just that, once

again, that lazy gene comes out and we stick to using the same password for every single site that we have to log into.

Why do we do that?

Because not only is it time-consuming to have to come up with a different complex password for each site, we have to remember them as well. The human brain can only hold so much information and to help us out, we write those passwords down – **which comes back to being lax and sloppy about security.**

Because we are using the same login details for every site, it makes it easy for those details to be stolen. A malicious attacker will go for a weak website, one which doesn't have so much security on it, and once they have your details from that site, it doesn't take a genius to guess that you probably used the same ones to login everywhere else!

That gives the attacker an open pass, a master key if you like, to everything you have access to.

The final piece of the puzzle, one of the weakest links, is the device that you are using. It's not that it's no good, it's just that, up until now, any application would run on your app, regardless of content, until it was proven to be a bad apple.

The only way that app would not run is if your anti-virus software or firewall picked it up and kicked it out. Not everyone has antivirus software installed or they don't use the one that is already provided with Windows. That means that so much malware gets through the net that once it starts, it is difficult to stop it.

So how does Microsoft intend to fix this? The current PKI (public key infrastructure) is way too expensive and complex to maintain, and it is constantly under attack. The current CA (certificate authority) system is also under attack.

An attacker can get to your certificate details before your IDP (Identity Provider) can give you a token, and that leaves every door in the house wide open. And, if that weren't enough, limited use of MFA (multi-factor authentication) leaves weak spots everywhere, weak spots that take little effort to get through.

In Windows 10, Microsoft is making it easier for you to log in while tightening the security net with MFA.

With a combination of **biometrics**, **PIN access** and **tying asymmetrical key pairs to a specific device**, Microsoft is aiming to make it so that no one else, except for you, can access your resources and your applications.

With Windows 10, Microsoft is bringing to market the next generation of user credentials. We'll run through them one by one in this book.

The comparison to Windows 7 and 8 Security features

Microsoft had to take a new approach to Windows 10 security for a couple of reasons.

First, security problems and challenges continue to evolve rapidly, and it was clear that there were new challenges that needed to be solved.

It was also clear that some of these challenges were a little bit more sophisticated than Windows 7 and Windows 8 were designed to handle.

To give you a quick overview, take a look at the table below, showing you the fundamental differences in security between Windows 7 and Windows 10:

Function	**Windows 7**	**Windows 10**
Identity Protection	Password theft is too common now and current multi-factor solutions are simply too expensive and too difficult to deploy.	Comes complete with an easy-to-deploy multi-factor solution, complete with anti-phishing and anti-theft features. Password-protection and PINs are included in multi-factor security solutions.
Data Protection	Offers the option of configurable disk encryption but doesn't have integrated Data Loss Prevention (DLP). Can use third party solutions but not always successful.	Has market leading disk encryption, very manageable and increased out-of-band (OOB) security updates. Data separation and DLP is fully integrated.
Threat Resistance	Apps are always trusted until they	Desktop machines can be locked down

	are a threat, and there is no way of detecting thousands of new threats that appear every day.	to a mobile level. There is the ability to have a trusted app model where those apps that are untrusted cannot run.
Device Security	The platform is securely built, but built on software alone, meaning malware can hide from security, embedding itself in devices.	The platform is built on integrated hardware and software security and offers protection from being switched on to being shut down. There are no possibilities for system tampering and malware has no place to hide.

Basically Microsoft took a holistic look at security and decided to attack some of the fundamental security flaws and challenges from a deep architectural perspective.

With Windows 10, Microsoft has implemented a wide variety of security solutions that protect both your software and the hardware:

- Windows Hello and Windows Passport handle ID protection.
- BitLocker and Enterprise Data Protection handle data protection.
- Device Guard and Windows Defender protect against multifaceted threats.
- UEFI Secure Boot, TPM 2.0 and Virtualization keep your hardware safe.

Let's take a closer look at each of these solutions.

How Microsoft Windows 10 Will Protect Your Identity

First up is identity protection. Identity theft is the one thing that concerns computer users the most.

Every day, more stories are published about people whose identity has been stolen and used to commit fraud and, that, quite understandably, make consumers nervous. Windows 10 looks set to make users feel good about using a computer again, to make them feel secure.

Windows 10 – Protecting Your Identity and Controlling Access

The next topic of discussion is a new solution to protect one's identity, a solution that leaves behind the old fashioned use of single factor authentication, like passwords. It is a solution that protects you when a breach happens in the data center.

It also protects your data from being stolen if your device happens to be compromised and it stops phishing attacks in their tracks.

Once you are enrolled in the system, your device becomes one of the two factors that you need for authentication; the other is a PIN number or biometric information, such as your fingerprint.

The systems in question are Windows Hello and Windows Passport, two systems that work together to provide the ultimate in identity protection. Let's go a little deeper and examine what each system has to offer.

This security solution benefits consumers and business users alike and provides the convenience of using a password without all the hassle of having to remember it or forgetting who you gave it to. Microsoft is taking security to a whole new level to bring its customers complete identity protection with multifactor authentication.

Let's take a look at the systems that Microsoft chose to use and why they chose them. First, biometrics. What is it exactly? Biometrics is the study of biological characteristics that can be measured. In computer security, biometrics is increasingly used to make it more difficult for systems to be hacked through the old-fashioned password system.

The biometrics in this instance refer to physical characteristics that can easily be checked against what information is stored in the system. There are a number of ways that biometrics are used for authentication:

Facial: the analysis of different facial characteristics

Fingerprint: analysis of the unique fingerprints of each person

Hand Geometry: the shape of the hands and the finger length

Retinal: analysis of the capillary vessels at the rear of the eye

Iris: analysis of the colored ring surrounding the pupil in the eye

Signature: how a person signs his or her name

Vein: pattern of the veins on the back of a hand and in the wrist

Voice: tone and pitch of a voice, as well as the frequency and cadence

Biometrics is still a relatively new development but it is fast becoming the way to go with computer security systems.

The Pros and Cons of Biometrics

There are pros and cons to every form of biometric authentication. Given that Microsoft has chosen to adopt this as a security measure, it is important to review the arguments for and against the use of the new technology.

The arguments for using it for network access revolve mainly around three key areas. The first and perhaps the most obvious is that biometric authentication uses attributes that are unique to the individual, making it the ideal form of security.

The second argument for using biometrics is that users will no longer be able to forget their passwords, or share them with others, knowingly or inadvertently. Password administration systems and overheads are considerably reduced as well and this is one of the driving factors in adopting biometric authentication.

The third argument is that it will be incredibly difficult for a person's biometric characteristics to be replicated, far more difficult than it is to replicate a password or user ID. Also, whereas tokens can be stolen or lost, biometric characteristics cannot.

Arguments against the use of biometrics are many, showing just how controversially it is viewed in some quarters. First and foremost, it is still expensive to implement biometric authentication measures, meaning that many organizations cannot afford it.

The cost of both the hardware and software required may be prohibitive to many, along with cost of integrating it with current systems in place.

There is also the argument that right now, biometric systems are only suited to simplistic networks. This is paired with some current thinking that, as an all-or-nothing technology, it may not suit many organizations at this stage.

All-or-nothing means that you can go to the expense of having biometric authentication on every single computer on the network, but it counts for nothing if a user can log on to the system from a remote location without needing to use it; that would undermine everything

and make the expense a complete waste of time.

There is also the argument that the storage of biometric information is an invasion of privacy, but those in favor of it say that it is only a representation of the data, not the original data that is being stored.

Of course, there is another angle to this – given the rate at which a successful technology will spread, there is concern that, should a user's biometric data be compromised, not only does it affect network security, that data could also be used for a large number of illegal activities.

One final but significant concern is that using biometric data is not the same as using a key and does not have the same random, secret nature of a key.

Neither does it have the ability to update and destroy itself. If a person's biometric data is compromised, it is not a simple case of issuing new biometric data – clearly that can't be done!

So, given all the controversy surrounding the use of biometrics for security, why has Microsoft opted to adopt it?

The simple answer is reliability. The consequences of having a system that runs using old-fashioned methods can be damaging, with confidential information stolen and data integrity compromised. Also let's face it, many of the applications we use in our daily lives require some form of authentication.

As far as Microsoft is concerned, by using biometric authentication to get into Windows 10, you can also use it to access all your Microsoft accounts and apps – there isn't a need to

remember separate passwords for each app.

Passwords can be stolen or replicated, biometric information cannot. In addition, biometric information can be positively linked to a specific person – for example, a credit card can be used without the actual user being there, whereas biometrics requires you to be at the computing device to log in.

Windows 10 is set up to provide modern biometric capabilities that allow users to easily unlock their devices and to unlock NGC – Next Generation Credentials – for a much more improved and secure password-free existence.

The Internet can be a hostile place and consumers want a safer, more reliable experience and a better authentication system than we have now.

They want a system that is secure; a system that leaves passwords in the dust, yet still gives them access to everything they need. With Windows 10, Microsoft set out to do just that, setting out a series of goals they wanted to meet:

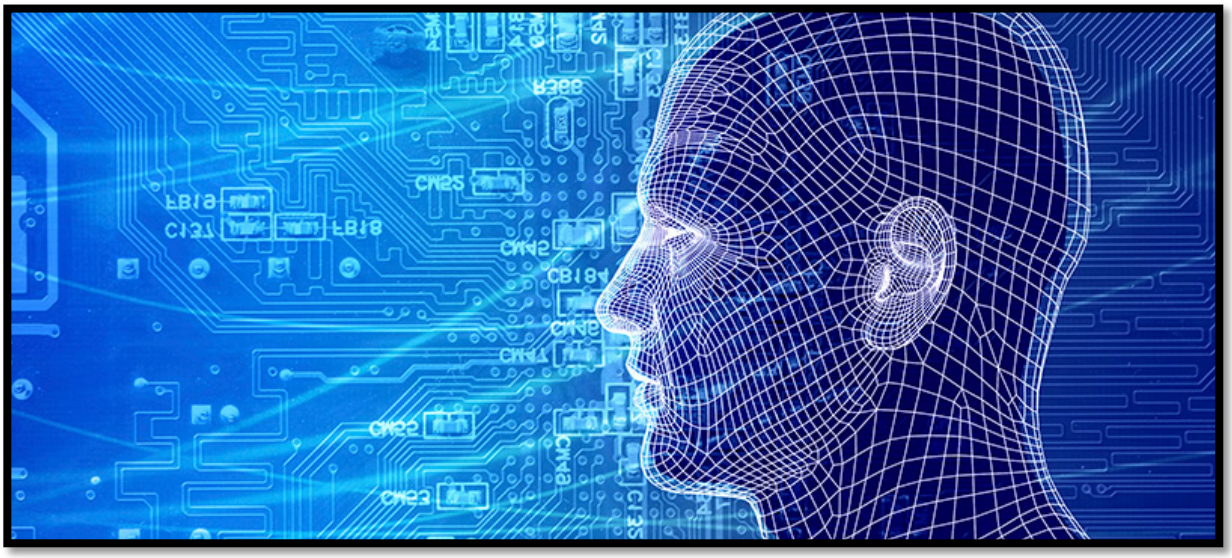
- To enable both consumers and enterprise users to be able to unlock their devices, make payments and secure their content – all without using a password and in a more secure way
- To develop hardware solutions that, at the very least meet, if not exceed, the expectations of the customer, hardware that is robust and easy to use
- To deliver biometric devices that are innovative and give the customer value

To this end, Windows 10 has been developed to support a wide range of biometrics – fingerprint, facial or iris recognition-whichever suits the user best. Special hardware is required to support this and those devices that meet the requirements of Windows 10 for biometric authentication will benefit in a number of ways:

- Easy and convenient logon and very strong authentication
- Enterprise level security with access to HBI (High Business Impact) resources
- Consistent inbox enrolment and usage across Windows enabled biometric devices

In addition, Windows 10 also supports an inbox Face Authentication solution that is available for all OEMs that provide the supported hardware, without the need to rely on third parties.

Facial Authentication



Windows 10 brings a new level of Face Recognition to the table; a system that allows for the easy authentication and unlocking of Windows devices, as well as access to content that is NGC-supported.

This is all without the need to use passwords or any additional authentication factors.

Features:

Windows 10 Face Authentication features include:

- An interface that is user-friendly, providing the capability for single sign-on. There is no need for the use of passwords as well, or any other authentication credentials.
- Enterprise grade authentication, as well as access to NGC supported content – network resources, purchased content and websites.
- Anti-spoofing measures are included to eliminate the chance of physical attack – no one except you can log on to your system.
- Using Clean Infrared, clean and consistent images can be produced, even in diverse lighting situations. The system also allows for slight changes in appearance, such as the addition or removal of facial hair, makeup, glasses, etc.

Use Cases

There are three primary use cases for Face Authentication:

1. **Authentication needed to unlock or login**

On average, the system takes less than 2 seconds to recognize your face, although it may take up to 30 seconds – but no more than that. This is expected to be used at a high frequency since it is required whenever a user needs to authenticate their device and get past the lock screen.

2. **Authentication to Purchase**

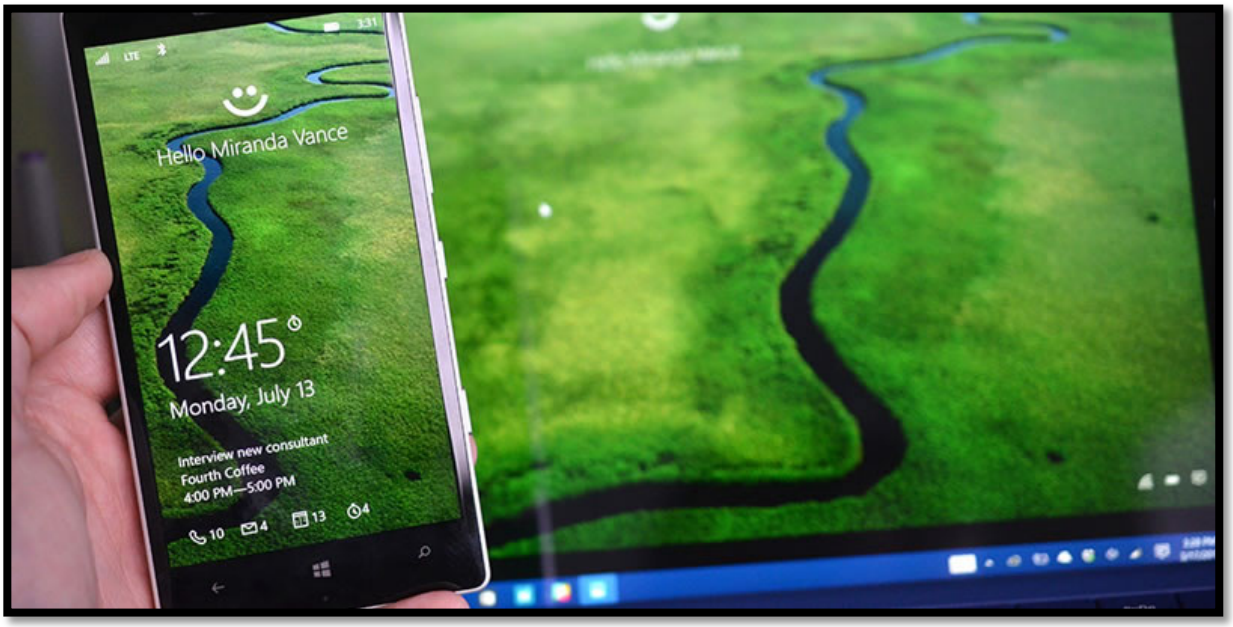
On average, the system will recognize a face in less than 2 seconds, but up to a maximum of 30 seconds. This is required every time an application needs a user to re-authenticate their details and is not expected to be a frequently occurring use case.

3. **Presence**

The average duration of recognition is 1.5 to 30 seconds although it may take longer. The frequency of usage is expected to be low and, using new presence API's, applications will be able to use sensors to determine if the authenticated person is present at the device or if it is an unknown or guest user.

So let's talk a little bit about Microsoft's facial detection security mechanism…

Windows Hello



Windows Hello provides biometric authentication, allowing you instant access to any of your Windows 10 devices, whether desktop or mobile.

Forget trying to remember cumbersome passwords–with Windows Hello you will be able to look at your webcam or use your fingerprint to be immediately recognized and allowed access.

As well as being much more convenient, it is also a more secure method than using a password.

Windows 10 introduces a new system that allows you to authenticate enterprise content, applications, and even online experiences without having a password stored where it can be stolen.

Windows Hello works with your face, your iris or with a fingerprint, (you will need a compatible webcam and/or fingerprint sensor). After implementation, only you and your partnered device can be used to access your Windows 10 apps, websites, and data. This is done using a series of modern sensors that will recognize characteristics that are personal to you.

Unless your device already has an Intel RealSense compatible camera or fingerprint sensor, you will need to upgrade to one of a large number of Windows 10 devices that will soon support Windows Hello.

For facial detection, Windows Hello uses software and special hardware to verify your identity – it won't work if someone holds up a photograph of you, for instance.

The Intel RealSense enabled cameras use infrared technology to take a very comprehensive 3D image of your face. This allows for not only a great feel for the look of your face, but the depth as well.

The cameras are stunningly reliable and can verify your identity in a wide range of lighting conditions.

Windows Hello is a solution that will be used not only by consumers but also by defense, government, health organizations, financial organizations and others to bring better security and eliminate the threat of imposters or hackers.

New Security Features in Windows 10

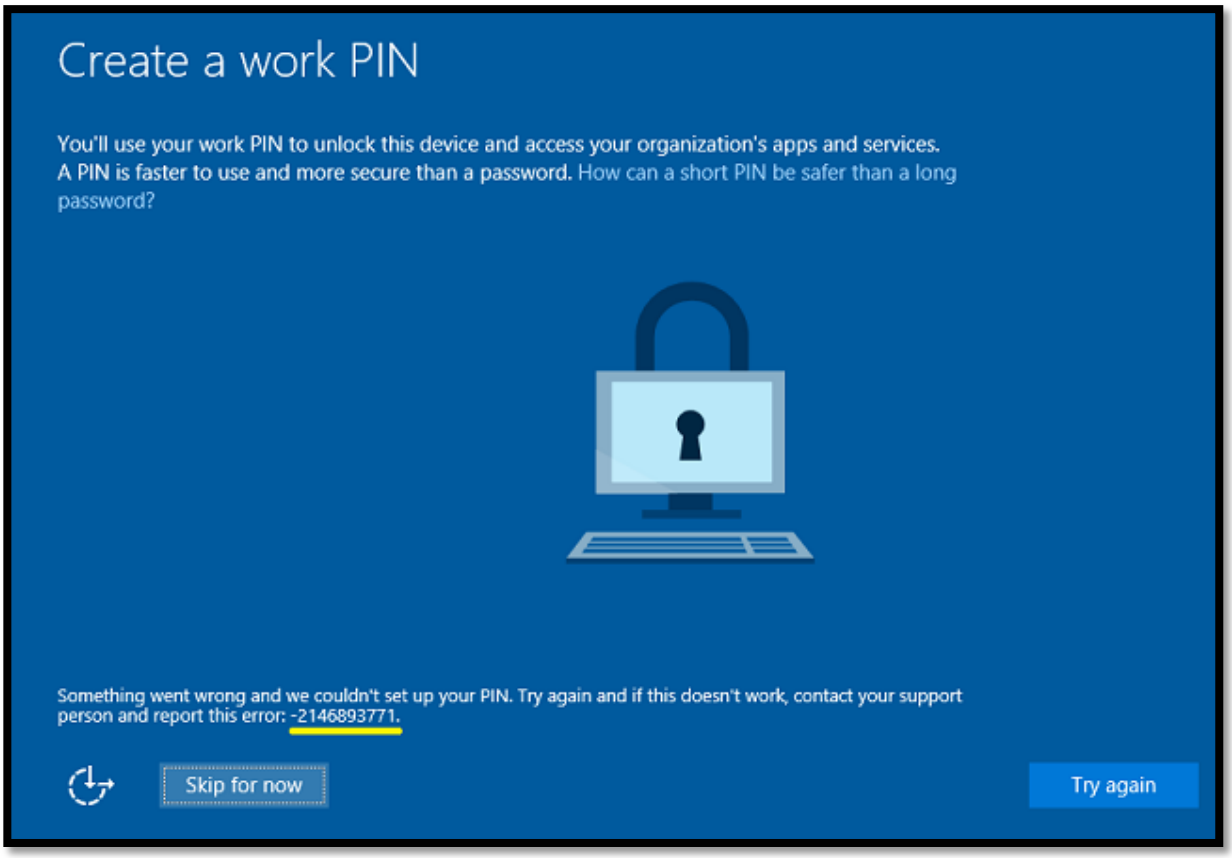
The following are some more of the new and exciting security features that Windows 10 is bringing to the table.

Microsoft Passport

Windows Hello is not the whole story, however. Microsoft has also introduced **Microsoft Passport**.

Passport is designed to do away with passwords, allowing system IT managers, website authors, and software developers to include a more secure way of letting you sign in to their apps or sites.

Instead of using the old-fashioned method of a password, Windows Passport is designed to securely verify your identity and authenticate you on websites, applications, and networks without the need to store a password on the servers – thus eliminating the threat of theft through hacking.



Windows 10 replaces the password system with a private key or PIN that will allow you access to either your own personal data or to your organization's data. That PIN is linked to your device only and will not work without it.

If you tried to log in using your PIN on another device, you would be barred from entering. Obviously, you will need to set up a separate PIN for each device that you intend to use but that just adds a further layer of security – no-one can access your data from just any device any longer, making your data and your identity safe from unwanted attention.

Why did Microsoft go down the route of using a PIN number? Surely that is just as bad as using a password, isn't it?

No.

A PIN is significantly faster to use and is way more secure than a password. Next question – how can such a short PIN be more secure than a complex password?

This is because it doesn't really have anything to do with size.

Where the PIN differs from a password is that a password can be used for ***access on any device***; the PIN is ***unique to a specific device***. That means that if someone were to steal your PIN and try to access your data, they couldn't do it, unless they were using the device the PIN was linked to.

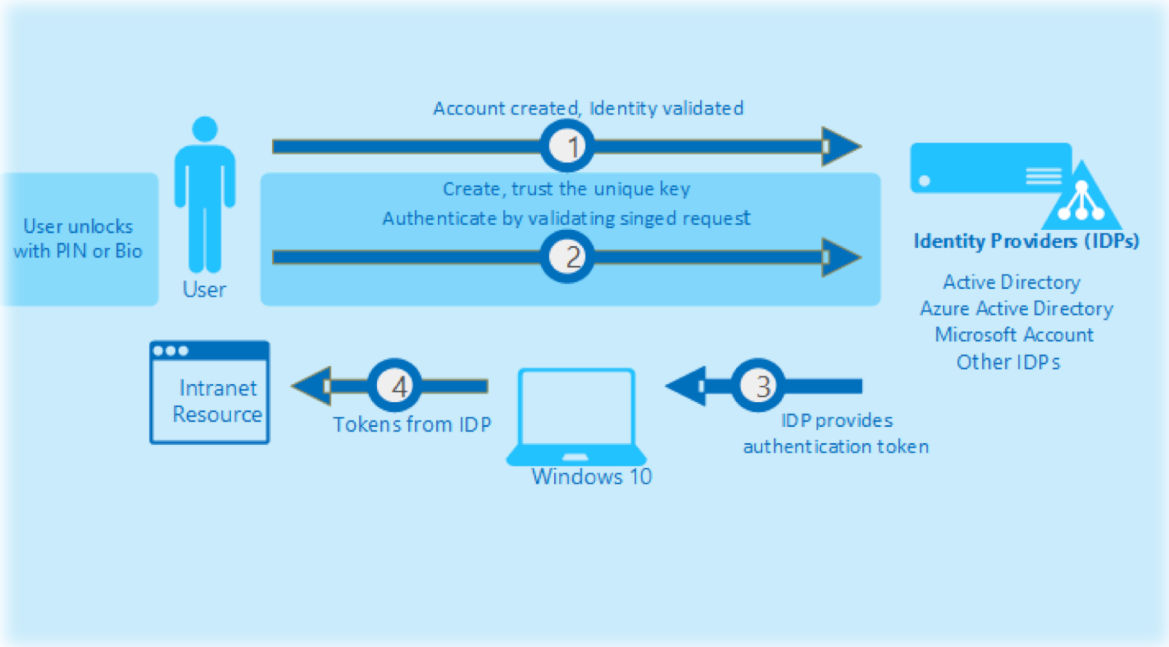
Even then, they would still need to get past the biometric login and that cannot be done by anyone other than you. Make sense? Think of it as being like your credit card PIN.

A person could not steal your PIN number and then use it on their own card in a cash machine. That PIN is tied to that card and that is how the Microsoft Passport PIN works too.

None of this is required – it is entirely your choice if you choose to use Microsoft Windows Hello and Passport. You may be concerned that your unique biometric information can be stolen and used, and it is for that reason that Microsoft stores your unique biometric information on your device only, not on any eternal system or server and it is shared only with you.

It can only be used as a method of unlocking your device and is never used to authenticate you over an open network.

Passport2Go



Passport2Go is part of the Passport system that allows you to specify whether a device is for personal or for business use.

Let's go through an example of Passport2Go in use.

> ***Fun Fact:*** ***Microsoft uses the fictional Contoso Company for examples in many of their presentations and documents***

Irwin works for a consulting company that provides its services to Contoso. Contoso gives its partners cloud-only accounts through **Azure Active Directory** (AAD) when it is necessary.

Irwin has a long-running engagement that requires him to have an AAD account and, through his work for Contoso, he has an allowance, which lets him buy a device that is ONLY for use for his Contoso work.

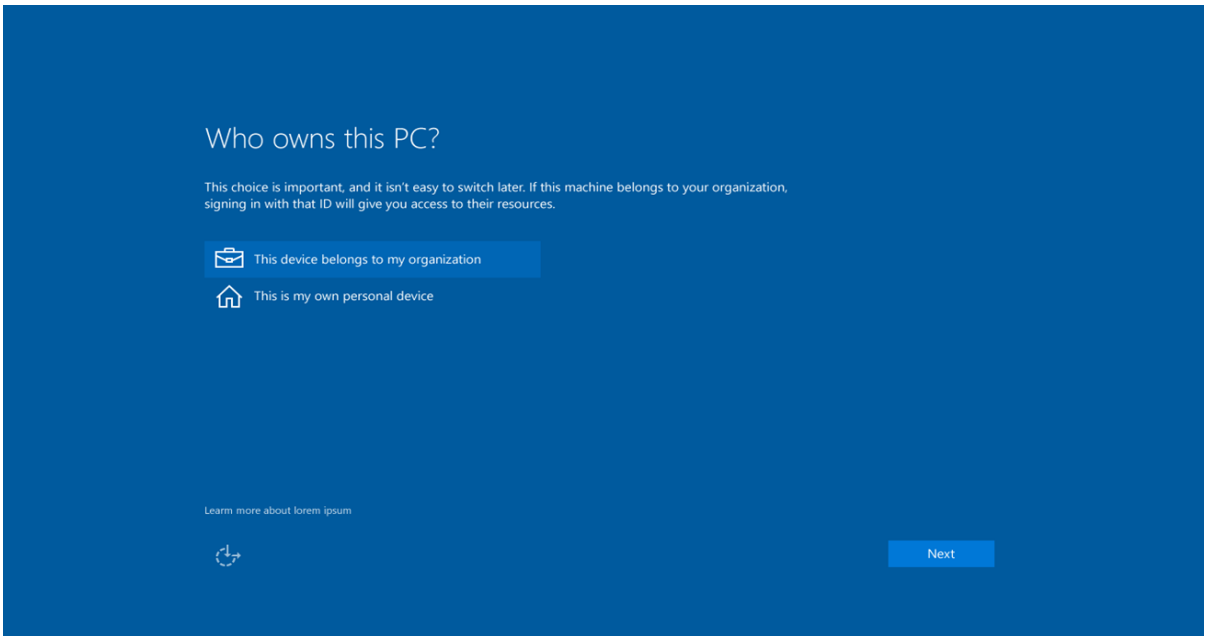
How does he set this device up so that he can only use it in this way?

> **By enabling Passport2Go.**

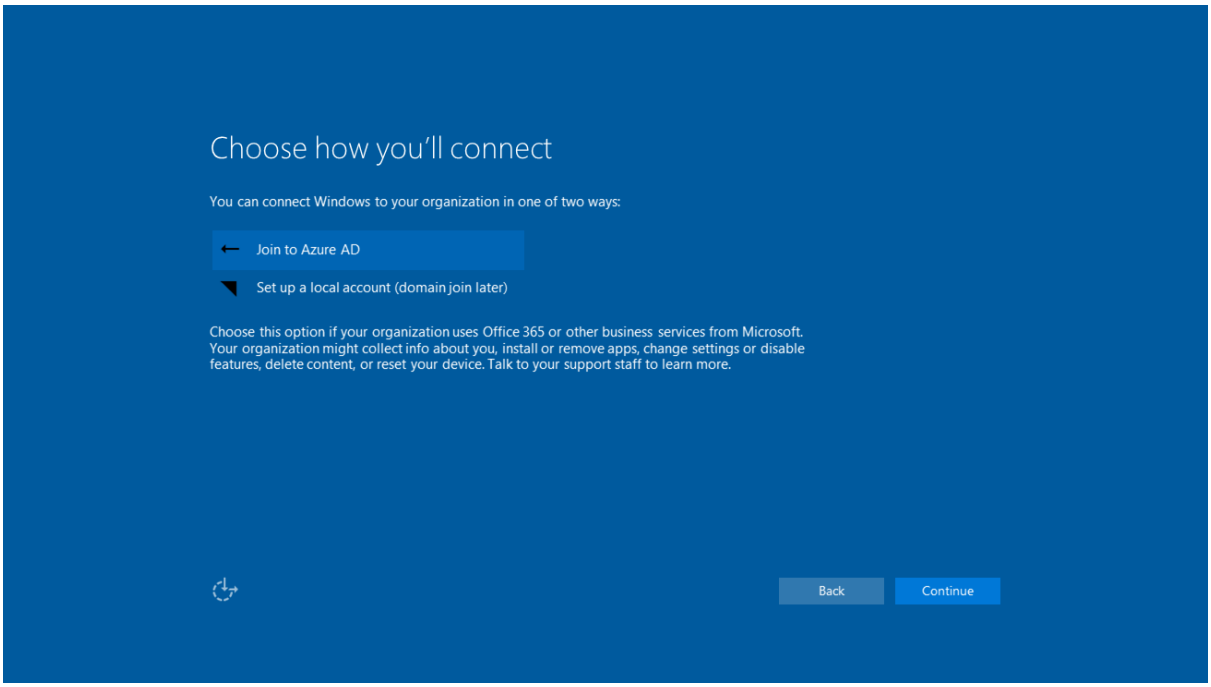
When you sign up to Passport2Go, you define whether your device is a personal or business use device.

On the next page, let's walk through the example:

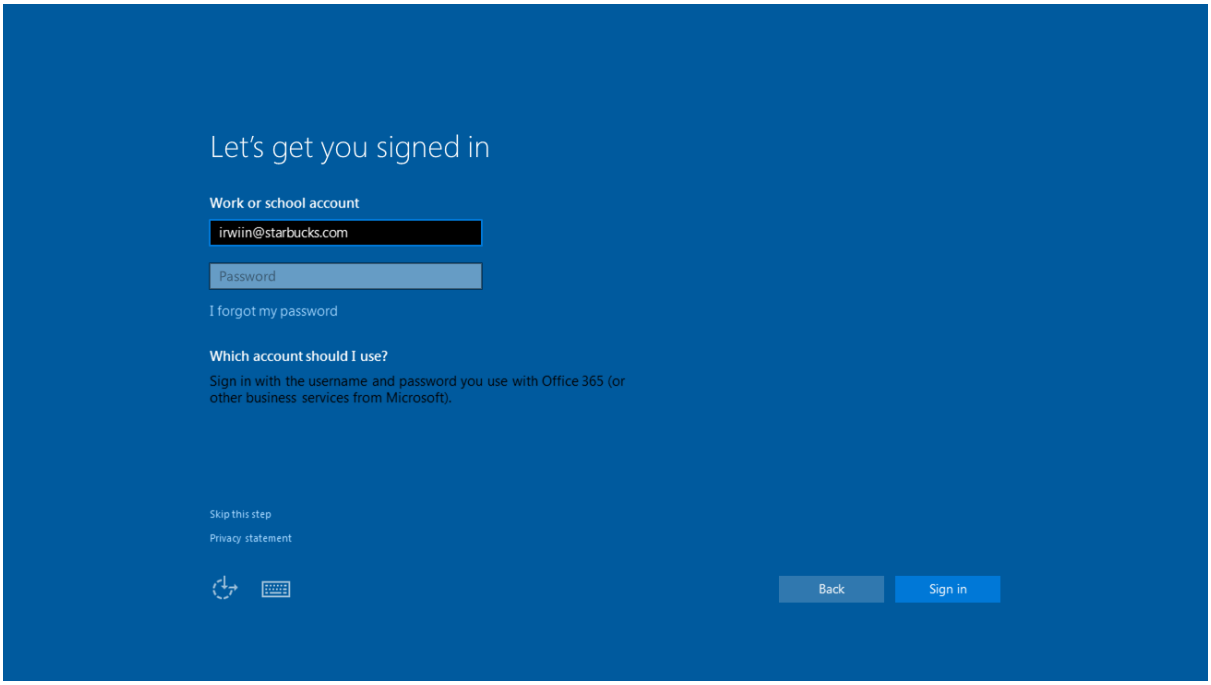
In our example, choosing organization use gives Irwin access to all the resources that he needs for his work.



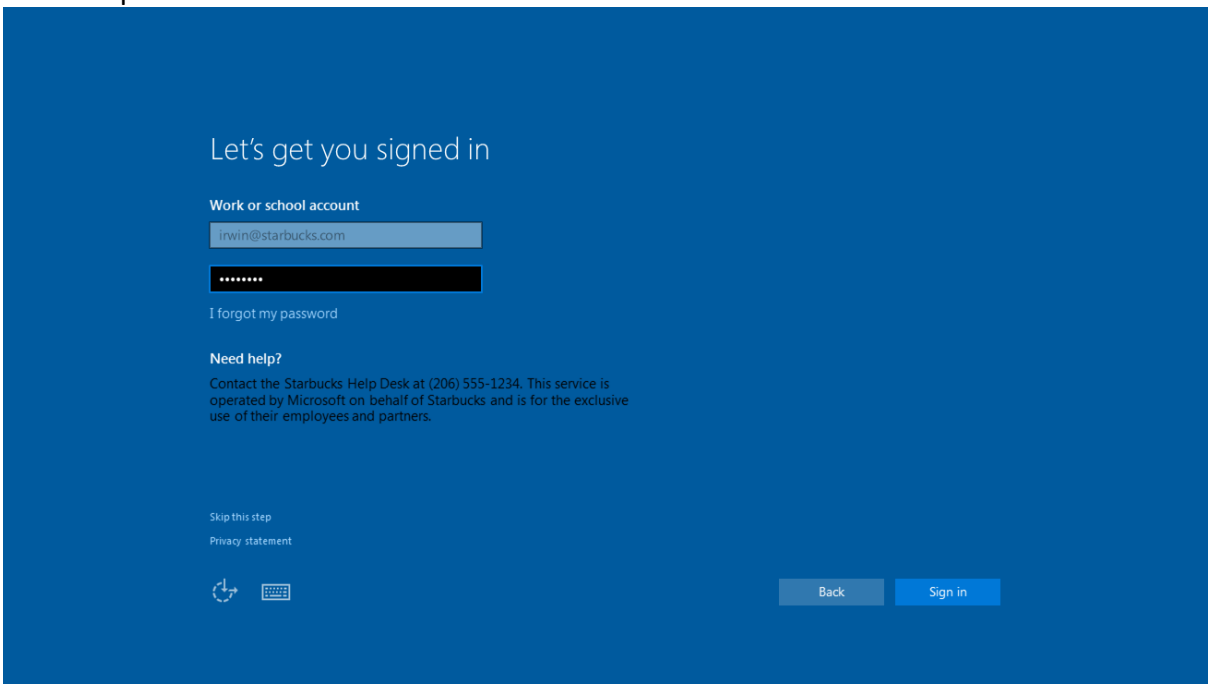
Next Irwin has to determine how he is going to connect. Because Contoso provides him with an AAD account, that is the option he selects.



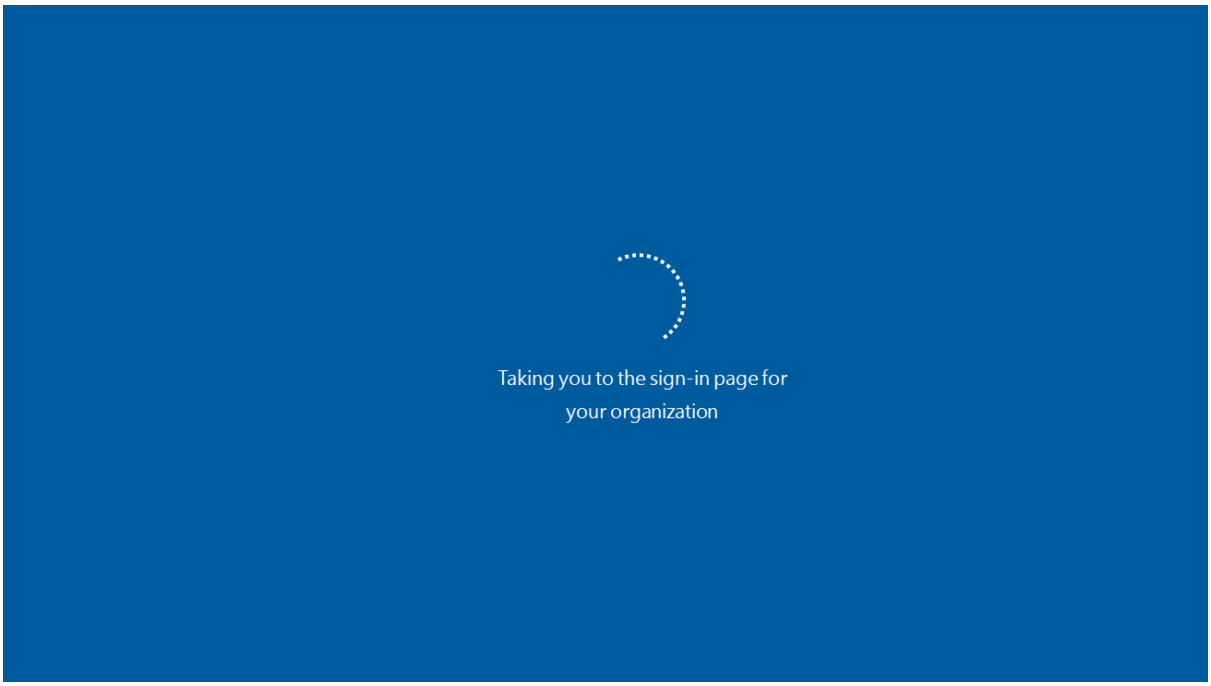
Irwin is now taken to the AAD sign in page where he signs in with his Microsoft or Office 365 credentials, starting with his email address.



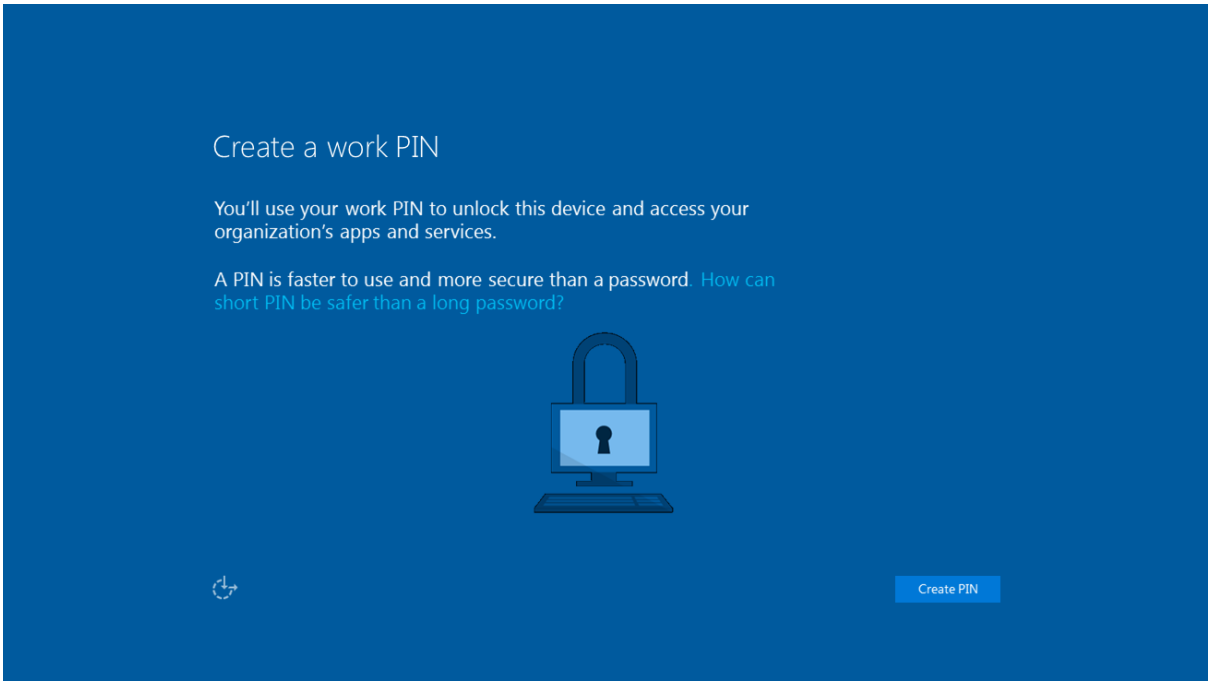
Then his password...



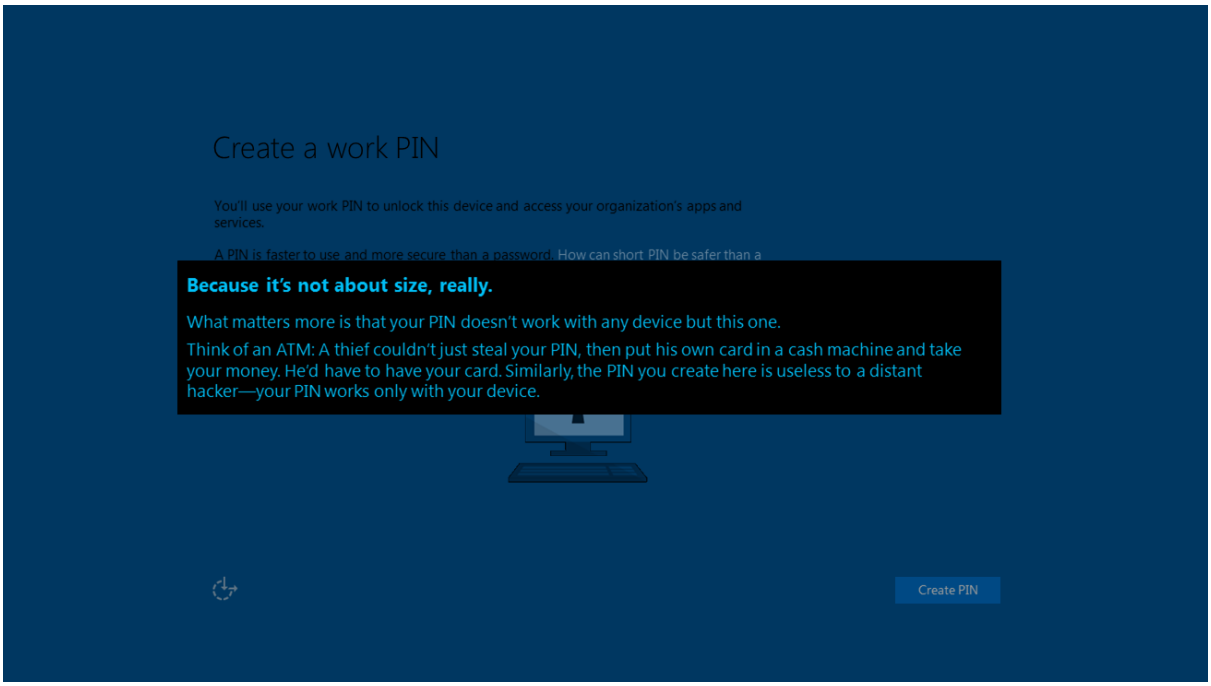
Irwin is then directed to the Contoso sign in page on AAD.



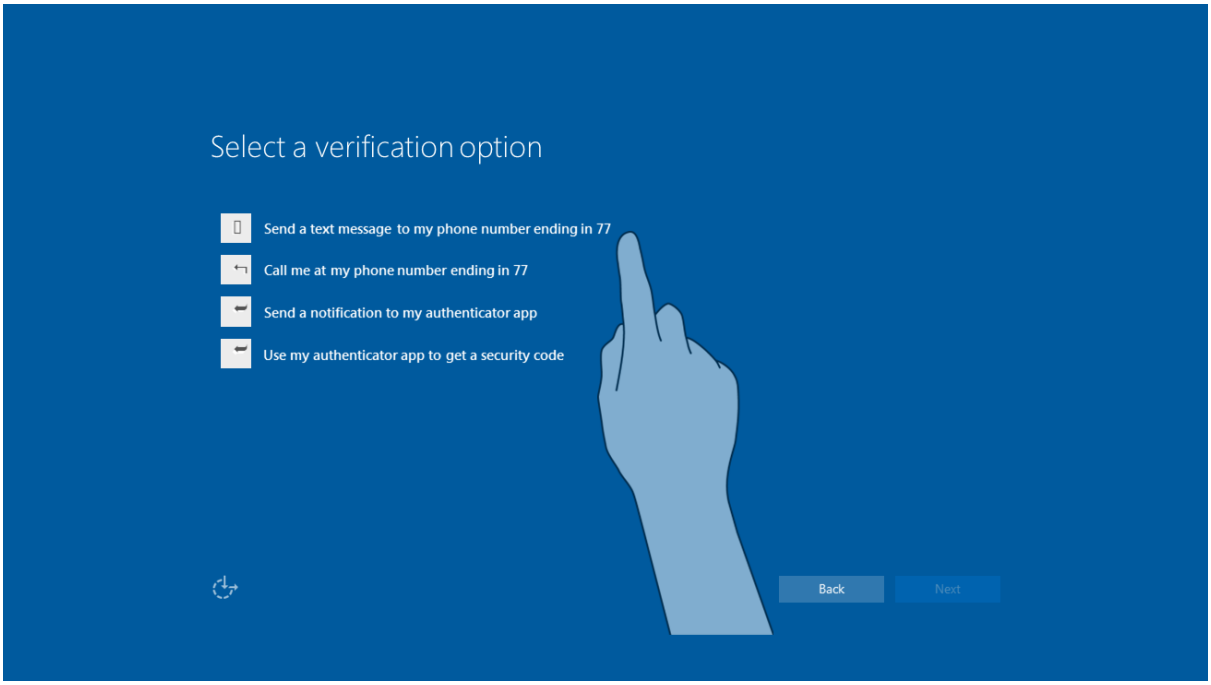
Now it's time for Irwin to set up his PIN number which will allow him to unlock the device and access everything he needs in order to do his work.



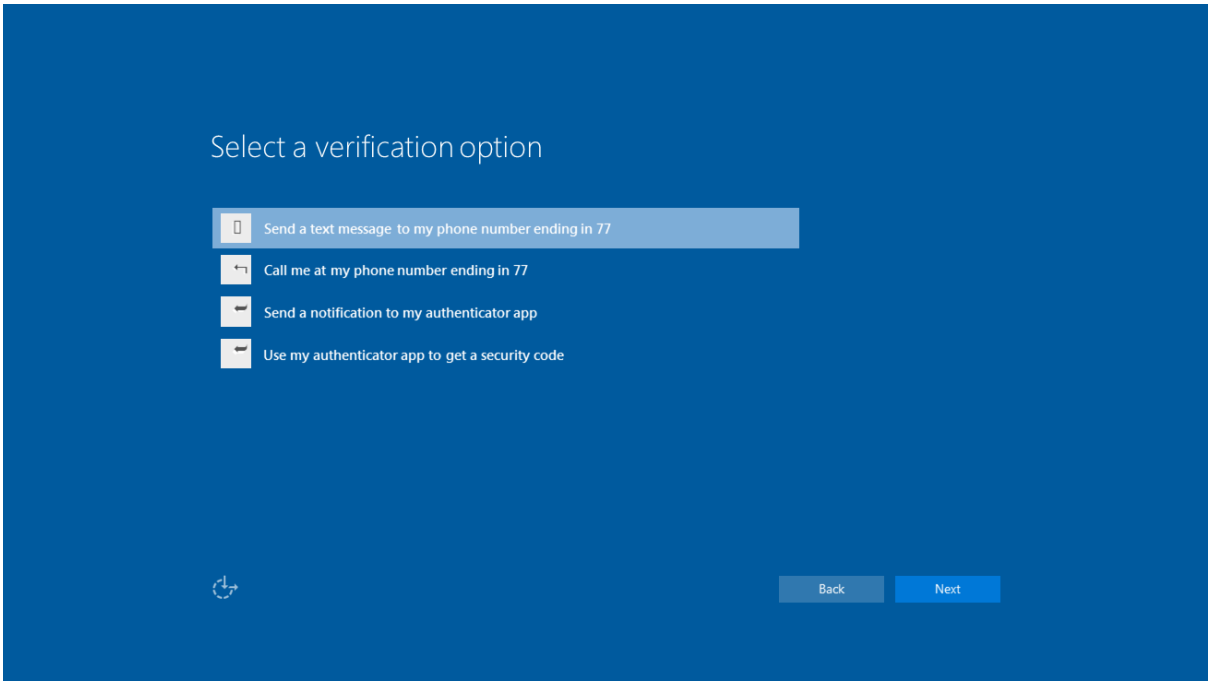
PIN numbers are far more secure than passwords and are much shorter. As we mentioned before, you may question how a shorter PIN number could be more secure than a long and complex password. Microsoft has the answer to that:



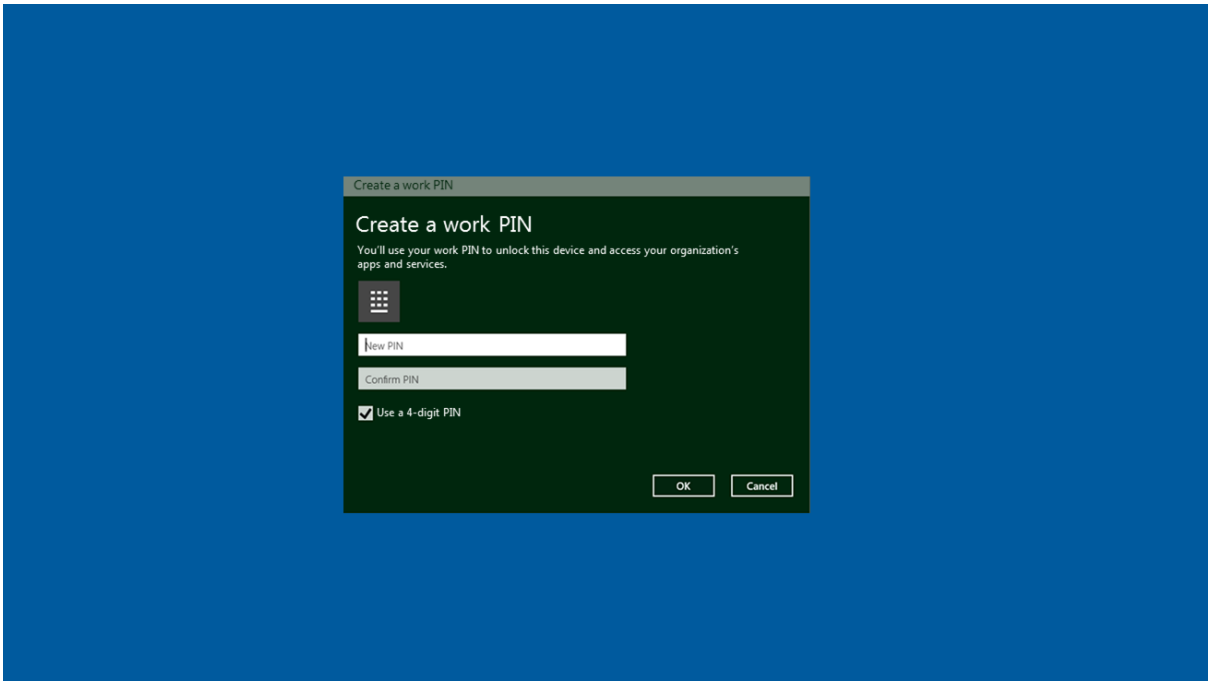
The next step for Irwin is to choose how to verify his account. He has a choice of four options – **text message, phone call, a notification that is sent to his authenticator app,** or **using the authenticator app to generate a security code.**



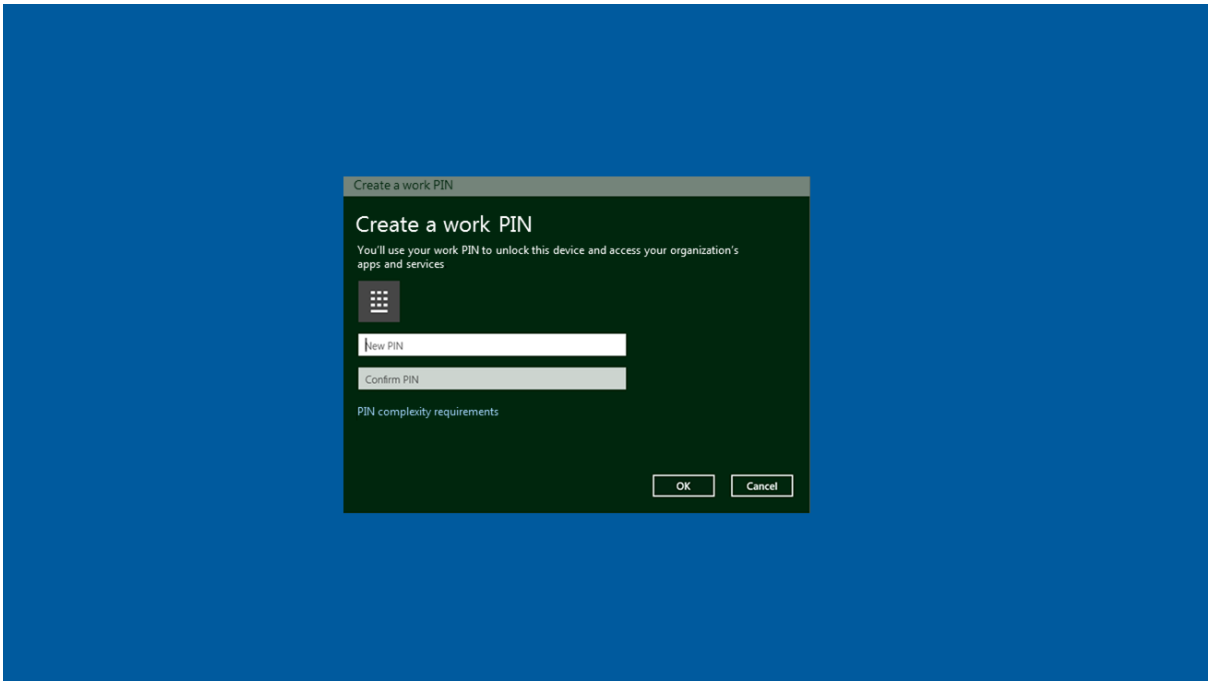
Irwin opts for the text message…



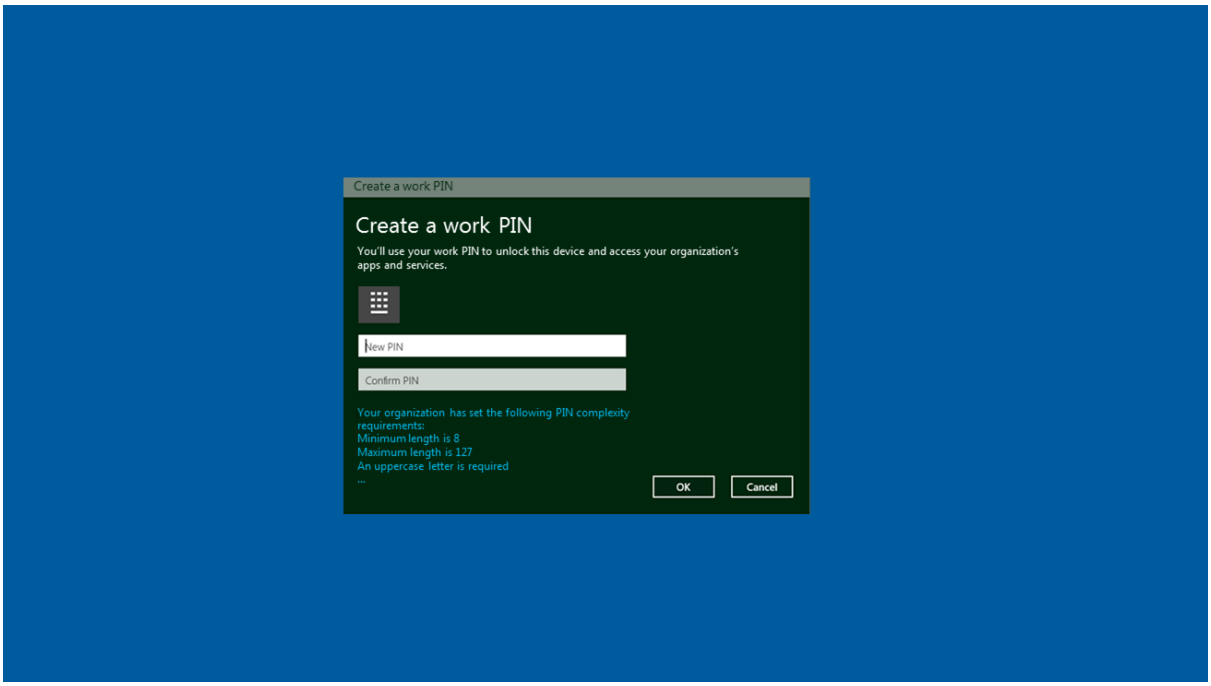
Once he has received the message verifying his account, Irwin can create his PIN.



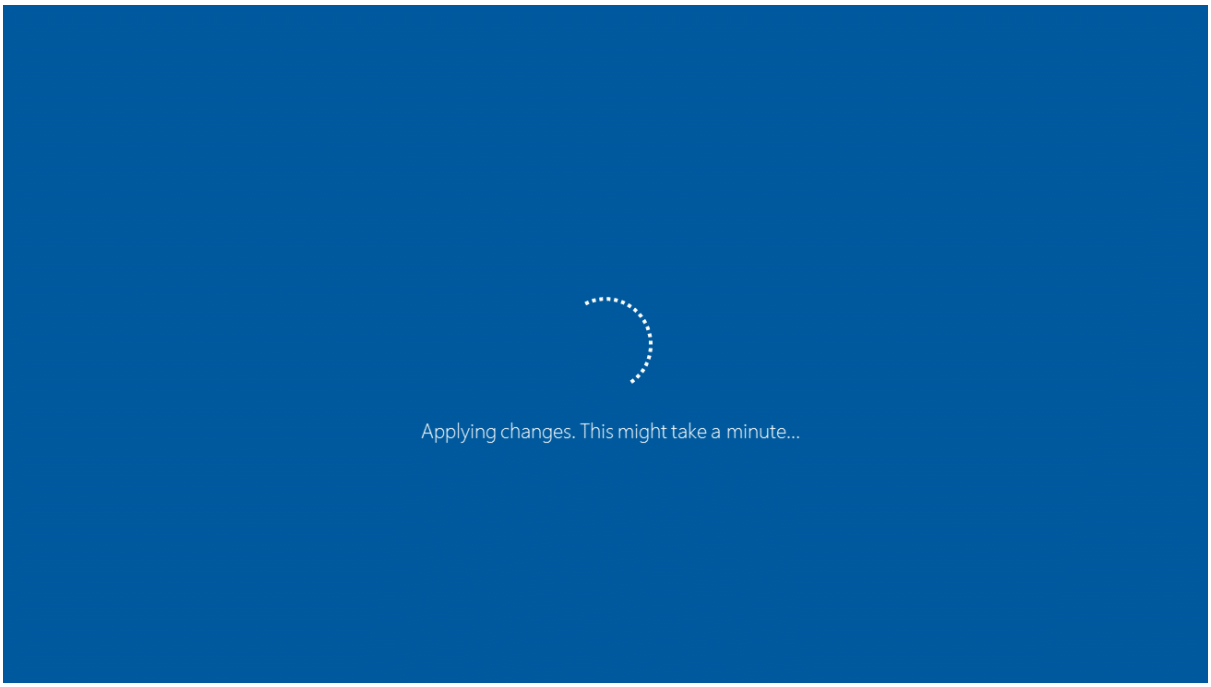
Because he has ticked the box that says, “Use a 4-digit PIN”, his new PIN is not accepted and he sees a message that tells him there are special requirements for the PIN.



Contoso has set specific requirements for the complexity of the PIN and these instructions are now revealed to Irwin, allowing him to create a PIN that ties in with what they want.

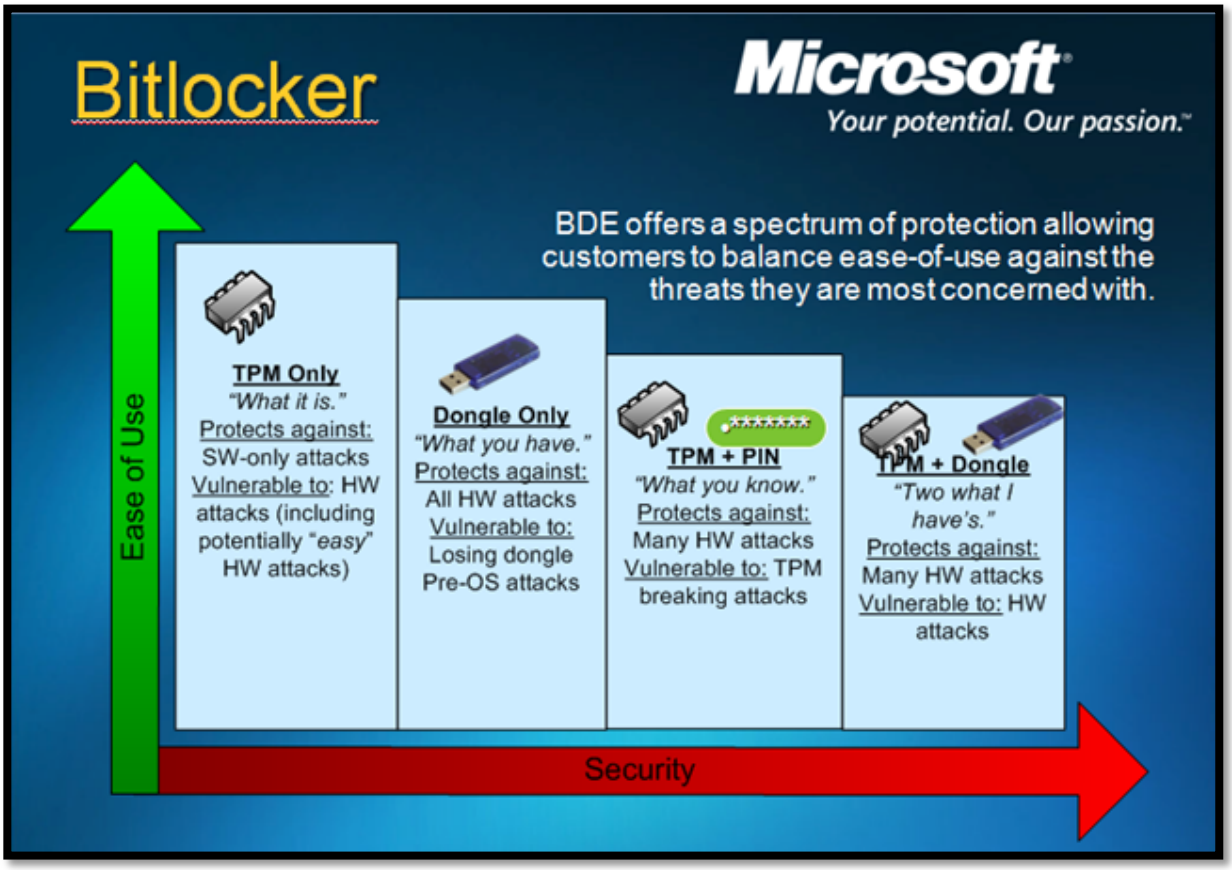


Once Irwin has successfully set his PIN up, the changes are applied, which may take a few seconds to a couple of minutes.



Finally, the NGC (Next Generation Credentials) container is loaded and Irwin has full access to all the apps and systems he needs for work.

BitLocker and TPM



Windows BitLocker Drive Encryption is a brand new security feature that protects your data more efficiently. It does this by encrypting every single piece of data that is stored on the Windows OS system volume – the partitions on your hard disks.

TPM – the Trusted Platform Module is a special chip that stores a key pair that is called the Endorsement Key. The key pair is kept inside the TPM chip and is not accessible by software.

When the user or an administrator takes on ownership of a device, a ***Storage Root Key*** is created. The key pair is generated by the TPM and is based on the Endorsement Key and a password specified by the owner.

Another key, which is called the ***Attestation Identity Key***, works to protect the device from unauthorized modifications by software or firmware. It does this by hashing vital parts of the software and firmware before they can be executed.

When the system tries to connect to a network, a server to check that they match expected values then verifies those hashes.

If any of the hashes have been modified since they were last verified, there will be no match and the system will not be able to gain entrance to the network.

Windows BitLocker uses TPM to protect the operating system and all the user data. It also helps to protect the user's computer from being tampered with, even if it is lost or stolen.

That said, BitLocker can be used without TPM but, **from 2016, Microsoft will require computers to have TPM 2.0.**

If you do use it without TPM, you must configure BitLocker to store your encryption keys onto a USB flash drive, which must then be used whenever you want to unlock the data that is stored on a particular volume.

Trusted Platform Module, or TPM, provides a number of essential security services, including:

- Securely recording boot process measurements.
- Deriving and sealing keys based on a specific boot sequence.
- Providing a root of trust to the Cloud.
- Protecting every one of these processes from malware or a malicious user.

TPM 2.0 goes a little further than that and updates the capabilities provided in TPM 1.2:

- Cryptographic strength is updated to meet modern standards in security.
- Is more flexible on cryptographic algorithms in order to better support government needs.
- Better management consistency across all implementations.

How Does BitLocker Drive Encryption Work?

In a nutshell, it protects your entire system by encrypting all of the data.

If a TPM is used to lock the encryption keys, those keys cannot be accessed until the state of the computer has been verified by the TPM.

If there are any signs of tampering, TPM will not authorize the release of the keys.

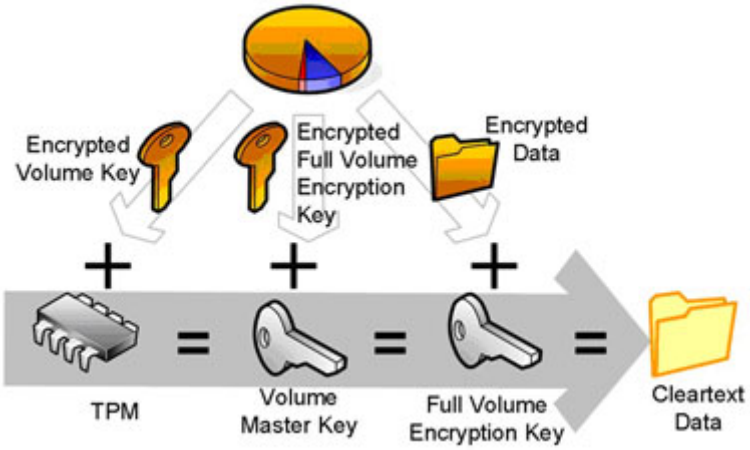
By encrypting the entire contents of the volume, you are protecting everything – your own personal data, the operating system itself, temporary files, Windows registry files, and the hibernation file.

Because the keys are locked by the TPM, even if your hard drive were stolen and inserted into another device, the thief would not be able to read your data.

When you start your device, the TPM compares a hash of system configuration values, along with a snapshot that was taken earlier, to verify the startup process.

If all is OK, the TPM will release the key, and the encrypted data can be unlocked. If your Windows installation shows signs of tampering, the key won't be released; it's as simple as that.

By default, BitLocker is set up to work with the TPM, and you can also combine this with a user-entered PIN or another startup key that is stored on a USB flash drive. This key is a requirement if you do not have a compatible TPM and you want the locking keys.



BitLocker goes a step further than that in Windows 10 – it can also be used to encrypt individual files. While it is normally used for the entire drive, if you need to send specific files using email or a USB key, they have to be encrypted on a file-by-file level.

Users can opt to encrypt their files from the "Save-As" dialogue box or by using Windows File Explorer. In this case, all you need to do is right click on a file and choose from the encryption options. All encrypted files then show up in green, allowing you to see at a glance what has and has not been protected.

One of the more common uses of BitLocker is downloading sensitive documents from a website. In this case, web files are automatically encrypted, giving you the peace of mind that comes from knowing that the information is completely secure.

Device Guard

So, Microsoft is going to protect your identity and your data but what about the device you are using?

Windows 10 includes a number of ways to lock down your device, adding in extra protection and threat resistance. Users inadvertently download most malware onto a device, so Microsoft is introducing a new system of only allowing trusted apps to be installed and/or run on your device.

Trusted apps are those that have been signed by the Microsoft signing service, although the device will have to be configured for this. That new feature is called Device Guard.

Device Guard is a new piece of firmware that runs at hardware level before and during the boot up process. It is designed to only allow applications and scripts that have been properly signed to load up and is already proving to be a popular feature, with many OEMs ready to install it on new devices.

Device Guard is a combination of software and hardware features that need to be configured together. When this is done, the device will be locked down to only run trusted applications.

It works by using the new virtualization-based security feature that Windows 10 includes – a system that isolates the Code Integrity service right from the Windows kernel and allowing the service to use enterprise-controlled policy defend signatures to determine what can and what can't be trusted.

The basic function of Device Guard is to test out each process that is being loaded up into the memory to be executed. It will run this test both before and during the boot up process and will check to see if the process is genuine based on signatures and will stop anything that does not have the proper signature from loading.

The technology that Device Guard uses is embedded at hardware level, as opposed to software, which isn't always 100% accurate at detecting malware. It uses virtualization for the correct decision–making process, to tell the device what it should and shouldn't allow to load up into the memory.

This level of isolation should stop malware in its tracks, as it won't be allowed to load on to the device, even if the attacker already has control of the systems where Device Guard is installed.

According to Microsoft, this system is more secure than the traditional anti-virus methods we use today, even more secure than app control technologies, like Bit9 and AppLocker, as these can be tampered with, either through malware or through system administration.

Required Hardware and Software for Device Guard

In order to use Device Guard, you will need to install the following hardware and software and then configure it:

- ✓ Device Guard will only work with **Windows 10**
- ✓ **UEFI Secure Boot** – helps to protect the integrity of the device at hardware level
- ✓ **Trusted Boot** – designed to help protect against attacks at the rootkit level
- ✓ **Virtualization-based Security** – Hyper-V protected container that separates windows 10 processes
- ✓ **Package Inspector Tool** – Helps users to create a list of the files that must be signed for Classic Windows applications

Why use Device Guard?

Every single day, thousands of new malicious files are created and using the traditional method of signature-based detection to fight the malware is not adequate anymore.

With Device Guard, that malware cannot be downloaded because the apps that contain it are not trusted. Up to and including Windows 8.1, an app would be trusted automatically unless a firewall or anti-virus blocked it – with Windows 10, an app won't will run unless it is trusted first.

Device Guard will also help to protect against Zero Day attacks and will also combat challenges put up by polymorphic viruses.

In an enterprise setting, the Code Integrity policy must be set up to determine which apps are trusted. As well as that, specific software and hardware configurations are required:

- UMCI – User Mode Code Integrity

- Kernel code integrity rules that include WHQL signing constraints – Windows Hardware Quality Labs
- Secure Boot that has db/dbx database restrictions
- OPTIONAL – virtualization based security to protect kernel mode apps, system memory and drivers from tampering
- OPTIONAL – TPM 2.0

Before you can use Device Guard, you should enable the virtualization-based security feature on capable devices, make sure that the Code Integrity policy is configured, and then configure any other settings that are required by you for Windows 10.

After that, Device Guard will work like this:

1. Your device boots up with U Secure Boot – this will stop rootkits from running, allowing Windows 10 to start up first.
2. Once safely started up, Windows 10 will start the Hyper-V virtualization-based security features, including Kernel Mode Integrity. These will protect the Windows kernel, any privileged drivers and your system anti-malware solutions by stopping malware from running in the boot process or in the kernel once the device has started up
3. Using UMCI, Device Guard checks your system to make sure that anything that is meant to run in User Mode is trusted, including Classic Windows apps, Universal Windows Platform, or a service. Only binaries that are trusted will be allowed to run.
4. As Windows 10 is starting up, TPM starts up as well, helping to protect sensitive information by providing a hardware component that is isolated from everything else. This protects your certificates and user credentials from attack or theft.

Enterprise Data Protection (EDP)

Microsoft also has a new DLP – data loss prevention – system.

While consumers can use it, it is aimed mainly at corporations, due to the large number of employee-owned devices that are now being used under the BYOD – "Bring Your Own Device" – banner.

Due to the large numbers of these devices, the risk of accidental data disclosure is now much higher than it ever was, basically because of the number of external apps and services that are also in use on the device – outside of the control of the enterprise.

This includes email, social media and cloud services, and all the applications we use on our mobile devices on a daily basis.

Yes, there are solutions that attempt to address this by asking employees to switch between containers for personal and corporate use but this isn't a very efficient way of working.

The new feature in Windows 10 is called **EDP – Enterprise Data Protection** – and it offers up a much better user experience while, at the same time, helps to keep personal and corporate activities separate.

EDP helps to protect corporate apps and data from the risk of disclosure without asking users to change the system they are working on.

Furthermore, in conjunction with RMS – Rights Management Services – EDP can also protect your corporate data on a local basis, even when your data is roaming or is being shared.

How Does EDP Work?

Enterprise Data Protection is designed to counteract and address everyday workplace challenges, such as:

- Dealing with severe data protection leaks
- Maintaining enterprise data privacy
- Managing those apps that are not policy-aware, in particular, on mobile devices
- Handles a previous inability to lock down an employee device, which would potentially allow data to be leaked

Levels of Protection

EDP can be set to four different levels of protection:

Block: The feature looks for data sharing that is not appropriate and blocks the employee from completing the share.

Override: The feature will look for any data sharing that is not appropriate, telling the relevant employees that they are doing something wrong. However, this can be

overridden at the employee level and the data can still be shared – but the action will be logged on the audit log.

Audit: EDP runs quietly in the background, logging all data sharing and flagging those that are inappropriate. However, it will not block anything, only monitor and record.

Off: EDP is not active and does not protect any of your data.

EDP Allows Better Work Flow

Because employees will no longer have to switch between environments or apps to protect enterprise data, workflow is uninterrupted and productivity can potentially increase significantly.

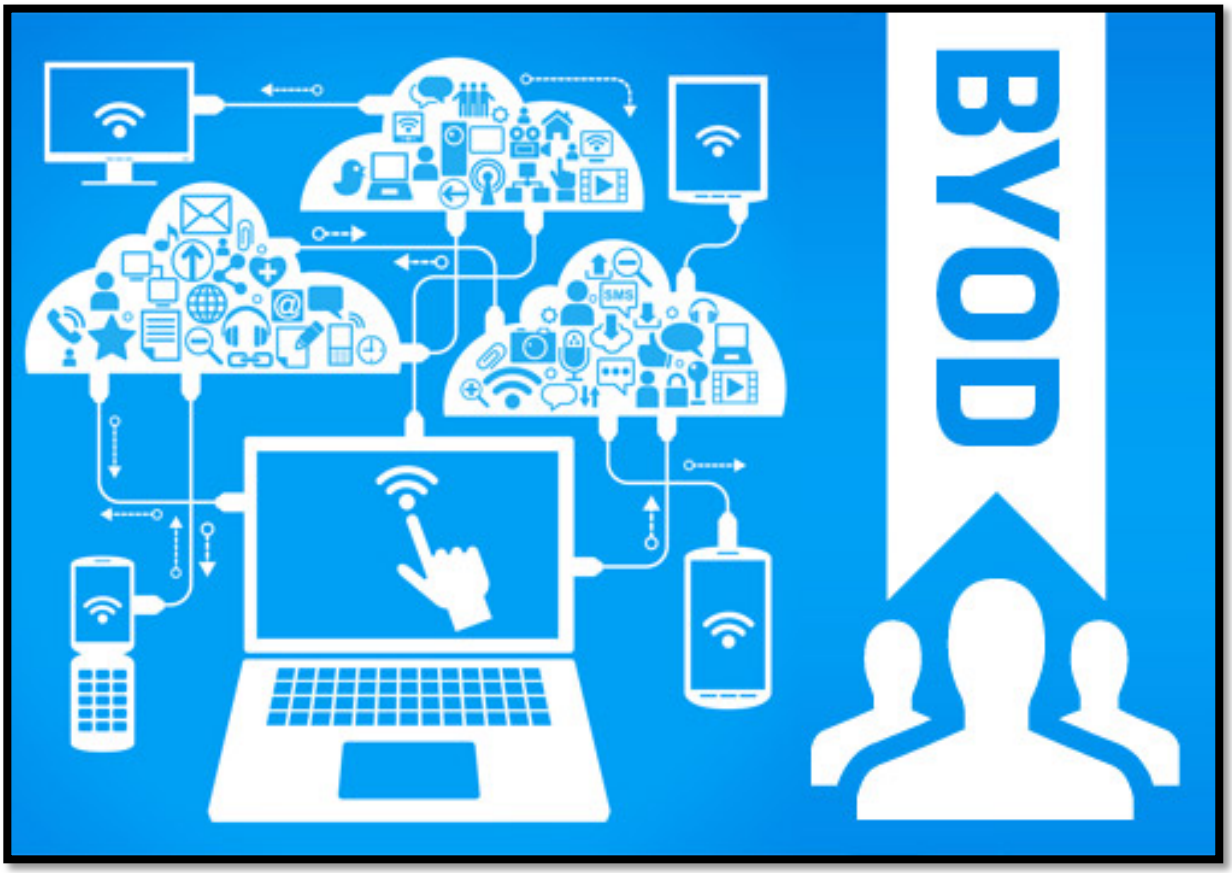
An example of this would be if an employee is checking their corporate email account and they receive a personal email. Instead of having to exit out of their corporate account, both messages would appear on the screen together.

Changing the Protection Levels on Documents

Employees have the ability to change the protection levels set on documents under Enterprise Data Protection.

They can only do this if the document is a personal one and has been incorrectly marked as enterprise. To do this, it requires employees to take an action and this will be logged for management to see.

Enterprise Data Security



Enterprise admins need to be able to maintain the confidentiality and the security of their data. With Enterprise Data Protection, you can make sure that corporate data is fully protected on devices owned by employees, even when the device is not being used.

When your employees create content on their devices, they are asked to define whether it is personal or corporate data – if it is corporate, it is immediately brought under the local data protection.

Wipe Enterprise Data Remotely

EDP also offers managers the option of remotely wiping all corporate data from a device that is managed by the corporation and used by the employee, without touching any of the personal data on that device. This is of huge benefit when a device is stolen or an employee leaves the company.

Corporate documents are stored locally on the device and are encrypted using an enterprise identity.

When you want to wipe the device, you will need to go through a verification process, after which a command can be sent through the mobile management system to remotely wipe the data. When the device is connected to a network, the data is removed and the encryption keys are irretrievably revoked.

This will only happen on devices that have been specifically targeted – all other devices will work normally.

Copying or Downloading Enterprise Data

When data is targeted for download from a corporate source like SharePoint or Office 365, it is determined to be enterprise data and will be encrypted before being stored locally.

The same will apply to any data that is copied from the enterprise to a USB flash drive. Because the data is already marked down as being enterprise data, the encryption will follow the data to the new storage device.

Privileged Apps and Restrictions

With Enterprise Data Protection, you will be able to control which apps can and cannot access enterprise data.

Those that can are added to a "privileged" app list and are subsequently allowed to access and use enterprise data. Anything that is not on this list is classified as personal and are blocked from accessing data, depending of course, on the level of protection you have set.

Privileged apps will act differently from personal or non-privileged apps. When a user wants to copy and paste data, a privileged app will allow it; non-privileged ones won't.

Should a person try to copy enterprise data to a non-privileged app, they will see a notification advising that policy restrictions are in place and the action could not be completed.

Persistent Data Encryption

Enterprise Data Protection allows you to keep your data safe even when the device is roaming. Apps such as OneNote and Office work in conjunction with EDP to persist data encryption across services and locations.

For example, an employee opens content in Outlook that is EDP encrypted, makes some changes to it and then attempts to save it under a new name, to try and get rid of the encryption.

That won't work because Outlook will automatically apply EDP to the new version of the document, ensuring that the data is kept fully encrypted and secure.

Helps Prevent Accidental Data Sharing

EDP also helps to protect corporate data from being accidentally shared in public spaces like the cloud. Say, for example an employee puts a document in a folder called DOCUMENTS.

This folder is synced automatically with OneDrive, which is on your privileged app list. It is then encrypted on a local level – it will not be synced to the employee's personal cloud.

Data sharing also covers other devices. Under the old system it was possible for data to be leaked to another device while it was being transferred between them. For example, an employee saves corporate data onto a USB flash drive that also has personal data on it.

The corporate data is encrypted while the personal data remains open. As well as that, the encryption follows the data, so even if it is copied to another device, it will stay encrypted.

The Benefits of EDP

The benefits of EDP include:

- ✓ Protection against the leakage of enterprise data, with little to no impact on the work practices of the employees
- ✓ Separation of personal and corporate data with no need for employees to switch apps or environments
- ✓ Extra data protection for existing business apps without having to update them
- ✓ The ability to wipe all corporate data off a device while leaving personal data untouched
- ✓ Audit reports to help with tracking issues
- ✓ Fully integrates with your current management system or mobile device management system to configure EDP for your corporation, as well as deploying and managing it
- ✓ Extra protection while roaming or sharing data

Enterprise scenarios

EDP addresses the following enterprise scenarios:

- Enterprise data can be encrypted on both employee and corporate owned devices
- Enterprise data can be wiped off remotely without touching personal data
- Specific apps can be chosen, called Privileged apps, which can access enterprise data. These apps are clearly recognized by employees. Non privileged apps can be blocked from having access to enterprise data
- Employees don't need to switch between enterprise or personal apps, thus eliminating interruption to work flow, provided enterprise policies have been put in place.

Windows Defender

Windows 10 users will still need to use specific anti-malware software to protect from malware that comes from other sources.

This is because Device Guard only protects against malicious software that attempts to load during the boot process – at this stage, no anti-malware software is able to protect your device.

Instead of taking the chance that users will forget to download a program, Microsoft has included Windows Defender, also available in Windows 8. Defender is automatically enabled on your system and runs silently in the background.

This ensures that, whether you opt for a third-party solution or not, you will have, at the very least, a baseline antivirus protection. However, unlike Windows 7, Windows 10 will not kick up a fuss if you choose to install a third party option as well.

Instead, it will simply disable Windows Defender, stopping it from protecting your device. Should you opt to uninstall the third party malware software, Windows Defender will automatically be re-enabled, thus ensuring that your device is never left without some kind of malware protection.

Formerly called Microsoft Security Essentials, Defender runs quietly, scanning every file as and when you access them, before they are actually opened.

If it finds malware or anything else that could cause a threat to your machine and your data, it will clean it up and quarantine the offending file automatically.

You will get a notification that Defender has detected malware, telling you that it is taking the necessary action to clean it up. The antivirus definitions will also be automatically updated through Windows Update and this process does not require a reboot of the device.

Configuration and Exclusions

The settings for Windows Defender are already integrated with Windows 10, in the brand new Settings app. This can be accessed via the Start menu, in the Update and Security

category under Settings. By default, it will automatically be enabled for real-time, cloud-based, and sample submission protection. If you disable the real-time protection for any reason, Windows Defender will automatically re-enable it, to keep you safe.

Both Cloud and sample submission protection let Defender share any information that it finds about threats, along with the actual malware file, with Microsoft.

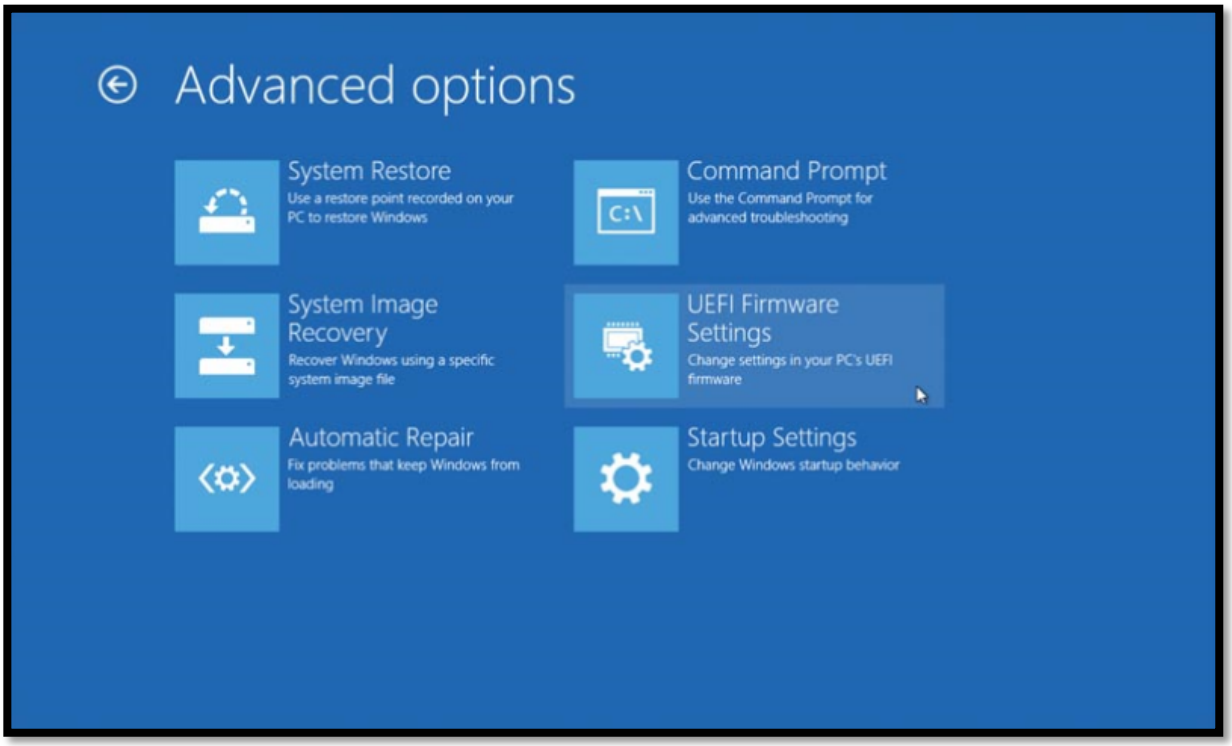
This is done in a bid to keep the definitions completely up to date and to allow Microsoft to continue improving and updating their security systems.

From the same menu, you can also set up Exclusions – these can be specific files, file types, folders and processes.

If, for example, Defender is slowing down your device performance because it keeps on scanning apps or files that you know to be safe, you can set an exclusion and tell it not to scan them.

These exclusions are to be used as and when absolutely necessary because having too many exclusions will render Defender useless, and leaves your device open to all kinds of threats.

UEFI



Unified Extensible Firmware Interface, or UEFI Secure Boot, is a more up to date replacement for BIOS, traditionally used to start up a computer.

Secure Boot is designed to shut out low-level malware and stop it from infecting and taking

over the boot process on any device. In the past, vendors that wanted the “Designed for Windows” certification had to have UEFI Secure Boot on their hardware.

In order to allow users of other systems such as LINUX, Microsoft had to include a toggle that would allow a user to turn off Secure Boot, at the very least for X-86 hardware. This allowed a user to open the door and install whatever they chose on their computers.

In Windows 10, Microsoft had originally said that they would not be supporting the on/off toggle and that all new hardware must ship with UEFI Secure Boot enabled.

However, it now transpires that, while Secure Boot must be enabled on all new Windows 10 hardware, OEMs have the option of whether to allow the end user to disable it or not. That is only for desktop machines; for Windows 10 mobile retail devices, the option to disable Secure Boot is not included.

The idea is to restrict the possibly of malware being downloaded by users who install an alternative operating system to dual boot their machines. At the time of this writing, Microsoft has not finalized their specs and, as such, the decision to put the onus on the OEM to include the toggle may be changed.

Advanced Threat Analytics

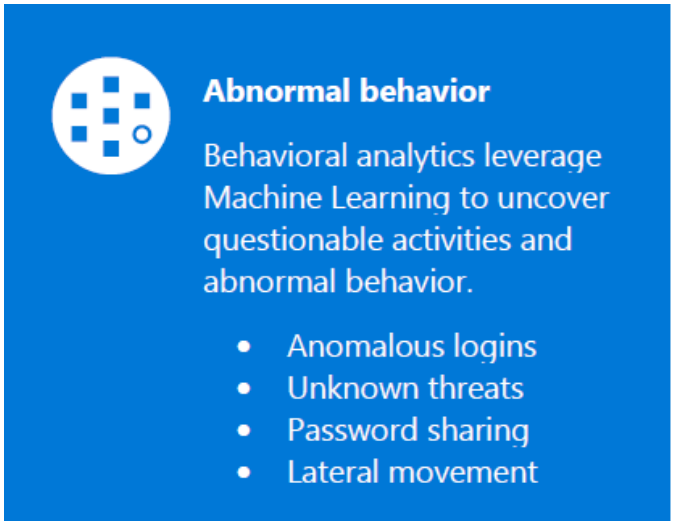
Security attacks today are more persistent, frequent, and sophisticated than ever before.

Regardless of which type of device you are using, it is safer to assume that you have been breached and that attackers may already be residing in your system than it is to go blindly about your work ignoring potential threats.

The following statistics tell a very sobering story:

- 200 + days – it isn't unusual for attackers to remain inside your system for this long without detection. They can do this because they take advantage of user accounts, privileged or otherwise, and hide inside the network. It takes sophisticated and advanced technology to find them and stop them, and to prevent others from attacking the system.
- 75% + - this is the percentage of network intrusions that result from a user's credentials being compromised.
- $500 billion – this represents the estimated cost of cybercrime to the global economy.
- $3.5 million – the average cost to a company for a data breach.

This is why Microsoft has come up with a brand new feature called **Advanced Threat Analytics or ATA**. ATA is designed as an on-premises threat analytics tool that works to detect threats and abnormal behaviour (see below) before they can cause damage.



To illustrate how it works, say you have a credit card and your provider monitors your spending behaviour.

If there is any suspicious activity, or activity outside your normal pattern, the provider contacts you to verify that the activity was yours. They may also place a temporary stop on the card while they verify it. This is the concept that Microsoft wants to bring to enterprise users.

The benefits of ATA are:

- Threats are detected using behavioural analysis of the user, monitoring how they use the system, and being alerted when there is any change to that pattern that looks suspicious.
- ATA is constantly evolving, forever learning from the user's behaviour, and adapting itself to reflect changes within a dynamic organization.
- It uses a simple attack timeline to focus on what is important – a very clear and efficient system that monitors and draws attention to the right things at the right time. In addition, it provides you with the information you need, i.e. the who, when, and where aspects of the attack. ATA also provides recommendations for the next step.
- ATA will also identify known risks and alert the right people – risks such as weak passwords, broken trust, weak and vulnerable protocols, etc.
- ATA also reduces the risk of false positives.

How Does It Work?

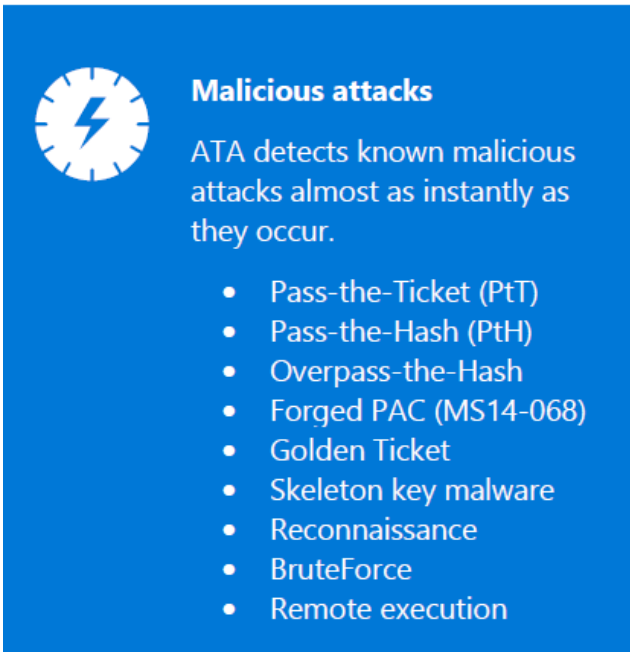
After ATA is installed, a non-intrusive port-mirroring configuration will copy all Active Directory related traffic to ATA, but will remain invisible to any hovering attackers. ATA will then analyse the data and work with SIEM – Security Information and Event Management – to look at related traffic and relevant events. All the information is stored locally, on-premises by ATA, and never leaves the organization.

The ATA detection engine begins learning and profiling the behavior of all users and then uses machine learning technology to paint an overview of the everyday activity.

Once it is familiar with your normal use behaviour, it will begin to look for anomalies and strange behaviour.

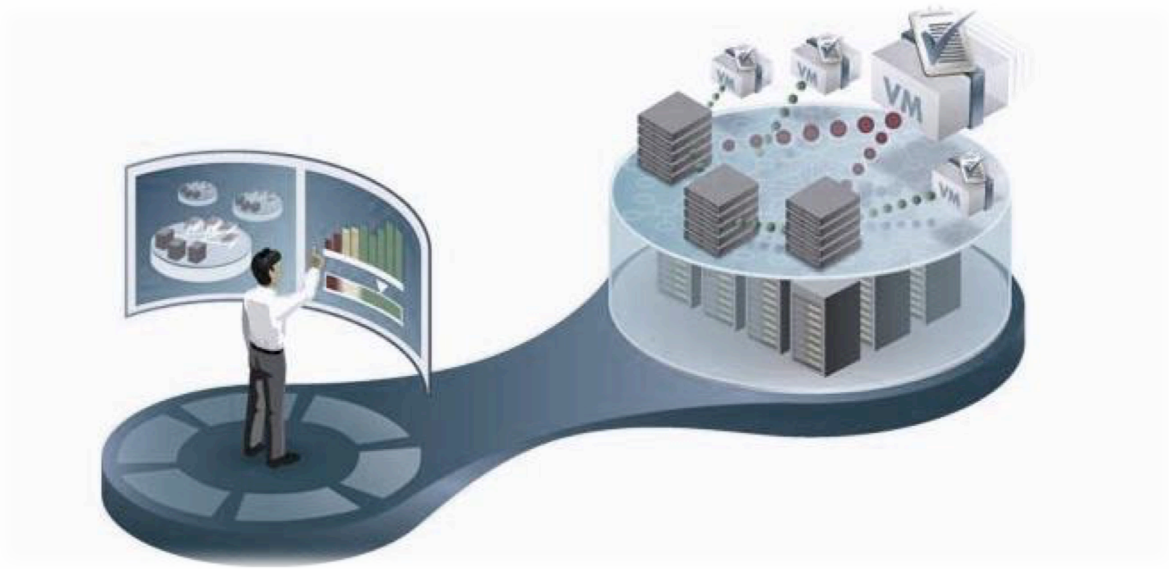
If these arise, it will raise a red flag and alert security teams, as soon as the system has compared and aggregated the anomaly with near real-time detection of security breaches and advanced attacks to build the timeline.

This also reduces the chance of false positives and better identifies malicious attacks, as shown below.



Microsoft ATA is a non-intrusive system that works quietly in the background without detection.

Virtual Secure Mode



Windows 10 is made up of a number of different containers, one of which houses the actual operating system. However, the security token for Active Directory that allows you to access your company network, and the LSA authentication service that issues it, are housed in a separate container that runs on top of the Hyper-V virtualization container.

These security tokens are the target for a good percentage of "*Pass the Hash*" security attacks. Once they have that token, they have your identity, which is as good as giving them your login details.

They have access to admin privileges and are able to run a tool, which can access and take the token. Once they have it, they can get around the networks and access servers without the need for a password.

Microsoft has made things more difficult for them by taking those tokens out of the software repository where they were previously stored and where they were susceptible to malware, and have locked them in a container. Once inside that container, not even Windows has access to them, even if the container is compromised in any way.

The container will not release any tokens or hashes; instead, when they are passed to Windows, it is done in a new format that cannot be replayed on the device. In addition, NTLM hashes are separated from the logon process, are randomized and managed in such a way as to protect them against a brute force attack.

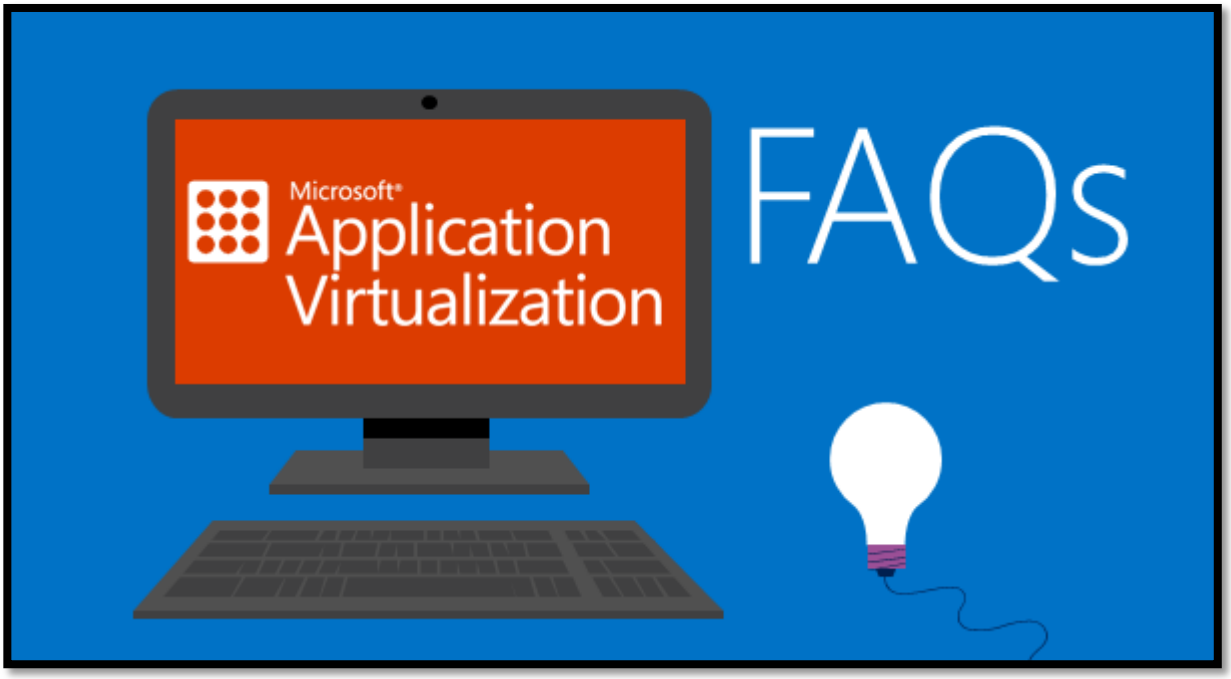
That container is called **VSM – Virtual Secure Mode.**

The VSM is, in effect, a mini version of the operating system, a Windows Core OS. It requires just 1 GB of memory and has sufficient capability to be able to run the LSA service that is needed for authentication purposes. It will have little to no effect on the performance of the device but you do need Windows 10, the next version of Windows Server on your Active Directory domain controller, and a CPU that has support for hardware virtualization.

In brief:

- Virtual Secure Mode isolates the sensitive processes into a Hyper-V container
- VSM runs Windows kernel and Trustlets inside of that container
- VSM protects the kernel and Trustlets even when Windows Kernel is compromised, thus keeping those tokens safe

Microsoft Virtualization Strategy and Security



For the last ten years or so, one of the biggest topics in the IT industry has been virtualization, mainly because of the sheer number of benefits that come with it for IT staff.

It brings the ability to make more out of hardware utilization capabilities, while at the same time offering sufficient scalability to get away from performance issues. There is also the capability to migrate virtual machines and cut down on downtime, and finally, the convenience that comes with being able to deploy new virtual machines quickly – manually or automated – thus reducing the workload of the IT department.

Microsoft has a goal in mind – what Hyper-V has done for server deployment and management; they want to do with the data center. To do that, they wanted to bring the whole structure down to the software level, which gives users the ability to automate many more data center aspects, and gain much more efficiency.

Over the last few versions of Windows Server, Microsoft has come a long way in improving Hyper-V and bringing it up, together with the supporting technologies, to a software-defined data center, packed with useful features. Those features cover every single aspect of the data center – networking, storage, and compute.

The last two versions of Windows Server introduced Storage Spaces, IP Address Management and multi-tenant site-to-site VPNs. Server 2016 is building on those and bringing additional features like Storage Replica.

Security Improvements

Windows Server 2016 also addresses a number of security issues in Hyper-V that are designed to bring more protection to Virtual Machines and halting malware, administrator attacks, and other attack vectors in their tracks.

Microsoft is completely aware of one of the biggest reasons why the Cloud has not been adopted in the way they had hoped, and that is corporate trust. Microsoft is now determined to prove to everyone, both corporate and consumer, that cloud solutions can offer data center security that is at least comparable, if not better, than it ever used to be.

Windows Server 2016 also offers support for a virtual TPM to be enabled in the virtual machine, and then configured.

The main benefit of this is the ability to be able to enable BitLocker encryption for all guest virtual machines, which will have the benefit of stopping unauthorized access to any files or to the system that is contained in the virtual drives.

Shielded Virtual Machines in Server 2016 is yet another security feature that allows a guest virtual machine to be protected from the host server administrator.

In this scenario, while an administrator can stop or start the shielded VM, they cannot alter its configuration, see what is on the virtual disks, or view processes that the guest OS is running.

This is the ideal solution for large environments that don't want the management side to see what is on a customer virtual machine, or for those industries that operate a need-to-know policy or strictly enforced separation of duties.

Enterprise Mobility – Identity in the Enterprise

Right now, managing identities within the Enterprise setting is cumbersome.

Windows 10 is going to change all of that and allow empowerment of enterprise mobility. The way things are set up now is as follows: all the users in the enterprise want to access everything, from anywhere, and from any device.

Management wants to control everything; as well as ensuring that data is secure and protected. This becomes difficult when end-users have the same login details from every site that they visit, and use the same password.

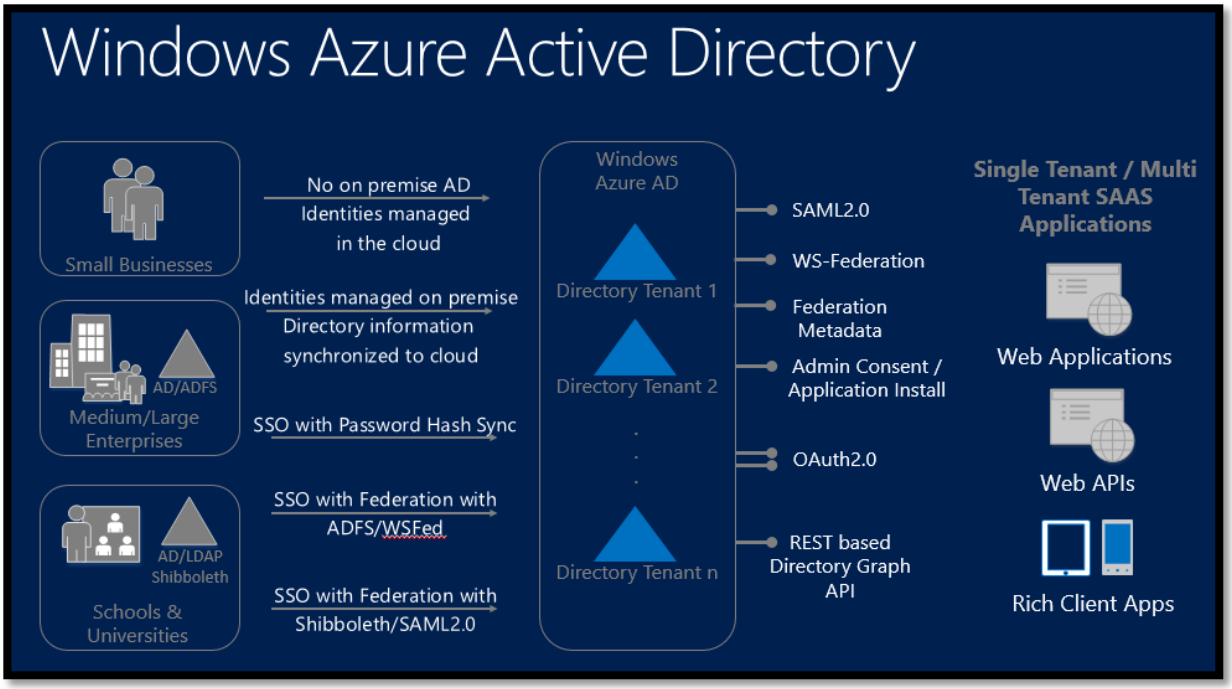
While this might be easy to start with, it all falls apart when one site requests a password

change … and then another one does … and another … and so on. The end user has to remember all of these different passwords.

So, in steps the HR department, with their company credit card to hand, and buys the latest software to manage everything. Then they have a problem – security. Thus they come to the IT department, confess what they've done, and then hand the problem over for them to solve.

That's where Windows 10 changes everything. Identity is the foundation to building the enterprise mobility strategy. Most businesses already have on-premises identity strategies, use Active Directory and other directories, and have their firewalls already set up.

They also have access to cloud apps on a separate infrastructure. Windows 10 brings something a little bit different and a whole lot better.



It's called **Azure Active Directory** and it brings together on-premises and cloud access in one easy place.

All you need is one simple connection to join the two together, and Windows 10 provides all the tools you need to make that connection.

What Azure Active Directory brings to enterprise users is one single sign on that gives you access to everything that you need. Before we go any further, let's just spend a minute talking about Azure Active Directory.

What is it, exactly?

AAD is an identity and access management solution that combines:

- Directory services
- Advanced identity governance
- App access management
- Standards based platform for developers

Azure AD allows your users to access 1000s of apps through one single sign on. Better than that though, it also allows you to pick and choose which apps they have access to through a number of different options.

AAD is:

- **Easy to use**. It provides enterprises with a simple way of managing identity and access to organizational apps and services, both on-premises and in the cloud. There are more than 2000 apps already reintegrated and it is easy to integrate your own apps with the single sign-on support.

- **Designed to empower users** by allowing them to sign on with either a work or a personal account for access to on-premises web and cloud applications. With self-service capabilities, they are also able to perform many of their own administrative tasks without having to contact the help desk.

- **Designed with enhanced security in mind**. Your enterprise can protect on-premises and cloud data by ensuring that proper access is given. You can also monitor the system for any anomalous activity and detect and deal with potential threats.

- **Set up to allow hybrid identities**. This allows you to integrate on-premises directories and enable workers to access corporate resources both securely and consistently, with just one single organization account. AAD can be used to enhance on-premises infrastructure, allowing self-service, security tools and built-in app connectivity.

- **Set up to provide a comprehensive reporting and analytics** system that enhances your security, allows you to monitor usage and view the performance of your environment.

Cloud App Discovery

Cloud app discovery allows you to monitor apps in the cloud. Right now, in the average enterprise, there are about ten times more cloud apps in use than the IT department realizes.

Cloud app discovery allows you to see exactly which apps are being used, who is using them, and how often they are used. You can export the details from your reports directly to a reporting tool and include them as part of your regular reports as well as using it for data

analysis.

Managing Your Directory on the Cloud
Another useful feature included in AAD is the Microsoft Identity Manager. This allows you to manage your on-premises identities and connect and share on-premises directories to Azure.

There are already more than 2,400 SaaS apps in the gallery and more can be integrated and added as needed, including those that are published using AAD Application Proxy. Because AAD stands in the middle, all of these apps and directories can be accessed on-premises and from mobile devices.

AAD App Proxy includes a connector that automatically connects it to the cloud, allowing for seamless syncing.

AAD also includes a comprehensive identity and access management console, providing centralized access admin for all apps, both reintegrated and other cloud based apps.

This makes life much easier for the end user because the admin can:

- Put users in groups and allow groups to access different sets of apps.
- Set up enterprise accounts for certain apps – one account, multiple users – and only the admin will know the login details. This prevents accidental sharing.
- The admin can also provision or de-provision users. If a user leaves a particular group or leaves the organization completely, he or she will automatically be de-provisioned, cancelling access to all of these apps.

There are also other built in security features to protect enterprise apps, namely:

- Security reporting that monitors and detects inconsistent access patterns and throws up alerts.
- The opportunity for an admin to step up an app to multi-factor authentication – if they doubt that a user is who they say they are, for example, they can add another step to the authentication process which will block access until that step has been successfully completed. The step could be a phone call or a text message.
- The access policies will depend on the state of a user's device, their location, and group membership.

How Microsoft Windows 10 Will Protect Your Data

As well as protecting your identity, an area that Microsoft is making great strides in, they are also working hard on coming up with new solutions to protect your data and information.

Next to identity, theft of data is the next most serious consideration for consumers and organizations alike. Current security systems only protect about half of your IT system and even then, that isn't fully protected.

Every time you switch on your computer or Windows mobile device, or every time you access the Internet or open an email, you run the risk of a hacker swooping in and taking control. Microsoft intends to stop that in its tracks with two upgraded systems.

Azure Rights Management and Information Rights Management

When data leaves your device, Microsoft has something called Azure Rights Management and Information Rights Management, both of which help to protect the loss of data from documents.

As of now, a user typically has to opt in to activate the protection that these two services offer and that can leave an enterprise with a bit of a problem – a gap through which data can be leaked, whether deliberately or inadvertently.

Azure Administrative Tasks

The end user can perform many of their own administrative tasks by visiting http://myapps.microsoft.com, or through the relevant app on Android or iOS. Through that, they can see how many apps they have access to, from any device.

They can also see all of their managed devices and can reset their own passwords without the need for the IT department to get involved. Lastly, they can also request access to apps and/or groups through the self-service options.

Azure Active Directory is embedded in Windows 10 and is available through three subscription options, depending on your needs – free, basic and premium. Over the next year, Microsoft is investing more time and money in improving the following areas of AAD:

- Admin Units – ability to split admin duties into groups
- Business-To-Business – a new feature that will be available that allows you to share your resources with business partners through AAD
- B2C – Identities for business to consumers
- Conditional Access – Ability to block outside access
- Privileged Identity Management – Options to make admin access temporary or permanent
- AAD Join – AAD controls everything and is fully embedded with Windows 10

Data Protection in Azure

Global cyber-attacks are on the rise and so are the costs associated with it. It is estimated that cybercrime extracts around 15-20% of the value that is created by the Internet.

In the last 2 years in the UK alone, more than 80% of large businesses and 60% of small ones reported a cyber-breach and, globally, the number of security compromises reported rose by about 34% in 2014. The estimated cost of cyber-attacks, in terms of lost growth and productivity, is thought to be around $3 trillion.

In order to protect their customers' data, Microsoft has introduced a number of security measures in Azure Active Directory. By default, AAD provides strong protection and there are also options that customers can choose to enable as well. First, let's look at data in transit.

By this, I mean data that is sent and received between a user and the service, between data centers and between users. Data that comes through the Microsoft Azure Portal or through storage API is automatically encrypted using https, along with strong ciphers. By default, FIPS 140-2 support is enabled to comply with government security standards.

All data that is imported or exported is encrypted with BitLocker, which is built in to Windows 10 and all customer data that goes between the data center and storage facilities is also encrypted.

For customers that access data in a storage facility or container, there are two options of access – http and https – Microsoft recommends using https as this is secure and encrypted.

If a customer chooses to access or send data using a web client, TLS should be implemented – TLS is Transport Layer Security and it is a protocol that makes sure that third parties cannot intercept or eavesdrop on data that is being sent between applications and their Internet users.

When we talk about data at rest, we are talking about data that is stored in one of a number of different containers. The containers that Microsoft provide data protection options for are listed below.

Virtual Machines – Windows/LINUX

Azure disk encryption is provided using BitLocker for Windows or DM-Crypt for LINUX. Virtual hard drives (VHD) are encrypted for both Windows and Linux VMs. The customer is given the option of enabling disk encryption on both the boot and the data volumes; the encryptions keys are stored in the key vault. This also applies to Azure Gallery and to running a VM in Azure.

How it Works

- The customer uploads their encrypted VHD to their Azure storage account

- They provision their BitLocker encryption keys or LINUX passphrase in their key vault and gives access to the platform to provision the VM
- At this point, they opt into disk encryption
- Azure service management updates the service model with the key vault and encryption configuration
- The platform provisions the encrypted VM

Key Vault Security

Everything revolves around the key vault because this is where the keys are stored – the encryption keys that are protecting your data. These keys are kept in an isolated vault so that, should your storage container become compromised, only an image of your date can be stolen – this is useless to any thief because the keys that unlock the data are elsewhere.

It is important to note that:

- Only the customer can control access to the keys that are in their private vault
- The customer can enable monitoring and logging, collecting the logs in their storage account – this enables them to see who has access or who has attempted access to their vault
- Encrypted disks are stored in the customer's storage account and Azure storage will automatically replicate them – the customer has control over how many copies are made
- Azure has no default access to the key vault – the customer must grant Read or Write permission.
- Azure cannot access the disk encryption feature in the vault

Azure Storage – Blobs, Tables, Queues

Client side encryption allows users to encrypt their data before it is uploaded to Azure as well as decrypting it again after downloading. Again, the keys are kept safe in the key vault and the storage service will never see the keys, nor is it capable of decrypting any data. For cloud-integrated storage, all data is encrypted on premises and is backed up in Azure.

SQL Server and SQL Database

Using TDE – Transparent Data Encryption – technology, the entire contents of a database in storage can be encrypted using a database encryption key, which is an AES-256 symmetric key.

This key is protected with a service-managed certificate, which is protected by SQL Database Server. The certificate is set on a 90-day cycle, after which a new one must be produced, thus lowering the chances of compromise through standing access.

HDInsight uses Azure storage and SQL Azure DB encryption to protect your data while Azure Backup Service uses Azure Disk Encryption to ensure your data cannot be lost, stolen or compromised in any other way.

Access Control and Auditing

So, Microsoft Azure AD has encrypted and protected all your data and your keys are stored away safely in a vault that only you have access to. That's not all there is to it though. Many of the fundamental security risks still exist on premises.

Mitigate the Risk of Compromised Accounts

Weak authentication is the key problem to security. Weak passwords, passwords that are written down or shared, or passwords that are stolen are the biggest way in for any attacker. Microsoft is looking to eradicate passwords and bring multifactor authentication in across the board.

All user accounts can be secured using Azure MFA, usable with both Azure Active Directory or the Windows Server Active Directory Federation Services, and this is backed up by a second factor for identification, usually a text or a phone call.

Users can also use existing PKI – smart cards or virtual smart cards – to protect their accounts using ADFS with the on-premises infrastructure.

Limiting Permissions

This is one of the most difficult concepts to get over but permissions should follow a "Least Privilege" principle, i.e. access is only granted when it is necessary for a specific role. Azure RBAC – Role-Based Access Control – now contains 20 different rules that can be assigned to users, under the headings of owners, contributors and readers, as well as custom roles.

Owners have full access to the data; contributors can add to it but cannot do anything else, while readers can only do just that – read the content but cannot make any changes. Users within the enterprise, or within groups can be given access to data under one of those roles, allowing IT to control who does what.

Privileged Accounts

Super user accounts deserve special management because they produce a special risk. JIT – Just-In-Time – access can be enabled, removing the risk of an attack through standing permissions or standing access.

JIT gives a user access to admin when they need it for a limited period of time and only to the feature they need access to. Managers can also set something called Azure AD PIM – Privileged Information Management.

This is where they can monitor the system, see who has access and who wants it, and set the policies that transition permanent access to temporary.

Using auditing and logging, management can also detect suspicious activity, including irregular logins, down to user level, through the use of advanced detection tools that are constantly monitoring every user account. In this way, threats can be detected and action taken before they become a problem.

What is the Operations Management Suite?

OMS, or Operations Management Suite is another new feature in Windows 10 and it is a simplified IT management solution.

It's a hybrid management service that supports Azure AD, AWS, VMWare, OpenStack, LINUX and Windows Server, and it connects to on-premises data center and cloud environments, giving IT managers one single portal that allows them to collect, analyze and search through thousands of pieces of data and records that are spread access the workloads and the servers.

These days, there is so much information, so much data, and so many apps that are spread across the infrastructure, across the cloud and cloud services, it is getting difficult to know how to handle it all.

IT managers still have the task of managing and securing all that data, no matter where it is kept and OMS makes that easier to handle.

The benefits gained from OMS are:

Log Analytics: Collect and search across many machine sources of data to identify where the problems lie in operational issues.

Availability: Regardless of where servers and apps are, OMS includes integrated recovery for them all, which is enabled by default.

Automation: Orchestration of complex and repetitive operations to provide a more efficient and cost effective hybrid cloud management system.

Security: The ability to monitor and identify the status of malware, find missing system updates and implement them and to collect security related events for analysis and audit purposes.

Extended System Center: OMS combines with the existing System Center to extend its capability to deliver the full hybrid cloud management system across any cloud or any datacenter.

Hybrid and Open: Very few organizations are now housed in a single data center and OMS steps in to manage your hybrid cloud, irrespective of the topology or the technology being used, and integrating seamlessly with the existing on premises infrastructure.

All of this makes protecting your data and preventing breaches and compromises easier than ever before.

Mobile Security

These days, not only do we use our devices for personal use, we also use them for business.

More and more business employees use smartphones and tablets for work and Windows 10 Mobile, formerly Windows Phone, is designed around segregating personal and business uses on the device and providing the right level of security and control over the business side.

Mobile devices are the number one target for a cyber-attack and, up until now, they have been more difficult to protect.

Microsoft has added in a number of security layers to protect a Windows mobile device from any number of malware and malicious attacks, allowing both end users and enterprises to relax a little, knowing that their security is in good hands.

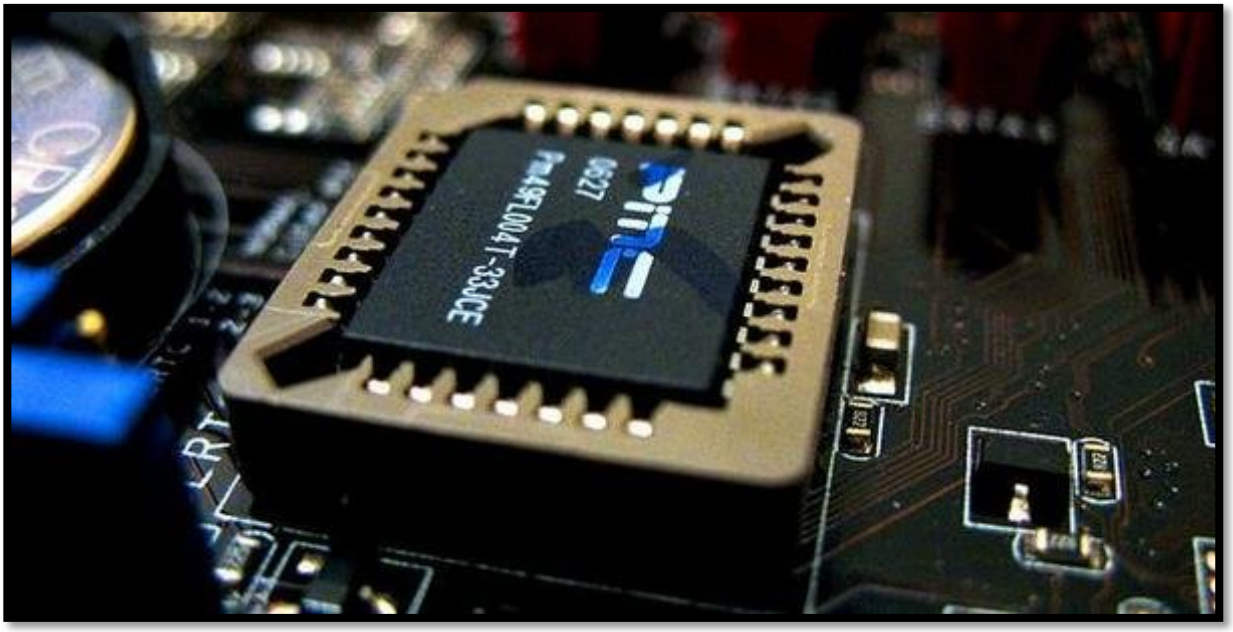
The first line of defense is a layer of security to protect the actual hardware. All new Window devices are equipped with a TPM 2.0 chip and have UEFI Secure Boot enabled. This is a Windows requirement and cannot be disabled by anyone.

The UEFI Secure Boot system is designed to start checking your system as soon as the device is powered on, checking that the TPM is the real thing and that the firmware, and any other software that starts up, is genuine and has been signed.

If it has not, it won't run, it's that simple. Once everything is declared as fit for work, UEFI will boot into the Windows Boot Manager and then into the OS itself.

The only exception to this is if there is a need to replace the OS through the use of a recovery application, in which case, the boot manager will boot into flash mode.

Just how secure is UEFI though? During the manufacturing process, a number of public key hashes are fused. These hashes link to specific processes that take place in the device.



All the drivers, loaders, applications and firmware within UEFI must be signed and a UEFI database will list all keys, image hashes and certificate authorities, stating whether they are trusted or untrusted.

A secured rollback system is in place – once UEFI has checked a system and declared it to be a safe and genuine environment, secured rollback prevents a rollback to any version other than that one, effectively stopping malware that could have been hiding in an insecure

version from being installed. UEFI will be kept fully up-to-date through the Windows Update system.

Other security of the hardware includes TPM, which was discussed earlier and which enables keys to be isolated from the OS – this means that if the system is breached in any way, those keys cannot be stolen – not even the OS itself can access them.

Health attestation completes the hardware protection layer. Health attestation is vastly improved from the version that came with Windows 8.1 and it allows Windows 10 to carry out a health check to the Cloud before it can gain access to any internal resources.

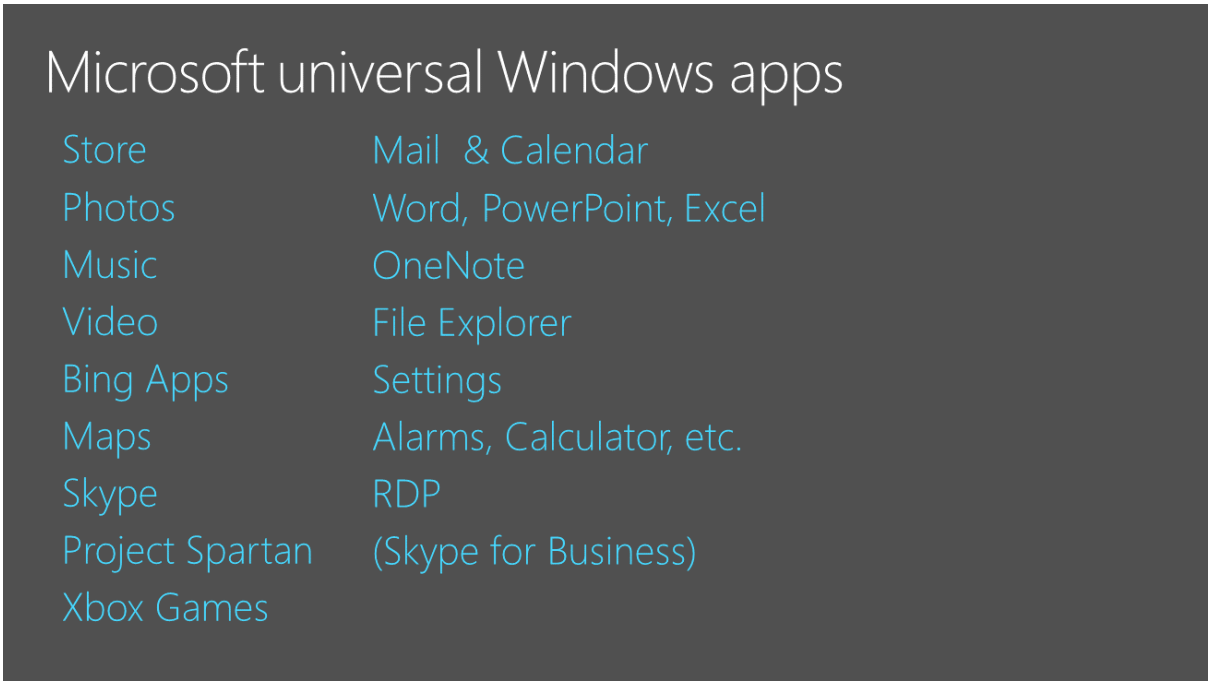
Features checked include Secure Boot, BitLocker, and other operation-essential features that need to be 100% healthy before Windows 10 can run fully.

The next layer of security is the Windows One Core. We examine the App Platform first, because it is what users interact with when they use Windows 10 on their mobile devices.

Windows 10 only supports modern apps or RT apps depending on your system, and not Win32 apps. The new security layer for the app platform model works like this:

- The OS runs in a TCB – Trusted Computer Base – where nobody can access it and nobody can make changes to it.
- Apps that are installed via the store or are shipped with a device are installed in a sandbox, or in a Least Privilege Chamber (LPC). When the app is put into the chamber, it is given permissions based on what it needs to run and no more. This means that it will only do what it says on the box and cannot be touched by malware that tries to order it to deviate from that. The permissions that are linked to that chamber cannot be changed or elevated by anyone, only by an upgrade with a new manifest.

Windows 10 for Mobile will come with a number of preinstalled apps, as follows:



All of these are modern apps and can be fully updated with new functions without the need to go through the mobile operator to deliver the update – instead, they will be updated through Windows Updates, under a feature called Windows as a Service.

Access to apps and services has always caused concern in terms of security. Microsoft is implementing a number of new features on both the Desktop and the Mobile versions of Windows 10 that will secure access more than ever before.

Many users are fed up with the current password system. Not only is it too much to have to remember multiple passwords, it is simply not secure. Most people tend to stick to the same password for everything – there are so many places that require ID to be proved now that you could probably produce a book filled with all the different access details you would need.

Businesses want more control over what their end-users are accessing, not to be nosy but to better understand patterns and to detect potential threats and/or security leaks. So Microsoft has come up with Windows Hello.

We know all about this from the desktop version and the Mobile version is the same, so to recap:

- Window Hello is a biometric system
- It uses clean IR for iris or facial recognition, or a fingerprint reader
- New hardware will need to be produced to complement this feature because today's mobiles do not have the capabilities to recognize facial or iris details; some may have an integrated fingerprint reader, this may also need to be updated; devices also need to be capable of 3D vision for detection purposes

- Microsoft is working hard to increase the FALSE Acceptance Rate – currently at 1/100,000, and to reduce the FALSE Rejection Rate, which is currently between 2-4%
- Passwords and/or PIN numbers may still be used, but the difference here is that these can be covered by MDM – Mobile Device Management – especially in BYOD situations

Microsoft Passport is another system that will be on Windows 10 for desktop and mobile and is a replacement for the old password system. Instead of a password, a key pair is generated, one public and one private, after a user has created trust with their IDP – identity provider.

The private key will never leave the device it is paired with. Users have a choice of providers, anyone that is a part of the FIDO Alliance, such as Microsoft themselves, Google, Facebook, Twitter, etc.

The difference with business users is that an end-user will create their Passport account, specifying whether the account is for business or personal use. When the user has to create trust, the IDP may require that a second layer of authentication is included to prove identity, perhaps a phone call or text message.

Once the trust has been created, the keys are produced and, when validated, an authentication token is sent to the device. That token can then be used on a number of third-party relying resources that trust those tokens.

An access token is created and this can be controlled by MDM – you can set a time limit on the access the user has to a particular site, meaning that they will need to re-authenticate after that limit expires if they want to gain access to the site again.

Enterprise expectations for corporate access are "anytime, anywhere, secure remote access", as shown below:

Furthermore, to enable data and access to be protected to and from a device, Microsoft has expanded their VPN capabilities in Windows 10. Again, these can be MDM-managed in a two main ways:

- On a per-application basis – IT can give user access to specific sites through a VPN and this is fully integrated with Enterprise Data Protection
- On an "Always-On" basis, which means users will access sites through a VPN on a permanent basis, until they turn it off; this can be managed and IT decides whether to allow a user to disable the VPN or not

BitLocker is also present on all devices, and this is designed to protect the data on a mobile device when it is lost or stolen. All corporate data is encrypted, which provides protection to them from cold boot attacks. In order for this to work, UEFI Secure Boot must be enabled, which is standard on Windows 10 Mobile.

Enterprise Data Protection on a mobile device is essentially the same as it is on a desktop environment. It is MDM-dependent and, once enrollment has taken place, trust has been created. The device will then be enrolled in MDM at the same time as the authentication token is issued.

This means that IT can set key policies to protect data on each individual device and for each individual user. This includes managing keys, setting enterprise apps for users, protecting the network and storage facilities, and audit controls. Part of this includes enterprise apps not being usable on a personal login, as they are kept entirely separate.

There are enlightened apps as well, such as MS Office. For example, if you open a new Word document or Excel template, a message will appear asking if this is for personal or business use.

Personal use documents are not encrypted whereas the enterprises ones are.

IT can also set permissions for things like Copy/Paste actions. Let's say, for example, that you copied a piece of data from a corporate document or website and tried to paste it to a personal one. IT can set a number of permissions here:

- Block altogether
- Allow
- Or Allow the user to decide

If a user opts to go ahead and paste the data, even though they have been warned it is of corporate origin, their actions are subject to audit controls.

Finally, IT can remove permissions automatically for people who leave employment or move to a different area of the enterprise. This means that any access to apps they had permission to use will automatically be removed.

MDM – Mobile Device Management and the Business Store

Today's business needs are changing fast and Microsoft is offering enterprise management what it needs with Windows 10. It used to be that a workday was a simple 9-5, Monday to Friday thing, with employees sitting at their desk in the office.

Their PCs would be connected to a LAN network; PCs that were provided and managed by the enterprise. They had just one device ecosystem to use with an extended operating system.

In this scenario, devices would have a long life because they were kept serviced and updated. Users could share files and data on-premises and their access to apps was controlled by the organization.

Management would be deeply involved in setting controls and policies and malware was seen as criminal activity and vandalism. The network perimeter worked as a good defense system and devices were vertically integrated for workers.

So, what's changed? The advent of the mobile device is what changed it all. More people are using their mobiles for work, and enterprises need to change to incorporate this new environment. Of course, this means that those devices are being used 24/7 for both work and personal activities.

Instead of working on a desktop connected to that LAN network, we are now working on our mobile devices, connected to any network. Not only are we using personal apps, we are using corporate apps, all on the same device.

We can use any number of ecosystems, including Android, iOS and Chrome, as well as Windows. Our devices are not lasting as long as the specific desktops that we had before because of the changes in hardware and specs.

Instead of using on-premises apps, we use SaaS and file-sharing apps. This means that access control is much harder because instead of being confined to the organization, now it is spread out over the user and the device as well.

Cloud-based management means there are fewer controls and malware is seen more as a weapon used for espionage. Instead of being knowingly secure, we must now operate under the assumption that our device has been breached and, if it hasn't, it will be at some point. Also, instead of vertically adapted devices, we now have dynamically adapted devices.

With more organizations and employees adopting BYOD, the security challenges are much harder. The sheer diversity of devices, apps, and networks is astonishing and with the loss of the perimeter defense system comes the much higher likelihood of attack.

Look at it this way – by the end of 2018, more than 50% of all users will automatically turn to their mobile device for online activities, before they even think about using a desktop environment. By the end of 2016, more than 40% of the world population will own a smartphone or a tablet. Add to that the more than 6.5 billion wireless connections in use today and you can see the scale of the problem.

Attacks are increasing in intensity; they are more organized, more persistent, and specifically targeted. In the last couple of years alone, the number of attacks on major, well-known retailers, such as Sony and eBay, have increased significantly and if they can be hacked, so can you.

The final layer of security that Microsoft has included is App Security. Up until now, there has been no control over which apps users download and install and from where. With

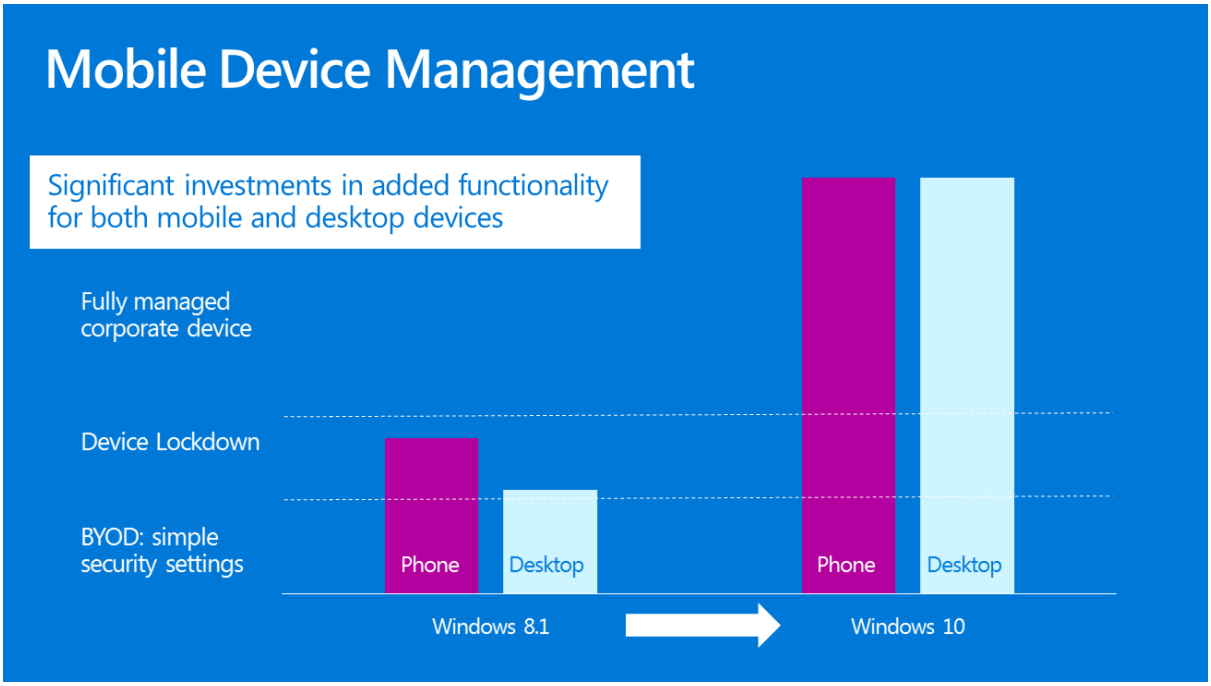
Windows 10, extra layers have been added in. Users can still purchase and download apps for personal use using their own LIVE ID.

However, there is now a Business store where app licenses can be purchased for use by end-users. These are placed within the Company Portal, a separate store within the store and permissions are given to the people that need them. This makes app deployment much easier, safer and far more secure.

Windows 10 brings choices to managers – traditional management, including Group Policy, System Center and all the related components, and then there's MDM, or Mobile Device Management. This has undergone some serious enhancement since its inception in Windows 8.1 and the capabilities have been expanded with Windows 10.

With Windows 8.1 and Windows Phone 8.1, devices had to meet enterprise security requirements before being able to access corporate data. Windows Phone 8.1 went a little further and enabled device lockdown, meaning that devices could be configured to run specific apps.

So, as shown below, Windows 10 devices are fully managed corporate devices when deployed by businesses.

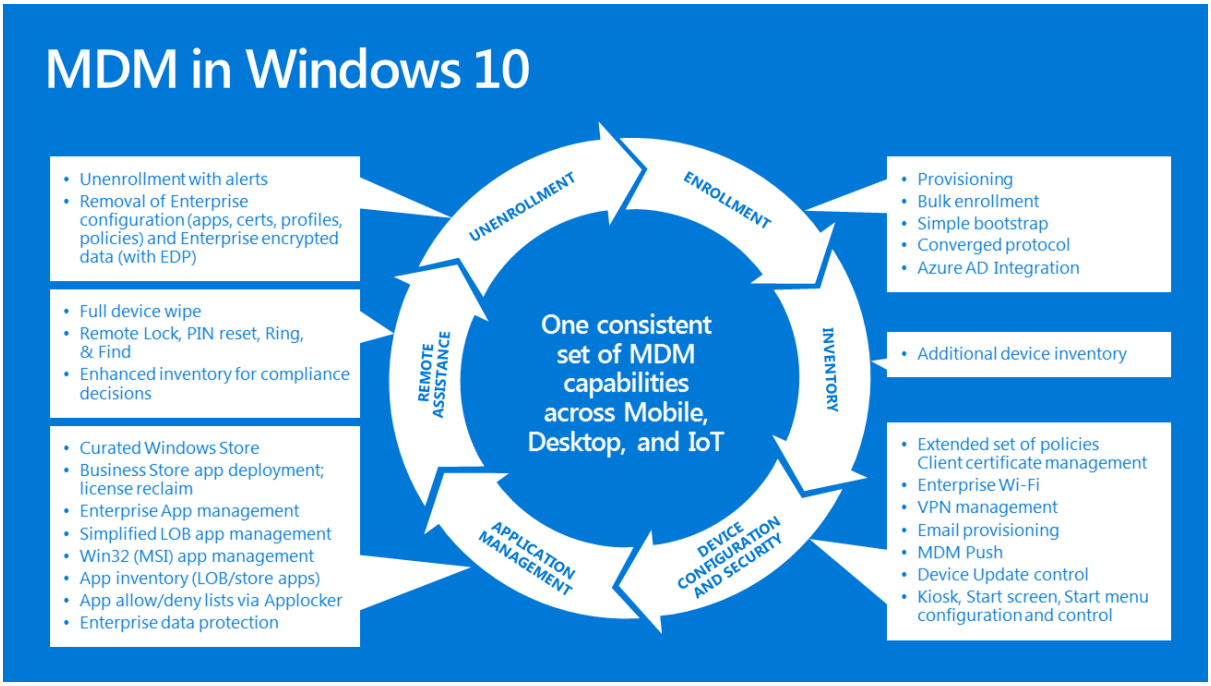


In Windows 10, Microsoft have enhanced each separate phase of MDM provisioning, including:

- Easy enrollment capabilities for automating MDM enrollment of the specific device as a part of the AAD Join process
- New configuration and Start Menu management tools

- New Windows Update controls, allowing you to set when specific updates are rolled out to MDM devices
- New configuration settings for Enterprise Data Protections and AppLocker
- Better integration with Windows Store and Business Store for automated app management
- Full capabilities for wiping devices

All of these capabilities and more will be fully supported on all types of devices, including Window Phones, tablets and Internet of Things devices, as illustrated below.



Active Directory is used by virtually all businesses today to provide security and identity services. All of the AD capabilities will be fully supported in Windows 10, but the biggest single change is the addition of full support for Azure Active Directory.

This means that Windows 10 is aware of all the directories and accounts in AAD and can use these in many different ways.

First, though, it is vital that you understand that you do not need to choose between AD and AAD – if you have AD you will automatically be able to use AAD as well, taking advantage of the extra capabilities.

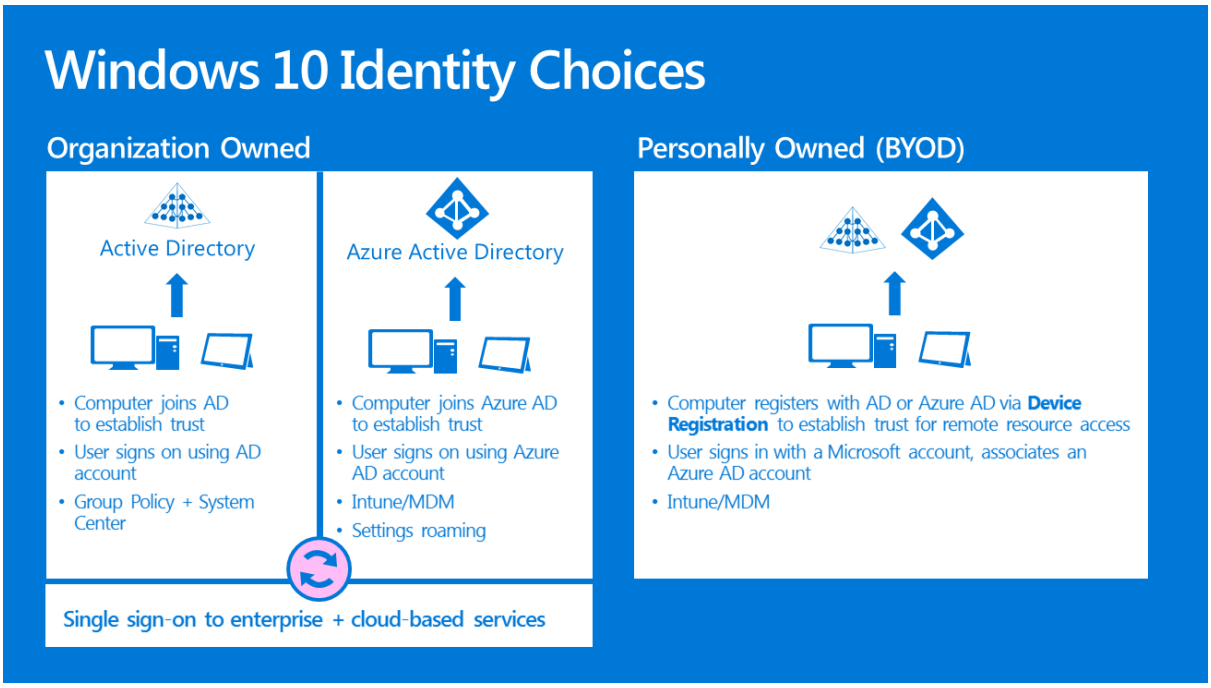
Windows 10 is able to support management of BYOD (personally owned), organizational devices and the same remains true when we talk about identity as well. A device that is owned by the organization can be joined to an AD domain to establish trust and can then be signed on with an AAD account.

You can also choose to join the device as an AAD tenant and then sign on with an AAD account, which will give full support for roaming through Azure storage.

The real value comes when the device is combined with both. After the AD domain has been synchronized with AAD, extra benefits are available in the form of single sign-on. Windows 10 automatically recognizes the association between the accounts, meaning that AD users can access cloud based services without having to log on again. And vice versa – AAD user can access on-premises data with no need for additional authentication.

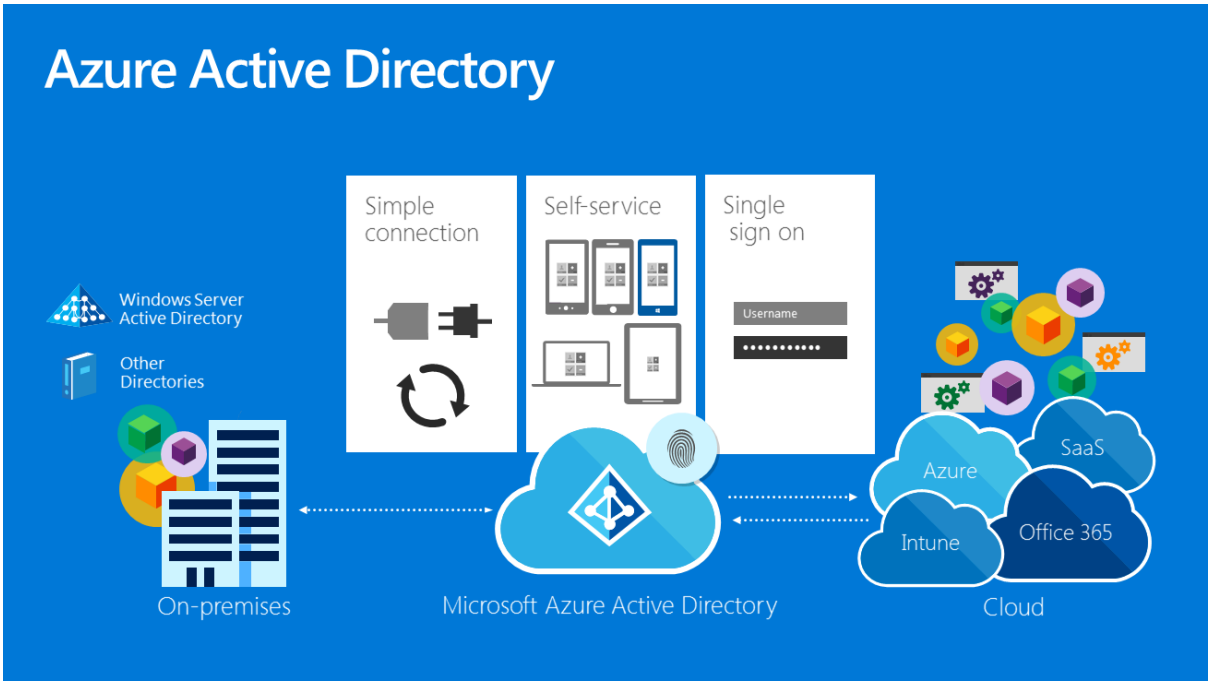
I'm not just talking about Microsoft cloud here though; I'm talking about having single sign on for hundreds of different SaaS (Software as a Service) providers. Simply define the connection between AAD and the services you want, and you are all set for single sign on.

For BYOD devices, Windows 10 will support device registration for registering personal devices. Once it is registered, as shown below, you gain an additional level of trust, which means that access would be allowed to all sorts of service and apps that an unregistered device couldn't get.



For AAD to be used, an AAD tenant must be set up for the organizations (those who use Intune or Office 365 will already have this). After that, the synchronization takes place between the AD domain and AAD using Azure AD Sync. This runs periodically to ensure that AAD is kept fully up to date.

All devices can join AAD or they can just leverage AAD accounts. Either way, they will gain single sign on access to cloud services, as well as getting app roaming settings and data for a wide range of devices.



Browser Security

On Windows 10 Phone devices, there will be only one browser – Edge. This is the replacement for Internet Explorer and is Microsoft's new, cutting-edge browser.

Of course, with a new browser comes a whole set of fresh security challenges and on a mobile device used as a corporate device, Edge can be MDM-managed.

Microsoft are introducing a whole new set of policies for Edge. To start with, there are Group Policies, which use the existing GO/GPP/SCCM infrastructure. There are also MDM policies that are on a par with the group policies and are brand new to Windows 10.

The MDM policies provide cross platform management capabilities for different operating systems and are a standards-based infrastructure. All of these packages add up into one nice, and neat result – a fully managed Microsoft Edge.

MDM is a way of consistently managing multi-platform devices using Extensible Markup Language, or XML, for data exchange. XML defines rules for encoding data in a way that both the device and a human can read.

MDM is fully supported by all major mobile manufacturers and it covers the entire life of the device, including:

- Device enrollment
- Configuration
- App management
- Remote assistance and inventory

- The retirement of the device

Microsoft Edge policies are scenario-driven, which means that they will depend entirely on the use and permissions of the device and the individual.

They are also consistent across all devices, regardless of what they are and include the following:

- Enterprise site list configuration
- Sending the Intranet to IE (for compatibility reasons)
- Allowing the browser on a mobile
- Default browser
- Allowing pop-ups
- Configuring cookies
- Allowing SmartScreen
- Allowing Active Scripting
- Configuring the home page
- Allowing Do Not Track
- Allowing Autofill
- Configuring Password Manager
- Disabling search suggestions in the address bar

All of this is designed to help keep corporate data safe by monitoring what corporate users can and cannot do and the capabilities they have access to.

This reduces the risk of malware, or any other unwelcome threat vector making it onto the mobile device and potentially accessing corporate data.

Enterprise Mobility Suite

Enterprise Mobility Suite (EMS) is Microsoft's answer to access control security. Right now, most corporate data is stored on premises, most likely in Active Directory, and is accessed through the Internet via browsers on mobile platforms and PCs.

In short, there is actually very little control over who accesses what, from where, and when. The weakest point in the system is the DMZ, or the perimeter, because there are so many ways of access that are difficult and cumbersome to keep control of.

Microsoft's solution is to build access control into all apps, on-premises and cloud services, as a way of containing data and stopping it from leaking.

So, at the base layer of EMS, on the mobile device, is MDM – Mobile Device Management. This is pretty much standard on most corporate devices and allows access to various services.

The next layer, compounding that, is Office 365 Mobile Productivity and this encompasses all Office apps, such as Word, Excel and OneDrive. This comes with two built-in libraries – Active Directory Authentication and Intune Data protection.

Finishing off is extensibility, which allows business apps interoperability with Office Mobile.

The first and most important part of EMS is conditional access control, a part of Azure AD premium that is made up of the following layers:

- **User attributes** – the user must identify who they are and the groups they belong to determine their access to specific apps. This also determines whether multi-factor authentication is required for them.
- **Device authentication** – the whole idea of security in Windows 10 is to tie a user to a device. Not only does the user have to prove who they are, they have to prove their device is compliant, is MDM-managed, and is not lost or stolen before they can be given access.
- **Applications** – these are based on business sensitivity and users are only given access to the apps they need, with IT setting up the appropriate permissions.
- **Network** – The EMS can determine where the user is accessing the network from and can decide if MFA is required, based on location and whether they are inside or outside the network

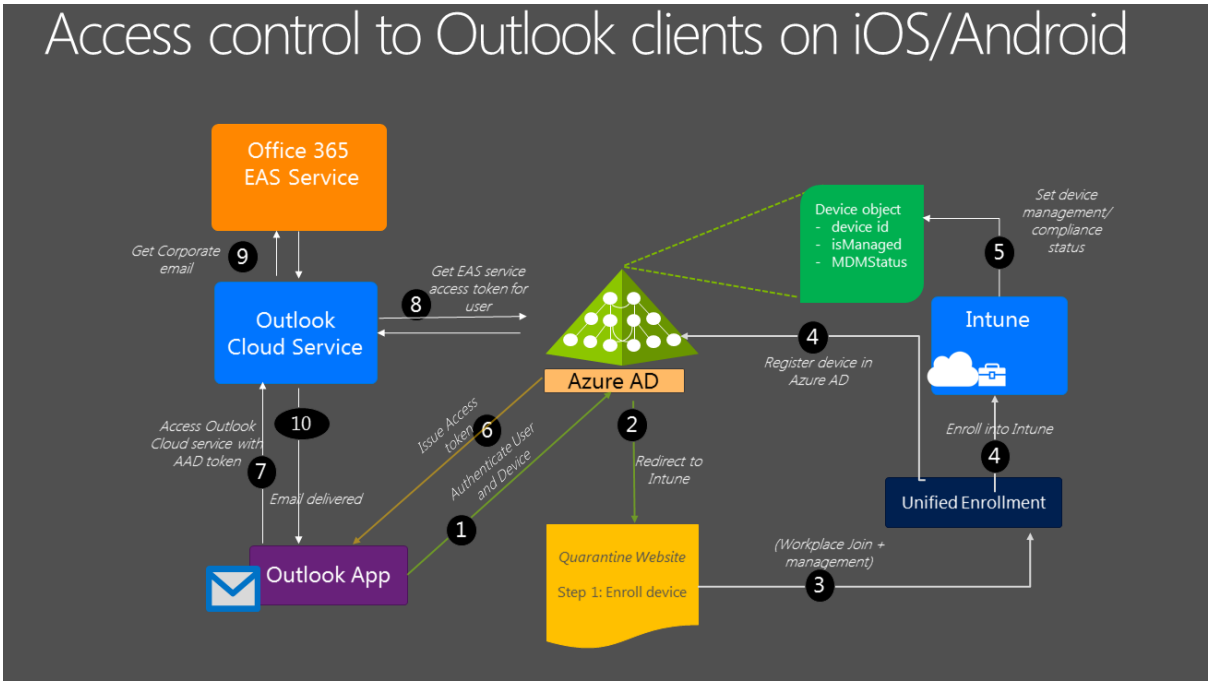
Office 365

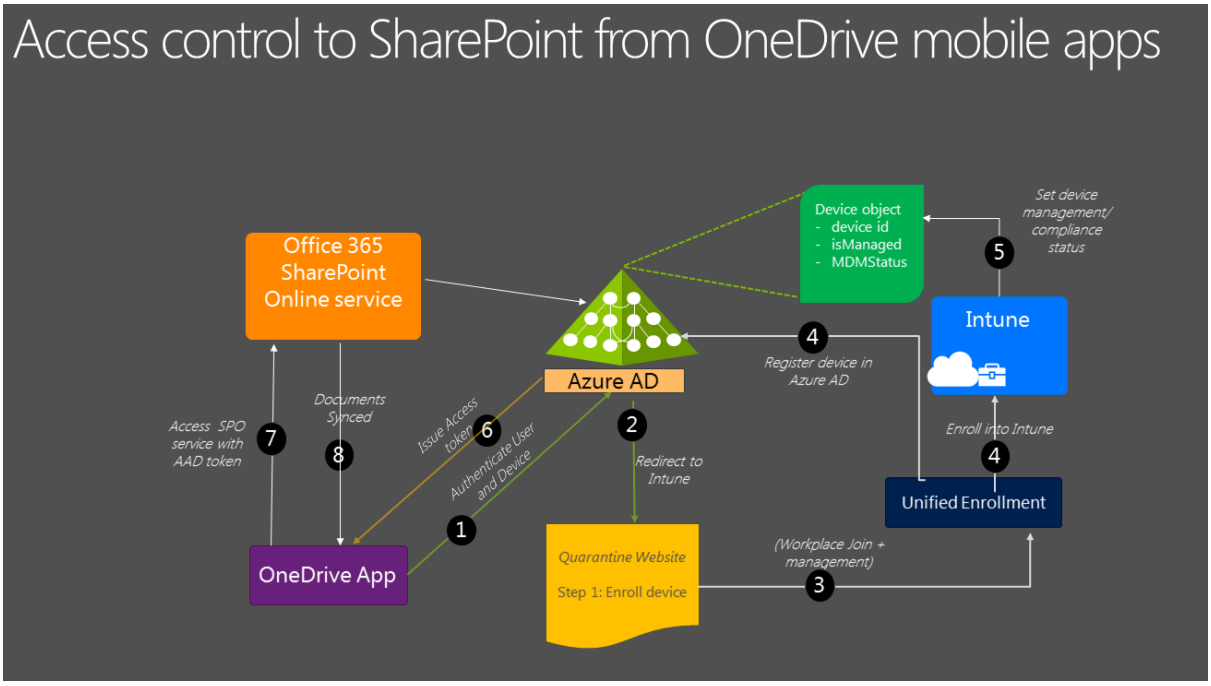
Under conditional access controls, users are blocked from using Office apps until they have been enrolled in MDM and are compliant with company policies.

Once they have been granted access, after identity authentication, all app data is encrypted and sharing is restricted to managed apps. Applied policies are enforced, which gives all Office 365 apps a built in layer of protection.

For data that is shared externally, i.e. emails and their attachments, the data is encrypted to secure it. Should a device be lost or stolen or an employee leave the company, all accesses are revoked and corporate data can be remotely wiped, taking access away from that individual and/or device.

The following two diagrams show the same access controls for the use of Outlook on iOS and Android and access to SharePoint from OneDrive Mobile:





Conditional Access to Azure AD Connected Applications

Azure AD comes complete with more than 2,000 preconfigured apps and access can be controlled on a per-app basis with MFA, per-app basis from extranet, and apps blocked from extranets. These are SaaS apps and IT can target specific groups of people to have access to specific apps only or can block groups or individuals from accessing certain apps. This means that users get to see only what they need to do their jobs and no more, restricting the chances of data leakage.

Device Conditional Access

Access can be restricted to only those devices that are managed and are compliant. Auto-Workplace Join PCs will be automatically marked as managed and will be included in the access policies. Any device whose attribute changes will have their access revoked and the user may be asked to provide a new set of credentials.

Support is built in for a number of different major SSL VPN providers, including Juniper, Cisco, Checkpoint, SonicWALL, SFS and other custom VPN payloads. Native VPN standards such as PPTP, L2TP and IKEv2 are supported, as is app-triggered VPN and multiple Wi-Fi authentication types, like WEP, WPA/WPA2, and Enterprise.

Windows as a Service – More Security via secure updates

We all know that things are changing and with those changes come new problems and new challenges.

End-users and vendors alike have expressed concern about adopting Windows 10, and some of the more common issues raised include:

- Concern that the upgrade to Windows 10 will break current apps
- Key software vendors are concerned that they won't have enough time to test and then issue their statements for support
- People feel that they need more time to plan for Windows 10
- There is too much interdependency between the editions for all the different MS products
- Deployment is too time-consuming and much too expensive
- Concern over security vulnerabilities
- People are saying that they need help to implement this brand new system

So, in terms of adoption, Microsoft has listened and this is what they feel end-users and business users want:

Agility:

- Access to new technology
- Microsoft needs to implement feedback quickly
- Transparency
- Enterprise-grade capabilities so that users can address the latest market trends
- Flexibility for mixed environments

Control:

- More stability
- Less upgrades
- A longer lifecycle for support
- More time to test and certify
- Predictability
- ISV statement of support

Windows as a Service provides a great experience for the consumer – updates are rolled out automatically through Windows Update and the sheer diversity of the user base keeps the updates on target and specific. In addition, BYOD devices are kept fully up-to-date and secure and millions of devices are updated each time.

On the other side of the coin, we have special systems. Systems like air traffic control, medical systems and banking systems. All of these are mission-critical and probably don't need all the updates, all of the time, but do get regular security updates.

In the middle, we have the business user. The business user is not a consumer and does not need as many updates as they do, certainly not all the time and not at inopportune moments.

They are also not a special system case, although they do need stability and planning etc. So, how should business users be treated, since neither of these update systems works particularly well for them?

Microsoft says that business users should be treated as the professionals that they are. They should be provided with updates **only after** the market has validated them.

In theory, this means they get access to the latest technology and value much sooner.

They should also have time to test and plan the update after its release to the broad market and these updates will be deployed via a brand new system called Windows Updates for Business.

Windows Update for Business

Windows Update for Business is a brand new feature, designed with the help of IT professionals from all over the world. The feature is designed to provide:

> **Roll out Rings**: The IT pro can specify which devices are updated and when, deploying the update in waves so as to work any kinks out of the system before they go to the critical devices.
>
> **Maintenance Windows**: IT pro specifies critical timeframes for when the updates should and should not be deployed.
>
> **Peer-to-Peer Delivery**: IT can enable this to deliver updates to branch offices and remote sites with limited bandwidth in a more efficient manner.
>
> **Integration with Existing Tools:** Such as Enterprise Mobility Suite, so that the tools are fully integrated in the system management.

Windows Update for Business is designed to reduce management costs and provide more control over the deployment of updates. It will also offer quicker access to critical security updates and provide quick access to the latest innovations from Microsoft on a regular and ongoing basis.

In the past, two software update options were available – Windows Update (WU), which is what we have now, aimed at BYOD devices, consumer devices and on test machines; and

Windows System Update Services (WSUS), which is aimed at those special systems, who need critical security updates.

Now we have Windows Update for Business (WUB). WUB allows managers to attach devices to updates, rather than the other way around.

You get to decide which devices get which updates and when, and critical security updates will be delivered to you for deployment on a regular basis.

Windows 10 and the Internet of Things

What is the Internet of Things? IoT is the future, the future of connecting things and devices, and while it remains largely unexplored and disjointed, the opportunities are huge. To give you some idea of the sheer scale of things to come:

- By the year 2020, there will be an estimated 28 billion "things" connected to the Internet – that's four for every person on earth.
- By 2017, the opportunities for wearable devices will be worth approximately $20 billion.
- By 2017, the opportunities for the Smart Home will be worth approximately $12 billion.

But, with these huge opportunities come huge challenges, such as:

- Proprietary hardware and protocols that complicate deployment
- Manageability, configuration and identity
- Security

IoT is broken down into two main areas – Consumer and Enterprise. On the consumer side, we tend to think mainly of home devices, for automation, security, entertainment and energy management.

The Enterprise side is a little less defined and largely unexplored. The IoT is complicated – there are thousands of connections out there and no real interoperability.

Each device connects to its own separate app and possibly to its own cloud and each one is separated from the others by a walled garden, a sandbox of activity.

To get any real value from the Internet of Things, all these devices need to be able to connect with each other, across brands, and across categories.

AllSeen and AllJoyn

AllJoyn is the name of an open source technology, a communications network that allows devices to talk to one another and to give those devices and apps a high degree of interoperability.

AllSeen is an alliance that was set up to oversee AllJoyn, to enable the Internet of Things to work and is also part of the LINUX Foundation open source project.

AllJoyn is designed to allow devices to:

- Discover nearby friendly devices
- Identify services that are running on other devices
- Adapt to devices that are coming and going, i.e. If two devices were once paired together and then disconnected, if they are paired again, they will remember the previous pairing and what was done when they were paired
- Manage diverse transports, also known as 'radio soup'
- Interoperate between all operating systems
- Exchange information, enabling one device to make another more powerful by knowing what services are running on that device.

Where Does Windows 10 Come In?

As a premier member of the AllSeen Alliance, Microsoft is bringing AllJoyn into Windows 10, in three separate Windows 10 for IoT editions:

Windows 10 IoT for Industry: Enterprise devices, a full version of Windows 10 running a Desktop Shell and including legacy support for Win32 and Universal Windows apps and drivers.

Windows 10 IoT for Mobile: Mobile device version with a Modern Shell, which can only run modern or universal windows apps and drivers, but not Win32.

Windows 10 IoT Core: This has no shell and no user interface. It is for devices that connect sensors together, for example, for mission critical systems. Another example is Internet TV boxes, such as Raspberry Pi, etc., with only one app running to pull everything together, gathering information and sending it all to Azure.

Microsoft is also working on the giving developers the ability to build their own apps for IoT, opening up the way ahead for full-scale interoperability.

IoT Azure Security

IoT presents a brand new set of challenges in terms of security, for both the developer and the architect.

Devices get deployed, often with no supervision, in public places. We want to be able to control things remotely, perhaps devices in our homes while we are away, perhaps a car-sharing vehicle using a smartphone.

All of this has to be done in a secure way, a way that can't be tampered with, spoofed, or degraded in any way. Microsoft has come up with a way to secure our IoT experience through Azure.

Digital security has often been sidelined; operational technology engineers focus on systems that are generally closed and isolated and IT engineers don't generally focus on personal safety.

However, it is a fundamental requirement now for IoT devices to be able to communicate with cloud-based analytic and control services, whether directly or indirectly. Together with the requirement for remote servicing and remote control of digital devices, it is past time to start looking beyond perimeter boundaries. This means that the basic network level security seen in most systems is simply not sufficient any more.

Service Assisted Communication is a proven model that allows for secure communication between devices with associated services, and also with those across local networks. SAC brokers the communication with a device by directing it through a trusted gateway, either at the field or in the cloud.

This means that the device can act as a network client to the gateway by directing it through a peer secured channel, which, in turn, limits the chances of unsolicited and malicious connection attempts.

Azure IoT hub is a supercharged version of Event hub with explicit support for field gateways and additional protocols. Customers will be able to go to Azure portal and build an IoT hub, giving them bidirectional capability. This capability gives you a way of talking directly to an IoT hub though https or amqps (advanced message queuing protocol-secured).

Inside the hub is an Identity Registry that allows millions of devices to be registered. Each registered device is federated against and via Azure Active directory to check their authenticity.

An IoT hub will be secure, with TLS always enforced – the hub will never allow a connection that is not secured, which means that any plain http traffic will be turned away at the door and redirected to a self-hosted gateway. Native support for Service Assisted Communication is built in, with the potential to hold on to millions of those bidirectional capabilities I mentioned earlier

Authentication takes place at the channel level and gateway authorization is given based on identity registry checks. Microsoft tags all messages with the device identity, stopping spoofing attempts in their tracks. Device management is included so that software updates can be managed as well as the ability to check on the state of a specific device.

As already discussed in detail, Window 10 is providing a trusted model for security across all hardware – secure boot, trusted driver validation, trusted app validation and security policy enforcement, as well as a whole boatload of secure networking capabilities.

Azure IoT services bring hyper scale connection capabilities, for collecting, storing and processing IoT data, as well as ensuring a secure communication stream between the cloud and devices, or field gateways, through the SAC system.

In the same way that a Windows 10 device can combine with any cloud platform, Azure IoT services will be able to provide support for any device and any operating system, provided a compatible communication stack is present. Additionally, through Azure, Microsoft is committed to securing data and to keeping it private; the same applies to all IoT data.

Summary

A tremendous amount of thought and planning have gone into making the Windows 10 ecosystem secure. Microsoft has taken the time to listen to customers, make adjustments and in many areas be proactive to lock down different elements of the O.S.

In areas like facial recognition (via Windows Hello), Microsoft are leading the way in helping bring industrial strength security to corporations AND the regular consumer.

As long as there are computers that are locked down, there will be hackers trying to break into them. With Windows 10 however, Microsoft have done their best to make it pretty damn hard for someone to get into your PC if you use the tools available to you.

I hope this book has been as much fun to read as it was for me to write. As usual, I would love to hear from you so feel free to email me at **securitybook@windows10update.com**

Additional Windows 10 Training

In addition, if you are looking for Windows 10 Training, we have a couple of classes on Udemy you should check out.

Introduction to Microsoft's Windows 10

https://www.udemy.com/introduction-to-windows-10/
This class is regularly $50. Here's a coupon code for $20 off - Windows10SecurityBook40

Setting up Windows 10 for Business

https://www.udemy.com/setting-up-windows-10-for-small-business/
This class is regularly $250. Here's a coupon code for $100 off - Windows10SecurityBook40

Thanks for taking this journey with me.

I appreciate your time.

Onuora Amobi.