Windows 10 Security Features

NHS Windows 10 Transformation

Prepared for

NHS

2018

Version 1.0 Final

Prepared by

Microsoft Services

Microsoft

Table of Contents

1 Overview

In this document we explore key Windows 10 security features to clarify what is available as part of the Windows 10 E5 licence and to explain how they can be used to provide increased levels of security. This is a guide for technical with a role or focus involving IT platform security.

Windows 10 delivers comprehensive, built-in and ongoing trusted security protection, including features such as Windows Defender Next Generation Protection (NGP, including Windows Defender Antivirus), Windows Firewall, and more. These help reduce the attack surface on Windows 10 devices and within applications in organisations to protect them from known threats such as viruses and malware and also from new and emerging threats.

The document also covers Windows Defender Advanced Threat Protection (ATP), a new platform available for Windows 10 Enterprise E5 customers only, which leverages built-in Windows 10 security features to bring enhanced Windows 10 device security management.

2 Context

2.1 Hardware and Software

This document covers multiple security technologies built into Windows 10. These technologies have varying hardware and software requirements and may offer different levels of protection depending on the context in which they are used.

The most significant hardware requirements include hardware-based virtualization capabilities, UEFI, Secure Boot, TPM or availability of biometric devices to enable certain security features. In some cases, these provide additional levels of protection to features that can otherwise be enabled without them.

Some examples are:

- **Windows Hello** can be enabled without a biometric device, using only a PIN and without TPM, using software-based protection. It is, however, significantly more secure when backed by TPM hardware, and more user friendly when using biometric data to unlock.
- **Windows Defender Application Control** can be enabled without Virtualization-based Security (VBS), therefore supports hardware that doesn't meet VBS requirements. However, Application Control will benefit from VBS to make the feature more resistant to exploits through kernel vulnerabilities, since code integrity enforcement will run in a hardware-based virtualized container, and not in the main OS kernel.

From the software perspective, a key requirement is the use of the 64-bit version of Windows 10 to enable some of the new security features that rely on, or benefit from, hardware-based virtualization, such as System Guard, Credential Guard, Application Guard, or Windows Defender Application Control (when enhanced with VBS). Some other security features described in this document will also work on 32-bit systems, such as Windows Firewall, AppLocker, Bitlocker or Windows Defender SmartScreen.

Another software requirement is to ensure that all system drivers have been tested and verified for compatibility with Hypervisor Code Integrity (HVCI) so that Virtualization-based Security can be enabled. This requirement may block the adoption of VBS on devices that support 64-bit Windows but do not have the drivers required for HVCI compatibility.

2.2 Product Naming and Use with 3rd Party Solutions

Traditionally, "Windows Defender" referred to the antispyware software built into Windows Vista and Windows 7. This has evolved into a full antivirus solution in Windows 8 and later, initially under the name of "Windows Defender Antivirus". It is now called "Windows Defender Next-Generation Protection".

In Windows 10, "Windows Defender" refers to a security suite rather than a specific product, with some of the previous Windows security features renamed accordingly. "Windows Firewall" and "Windows SmartScreen", for example, are now known as "Windows Defender Firewall" and "Windows Defender SmartScreen" respectively.

Newly introduced features in Windows 10 have also been renamed over time, such as "Device Guard" and "Configurable Code Integrity", now named "Windows Defender System Guard" and "Windows Defender Application Control".

In summary, none of these features require you to have Windows Defender Antivirus as your real-time antimalware and can work with third-party antivirus solutions. The same is applicable to security features outside of Windows Defender branding, such as Windows Hello, AppLocker or Bitlocker.

It's worth noting that whilst many security features within the "Windows Defender" brand don't require Windows Defender Antivirus as real-time antimalware, some of them do.

Of the four features are under the "**Windows Defender Exploit Guard**" umbrella, three require Windows Defender Antivirus as your real-time antimalware, and won't work with third-party antivirus solutions:

- Attack Surface Reduction Rules
- Network Protection
- Controlled Folder Access

The fourth feature, Exploit Protection, is compatible with the use of third-party antivirus solutions.

It is not a pre-requisite that Windows Defender Antivirus (WDAV) is used as part of the **Windows Defender ATP** deployment and in fact ATP Endpoint Detection and Response (EDR) will work comfortably with most other AV solutions.

However, there are certain benefits with by using WDAV particularly related to response actions.

When a 3rd party AV solution is installed on a Windows 10 device the WDAV service puts itself into passive mode. **It is critical that the WDAV service is not forcibly deactivated** using a GPO or some other method. For details: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/windows-defender-antivirus-compatibility

It is **strongly recommended** that if you are running a 3rd party AV solution within your estate, you also maintain current WDAV signature updates. By design, if your primary AV fails for some reason, WDAV will promote itself into active mode so that AV protection is maintained. For details: https://docs.microsoft.com/en-gb/windows/security/threat-protection/windows-defender-antivirus/manage-updates-baselines-windows-defender-antivirus

ATP functionality available with WDAV Active / Passive configurations:

WDAV Configuration	WDATP Response Features Affected
Defender AV Active	All features operating: • Isolate • Kill / Quarantine (process running) • Block (prevents process running in the first place) • Auto Investigation and Remediation, available in 1803 and above
Third Party AV Active (Defender AV Passive)	Block file response action not available All other features operating

3 Windows 10 Security Features

3.1 Malware Protection

All editions of Windows 10 include two key components that help protect against software threats: Windows Defender Next Generation Protection (NGP) and Windows Defender SmartScreen.

These features are available in both Windows 10 32- and 64-bit, and don't require any specific hardware requirements.

3.1.1 Windows Defender Next Generation Protection

Windows Defender NGP keeps your PC safe with trusted protection built-in to Windows 10. Windows Defender NGP delivers comprehensive, ongoing and real-time protection against software threats such as viruses, malware and spyware across email, apps, the cloud and the web.

Windows Defender NGP provides the following features:

- **Real-time protection**, through always-on scanning, advanced file and process behaviour monitoring and heuristics
- **Cloud-delivered protection** (also known as Microsoft Advanced Protection Service, or MAPS) provides near-instant detection and blocking of new and emerging threats, leveraging machine learning and the Intelligent Security Graph (Connecting an ecosystem of security solutions through the Intelligent Security Graph, helps streamline security operations and improve defences)
- **Limited Periodic Scanning**, a special type of threat detection and remediation that can be enabled when you have installed third-party antivirus product on a Windows 10 device, to periodically check for threats. This feature is primarily intended for consumers, and Microsoft does not recommend using this feature in enterprise environments
- **Offline scans**, run outside of Windows to remove rootkits and other threats that hide from the Windows operating system. This tool uses a small, separate operating environment, where evasive threats are unable to hide from antimalware scanners

Windows Defender NGP is automatically enabled and installed on devices that are running Windows 10, noted as **active mode**. However, when using third-party antivirus solutions, Windows Defender NGP will enter either **passive mode** or **automatic disabled mode** depending if the device is enrolled in the Windows Defender ATP service or not:

- **In active mode**, Windows Defender NGP scans files and remediates threats in real-time
- **In automatic disabled mode and passive mode**, Windows Defender NGP will not be used as a real-time protection solution and it will not remediate threats. If the protection offered by a third-party antivirus product expires or stops providing real-time protection, Windows Defender NGP will automatically enable itself to ensure protection is maintained on the device. You can still manage updates for Windows Defender NGP but can't move Windows Defender NGP into the normal active mode if the device has an up-to-date third-party product providing real-time protection
- **In automatically disabled mode**, the limited periodic scanning feature is available. This feature is intended for consumers, and not recommended in enterprise environments.

In passive mode, in cases where Windows Defender NGP will not be used as the real-time protection solution, and therefore will not be remediating threats, files will still be scanned and reports provided for threat detection purposes and these will be shared with the Windows Defender ATP service

The following matrix summarises the states that Windows Defender NGP will enter on Windows 10 devices when Windows Defender and third-party antivirus products are enrolled in Windows Defender ATP Endpoint Detection and Response (EDR):

Protection Solution	Device Enrolled in Windows Defender ATP EDR	Windows Defender NGP State
Windows Defender NGP	Yes	Active mode
Windows Defender NGP	No	Active mode
Third-party Antivirus	Yes	Passive mode
Third-party Antivirus	No	Automatic disabled mode

3.1.2 Windows Defender SmartScreen

Windows Defender SmartScreen helps to provide an early warning system against websites that might engage in phishing attacks or attempt to distribute malware through a socially-engineered attack. Windows Defender SmartScreen helps to protect staff if they try to visit sites previously reported as phishing or malware websites, or if a staff member tries to download or execute potentially malicious programs downloaded from the Internet. For example, if a radiologist opens an email which unbeknown to them is a phishing email, and clicks on a link and that in turn triggers certain malicious events etc. The primary benefits of Windows Defender SmartScreen are:

- **Operating system integration.** SmartScreen is integrated into the Windows 10 operating system and checks any files an application (including 3rd party browsers and email clients) attempts to download and run
- **Anti-phishing and anti-malware support.** SmartScreen helps to protect your staff from sites that are reported to host phishing attacks or attempt to distribute malicious software. It can also help protect against deceptive advertisements, scam sites, and drive-by attacks. Drive-by attacks are web-based attacks that tend to start on a trusted site, targeting security vulnerabilities in commonly-used software. Because drive-by attacks can happen even if the user does not click or download anything on the page, the danger often goes unnoticed
- **Reputation-based URL and app protection.** SmartScreen evaluates a website's URLs to determine if they're known to distribute or host unsafe content. It also provides reputation checks for apps, checking downloaded programs and the digital signature used to sign a file. If a URL, a file, an app, or a certificate has an established reputation, your staff won't see any warnings. However, if there's no reputation, the item is marked as a higher risk and presents a warning

- **Improved heuristics and diagnostic data.** SmartScreen is constantly learning and adapting in order to stay up-to-date, so it can help protect against potentially malicious sites and files
- **App Install Control.** App Install Control is a feature of Windows Defender SmartScreen that helps protect PCs by allowing users to install apps only from the Windows Store

3.2 Hardware-based Isolation

Hardware based isolation capabilities in Windows 10 help protect devices and applications from new and emerging threats beyond the protection offered by anti-malware features like Windows Defender NGP or Windows Defender SmartScreen.

These Windows 10 technologies help reduce the chance and potential damage of an attack with protection at different layers with different system requirements. Several of these technologies can benefit from the hardware-based isolation features in Windows 10. Furthermore, over the course of different Windows 10 releases, some of the technologies have received different names, so this section will clarify details surrounding these.

3.2.1 Virtualization-based Security

Windows 10 introduced the concept of Virtualization-based Security (VBS), enabling hardware isolation of the most sensitive Windows 10 services and data.

VBS uses hardware virtualisation features to create and isolate a secure region of memory from the normal operating system. Windows can use this "virtual secure mode" to host security solutions, providing them with greatly increased protection from vulnerabilities in the operating system, and preventing the use of malicious exploits which attempt to defeat protections.

VBS uses the Hyper-V hypervisor to create this virtual secure mode, and to enforce restrictions which protect vital system and operating system resources, or to protect security assets such as authenticated user credentials. With the increased protections offered by VBS, even if malware gains access to the OS kernel the possible exploits can be greatly limited and contained, because the hypervisor can prevent the malware from executing code or accessing platform secrets.

Some Windows 10 security features rely on Virtualization-based Security support:

- **Windows Defender System Guard** uses VBS to significantly strengthen kernel mode code integrity, checking all kernel mode drivers and binaries before they're started and preventing unsigned drivers or system files from being loaded into system memory. Additionally, kernel memory pages are only made executable after code integrity checks inside the secure region have passed, and executable pages are not writable. That way, even if there are vulnerabilities like a buffer overflow that allow malware to attempt to modify kernel memory, code pages cannot be modified, and modified memory cannot be made executable
- **Windows Defender Application Control,** while this does not require VBS to run, it can be further protected by leveraging System Guard, so the code integrity service runs inside a secure environment, providing stronger protection against kernel exploits that could attack Windows Defender Application Control (WDAC)
- **Windows Defender Application Guard** uses VBS to isolate Microsoft Edge browser sessions from the host operating system, so malicious web content cannot access corporate data or damage the host

- **Windows Defender Credential Guard** uses VBS to isolate and protect secrets so that only privileged system software can access them (e.g., NTLM password hashes and Kerberos ticket-granting tickets) to block pass-the-hash (PtH) or pass-the-ticket (PtT) attacks
- **Other technologies** such as Virtual TPM and Windows Hello biometric stack also rely on VBS technology to secure and maintain the integrity of critical system services and data at run time

Virtualization-based Security requires the following hardware components to be present and properly configured:

Hardware requirement	Details
64-bit CPU	Virtualization-based Security (VBS) requires the Windows hypervisor, which is only supported on 64-bit Windows running on 64-bit IA processors with virtualisation extensions, including Intel VT-X and AMD-V
Second Level Address Translation (SLAT)	VBS also requires that the processor's virtualisation support includes Second Level Address Translation (SLAT), either Intel VT-X2 with Extended Page Tables (EPT), or AMD-v with Rapid Virtualization Indexing (RVI)
IOMMUs or SMMUs (Intel VT-D, AMD-Vi, ARM64 SMMUs)	All I/O devices capable of Direct Memory Access (DMA) must be behind an Input-Output Memory Management Unit (IOMMU) or System Memory Management Unit (SMMU). An IOMMU can be used to enhance system resiliency against memory attacks
Trusted Platform Module (TPM) 2.0	TPMs, either discrete or firmware, will suffice. Not strictly required to enable VBS as shown in Device Guard (DG) Readiness Tool, but enhances its security, so it is highly recommended, as it is for other features like BitLocker or Windows Hello
Firmware support for SMM protection	System firmware must adhere to the recommendations for hardening System Management Mode (SMM) code described in the Windows SMM Security Mitigations Table (WMST) specification. The WSMT specification contains details of an Advanced Configuration and Power Interface(ACPI) table that was created for use with Windows operating systems that support Windows VBS features. Firmware must implement the protections described in the WSMT specification and set the corresponding protection flags as described in the specification to report compliance with these requirements to the operating system
Unified Extensible Firmware Interface (UEFI) with Secure Boot	Virtualization-based Security requires Secure Boot and can be optionally enabled with the use of Direct Memory Address (DMA) protection. DMA protection requires hardware support and will only be enabled on correctly configured devices

Hardware requirement	Details
Unified Extensible Firmware Interface (UEFI) Memory Reporting	UEFI firmware must adhere to the following memory map reporting format and memory allocation guidelines for firmware to ensure compatibility with VBS: - UEFI v2.6 Memory Attributes Table (MAT). Firmware must cleanly separate Extensible Firmware Interface (EFI) runtime memory ranges for code and data, and report this to the operating system - EFI Page Protections. All UEFI memory that is marked executable must be read only. Memory marked writable must not be executable. Entries may not be left with either of the attributes set, indicating memory that is both executable and writable
Secure Memory Overwrite Request (MOR) revision 2	Secure MOR v2 is enhanced to protect the MOR lock setting using a UEFI secure variable. This helps guard against advanced memory attacks. For details, see Secure MOR implementation. This is not strictly required to enable VBS, as shown in DG Readiness Tool, but enhances its security, so is highly recommended
Hypervisor Code Integrity (HVCI)-compatible drivers	Ensure all system drivers have been tested and verified to be compatible with HVCI. The Windows Driver Kit and Driver Verifier contain tests for driver HVCI compatibility. Use the Device Guard and Credential Guard hardware readiness tool

Virtualization-based Security has the following operating system requirements:

- **Hyper-V Hypervisor enabled**. Virtualization-based Security uses the Windows Hypervisor to provide support for security services
- **Windows 10 64-bit**. The 64-bit operating system version is a requirement to enable Hyper-V

3.2.2 Device Guard

When Windows 10 was launched, Microsoft introduced the term "Device Guard"; a set of hardware and operating system technologies that, when configured together, allow enterprises to lock down Windows 10 systems so they operate with many of the properties of mobile devices.

Device Guard primarily consisted of two independent security technologies:

- **Virtualization-based protection of code integrity (HVCI),** which hardens the OS against kernel memory attacks. This feature relies on the Windows Virtualization-based Security feature which requires compatible hardware, firmware, and kernel driver components
- **Configurable code integrity (CI),** which restricts devices to only run authorised apps through a single system-wide policy. This feature has no specific hardware or software requirements other than Windows 10, although can benefit from having HVCI also enabled

When Device Guard was initially released, many customers believed that the two features (CI and HVCI) were inexorably linked and could not be deployed separately. In fact, there are no direct dependencies between these two features.

With the release of Windows 10 1709 Microsoft gave the Configurable CI feature and related enhancements its own name, becoming **Windows Defender Application Control**.

Similarly, since the initial release of Windows 10 1507, enterprise customers have had the option to enable Virtualization-based Security (VBS) and Hypervisor protected Code Integrity (HVCI) to increase platform threat resistance. In Windows 10 1709 Microsoft consolidated these system integrity features in **Windows Defender System Guard** and have named the VBS secure environment the **Windows Defender System Guard container.**

The term "Device Guard" will remain as a broad term to describe the fully locked down state achieved through the use of Windows Defender Application Control (WDAC), HVCI, and hardware and firmware security features. Microsoft is working with OEM partners to identify specifications for devices that are "Device Guard capable". This approach enables customers to easily purchase devices that meet all the hardware and firmware requirements of the original "Device Guard" locked down scenario for Windows 10 based devices.

3.2.3 Windows Defender System Guard

Windows 10 uses containers to isolate sensitive system services and data, enabling them to remain secure even when the operating system has been compromised.

Windows 10 protects critical resources, such as the Windows authentication stack, single sign-on tokens, Windows Hello biometric stack, and Virtual Trusted Platform Module, by using a container type called Windows Defender System Guard (WDSG). This leverages the Virtualization-Based security capability in Windows 10 coupled with the associated VBS hardware requirements.

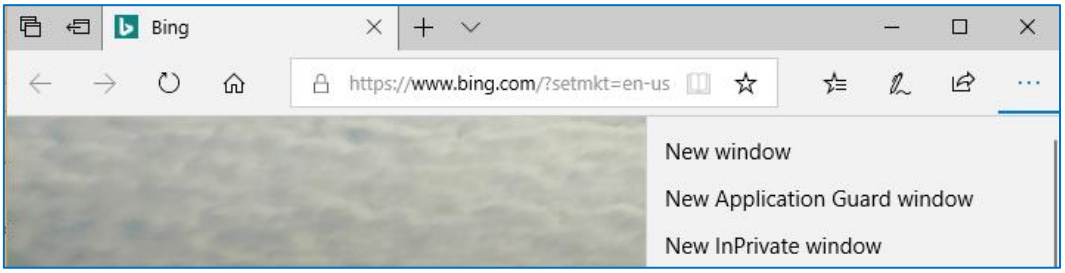
WDSG includes a series of technologies that enable remote analysis of device integrity. As Windows 10 boots, a series of integrity measurements are taken by WDSG using the device's Trusted Platform Module 2.0 (TPM 2.0). This process and data are isolated, at the hardware level, away from Windows to help ensure that the measurement data is not subject to tampering , for example if the platform were compromised. From here, the measurements can be used to determine the integrity of the device's firmware, hardware configuration state, and Windows boot-related components. After the system boots, WDSG signs and seals these measurements using the TPM. Upon request, a management system such as Intune or System Center Configuration Manager (SCCM) can acquire the data for remote analysis. If WDSG indicates that the device lacks integrity, the management system can take a series of actions, such as denying the device access to resources.

3.2.4 Windows Defender Application Guard

Windows Defender Application Guard (WDAG) is designed for Windows 10 and Microsoft Edge and enables untrusted sites, as defined by the enterprise, to be isolated. This helps protect organisations while staff browse the Internet and leverages Windows Hypervisor and Virtualization-based Security to create a virtualised environment for Microsoft Edge. For example, a GP browses the internet in search of vaccination information – a pop up window appears encouraging her to redirect to an untrusted site which triggers a malicious event.

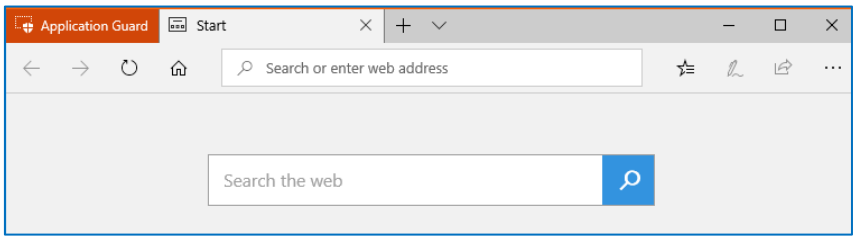
Administrators define the organisational set of trusted websites, cloud resources, and internal networks. Anything not on this "whitelist" is considered to be "untrusted".

Application Guard can work in either **standalone mode**, where the user chooses when to use it, through Microsoft Edge interface:



Or for, enterprise environments, it can work in **enterprise-managed mode**, where administrators can use the Windows Network Isolation feature to define corporate boundaries. This customises the Application Guard experience to meet and enforce organisational needs on devices by defining what websites, cloud resources, and internal networks are trusted.

If an employee attempts to browse an untrusted site through either Microsoft Edge or Internet Explorer, Microsoft Edge opens the site in an isolated Hyper-V-enabled container, which is separate from the host operating system. This container isolation means that if the untrusted site turns out to be malicious, the host PC is protected, and the attacker can't gain access data. While in isolation, improper user interactions and app vulnerabilities can't compromise the kernel or any other apps running outside of the virtualised environment.



Administrators can also control the level of interaction between the Application Guard container and the host device, such as data persistence (cookies, favourites, etc. across WDAG sessions), clipboard usage (text, images or both, either unidirectional or bidirectional), printing capabilities (PDF, XPS, local and network printers), usage of hardware-accelerated graphics or the ability to save files to the host.

WDAG has the following hardware requirements:

- Virtualization-based Security (requires 64-bit CPU, SLAT, VT-x or AMD-V, etc.)
- 4 cores, 8 GB of RAM and 5GB of free disk space or more for optimal performance
- Although not strictly required, it is strongly recommended to use hardware with IOMMU support (VT-d or AMD-Vi)

By default, for performance reasons, WDAG won't work without these hardware requirements.

3.3 Application Control

By using an application whitelisting approach, Windows 10 application control technologies aim to protect the device through policies that prevent end users or attackers from executing arbitrary programs which put the device, user credentials, data or other corporate assets at risk.

3.3.1 AppLocker

AppLocker is a whitelisting app control that be used to determine which applications users are able to run. For example, the organisation's approved theatre booking application would need to be whitelisted so that it can run.

When a user runs a process, that process has the same level of access to data that the user has. As a result, sensitive information could easily be deleted or transmitted out of the organisation if a user knowingly or unknowingly runs malicious software.

AppLocker can help mitigate these types of security breaches by restricting the files that users or groups can run. These include executable files, scripts, Windows Installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers.

AppLocker advances the application control features and functionality of Software Restriction Policies with new capabilities and extensions that allow administrators to create rules to allow or deny apps from running based on unique identities of files and to specify which users or groups can run those apps, allowing administrators to:

- Define rules based on file attributes that persist across application updates, such as the publisher name (derived from the digital signature), product name, file name, and file version. Rules can also be created based on the file path and hash
- Assign a rule to a security group or an individual user
- Create exceptions to rules. For example, you can create a rule that allows all users to run all Windows binaries, except the Registry Editor (regedit.exe)
- Use audit-only mode to deploy the policy and understand its impact before enforcing it
- Create rules on a staging server, test them, then export them to a production environment and import them into a Group Policy Object
- Simplify creating and managing AppLocker rules by using Windows PowerShell

AppLocker does not have any specific hardware requirements, although the operating system version must be Windows 10 Enterprise.

3.3.2 Windows Defender Application Control

One of the AppLocker limitations is that protection is handled through a Windows service called "Application Identity" and configured through group policies that make persistent registry entries in the computer's policy. A user or attacker that gains administrative privileges could easily circumvent AppLocker by changing registry entries or stopping the service. Another limitation is that AppLocker applies only to programs that are run in user-mode but cannot prevent malicious code that is run in kernel-mode.

Windows Defender Application Control is the new name for an existing feature introduced in Windows 10 1709 and previously called **Configurable Code Integrity (CI)**, part of the Windows Device Guard state, which enables the deployment of a system-wide policy to a machine, controlling what is allowed to run.

Configurable Code Integrity (CI) policies enable Windows 10 device restrictions, allowing only authorised apps to run, taking policy-based application control solutions, such as AppLocker, to the next level:

- **CI policy applies beyond code running in user mode, to non-interactive processes, kernel mode hardware and software drivers, and even code that runs as part of Windows.** It takes effect early in the boot sequence before nearly all other operating system code and before traditional antivirus solutions can run. It also protects Windows Scripting hosts, MSIs and makes unsigned PowerShell code run in "Constrained Language Mode"
- **CI policy can be protected from tampering by digital signature.** In AppLocker, a user with administrative credentials could make changes to an AppLocker policy on a local device and override it. In Application Control, using digitally signed policies means that changing the policy requires not just administrative privilege on the system, but also access to the organisation's digital signing process. This makes it extremely difficult for an attacker or malware that manages to gain administrative privilege to alter the application control policy
- **CI enforcement mechanism can be protected by HVCI (VBS).** While Windows Defender Application Control can run on any Windows 10 device, it benefits from increased security gained through the use of Virtualization-based Security, which enables the code integrity feature to run in a hardware-based virtualized container. This creates the condition where even if a vulnerability exists in kernel mode code, the likelihood that an attacker could successfully exploit it is significantly diminished. An attacker who compromises the kernel is prevented from having enough privileges to override the application control policies enforced by configurable CI

Note that Windows Defender Application Control does not replace AppLocker, which is still useful for applying user-based or group-based application control policies, and to manage security around batch scripts (.bat, .cmd) etc.

3.4 Protecting Against Exploits

Exploit protection technologies aim to protect the device from new and emerging threats that anti-malware solutions cannot detect, by implementing controls over common attack vectors on software systems.

3.4.1 Exploit Mitigation Experience Toolkit (EMET)

The Enhanced Mitigation Experience Toolkit (EMET) was designed to assist customers with their defence-in-depth strategies against cyberattacks, helping to detect and block exploitation techniques commonly used for exploiting memory corruption vulnerabilities and to complement other defence-in-depth security measures, such as Windows Defender NGP software.

EMET helped protect against new and undiscovered threats, even before they were formally addressed through security updates or antimalware software, by the application of 14 security mitigation rules.

EMET 5.5.x was supported up to Windows 10 1607 and reached end of life on 31 July 2018. However, many of the features in EMET have been included in the Windows Defender Exploit Guard exploit protection feature, and existing EMET configuration profiles can be converted and imported into Exploit Guard.

3.4.2 Windows Defender Exploit Guard

Windows Defender Exploit Guard (Windows Defender EG or WDEG) is a new set of host intrusion prevention capabilities for Windows 10, allowing organisations to manage and reduce the attack surface of applications used by staff.

Windows Defender Exploit Guard consists of four distinct features:

- Exploit Protection
- Attack Surface Reduction (ASR)
- Network Protection
- Controlled Folder Access

From these four Windows Defender Exploit Guard features, **only Exploit Protection is compatible with third party antivirus solutions**, while the rest require Windows Defender NGP real-time protection to be enabled.

Exploit Protection. applies memory exploit mitigation techniques to the applications organisations use, allowing configuration of rules both individually or to all applications. Exploit Guard has an audit mode, allowing evaluation of how the exploit protection will impact an organisation if it is enabled. The following link provides a feature comparison table between EMET and Exploit Guard: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/exploit-protection-exploit-guard

Attack Surface Reduction Rules. Reduce the attack surface of applications with intelligent rules that stop attack vectors used by Office, Windows Scripting Host, Adobe Reader and mail-based malware. Examples include executable files and scripts used in Office apps or web mail that attempt to download or run files, scripts that are obfuscated or otherwise suspicious, and application behaviours that are not usually associated with normal day-to-day work. The set of rules that can be enabled are described in more detail here: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/attack-surface-reduction-exploit-guard

Additionally, Attack Surface Reduction Rules require Windows 10 Enterprise E5 subscription. For the rest of the features, E5 is still recommended, as it provides automated reporting into the Windows Defender ATP console, and provides additional cloud-powered capabilities, including the Network Protection ability to block apps from accessing low-reputation websites and an Attack Surface Reduction rule that blocks executable files that meet age or prevalence criteria.

Network Protection Network protection helps prevent employees from using any application to access dangerous domains that may host phishing scams, exploits, and other malicious content on the Internet.

Controlled Folder Access is a feature that helps protect your documents and files from modification by suspicious or malicious apps. Controlled folder access is supported on Windows Server 2019 as well as Windows 10 clients. More information can be found here: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/controlled-folders-exploit-guard

3.5 Protecting Against Network Threats

3.5.1 Windows Defender Firewall

Windows Defender Firewall with Advanced Security provides host-based, two-way network traffic filtering for a device, blocking unauthorised network traffic flowing into or out of the local device.

Windows Defender Firewall also works with Network Awareness so that it can apply security settings that are appropriate for the types of networks to which the device is connected.

Windows Defender Firewall offers the following benefits:

- **Reduces the risk of network security threats.** Windows Defender Firewall reduces the attack surface of a device, providing an additional layer to the defence-in-depth model
- **Integration with IPSec.** Windows Defender Firewall provides a simple way to enforce authenticated, end-to-end network communications. It provides scalable, tiered access to trusted network resources, helping to enforce integrity of the data, and optionally helping to protect the confidentiality of the data
- **Extends the value of existing security investments.** Windows Defender Firewall is designed to complement existing non-Microsoft network security solutions through a documented application programming interface (API)
- **Integrated with Windows Store apps.** Windows Firewall enables connectivity of Universal Windows Platform apps to be allowed or blocked

Windows Firewall does not have any specific hardware and software requirements other than Windows 10.

> **Important**
>
> It is important to note that some third-party antivirus solutions include a host-based firewall. Windows Defender Firewall must be explicitly deactivated when using a third-party firewall solution to avoid the possibility of communication issues arising from running two firewall solutions simultaneously.

3.5.2 Windows Defender Exploit Guard Network Protection

Windows Defender Exploit Guard **Network Protection** extends the malware and social engineering protection offered by Windows Defender SmartScreen in Microsoft Edge to cover network traffic and connectivity on an organisation's devices. Network Protection prevents users from using any application to access dangerous domains that may host phishing scams, exploits, and other malicious content on the Internet, by blocking all outbound HTTP(s) traffic that attempts to connect to low-reputation sources. It also prevents users from bypassing SmartScreen when using third-party browsers

3.6 Protecting Against Ransomware

There are many forms of ransomware attacks, but one of the most common forms is where a malicious individual encrypts a user's important files and then demands something from the user, such as money or information, in exchange for the key to decrypt them. Ransomware attacks are on the rise, particularly those that encrypt files that are stored in the user's cloud storage. For more information about ransomware, see the Windows Defender Security Intelligence site.

3.6.1 Controlled Folder Access

Windows Defender Exploit Guard **Controlled Folder Access** helps protect files in Windows system folders and customisable folders from changes made by any application that is not explicitly marked as allowed through Controlled Folder Access. This prevents any random application, including file-encrypting ransomware malware, from modifying system or user folders.

3.6.2 OneDrive for Business

You can use versioning to protect OneDrive for Business libraries from some, but not all, of these types of ransomware attacks. Versioning is enabled by default in OneDrive for Business. When versioning is enabled you can look at earlier versions and recover them, if necessary. That enables you to recover versions of items that pre-date their encryption by the ransomware.

For detailed steps to do this, see Restore a previous version of a document in OneDrive for Business.

Versioning does not protect against ransomware attacks that copy files, encrypt them, and then delete the original files. However, end-users can leverage the Recycle Bin to recover OneDrive for Business files after a ransomware attack occurs.

Alert policies in the Office 365 Security and Compliance Center can be configured to generate alerts and email notifications when certain activities are detected in OneDrive for Business:

- Malware campaign detected in OneDrive. Generates an alert when an unusually high volume of malware or viruses are detected in files located in OneDrive accounts in your organisation.
- Unusual external user file activity. Generates an alert when an usually large number of activities are performed on files in OneDrive by users outside of your organisation. This includes activities such as accessing files, downloading files, and deleting files.

- Unusual volume of external file sharing. Generates an alert when an usually large number of files in OneDrive are shared with users outside of your organisation.
- Unusual volume of file deletion. Generates an alert when an unusually large number of files are deleted in OneDrive within a short time frame.

3.7 Protecting Against Credential Theft

Credential protection technologies in Windows 10 are aimed at protecting user credentials by using hardware based, biometric technologies.

3.7.1 Windows Credential Guard

Windows Defender Credential Guard uses Virtualization-based Security to isolate and protect secrets so that only privileged system software can access them (e.g., NTLM password hashes and Kerberos ticket-granting tickets). This is design to block pass-the-hash or pass-the-ticket (PtH) attacks.

When Windows Defender Credential Guard is enabled, NTLMv1, MS-CHAPv2, Digest, and CredSSP cannot use the signed-in credentials. Consequently, single sign-on does not work using these protocols. However, applications can prompt for credentials or use credentials stored in the Windows Vault which are not protected by Windows Defender Credential Guard.

When Windows Defender Credential Guard is enabled, Kerberos does not allow unconstrained Kerberos delegation or DES encryption. This applies for both "signed-in" credentials and also for prompted or saved credentials.

By enabling Windows Defender Credential Guard, the following features and solutions are provided:

- **Hardware security.** NTLM, Kerberos, and Credential Manager take advantage of platform security features, including Secure Boot and virtualisation, to protect credentials
- **Virtualization-based Security.** Windows NTLM and Kerberos derived credentials and other secrets run in a protected environment isolated from the running operating system
- **Better protection against advanced persistent threats.** When Credential Manager domain credentials, NTLM, and Kerberos derived credentials are protected using Virtualization-based Security, the credential theft attack techniques and tools used in many targeted attacks are blocked. Malware running in the operating system with administrative privileges cannot extract secrets that are protected by Virtualization-based Security

Windows Credential Guard has specific hardware requirements:

Requirement	Details
Virtualization-based Security (VBS)	Credential Guard requires VBS. You can learn more about VBS by reading Virtualization-based Security (VBS)
Secure Boot	Hardware-based Secure Boot must be supported. To learn more, see Secure Boot
Secure Boot configuration and management	You must be able to add ISV, OEM, or Enterprise certificates to the Secure Boot database at manufacturing time Microsoft UEFI Certification Authority (CA) must be removed from the Secure Boot database. Support for third-party UEFI modules is permitted but should leverage ISV-provided certificates or OEM certificates for the specific UEFI software
Secure firmware update process	Like UEFI software, UEFI firmware can have security vulnerabilities. It is essential to have the capability to immediately patch such vulnerabilities when found, through firmware updates. UEFI firmware must support secure firmware update following Hardware Compatibility Specification for Systems for Windows 10 under System.Fundamentals.Firmware.UEFISecureBoot.
United Extensible Firmware Interface (UEFI)	To learn more, see United Extensible Firmware Interface (UEFI) firmware requirements.

To simplify the adoption of Windows Credential Guard, customers can download the Device Guard and Credential Guard hardware readiness tool in order to determine if a device is able to run Window Defender Credential Guard.

3.7.2 Windows Hello for Business

Windows Hello for Business (WHfB) replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to the device and uses a biometric (facial recognition or fingerprints) or PIN gesture to unlock it from its protected storage. If available, the TPM will be used to protect both the Windows Hello for Business keys, as well as the biometric template and/or PIN. For example, when a GP is busy speaking to a patient organisational policy may cause her computer to present the lock screen. Rather than having to use the keyboard to unlock her computer she can use Windows Hello for Business to perform the unlock operation using facial recognition.

Windows Hello for Business addresses the following problems with passwords:

- Strong passwords can be difficult to remember, and as a result, users often re-use passwords on multiple sites
- IT Support resources spending unproductive time on password resets
- Server breaches can expose symmetric network credentials (passwords)
- Passwords are subject to brute force, shoulder-surfing and replay attacks
- Users can inadvertently expose their passwords due to phishing attacks

It is important to appreciate that Windows Hello , included in all Windows 10 editions, can behave in two different ways under the covers. When using a local account or an identity provider without Windows Hello support, Windows Hello is used only locally on the device as a "convenience sign-in", allowing the user to use a biometric or PIN gesture to unlock the device and authenticate to network resources. This actually uses regular user name and password authentication credentials protected with biometric or PIN gesture. With proper Windows Hello support in the identity provider (sign in using Microsoft account, Azure Active Directory, Windows Hello-ready Active Directory, or third party identity providers with FIDO v2.0 support), authentication is actually backed by asymmetric (public/private key) or certificate-based authentication. Beginning in version Windows 10 1607, Windows Hello as a convenience PIN is disabled by default on all domain-joined computers.

Windows Hello for Business can use either keys (hardware or software) or hardware or software certificates. Enterprises that have a public key infrastructure (PKI) for issuing and managing certificates can continue to use PKI in combination with Windows Hello. Enterprises that do not use PKI or want to reduce the effort associated with managing certificates can rely on key-based credentials for Windows Hello but still use certificates on their domain controllers as a root of trust.

Windows Hello for Business has two deployment models, Hybrid and On-premises:

- Hybrid deployments are for enterprises that use Azure Active Directory
- On-premises deployments are for enterprises who exclusively use on-premises Active Directory

Environments that use Azure Active Directory must use the hybrid deployment model for all domains in that forest.

Each deployment model has two trust models: Key trust or certificate trust. The trust model determines how you want users to authenticate to the on-premises Active Directory:

- The **key-trust model** is for enterprises who *do not* want to issue end-entity certificates to their users and have an adequate number of Windows Server 2016 domain controllers in each site to support key-based authentication
- The **certificate-trust model** is for enterprises that *do* want to issue end-entity certificates to their users and have the benefits of certificate expiration and renewal, similar to how smart cards work. The certificate trust model also supports enterprises which are not ready to deploy Windows Server 2016 Domain Controllers.

With some variations depending on deployment options, Windows Hello for Business has three main steps:

- Device registration is a prerequisite to Windows Hello for Business keys provisioning, across cloud, hybrid, or on-premises deployments. For cloud and hybrid deployments, devices

register with Azure Active Directory. For on-premises deployments, devices register with the enterprise device registration service hosted by Active Directory Federation Services (ADFS)

- After device registration, Windows Hello for Business provisioning enables a user to enrol a new, strong, two-factor credential used for password-less authentication. The provisioning experience varies depending on device registration and deployment types
- Once Windows Hello for business credentials (key or certificate-based) have been provisioned, Windows Hello-based authentication can occur. Keys are unlocked through biometrics or PIN gesture and the key material is used to obtain an authentication token from the identity provider

On the client side, Windows Hello for Business does not strictly require any special hardware for a minimum setup. However,

- The Windows Hello provisioning process creates a cryptographic key pair bound to the Trusted Platform Module (TPM), if a device has a TPM 1.2 or later, or protected in software (and configuration allows Windows Hello for Business without TPM). TPM is recommended, as it protects keys from replay attacks and other software-based attacks
- Biometric gestures require specialised hardware, such as fingerprint readers or Infrared cameras. Organisations should check with their hardware provider regarding the availability of biometrics that support Windows Hello

Windows Hello for Business implementation has different infrastructure requirements depending on the deployment options. These can be checked by visiting: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification. Regardless of the deployment option of choice, there are some common infrastructure requirements:

- Active Directory Windows Server 2016 schema
- Windows Server 2008 R2 Domain/Forest functional level
- Windows Server 2012 or later Certificate Authority
- Multi-factor authentication

3.8 Data Protection

Data protection technologies in Windows 10 are aimed at protecting user data in the event a device is lost or stolen.

3.8.1 BitLocker Drive Encryption

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threat of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

BitLocker provides full volume encryption for operating system volumes, as well as fixed and removable data volumes (“BitLocker To Go”). To support fully encrypted operating system volumes, BitLocker uses an unencrypted system volume for the files required to boot, decrypt, and load the operating system. This volume is automatically created during a new installation of both client and server operating systems.

For the operating system drive, BitLocker can use the system integrity check provided by Trusted Platform Module (TPM) 1.2 or later. On computers that do not have a TPM available, you can still use BitLocker to encrypt the Windows operating system drive, requiring either a USB based start-up key or an operating system volume password to protect the operating system volume. However, both options do not provide the pre-startup system integrity verification offered by BitLocker with a TPM to ensure that the computer has not been tampered with while the system was offline.

For fixed and removable drives, Bitlocker relies on a volume password that enables Windows to mount the volume. This password can be automatically provided without user interaction ("auto-unlock") when the operating system drive is also protected by BitLocker.

In addition to the TPM, BitLocker offers the option to lock the normal startup process until the user supplies a personal identification number (PIN) or inserts a removable device, such as a USB flash drive containing a start-up key. These additional security measures provide multifactor authentication and assurance that the computer will not start or resume from hibernation until the correct PIN or startup key is present.

In a domain environment, Bitlocker allows "Network Unlock", allowing a computer to bypass the PIN entry prompt when connected to a wired corporate network, by leveraging a certificate. Without Network Unlock, operating system volumes protected by TPM in conjunction with PIN require a PIN to be entered when a computer reboots or resumes from hibernation. This can make it difficult for enterprises to roll-out software patches to unattended desktops, for example, by Wake on LAN.

In Windows 10, BitLocker supports the new FIPS-compliant XTS-AES encryption algorithm with both 128-bit and 256-bit keys. XTS-AES provides additional protection from types of attack on encryption that rely on manipulating cipher text to cause predictable changes in plain text. XTS-AES is only supported on Windows 10 1511 and later versions, so removable drives should continue to use AES-CBC 128-bit or AES-CBC 256-bit algorithms when compatibility with Windows 7 and Windows 8.1 is required.

For recovery scenarios, BitLocker uses a 48-digit recovery password created when BitLocker is turned on for the first time, for each encrypted drive. The 48-digit recovery key can be printed or saved to a USB drive. The recovery key can be used to regain access to a computer when the drive Windows is installed on is encrypted using BitLocker Drive Encryption and BitLocker detects a condition that prevents it from unlocking the drive at start-up. A recovery key can also be used to gain access to files and folders on a removable data drive (such as an external hard drive or USB flash drive) encrypted using BitLocker To Go, if for some reason you have forgotten the password or the computer cannot access the drive.

When planning for BitLocker deployment it is recommended that organisations create a recovery model. Microsoft recommends organisations use Microsoft BitLocker Administration and Monitoring (MBAM) for managing BitLocker and storing BitLocker recovery information. Alternatively, it's possible to use Active Directory Domain Services (ADDS) to store BitLocker recovery information, however, this is not recommended by Microsoft.

BitLocker has the following requirements:

- For BitLocker to use the system integrity check provided by TPM, the computer must have TPM 1.2 or later
- Enabling BitLocker without TPM requires saving a startup key on a removable device
- The firmware must be able to read from a USB flash drive during start-up

- The boot order must be set to start first from the hard disk, and not the USB or CD drives
- The hard disk must be partitioned with at least two partitions:
    - One partition for the operating system drive, formatted with NTFS file system
    - One partition for the system drive, containing boot manager files to load Windows, must be unencrypted, and formatted with FAT32 on UEFI-based computers or NTFS on BIOS-based computers, and have a size of approximately 350 MB, and set as the active partition
- For Network Unlock, the client hardware is required to have a DHCP driver implemented in its UEFI firmware, a server running Windows Deployment Services (WDS), a DHCP server separate from WDS server, and optionally a Certification Authority (CA)

3.8.2 Automatic Device Encryption

Automatic device encryption is a new way to protect data on Windows 10 devices, it is enabled by default on Windows 10 1703 or later after users sign in with a Microsoft Account or an Azure Active Directory account, when the hardware meets certain requirements. Device encryption is not enabled with local or domain accounts.

Device encryption is enabled when:

- The device contains a TPM with PCR7 support
- UEFI Secure Boot is enabled
- Platform Secure Boot is enabled
- Direct memory access (DMA) protection is enabled
- InstantGo (AOAC) requirements or HSTI validation is met

Original Equipment Manufacturer (OEM) organisations can choose to disable this feature in order to implement their own encryption technology to a device using a registry key described here: https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-bitlocker

4 Windows Defender Advanced Threat Protection

Windows Defender Advanced Threat Protection (Windows Defender ATP) is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

The Windows Defender ATP platform is where the capabilities that are available across multiple products come together to give Security Operations teams the ability to effectively manage their organisation's network. Windows Defender ATP provides a single pane of glass to detect, investigate and respond to threats, leveraging signals across all onboarded devices including suspicious activities monitoring and events from Windows security features such as Windows Defender NGP, Windows Defender Application Guard, Windows Defender Device Guard, Windows Defender Exploit Guard, Windows Defender SmartScreen or Windows Defender Firewall.

Windows Defender ATP requires one of the following Microsoft Volume Licensing offers:

- Windows 10 Enterprise E5
- Windows 10 Education E5
- Microsoft 365 E5 (M365 E5) - which includes Windows 10 Enterprise E5

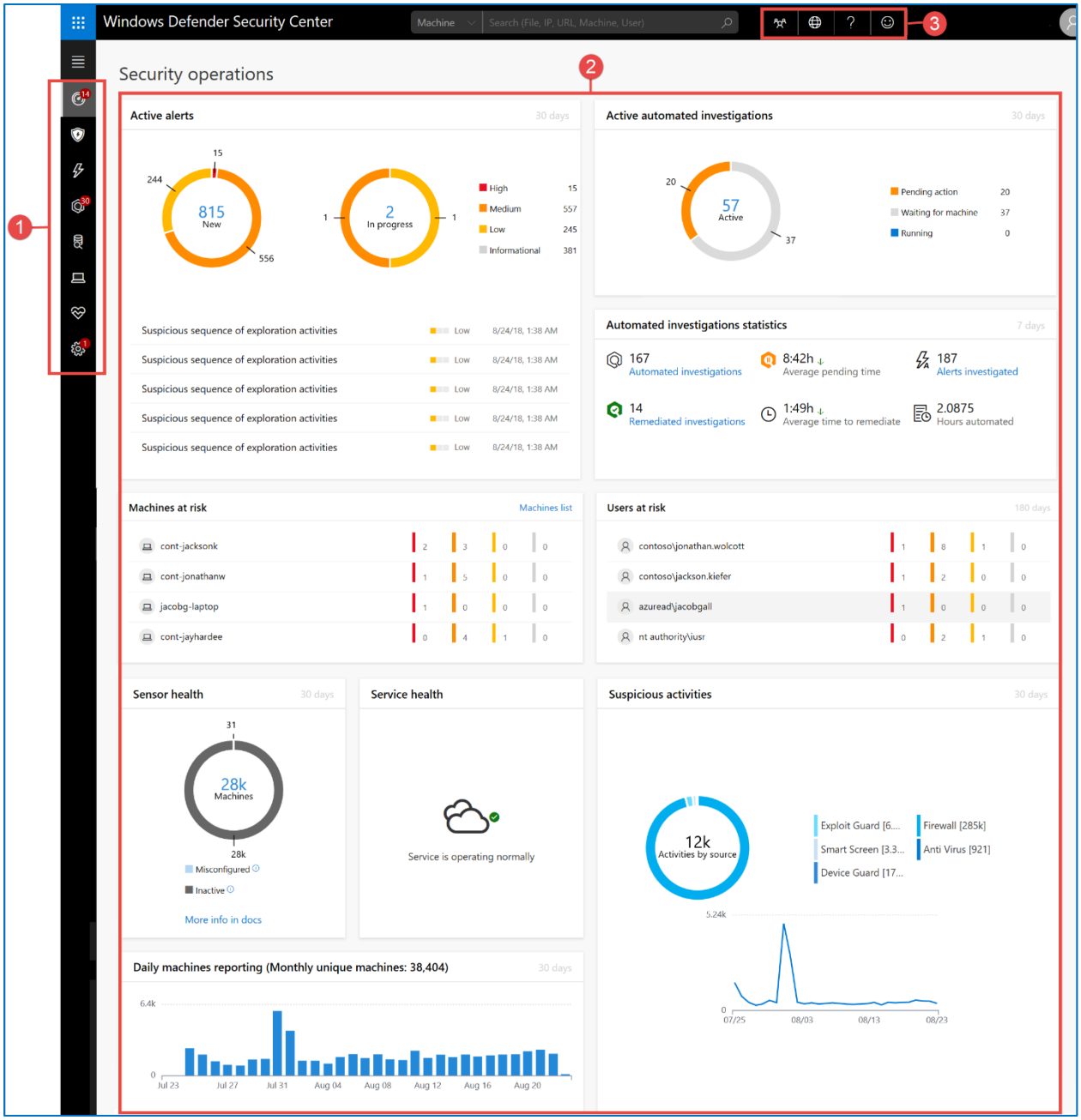
However, Windows Defender ATP also supports onboarding of other operating systems too:

- Windows 7 SP1 Enterprise and Pro
- Windows 8.1 Enterprise and Pro
- Windows 10 Enterprise, Education, Pro and Pro Education
- Windows Server 2012 R2, 2016, 1803 and 2019
- Specific versions of macOS X and some Linux distributions (requires 3rd party licensing)

When onboarding the service for the first time, you can choose to store your data in Microsoft Azure datacentres in the European Union, the United Kingdom, or the United States. Once configured, you cannot change the location where your data is stored. This provides a convenient way to minimise compliance risk by actively selecting the geographic locations where your data will reside. Customer data in pseudonymised form may also be stored in the central storage and processing systems in the United States.

4.1 Windows Defender Security Center

Windows Defender ATP capabilities can be accessed through the Windows Defender Security Center web portal, https://securitycenter.windows.com. This gives enterprise security operations teams a single pane of glass experience to help secure networks. Security centre teams can view, sort and triage alerts from endpoints as well as research for more information such as filenames or IP addresses on observed threat indicators.

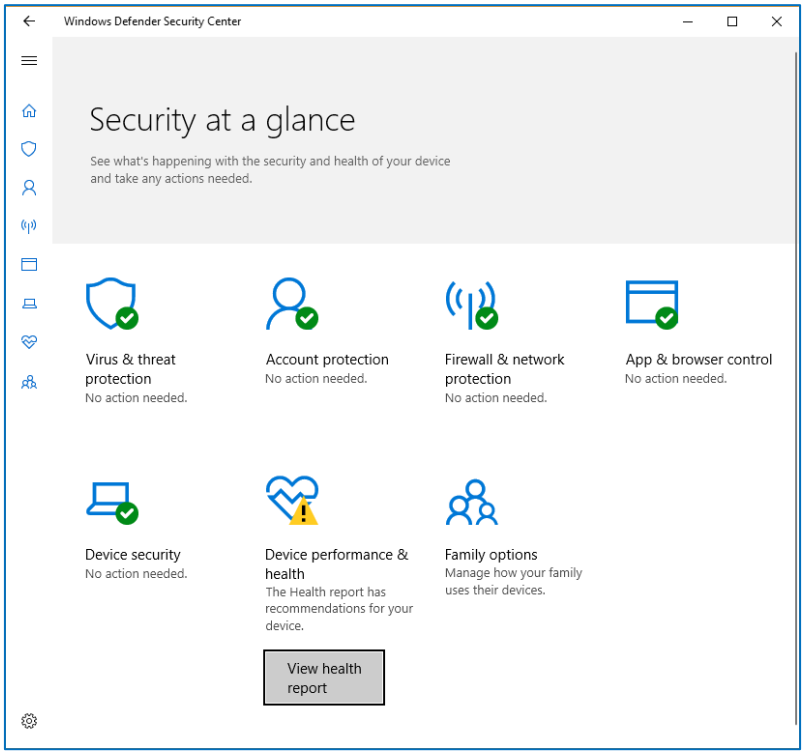

Windows Defender Security Center
Machine
Search (File, IP, URL, Machine, User)
Security operations
1
2
3
Active alerts
30 days
15
244
815
New
556
1
2
In progress
1
High 15
Medium 557
Low 245
Informational 381
Suspicious sequence of exploration activities Low 8/24/18, 1:38 AM
Suspicious sequence of exploration activities Low 8/24/18, 1:38 AM
Suspicious sequence of exploration activities Low 8/24/18, 1:38 AM
Suspicious sequence of exploration activities Low 8/24/18, 1:38 AM
Suspicious sequence of exploration activities Low 8/24/18, 1:38 AM
Active automated investigations
30 days
20
57
Active
37
Pending action 20
Waiting for machine 37
Running 0
Automated investigations statistics
7 days
167
Automated investigations
8:42h
Average pending time
187
Alerts investigated
14
Remediated investigations
1:49h
Average time to remediate
2.0875
Hours automated
Machines at risk
Machines list
cont-jacksonk 2 3 0 0
cont-jonathanw 1 5 0 0
jacobg-laptop 1 0 0 0
cont-jayhardee 0 4 1 0
Users at risk
180 days
contoso\jonathan.wolcott 1 8 1 0
contoso\jackson.kiefer 1 2 0 0
azuread\jacobgall 1 0 0 0
nt authority\iusr 0 2 1 0
Sensor health
30 days
31
28k
Machines
28k
Misconfigured
Inactive
More info in docs
Service health
Service is operating normally
Suspicious activities
30 days
12k
Activities by source
Exploit Guard [6....
Smart Screen [3.3...
Device Guard [17...
Firewall [285k]
Anti Virus [921]
5.24k
0
07/25
08/03
08/13
08/23
Daily machines reporting (Monthly unique machines: 38,404)
30 days
6.4k
0
Jul 23
Jul 27
Jul 31
Aug 04
Aug 08
Aug 12
Aug 16
Aug 20

The Windows Defender Security Center portal has three main areas:

<table>
<tr><th>Area</th><th>Description</th></tr>
<tr><td>(1) Navigation pane</td><td>Use the navigation pane to move between the Dashboards, Incidents, Alerts queue, Automated investigations, Machines list, Service health, Advanced hunting, and Settings
<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>Dashboards</td><td>Access the Security operations, Secure Score and Threat analytics dashboards</td></tr>
<tr><td>Alerts Queue</td><td>View alerts generated from onboarded devices</td></tr>
<tr><td>Automated investigations</td><td>Displays a list of automated investigations that have been conducted in the network, the status of each investigation and other details such as when the investigation started and the duration</td></tr>
<tr><td>Advanced hunting</td><td>Advanced hunting allows users to proactively hunt and investigate across an organisation using a powerful search and query tool</td></tr>
<tr><td>Machines list</td><td>Displays the list of machines that are onboarded to Windows Defender ATP, some information about them, and the corresponding number of alerts</td></tr>
<tr><td>Service health</td><td>Provides information on the status of the Window Defender ATP service. Verify that the service is healthy or if there are current issues</td></tr>
<tr><td>Settings</td><td>Shows the settings selected during onboarding and allows the user to update industry preferences and retention policy period. It is also possible to set other configuration settings such as email notifications, activate the preview experience, enable or turn off advanced features, SIEM integration, threat intel API, build Power BI reports, and set baselines for the Secure Score dashboard</td></tr>
</table></td></tr>
<tr><td>(2) Main Portal</td><td>Main area displaying the different views such as the Dashboards, Alerts queue, and Machines list</td></tr>
<tr><td>(3) Community Center, Time settings,</td><td>Access the Community Center to learn, collaborate, and share experiences about the product, Windows Defender ATP Guide, Microsoft support and feedback.</td></tr>
</table>

Area	Description
Help and support, Feedback	

Note that there is also a Windows Defender Security Center app, referring to the Windows 10 built-in app that provides a central view on Windows Defender components and other security features on the local computer. This app is not part of the Windows Defender ATP platform.



5 Adoption of Security Technologies in the NHS

With reference to the Top Windows 10 Recommendations guide for the deployment of Windows 10 at the NHS the following three key suggestions were included regarding security:

- Windows 10 is the most secure version of Windows to date and has a great and continuous evolving set of features and capabilities to protect devices, users, data and shared infrastructure against modern security threats. However, although upgrading to Windows 10 inherits some security benefits, the real improvements on security posture comes with the adoption of the new security features and enhancements, such as Virtualization-based Security, Credential Guard, Windows Defender Application Control or Windows Hello. Security is a high priority for every organisation, and deserves investment in understanding, evaluating and implementing these new capabilities within the organisational environment
- The National Cyber Security Centre (NCSC) publishes security guidance that is a crucial part of ensuring that the UK has the capacity to respond to an ever-increasing cyberthreat. The NCSC publish practical and proportionate security guidance to protect both new and existing IT systems, and the UK's critical national infrastructure. As an expedient way of implementing the NCSC guidelines, it is recommended that organisations take advantage of the Microsoft HeadStart for NHS materials to deliver a modern, secure desktop experience
- Consider the Securing Privileged Access journey, focused on usage of dedicated administrative credentials and Privileged Access Workstations (PAWs). Cyber attackers are focusing on privileged access to systems such as Active Directory to rapidly gain wide access across organisations' systems and data. Securing privileged access is a critical step to establishing security assurances for business assets in a modern organisation. Privileged Access Workstation design should consider implementing most of the platform security features to provide a trustworthy device where administrative accounts can perform their job with minimum security risk. For more details on PAWs: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations

While all Windows 10 security features described in this document significantly contribute to raising the security bar for end user devices, some of them are more complex to adopt than others. Certain environments may require a deeper and longer piloting processes to ensure that security does not impede business productivity.

The section below reviews the most relevant items that NHS organisations should consider, when looking to adopt the previously described Windows 10 security technologies to improve end-user device security.

5.1 Adopting hardware-based isolation

Virtualization-based Security (VBS) is a key element of the Windows 10 security stack and is required to implement some of the new Windows 10 security technologies, such as Windows Defender System Guard, Windows Defender Credential Guard or Windows Defender Application Guard. Some other

technologies do not strictly require it, but benefit from enhanced protection when VBS is enabled, such as Windows Defender Application Control and Windows Hello.

Furthermore, in upcoming releases of Windows 10, Microsoft are bringing a subset of VBS features to all editions of Windows (not just Enterprise), helping to ensure customers remain safe from increasingly sophisticated attacks. Devices that meet hardware and firmware requirements will have parts of VBS enabled by default. Additionally, as part of this effort, Hypervisor Protected Code Integrity (HVCI) will also be available and turned on by default in clean operating system installs. This enhancement ensures that the kernel process that verifies code integrity will run in a secure environment provided by VBS. This allows Windows 10 to protect the widest possible range of users and scenarios.

For this reason, it is recommended that NHS organisations evaluate and deploy Virtualization-based Security on Windows 10 devices. For this purpose, **ensure devices comply with virtualisation-based** hardware requirements **and are properly configured to leverage them** (including enabling Secure Boot and boot from UEFI 2.3.1 firmware), and are running **Windows 10 64-bit** so that the Windows Hypervisor is available.

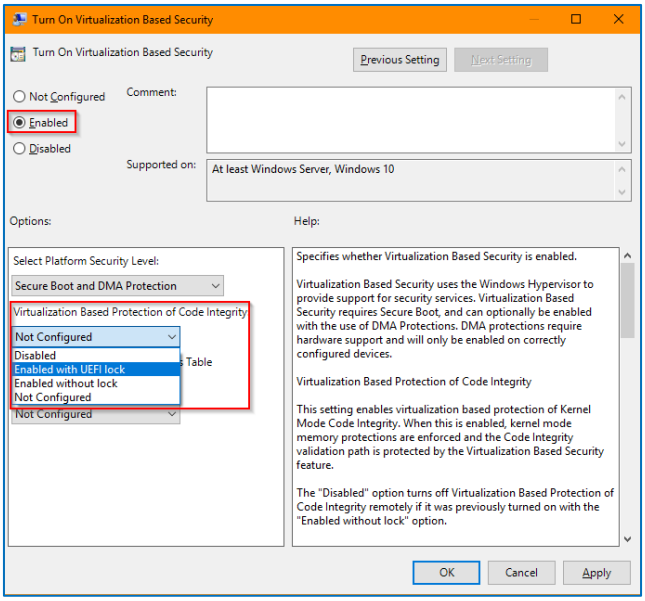
Note that to boot from UEFI firmware, disks must be partitioned with **GPT instead of the MBR partitioning** scheme. Existing Windows 7 or Windows 10 devices running in legacy BIOS emulation (on UEFI-capable devices) use MBR partitioning, and require conversion to GPT partitioning, to boot from native UEFI to leverage new Windows security features that rely on VBS.

From a compatibility perspective, it is vital to ensure that **all system drivers have been tested and verified as compatible with Hypervisor Code Integrity (HVCI).** Additionally, some applications may also be incompatible with HVCI. Issues such as application or system malfunctions or instability, or system crashes may occur during or after enabling HVCI (VBS). The Device Guard and Credential Guard hardware readiness tool can be used to check the HVCI compatibility of all installed drivers on the device before enabling it. While running the Readiness Tool, Device Guard must be disabled, otherwise this might prevent the driver from loading and would not be available for the Readiness Tool to test.

Another compatibility aspect of enabling VBS is that Virtualization-based Security uses the Windows Hypervisor to provide support for security services. This may cause issues with **third-party OS virtualisation solutions** running on Windows 10 with VBS enabled. Please check with your virtualisation software provider for details on compatibility with VBS.

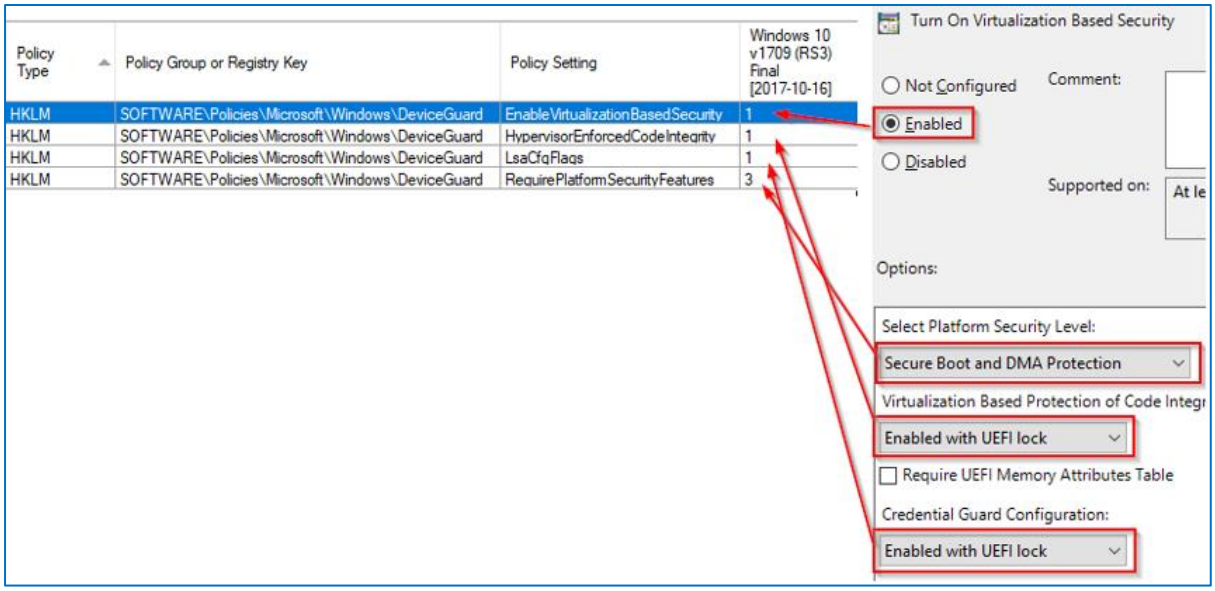
When enabling VBS through group policy, there are two options:

- **Enabled with UEFI lock** ensures that Virtualization Based Protection of Code Integrity cannot be disabled remotely. To disable this feature, you must set the Group Policy to "Disabled" as well as remove the security functionality from each computer, with a user physically present, to clear configuration persisted in UEFI
- **Enabled without lock** allows Virtualization-based Protection of Code Integrity to be disabled remotely by using Group Policy



While using **UEFI lock** is recommended, during piloting and validation scenarios, using **Enabled without lock** allows you to choose the "Disabled" option to turn off HVCI remotely without needing user intervention during system boot.

When **using Microsoft or NCSC Security Baselines** (which build on top of the Microsoft Baselines) **VBS is enable** with all available features in the most complete security configuration possible.



Note: The **Require UEFI Memory Attributes Table** option is not enabled. This option enables Virtualization Based Protection of Code Integrity only on devices with UEFI firmware support for the Memory Attributes Table. Devices without the UEFI Memory Attributes Table may have firmware that is incompatible with Virtualization Based Protection of Code Integrity. In some cases, this can lead to system crashes, data loss or incompatibility with certain plug-in cards. There have been a few scenarios (i.e. a RAID controller) where enabling HVCI without MAT support caused issues, so the option to require MAT was added to policy settings.

While requiring MAT to enable HVCI is the most compatible option (HVCIMATRequired=1), the trade-off is that only very new machines will have UEFI with MAT support today. Most machines without MAT support are capable of supporting HVCI, but requiring MAT causes the HVCI feature to be blocked for them.

For this reason, the Microsoft Security Baselines do not recommend the option is enabled, rather HVCI MAT Required should be disabled and testing conducted using appropriate computer hardware models.

5.2 Adopting Windows Defender Credential Guard

Built on top of Virtualization-based Security, Credential Guard significantly mitigates the risk of pass-the-hash and pass-the-ticket attacks.

As per the HVCI feature, enabling Credential Guard is recommended as part of both the Microsoft and NCSC Security Baselines, with the UEFI lock option also recommended, to provide the best protection.

The potential compatibility issue with Credential Guard is that when enabled, it will break single-sign on experiences relying on NTLMv1, MS-CHAPv2, Digest and CredSSP protocols, as those cannot use the signed-in credentials with Credential Guard enabled. Applications can prompt for credentials or use credentials stored in the Windows Vault which are not protected by Windows Defender Credential Guard.

Additionally, when Credential Guard is enabled, Kerberos does not allow unconstrained Kerberos delegation or DES encryption, not only for signed-in credentials, but also prompted or saved credentials. This may cause issues with distributed applications that rely on unconstrained Kerberos delegation.

5.3 Adopting BitLocker Drive Encryption

BitLocker Drive Encryption is an important security feature, not only from the perspective of preventing unauthorised access to enterprise data stored in stolen or lost devices, but also from the perspective of preventing an attacker tampering with the device while it is offline.

BitLocker Drive Encryption is a well-known security feature already used in most Windows Vista, Windows 7 and Windows 8.1 deployments. By default, Windows 7 uses AES 128-bit with Diffuser as the default encryption method, while Windows 8.0 up to Windows 10 1507 uses AES-128 bit by default, as the Diffuser option was deprecated. Starting with Windows 10 1511, BitLocker uses XTS-AES 128-bit by default for operating system and fixed drives, and AES-CBC 128-bit for removable drives.

Default or previously configured encryption settings applied to existing devices may differ from current Microsoft and NCSC baselines, which recommend XTS-AES 256-bit for operating system drives and AES-CBC 256-bit for removable drives.

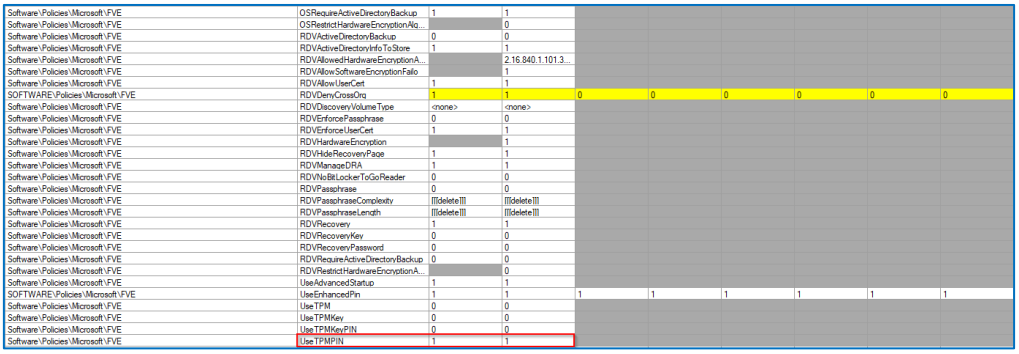
This may lead to a challenge in certain Windows 10 migration scenarios, as once a drive is encrypted with a previous method, changing the method requires either decryption and re-encryption of the drive; or backing up any user data, formatting the drive, re-encrypting it again with the new encryption method and finally restoring the user data.

BitLocker greatly benefits from TPM hardware to prevent device or operating system tampering while the system is offline. While not strictly required, TPM 2.0 usage is highly recommended.

To prevent device data loss from a BitLocker recovery scenario (due to firmware tampering or other conditions that cause a BitLocker 'lock-out'), at a minimum, ensure Bitlocker recovery information is stored in Active Directory. Additionally, consider deploying the Microsoft Bitlocker Administration and Management tool (MBAM), which enables a dedicated security vault for BitLocker recovery keys, plus additional BitLocker management features (such as single use BitLocker recovery keys, with automated key rotation). See https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/mbam-v25/about-mbam-25 for further details.

BitLocker recommended configuration settings in the Microsoft Security Baselines have changed over time, now being less restrictive than initial recommendations. For example, in the Windows 7 and 8.1 baselines, requiring Active Directory backup for OS drives or enable TPM+PIN was recommended. These settings are now left to customer preference, based on how organisations want to configure BitLocker in their environment. However, some older recommendations could still be considered a requirement for certain environments, so is worth evaluating the additional options beyond those recommended in the baselines.

Policy Group or Registry Key	Policy Setting	_MSFT Baselines - Windows 7 SP1 [2012-02-14]	_MSFT Baselines - Windows 8.1 [2014-08-15]	_MSFT Baselines - Windows 10 v1507 (TH1) Final Refreshed without EMET [2017-10-16]	_MSFT Baselines - Windows 10 v1511 (TH2) Final [2016-01-22]	_MSFT Baselines - Windows 10 v1607 (RS1) and Windows Server 2016 Final [2016-10-17]	_MSFT Baselines - Windows 10 v1703 (RS2) Final [2017-08-30]	_MSFT Baselines - Windows 10 v1709 (RS3) Final [2017-10-16]	_MSFT Baselines - Windows 10 v1803 (RS4) Final [2018-04-30]
Software\Microsoft\Windows\CurrentVersion\Policies\System	MaxDevicePasswordFailedAttempts			10	10				
SOFTWARE\Policies\Microsoft\FVE	DisableExternalDMAUnderLock							1	1
Software\Policies\Microsoft\FVE	EnableBDEWithNoTPM	0	0						
Software\Policies\Microsoft\FVE	EncryptionMethod	2							
SOFTWARE\Policies\Microsoft\FVE	EncryptionMethodNoDiffuser		4	4	4				
SOFTWARE\Policies\Microsoft\FVE	EncryptionMethodWithXtsFdv				7	7	7	7	7
SOFTWARE\Policies\Microsoft\FVE	EncryptionMethodWithXtsOs				7	7	7	7	7
SOFTWARE\Policies\Microsoft\FVE	EncryptionMethodWithXtsRdv				4	4	4	4	4
Software\Policies\Microsoft\FVE	FDVActiveDirectoryBackup	0	0						
Software\Policies\Microsoft\FVE	FDVActiveDirectoryInfoToStore	1	1						
Software\Policies\Microsoft\FVE	FDVAllowedHardwareEncryptionAl...		2.16.840.1.101.3...						
Software\Policies\Microsoft\FVE	FDVAllowSoftwareEncryptionFailo		1						
Software\Policies\Microsoft\FVE	FDVAllowUserCert	1	1						
Software\Policies\Microsoft\FVE	FDVDiscoveryVolumeType	<none>	<none>						
Software\Policies\Microsoft\FVE	FDVEnforcePassphrase	0	0						
Software\Policies\Microsoft\FVE	FDVEnforceUserCert	1	1						
Software\Policies\Microsoft\FVE	FDVHardwareEncryption		1						
Software\Policies\Microsoft\FVE	FDVHideRecoveryPage	1	1						
Software\Policies\Microsoft\FVE	FDVManageDRA	1	1						
Software\Policies\Microsoft\FVE	FDVNoBitLockerToGoReader	0	0						
Software\Policies\Microsoft\FVE	FDVPassphrase	0	0						
Software\Policies\Microsoft\FVE	FDVPassphraseComplexity	[[delete]]]	[[delete]]]						
Software\Policies\Microsoft\FVE	FDVPassphraseLength	[[delete]]]	[[delete]]]						
Software\Policies\Microsoft\FVE	FDVRecovery	1	1						
Software\Policies\Microsoft\FVE	FDVRecoveryKey	0	2						
Software\Policies\Microsoft\FVE	FDVRecoveryPassword	0	2						
Software\Policies\Microsoft\FVE	FDVRequireActiveDirectoryBackup	0	0						
Software\Policies\Microsoft\FVE	FDVRestrictHardwareEncryptionAl...		0						
SOFTWARE\Policies\Microsoft\FVE	MinimumPIN	7	7	7	7	7	7	7	7
Software\Policies\Microsoft\FVE	OSActiveDirectoryBackup	1	1						
Software\Policies\Microsoft\FVE	OSActiveDirectoryInfoToStore	1	1						
Software\Policies\Microsoft\FVE	OSAllowedHardwareEncryptionAlg...		2.16.840.1.101.3...						
SOFTWARE\Policies\Microsoft\FVE	OSAllowSecureBootForIntegrity		1	1	1	1	1	1	1
Software\Policies\Microsoft\FVE	OSAllowSoftwareEncryptionFailover		1						
Software\Policies\Microsoft\FVE	OSHardwareEncryption		1						
Software\Policies\Microsoft\FVE	OSHideRecoveryPage	1	1						
Software\Policies\Microsoft\FVE	OSManageDRA	0	0						
Software\Policies\Microsoft\FVE	OSPassphrase		0						
Software\Policies\Microsoft\FVE	OSPassphraseASCIIOnly		0						
Software\Policies\Microsoft\FVE	OSPassphraseComplexity		[[delete]]]						
Software\Policies\Microsoft\FVE	OSPassphraseLength		[[delete]]]						



Software\Policies\Microsoft\FVE	OSRequireActiveDirectoryBackup	1	1						
Software\Policies\Microsoft\FVE	OSRestrictHardwareEncryptionAlg...		0						
Software\Policies\Microsoft\FVE	RDVActiveDirectoryBackup	0	0						
Software\Policies\Microsoft\FVE	RDVActiveDirectoryInfoToStore	1	1						
Software\Policies\Microsoft\FVE	RDVAllowedHardwareEncryptionA...		2.16.840.1.101.3....						
Software\Policies\Microsoft\FVE	RDVAllowSoftwareEncryptionFallo		1						
Software\Policies\Microsoft\FVE	RDVAllowUserCert	1	1						
SOFTWARE\Policies\Microsoft\FVE	RDVDenyCrossOrg	1	1	0	0	0	0	0	0
Software\Policies\Microsoft\FVE	RDVDiscoveryVolumeType	<none>	<none>						
Software\Policies\Microsoft\FVE	RDVEnforcePassphrase	0	0						
Software\Policies\Microsoft\FVE	RDVEnforceUserCert	1	1						
Software\Policies\Microsoft\FVE	RDVHardwareEncryption		1						
Software\Policies\Microsoft\FVE	RDVHideRecoveryPage	1	1						
Software\Policies\Microsoft\FVE	RDVManageDRA	1	1						
Software\Policies\Microsoft\FVE	RDVNoBitLockerToGoReader	0	0						
Software\Policies\Microsoft\FVE	RDVPassphrase	0	0						
Software\Policies\Microsoft\FVE	RDVPassphraseComplexity	[[[delete]]]	[[[delete]]]						
Software\Policies\Microsoft\FVE	RDVPassphraseLength	[[[delete]]]	[[[delete]]]						
Software\Policies\Microsoft\FVE	RDVRecovery	1	1						
Software\Policies\Microsoft\FVE	RDVRecoveryKey	0	0						
Software\Policies\Microsoft\FVE	RDVRecoveryPassword	0	0						
Software\Policies\Microsoft\FVE	RDVRequireActiveDirectoryBackup	0	0						
Software\Policies\Microsoft\FVE	RDVRestrictHardwareEncryptionA...		0						
Software\Policies\Microsoft\FVE	UseAdvancedStartup	1	1						
SOFTWARE\Policies\Microsoft\FVE	UseEnhancedPin	1	1	1	1	1	1	1	1
Software\Policies\Microsoft\FVE	UseTPM	0	0						
Software\Policies\Microsoft\FVE	UseTPMKey	0	0						
Software\Policies\Microsoft\FVE	UseTPMKeyPIN	0	0						
Software\Policies\Microsoft\FVE	UseTPMPIN	1	1						

5.4 Adopting Windows Defender AV, Exploit Guard and SmartScreen

Windows Defender NGP, SmartScreen and some exploit protection configurations are enabled by default in Windows 10 to provide protection against malware and web-based attacks.

The Microsoft and NSCS security baselines include configuration designed to prevent users from bypassing SmartScreen blocks or disabling Windows Defender NGP features.

Windows Defender NGP real-time protection is required for most Windows Defender Exploit Guard features to work (Attack Surface Reduction rules, Network Protection and Controlled Folder Access), and Microsoft and NCSC security baselines include configuration items for Exploit Guard features; these won't work without Windows Defender NGP real-time protection enabled.

These are important points to consider when third-party antivirus solutions are used in the estate instead of Windows Defender NGP, as most Windows Exploit Guard features cannot be used, and these baselines settings will likely need to be disabled for these third-party antivirus solutions to work correctly. Additionally, administrators may want to hide certain options in the Windows Security Center app.

5.5 Adopting Windows Defender Firewall

Windows Defender Firewall is another Windows 10 feature that comes enabled by default and is enforced by Microsoft and NCSC security baselines.

Additionally, the NCSC baselines rely on Windows Defender Firewall rules to enforce the use of an 'Always-on VPN', as part of the NCSC assured data-in-transit protection security principle. This security design principle means that VPN gateways and Internet proxy servers must be properly configured and sized to accommodate sustained device connectivity whilst providing acceptable Internet-access speed for all remote devices over the VPN service.

When choosing to implement a third-party host based firewall instead of Windows Firewall, organisations will need to consider that having Windows Defender Firewall enabled together with another firewall product may cause unintended network communication behaviour and this is likely to drive some deviation from the NCSC baselines. To implement the recommended NCSC baselines settings for always-on VPN enforcement will require configuration of the third-party product to provide equivalent behaviour.

Certain Windows features and Windows-as-a-Service oriented services such as Delivery Optimization, Windows SmartScreen, Windows Analytics or Windows Defender ATP may require administrators to

closely identify and define host-based firewall exceptions to allow communications with related service endpoints on the Internet when the device is outside the corporate network and not connected via VPN.

5.6 Adopting Application Control

AppLocker functionality is a whitelisting technology to control which applications can be executed, and also to block specific programs from being executed. Examples include blocking obsolete versions of corporate applications, preventing known malware payloads or restricting the use of unsupported browsers within the organisation.

AppLocker rules are also defined in the NCSC baselines to block the execution of any application outside of the Windows or 'Program Files' folder locations, with a few exceptions such as Microsoft OneDrive binaries. This means that applications installed in non-standard locations and user-installable applications such as Microsoft Teams or Click-To-Run applications that don't require administrative rights (and are running from the user's profile), will be blocked by default when using the NCSC baselines. Additional AppLocker rules are required to enable the execution of any known business-related applications from these types of locations.

Leveraging Windows Defender Application Control (WDAC) requires additional planning and testing when it comes to application control through whitelisting, compared to AppLocker. Unlike AppLocker, which allows restrictions based on the whitelist at user level, Windows Defender Application Control defines a **single, device-based policy** that determines what is allowed, while everything else is blocked. The policy can be digitally signed for additional security, and potentially used to block non-interactive services, drivers and Windows components. It is more complex to initially define and maintain than AppLocker rules, especially when business applications can vary significantly from device to device and would require multiple WDAC policy files.

To help organisations adopt Windows Defender Application Control, it supports a feature based on AppLocker called Managed Installer which allows administrators to automatically authorise applications that are deployed and installed from a designated software distribution solution (such as System Center Configuration Manager). A managed installer helps IT administrators balance security and manageability requirements when employing application execution control policies. It provides a solution that does not require explicit rules for software being managed through software distribution. However, this means that to leverage this feature all software that being run in the organisation has to be managed through the software distribution solution. The managed installer feature also has certain limitations and security implications when compared to explicit rules in the code integrity policy. See here for additional information.

5.7 Adopting Windows Hello for Business

When considering the deployment of Windows Hello for Business, it is important to understand that it implies certain configuration, recommended hardware (TPM 2.0) on the end user device, and specific infrastructure services be available in the corporate network to accommodate its requirements.

Furthermore, deployment varies depending on how your identity provider is configured: Active Directory, Azure Active Directory and/or ADFS. These will influence whether you choose between hybrid and on-premises deployments, and between key-based and certificate-based trust models.

Windows Hello for Business implementation has different infrastructure requirements depending on the deployment options, which can be reviewed here: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification.

Regardless of the chosen deployment option, there are some common infrastructure requirements. Adopting this security feature requires a coordinated effort across Workplace, Security, Identity and Infrastructure teams within the organisation covering these areas:

- Active Directory Windows Server 2016 schema
- Windows Server 2008 R2 Domain/Forest functional level
- Windows Server 2012 or later Certificate Authority
- Multi-factor authentication

6 References

Malware protection

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/windows-defender-antivirus-in-windows-10

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/windows-defender-antivirus-compatibility

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-smartscreen/windows-defender-smartscreen-overview

Hardware-based isolation

https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-recommendations#tpm-20-compliance-for-windows-10

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/how-hardware-based-containers-help-protect-windows

https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows-defender-application-control?ocid=cx-blog-mmpc

https://cloudblogs.microsoft.com/microsoftsecure/2017/10/23/hardening-the-system-and-maintaining-integrity-with-windows-defender-system-guard/?source=mmpc

https://techcommunity.microsoft.com/t5/Windows-Insider-Program/Windows-Defender-System-Guard-Making-a-leap-forward-in-platform/td-p/167303

https://www.youtube.com/watch?v=AztAJdBdcec

https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs

Application Control

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/what-is-applocker

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control

Exploit Protection

https://web.archive.org/web/20180706044327/https://technet.microsoft.com/en-us/security/jj653751

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/exploit-protection-exploit-guard

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/attack-surface-reduction-exploit-guard

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/network-protection-exploit-guard

Network Protection

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/isolating-apps-on-your-network

Credentials Protection

https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-credential-guard

https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-how-it-works

Data Protection

https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-device-encryption-overview-windows-10

https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-recovery-guide-plan

https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-network-unlock-faq

https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/device-encryption-for-oem

Windows Defender ATP

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/windows-defender-advanced-threat-protection

https://docs.microsoft.com/en-us/windows/security/threat-protection/

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/onboard-configure-windows-defender-advanced-threat-protection

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/data-storage-privacy-windows-defender-advanced-threat-protection

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-endpoints-windows-defender-advanced-threat-protection

https://www.youtube.com/watch?v=qxeGa3pxIwg