WINDOWS 10 SECURITY

NEW SECURITY FEATURES REVIEW
# TABLE OF CONTENTS

1. MANAGEMENT SUMMARY  
   3

2. VIRTUALIZATION BASED SECURITY  
   4
   2.1. INTRODUCTION  
   4
   2.2. CREDENTIAL GUARD  
   5
   2.3. DEVICE GUARD  
   6
   2.4. LIMITATIONS  
   7
   2.4.1. DEPLOYMENT  
   7
   2.4.2. CONFIGURATION  
   7
   2.4.3. COMPARING PROTECTIONS AGAINST CURRENT ATTACKS  
   8
   2.5. ATTACKS AND PROTECTIONS SUMMARY  
   9

3. AUTHENTICATION AND AUTHORIZATION  
   10
   3.1. WINDOWS HELLO  
   10
   3.2. MICROSOFT PASSPORT  
   10

4. MICROSOFT EDGE  
   11
   4.1. EXPLOIT MITIGATIONS  
   11
   4.1.1. DEFAULT EPM MODE  
   11
   4.1.2. REDUCED ATTACK SURFACE  
   11
   4.1.3. INTEGRATED PLUGINS  
   11
   4.1.4. SANBOXED EXTENSIONS  
   11
   4.1.5. ENHANCED EXPLOITATION PREVENTION MECHANISM  
   12
   4.1.6. BINARY INJECTION MITIGATION  
   12
   4.2. SMARTSCREEN FILTER  
   12

5. THIRD PARTY APPLICATIONS  
   13
   5.1. DETAILS  
   13
   5.2. SUMMARY  
   14

6. ANTIMALWARE  
   15

7. REQUIREMENTS SUMMARY  
   16
1. MANAGEMENT SUMMARY

As with every release of a Microsoft operating system, new security features form part of the Windows 10 release. As such, some clarification on their goals and recommendations is required by IT departments. The aim of this document is to present the security features introduced by Microsoft in Windows 10 Enterprise and on releases up to and including Threshold 2, which is the latest version at the time of writing.

Several of these features are based on virtualization technologies provided by recent processors (Intel i5 and later) and are regrouped by Microsoft under the term Virtualization Based Security. Virtualization provided by the processor makes it possible to enforce segmentation between different realms, since security as dealt with by the traditional userland/kerneland concept is not sufficient enough against today’s attacks. In order to achieve its security objectives, however, virtualization requires the use of UEFI and Secure Boot to provide a trusted boot mechanism for the privileged realms. VBS includes Credential Guard and Device Guard.

As passwords create a headache for many organizations Microsoft is also adding authentication mechanisms based on simplified Multi-factor Authentication (MFA) and the use of biometrics. Microsoft has called the new authentication/SSO mechanism Microsoft Passport, and the biometric authentication mechanism is performed by Windows Hello.

With regards to authorization, Windows 10 Enterprise delivers better integration of Dynamic Access Control, a feature from Windows Server 2012, enabling it to use contextual information (such as the user’s device name or network location) to increase the granularity of access rights to corporate resources. The Enterprise Data Protection feature also enables improved management of information, acting as a Data Leakage Protection (DLP) solution, and making it possible to establish a strict separation between corporate and private worlds, to create encryption rules and initiate remote wipe.

Windows 10 Enterprise also comes with a new edition of Microsoft browser, named Edge, which also includes new security features that aim to thwart standard software exploitation and protect users. Some of these preventative software exploitation features are also available to 3rd party applications compiled with Visual Studio 2015.

Previous security features are still available under Windows 10 Enterprise, such as BitLocker, and are easier to deploy when paired with Windows Server 2012 (or later). Previous solutions such as Windows Defender have been upgraded in order to leverage other protective features and have better enterprise integration.

It should be noted that the security of Windows 10 workstation should be implemented within a wider strategy that can be based on newer Microsoft technologies such as Local Administrator Password Solution (LAPS) or Advanced Threat Analytics (ATA), configured at the domain level.
2. VIRTUALIZATION BASED SECURITY

2.1. INTRODUCTION

Since 2007, both Intel and AMD have incorporated virtualization features into their processors, allowing virtualization to take place with this technology rather than software. Intel technology is named VT-x and makes it possible to create virtual processors, each with separate memory space. Another solution, named VT-d, is specific to the Virtualization Technology for Directed I/O, which is used when a virtual machine needs to communicate with a specific device.

This last point is important, as without memory segmentation it would be possible for virtual machines to spy on each other’s address space, resulting in data leakage. By leveraging this technology, with no known serious flaws disclosed to date, Windows has created another level of separation on top of the traditional rings (which are also enforced by the processors at both the instruction level and the memory page level) whereby the kernel is run at the Ring 0 level and the userland applications at the Ring 3 level (less privileges).

Note: In the following section, VBS relates to Virtualization Based Security and not Microsoft Visual Basic Studio solution.

VBS offers two Virtual Trust Levels (VTLs), as depicted in the schema below:

0. Normal World
1. Secure World

![ARCHITECTURAL LAYER OVERVIEW](image)

Figure 1 A. Ionescu, battle of SKM and IUM, Blackhat US’15

The use of memory page rights enables the following options:
- Blocking read access: allows secrets in VTL 1 to be hidden from VTL 0
- Blocking read and execution: allows execution of code or modification of code (if write access also denied) to be prevented
- Blocking write access: allows modification of executable pages shared between VTL 0 and VTL 1
Applications running in VTL 1 are called Trustlets.

Obviously, if virtual machine file systems are stored on the hypervisor’s file system and loaded by a compromised kernel, this method becomes redundant. For this reason, the implementation of VBS under Windows 10 Enterprise relies on Trusted Platform Module (TPM), Secure Boot and code signing certificates in order to validate code that should be loaded in privileged virtual machines. At boot, a small footprint hypervisor signed by Microsoft is run, the role of which is to load the virtual machines running Trustlets at the required privilege levels.

The protection of virtual machines, which run at a higher privilege level, from unauthorized access by devices through DMA, is provided by VT-d IOMMU.

VBS is the base for several security components of Windows 10 and Windows Server 2016: Credential Guard, Device Guard and vTPM for Windows 10 and Guarded Fabric for Windows Server 2016.

As Guarded Fabric is related to Windows Server 2016, just a brief summary is necessary. Guarded Fabric removes the risk of a malicious Hyper-V administrator either tampering with a virtual machine or accessing its file system using their access rights. With Guarded Fabric, virtual file systems are encrypted and the key is only provided to the hypervisor by the TPM once these components have proved their integrity.

2.2. CREDENTIAL GUARD

In Windows architecture a specific service, Local Security Authority Subsystem Service (LSASS) is responsible for handling credentials and cryptographic material. Only LSASS is allowed to access the credentials store once the system has booted, and as such, Windows authentication mechanisms rely on it to perform validation of credentials.

Since the release of Windows XP, one of the most common attacks involves malicious actors with administrative privileges initiating a service that injects executable code into LSASS. This code then retrieves the stored credentials, either by extracting hashes to crack or pass (e.g. fgdump, Pass-the-Hash), or by using the query API to decrypt the memory that contains the clear-text credentials from opened users sessions (as performed by Mimikatz).

In order to prevent this type of attack, Microsoft had implemented several security measures in previous versions of Windows, all of which were defeated. The latest efforts at improving security involved making LSASS a Protected Process Light – a security feature that prevents access to the process by unauthorized third party accesses. Authorization relies on code signing certificates that contain specific EKU (Extended Key Usage) delivered by Microsoft. This approach is bypassed by signing the attack tool with a legitimate code signing certificate that can be bought from Microsoft. For example, the Mimikatz author possesses such a certificate, allowing them to use this tool. Recently, Microsoft also extended PatchGuard (a kernel’s structure integrity mechanism, introduced in the 64-bit version of Windows XP SP1) in order to check the integrity of protected processes, detect an attack and reboot the host – but this is only relevant as long as the process has not been reverted to its original state.

Another point worth noting is that Microsoft’s implementation of Kerberos relies on the NTLM hash as the RC4 key in the Kerberos pre-authentication process (AS-REQ). As such, the extraction of this information from the Kerberos provider service allows execution of a standard pass-the-hash attack, trying to crack the hash or even to perform a valid TGT (Ticket Granting Ticket) Kerberos request. Moreover, the AES keys that can be retrieved from the Kerberos provider memory also allow an attacker to perform a valid TGT request. Both of these attacks that retrieve a valid TGT are known as overpass-the-hash.

By leveraging VBS, Windows 10 Enterprise is splitting LSASS into a service and a trustlet (LSALSO) that access the domain credentials for current user sessions. As such, attack tools that inject code into the service are no longer effective, since they will not be able to access the hashed values or the encrypted blob of memory.

Even though it is possible to obtain a signing code certificate to generate a valid trustlet that can run in VTL 1, trustlets are separated from each other both by design and as a result of the technologies used, and an attacker will not be able to perform malicious actions.
2.3. DEVICE GUARD

Device Guard is a code integrity feature introduced in Windows 10 Enterprise. It is the successor of AppLocker, introduced in Windows 7, and the Software Restriction Policies (SRPs) before it. The goal of this feature is to prevent execution of unauthorized binaries on endpoints, in a blacklist and/or whitelist mode.

Even if most current attacks start with the exploitation of software vulnerabilities in client-side applications (ex. browsers and extensions) the next step of attackers is deploy a binary that performs their desired actions (ex: ransomware, RAT, …). Upon proper configuration, whitelisting solutions such as AppLocker or Device Guard will block this step.

SRPs enabled the creation of execution rules based on the three core criteria:

- File path
- File hash
- Code signing certificate

AppLocker uses the same core criteria but has addressed some of the limitations of SRPs. While previously, it was only possible to create rules at the computer level, AppLocker allows rulesets to be applied at the group or user level in an Active Directory. Moreover, it is possible to set AppLocker rules in an audit mode and have more granular rules, for example based on the publisher information extracted from a signed binary.

**Note:** AppLocker features should not be confused with PatchGuard, which prevents the execution of unsigned drivers.

The AppLocker approach can be circumvented if an attacker is already on the device (e.g. executing code in the memory of an authorized process, or through an opened RDP session) and tampers with the components and rulesets. Moreover, AppLocker stops at the user level and does not allow system administrators to create rules for drivers. By leveraging VBS, Windows 10 Enterprise can perform code integrity operations in trustlets, protecting the mechanism against tampering.

In order to prevent the ruleset being tampered with, Microsoft also recommends using the feature to digitally sign the ruleset.
2.4. LIMITATIONS

2.4.1. DEPLOYMENT

One of the requirements for Virtualization Based Security is a VT-x and VT-d compatible processor, but also the use of UEFI as the firmware interface, (instead of the legacy BIOS). With Windows 7 the boot process of the operating system was changed, in order to leverage the new features of this technology. Due to backward compatibility issues, however, Windows releases are always delivered with both the BIOS and UEFI compatible kernels.

Many organizations installed Windows 7 Enterprise using the default features and by extension, used the legacy boot manager rather than the one based on UEFI. If the company is planning an “in place” upgrade of Windows 7 hosts to Windows 10, this can complicate the migration process, as UEFI cannot be set as the firmware interface through this method. As a result, VBS features are not be available.

The screenshot below is an example of a Windows 7 Enterprise installation based on BIOS (legacy) mode. An UEFI installation indicates the following path for the boot manager:

\EFI\Microsoft\Boot\bootmgfw.efi

Deployment limitation can also occur when Windows Server 2016 instances, which also implement VBS features, are running on a hypervisor that precedes Windows Server 2016, and does not implement vTPM in Microsoft Hyper-V. So far, the states of 3rd party hypervisors vary: Xen implements vTPM whereas VMware ESX seems not to.

2.4.2. CONFIGURATION

One of the challenges of whitelisting solutions is the amount of work they require in order to be properly deployed and, more importantly, maintained over time. Keeping static images in the entire company is not always possible, and even with rulesets that can be applied to specific groups, this is not a simple task. In order to deal with this challenge, it is recommended to go through an initial validation step, using the auditing mode before switching to a full lockdown for AppLocker and Device Guard.

Regarding configuration, it should be noted that some %SYSTEMROOT% subfolders or other standard folders are writable by standard users, so these should be validated with care and the default rules should be reviewed.
Another common bypass technique is to use binaries signed by Microsoft that allow new processes to be started, based on the user’s content (such as JavaScript, libraries, PowerShell scripts, etc.) but these also need careful review.

It should also be noted that authorized binaries might be prone to software vulnerabilities that allow attackers to execute code inside them. Shellcode will perform all actions (limited by the privileges assigned to the process). In order to implement more complex actions, attackers usually download and execute a binary, or load a library from the shellcode. Although this can be blocked by whitelisting solutions, some Windows API functions have flags that discard AppLocker (fixed in KB2532445 and not present in Windows 10 Enterprise).

More information on how to prevent execution of code in authorized processes through software vulnerability exploitation, can be found in "Exploitation Mitigation" below.

A difference in configuration from AppLocker is that with VBS, policies are applied to computer objects and not users, as the solution requires hosts to run both the hardware and the right services.

2.4.3. COMPARING PROTECTIONS AGAINST CURRENT ATTACKS

Credential Guard can only protect domain credentials, even on a Windows 10 Enterprise host. As such, all local account credentials are still extractable using the same tools as presented above (e.g. Mimikatz).

Although the NTLM hashes and the user AES keys for Kerberos are handled by LSASS in the trustlet, the TGTs (Ticket Granting Ticket) generated by the authentication server upon successful request for accessing a specific service, are not. As such, it is still possible to retrieve the session key for a specific service and use it during its validity period (10 hours, by default).

Retrieving the TGS also enables the retrieval of the session key encrypted with the service account password’s hash. If RC4 is the default encryption, it is possible to perform a brute-force attack in order to retrieve the service account NTLM hash. For services such as MSSQL, where the service account is defined by an administrator, it might be possible to retrieve the password as well. However, as AES has been the default encryption scheme since Windows Server 2008, the chance of a malicious actor performing a successful brute-force attack in a short period of time is reduced, as AES is more resource consuming and a salt is used.
## 2.5. ATTACKS AND PROTECTIONS SUMMARY

<table>
<thead>
<tr>
<th>Attack</th>
<th>Windows 10 protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extraction of domain accounts NTLM hashes</td>
<td>Credential Guard</td>
</tr>
<tr>
<td>Extraction of local accounts NTLM hashes</td>
<td>Still possible</td>
</tr>
<tr>
<td>Extraction of clear-text domain passwords for running sessions</td>
<td>Windows 8.1 removed clear-text</td>
</tr>
<tr>
<td>Extraction of clear-text local passwords</td>
<td>Windows 8.1 removed clear-text</td>
</tr>
<tr>
<td>Extraction of secrets through DMA</td>
<td>Credential Guard (VT-d / IOMMU)</td>
</tr>
<tr>
<td>Pass-the-Hash on domain accounts</td>
<td>Credential Guard</td>
</tr>
<tr>
<td>Overpass-the-hash</td>
<td>Credential Guard</td>
</tr>
<tr>
<td>Pass-the-ticket (TGS)</td>
<td>Still possible</td>
</tr>
<tr>
<td>Bootkit</td>
<td>Secure Boot (UEFI)</td>
</tr>
<tr>
<td>Rootkit loaded before anti-malware solution</td>
<td>ELAM(^1) and Device Guard</td>
</tr>
<tr>
<td>Malware and unauthorized applications</td>
<td>Device Guard (or AppLocker)</td>
</tr>
<tr>
<td>Tampering with whitelisting solution</td>
<td>Device Guard</td>
</tr>
<tr>
<td>Tampering with whitelisting ruleset</td>
<td>Device Guard signed ruleset</td>
</tr>
</tbody>
</table>

---

\(^1\) Early Launch Anti-Malware
3. AUTHENTICATION AND AUTHORIZATION

3.1. WINDOWS HELLO

Windows Hello is Microsoft’s new technology for biometric-based authentication. The set of methods currently include the following:

- Face recognition
- Iris scan
- Fingerprint scan

Face recognition has to be performed with a certified camera. At the moment this means either the camera in the Surface Pro 4 that includes an infrared sensor, or 3D cameras such as Intel RealSense. The iris scan is specific to Windows 10 Mobile devices such as the Nokia Lumia 950. As with face recognition, the method for iris scanning is based on both a high resolution camera and an infrared camera.

All methods require the user to define a PIN code to unlock the device first. This PIN complexity can be configured by GPO and contains not only numeric values but alphanumeric and special characters as well. Once the PIN is defined, the user can enroll the device using one of the supported methods.

Secrets for Windows Hello are stored on the host TPM chip and are not transmitted outside of the device.

3.2. MICROSOFT PASSPORT

Passport is the new key-based authentication mechanism supported by Windows 10. It is compatible with the FIDO alliance specification and is based on a multi-factor authentication principle. It consists of an enrolled device and either Windows Hello or a PIN. As the secrets unlocked by Hello or the PIN are stored in the device TPM chip, the device itself is considered as the other half of the two-factor authentication system.

When the device is enrolled, a public/private key pair is generated locally (key-based mode), if the company has a PKI infrastructure (certificate based mode), a certificate is created. The hardware key generation model is more secure, as the private key is generated and stored in either the private or corporate containers of the TPM chip. With the separated containers, remote wipes of the corporate container are only possible through the use of Intune.

Kerberos-based authentication in an active directory environment will use a nonce signed by the user’s private key or certificate linked to a device. The authentication server will then validate this signature to authorize the start of a Kerberos session. As the keys or certificate are linked to a device, an attacker should not be able to reuse it on another host, though the TPM storage of the user’s secrets should prevent this from happening in the first place.

Passport requires an AD FS and is compatible with both on-premise Active Directory environment (upgrade to Windows Server 2016 schema necessary) and Azure AD. The usage of key based authentication, however, requires Windows Server 2016 domain controllers.
4. MICROSOFT EDGE

4.1. EXPLOIT MITIGATIONS

Edge is Microsoft’s successor to Internet Explorer and, from what Microsoft claims, delivers additional security to the browser. The security features of Edge are outlined below.

4.1.1. DEFAULT EPM MODE

Windows 8 introduced Enhanced Protection Mode for Internet Explorer, without any plugins and using Application Containers, but these features were hardly used due to the broken compatibility with plugins.

Being a new browser, Edge does not need to keep backward compatible. As such, it enables EPM by default and runs both the broker and the renderer processes in 64-bit mode (only the broker process was 64bit on Windows 8).

4.1.2. REDUCED ATTACK SURFACE

For years, Browser Helper Objects and ActiveX controls were an attack vector for IE. They acted either as vulnerable components or as a way to generate executable code in the browser context (ROP exploitation) as most of the time they lacked enhanced security or were not compiled as position independent. In Edge, both BHOs and ActiveX have been dropped. For the same reason, scripting languages such as VBScript are also no longer supported.

**Note:** While add-ons are disabled and Edge code base is compiled with mitigation mechanisms, 3rd party tools such as security products might be injecting executable code with less security in the Edge address space and should, as such, be carefully reviewed.

4.1.3. INTEGRATED PLUGINS

Although it is recommended to disable Flash and PDF readers plugins due to security concerns, Edge will now integrate them as part of the browser. The fact that this opens up another attack vector is balanced by the fact that updates for those components can now be deployed using Windows Updates.

4.1.4. SANBOXED EXTENSIONS

The plugin mechanism has been redesigned in order to leverage protection provided by the EPM sandbox. Although sandbox escape vulnerabilities have been demonstrated in the past, this is a highly recommended feature nowadays as it makes the attacker’s task more complicated.
4.1.5. ENHANCED EXPLOITATION PREVENTION MECHANISM

The most recent vulnerabilities impacting Internet Explorer and browsers in general are related to a class of memory corruption vulnerabilities known as Use-After-Free (UAF). Several exploit mitigation techniques have now been integrated into the Edge codebase, such as MemCG and Abandonment. These features combined with other mitigation mechanisms such as DEP and ASLR make it more difficult for an attacker to successfully exploit vulnerabilities.

![Image of Edge processes Integrity Level](image)

**Figure 3: Edge processes Integrity Level**

4.1.6. BINARY INJECTION MITIGATION

As presented in the point above, removing plugins does not completely solve the binary injection problem, as processes with sufficient rights might inject or load libraries into Edge. Windows 10 Enterprise TH2 brings an additional security feature based on code integrity (Device Guard is not required) that will only load Windows components or WHQL signed binaries (Windows Hardware Quality Lab, used for device drivers).

**Note:** This feature is not limited to Edge and is available to all applications from Windows 10 TH2 onwards, if configured in the process mitigation policy.

This mitigation policy is however not a silver bullet as it is still possible to inject executable code if it is running only in memory, in the form of a shellcode.

4.2. SMARTSCREEN FILTER

The SmartScreen filter makes it possible to detect whether or not the web site being visited is known to be malicious. Microsoft does this by performing a validation for each request the user makes, either through Edge or through applications from the Windows Store.

![Image of SmartScreen Filter](image)

**Figure 4 Traffic from SmartScreen Filter when accessing a known bad URL**
5. THIRD PARTY APPLICATIONS

5.1. DETAILS

As the Windows platform uses many external applications, it makes sense to check the default compilation options related to security in Visual Studio 2015. Although this is less relevant than with platforms such as iOS and Android where applications are usually recompiled with the latest toolset for each new OS release, it provides an overview of the security features that will be included in Windows 10 releases of 3rd party applications.

The Edge MemCG and Abandonment features presented above are specific to the browser HTML and JavaScript objects, and as such, are not available to a wider audience.

Although the kernel is in charge of loading binaries and creating their execution environment, providing randomization for the usage of Address Space Layout Randomization (ASLR), modules still need to be compiled as Position Independent Executable (PIE) in order to benefit from this security feature. In Visual Studio 2015 modules are compiled as PIE by default, using the `/DYNAMICBASE` linker option. In 64-bit environments, 64-bit applications can benefit from a larger entropy using the `/HIGHENTROPYVA` which is also compiled by default for these processes.

In order to prevent stack based buffer overflow a detection mechanism can be put in place by adding code at compilation time. This protection, named stack canary, consists in storing a randomized value before the saved instruction pointer during the function prologue and validating this value in the epilogue. In case a stack based buffer overflow is performed, the attacker will need to overwrite this value which will not match during detection phase. This feature is strong as long as the randomized value is kept unknown to the attacker (ie. high entropy and no memory disclosure vulnerability impacting the application. This feature is enabled using the `/GS` compiler option.

Memory pages privileges can also be set in order to restrict execution rights to writable pages, in order to prevent an attacker from writing shellcode in the process address space. This feature can leverage CPU functionality (NX bit on Intel processors for example) or be performed in full software mode on older processors. Visual Studio 2015 also enables the Non-Executable bit (NX) using the `/GS` compiler option.

When exploiting software flaws, such as heap overflows or arbitrary writes more generally, attackers usually replace the function pointers in writable pages. On Linux systems, a common technique is to rewrite the Global Offset Table (GOT) or Procedure Linkage Table (PLT) of the process in which the pointers to dynamically loaded code are loaded. The same technique is not possible in Windows since the OS loader merges the Import Address Table (IAT) with the read-only data into the .rdata section of the process (mitigated by RELRO option of the linker on Linux). However, function pointers in C++ objects (especially vtable) can still be overwritten, and as merging them in the .rdata section is not possible, Microsoft has implemented a technic named Control Flow Integrity (CFI). The goal of CFI is to validate function pointer addresses at runtime, based on information calculated during the compilation phase. Visual Studio 2015 allows the implementation of this feature using the `/guard:cf` compiler option, disabled by default.

Another type of function pointer that used to be overwritten in Windows applications is Structured Exception Handler (SEH). Microsoft implemented SafeSEH security from Windows Vista onwards, and this is still the latest version available. This feature is enabled using the `/SAFESEH` linker option on 32-bit applications. As 64-bit applications do not use the stack to store exception handlers (function pointers) but use instead a table defined during the linking process that is stored in a read-only memory page, this option is not available for this platform.

The binary injection mitigation feature presented above and implemented in Edge from Windows 10 TH2 onwards, is also available to 3rd party applications by using the `/INTEGRITYCHECK`. This feature is disabled by default and due to the potentially undesired side effects it could cause, it is recommended to test the application carefully before enabling it in production code.
5.2. SUMMARY

<table>
<thead>
<tr>
<th>Name</th>
<th>Compiler/linker option</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASLR</td>
<td>/DYNAMICBASE (32 AND 64 BIT) /HIGHENTROPYVA (64 BIT)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Non-Executable bit</td>
<td>/NXCOMPAT</td>
<td>Enabled</td>
</tr>
<tr>
<td>Stack canary</td>
<td>/GS</td>
<td>Enabled</td>
</tr>
<tr>
<td>Control Flow Integrity</td>
<td>/guard:cf</td>
<td>Disabled</td>
</tr>
<tr>
<td>Safe SEH</td>
<td>/SafeSEH (32 bit)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Binary injection mitigation</td>
<td>/INTEGRITYCHECK</td>
<td>disabled</td>
</tr>
</tbody>
</table>
6. ANTIMALWARE

Although most enterprises rely on a 3rd party antimalware solution, Microsoft provides a solution of its own: Windows Defender. Introduced in Windows 8, Defender has been updated in order to provide better integration with enterprise management, either through group policies, SCCM or through InTune.

Further integration with standard applications and 3rd party antimalware solutions is put in place through the antimalware scan interface (AMSI) that allows file scans to be requested. The Early Launch AntiMalware (ELAM) feature can also be used by 3rd party security solution providers, provided that their code is signed by Microsoft.²

**Note:** This could also provide an option for attackers to stealing a signing certificate from a trusted editor in order to run signed malware undetected.

ELAM and UEFI that are configured to use Secure Boot make Windows Defender tamper proof.

Microsoft’s large network of partners facilitates threat information exchange, and enterprises can participate in this exchange through sharing the threats detected by Windows Defender real-time protection.

---

# 7. REQUIREMENTS SUMMARY

The base requirement for features presented in this document is Windows 10 Enterprise edition. Some additional requirements might be required for each individual feature.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Guard</td>
<td>• Physical host&lt;br&gt;• x64 architecture&lt;br&gt;• TPM 1.2 or 2.0&lt;br&gt;• UEFI firmware interface (min. 2.3.1)&lt;br&gt;• Intel VT-x or AMD-V&lt;br&gt;• Second Level Address Translation (Intel EPT or AMD RVI)&lt;br&gt;• Intel VT-d (memory attacks through devices)</td>
</tr>
<tr>
<td>Device Guard</td>
<td>• x64 architecture&lt;br&gt;• TPM (optional)&lt;br&gt;• UEFI firmware interface (min. 2.3.1)&lt;br&gt;• Intel VT-x or AMD-V&lt;br&gt;• Second Level Address Translation (Intel EPT or AMD RVI)&lt;br&gt;• Intel TV-d or AMD-V IOMMU (memory attacks through devices)</td>
</tr>
<tr>
<td>Windows Hello</td>
<td>• Compatible camera (infrared or 3D for face recognition)&lt;br&gt;• Compatible mobile phone (iris scan)&lt;br&gt;• Compatible fingerprint reader</td>
</tr>
<tr>
<td>Microsoft Passport</td>
<td>• Windows Server 2016 schema upgrade&lt;br&gt;• Windows Server 2012R2&lt;br&gt;• Windows Server 2016 (key based authentication)&lt;br&gt;• PKI infrastructure (certificate-based authentication)</td>
</tr>
</tbody>
</table>

## ABOUT KUDELSKI SECURITY

Kudelski Security is a premier cybersecurity solutions provider, working with the most security-conscious organizations in Europe and across the United States. Our long-term approach to client partnerships enables us to continuously evaluate their security posture to design and deliver solutions to reduce business risk, maintain compliance and increase overall security effectiveness. For more information about capabilities including consulting, technology, managed security services or custom innovation, visit: www.kudelskisecurity.com

Follow us on LinkedIn [https://www.linkedin.com/company/kudelski-security](https://www.linkedin.com/company/kudelski-security)
Follow us on Twitter [@KudelskiSec](https://twitter.com/KudelskiSec)
Visit our Blog [http://cybermashup.com](http://cybermashup.com)
Visit our Website [https://www.kudelskisecurity.com](https://www.kudelskisecurity.com)

Limitations on Use:

This publication is provided “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This publication could include technical inaccuracies or typographical errors. Kudelski Security reserves the right to make changes to the information herein at any time; these changes may be incorporated in new editions of the publication.

©2016 Kudelski Group / All rights reserved

Kudelski and Kudelski Security are trademarks of Kudelski Group