



# NATIONAL SECURITY AGENCY CYBERSECURITY INFORMATION

## Windows 10 for Enterprises Security Benefits of Timely Adoption

The National Security Agency (NSA) recommends Semi-Annual Channel releases of Windows<sup>®1</sup> 10 Enterprise 64-bit for use on all Windows-based National Security Systems, including the Department of Defense (DoD) and the Defense Industrial Base.

This document describes features present in Windows 10 Enterprise 64-bit that can disrupt exploitation techniques and tools used against National Security Systems today and how the timely adoption of new releases can help to protect systems in the future. The functionality of many of these features has been evaluated through the National Information Assurance Partnership (NIAP)<sup>[1]</sup>.

### Semi-Annual over Long-Term Servicing

Microsoft<sup>®1</sup> provides two servicing options for Windows 10 Enterprise clients<sup>[2]</sup>.

- The **Semi-Annual Channel (SAC)** option includes new or updated features that Microsoft deems ready for broad deployment in each release. With two releases each year, SAC is ideal for most users that require the latest features immediately. NSA recommends SAC for wide adoption on desktop, office automation, and enterprise systems.
- The **Long-Term Servicing Channel (LTSC)** option is Microsoft's model of releasing a major version of Windows every two to three years. Systems using LTSC will receive critical security updates in between releases, but will not receive new security features, architectural security fixes, or feature enhancements until the next OS release. The LTSC release is not recommended

for desktop systems due to the disadvantages of not receiving new security features and architectural fixes.

Historically, each iteration of security updates in the SAC has included a notable increase in the use of Control Flow Guard in the compilation of system files, hardening the system against arbitrary code execution.

SAC releases include major updates to the Credential Guard feature. Windows 10 version 1511 introduced Credential Manager support, and version 1607 includes Virtual Secure Mode and Hyper-V<sup>®1</sup> enabled by default. LTSC maintains an older base version of Credential Guard from mid-2015.

Windows Defender Exploit Guard provides many threat mitigations and improvements to reduce the attack surface of applications by replacing the deprecated Enhanced Mitigation Experience Toolkit (EMET). Microsoft introduced Exploit Guard with Windows 10 version 1709. LTSC does not yet include Exploit Guard.

When 46 public User Account Control (UAC) bypass techniques<sup>[3]</sup> were tested by NSA on two recent versions of Windows, the results showed a 80.43% bypass success rate in Windows 10 version 1507 (LTSC), with only a 36.96% success rate in 1709 (SAC). Using SAC for timely adoption of releases mitigates most additional techniques that are not explicitly patched in Microsoft security updates.

New major features are added with each SAC release, as well as a number of minor security features. Recent examples include:

- Windows Information Protection (WIP) provides a barrier between personal and enterprise data to prevent data leakage.

<sup>1</sup> Windows, Microsoft, and Hyper-V are registered trademarks of Microsoft Corp.

[1] "NIAP Certification of Windows 10" [Online]. Available: <https://www.niap-ccevs.org/Product/CompliantCC.cfm?CCID=2016.1052>

[2] "Windows 10 release information" [Online]. Available: <https://technet.microsoft.com/en-us/windows/release-info.aspx>

[3] "UACME: Defeating Windows User Account Control" [Online]. Available: <https://github.com/hfiref0x/UACME>



- Windows Defender Advanced Threat Protection (ATP) uses cloud heuristics and machine learning to detect and block emerging malware not yet seen.

NSA recommends SAC because this channel provides significant benefits over LTSC by expeditiously providing security features and enhancements.

## 64-bit over 32-bit

Aside from allowing systems to use significantly more physical memory, the 64-bit version of Windows introduces several important security features.

- **Address Space Layout Randomization (ASLR)** uses the larger address space of the 64-bit operating system to mitigate in-memory attack vectors more effectively by positioning system libraries with greater variability.
- **PatchGuard** (Kernel Patch Protection, KPP) halts the system and produces a crash dump if it detects modification of the Windows kernel. PatchGuard is only supported on the 64-bit version of Windows.
- 64-bit Windows enforces mandatory kernel-mode and user-mode **driver signing** which prevents malware from bypassing validation at boot time.
- 64-bit processes use hardware-based **Data Execution Protection (DEP)**. DEP allows Windows to mark areas of memory as non-executable (NX) to help mitigate code injection and buffer overflow attacks.

## Enterprise over Professional

The Enterprise edition of Windows provides advanced capabilities to protect against modern security threats. Many NSA-recommended mitigations require security features that are present only in the Enterprise edition of Windows.

- **AppLocker**<sup>2</sup> provides application whitelisting, which allows for greater administrative control over application execution policy. AppLocker enables logging of application executables,

provides visibility into application inventory, and prevents the execution of common malware.

- **Virtual Secure Mode (VSM)** uses Microsoft's hypervisor (Hyper-V) to isolate critical system services: Kernel Mode Code Integrity (KMCI), Hypervisor Code Integrity (HVCI), and the Local Security Authority Subsystem Service (LSASS)<sup>[4]</sup>. Because the VSM virtual machine is separate from the host operating system (OS), malware cannot tamper with the service or modify its data.
- **Credential Guard** places an isolated version of LSASS in VSM providing a mitigation for some forms of Pass-the-Hash attacks.
- Windows Defender **Application Guard** uses Hyper-V to isolate the Microsoft Edge<sup>®1[5]</sup> web browser from the host while the user browses untrusted sites.
- **Device Guard** prevents untrusted code from executing by ensuring that only trusted, signed code runs after the boot loader. Device Guard moves code integrity mechanisms into VSM, and enforces signing for boot binaries and firmware.

## Windows 10 Enterprise 64-bit Semi-Annual Channel

Microsoft introduced their newest update strategy, Windows as a Service, in Windows 10. With this new approach, Microsoft has increased the pace of incorporating security improvements into the OS.

The 64-bit version of Windows 10 Enterprise Semi-Annual Channel leverages the largest set of security features and improvements offered by Microsoft, making it NSA's recommendation for installation on National Security Systems.

### Disclaimer of Warranties and Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

### Contact Information

Client Requirements or General Cybersecurity Inquiries  
Cybersecurity Requirements Center (CRC), 410-854-4200  
email: [Cybersecurity\\_Requests@nsa.gov](mailto:Cybersecurity_Requests@nsa.gov)

<sup>2</sup> AppLocker and Microsoft Edge are registered trademarks of Microsoft Corp.

[4] "Windows 10 Device Guard and Credential Guard Demystified" [Online]. Available: <https://blogs.technet.microsoft.com/ash/2016/03/02/windows-10-device-guard-and-credential-guard-demystified/>

[5] "Introducing Windows Defender Application Guard for Microsoft Edge" [Online]. Available: <https://blogs.windows.com/msedgedev/2016/09/27/application-guard-microsoft-edge/>