Virtualization Based Security

Virtualization-Based Security, or VBS, is a powerful security feature available in Windows 10 and Windows 11. It leverages virtualization technology to abstract computer processes from the underlying operating system and potentially even hardware. This isolation of processes from one another aims to protect the operating system and the device from malware attacks.

VBS enforces restrictions to safeguard vital operating system resources and security assets such as authenticated user credentials. The technology relies on the hypervisor for virtualization, which creates virtual machines that host system processes and store data instead of performing these tasks on the computer's operating system.

The idea behind VBS is that if a process is attacked, the attack cannot spread outside of the virtual machine. This limits the attacker from exploiting a vulnerability to steal data from another application or the whole computer with ransomware.

VBS can be enabled internally within the device or by using an external third-party solution such as Bromium micro-virtualization. In this case, we will focus on internal VBS integration.

Windows 10 includes VBS as part of the Windows Defender Device Guard and Credential Guard features. These features utilize Virtual Secure Mode (VSM), which runs specific processes and stores data independently of the operating system using Microsoft Hyper-V installed directly on the computer's hardware.

Device Guard ensures that only trusted code and signed, verified firmware can run on the computer. Meanwhile, Credential Guard uses VSM to secure user logins, passwords, and other authentication data to prevent unauthorized access to the machine. By utilizing VBS, Windows 10 provides an extra layer of security to protect against modern threats.

VBS (Virtualization-Based Security) is feature that needs to be enabled manually(Both windows 10 and 11), and there are specific hardware and software requirements that must be met before VBS can be enabled.

To enable VBS, the hardware must support Second Level Address Translation (SLAT), and the operating system must be 64-bit with a compatible processor. Additionally, the device must have a Trusted Platform Module (TPM) version 2.0 or later and have virtualization extensions enabled in the BIOS.

Note that TPM is not a mandatory requirement

Once the hardware and software requirements are met, VBS can be enabled using the Group Policy Editor or the command line. However, it is important to note that enabling VBS may impact device performance, and not all applications may be compatible with VBS. Therefore, it is recommended to test the impact of enabling VBS on a test device before enabling it on a production machine.

[More Resources](https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs)