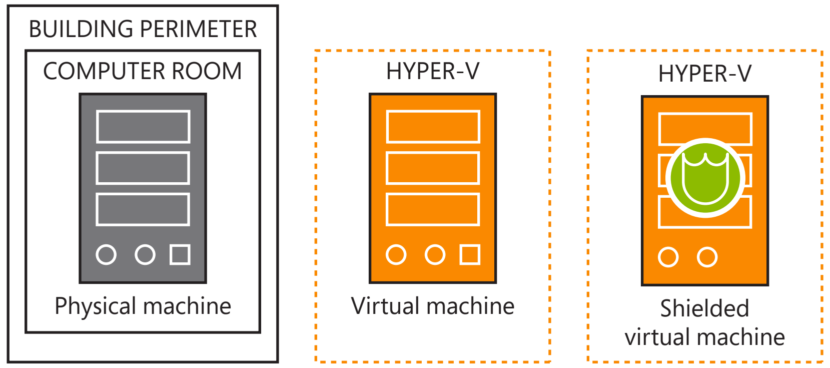
Who has access to the data?



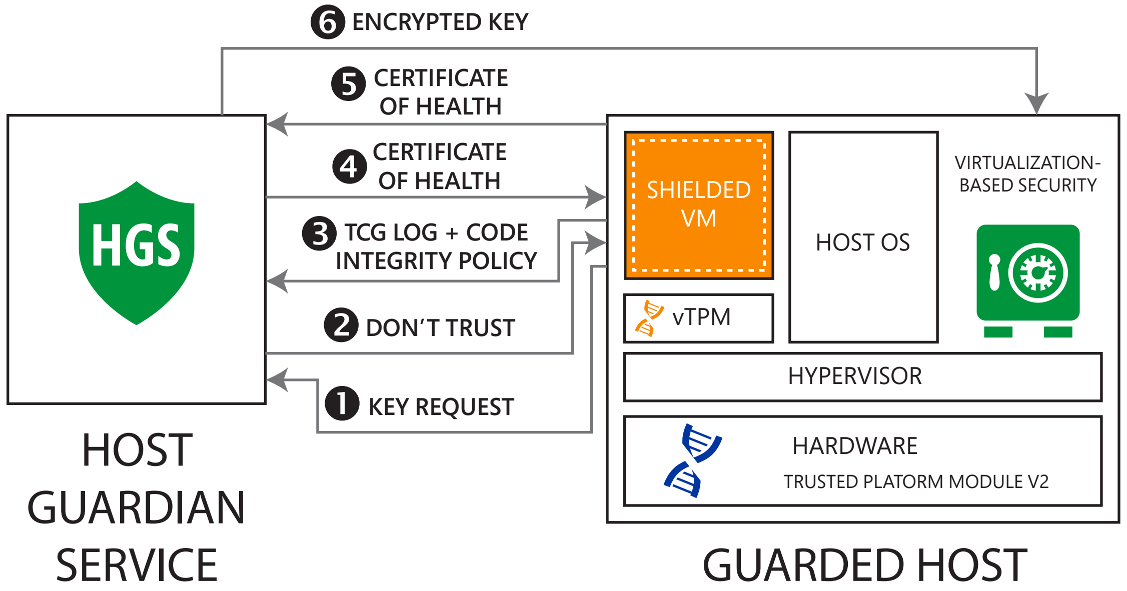
	Physical machine	Virtual machine	Shielded virtual machine
Server administrator	✓	✓	✗*
Storage administrator	✗	✓	✗
Network administrator	✗	✓	✗
Backup operator	✗	✓	✗
Virtualization-host administrator	✗	✓	✗
Virtual machine administrator	✗	✓	✓

*Configuration dependent

Shielded VMs

Windows Server 2016 Hyper-V provides Shielded VMs to protect VM data and state from compromised and malicious fabric administrators. A Shielded VM is a generation 2 VM (supports Windows Server 2012 and on) that has a virtual TPM, is encrypted using BitLocker and can only run on healthy and approved hosts in the fabric.

Shielded Virtual Machine Attestation Process



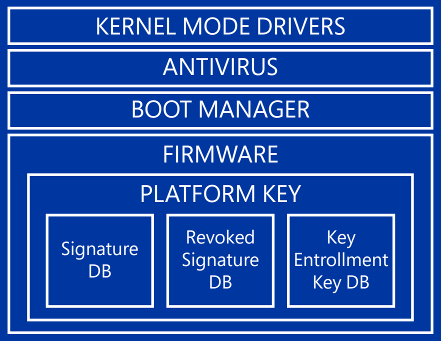
1. The Hyper-V Host sends a key request to the HGS.
2. The HGS replies that it can't verify the Hyper-V host is a legitimate host,
3. The Hyper-V host sends its health and identity information to HGS.
4. The HGS supplies a certificate of health to the Hyper-V host.
5. The Hyper-V host makes the request again with the certificate to the HGS.
6. The HGS sends an encrypted key to the virtualization-based security area of the Hyper-V host.

Guarded Fabric:

Component Parts

To ensure Hyper-V hosts are healthy, multiple components including hardware security features are used to measure the code and state from the moment the machine is powered on.

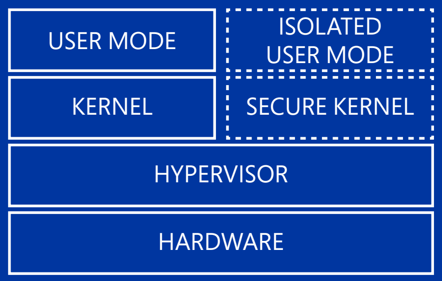
CODE INTEGRITY



KERNEL MODE DRIVERS
ANTIVIRUS
BOOT MANAGER
FIRMWARE
PLATFORM KEY
Signature DB | Revoked Signature DB | Key Entrollment Key DB

Code Integrity uses Virtualization-based Security to ensure that only allowed binaries can be run on the system since the moment the machine is started.

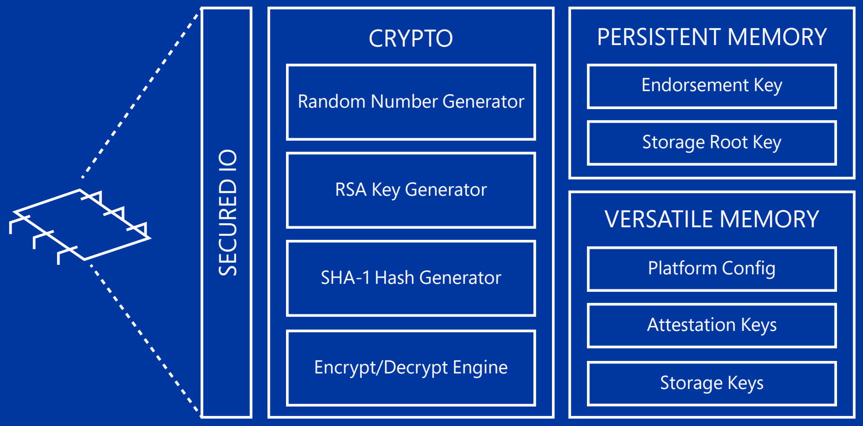
VIRTUALIZATION-BASED SECURITY



USER MODE | ISOLATED USER MODE
KERNEL | SECURE KERNEL
HYPERVISOR
HARDWARE

Virtualization-based Security (VBS) uses hardware security technology to create an area that is isolated from kernel and applications preventing external attacks.

PHYSICAL AND SYNTHETIC TPM V2



SECURED IO

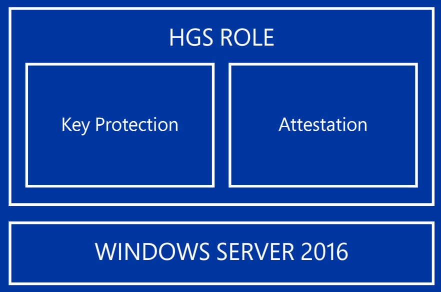
CRYPTO: Random Number Generator; RSA Key Generator; SHA-1 Hash Generator; Encrypt/Decrypt Engine

PERSISTENT MEMORY: Endorsement Key; Storage Root Key

VERSATILE MEMORY: Platform Config; Attestation Keys; Storage Keys

The Trusted Platform Module (TPM) is an international standard for a secure crypto-processor. Windows Server 2016 Hyper-V enables a virtual TPM device for VMs so that they can take advantage of features such as: BitLocker. The virtual TPM does not require a physical TPM to be present.

HOST GUARDIAN SERVICE (HGS)



HGS ROLE: Key Protection | Attestation
WINDOWS SERVER 2016

Host Guardian Service is used to implement a Guarded fabric by providing health attestation for the Hyper-V hosts and key protection for the key material that is required to run Shielded VMs.

Microsoft