Leveraging the New Windows Server 2016 Hyper-V Shielded VM Feature for Compliance with ISO 27001, PCI, and FedRAMP

December 24, 2015

Coalfire Systems, Inc.
www.coalfire.com

TABLE OF CONTENTS

Contents

Introduction

With Windows Server 2016, Microsoft introduces new security features to help protect access to tenant data by enabling encryption of Virtual Machines. While these new features were developed to respond to concerns about how to implement effective security in a cloud environment, there are aspects of these new features that complement any existing compliance requirements a user of Windows Server must adhere to. In this paper, we will discuss an innovative new Hyper-V Virtual Machine (VM) encryption feature of Windows Server 2016 and how this new VM encryption feature can be used to meet compliance and security objectives present in many business or enterprise information systems running Windows Server 2012 and later versions as virtual machines.

In order to help customers navigate this new capability, Microsoft worked closely with Coalfire, a recognized third-party IT compliance firm, to define each security and compliance objective in relation to the capabilities of the Hyper-V Shielded VM feature, and provide an example use case for each compliance and security objective. In addition, Appendix A contains a mapping between these broad security and compliance objectives and the security control requirements present in ISO 27001, PCI DSS, and FedRAMP.

Overview of the Hyper-V Shielded VM Feature

In any discussion of virtualization and information system security, one commonly discussed issue is the addition of a new trust boundary within any virtualized information system: the trust boundary present between the datacenter or virtualization administrator and the customer 'tenant'.

In order to adequately define this new trust boundary, it is important to ensure that administrative functionality and responsibility is appropriately separated from VM tenant functionality and responsibility. In a well-designed virtualized environment, the fabric administrators have access to and responsibility for the underlying physical infrastructure, network and hypervisor management, and any additional components present in the environment virtualization 'fabric'. The fabric administrators should not have access to anything deployed within the VMs themselves. In contrast, the VM owners (e.g.: tenants) have access to and responsibility for the OS and workloads deployed on the VM itself and no visibility into the underlying fabric.

While proper separation between fabric administrator functionality and VM owner functionality is ideal, in practice it becomes hard to implement, as the fabric administrator effectively has access to anything that is in use within the virtualized environment, including the VMs themselves.

In the event of a security breach involving a fabric administrator account or other unauthorized access to physical storage components, administrative network traffic, backup functionality or other components of the virtualization fabric, this inability to segregate tenant VMs effectively means that tenant VMs are implicitly compromised the moment the security breach takes place. This fundamental issue has led to numerous workarounds in highly virtualized environments – certain security sensitive workloads, such as Active Directory Domain Controllers are traditionally left on physical hosts to ensure they can be appropriately protected without granting access to fabric administrators who are not appropriately credentialed.

In response, Windows Server 2016 has a new innovative feature that helps to better protect VM data within the underlying virtualization fabric. Known as Hyper-V Shielded VMs, this feature allows customers using Windows Server 2016 Hyper-V to encrypt any generation 2 VM (Windows Server 2012 and on) so that it is better protected from fabric based attacks.

In order to help protect that the encryption is not compromised by unauthorized access or malicious activity, Windows Server 2016 Hyper-V Shielded VMs introduce a virtualization concept known as the ‘trust plane’. At the heart of the trust plane is a new technology called: “Virtual Secure Mode” (VSM). Windows Server 2016 uses the hypervisor and the underlying physical hardware to create a virtual space that is entirely separate from the rest of the information system. Inside VSM there are only specific binaries that can be run and information that is not accessible to the administrator. Hyper-V uses the VSM ‘trust plane’ to execute and store security critical operations like secure key management as well as VM and hardware integrity verification. All VSM operations are automatically conducted without fabric administrator input or access.

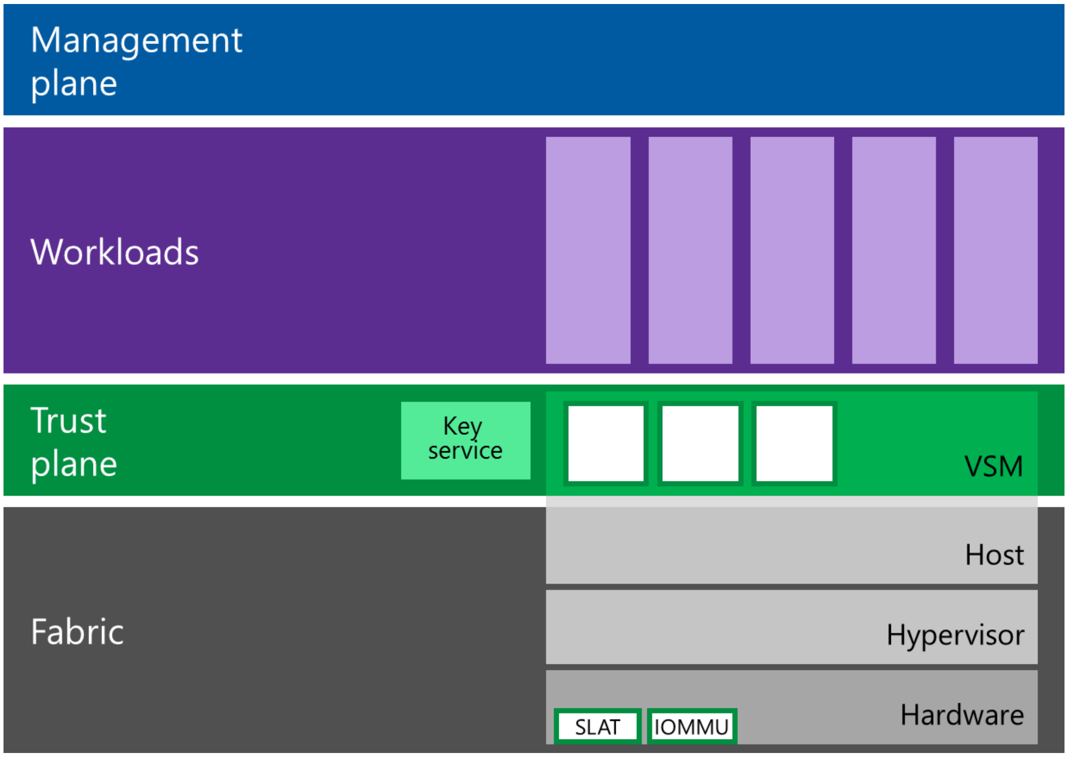

Figure 1 – visual diagram of the ‘trust plane’ concept

With this ‘trust plane’ concept, Windows Server 2016 can employ BitLocker encryption and assurance to better protect live, operational virtual machines and their associated data files and databases from unauthorized fabric administrator access. Hyper-V Shielded VM functionality can be used with VMs running multiple versions of Windows Server, including Windows Server 2012 R2 and Windows Server 2016.

While Shielded VMs are treated just like any other Virtual Machine by the underlying fabric management tools, they provide tenants several important protections that were not previously available in Windows Server:

- First, tenant VM disks can now be encrypted using the Shielded VM feature while at rest and when the VM disks are transmitted on the network.
- Second, Shielded VMs can only executed in a Hyper-V fabric that is deployed on physical hosts that are appropriately configured and verified by remote Trusted Platform Module (TPM) attestation.
- Third, tenant VMs configured as Shielded VMs are no longer implicitly accessible to fabric, storage, network administrators and are hardened (based on configuration) against all malicious host administrator access.

The Hyper-V Shielded VM feature allow Windows Server 2016 Hyper-V customers to achieve a higher level of assurance for all tenant VMs present in their virtualized environment and provides a path forward for Windows Server 2016 customers exploring the virtualization of security sensitive workloads such as Active Directory Domain Controllers.

The Windows Server 2016 team has designed the Hyper-V Shielded VM feature to effectively complement existing customer virtualization fabric architecture; Shielded VMs can be paused, stored, restarted, migrated, backed up, and recovered using the same processes, tools, and operational models already in place for VMs not protected using the Hyper-V Shielded VM feature.

Leveraging Hyper-V Shielded VM Capabilities for Security and Compliance with ISO 27001, PCI, and FedRAMP

In addition to providing customers a powerful and effective way of providing encryption and assurance capabilities for tenant VMs, the new Hyper-V Shielded VM feature can also help Windows Server 2016 customers more effectively meet compliance with several common compliance frameworks. The Windows Server 2016 team has worked to provide customers a good idea of control or requirement applicability for this feature across three common compliance frameworks: ISO 27001, PCI DSS, and FedRAMP.

Although compliance does not directly equate to security, many Windows Server 2016 customers are required to adhere to different compliance standards as part of doing business. This new Windows Server 2016 feature is broadly applicable to numerous different controls within ISO 27001, PCI DSS, and FedRAMP, and provide customers an easier and more efficient way to meet applicable control requirements that are already in place.

The cryptographic protections and integrity assurance provided by the Hyper-V Shielded VMs feature and the underlying VSM technology can help customers navigate several high-priority compliance and security objectives.

Enforcing Separation of Duties

First, the cryptographic protections provided by Hyper-V Shielded VMs can be used to ensure technical enforcement is in place for separation of duties requirements between for customers who are deploying different internal corporate organizations, functions, and business processes in the same virtualized environment.

An example use case for Hyper-V Shielded VMs being deployed to enforce separation of duties requirements within a corporation is as follows: an enterprise deploys Hyper-V Shielded VMs for all internal corporate workloads to ensure that corporate IT fabric administrators will not implicitly have access to sensitive data handled by those workloads, including HR and payroll department workloads that handle personally identifiable information (PII); financial workloads that handle financial data flows; PCI cardholder data environments that process or transmit cardholder data, or developer environments where custom code is under development.

Implementation of Least Privilege Access and Partitioning Tenant Functionality

Second, customers who are using Windows Server 2016 in a service provider hosting environment, Hyper-V Shielded VMs can be used to provide least privilege assurance for tenant workloads that contain tenant data that should not be accessed by service provider fabric administrators.

An example use case for Hyper-V Shielded VMs being deployed to support service provider tenant data protections is as follows: A service provider wants to deploy a Windows Server 2016 based ‘Infrastructure as a Service’ cloud service accessible to their own customer base. In order to provide their tenant customers the highest level of assurance that their data is not accessible to service provider fabric administrators, the service provider deploys all tenant VMs as Shielded VMs to ensure they can attest to applying appropriate configuration to help better protect tenant VM access from the service provider’s staff that is managing the underlying fabric.

Protecting Information Stored in Shared Resources

Third, Hyper-V Shielded VMs provide customers the ability to virtualize security sensitive workloads that are traditionally deployed on physical hosts, such as Active Directory Domain Controllers. Unlike past security-sensitive hypervisor implementations, Shielded VMs provide hardware-based cryptographic assurance that workload VMs are running on designated systems with a known configuration. This cryptographic assurance is then extended through encryption to the VM disks and VM memory. This allows Shielded VMs to provide better assurances normally reserved for implementations of dedicated physical hardware, effectively providing an optional path forward for organizations that are already planning on virtualizing information workloads traditionally confined to heavily restricted environments that require dedicated hardware for operation.

An example use case of this assurance capability is as follows: a project-driven organization which is exploring the use of virtualization but must adhere to extremely specific data protection requirements for certain projects decides to implement Hyper-V Shielded VMs for project workloads. This decision is made to help better protect from IT and fabric administrators accessing project files they are not permitted to access and also allows the organization to save significant cost by virtualizing much of their previously dedicated infrastructure.

Protection of Data at Rest

Fourth, Hyper-V Shielded VMs provide customers the ability to deploy natively encrypted tenant VMs that can be dynamically provisioned without any additional configuration. This capability allows service providers and their tenants to better meet security and compliance requirements that mandate the cryptographic protection of data at rest.

An example use case is an organization that must adhere to cryptographic requirements concerning payment cardholder data but has limited overhead to ensure appropriate operation and maintenance of their cardholder data environment and storage of cardholder data. To ensure administrators have one less compliance requirement to worry about, the organization deploys Shielded VMs for the entire cardholder data environment to provide complete cryptographic coverage with no additional configuration.

Security Function Verification and Host Integrity Monitoring

Finally, Hyper-V Shielded VMs and the underlying VSM technology provide customers with robust built-in verification of the fabric integrity, and validity of the underlying physical hardware components the fabric is deployed on. Prior to provisioning or starting up a Shielded VM, Hyper-V and related Windows Server technologies work to check the integrity and overall health of the underlying physical host prior to allowing the Shielded VM to begin operation. This verification incorporates hardware-based TPM assurance. These protections ensure Hyper-V will not launch a Shielded VM on a physical host that has not been properly configured to provide appropriate protections for the overlaid virtualization fabric.

Appendix A: Hyper-V Shielded VM Compliance Mapping to ISO 27001, PCI, and FedRAMP

Hyper-V Shielded VM Security and Compliance Capability	ISO 27001: 2013	PCI DSS 3.1	FedRAMP; NIST 800-53 Revision 4
Enforcing Separation of Duties	A.6.1.2– Segregation of duties	6.4.2 – Separation of duties between test and production environments	AC-5 – Separation of Duties
Implementation of Least Privilege Access and Partitioning Tenant Functionality	A.9.2.3 – Management of privileged access rights A.12.1.4 – Separation of development, testing, and operational environments	6.4.1 – Test and Production Environment Separation 7.2 – User access control on need-to-know basis 7.2.3 – Default “deny-all” setting	AC-6 – Least Privilege AC-6 (10) – Prohibit Non-Privileged Users from Executing Privileged Functions SC-2 – Application Partitioning
Protecting Information Stored in Shared Resources	None	8.7 – Restricted access to databases containing cardholder data	SC-4 – Information in Shared Resources
Protection of Data at Rest	A.8.2.3 – Media Access	3.4 – Verifying stored PAN is unreadable 3.4.1 – Disk encryption usage and access control 6.5.3 – Insecure cryptographic storage	SC-28 – Protection of Information at Rest SC-28(1) – Protection of Information at Rest
Security Function Verification and Integrity Monitoring	None	11.5 – Change-detection mechanism deployment	SI-6 – Security Function Verification SI-7 – Software, Firmware, and Information Integrity