# Entrust enhances security of VMs deployed within Microsoft Windows Server 2016

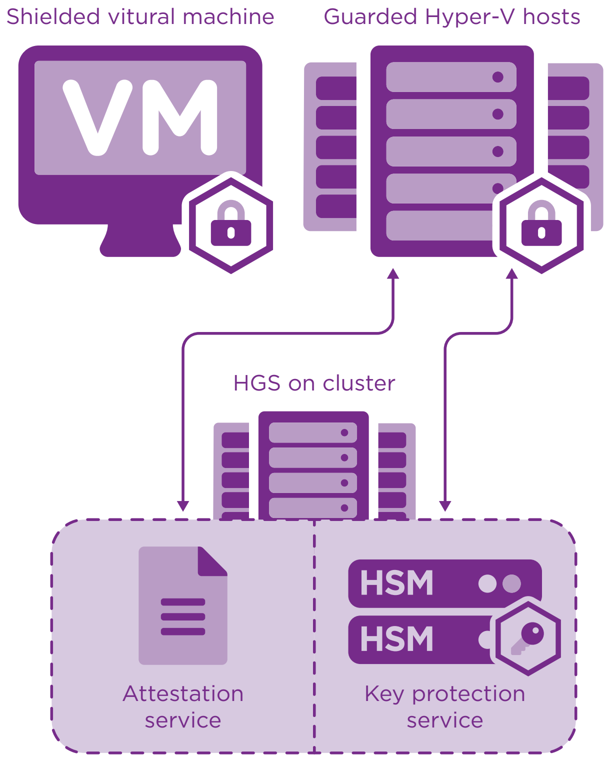
Provide hardware protection for the encryption keys used to secure virtual machines

**HIGHLIGHTS**

- Protect virtual machines (VMs) from compromised hosts and rogue administrators
- Offer strong separation between computing environment and sensitive workloads
- Attest that host infrastructure is qualified to run VMs
- Enhance control and security of VMs running in the cloud
- Provide a certified root of trust for regulatory compliance

## The problem: widespread use of VMs running sensitive workloads are at risk of compromise from internal and external threats

VMs are only as secure as the access controls set by the administrators that manage them. The more administrators having access to the virtual environment, the greater the risk of accidental and deliberate exposure of access credentials and sensitive data such as personally identifiable information (PII) and transactions. Mitigating the risks of potential attacks is therefore of paramount importance.



Entrust nShield® hardware security modules (HSMs) integrate with the Host Guardian Server (HGS) to protect the private key needed to decrypt sensitive workloads and their data.

LEARN MORE AT ENTRUST.COM/HSM

# Entrust enhances security of VMs deployed within Microsoft Windows Server 2016

## The challenge: securing VMs and reducing the potential risks introduced by compromised hosts and rogue administrators

One of the most important goals of a hosted environment is to guarantee the security of all its VMs. The use of a guarded fabric with an attestation service can ensure that only known and healthy hosts can run critical VMs. To mitigate the potential risks of attack that could be carried out by rogue administrators managing the release of keys that control access to different workloads, automated processes must be put in place in a manner that does not affect operational performance.

## The solution: Windows Server 2016 Hyper-V Shielded VM and Entrust nShield HSMs to protect sensitive VM workloads

Part of the Windows Server 2016 Hyper-V, Shielded VM is a native option that encrypts estates of VMs in data centers. Available for on-premises and cloud-based deployments, Shielded VM enables the creation of a guarded fabric that provides a more secure environment for VMs. The guarded fabric comprises one HGS – typically a cluster of 3 nodes, one or more Guarded Hosts, and a set of Shielded VMs. Shielded VM uses a virtual trusted platform module encrypted with BitLocker, and can only run on healthy and approved hosts in the fabric. The HGS uses a cryptographic process to attest to the health of a guarded host and its VMs, and to unlock and run the VMs on positively attested guarded hosts.

Shielded VM integrates with nShield® Connect HSMs to establish a hardware root of trust for the safekeeping and the management of attestation and encryption keys required for protecting sensitive VM workloads and their data. nShield HSMs protect the private key used by the HGS.

## Why use Entrust nShield HSMs with Microsoft HGS shielded VM?

Entrust nShield HSMs enhance the security posture of a Shielded VM deployment in a way that auditors can quickly recognize; notably the nShield HSMs are validated by NIST to meet FIPS 140-2 Level 3 and Common Criteria EAL4+. Acting as a root of trust, nShield HSMs integrate with the HGS to provide enhanced logical and physical protection of private keys. The combination delivers an auditable method for enforcing security policies, enabling customers to:

- Secure keys within carefully designed cryptographic boundary that use robust access control mechanisms, so keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed by the HGS
- Deliver superior performance to support demanding applications

# Entrust enhances security of VMs deployed within Microsoft Windows Server 2016

nShield HSMs provide a hardened environment for performing secure cryptographic processing, key protection, and key management. nShield HSMs:

- Provide a tightly controlled tamper resistant environment for safekeeping and managing encryption keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, CNG) and native APIs web services in conjunction with Web Services Option Pack

## Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

Microsoft strives to produce innovative products and services that meet customers' evolving needs. Entrust nShield HSMs are certified to support a wide range of Microsoft security solutions and deliver the industry's most operationally efficient key management framework. Entrust enables Microsoft customers to utilize cryptographic security to enhance their business as well as satisfy evolving compliance requirements, facilitating the secure adoption of new technologies. Entrust is a Gold Certified Microsoft partner.

**www.microsoft.com**

Gold Microsoft Partner Microsoft

## Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about Entrust nShield HSMs

**HSMinfo@entrust.com**

**entrust.com/HSM**

## ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
**entrust.com/HSM**

ENTRUST

**Contact us:**
**HSMinfo@entrust.com**