



ENTRUST



Entrust KeyControl Vault for VM Encryption

Data encryption, multi-cloud key management, and workload security

HIGHLIGHTS

- Complete workload lifecycle encryption management
- Enterprise Key Management Server (KMS)
- Strong and granular virtual machine (VM) encryption: live boot (OS) and data partition encryption
- Access controls for separation of duties among administrators
- Seamless integration with Entrust nShield® HSMs for FIPS 140-2 Level 3 certified root of trust

Managing keys for encrypted workloads can get complex

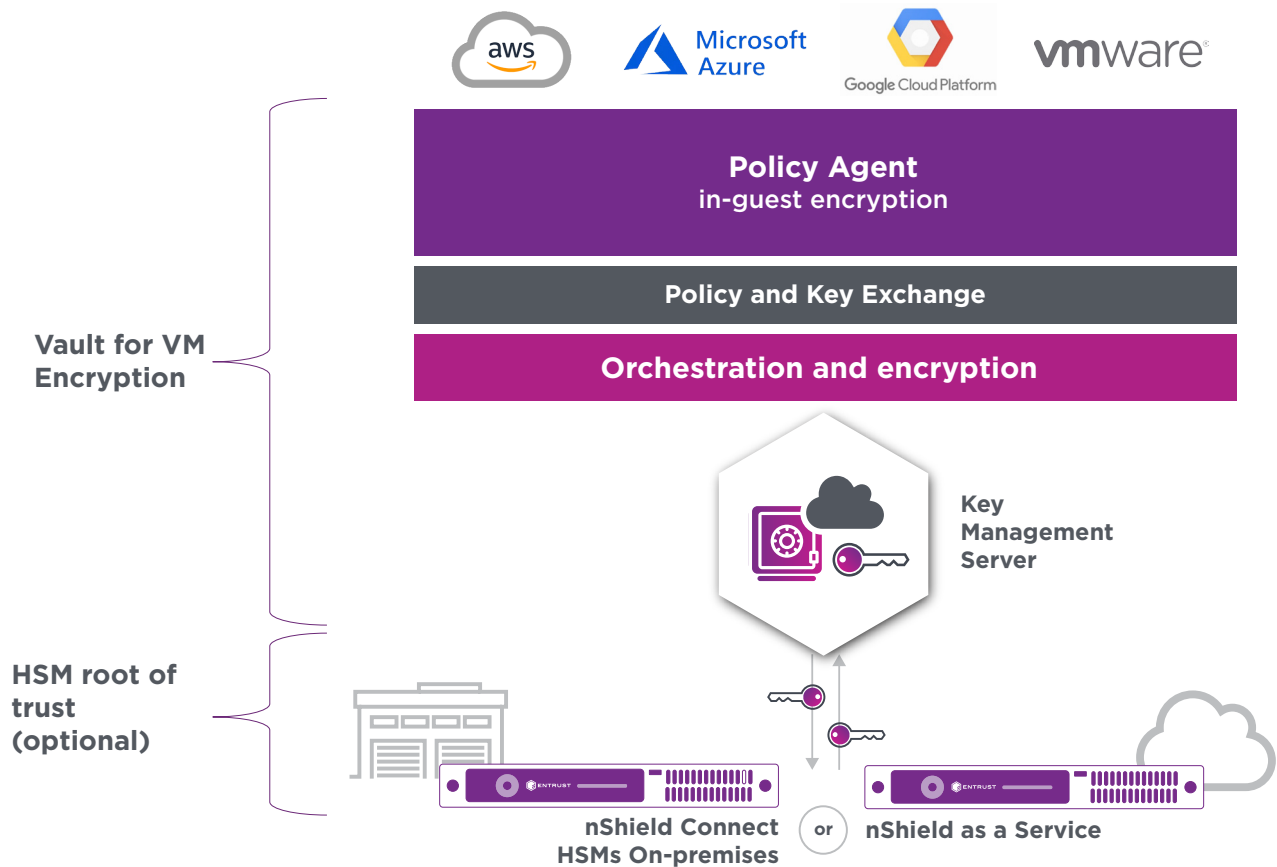
Workloads go through many lifecycles, from staging to deployment to backup and eventual decommissioning. Each stage poses different risks of potential data theft or other misuse.

Workload encryption is not a deploy once and forget operation

It is critical to frequently rotate data encryption keys. Managing workload encryption from each cloud vendor's platform is complex and increases the risk of inconsistent policies and human mistakes. Built-in key management policy reduces complexity and ensures consistency.

Entrust KeyControl Vault for VM Encryption provides encryption and key management for virtual machines located in data centers and private, public, or hybrid cloud environments secures multi-cloud workloads throughout their lifecycle and reduces the complexity of protecting workloads across multiple cloud platforms. This provides greater protection of your organization's critical and sensitive information while enabling compliance with data privacy regulations.

Entrust KeyControl Vault for VM Encryption



Policy Agent features:

- Full encrypted path from the VM, through the hypervisor to the storage.
- Support for cloning and replication.
- Dynamic rekey on Windows and Linux
- Filesystem resize for encrypted devices
- Support for Amazon S3 storage
- Linux file-level and folder-level encryption
- Migration of encrypted disks between VMs in the same Cloud VM Set.
- Support for Windows failover clusters.
- Root and swap encryption for Linux and boot drive (C:) encryption for Windows.

Deployment platform support

- CentOS
- Red Hat Enterprise Linux
- Ubuntu
- SUSE Linux Enterprise Server
- AWS Linux
- Windows Server Core 2012 R2, 2016, and 2019
- Windows Server 2012, 2012 R2, 2016, 2019, and 2022
- Windows 8.1 and 10

Deployment media

- ISO
- OVA (Open Virtual Appliance)
- Amazon Machine Image (AMI) available via Amazon marketplace
- Virtual Hard Disk (VHD) available via Microsoft Azure marketplace



Entrust KeyControl Vault for VM Encryption

KEY FEATURES & BENEFITS

Managing encrypted workloads in a multi-cloud infrastructure

KeyControl allows you to manage your encrypted workloads across different infrastructures, including on-premises and with the leading public cloud platforms. With KeyControl, you get a centralized and scalable solution to control all your encryption keys.

Deep workload protection

KeyControl provides granular encryption for better security. The protection boundary does not stop at the hypervisor or at the data store; VMs are individually encrypted. Inside the VM, unique keys can be assigned to encrypt each partition, including the boot (OS) disk and swap partitions.

Easy to deploy and manage

KeyControl provides deployment flexibility with a single interface for all workload encryption, which eliminates the complexity of using each platform's own encryption feature separately.

- Superior user experience
- Zero downtime encryption
- High-availability clustering ensures disaster recovery capabilities

Access controls

KeyControl allows for robust policy-based access controls to enforce separation of duties across different user personas. Prevent root users or system administrators from accessing sensitive data by enforcing access controls on encrypted volumes.

Deduplication support

Previously, the concern existed that encryption and deduplication could not co-exist, given that encrypting data makes every block different. KeyControl's unique approach offers AES 256-bit encryption while maintaining 91% of storage deduplication benefit.

Platform support

- **Private cloud platforms:**
 - vSphere
 - OVHCloud
 - VxRail
 - Quantum
 - NetApp
 - Nutanix
- **Public cloud platforms:**
 - Amazon Web Services (AWS)
 - IBM Cloud
 - Microsoft Azure
 - VMware Cloud (VMC) on AWS
 - Google Cloud Platform (GCP)
- **Hypervisor support:**
 - ESXi
 - AWS
 - Azure
 - KVM
 - GCP

Entrust KeyControl Vault for VM Encryption

Technical specifications

- Encrypt boot (OS), swap, and data partitions
- Support for encrypting Windows GPT boot drives, including UEFI Secure Boot drives
- Individual keys per partition
- Strong AES (128/256 bit) encryption with Intel hardware acceleration support
- Seamless integration with Entrust nShield FIPS 140-2 Level 3 hardware security modules
- Zero downtime encryption with automatic re-keying
- Dynamic partition resizing for Windows VMs
- High-availability (HA) support with active-active cluster (up to 8 KMS servers per cluster)
- Single encryption key for deduplication support
- Certified for VMware vSphere and vSAN encryption
- REST-based API integration for DevOps
- Protect encrypted workloads against unauthorized access with boot and clone protection

KeyControl

Enterprise Key Lifecycle Management & Compliance Platform

KeyControl Compliance Manager

Global Compliance Dashboard - Policy Enforcement - Granular Key Inventory - Audit/Risk

KEYCONTROL VAULTS & USE CASES

Vault for KMIP <ul style="list-style-type: none">Database ProtectionVirtual Machine ProtectionData SecurityStorage Protection	Vault for Databases - TDE <ul style="list-style-type: none">Database Protection	Vault for Secrets Management <ul style="list-style-type: none">Secrets ManagementSSH Key ManagementPrivileged Account & Session Management	Vault for Tokenization <ul style="list-style-type: none">123-456XXX-XXXData TokenizationData Encryption	Vault for VM Encryption <ul style="list-style-type: none">Agent-Based VM Encryption	Vault for Cloud Key Management <ul style="list-style-type: none">BYOKHYOK
---	--	---	---	--	---

Entrust KeyControl Vault for VM Encryption is part of a suite of products designed to manage key and secret lifecycles at scale for encrypted workloads in virtualized environments across on-premises, multi-cloud, and hybrid deployments.

For more details on the KeyControl platform, KeyControl Compliance Manager, and the range of vaults download the Entrust KeyControl Solution Brochure.

Learn more at [entrust.com](https://www.entrust.com)



Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223