PRODUCT BRIEF

Dell EMC CloudLink®: Key Management and Encryption for Private, Public, and Hybrid Clouds

Contents

- Virtual machine encryption
- KMIP-compliant key management
- A new approach to cloud encryption
- Confidently secure machine images and sensitive data

CloudLink highlights

- Virtual machine boot and data volume encryption with pre-boot authorization
- Provides infrastructure-level data-at-rest encryption of Dell EMC ScaleIO devices
- CloudLink Center provides Key Management Interoperability Protocol (KMIP) integration with KMIP-compatible encryption clients
- Certified VMware Ready™ Key Management Server
- Verifies the integrity of your VMs, securing against unauthorized modifications
- Geo-fencing capabilities ensure VMs may only boot and run in trusted locations
- Easy-to-deploy CloudLink Center virtual appliance manages encryption keys and security policy
- Provides a single administration interface for monitoring and controlling security across private, hybrid, and multiple public clouds

Modern enterprises are seeking to embrace the hybrid cloud model to leverage shared infrastructure in private data centers and realize the significant benefits offered by public cloud environments for deployment flexibility, infrastructure scalability, and cost-effective resource use.

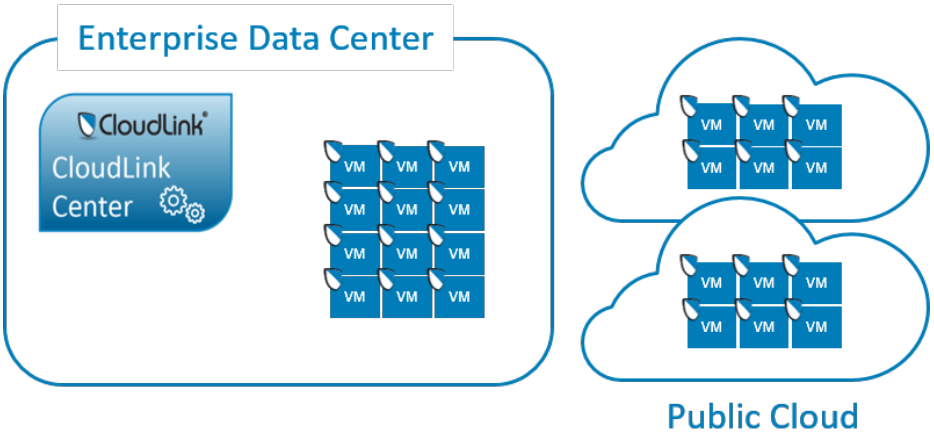
Cloud computing is based on a shared, multi-tenant, and software-defined compute, network, and storage architecture. Data owners are responsible for securing sensitive data across public and private clouds, but traditional security controls no longer apply. New solutions must address privacy, regulatory, and data remanence (residual data) requirements. They must also provide the flexibility to support various encryption approaches for diverse use cases.

Storage infrastructure-level encryption provides a convenient way to secure data in the private data center that is completely transparent to the applications deployed on the physical and virtual infrastructures that consume the storage.

Virtual machine-level encryption offers an infrastructure-agnostic approach that is portable across private and public clouds and keeps VMs secure during the migration process.

Vital to these approaches is external, policy-based key management that ensures encryption keys, and therefore sensitive data, are controlled by the data owner.

CloudLink provides policy-based key management, and supports multiple data at rest encryption options for virtual machines across a broad spectrum of cloud platforms.



CloudLink highlights

- CloudLink Center provides a complete set of REST APIs
- Flexible, full lifecycle key management, whether on-premises or in the cloud
- FIPS 140-2 certified encryption and key management
- Support for HSMs and Azure Key Vault for high assurance key generation and storage
- Lightweight CloudLink SecureVM Agent can be deployed in seconds
- Supports a broad range of public and private cloud platforms, including VMware® vSphere™, VMware vCloud Air™, Microsoft® Hyper-V®, Microsoft Azure™ and Amazon Web Services

CloudLink benefits

- Leverages trusted and familiar OS encryption tools for complete application transparency, highest performance, and confidence that future OS versions are supported
- Gives you complete and independent control of your data in public clouds and shared infrastructure
- Multiple VM-level and ScaleIO device encryption options allow you to choose the most appropriate data at rest encryption solution to meet your requirements
- Simple, easily automated deployment in new or existing applications without re-architecture
- Boot volume encryption protects against data leakage from swap, configuration, and temporary files
- Broad cloud support frees you from cloud lock-in, addresses data remanence, and lets you select environments that best meet your applications' needs

Virtual machine encryption

CloudLink SecureVM allows you to control, monitor, and secure your Windows and Linux VMs—whether they are servers or desktops—everywhere in your hybrid cloud.

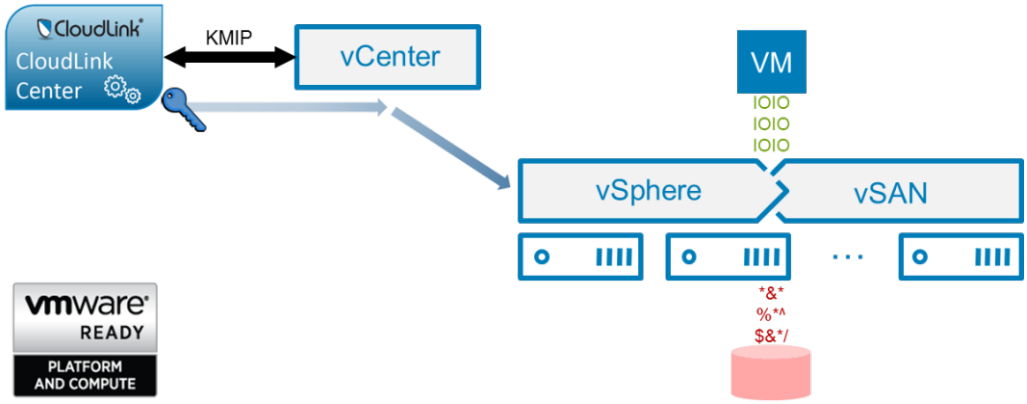
Encryption of VMs' volumes means you can protect access to your VMs and sensitive data in the cloud by implementing your own data segmentation and isolation controls.

You also define the security policy that must be met for a VM to boot, including geo-fencing to address data sovereignty requirements and VM integrity to secure against tampering. CloudLink SecureVM ensures that only trusted and verified VMs have the ability to run and access sensitive data.

KMIP-compliant key management

CloudLink is a KMIP-compliant key management server (KMS), which allows it to manage keys for various encryption end-points.

New VMware encryption technologies, including VMware vSphere encryption which provides VM-level encryption, as well as VMware vSAN encryption which provides software-defined storage level encryption, both require the use of an external KMIP-compliant server.



CloudLink is a certified VMware Ready™ KMS, giving VMware customers complete flexibility for their data encryption needs. You can benefit from the ease of configuring encryption at the hypervisor level for native VMware environments or use CloudLink SecureVM to give you granular control of your VMs and data as they sit in VMware environments and/or hybrid and multi-cloud environments comprised of heterogeneous virtualization platforms.

A new approach to cloud encryption

CloudLink uses native OS encryption to encrypt VMs. This approach provides the assurance of trusted, proven encryption to achieve complete application and OS transparency. While delivering best in-class performance, using native encryption also avoids the risks associated with proprietary encryption tools.

On Windows machines, CloudLink uses Microsoft BitLocker. CloudLink extends BitLocker functionality with policy-based key management and orchestration, allowing the use of BitLocker for automated encryption of boot and data volumes while giving control of security policy and encryption keys to enterprise administrators. On Linux machines, CloudLink uses encryption packages included in the Linux kernel to secure the root partition and specified devices.

Confidently secure machine images and sensitive data

CloudLink SecureVM provides the security controls necessary to move forward with server and desktop cloud initiatives. CloudLink SecureVM extends security protection beyond data to the virtual machine itself. This security protection is particularly important for Windows applications that may save sensitive data to an OS volume via swap or temporary files. It is common for configuration files stored on the OS volume to contain sensitive information, including account credentials for connecting to databases, other types of servers, or applications. It is critical to control and secure access to data on the OS volume.

You must also consider risks to gold master images and powered-off VMs. Checking the integrity of VMs before launch to detect unauthorized changes, and sending alerts when appropriate, is increasingly important as the scale of cloud deployments grows.

CloudLink SecureVM gives you independent control of your sensitive data and cloud workloads. Its flexibility and simplicity allows you to embrace the cloud and secure your data with confidence.

Contact us

To learn more, contact your local representative or authorized reseller.

Authors: Tim Bramble, Brian Coe.