PRODUCT BRIEF

CloudLink SecureVM for the Hybrid Cloud

CloudLink® SecureVM highlights

- Virtual machine boot and data volume encryption with pre-boot authorization
- Leverages trusted and familiar OS encryption, including Microsoft BitLocker
- Verifies the integrity of your VMs, securing against unauthorized modifications
- Provides a single administration interface for monitoring and controlling security across private, hybrid and multiple public clouds
- Provides full key lifecycle management
- Supports existing tools like Azure Key Vault, Microsoft® Active Directory and Amazon S3 for key storage
- Easy-to-deploy CloudLink Center virtual appliance manages encryption keys and security policy
- Lightweight CloudLink SecureVM Agent can be deployed automatically using Microsoft Group Policy or scripting
- Supports a broad range of Windows and Linux instances across various cloud platforms, including VMware® vCloud Air™, Microsoft Azure™ and Amazon Web Services®

Today's enterprises are looking to move workloads to the cloud to leverage significant benefits for deployment flexibility, infrastructure scalability, and cost-effective use of resources. However, they must overcome significant cloud computing challenges.

Cloud computing is based on a shared, multi-tenant compute, network and storage architecture. Data owners are responsible for securing sensitive data across both public and private clouds, and 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.

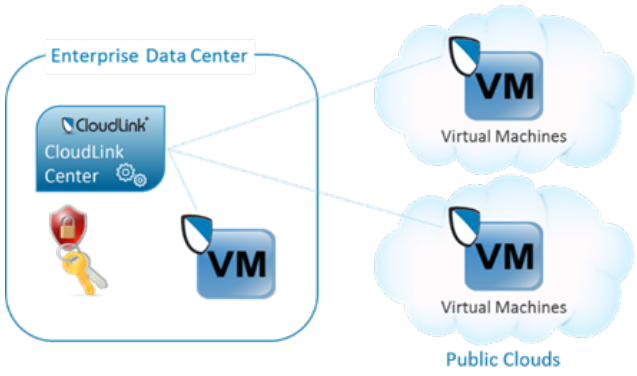
In addition to challenges of securing sensitive data in the cloud, there's a growing concern about securing virtual machine images themselves against malicious or accidental tampering. CloudLink® SecureVM not only secures sensitive data in the hybrid cloud, but protects the integrity of the VM itself against unauthorized modifications. SecureVM operates independently from the infrastructure of your cloud service provider, giving you the freedom to apply encryption when and where it's best suited for you.

VIRTUAL MACHINE ENCRYPTION FOR THE HYBRID CLOUD

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

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 verifying the VM integrity, to secure against malicious tampering. SecureVM ensures that only trusted and verified VMs have the ability to run and access sensitive data in the cloud.



REDEFINE

EMC²

SecureVM Benefits

- Leverages proven OS encryption tools for complete application transparency, highest performance and confidence that future OS versions will be supported
- Simple deployment in new or existing applications without re-architecture that can be automated easily to scale as required
- Boot volume encryption protects against data leakage through swap, configuration and temporary files
- VM integrity verification guards against malicious tampering
- Integrates with existing tools allowing you to store and manage keys where and how you like
- Broad cloud support frees you from cloud lock-in, addresses data remanence, and lets you select environments that best meet your applications' needs
- Gives you complete and independent control of your data in public clouds and shared infrastructure

A NEW APPROACH TO CLOUD ENCRYPTION

SecureVM works together with native OS encryption. This approach provides the assurance of using trusted, proven encryption to achieve complete application and OS transparency. While providing best in-class performance, using native encryption also avoids the risks associated with proprietary encryption tools.

On Windows VMs, SecureVM uses Microsoft BitLocker technology, a proven and high-performance volume encryption solution widely implemented for physical machines. SecureVM extends BitLocker functionality as its native authentication mechanisms are not supported in cloud environments. SecureVM's proven policy-based encryption key management allows use of BitLocker for automated encryption of boot and data volumes in the cloud while giving control of security policy and encryption keys to enterprise administrators. On Linux VMs, SecureVM uses encryption packages included in the Linux kernel to provide encryption of the root partition encryption and specified mount points.

SecureVM is perfect for hybrid cloud deployments, securing VMs wherever they reside and allowing storage and management of their keys within the private cloud (the enterprise datacenter).

CONFIDENTLY SECURE MACHINE IMAGES AND SENSITIVE DATA

SecureVM provides the security controls necessary to move forward with server and desktop cloud initiatives. SecureVM extends security protection beyond data to the virtual machine itself. This security protection is particularly important for Windows applications that may leak sensitive data to an OS volume via swap or temporary files. It's 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's 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.

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

07/2015 Product Brief
H14453

REDEFINE

Product Brief

EMC²