PRODUCT BRIEF

EMC CloudLink® SecureVM: Key Management and Encryption for Hybrid Clouds

CLOUDLINK HIGHLIGHTS

- Virtual machine boot and data volume encryption with pre-boot authorization
- Provides infrastructure-level data-at-rest encryption of EMC ScaleIO devices
- Verifies the integrity of your VMs, securing against unauthorized modifications
- 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
- CloudLink Center provides a complete set of REST APIs
- Flexible, full lifecycle key management, whether on-premises or in the cloud
- 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

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

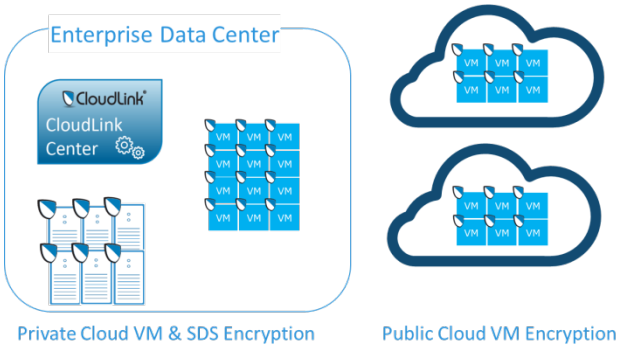
Cloud computing is based on a shared compute and a shared, multi-tenant, software-defined network and storage architecture. Data owners are responsible for securing sensitive data across public and private clouds, but traditional security controls no longer apply. New solutions must address privacy, 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 datacenter 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 while allowing VMs to remain secure during and after the migration process.

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

CloudLink provides policy-based key management and data at rest encryption for both virtual machines and EMC ScaleIO devices.



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

CLOUDLINK BENEFITS

- Leverages trusted and familiar OS encryption tools for complete application transparency, highest performance, and confidence that future OS versions will be supported
- Gives you complete and independent control of your data in public clouds and shared infrastructure
- VM and ScaleIO device encryption options allow you to choose the most appropriate data at rest solution to meet your requirements
- Simple, easily automated deployment in new or existing applications without re-architecture
- Boot volume encryption protects against data leakage through 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

CONTACT US

To learn how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller

SCALEIO DATA SERVER DEVICE ENCRYPTION

CloudLink also provides infrastructure-level encryption, allowing you to secure ScaleIO Data Server (SDS) devices. Because CloudLink operates directly on SDS devices, it provides data at rest encryption that is completely transparent to applications with sensitive data. Agents need not be deployed at the application layer as all data written to the SDS devices is fully encrypted.

Since encryption is done at the final stage before data is written to the SDS devices there is no impact to ScaleIO features, which ensures that you can still take advantage of ScaleIO's enterprise grade protection and resiliency.

A NEW APPROACH TO CLOUD ENCRYPTION

CloudLink 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 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 leak 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 hybrid cloud and secure your data with confidence.

06/2016 Product Brief
H14453.1