CloudLink® SecureVSA
SOFTWARE DEFINED STORAGE ENCRYPTION FOR THE HYBRID CLOUD

Cloud computing offers undeniable benefits for deployment flexibility, infrastructure scalability, and cost-effective use of resources. It makes sense to take advantage of these benefits and deploy enterprise workloads in the cloud. However, cloud computing is based on a shared, multi-tenant compute, network and storage architecture where traditional security controls no longer apply. As a result, concerns over cloud security, manageability, performance, and reliability have been the biggest barriers to the more rapid and wide-spread adoption of cloud services. Many organizations moving to the cloud require a data-at-rest security solution that is simple to deploy and allows them to control encryption policy and keys independent of any service provider intervention. As projects evolve, cloud encryption must span workloads distributed across both public and private clouds, and also provide the flexibility to support a variety of encryption approaches to address the unique needs of varied use cases.

CloudLink® SecureVSA delivers FIPS 140-2 validated virtual storage encryption without requiring deployments of software agents or workload changes. This approach dramatically simplifies security management across private, hybrid, and multi-cloud environments. For medium to large enterprises, SecureVSA offers significant cost savings and flexibility.

SOFTWARE-DEFINED STORAGE ENCRYPTION FOR THE HYBRID CLOUD

SecureVSA is installed as a virtual appliance in hybrid clouds to secure virtual resource pools – virtual machines (VM), networks, and data stores – in multi-tenant environments. SecureVSA integrates seamlessly with virtualization and cloud infrastructures, and can be set up as a cloud service template, making it easy for you to order and self-provision. SecureVSA is suitable for Amazon AWS, Microsoft Azure, and VMware vCloud Hybrid Service, as well as any IaaS clouds based on VMware vSphere or vCloud Director and Microsoft Hyper-V. You can choose the cloud service provider best suited for your requirements. SecureVSA is completely transparent to end-users.

SecureVSA provides:

- Enterprise-controlled security. All network communication and storage data are encrypted with the data owner having full control over keys and security policy. You can manage keys in the CloudLink Center or, for the highest level of key protection, with RSA Data Protection Manager as a key store.

- Ease of deployment and use. SecureVSA delivers FIPS 140-2 compliant encryption while requiring no changes to the workloads making use of its secure storage and networking.

Encryption of data-at-rest and data-in-motion. In addition to encrypting data-at-rest, SecureVSA secures data moving between a data center in the enterprise and a virtual data center in the cloud.

HIGHLIGHTS

For the enterprise:

- Secure storage for virtualized and cloud workloads

- Simple to deploy, agentless solution

- Enterprise-controlled encryption

- Secure both data-at-rest and data-in-motion

- Secure back-up and disaster recovery to the cloud

- Integrates with CloudLink Platform, which provides data encryption and management to protect mission-critical information:

- Single pane of glass to deploy and manage data

- Modular and granular approach to encryption for maximum flexibility and scalability: storage, VM, file, or application

For the Cloud Service Provider:

- Addition of encryption services to cloud service portfolio for broader customer appeal

- Expansion of potential customer base by enabling hosting of workloads subject to regulatory compliance

- Cost reduction through secure coexistence of multiple tenants on a single host/storage array

SecureVSA
## SOFTWARE DEFINED STORAGE ENCRYPTION FOR THE HYBRID CLOUD

CLOUDLINK SecureVSA ARCHITECTURE

CloudLink SecureVSA is a storage infrastructure-level data at rest encryption solution for virtual and cloud environments. SecureVSA supports two implementation modes – encrypted datastore mode and encrypted NAS mode. In encrypted datastore mode, SecureVSA is providing encrypted storage for hypervisor use (VMware vSphere and Microsoft Hyper-V).

In datastore mode, virtual machines (VM) associated with the encrypted datastore can be thought of as running within an encrypted 'container'.   The VMDK files associated with the VM reside within encrypted storage. The entire VM can reside within the encrypted datastore or administrators can specify that just the data volumes be placed in the encrypted datastore. The benefit of this approach is that it is agentless and therefore completely transparent to virtualized servers and their applications. It also offers the benefits of supporting standard VMware features such as DRS, HA and FT.

In encrypted NAS mode, SecureVSA provides encrypted file shares at the network level for servers and end users. Encrypted NAS mode is also an agentless data at rest encryption solution with the encryption being completely transparent to the server and application attaching or mapping to the network attached storage.

SecureVSA can be used to encrypt large amounts of storage. It provides the ability for administrators to combine or aggregate virtual volumes assigned to it into a single encrypted volume. Alternatively each attached volume can be encrypted with unique encryption keys and be presented individually.
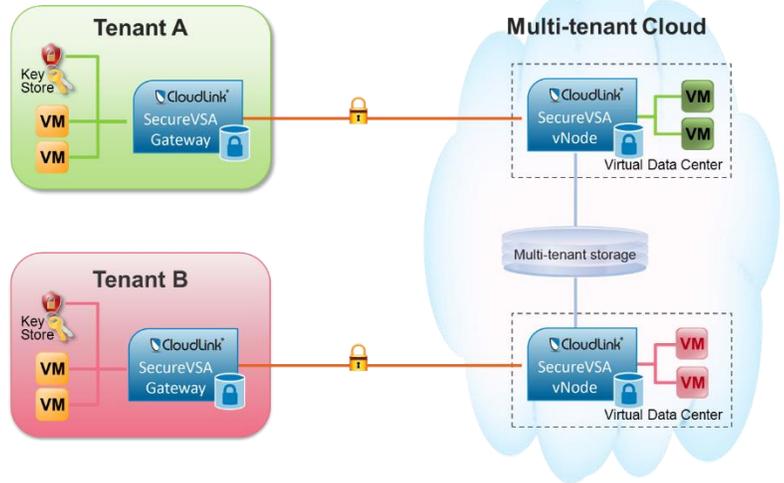
CLOUDLINK SecureVSA: AN ADDITIONAL LAYER OF CONTROL IN CLOUDLINK PLATFORM

CloudLink Platform encompasses several encryption products designed to enable IT/IS teams to efficiently deploy, manage, and report on data security controls while also providing the agility to react to business change and ensuring security policy is met. CloudLink offers:

- **flexibility** to secure data at multiple layers from storage, to virtual machine, to the application level.
- **customizable** modular architecture to select the most appropriate encryption approach for your environment and application requirements.
- **seamless** integration with virtualization, cloud, and key management platforms for full data security control while leveraging existing IT processes.

CloudLink Platform provides "single pane of glass" visibility to control, manage, and report on data security no matter where workloads reside – in an on-premise private cloud, or a public or hybrid cloud environment – which reduces risk to sensitive data and streamlines regulatory compliance initiatives.