CloudLink®
SECURE THE CLOUD. TRUST THE CLOUD.

RSA® READY

WHITE PAPER

RSA® DATA PROTECTION MANAGER WITH CLOUDLINK® SECUREVSA

INTRODUCTION

Today's business environments require organizations of all types to reduce costs and create flexible business processes in order to compete effectively in an ever-changing marketplace. The pace of technological change continues to increase, yet there is an ongoing need to reduce IT costs, leading many companies and government agencies to look for alternative approaches. This has led to a high level of interest in private, public and hybrid cloud computing solutions that transform the IT infrastructure into a dynamic, on-demand utility. According to IDC, worldwide business spending on public cloud services in 2012 will be $40 billion US dollars. And between 2012 and 2016, cloud service spending is projected to expand at a compound annual growth rate of 26.5%[1].

However, cloud computing also brings new challenges and risks to businesses. Many studies point to the fact that security is the number one enterprise concern with cloud adoption. The fear of losing control of corporate data and the risk of data breaches in the cloud hinder the wide adoption of cloud services. Security issues must be addressed and new cloud security technologies must be developed in order to unlock cloud computing benefits.

CloudLink® SecureVSA is an award-winning security and compliance solution designed to address data protection for multi-tenant clouds and virtualization environments. SecureVSA encrypts data-in-motion and data-at-rest in the cloud, providing enterprises with the ability to maintain ownership and control of the data and encryption keys used to secure the data.

SecureVSA is a virtual appliance solution which creates volumes from shared cloud storage and encrypts them using enterprise tenant keys. The keys are stored by the enterprise and remain completely under enterprise control. This approach allows enterprises to leverage the cloud services for sensitive workloads and data, while remaining confident that their intellectual property, customer information, regulated data (PII, PCI) and other corporate data are protected from cloud administrators, other tenants, and other potentially malicious entities. In addition, SecureVSA

[1] *Worldwide and Regional Public IT Cloud Services 2012-2016 Forecast* (IDC #236552)

enables enterprises to achieve compliance with regulations such as PCI-DSS and HIPAA without requiring changes to their IT infrastructure, be it on premise or cloud-based.

RSA® Data Protection Manager (DPM) is an integrated security solution that delivers extremely efficient and comprehensive data protection. DPM is designed to ensure that large numbers of keys are preserved, across geographic and organizational boundaries, without risk of key loss or compromise. It distributes encryption keys when and where they are needed, protecting them in transit and ensuring they are provided only to authenticated and authorized entities. Through its enterprise-grade capabilities, DPM complements SecureVSA's storage encryption to provide a ground-breaking cloud security solution with unparalleled flexibility and ease of deployment.

CLOUDLINK SECUREVSA WITH RSA DATA PROTECTION MANAGER

Together, SecureVSA and RSA DPM offer complete protection of data-in-motion and data-at-rest. The security offered by RSA's leading key management platform is complemented by the convenience, ease of use and cost-effectiveness of the policy-based control SecureVSA provides.

CLOUDLINK SECUREVSA ARCHITECTURE

The SecureVSA software solution consists of three main components.

CloudLink vNode is a software virtual appliance deployed in the cloud. The CloudLink vNode acts as a secure virtual storage appliance, providing encrypted storage to authorized enterprise workloads. The CloudLink vNode's encrypted storage can be presented either as a secure datastore to the hypervisor host or as one or more secure shared network drives, directly to VMs and physical workloads, via NFS, CIFS, or iSCSI. Together, the CloudLink Gateway and CloudLink vNode provide a secure VPN with layer 2 or layer 3 network overlay to ensure that all communications between the virtual data center in the cloud and the enterprise data center are encrypted. They also provide end-to-end SLA performance monitoring and testing of the network link over which they are connected. In a multi-tenant cloud, one or more CloudLink vNodes are deployed per tenant. CloudLink vNode interacts with the cloud infrastructure layer to collect logs and events, monitor virtual machines and storage, and feed the management information back to the enterprise.

CloudLink Gateway is a software virtual appliance deployed inside the enterprise data center, providing a gateway to the cloud. CloudLink Gateway can operate in stand-alone mode, acting as a secure virtual storage appliance. Additionally, it can communicate with one or more CloudLink vNodes to create SLA-monitored encrypted network tunnels to the enterprise's cloud-based virtual data center(s). The CloudLink Gateway generates enterprise controlled encryption keys, places them in a secure key store and delivers them via the secure tunnels to the CloudLink vNodes

deployed in the cloud. In addition, it authenticates CloudLink vNodes, monitors connectivity, and initiates performance testing.

CloudLink Center is a web-based management application that can also be delivered as a VMware vSphere™ Client plug-in. CloudLink Center provides role-based access control, defining security administrator, and administrator and observer users. It configures and manages all encrypted storage volumes and associated encryption keys, presents the deployment's network topology, manages secure VPN connections between the CloudLink Gateway and each CloudLink vNode, monitors network and virtual storage performance, initiates performance testing, and reports events and maintains audit logs.

CloudLink Gateway and the CloudLink Center management application are delivered together as a single virtual appliance.

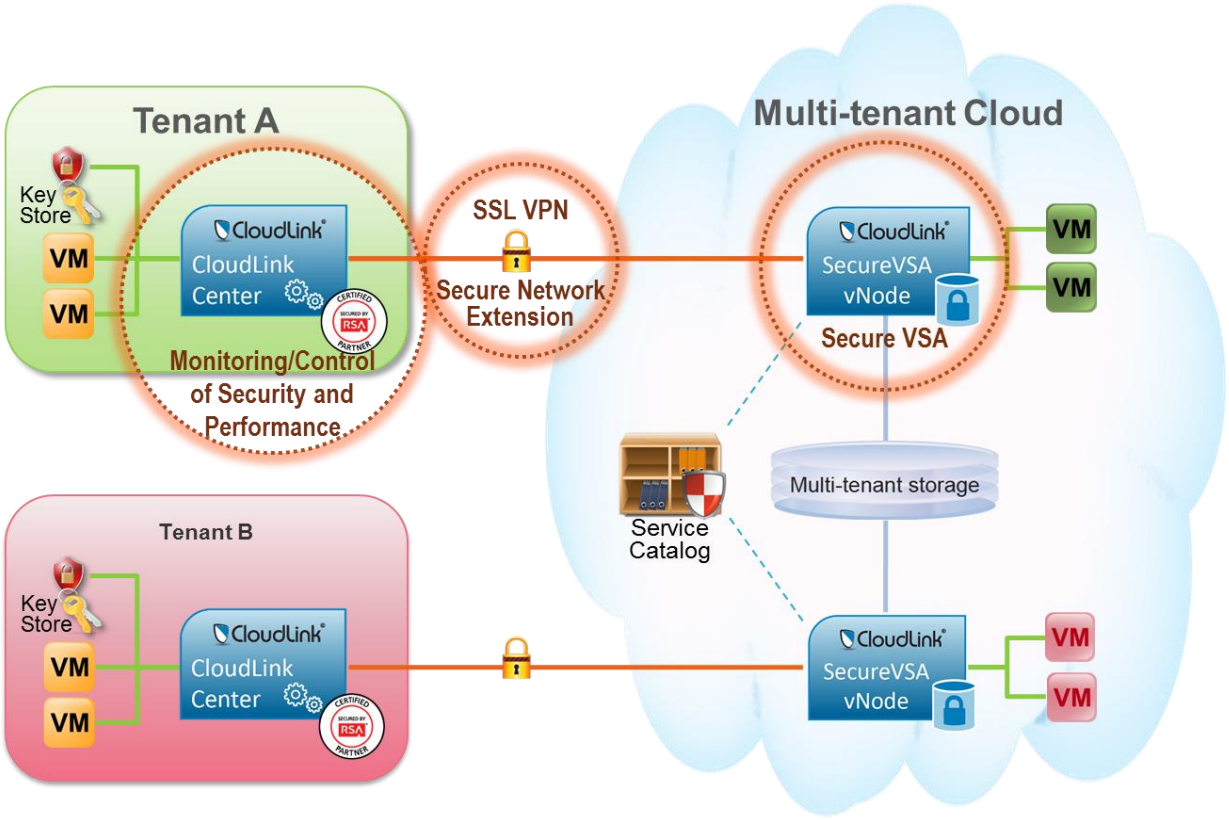

Figure 1: CloudLink SecureVSA Architecture

ENCRYPTION KEY MANAGEMENT

CloudLink Gateway provides out-of-box integration with RSA Data Protection Manager (DPM). All storage key encryption keys (KEKs) created and managed by CloudLink Gateway can be stored securely in DPM. DPM provides centralized key vaulting, protection and recoverability of the keys. The keys are generated by CloudLink Gateway and provided to DPM for safe storage. They are then

retrieved by the CloudLink Gateway and provided to nodes needing to provide access to their encrypted storage volumes; such as, to *unlock* the volumes. At any time, a security administrator using CloudLink Center can instruct SecureVSA to "lock" one or all of a node's encrypted volumes. CloudLink Center then issues a "lock" command to the node at which point the node destroys its cached version of the storage KEK(s).

DPM ships in multiple form factors: hardware appliance, virtual appliance and a software server deployable in customer software infrastructure. Both the hardware and virtual appliances come with a pre-packaged software stack including a web application server, enterprise class database and access management, as well as the ability to integrate with industry standard FIPS 140-2 level 3 modules. Client applications authenticate with the server using mutual SSL. A client application using a DPM client for encryption/key management can operate with a local protected cache for keys.

A typical deployment architecture for key management would be comprised of at least two nodes within the primary site for high availability that are load balanced and more nodes in remote sites for scalability or disaster recovery purposes, all clustered together. All nodes in a cluster are active. DPM appliances come with built-in replication to keep all the nodes in synch. DPM virtual and hardware appliances can be deployed in an identical fashion.

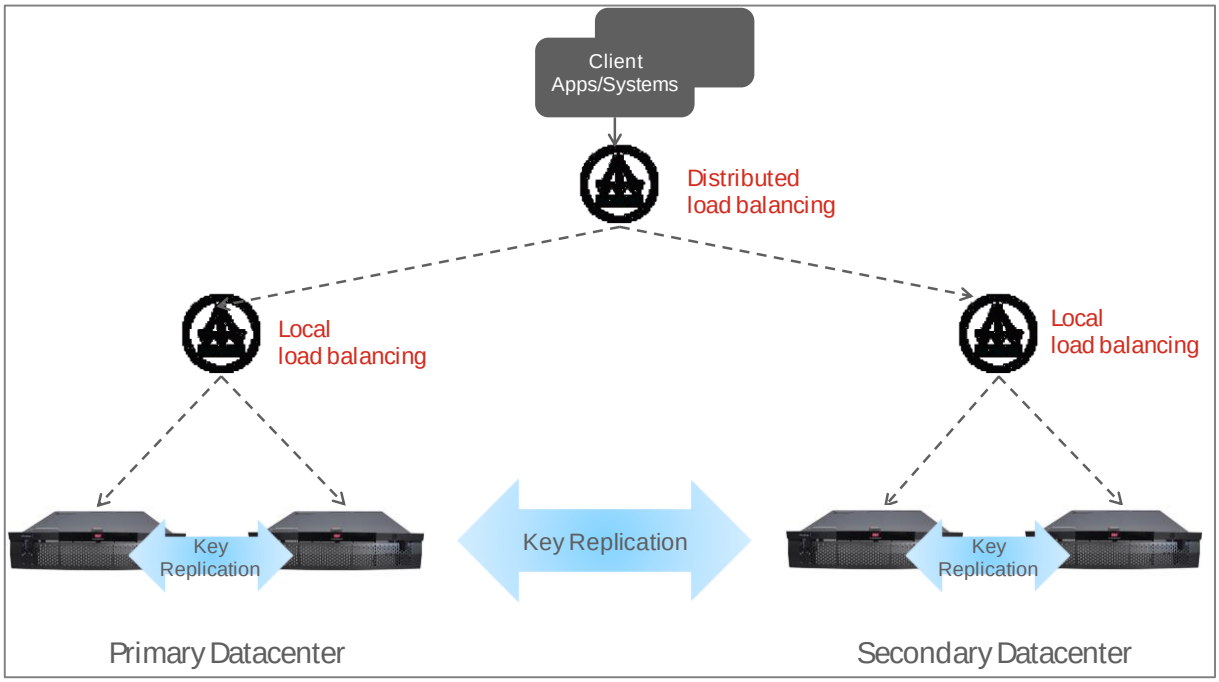

Figure 2: Typical RSA DPM Deployment Architecture

DEPLOYMENT SCENARIOS

ENTERPRISE DATA CENTER EXPANSION INTO THE CLOUD

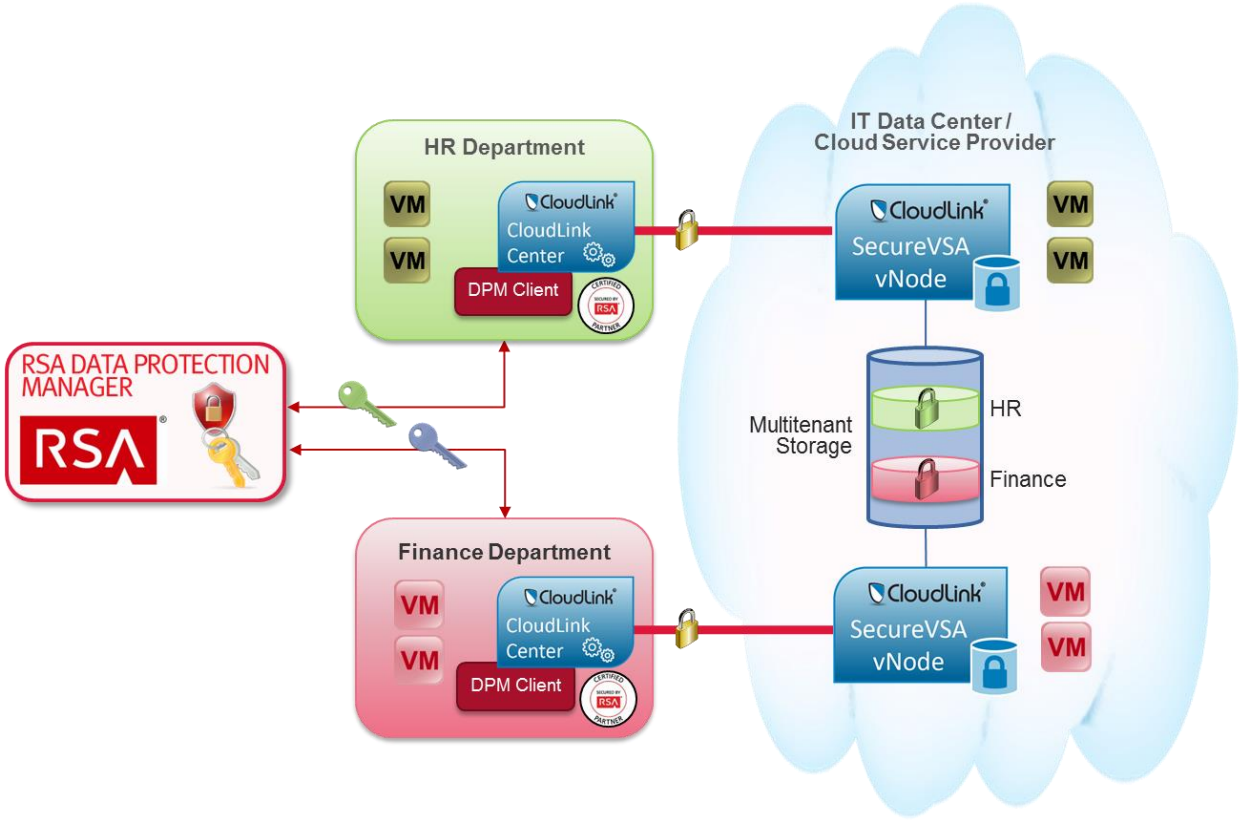

Figure 3: Enterprise data center expansion into the Cloud

Large enterprises have multiple (often dozens or even hundreds of) departments, each requiring isolated and protected access to sensitive information. For example, an HR department records and maintains personal information on its employees whereas a Finance department maintains highly sensitive company data. HR systems and administrators should not necessarily have access to financial data and finance systems and analysts should not necessarily have access to employees' personal information. Each department can therefore be considered a separate tenant in the enterprise's data center with its own requirements concerning data security in motion and at rest. These requirements may be internally imposed; for example, by corporate policy or externally imposed; for example, by regulations such as PCI and HIPAA. As a result, the segregation and protection of each tenant's workloads and the data they consume when stored in and transmitted over shared infrastructure is a primary concern, regardless of whether the infrastructure is hosted in an enterprise data center (private cloud) or a public cloud.

CloudLink vNodes provide departments with their own virtual encrypted storage, partitioning large multi-tenant storage into smaller volumes, each encrypted with its own key. CloudLink Gateway grants the department exclusive control over the storage encryption keys. Because encrypted

information is only as secure as the keys used to encrypt it, it is vital that the potentially hundreds of keys maintained by an enterprise are handled with the utmost care.

By incorporating the RSA DPM client, each CloudLink Gateway instance can entrust its storage KEKs to RSA DPM. It does this by requesting that RSA DPM manage KEKs on its behalf. CloudLink Gateway provides these keys to its corresponding CloudLink vNodes where they are used to encrypt the DEKs of the CloudLink vNode's encrypted storage volumes. CloudLink Gateway can, at any time, instruct a CloudLink vNode to lock its storage volume. In order to unlock the storage, CloudLink Gateway must obtain the appropriate KEK from RSA DPM and provide it again to the CloudLink vNode. All communication between CloudLink Gateway and RSA DPM occurs via a certificate-based mutually authenticated secure session.

STORAGE ENCRYPTION FOR MULTI-TENANT MANAGED SERVICE PROVIDER DEPLOYMENTS

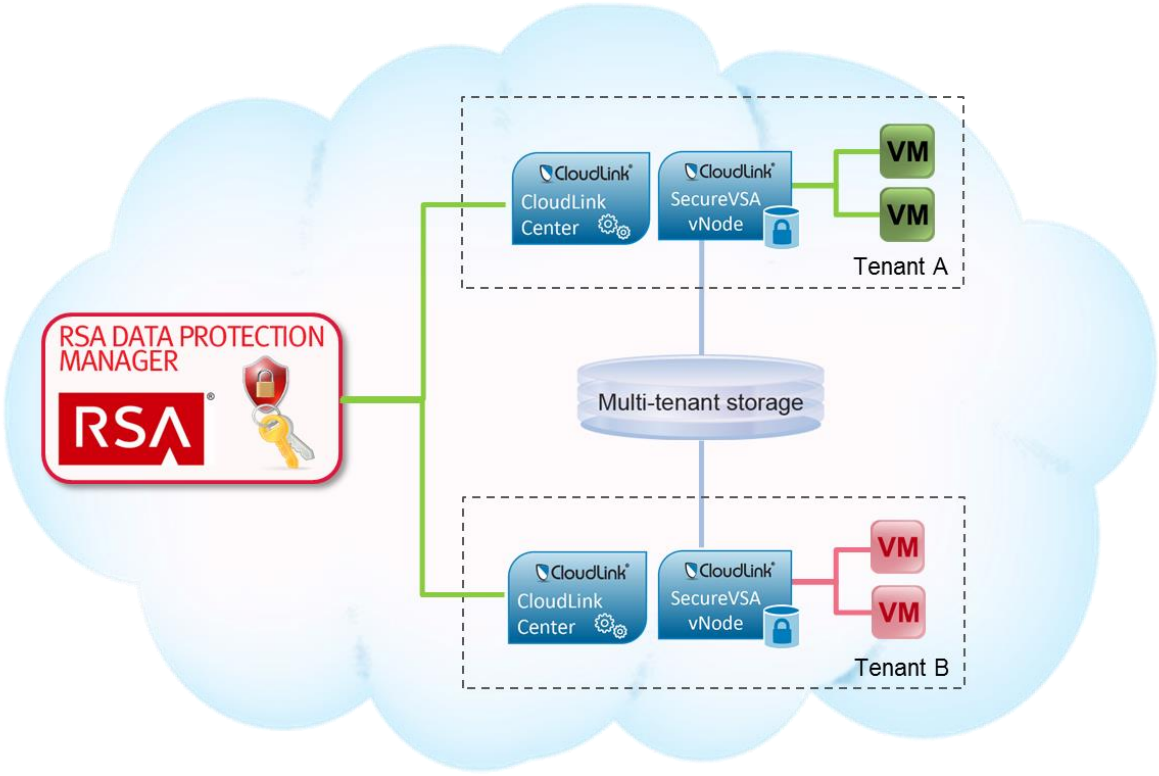

Figure 4: Storage Encryption for multi-tenant Managed Service Providers

Increasingly, enterprises are relying on Managed Service Providers (MSPs) to establish outsourced IT infrastructure and services on their behalves. In order to maintain successful cost margins, MSPs would like to leverage as much shared infrastructure as possible, including shared compute, network and storage resources. However, with the ever-growing focus on cloud security and need to satisfy regulatory compliance requirements, MSPs are charged with deploying demonstrable security for data-in-motion and data-at-rest within their existing offerings.

RSA® DATA PROTECTION MANAGER WITH CLOUDLINK® SECUREVSA

Traditional approaches to achieving data security in multi-tenant managed environments have centered on isolation of tenants' infrastructure by ensuring that each tenant was provided with their own physical compute, network and storage resources. Solutions such as encrypting storage switches and self-encrypting drives provided encryption to further protect data-at-rest. Unfortunately, this approach has proven very challenging and expensive in today's virtual data centers where highly efficient resource utilization and resulting cost savings have become the norm.

SecureVSA offers MSPs the opportunity to leverage shared storage for multiple tenants while affording the tenants complete control and security over sensitive data stored there. A CloudLink Gateway virtual storage appliance can be deployed for each tenant requiring data-at-rest security. CloudLink Gateway encrypts virtual disks assigned to it by the underlying hypervisor with the tenant's keys and exposes them as secure volumes. Tenant VMs may access the volumes as shared secure network drives. Alternatively, the encrypted volumes may be exposed directly to the hypervisor in order to create secure datastores into which the VMs may be placed, providing "agentless" encryption which requires no changes to workload VMs and is completely transparent to them.

Through each CloudLink Gateway's CloudLink Center interface, tenants can monitor and control the availability of their encrypted volumes by choosing whether KEKs are made available to the CloudLink Gateway's cipher. CloudLink Center's *lock* operation withdraws the KEK for an encrypted volume from the CloudLink Gateway, preventing it from decrypting the volume's data encryption key (DEK) and rendering the data stored on the volume unavailable. Conversely, the *unlock* operation provides the KEK for an encrypted volume to the CloudLink Gateway which then uses it to decrypt the volume's DEK and uses the DEK to decrypt and make the data available.

Key encryption keys for all secure volumes exposed by tenant CloudLink Gateways may be stored in RSA DPM. This ensures that they remain protected by the industry-leading key manager, while remaining centralized and easily accessible by the CloudLink Gateways. MSPs benefit from being able to leverage a single key management solution for their various needs while enjoying the reassurance offered by DPM's powerful security and built-in high-availability features.

CONFIGURING CLOUDLINK SECUREVSA INTEGRATION WITH RSA DPM

To use RSA Data Protection Manager (DPM) to store CloudLink KEKs, ensure that an RSA DPM host, version 3.1 or later, is accessible by the CloudLink Gateway via its private LAN network. More information on deploying, configuring and using SecureVSA may be found in the *CloudLink SecureVSA Deployment Guide* and the *CloudLink SecureVSA Administration Guide*.

To prepare RSA Data Protection Manager for storage of CloudLink KEKs:

1. Log on to the RSA Data Protection Manager console.
2. Create an identity that belongs to a particular RSA DPM identity group (***Figure 5***).

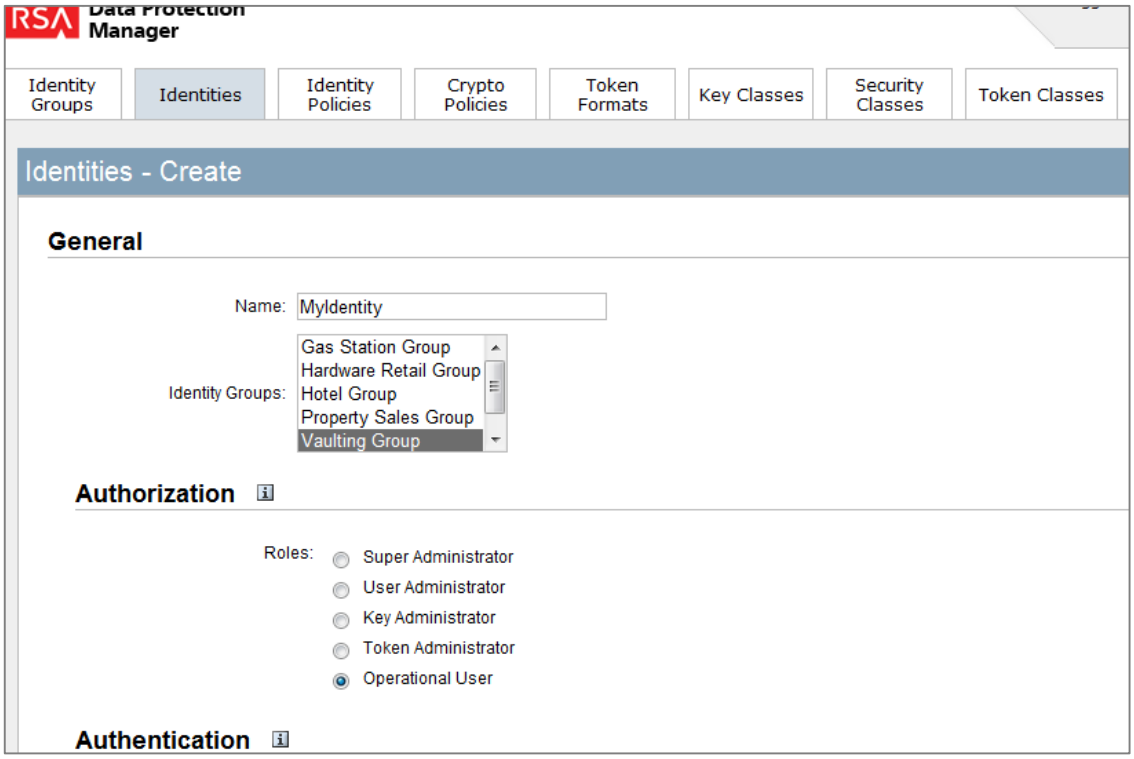

Figure 5: Creating an RSA DPM identity

3. Create a security class object with “Infinite” duration that belongs to the same RSA DPM identity group (***Figure 6***).

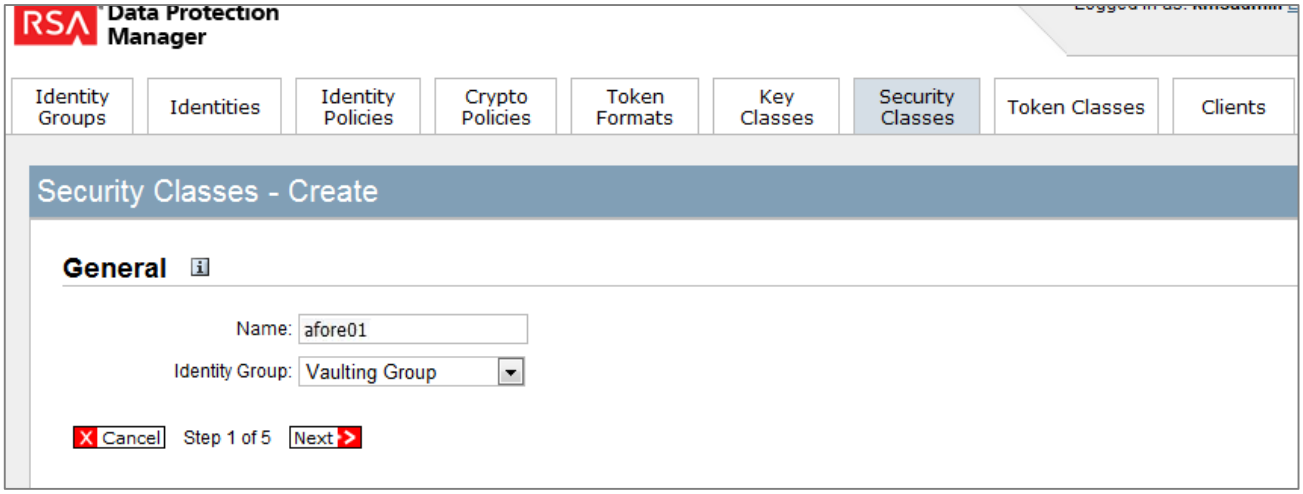

Figure 6: Creating a security class object

To configure SecureVSA to use RSA Data Protection Manager as its key store:

1. Open CloudLink Center on the Gateway using the *secadmin* user account.
2. On the left side of the window, at the top of the VMs list in the **Topology Tree**, select the Gateway.
3. Click **Security** tab and then the **Key Store** tab.
4. To configure CloudLink Center to use RSA Data Protection Manager for KEK storage, in the **Location** panel, click the **RSA DPM** link.
5. In the RSA DPM Configuration panel (***Figure 7***), specify the RSA DPM parameters

Host	The RSA DPM host IP address.
Port	The TCP port number configured on the RSA DPM host (default port = 443).
Security Class Name	The name of the security class configured on the RSA DPM host for the RSA DPM client.
Trust Certificate	The RSA DPM server certificate.
Client Certificate	The RSA DPM client certificate.
Password	The password used during the RSA DPM client certificate creation.

NOTE: Ensure that RSA DPM server and client certificates are created and saved on the RSA DPM host.

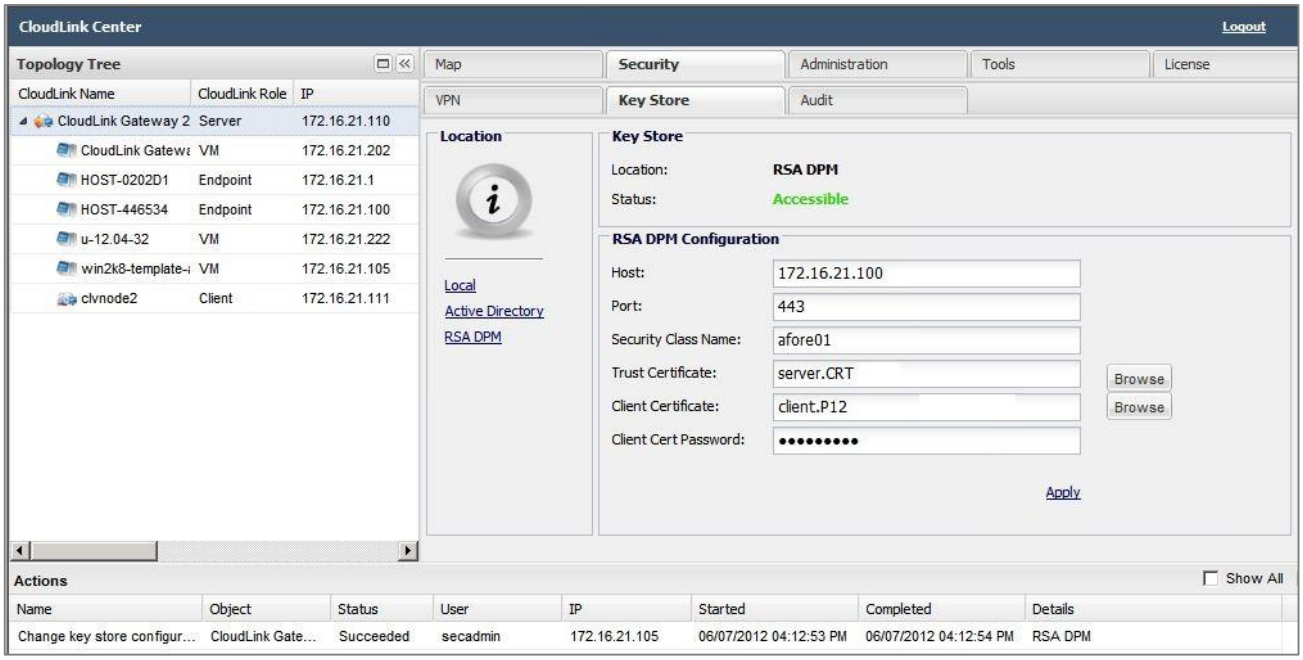

Figure 7: RSA DPM Configuration panel in CloudLink Center

6. Click **Apply** to save the parameters.

Upon successful configuration, CloudLink Center displays RSA DPM's status as *Accessible*. It creates a new "Change key store succeeded" entry in the CloudLink Center action log (***Figure 7***) and records a "Key store change" security event (***Figure 8***).

Figure 8: "Key store change" security event recorded by CloudLink SecureVSA

In addition, CloudLink Center is listed In the RSA DPM management console as one of its managed clients (***Figure 9***).

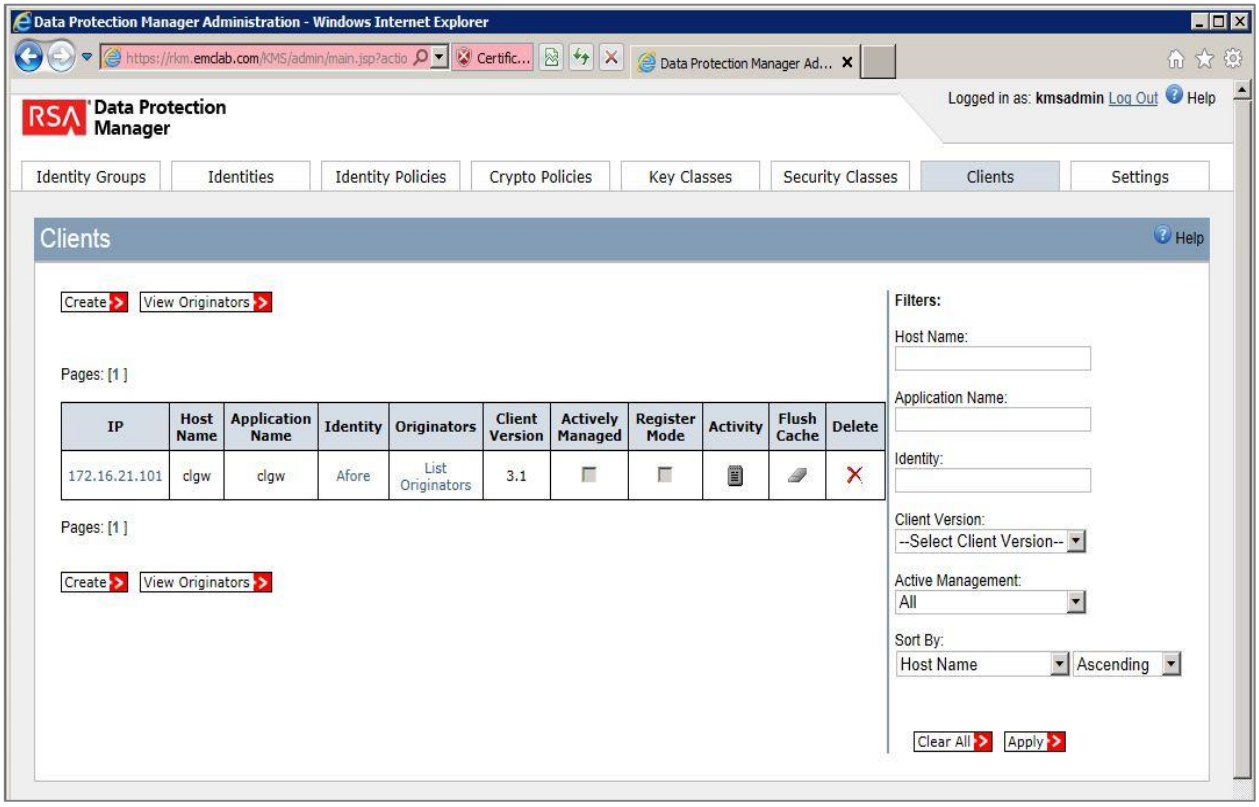

Figure 9: CloudLink SecureVSA listed as managed client in RSA DPM management console

Information on CloudLink SecureVSA storage KEKs entrusted to RSA DPM may be viewed in the DPM management console by RSA DPM administrators with appropriate permissions (***Figure 10***).

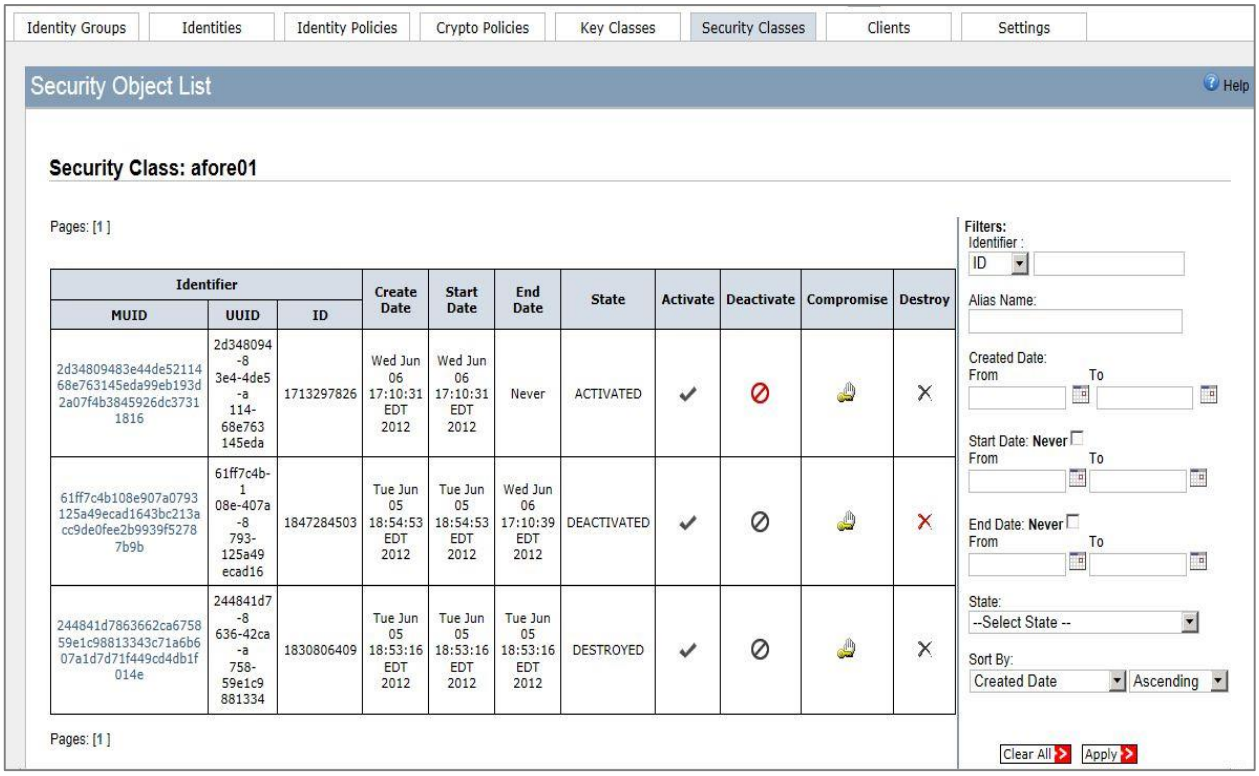

Figure 10: CloudLink key information displayed in RSA DPM management console

CONCLUSION

Enterprises adopting private, public or hybrid cloud services wrestle with the challenges of data protection and maintaining control of their data in multi-tenant cloud environments. In addition, service providers want to increase efficiency and lower costs by leveraging shared infrastructure for multiple tenants without sacrificing data security or regulatory compliance.

Together, SecureVSA and RSA Data Protection Manager address these challenges by encrypting data-at-rest in the cloud, while providing enterprises the ability to maintain ownership and control of the data and the encryption keys used to secure the data. This solution is infrastructure and application agnostic and supports various private and public cloud platforms. Key encryption keys are maintained centrally and protected by DPM's enterprise-class key management and high-availability capabilities.

Contact us for more information

CloudLink Technologies: Phone +1 (613) 224-5994 | Email info@cloudlinktech.com | Click cloudlinktech.com