CloudLink®
SECURE THE CLOUD. TRUST THE CLOUD.

SOLUTION BRIEF

ENTERPRISE-WIDE DATA SECURITY WITH CLOUDLINK® SECUREVSA AND RSA® DATA PROTECTION MANAGER

CLOUDLINK® SECUREVSA

Concerns over cloud security, manageability, performance, and reliability have been the biggest barriers to the more rapid and wider spread adoption of cloud services. Leveraging cloud infrastructure, be it public, private or hybrid, offers enterprises significant cost savings and flexibility. CloudLink® SecureVSA combines cloud infrastructure security and manageability with performance monitoring to protect mission-critical data-in-motion and data-at-rest. SecureVSA consists of three main components:

1. **CloudLink vNode** is a software virtual appliance deployed in public, private or hybrid clouds. The CloudLink vNode provides AES-256 encrypted storage and acts as the communications endpoint between VMs in the virtual data center (VDC) and the enterprise network. CloudLink vNode works with CloudLink Gateway for end-to-end network performance monitoring and testing, and to obtain the keys used to encrypt storage. Inside the cloud, CloudLink vNode interacts with the cloud infrastructure layer to encrypt storage, collect logs and events, monitor the VMs and storage, and feed the management information back to the enterprise.
2. **CloudLink Gateway** is a software virtual appliance deployed within individual enterprise departments. The CloudLink Gateway communicates with the CloudLink vNodes deployed in the cloud to create a secure VPN overlay to the department specific VDCs. The CloudLink Gateway authenticates CloudLink vNodes, monitors connectivity, initiates performance testing, and pushes the department controlled storage encryption keys via the secure tunnel to the CloudLink vNodes deployed in the cloud.
3. **CloudLink Center** is a management application that can be utilized as a web application or as a VMware vCenter™ plug-in. It manages the CloudLink Gateway and CloudLink vNode, administers trust policies, configures encrypted storage volumes, monitors end-to-end network performance, reports events, logs and alarms, and presents the deployment's network topology.

RSA® DATA PROTECTION MANAGER

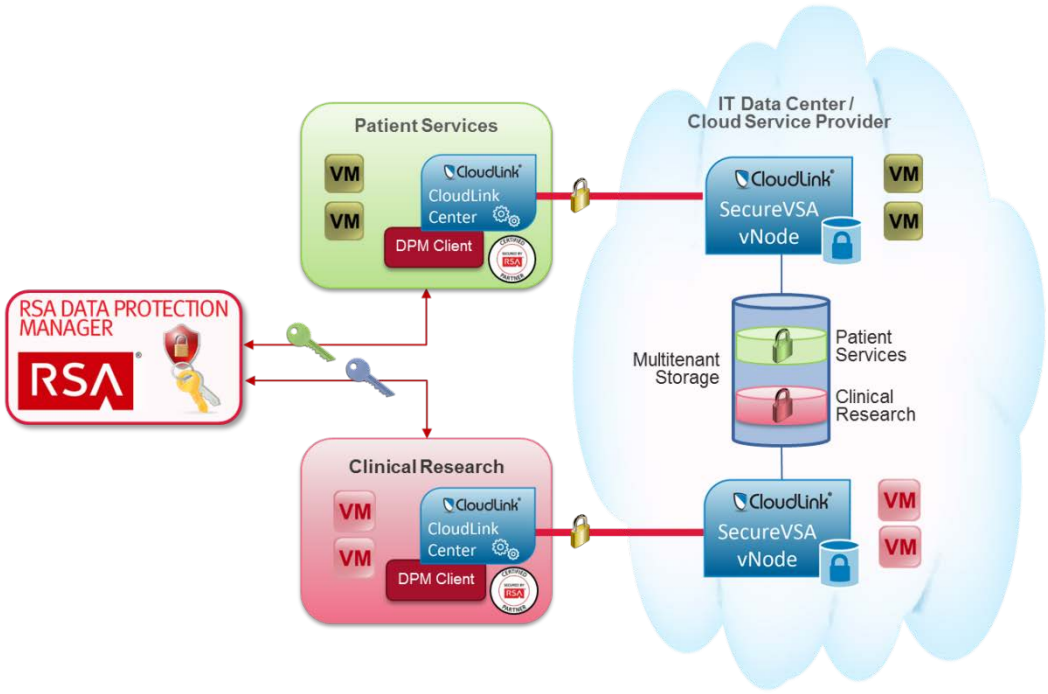
RSA® Data Protection Manager (formerly RSA Key Manager) is an integrated security solution that gives customers an extremely efficient and comprehensive data protection solution. As an integral part of RSA Data Protection Manager (RSA DPM), enterprise key management is an easy-to-use management tool for encrypting keys at the database, file server and storage layers. It's designed to lower the total cost of ownership and simplify the deployment of encryption throughout the enterprise. It also helps ensure that information is properly secured and fully accessible when needed at any point in its lifecycle through a powerful management console and built-in high availability features.

BENEFITS:

- Departmental control of trust in multi-tenant cloud infrastructure
- Secure and easy management of a multitude of keys required for enterprise departments
- Seamless extension of key management into cloud and virtualized domains
- Cloud network performance management and security policy monitoring
- Regulatory compliance through data encryption with department-controlled keys
- Eliminates the need for physical-level storage encryption, allowing completely virtual environments
- Simplifies storage backup and replication by segmenting larger array in per-tenant encrypted volumes
- OPEX savings via seamless extension into the public cloud
- CAPEX savings via use of shared cloud infrastructure

FEATURES:

- Encryption of data-in-motion and data-at-rest in a virtualized/cloud environment
- Maintains virtualization environments by eliminating the requirement to encrypt at the physical level
- Encryption key and security policy management by individual enterprise departments
- Secure Layer 2 (Ethernet) Overlay offering enterprise network extension into the cloud
- End-to-end network performance monitoring and diagnostics
- Integration with VMware vCenter
- Full utilization of host hardware acceleration for AES encryption



INTEGRATED SOLUTION

Together, SecureVSA and RSA Data Protection Manager 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 that SecureVSA provides.

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 key. Because encrypted information is only as secure as the keys used to encrypt it, it's 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 encryption keys to the RSA DPM. It does this by requesting that the RSA DPM generate and manage storage encryption keys on its behalf. CloudLink Gateway provides these keys to its corresponding CloudLink vNodes where they're used to encrypt the data encryption keys 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 key from the 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.

Contact us for more information

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