AFORE

SECURE THE CLOUD. TRUST THE CLOUD.

WHITE PAPER

PROTECTING DATA IN MULTI-TENANT CLOUDS

1 Introduction

Today's business environment requires organizations of all types to reduce costs and create flexible business processes 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 will expand at a compound annual growth rate of 26.5%[1].

However, cloud computing also brings new challenges, issues and risks to the business. Much of the research indicates that security is the number one concern of cloud adoption. The fear of losing control of corporate data and the risk of data breaches in the cloud can potentially 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.

AFORE CloudLink® is an award winning security and compliance solution designed to address data protection for multi-tenant clouds and virtualization environments. This paper describes the security problems CloudLink solves, how CloudLink works and what benefits CloudLink brings to cloud service providers, enterprises and government organizations.

2 Problem Statement

Cloud computing can be characterized by the following attributes:

- Virtualization infrastructure: Workloads typically run on a virtualized infrastructure consisting of virtual servers, virtual networks and virtual storage.
- Multi-tenancy: Multiple cloud service customers can share the same hypervisor, the same physical server and the same physical network and storage for their workloads and data.

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

- Dynamic, mobile and software defined: Cloud computing resources are dynamically allocated and consumed. Each customer can have their own virtual data center. The resources that workloads consume are mobile, i.e. they can be migrated between two physical data centers and among different hardware platforms. The dynamics and mobility of virtual data center resources are defined by software.
- Managed by cloud administrators: Cloud computing infrastructure is managed by cloud service provider administrators who have full access to the data on the servers and the storage.

These cloud computing characteristics create new security challenges for cloud service customers.

2.1 Protecting data and maintaining control in multi-tenant cloud

Enterprises have spent many years building solid processes, scalable procedures and internal systems expertise to make their data centers secure, reliable and manageable in order to be compliant with business and regulatory requirements. When moving workloads to the cloud, enterprises need to extend their security management into the cloud and maintain control of their data in order to protect intellectual property, sensitive information and brands, while continuing to pass security audits.

Government agencies are also modifying regulations and policies to cover the cloud and virtualization environments, in general. The data in a virtualized cloud environment are also subject to regulatory compliance requirements such as PCI and HIPAA. Several new government cloud computing recommendations clearly state that cloud service consumers are responsible for compliance with these regulations. For example, US NIST states that "when data or processing is moved to a cloud, the consumer retains the ultimate responsibility for compliance"[2]. UK ICO states in its "Guidance on the use of cloud computing" [3] that cloud service consuming organizations will continue to be data controllers and will be required to meet their obligations under the Data Protection Act.

Failing to protect data in the cloud will result in damage to the enterprise's brand, loss of intellectual property and competitive advantage, and significant financial cost related to litigation and penalties. According to Ponemon, the average cost of a data breach event was $US5.5 million in 2011[4].

Therefore, the first challenge of cloud security is how to protect cloud consumers' data in a multi-tenant environment from side attacks launched by other malicious tenants and from "insider" attacks launched by the malicious cloud administrators, and to provide a mechanism for cloud consumers to control their data and meet compliance requirements.

[2] NIST 800-146"Cloud Computing Synopsis and Recommendations" May 2012

[3] ICO, "Guidance on the Use of Cloud Computing" version 1.1, Oct 2, 2012

[4] Ponemon, ""U.S. Cost of a Data Breach" Study, 2011

2.2 Traditional data protection methods are insufficient

Traditional data protection and security methods assume that there is a clear perimeter between outsiders and insiders, and that all data to be protected are in an enterprise-controlled data center behind multi-tier firewalls with enterprise security administrators in complete control of security policy. However, these traditional methods have proven insufficient in the cloud.

First, traditional data protection products are not designed for multi-tenant environments. Typically they are either physical machine based to protect data on a specific physical machine such as disk encryption or storage-based to encrypt data on a storage device via encryption capability on storage devices or on SAN switches. These solutions have their own limits in a cloud environment. For example, some physical machine based solutions do not support virtualized environments; storage based solutions do not support multi-tenancy and it becomes extremely expensive to allocate dedicated physical storage to each tenant, which also defeats the cloud multi-tenant benefit.

Second, the boundary between insiders and outsiders is very vague in the cloud environment. Outside cloud administrators become “insiders” from the perspective of managing the infrastructure and hypervisor. Both legitimate virtual machines (VMs) and rogue VMs can be behind cloud service provider firewalls. The side attack threat and malicious insider attack risk in multi-tenant clouds is significantly higher than in traditional on-premise data center environments. Relying on perimeter security methods to secure cloud data is not sufficient.

Third, none of the traditional data protection solutions is able to provide a mechanism for cloud customers to control data residing in cloud environments. Cloud environments require a split horizon security management approach where cloud administrators are responsible for securing infrastructure and cloud consumers are responsible for securing their own workloads and data.

2.3 Data Remanence

Cloud services are dynamic and on-demand. Whenever a cloud provider is changed, resources are scaled down, physical hardware is reallocated, or storage disks are sent out for repair, it may be impossible to carry out the data deletion procedures specified by the security policy, since full data deletion is only possible by destroying the disks which may also contain data owned by other cloud customers. Solving data remanence issues in the cloud in a cost effective way and proving to security auditors that digital shredding procedures have been carried out is a unique challenge to both cloud service consumers and cloud service providers.

3 CloudLink® - Securing the Multi-Tenant Cloud

AFORE CloudLink® is designed to provide cryptographic protection of sensitive data while maintaining the data owner’s control over security and compliance in a multi-tenant virtualized cloud environment.

It is a software solution that enables secure Infrastructure as a Service (IaaS) in private, public or hybrid cloud environments.

3.1 CloudLink® Architecture

The following three components comprise the CloudLink software solution.

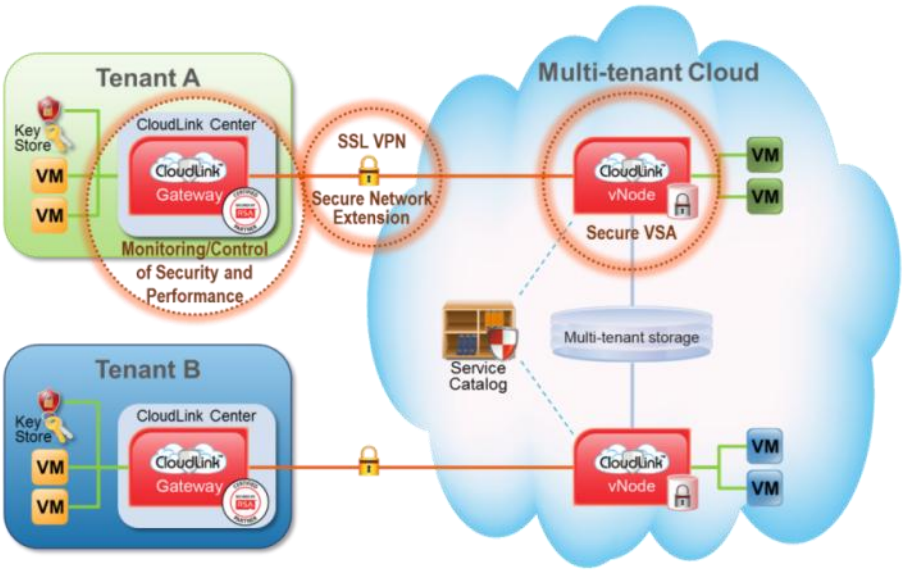
CloudLink Center is a Web-based management application that can also be delivered as a VMware vSphere™ Client plug-in. CloudLink Center provides role-based access control, defining security administrator, administrator and observer users. It manages layer 2 or layer 3 VPN connections between the CloudLink Gateway and each CloudLink vNode, manages storage encryption keys, monitors network and virtual storage performance, initiates performance testing, and reports events and maintains audit logs.

CloudLink vNode is a software virtual appliance deployed in the cloud. The vNode acts as a secure virtual storage appliance providing encrypted storage to authorized enterprise workloads. The vNode secure storage can either be presented as a secure datastore to the hypervisor host or as a secure shared network drive directly to VMs via NFS, CIFS, or iSCSI. The vNode also acts as the communications endpoint, providing a secure VPN to ensure that all communications between the virtual data center in the cloud and the enterprise data center are encrypted. In a multi-tenant cloud, a vNode is deployed on a per-tenant basis, with at least one vNode per tenant. Together, CloudLink Gateway and vNode provide end-to-end network performance monitoring and testing. Inside the cloud, 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 that provides a gateway to the cloud. The CloudLink Gateway communicates with one or more CloudLink vNodes to create SLA-monitored encrypted network tunnels to the enterprise's cloud-based virtual data center. The Gateway generates enterprise controlled encryption keys, places them in a secure key store and delivers them via the secure tunnels to the vNodes deployed in the cloud. In addition, it authenticates vNodes, monitors connectivity, and initiates performance testing.

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

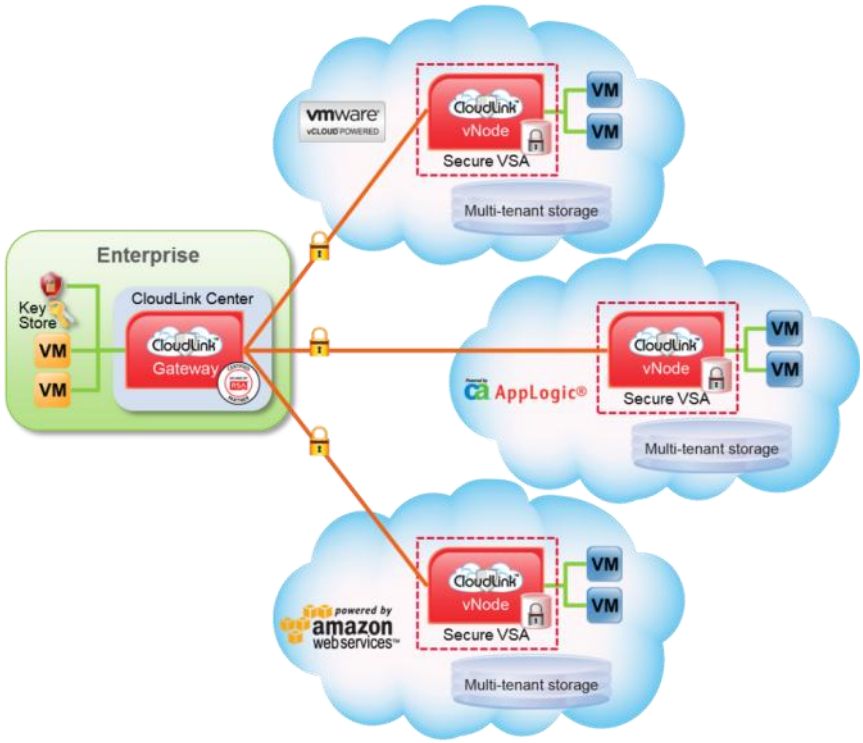
Figure 1: CloudLink Architecture



3.2 IaaS Cloud Agnosticism

CloudLink is suitable for any IaaS cloud environment. It currently supports VMware vSphere™, VMware vCloud Director™, CA AppLogic® and Amazon Virtual Private Cloud™ infrastructures, allowing organizations to choose from the widest array of Cloud Service Providers.

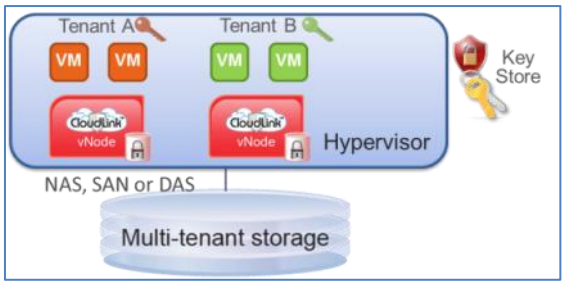
Figure 2: Suitable for multiple IaaS environments



3.3 Encryption of data at rest

The CloudLink solution provides secure virtual storage appliances which are deployed on a per-tenant basis in a multi-tenant cloud. In this shared cloud infrastructure environment, storage is connected to the hypervisor either directly or via standard SAN (FC, FCoE), NAS or iSCSI methods. Each tenant deploys its own vNode virtual appliance on top of this shared infrastructure. The vNode carves out a secure volume from the shared storage. Each tenant encrypts the volume and stores the encryption key safely on its premises and within its control. By doing this, multiple secure virtual storage volumes are created on top of the shared storage infrastructure. All data in each secure volume are AES-256 encrypted with a unique encryption key controlled by the tenant.

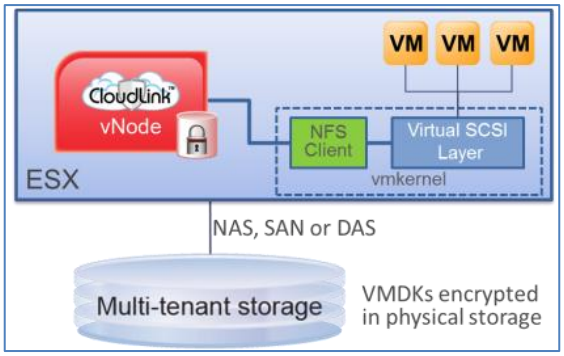
Figure 3: How CloudLink Encrypts Data at Rest



Once a secure virtual storage volume is created, vNode exposes this volume in one of two ways:

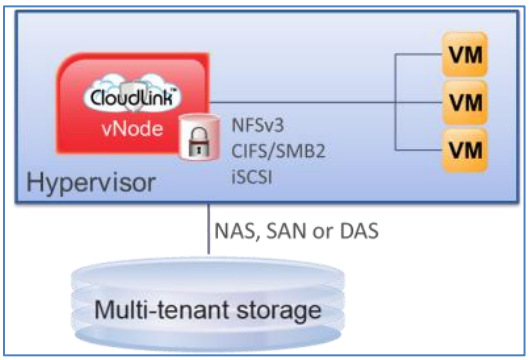
1. **Secure datastore mode:** In this mode, vNode presents itself as a secure NFS server to the VMware ESX host. The ESX host presents this vNode as a secure datastore. A VM can add a secure disk from this datastore and all virtual machine disks (vmdk files) are encrypted within this datastore.

Figure 4: Secure Datastore mode



2. **Secure NAS mode:** In this mode, vNode presents its secure volumes as shared network drive via NFS, CIFS/SMB or iSCSI directly to virtual or physical machines.

Figure 5: Secure NAS mode



3.4 Encryption of data in motion

To support secure cloud on-boarding, CloudLink provides end-to-end secure communications between the enterprise data center and the cloud-based virtual data center using robust AES-256 encryption algorithms. Between the enterprise data center and virtual data center in the cloud, CloudLink creates a secure VPN tunnel. All communication between the enterprise data center and cloud workloads and cloud storage are encrypted. The tunnel can be configured either in layer 2 mode, which extends the enterprise's subnet into the cloud, or in layer 3 mode.

3.5 Encryption key management

For each encrypted data store, there are two encryption keys. The data encryption key (DEK) is generated by the vNode and is used to encrypt the data. The DEK is then encrypted with a Key Encryption Key (KEK) and stored, on disk, with the data. Enterprise security administrators have full control of the encryption keys and the KEKs can be updated regularly by enterprise security administrators via the secure in-band management channel. Special care is taken to ensure that the enterprise-owned data are never stored or transferred in clear text and can be promptly withdrawn by the enterprise at will. Cloud administrators do not have access to DEKs and KEKs, therefore neither cloud administrators, nor other tenants or intruders can access the enterprise data in the cloud.

KEKs are generated and managed by the CloudLink Gateway on the enterprise premises. They must be changed regularly per enterprise key management policy and kept in a safe place in order to ensure the safety of encrypted data. CloudLink supports three different key stores:

- RSA® Data Protection Manager (DPM) provides a FIPS140-2 compliant key store, which is tamper proof and supports high availability. The RSA DPM client has been integrated into CloudLink Gateway.

- Microsoft® Active Directory® (AD) provides an alternate secure encryption key store. This option allows an enterprise to leverage its existing AD deployment and securely store cloud encryption keys.
- KEKs may also be stored within the CloudLink Gateway. This option is suitable for trials and testing but is not recommended for production deployment.

3.6 Manageability

An essential requirement of adopting cloud services is to preserve overall management and control of the IT infrastructure, whether physically located at a local data center or located in the cloud. Management capabilities must be extended to physical and virtual servers, storage, security policies, applications and networking elements. CloudLink equips enterprise IT administrators with a powerful suite of capabilities to monitor and manage the end-to-end communications between workloads in the enterprise data center and those residing in the cloud.

Extension of enterprise control and management into the cloud: CloudLink Center is a Web-based console accessed via a Web browser. In addition, a VMware vSphere™ Client plug-in is provided, enabling IT managers to launch CloudLink Center from their VMware vCenter™ management tool. Enterprise IT administrators can use CloudLink Center to manage security policies and encryption keys, and monitor security and cloud network performance from within the enterprises' trusted boundary.

SLA monitoring: Network SLA and performance monitoring tools are essential elements of cloud management. The wide area network connectivity between the data center and cloud environment may traverse several service provider networks, creating the potential for performance issues. When an application is not performing as expected it is important to determine the cause of the bottleneck.

CloudLink Center provides powerful capabilities to monitor the communications infrastructure across the data center and wide area networks, through the cloud provider's network and into the virtual data center servers in the cloud. This end-to-end visibility equips both the enterprise IT manager and cloud service provider administrator with the information required to identify performance issues and conduct troubleshooting operations in order to ensure that SLA objectives are being met.

- **Connection status monitoring:** The CloudLink Gateway and vNode continuously exchange heartbeat messages to monitor the link status from the enterprise data center to the cloud. Administrators are notified of any link status failure via the CloudLink Center topology map and the alarm panel. In addition, CloudLink's notification capabilities may be extended using its support for syslog and SNMP.

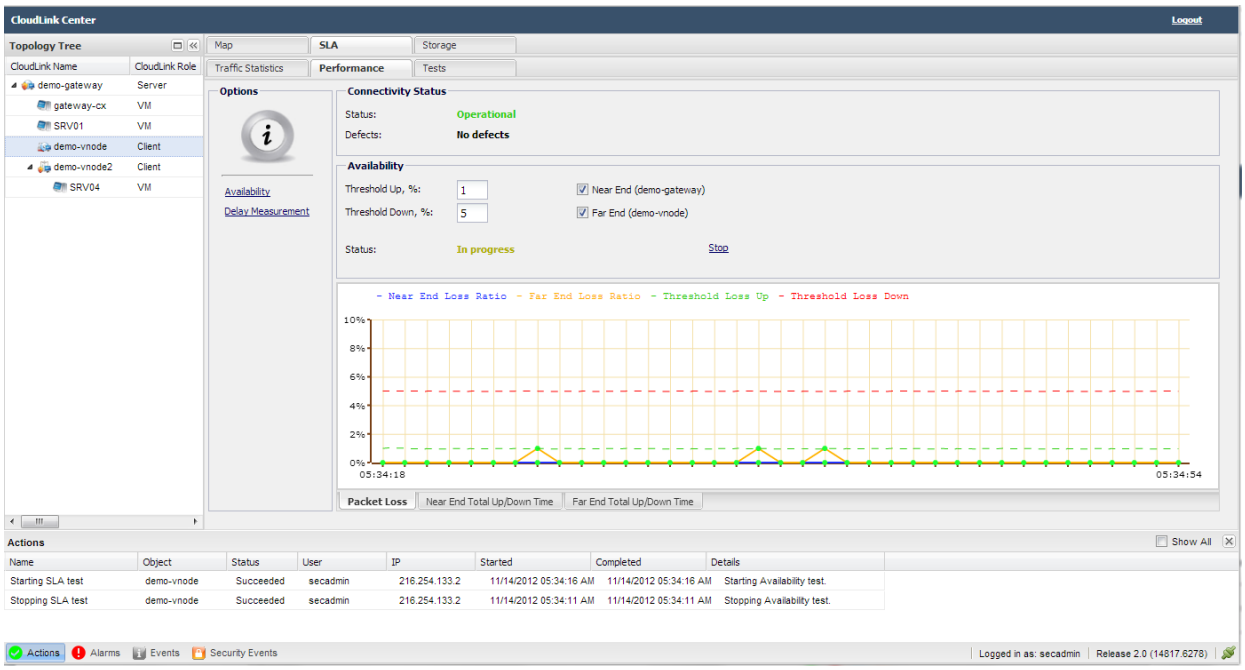
- **Delay measurement:** CloudLink monitors round trip delay (latency) and delay variation (jitter). The delay measurement diagnostics can be performed without disrupting service.

- **Loss measurement:** CloudLink uses synthetic loss measurement technology to characterize the packet loss in the network. Users can initiate loss measurement testing to measure the near end (Gateway side) packet loss ratio and far end (vNode side) packet loss ratio.

- **Loopback test:** CloudLink supports loopback capabilities for troubleshooting and fault localization. Users can initiate loopback tests from the Gateway to the vNode or vice versa.

- **Throughput test:** CloudLink allows users to perform throughput tests to measure the level of bandwidth between the data center and virtual data center in the cloud to ensure it meets the subscribed rates.

Figure 6: Powerful SLA Monitoring and Diagnostics



Role based administration: CloudLink Center supports role based administration to separate security management from IT infrastructure administration. There are three roles pre-defined in CloudLink: security administrator (secadmin), regular IT administrator (admin) and observer for monitoring. Each role has its own unique privilege set as defined in the following table.

Table 1: CloudLink Administration Roles and Privileges

Operation	secadmin	admin	observer
Control of keys for encrypted storage	✓	✗	✗
VPN configuration and control	✓	✓	✗
Network Performance and SLA monitoring	✓	✓	✓
View VM Security Audit status	✓	✗	✗
View Security Events	✓	✗	✗
View Actions	✓	✓	✗
View Alarms and Events	✓	✓	✗
Syslog/SNMP configuration	✓	✓	✗

4 CloudLink Benefits

CloudLink provides a data protection solution for enterprise customers allowing them to leverage multi-tenant clouds for their elastic workload requirements, expanding storage needs or disaster recovery purposes. It ensures that enterprise data in the cloud are secure and still under enterprise control. It also enables cloud service providers to augment their service offering to meet their customers' data protection requirements and accelerate wide adoption of their services.

Enable the enterprise to meet data protection compliance requirements in a multi-tenant cloud. By deploying CloudLink in the cloud, an enterprise is able to demonstrate encryption of data at rest for personal identity information (PII) or other sensitive information and encryption of data in motion between the enterprise premises and external clouds. This is a vital part of achieving compliance with PCI DSS, HIPAA and other regulations. The enterprise is also able to demonstrate to the auditor that it does not lose control of the data. The enterprise holds the encryption keys, controls the security policies and can monitor data security events in the cloud.

Solve data remanence issues in a multi-tenant cloud. CloudLink provides a very cost effective approach for solving data remanence issues. Data stay encrypted at all times on the cloud storage device. CloudLink ensures that there is no data leakage in situations where disks need to be repaired

by a 3rd party or the disks are lost. When a cloud customer decides to terminate the cloud service, removing the encryption key renders all the data remaining in the cloud useless.

Empower the enterprise with control in the cloud. CloudLink provides the enterprise with overall control of cloud security by giving the enterprise sole control of encryption keys and security policies. It enables the enterprise to monitor cloud network performance in a manner consistent with the tools used to manage their own data centers. By deploying CloudLink, enterprises gain end-to-end control and extend their management capabilities into the cloud.

Enable value added services for cloud providers. CloudLink gives cloud service providers the ability to differentiate their service offerings. CloudLink virtual appliances can be published as vApp templates in cloud service providers' value added service catalogs, generating additional revenue for the provider. Each CloudLink virtual appliance runs in a designated virtual data center and is therefore well suited to service providers' multi-tenant cloud environments.

No IT infrastructure and application changes required. CloudLink is a "plug and play" solution operating within an existing IT infrastructure. No change is required to storage, workloads and networks, and no additional hardware is required. This transparency brings several benefits. First, your existing infrastructure investment is protected. Second, the operation cost is much lower than solutions which require installing encryption agents in every guest virtual machine. Third, there is a much lower front-end investment by eliminating the need to add encryption capable hardware equipment and dedicated storage devices for tenants.

Unlock the economic benefits of the cloud. CloudLink combines security, performance and manageability in a single solution that integrates seamlessly with VMware vSphere™, VMware vCloud Director™, CA AppLogic® and Amazon Virtual Private Cloud™ environments. CloudLink accelerates the adoption of private, public and hybrid cloud services while protecting the existing data center and IT investment.

5 Conclusions

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. CloudLink answers the challenges by encrypting both data in motion and data at rest in the cloud, providing the enterprise the ability to maintain ownership and control of the data and encryption keys used to secure the data. This solution is infrastructure and application agnostic and supports various private cloud platforms and public cloud platforms. By protecting the enterprise's data and giving the enterprise control over their data, CloudLink enables trust in a multi-tenant cloud.

-###-