Securing cloud workloads can be complex

Moving to the cloud offers enterprises significant benefits in terms of business agility and IT cost management; however, there are security and deployment challenges.

Cloud computing is based on a shared, multi-tenant architecture. Traditional security controls no longer apply in the cloud, yet sensitive data must be secure to address privacy, regulatory, and data remanence (residual data) requirements, while virtual machine images themselves must be verified to protect against malicious or accidental tampering. As workloads are often distributed across both public and private clouds, data security must be easy to deploy and manage without having to re-architect applications. It must also provide the flexibility to support a variety of encryption approaches to address a variety of use cases.

Organizations need a way to address cloud security by extending existing, proven tools, rather than introducing new methods that add to deployment complexity and operational risk – all while ensuring security control remains in their hands.

Boot and Data Volume Security for vCloud Air VM’s

CloudLink® SecureVM allows you to implement your own data security so that you can protect access to your VM’s and sensitive data residing in your VMware vCloud Air virtual data center.

SecureVM unlocks native Windows Bitlocker and Linux OS encryption features with a centralized management approach, giving you visibility and control over when and where VMs and data are run and accessed while retaining full control of the encryption keys. With SecureVM, cloud encryption becomes easy to deploy, relying on encryption tools already provided by the OS vendors, rather than introducing proprietary technologies that must be integrated and proven with each new OS release. With SecureVM, organizations can confidently embrace the cloud knowing that VM data security, regulatory compliance and data remanence requirements are met.

Deploy with Ease. Secure with Confidence.

With the vCloud Air and SecureVM solution you:

- Use native OS encryption tools to reduce cost and complexity
- Protect the entire VM including boot and data volumes without re-architecting how your applications store data
- Leverage existing key management tools, like RSA® DPM and Microsoft® AD, to hold keys on premise or in the cloud—plus, customer-controlled encryption keys ensure that third parties won’t have access to your data
- Manage and monitor security and performance across the hybrid cloud
Bring Your Own Data Security to vCloud Air

SecureVM provides you with the security controls necessary to move forward with server and desktop cloud initiatives by extending security protection beyond the data to the VM itself. SecureVM enables encryption of the entire VM running in the vCloud Air. This enables you to define the security policy that must be adhered to for a VM to start, including the ability to verify the integrity of the VM, offering protection against unauthorized modifications. SecureVM ensures that only trusted and verified VMs have the ability to run and access sensitive data residing in the cloud.

Native authentication mechanisms typically found in hardware environments are not supported in cloud environments, however SecureVM’s proven encryption key policy management unlocks native OS encryption such as Microsoft BitLocker®, and allows it to be used for automated encryption of boot volumes in the cloud while enabling enterprise administrators to control security policy and encryption keys.

SecureVM also supports encryption of Linux root partitions, folders/directories, and mount points.

SecureVM includes a comprehensive suite of auditing, SIEM integration and key management options to ensure your hybrid cloud workloads can be monitored and secured wherever they reside.

SecureVM is part of the CloudLink data security platform which includes a suite of encryption modules, including CloudLink SecureVSA for vCloud Air, to protect workloads at multiple layers to help secure business applications, hosted desktops and file shares—all provisioned and managed from a centralized hybrid cloud management console.

Embrace the Cloud with Confidence

CloudLink SecureVM enables you to embrace the cloud with confidence. To learn more about how vCloud Air and SecureVM provides unmatched ease of deployment and management of data encryption for your hybrid cloud, visit the CloudLink SecureVM marketplace and get started with a free SecureVM trial today!

www.cloudlinktech.com/vcloudair

Data Encryption for your VMs

VMware and CloudLink enable you to seamlessly extend to the cloud, and ensure your virtual machines and data remains secured and under your control.

“Cloud security is a top priority for many enterprises. Cloud security solutions must leverage the enterprise’s existing data security technology and operational expertise. CloudLink SecureVM unlocks native OS encryption with a centralized management approach that allows IT management, cloud architects, security teams and CISOs to have control over when and where their VMs and data are run and accessed. Together, VMware and CloudLink enable you to confidently adopt vCloud Air knowing that your data will remain secure and regulatory compliance requirements will be met.”

—Alex Berlin, CEO of CloudLink

www.cloudlinktech.com/vcloudair