Product Brief

SecureDoc CloudVM for Azure

Key Management & Encryption for Microsoft Azure Virtual Workloads

- Unified Encryption Strategy across Cloud and Endpoints
- High Performance Persistent Encryption and Fast Conversion
- Smart Policy and Engine Enforcement

Don't expect your Cloud Provider to protect your corporate assets

Security is a top concern for companies looking to deploy a cloud strategy, but there are ways to reduce the worry.

Organizations can and should adopt security provisions that are designed specifically to protect cloud applications, data and workloads, and meet all necessary compliances.

Granular Control

Geographic: manage allowable cloud regions

Time-based: manage rules around date and time patterns

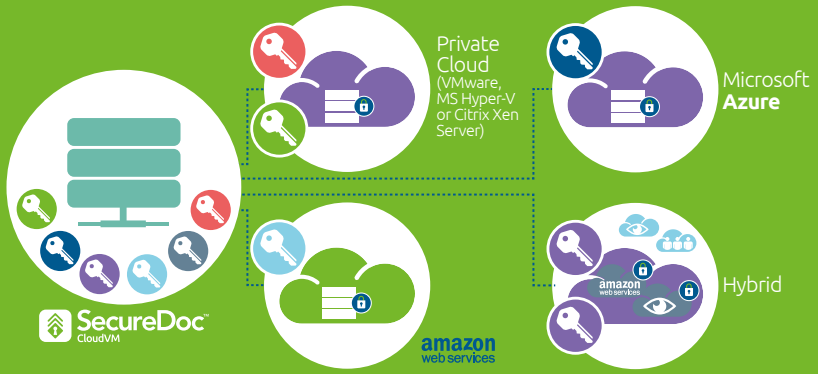
Clone: manage clones from Golden image, and set number of clones permitted

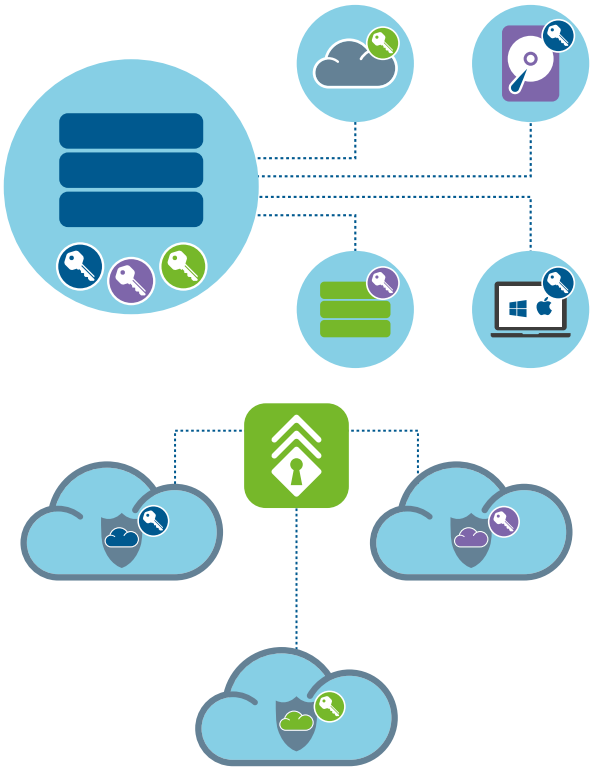
Customer Controlled On-Premise Key Management

SecureDoc CloudVM is WinMagic's comprehensive and sophisticated full disk encryption and volume encryption solution and intelligent key management for all your Azure virtual machines. Powered by WinMagic's application-aware Intelligent Key Management, it ensures that your volume and full disk encryption keys are in full and exclusive control of your organization at all times - while protecting data in your private, public and hybrid cloud environments. Fabric Admins have no ability to read or access data in your memory or disk at any time.

SecureDoc CloudVM enables a unified encryption strategy across any end point, virtualized or cloud IaaS environment. SecureDoc's common platform offers organizations less complexity, more flexibility, and higher security, without cloud platform lock-in. The solution increases visibility and strengthens data security within virtual environments by controlling the encryption key management system across a vast array of layers including: endpoints, file servers, virtual servers, enterprise file sync and share (EFSS) solutions and Internet of Things (IoT) instances.

SecureDoc CloudVM's smart policy & engine enforcement extends granular policy and support for all cloud automation requirements. Organizations can restrict or allow keys required to boot subject to a number of conditions including geographic, time-based and cloning.





Unparalleled Conversion Times

With SecureDoc CloudVM, IT Administrators can configure profiles, installation and deployment settings, and create a download package through a web console without relying on a Windows console.

Multiple help desk administrators can be provided access through the web without having to install the Windows console application.

Persistent Encryption & High Performance

WinMagic's SecureDelete ensures that your data is secured when you're finished with your virtual instance by removing the key and thus preventing any future access to the data. The solution also ensures adherence to an organization's power off policy.

With SecureDoc CloudVM, organizations can be confident that workloads remain encrypted from inception to completion. Persistent Encryption prevents the unintended creation of plain text copies of encrypted files, regardless of where they are created.

With SecureDoc CloudVM there is no need to decrypt and re-encrypt when VM/volumes are cloned, moved, or replicated. The solution also aids and supports Auto Scaling, Duplication, Clone, Migration, Backup, High Availability, and Disaster Recovery Support.

Authenticate VMs through a remote management server

With SecureDoc CloudVM, the server makes the decision to boot (or not) based on the server policy for your organization as defined by the administrator. The encrypted VM pre-boot will check against a remote key management server for authentication before granting access to your data.

SecureDoc Pre-Boot for the Cloud

SecureDoc CloudVM offers the utmost flexibility for customers seeking secure pre- boot authentication solutions. Authentication and authorized key distribution takes place prior to workloads being deployed to ensure that only authorized individuals are accessing your data from an expected place and device. Through SecureDoc's Server Policy Engine, the authentication process is completely automated - freeing your resources to undertake other tasks in their workflow.

SecureDoc's policy engine ensures that snapshots, replicated, or cloned VMs are authorized and authenticated by the SecureDoc server before booting. This ensures no clone machines exist without proper encryption and associated keys.

SecureDoc by WinMagic

System Requirements

Cloud Platforms:

- Microsoft Azure
- Amazon EC2
- Microsoft HyperV

Server Platforms:

- Server 2012 R2
- SQL 2014

Client Platforms:

- Windows Server 2012R2
- Windows Server 2012
- Windows Server 2008R2
- Windows Server 2008
- Ubuntu 14.04.3
- RHEL 7.2

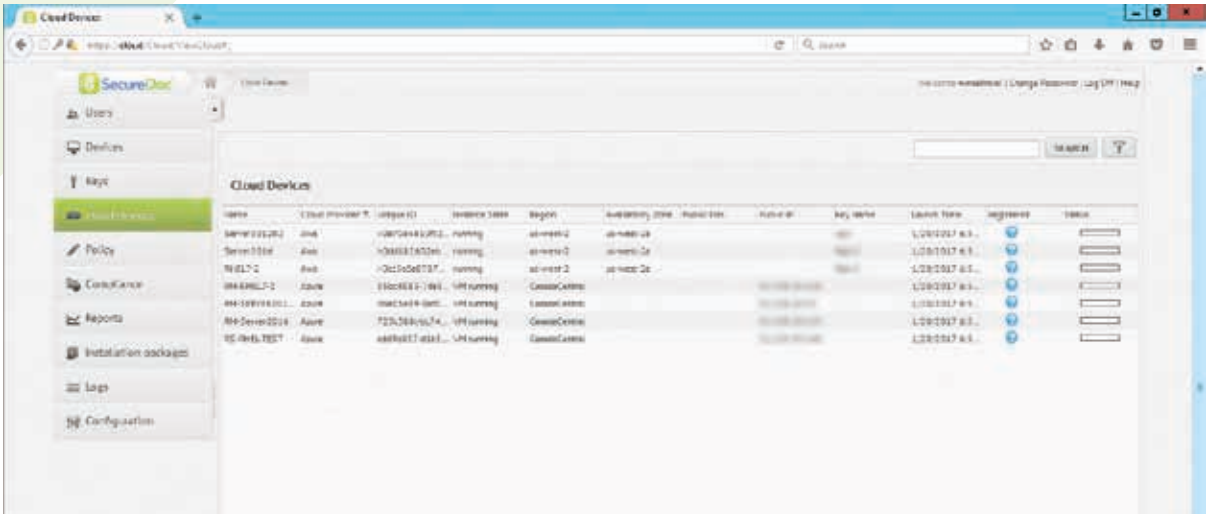
Remote Management for Compliance & Auditing

With SecureDoc CloudVM, there's no more guessing if your Azure VMs are secured. IT Administrators receive full remote management and deployment capability via the SES console, enabling them to import all VMs from public cloud providers and simultaneously view all cloud instances, with positive identification of which VMs are secured.

Instant visibility in an easy to read dashboard helps verify compliance across numerous security standards with auditing tools that report on each instance secured.

SecureDoc CloudVM has the capability to seamlessly sync cloud devices from the private and public cloud providers (AWS and Azure) at a desired interval. A "sync interval" configuration option allows SES administrators to set the sync interval value (in hours) to update the cloud device standards.

Management Portal Snapshot



Authenticate. Encrypt. Achieve.