Product
Brief

SecureDoc CloudVM

Enterprise & Policy-based Control for Virtual Workloads

- Protects Cloud IaaS workloads, data, and DevOps environments against breach
- Enables Fast Online and Offline Conversion
- Supports and Facilitates Compliance
- Simplifies Deployment & Daily Administration

Product
Brief

You can't defer the responsibility to protect your data

Ultimately, enterprises are responsible for protecting their own data and workloads in the cloud. The best way to do that is with a third party encryption solution that encrypts your data wherever it is in your virtual environment, and ensures that only you have the keys.

Time, money and effort spent trying to manage multiple data security solutions is time not spent on growing your business.

WinMagic understands this, and have leveraged all the strengths we've built into our endpoint encryption to create SecureDoc CloudVM - a flexible and high-performance data security solution that protects virtualized or cloud workloads and data against undisclosed government access, malicious insiders, or intrusion by external parties. SecureDoc CloudVM is a perfect match for enterprises seeking greater control and certainty over their data security regardless if a VM is active, or has been deleted, or wherever it is in the DevOps cycle.

Protect Your Data against Undisclosed Government Access or CSP Insider Threats

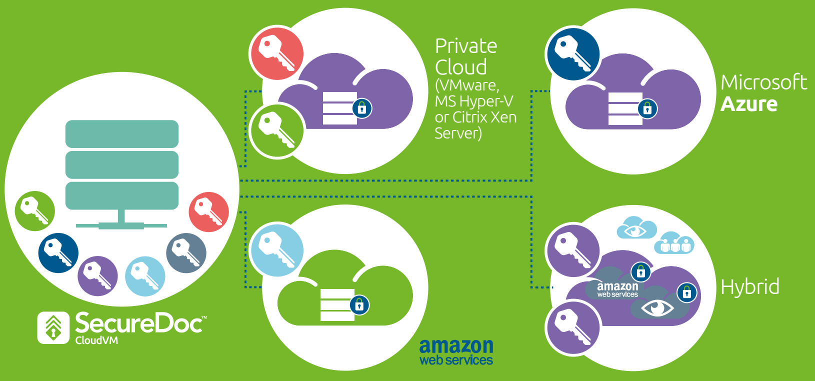
Emerging hypervisor vulnerabilities create a security gap. So why leave keys open to theft or transfer of authority? With in-guest (client-side) encryption provided by SecureDoc CloudVM, the encryption management is decoupled from the hypervisor, meaning that keys and data are never exposed to Government Agencies or dangerous Insiders. Furthermore, if there's a breach at your cloud solutions provider's facilities, your encrypted data and keys won't be compromised. **Now that's peace of mind you can trust**.

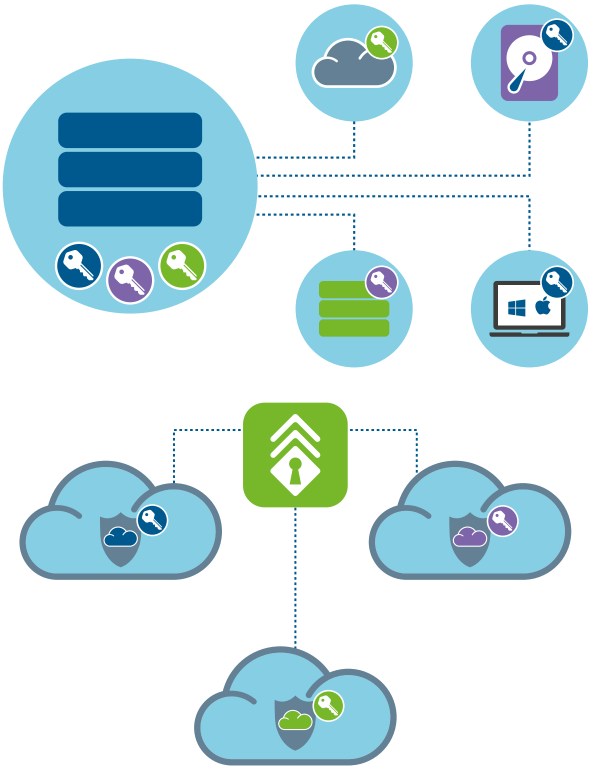
Granular Control

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





Pre-Boot Protection for the Cloud

SecureDoc CloudVM offers the utmost flexibility for customers seeking secure pre-boot authentication solutions. 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.

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 clone VMs are authorized and authenticated by the SecureDoc Enterprise Server before booting.

Guarantee Fast & Responsive Performance

Competition is fast and furious, and time to market is one of the staple benefits of the cloud. So don't let heavy encryption processes stand in your way. SecureDoc CloudVM encryption software integrates easily with existing encryption technologies and VMs in a fast and seamless manner. SecureDoc CloudVM also provides **the industry's only online conversion for both Windows and Linux**, saving you valuable time and money by allowing encryption while the VM is active and in-use, or when offline, not forcing you to turn down or wait for your VMs to complete encryption. Additionally, by enabling quick encrypt - encrypting only the data on the VM, rather than the full drive - SecureDoc CloudVM saves your business hours in valuable time.

Avoid Vendor, Hypervisor or Hardware Lock-in

Portability is a key attribute of cloud computing, and the Infrastructure as a Service model. So why apply old IT equipment models that lock you in to a single vendor?

WinMagic's intelligent key management and persistent cloud encryption allows you to maximize the benefits of the cloud, shifting workloads and data when and as you see fit. There is no need to decrypt and re-encrypt when VM/volumes are cloned, moved, or replicated. When you're finished with your virtual instance, WinMagic's SecureDelete ensures that your data is secured by removing any and all key materials and authentication components, thus preventing any future access to the data.

Enforce Data Sovereignty & Data Governance Policies

Although audit and compliance functions have always played an important role in data security governance, with cloud services facilitating global data movement, these functions have become even more critical. SecureDoc CloudVM's enhanced granular control helps enterprises meet data sovereignty, data security requirements by tightly defining the operational boundaries of your VMs, and any other parameters such as how your VMs are accessed, shared, cloned or replicated.

SecureDoc™ by WinMagic

Key Features

- Is separated from the Hypervisor, protecting data at breach
- Enterprise control of keys
  - Rapid deployment and revocation of keys
- Pre-Boot Authentication / PBConnex
  - Authenticates VMs through a remote management server
- Policy Engine:
  - Ensures data governance, data sovereignty
  - Prevents against sprawl, and side attacks
  - Restricts clones from booting
  - Ensures Persistent Encryption
  - Provides a single platform, with no silos
  - Permits auto-scaling
- Support multiple subscription IDs from Azure and AWS
- Supports ability to encrypt multiple disks (Volumes) on Linux VM for all supported OS
- Fast conversion, by encrypting data only
- Eliminates portability restrictions
- Supports Online and Offline encryption
- Interrupt-supported Encryption
- Single View via Web Console (SES)
  - Auditing & reporting tools reporting on each instance secured
  - CryptoErase capability
- FIPS 140-2 for Windows

Easily Manage Compliance Efforts

Compliance and audit failure is a top concern for C-Suite executives. WinMagic's SecureDoc CloudVM helps ensure enterprises meet compliance needs by providing user-friendly audit tools to track and report that VMs and data are always in a protected state.

With SecureDoc CloudVM, there's no more guessing if your VMs are secured. Instant visibility through an easy-to-read dashboard helps verify compliance across numerous security standards with auditing tools that report on each instance secured.

Reduce the Burden of Daily Administration

Concerned about what a lack of available skilled resources or the burden on your existing ones is doing to your cloud plans? Overcome these concerns by simplifying the daily administration tasks associated with securing your cloud IaaS environment.

WinMagic's SecureDoc Enterprise Server provides IT Administrators full remote management and deployment capability via the SES console. The simple-to-use console provides the ability to import all VMs from public cloud providers (Amazon Web Services, Microsoft Azure, or others) for management; simultaneously view all cloud instances, with positive identification of which VMs are secured; SecureDelete (CryptoErase) drives when needed; or, even manage user credentials. SecureDoc CloudVM also ensures adherence to an organization's power-off policy, further removing concerns about gaps caused by employees.

Supported Platforms & Systems

Cloud Platforms:

- Amazon EC2
- Microsoft Azure
- Microsoft HyperV
- VM Ware
- IBM Softlayer
- Citrix

Client Systems

- Windows Server 2012R2
- Windows Server 2012
- Windows Server 2008R2
- Windows Server 2008
- Ubuntu 14.04.3 / 16.04 / 16.04.1
- RHEL 7.2 / 7.3
- CENTOS 7.2 / 7.3

Public Gallery

- AWS: RHEL 7.2 / 7.3
- Microsoft Azure: RHEL 7.2 / 7.3

Management Server Platforms

- Server 2012 R2
- SQL 2014