Tech Brief

SecureDoc Encryption and Key Management for Lenovo Data Center & Cloud Infrastructures

Transitioning modern data centers and virtualized environments share a common need – the need for a consistent data security from Bare Metal, to HCI, to Private Clouds Servers and a **Single Solution to Secure it All**.

Unifying Data Security

Encryption is a core requirement in modern data centers and private cloud environments. A rise in breaches has led most data security regulations – like the European Union General Data Protection Regulation (EU GDPR) – to now mandate encryption, versus recommend it as an optional security function.

WinMagic's SecureDoc Enterprise Server (SES) is the only storage, IaaS, HCI and bare metal encryption solution that address ALL of Lenovo's DCG portfolio – from Azure Private Cloud, to Nutanix and Scale HCI, to bare metal x86 servers and beyond. And it's all managed from a single platform:

- **OS-Agnostic:** Windows and Linux servers
- **Hypervisor/Cloud Agnostic:** Microsoft Azure, Microsoft Hyper-V, Amazon EC2 client, Nutanix, Scale Computing, VMware, Citrix
- **SED Management:** TCG Opal & TCG Enterprise Self-Encrypting Drives (SEDs)

Single Key Manager for Lenovo DCG Products

When it comes to key management, WinMagic's SES solution is the best in the industry at unifying key management under a single solution. With FIPS-140-2 certified secure key storage, WinMagic manages a strict set of granular policies established by the enterprise administrators to ensure what authorized devices or VMs can boot and with what keys, the user-based key assignments for any given properties, and the level of rights for individual or group administrators. Through unifying key management, enterprises are able to manage associated encryption keys for any and all use across the organization's platforms under a single view, and single software solution. No more messing around with costly Hardware Security Modules (HSMs, or incompatibilities that disrupt persistent protection of your data).

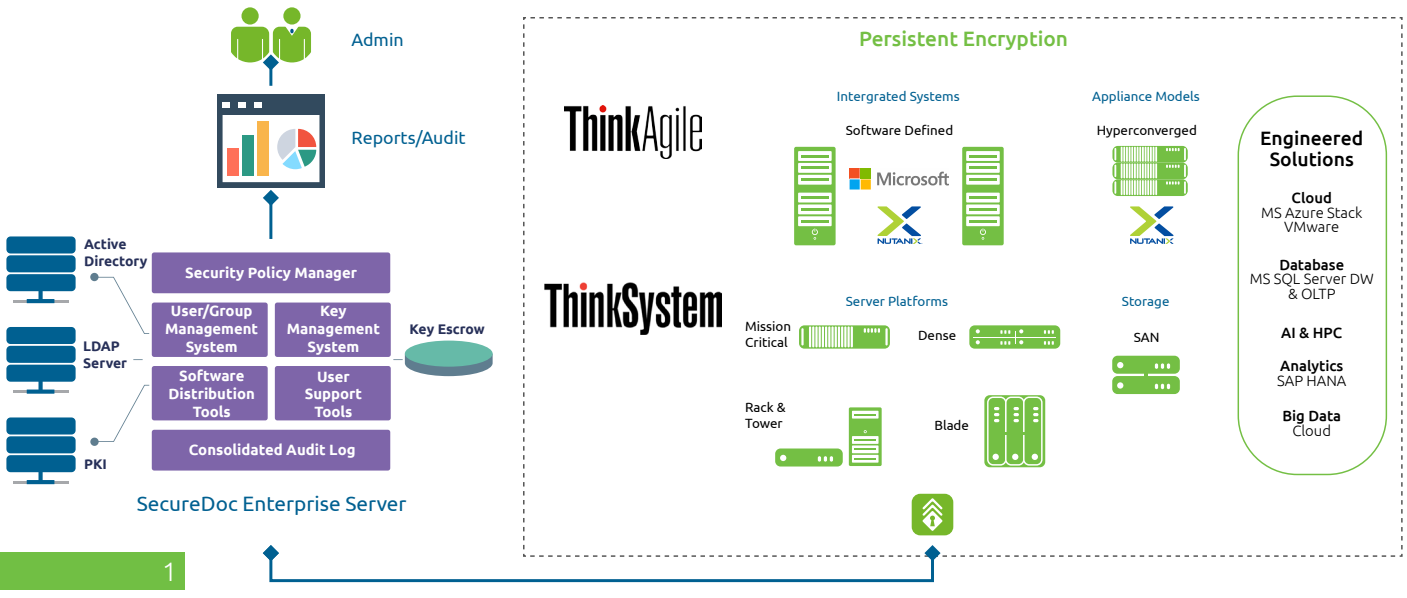
Industry's Highest Performance Encryption

Competition is fast and furious, and time to market is one of the staples to beating the competition. So why let heavy encryption processes stand in your customer's way? SecureDoc CloudVM encryption software integrates easily with existing encryption technologies and VMs in a fast and seamless manner. SecureDoc CloudVM provides the industry's only online conversion for both Windows and Linux, saving valuable time and money by allowing encryption while the VM is active and live, or when offline, not forcing them to turn down or wait for their VMs to complete encryption. Additionally, by enabling quick encrypt – encrypting only the data on the VM, rather than the full drive – SecureDoc CloudVM saves businesses hours in valuable time.

Improve Auditing & Compliance Reporting across DCG all Infrastructure

Compliance and audit failure is a top concern for C-Suite executives, so why keep guessing if VMs are secured? SecureDoc 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, instant visibility through an easy-to-read dashboard helps verify compliance across numerous security standards (EU-GDPR, PCI DSS, NIST, as well as HIPAA, and others) with auditing tools that report on each instance secured.

- Single-view console reduces risk of out of compliance devices
- Central management of all encryption keys and policies
- Simplified reporting & auditing for compliance initiatives
- Fast & comprehensive deployment reduces costs



Tech Brief

Lenovo

SecureDoc™ by WinMagic

Lenovo Servers are designed to run in-memory databases, large transactional databases, batch and real-time analytics, ERP and CRM applications and virtualized server workloads. With that array of capabilities, it just makes sense to have a **single solution that protects it all.**

SecureDoc Encryption as a Platform across the Lenovo DCG Portfolio - from Bare Metal to Cloud

Authentication: Exclusive Pre-Boot Network Authentication via WinMagic's **PBConnex** solution

Key Management: Exclusive Enterprise Control of encryption keys

Compliance Reporting: Single Console for reporting and monitoring across all SecureDoc protected platforms

Data Security for Physical Client Solutions: SecureDoc OSA (Operating System Agnostic) for Servers: Windows, x86, Linux)

- Centrally managed through SecureDoc Enterprise Server (SES)
- Manage TCG Opal & TCG Enterprise Self-Encrypting Drives (SEDs)
- Support Windows, x86, and any distribution of Linux (except hardware RAID)
- Installation is performed at pre-boot which eliminates the need to create an OS-specific installation package, and helps avoid bothersome compatibility issues
- Enable secure remote unattended booting/rebooting of servers via PBConnex – WinMagic's Pre-Boot Network Authentication, before the operating system ever loads – something traditionally impossible for encrypted servers – removing a key pain point for IT administrators

Data Security for Client Virtualization Solutions: SecureDoc Cloud VM

- Retain exclusive control of encryption keys – protecting them in shared environments
- Protect workloads with persistent VM-level encryption of VMs
- Build VM templates with encryption running, or, launch encrypted VMs at the get-go, cutting time-to-market
- Reduce downtime by eliminating the need to decrypt or take VMs offline to complete encryption
- Support ability to encrypt multiple disks (Volumes) on Linux VM for all supported Operating Systems
- Securely terminate individual workloads, not just drives
- Enforce Data Sovereignty and Data Governance Policies with enhanced granular control of VMs; tightly defining how and where VMs are accessed, shared, cloned or replicated
- Easily integrate with other HCI providers like Nutanix, Pivot3 and Scale Computing
- Encrypt VDI instances with SecureDoc for compliance, security automation, and clone management, and secure decommissioning
- Supports Microsoft Azure, Microsoft Hyper-V, Amazon EC2 client., Nutanix, Scale, VMware, Citrix
- For more information on CloudVM Supported Platforms & Systems visit HERE

Servers

ThinkSystem / SystemX

Whether deployed as a bare metal storage server solution, or integrated within a Lenovo-engineered virtualization solution, Lenovo's ThinkSystem x86 servers and SystemX servers already offer a level of protection capable of stopping many data threats.

WinMagic's SecureDoc software integrates easily within Lenovo's **Chain of Trust**, taking SED management and device protection to the next level.

For Think Servers protected by SEDs, **SecureDoc's OSA for Servers solution eliminates the need to create an OS-specific installation package, and helps avoid bothersome compatibility issues** – simplifying data security.

Hardening the authentication process for SEDs, WinMagic's Pre-Boot Network Authentication solution, **PBConnex** enables secure remote unattended booting/rebooting of servers before the operating system ever loads – something traditionally impossible for encrypted servers – removing a key pain point for IT administrators.

- Transparent to users, with little to no performance impact
- Simple and secure integration, with interoperability across solutions that include ThinkSystem as well as others
- CryptoErase drives as needed
- Encryption status of all ThinkSystem servers can be monitored in a unified view with other DCG solutions on WinMagic's SES

FlexSystems

Lenovo's Storage DX Series appliances were designed to provide a single storage management user interface to simplify third-party storage virtualization. And, virtualized storage needs a data security solution that can protect data as it moves.

SecureDoc CloudVM easily integrates with Lenovo DX Series appliances, providing persistent VM-level protection for synchronously & asynchronously replicated data, no matter what state data may be in – active, live, offline or at rest. Customers don't even need to worry if the snapshot or clone resides on a self-encrypting drive, because it is already encrypted wherever it goes.

- If protecting the drives with an SED, SecureDoc's OSA for Servers solution eliminates the need to create an OS-specific installation package, and helps avoid bothersome compatibility issues – simplifying data security.

Storage

DX Series

Lenovo's Storage DX Series appliances are designed to provide highly efficient, high-capacity storage to meet the needs of quickly scaling data. And that data typically comes with a need for high performance, geographic and geo-control restrictions.

Enterprises can't risk failing data protection regulations, like EU-GDPR. SecureDoc attaches easily to Lenovo's DX Series appliances, providing persistent VM-level protection against data threats wherever that data may within the customer's environment.

- Enforce Data Sovereignty and Data Governance Policies with enhanced granular control of VMs; tightly defining how and where VMs are accessed, shared, cloned or replicated

Software-Defined Storage/Infrastructure

ThinkAgile SX for Azure

Where the ThinkAgile SX for Microsoft Azure Stack hybrid cloud offering keeps data secure in your data center, SecureDoc attaches easily to the solution, providing persistent VM-level protection against data threats wherever that data may go, including outside of the stack.

- Granular policy control
- Greater protection for VMs as authentication occurs via remote management server, before the VM ever loads
- Key manager can be assigned as a virtual appliance in Cloud Service Provider marketplaces
- Supports multiple subscription IDs from Azure and AWS
- Licenses available in

Think Agile SX & HX for Nutanix

SecureDoc CloudVM, a Nutanix AHV certified solution, allows enterprises to fully encrypt virtual servers and data at the VM-level within Nutanix's Acropolis HyperVisor.

SecureDoc Cloud VM provides persistent protection against data threats.

- Support movement of VMs from within Nutanix Clusters, or to any cloud
- Add transparency to cloud operations.
- Protects High Availability, Cloning & Duplication of snapshots
- Pre-boot authentication, controlling access and authentication of new workloads before use
- Support multiple subscription IDs from Azure and AWS
- Encrypt multiple disks (Volumes) on Linux VM for all supported OS, with no compatibility issues

NUTANIX READY • AHV •

SAP HANA

Lenovo's solutions for SAP HANA were designed to allow customers to easily create multi-node, networked, scale-out configuration, also allowing for integration of high availability with automatic failover. This modular approach eases scalability, but can present challenges when it comes to securing data as it moves within and outside of the environment.

SecureDoc CloudVM integrates easily with Lenovo's SystemX and ThinkSystem and platforms to protect data wherever it may reside.

Support movement of VMs from node to node, or to any cloud

- Separated Key Management for exclusive enterprise control
- Variable licensing model to meet the burst needs of the SAP HANA solution

READY TO DELIVER A SECURE, COMPLIANT AND UNIFIED DATA SECURITY SOLUTION FOR YOUR CUSTOMERS? GET STARTED TODAY

WinMagic is committed to Lenovo and its' customers' success. We offer data security solutions that can cover them from endpoints, to data center, to the cloud. To get started with unifying your customers' data security efforts, email your WinMagic representative today.

WINMAGIC®

US & Canada +1 888 879 5879 | **United Kingdom** +44 0148 334 3020 | **Germany** +49 69 175 370 530 | **Japan** +03 5403 6950 | **India** +91 124 4696800 | **APAC** +65 9634 5197