

Protecting VDI in the Datacenter With SecureDoc

Secure your transition from Physical to Virtual Desktops

- Transparently encrypt data across VDI deployments
- Securely decommission VDI workloads
- Prevent insider theft or malicious access



Desktop virtualization deployment will continue to grow through 2020 as organizations seek to deliver business applications to the digital workspace.”

Desktop Virtualization Is Foundational to Building a Digital Workplace – Gartner (May 2017)

Hyperconvergence is driving VDI adoption

Emergence of the Software-Defined Data Center (SDDC) and Hyper-Converged Infrastructure (HCI) have quickly reduced previously high storage costs, and enabled businesses to deliver high performance with radically simplified infrastructure management, ideal for VDI.

As enterprises extend virtualization from servers to desktops, traditional endpoint security threatens to reverse the performance benefits of VDI. Furthermore, plans for virtualization are thwarted by compliance requirements for mission-critical workloads, which the base virtualization platform is not designed to meet.

Where does compliance fit in?

As privacy awareness grows among consumers, businesses must comply with rapidly evolving data security and privacy regulations. When it comes to encryption, the text is clear:

PCI DSS

The Payment Card Industry (PCI) Data Security Standard mandates protection cardholder of data including encryption wherever it is stored, even in the datacenter.

HIPAA-HITECH

Protected health information (PHI) must be encrypted to securely dispose data and provide safe harbor from data breaches and the penalties that ensue.

EU GDPR

The new EU General Data Protection Regulation (GDPR) also mandates the use of encryption to protect personal data, particularly in datacenter and cloud environments.

Desktop to Datacenter.

As enterprises migrate from desktop to datacenter, IT teams can now support more workloads and more users faster than ever before.

Simplify Management – Desktops hosted in the datacenter help IT to isolate and centrally manage images, applications and user data.

Increase Mobility – VDI isn't just for IT; it also helps your users access their workspace from virtually any device anywhere.

Reduce Costs – Less computing on the endpoint extends device lifecycles and enables IT to deploy much cheaper, less powerful thin clients.

The Security Question.

Another key benefit of Virtual Desktop Infrastructure is that – in most cases – only a screen image of the VDI workload is sent to the endpoint device, not the data itself. That way, businesses significantly minimize the risk of data breach if a device is lost or stolen. However, let's think for a moment about where that data resides now. Datacenters host a blend of assets, including virtual machines, desktop images, snapshots and clones, and storage systems for user data.

Data Sprawl Dilemma

As business migrate from physical to virtual, endpoint data has moved from a single hard drive to multiple points across the datacenter. Even more, a virtual machine is just a file, simple to copy, move and access. Controlling where your workloads reside and who has access becomes especially difficult in hybrid and distributed cloud infrastructure.

Compliance Pressure

Today enterprises face multiple data security and privacy rules, including the new EU GDPR, PCI DSS and HIPAA. As a baseline, these regulations require that confidential information – whether PHI or PII – be protected wherever it is stored, including the datacenter and cloud infrastructure.

Performance Bottlenecks

The most obvious issue with any security solution for VDI deployments is performance. Unlike servers, user demand can result in excessive compute and storage consumption. Encryption is a necessary, but naturally disruptive technology, particularly as VDI instances boot.

Protecting VDI in the Datacenter.

Virtualized platforms are the latest frontier for security exploits as cybercriminals discover new ways to target infrastructure, systems and confidential data.

Encryption is the foundational last line of defense to ensure that, even if an intruder circumvents your perimeter, they cannot gain access to your data without the proper encryption key.

SecureDoc for VDI

Encrypt VDI Workloads

SecureDoc offers the ability to encrypt VMs running persistent and non-persistent VDI desktops with FIPS 140-2 certified protection.

Always-On Encryption

VM-level encryption protects VDI workloads wherever they reside, even as they move across different platforms, hypervisors and hardware.

Protect User Data

Use SecureDoc File Encryption (SFE) to isolate and control user access to files stored on the virtual desktops or in a network file share.

Deploy Within Minutes

SecureDoc is quick to install and deploy. Simply create an encrypted master image to deploy across your desktops – pooled or personal.

Prevent Insider Threats

Even if an insider gained access to a VM, the data is unreadable and unusable without access to key management.

Securely Decommission Workloads

Remotely revoke or destroy the key to securely dispose desktop VM images, virtual disks and all related data when it is ready to be retired.

Build Your Enterprise Encryption Strategy.

Our industry-leading encryption solutions are great on their own, but even better as a platform. WinMagic offers a unified approach to protect your data across endpoints, datacenter and cloud workloads – all delivered from a single, unified key management platform.

Questions? Get in touch with us at <https://www.winmagic.com/contact>.

SecureDoc for VDI

Key Features:

- FIPS 140-2 validated Full Disk Encryption for desktop VMs
- Transparent File Encryption for defense-in-depth
- Less than 3% performance impact on VDI workloads
- Fast, transparent boot authentication
- Manage keys and policies via SecureDoc Enterprise Server
- Monitor and audit compliance with a single pane-of-glass

Supported Platforms:

- VMware Horizon
- Citrix XenDesktop

Authenticate. Encrypt. Achieve.