

CXO

SECURITY
BRIEFING

Simpler together

Unified data security for your
hyper-converged future

 **SecureDoc**[™]
by WinMagic

 **WINMAGIC**[®]

Forward-thinking CIOs are moving towards a simpler future

Data challenges are evolving, fast. CIOs charged with delivering transformative new levels of efficiency and scale are looking towards a converged IT future, and ready-to-roll Hyper-Converged Infrastructures (HCI) are leading the charge. These deliver an agile public and private cloud vision in one, freeing organizations to deploy systems within minutes, scale up easily with modular building blocks and integrated infrastructure, and manage specialist VM environments with generalist IT teams.

Security is the final frontier

IT leaders have held back from deploying the well-documented benefits of convergence because of ongoing data security concerns. In an era complicated by growing compliance demands and morphing cyber threats, they are right to be anxious.

The good news is that a new kind of unified security approach can mitigate security risks and compliance stress, in one. What's needed are security tools built from the ground up to deliver continuous and continuous encryption across all physical, virtual and cloud assets. Security which is guaranteed compatible with any type of hypervisor technology and is ready to scale, regardless of how many nodes are added to a converged environment. That's exactly what proven encryption specialists can now deliver.

This paper is aimed at CIOs poised on the verge of a visionary new converged infrastructure strategy, but nervous about taking the next step. It shows how progressive IT leaders are already delivering end-to-end converged solutions protected by continuous encryption to secure both their endpoints and their virtualized and hybrid cloud environments. Straightforward, scalable infrastructures, supported by straightforward and continuous security: simpler together.

You'll learn how this kind of unified security approach is freeing organisations to build simply secure, compliant and unified hyper-converged IT systems, with intelligence applied to encrypted workloads. So, CIOs and data centre leads can remain in control of data security while being freed to build an agile Anywhere Enterprise.

HCI is coming: the time to investigate a simpler security approach is now

The Gartner Magic Quadrant for Integrated Systems dated October 2016 states that hyper-convergence is disrupting the integrated system market. It also makes the following Strategic Planning Assumption: "By 2019, approximately 30% of the global storage array capacity installed in enterprise data centers will be deployed on software-defined storage (SDS) or hyperconverged integrated system (HCIS) architectures based on x86 hardware systems, up from less than 5% today. Twenty percent of mission-critical applications currently deployed on three-tier IT infrastructure will transition to HCISs by 2020." That makes taking a look at a new, unified security paradigm a vital and pressing first step.

Continuous, everywhere encryption: taking you from vision to viable.

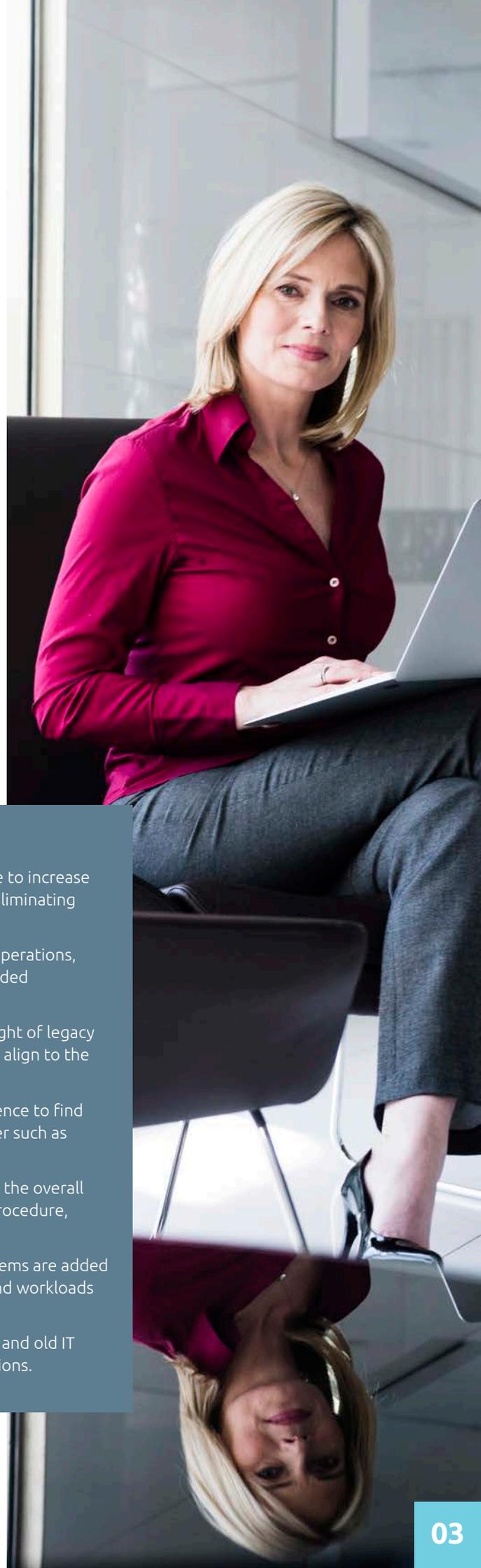
Hyper-convergence essentially gives you a visionary 'datacenter in a box' – leveraging web-scale engineering and design to converge compute, storage, networking, and management software into a single resilient, software-defined solution with rich machine intelligence.

This kind of converged approach is popular because it makes infrastructure practically 'invisible', liberating IT teams to focus their skills and energy on the important applications and services that power their business. They can rapidly deploy mixed-workload and virtual desktop integrated infrastructure solutions across local or remote locations, better manage storage and enjoy unrivalled flexibility when it comes to deploying IT resources and creating private VMs.

A unified, turnkey security approach makes it all viable

The security and data governance concerns that dog IT leaders are as real as the penalties for data breaches and non-compliance that hang over them. So how does a simplified security approach powered by a continuous, everywhere encryption strategy make the benefits of convergence not just technically possible, but also strategically viable?

Keep reading to find out.



Business needs driving the convergence vision



Increasing efficiency: IT departments are under growing pressure to increase the efficiency of technology, systems and users – and that means eliminating IT silos



Time management: Businesses are looking to shed traditional IT operations, pro-longed product evaluation and integration processes or extended return-on-investment metrics that no longer work.



Matching skills to tasks: IT staff are being crushed under the weight of legacy infrastructure, and struggle to add IT staff with technical skills that align to the new applications and systems.



Resource management: Businesses are turning to hyper-convergence to find better ways to manage existing and future needs of the data center such as space, power, and cooling.



Meeting budgets: They are also seeking to improve their focus on the overall scale of all the resources they command as a standard operating procedure, rather than on individual components.



Reducing risks: Unfortunately, as more diverse hardware and systems are added to an IT environment, achieving the critical goal of securing data and workloads becomes more difficult.



Improve agility: Today's commerce markets are cut-throat places, and old IT issues can't be allowed to get in the way of critical business operations.



Why unified, continuous encryption is needed, right now

By deploying the right unified encryption and intelligent key management security solution across endpoints, virtualization and Cloud IaaS, IT leaders can simplify their security stance and alleviate operational pressures while mitigating compliance and cyber-attack risk. Add in the benefits of industry-leading SecureDelete, which encrypts data and renders it useless in the event of a breach by removing credentials and keys, and security finally stops being a limiting strategic factor.

Unlock future advantage

1 Reduce compliance pressures

Data security and privacy regulations are quickly evolving. With EU GDPR mandating the use of encryption – organizations face not just stiff but potentially lethal fines, penalties and brand damage without it. The penalties could paralyse a mid-size enterprise or even shut it down. Fines for non-compliance reach up to 4% of global revenue or €20 million, and penalties extend to a temporary ban on operations. PCI DSS, SOX, HIPAA-HITECH, FISMA and FedRAMP also loom large over the convergence ambitions of enterprise leaders.

2 Tackle growing data breaches

Data breaches resulting from lost or stolen devices, compromised cloud resources, and unauthorized access to or exposure of keys are on the rise. Encryption is your first line of defense if a perimeter is compromised. According to Gemalto's Breach Level Index, over 9 billion data records have been lost or stolen worldwide since 2013. Only 4% of breaches were 'secure breaches' where encryption was used and the stolen data was rendered useless.

3 Cut spiralling ownership costs

Think user downtime, IT frustrations and helpdesk overload. The cost of running today's increasingly complex and silo'd IT environments is exorbitant. IT leaders need solutions designed to deliver robust security in a seamless model without introducing a performance overhead or unexpected costs down the line.

4 Combat untenable management complexity

There's no point converging to simplify your infrastructure management and then being left with a complex multi-OS encryption key and security policy environment to run. Add in native and hardware-based encryption solutions, and security management quickly becomes a daily nightmare. To really enjoy the benefits of a dramatically simplified, converged infrastructure strategy, you need one dramatically simplified and unified security console to manage it all.

[Dive into the technical detail overleaf.](#)

Unified security for a simplified future

Rolling out one robust, validated encryption and encryption management solution for virtualized workloads and any hypervisors delivers a simple route to new era agility, cost and compliance control.

Intelligence can be applied across encrypted workloads and combined with scalable key management spanning a multi-platform IT environment, simplifying security at root. As a result, organizations can stay in constant control of data security across their converged infrastructure – protecting it against data loss or breach, unapproved copying and snapshots, relocation, public cloud exploitation and other threats, and keeping VM workloads compliant.

Importantly, when an IT team is finished with virtual instances, powerful functionality by WinMagic ensures that data is secured by removing the encryption key, preventing any future access to it. This gives administrators visibility and control from image to server stand-up, while delivering end-to-end auditing and compliance confidence at a management level.

- Protect VMs in-transit from clusters to any cloud
- Support High Availability (HA) and minimize downtime with multi-platform key management
- Control access to new and existing workloads with secure pre-boot authentication

Strengthen compliance

SecureDoc CloudVM from WinMagic helps ensure that enterprises stay compliant by providing user-friendly audit tools to track and report on the always-protected state of VMs and data within a converged environment. It's the simple way to enforce and monitor compliance with centralized dashboards and actionable security intelligence to prevent non-compliance and assist with audits.

- Meet data sovereignty and other data security requirements
- Enjoy enhanced granular control, tightly defining how VMs are accessed, shared, cloned or replicated (time, geolocation, duplication, etc.)
- Control and audit access to encryption keys to easily prove compliance and minimize risk

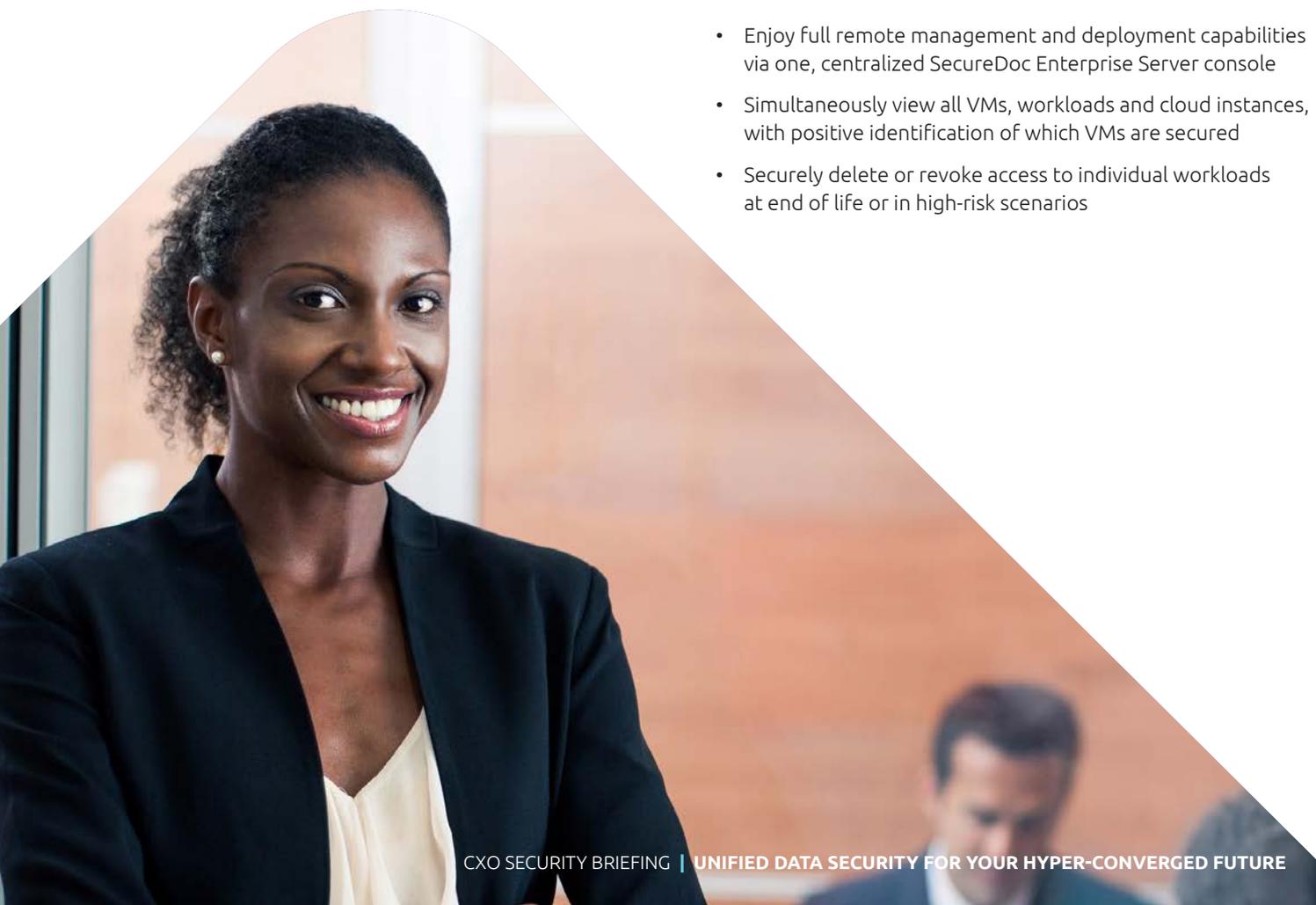
Ease scalability

When it comes to virtualization, scalability is key. SecureDoc CloudVM supports scalability requirements with easily deployable encryption licenses and multi-node key management for failover and high availability supporting your growth or burst needs regardless of the speed or scale of change.

Reduce Operation and Time Costs

Why waste critical IT resources? WinMagic can help IT Administrators to reduce daily workloads and TCO by simplifying IT management and delivering seamless deployment, authentication, and recovery processes.

- Enjoy full remote management and deployment capabilities via one, centralized SecureDoc Enterprise Server console
- Simultaneously view all VMs, workloads and cloud instances, with positive identification of which VMs are secured
- Securely delete or revoke access to individual workloads at end of life or in high-risk scenarios





A new approach for a secure new converged era.

Why do some of the world's most respected convergence vendors like Nutanix and Scale Computing partner WinMagic to deliver an always-on, end-to-end encryption solution for building and securing virtualized and cloud environments?

Integrated

Strategic partnerships with some of the world's biggest technology organizations like HP and Lenovo are matched by our track-record of developing and distributing unmatched data security solutions, built around partnerships with recognized OEMs and innovation leaders.

Respected

We're one of the most respected names in the security industry, recognized as a leading innovator in encryption and key management for 20+ years and counting.

Certified

Our advanced crypto technology is validated against the highest standards in security, including FIPS 140-2, Common Criteria, and OPSWAT.

Trusted

We're trusted by a global network of more than 2,500+ diverse customers from government to the enterprise and everything in between.

Start building a business case for IT convergence.

Talk to the experts at WinMagic. We can walk you through the next steps, review your operation and even conduct a free expert risk review on request to help you map a path to secure converged IT.



info@winmagic.com | www.winmagic.com

 **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 Singapore
+65 9634 5197