SecureDoc™
by WinMagic

CXO
BRIEFING

I am unified.

How progressive CIOs and CISOs are unifying data protection once and for all, across any cloud, anywhere, any time.

I am unified.

Finally, my IT infrastructure can move securely at the speed of my business.

New unified thinking.

In a recent Research Note, Gartner made the following Strategic Planning Assumption: “Through 2020, 95% of cloud security failures will be the customer’s fault.” *Jay Heiser, Gartner Research Note, July 2016: Clouds are secure, are you using them securely?*

Will you be part of that statistic? In this new data privacy era, with stern new EU Global Data Protection Regulations (GDPR) just around the corner, the security buck stops with your organization. The strategic data protection choices you make over the next year will make, or break, your success over the next decade. 64% of enterprise respondents to a wide-ranging IDG survey say that they have concerns about the security of cloud, with that number rising to 69% as the size of a business diminishes.[1] Of course, they are right to be worried.

The big question is: how can you confidently keep enjoying the unrivalled TCO and flex that cloud offers while keeping your critical corporate data secure and compliant? Time, money and effort spent trying to manage a complex tangle of data security solutions is time not spent on growing your business. Complexity also makes your chosen data protection strategy more expensive and open to failure.

That’s why WinMagic has leveraged all the strengths built into our industry-defining endpoint encryption solution to create a unified, any cloud approach fit for the new era. It’s built around our flagship, progressive cloud security solution called SecureDoc CloudVM.

This new solution reimagines how cloud security works, radically simplifying and fundamentally strengthening it with a unified new approach that centres around policy-based key management, enterprise control and high operational performance. It’s designed to protect all your virtualized and Cloud IaaS workloads against major threats. Any cloud. Anytime. Anywhere. No data silos or complex shifting between platforms; everything just unified.

It’s the easy way to get the cloud security conundrum cracked. Once and for all.

[1] 2015 IDG Enterprise Cloud Computing Survey

Strengthen data protection **in one**.

In the new security era, *Shared Responsibility* is every IT team's mantra. Because while all third-party cloud providers carefully secure their cloud perimeter and infrastructure, they universally push the responsibility for security of data *within* the cloud back to customers like you.

Does your Cloud provider have strict policies about keeping your data kept separate from other client's data in a multi-tenant environment? Who exactly can actually access your data? Do you trust their security and authentication procedures? What about their staff? What's your appetite for risk?

If, like most CIOs and CISOs, you have a low risk appetite, then you need a sure-fire strategy for success. A way to protect your data and workloads in the Cloud with an enterprise-controlled encryption solution that ensures *only you* have the keys. That way, if there's a breach at your cloud solution provider's facilities, your encrypted data and keys won't be compromised.

Our new unified data protection approach achieves just that. It rewrites the rules of security with a new breed of client-side encryption which uniquely separates encryption management from specific clouds, workloads and the hypervisor. This critical design change transforms cloud security by separating hypervisor security exposure from data exposure and stopping vulnerable encryption keys being left open to theft or the transfer of authority.

Protect against three key threat vectors

Adopting this approach frees you to defend and protect all your virtualized and cloud workloads against the three key threat vectors: undisclosed government access, malicious insiders or user error within your cloud provider or your own business and intrusion by external parties.

- **Protect against undisclosed Government Access:** Enterprise-controlled authentication stops keys and data being given to Government Agencies or other authorities without your knowledge and mandate – so you stay in charge of your data, at all times. This is important in these times of increasing legislation and well-intended top-down intervention.
- **Safeguard against privileged insiders:** These are often the most dangerous threat agents, working either with your Cloud provider or within your own admin team, capable of causing huge damage through clumsy mishandling or deliberate mischief.
- **Prevent intrusion by third parties:** Public cloud providers are a target for hackers and even private clouds aren't impervious to attack. A staggering 7,094,922,061 data records have been lost or stolen since 2013 according to BreachLevelIndex.com and only 4% of those were 'secure breaches' where encryption was used to render the stolen data useless.

Granular visibility and control are yours

Thanks to an automated pre-boot authentication feature, the SecureDoc VMCloud server can choose to boot– or not – based on policies you define, with snapshots, replicated, or clone VMs also requiring authentication before booting. This entirely unique authentication feature prevents malicious client-side attacks, VM sprawl and rogue copied VM instances. Each VM also carries with it an audit and compliance report detailing when it was created, by who and if it was secured or not. So now, if there's a security breach at your public cloud facility, your encrypted data and keys won't be compromised. You're free to pursue the cost and agility advantages of a public, private or hybrid cloud strategy.

Get compliance ready **in one.**

A perfect storm is brewing, with cloud services smoothing and facilitating the global movement of data at the same time that data privacy regulations evolve and become much more financially punitive.

To take one imminent example, on 25th May 2018 new EU GDPR regulations pass into law. These will apply to any organization handling the personal data of EU citizens and non-compliance could mean big fines - up to the greater of 20 million Euros or 4 per cent of annual turnover. This increase in data security and data privacy penalties means that CISOs are becoming increasingly pre-occupied with compliance: both how to deliver it and how to demonstrate it.

What if you could monitor and control your whole data universe?

A new unified approach can help you gain the controls and auditability you need to comply with internal policies and mandates and stay compliant with data security and privacy regulations across all of your Cloud IaaS deployments: public, private or hybrid. It can give you instant visibility across your data universe with user-friendly, policy-based audit tools and reports alongside an easy-to-read dashboard that lets you track the exact protection status of all your cloud and VM workloads. You can also monitor other key parameters such as how your VMs are accessed, shared, cloned or replicated, helping you ensure data governance and sovereignty.

Enhanced granular control and tightly defining the operational boundaries of your VMs will help you to ensure that each individual's data is kept within their resident country: a key mandate of EU GDPR. The SecureDoc CloudVM solution will also help you enforce data sovereignty rules by ensuring that no VM boots up in an unauthorized data center.

You'll be supported to adapt to the evolving compliance demands of your sector too, efficiently fulfilling the requirements of EUGDPR, PCI DSS, HIPAA and SOX and whatever's around the corner while protecting data to US Government grade FIPS 140-2 standards across your Windows environment.

I am unified.

Compliance is virtually automated.

It's the perfect solution for tough regulatory times.

Radically simplify operations **in one**.

In today's furiously competitive global marketplace, time to market is one of the key ways that you can win. Many IT leaders are rightly concerned about customer-facing innovation projects getting postponed or shelved due to a lack of available skilled resources and the security management burden on existing IT teams and budgets.

By simplifying the daily administration tasks associated with securing your cloud IaaS environment, you'll significantly lighten cloud management loads, so you can focus resources back on business growth. Benefits like remotely managing encryption and deployment, easy CryptoErase drives and managing user credentials through our SES WebConsole can save significant people hours. SecureDoc CloudVM helps you simplify it all:

- **Quick and easy management.** Our unified, policy-based, highly automated admin approach managed through one user-friendly console streamlines deployment, day-to-day management and reporting.
- **Zero disruption.** Integrating our encryption software with existing encryption technologies and VMs is fast, seamless, and can be completed while a VM is active and live, or offline for both Windows and Linux environments. The encryption process happens without disrupting your working environment.
- **Incredible portability.** If you're still following an old IT security model that locks you in to a single vendor, you're missing a trick. Portability is a key attribute of the Cloud IaaS model. One intelligent key management and cloud encryption approach across your environment lets you to maximize the benefits of the cloud, shifting workloads and data as you see fit. You can flex with the demands of the business and scale up and down at speed with one data protection platform and enjoy common key management across any cloud. You can move encrypted workloads from one cloud to another and clone and replicate them without the need to decrypt and re-encrypt.
- **Public freedom.** Your admins can seamlessly import, sync and manage VMs from public cloud providers such as AWS and Microsoft Azure, and simultaneously view the security of individual cloud instances.
- **Centralized control.** Thanks to a central Server Policy Engine, the authentication process is completely automated – freeing your people to focus on other tasks in their workflow. Snapshots, replicated, or clone VMs are authorized and authenticated before booting, ensuring that no clone machines exist without proper encryption and the associated keys.

I am unified.

Managing information governance with one dashboard lets our teams focus back on business growth.

I am unified.

Having one data protection shield across clouds has revolutionized our business.

Any cloud. Anywhere. Any time. **Solve data protection, once and for all.**

Why partner with WinMagic to transform data protection, smooth compliance and revolutionize operational efficiency? Because we're the leading the charge towards a new era Anywhere Enterprise. Thousands of commercial and public sector organizations already trust us to help them succeed. We also have long and exciting partnerships in place with a raft of industry leaders from HP to Intel, Lenovo and Western Digital.

Our experts can help you optimize your front-end and secure your back-end. It's everything you need to build a new era, agile, competitive operation fit for 2017, and beyond.

So why not get in touch?

We can walk you through the next steps, review your operation and even conduct a free expert security audit on request. You have nothing to lose and tremendous operational flex, cost reduction, simplified compliance and peace of mind to gain.

info@winmagic.com | www.winmagic.com

WINMAGIC®

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