CXO
SECURITY
BRIEFING

Beyond protection to proof

How CIOs are achieving compliance using encryption management in the new regulatory era

SecureDoc™ by WinMagic

WINMAGIC®

What if you could bring real clarity and control to compliance?

The digital workspace is rapidly transforming every corner of your operation. It's enabling new levels of speed, collaboration and cost efficiency across critical lines of business and around your dispersed global operation. But as your IT environment gets more complex, so do the regulations and IT solutions designed to protect and govern it.

Compliance demands are gathering pace, strength and impact.

With EU GDPR now passed into law, you have one more privacy minefield to navigate if you handle the personal data of any EU residents, even if you're not actually trading in Europe. That's alongside the multiple regulatory frameworks across the globe with which you already need to comply including HIPAA, PCI-DSS, POPI , CIS and Sarbanes-Oxley amongst others. Question is: how can you keep delivering the incredible agility, collaborative ease, cost-efficiency and control that has helped IT organically thrive across your organization while also ensuring data protection and governance into your IT approach so you don't fall foul of regulators?

- Data protection is a clear priority. You need to shield your organization from the risk of financial non-compliance penalties and bad press by protecting sensitive operational data, wherever it resides, from unauthorized access, user error or malicious attacks from within your organization or Cloud Service Provider.
- But not at the cost of productivity. You also need to continue to liberate workforces and cost-efficiently empower uptime, seamless security processes and effortless collaboration to drive the bottomline in your competitive global markets.

It's no wonder achieving compliance has become such a pre-occupation amongst CIO, CISO and IT Director communities — it's such a complex game to win and the rules are constantly shifting. Luckily WinMagic is on a mission to simplify compliance and this CXO Briefing is your 'how to' guide.

The BitLocker encryption that comes free with Windows 10 has been seen as a saviour by many solution-hungry and budget poor IT departments. And indeed BitLocker is great at doing the one job it's designed to do: locking down Windows workloads – whether endpoints or servers. But as this paper will show, you need to do a fair amount of work with the good stuff BitLocker offers to make it an effective compliance and business productivity solution.

We'll show you how to make BitLocker work for your business, alongside other encryption solutions like FileVault for macOS and Self-Encrypting Drives. The secret? Deploying a simple and unified approach to encryption management that lets you deliver a seamlessly productive user experience alongside effortless security and compliance, in one.
Read on to learn more.

Complexity is a real challenge

There are many 'forward-thinking' security approaches out there; next generation data protection solutions that promise to secure one piece of your IT estate or another. You've likely already invested in a patchwork of encryption and other security solutions to try protect the growing data sprawl that the new digital workplace creates.

But if locking down data is just one half of your challenge, how do you deliver security without compromising on the practical realities of day-to-day business workflows — which is the other half of your challenge? How do you integrate and manage all your solutions? Spot where the security gaps lie and close down vulnerabilities? Automate governance and reporting?

BitLocker alone isn't enough

If you've migrated to Windows 10, the 'free' BitLocker encryption that comes rolled up into the software will be a key piece of this complex picture for your IT organization. While the complimentary FIPS 140-2 compliant full drive encryption for Windows 10 devices it offers sounds great, with increasing regulatory pressure, businesses don't just need workload protection. They need to prove they're protected.

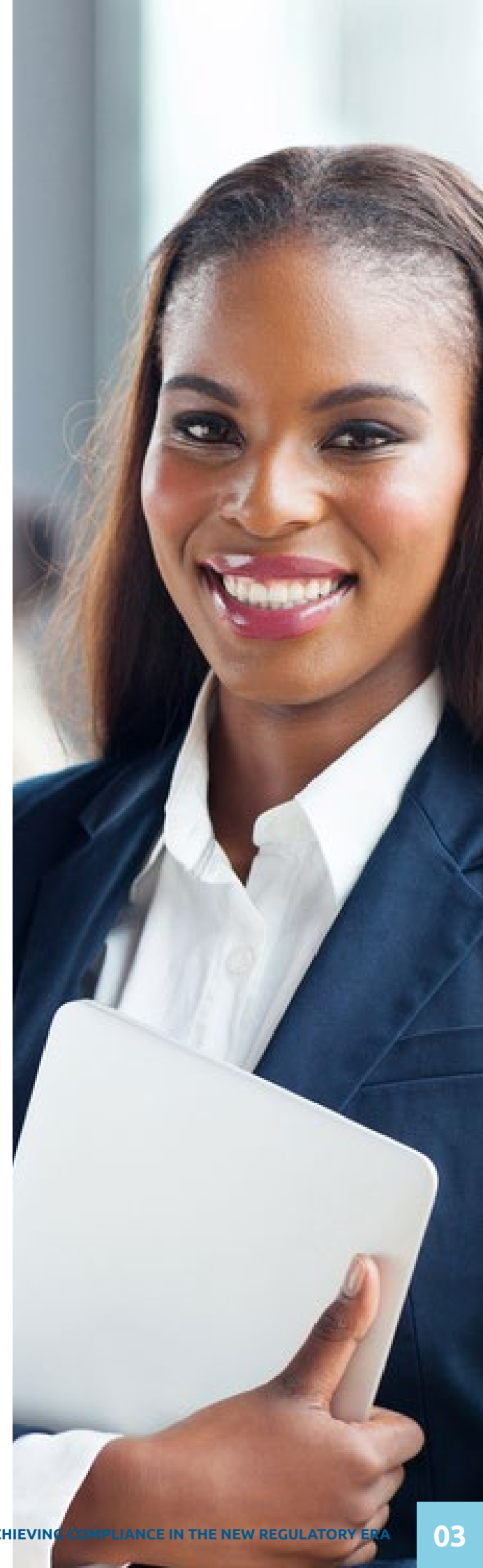
> You can't use BitLocker to prove encryption in the way regulators require, because it doesn't offer centralized management visibility and control.

It also doesn't deliver simple pre-boot authentication, any user or application with privileged rights can tamper with encryption settings and disable BitLocker, for malicious reasons or just because they find the complex PIN access obstructive or irritating. That means BitLocker alone simply can't help you prove the protected status of Windows devices and workloads, or make you compliant.

IT leaders looking for the highest levels of security may opt to back up TPM (Trusted Platform Module) with PIN authentication to deliver pre-boot protection. But that leaves users having to log in twice, handle arduous recovery processes and concurrently remember multiple PINs for different devices. This makes BitLocker a less than practical solution in the real world, getting in the way of user productivity and creating unmanageable IT helpdesk workloads. Alternatively, TPM-only demands no user interaction whatsoever, but neither does it offer adequate protection on its own.

> So while BitLocker solves one problem, it also creates another. How can businesses deliver the encryption protection that their business clearly needs, without the endless user disruption it really can't afford?

Keep reading to find out.



What BitLocker does well and where it needs support

Microsoft itself is very clear about the BitLocker security / practicality compromise.

One one hand, they say that BitLocker without pre-boot authentication (TPM-only) "…offers the lowest level of data protection" and "can be affected by potential weaknesses in hardware." Meanwhile BitLocker with pre-boot authentication (TPM + PIN)* "inconveniences users and increases IT management costs." *

BitLocker: the good, the bad and the potentially ugly

Good

- **Native:** Because it's built-in OS encryption, BitLocker delivers better performance and compatibility than third-party solutions
- **Complementary:** Some basic management tools are already included in MDOP for Windows Software Assurance/ Volume Licensing customers
- **Integrated:** BitLocker is supported in Microsoft Azure with Azure Disk Encryption

Bad

- **Costly:** BitLocker needs a lot of IT Helpdesk and management support; cannot manage macOS or Linux devices
- **Management complexity:** Managing it requires a minimum of two servers and relies on open and insecure Group Policy Objects to manage data protection policies
- **Poor user experience:** BitLocker PIN authentication processes are disruptive to users

Potentially ugly

- **Compliance gaps:** BitLocker isn't tamperproof, so you can't use it to demonstrate that devices remain in an encrypted and compliant state after deployment. TPM-only authentication does not provide sufficient security if a device is lost or stolen.
- **Negative press and stiff penalties:** This leaves you exposed to serious reputational damage and ugly fines: up to 4% of annual global turnover in the case of the new EU GDPR.

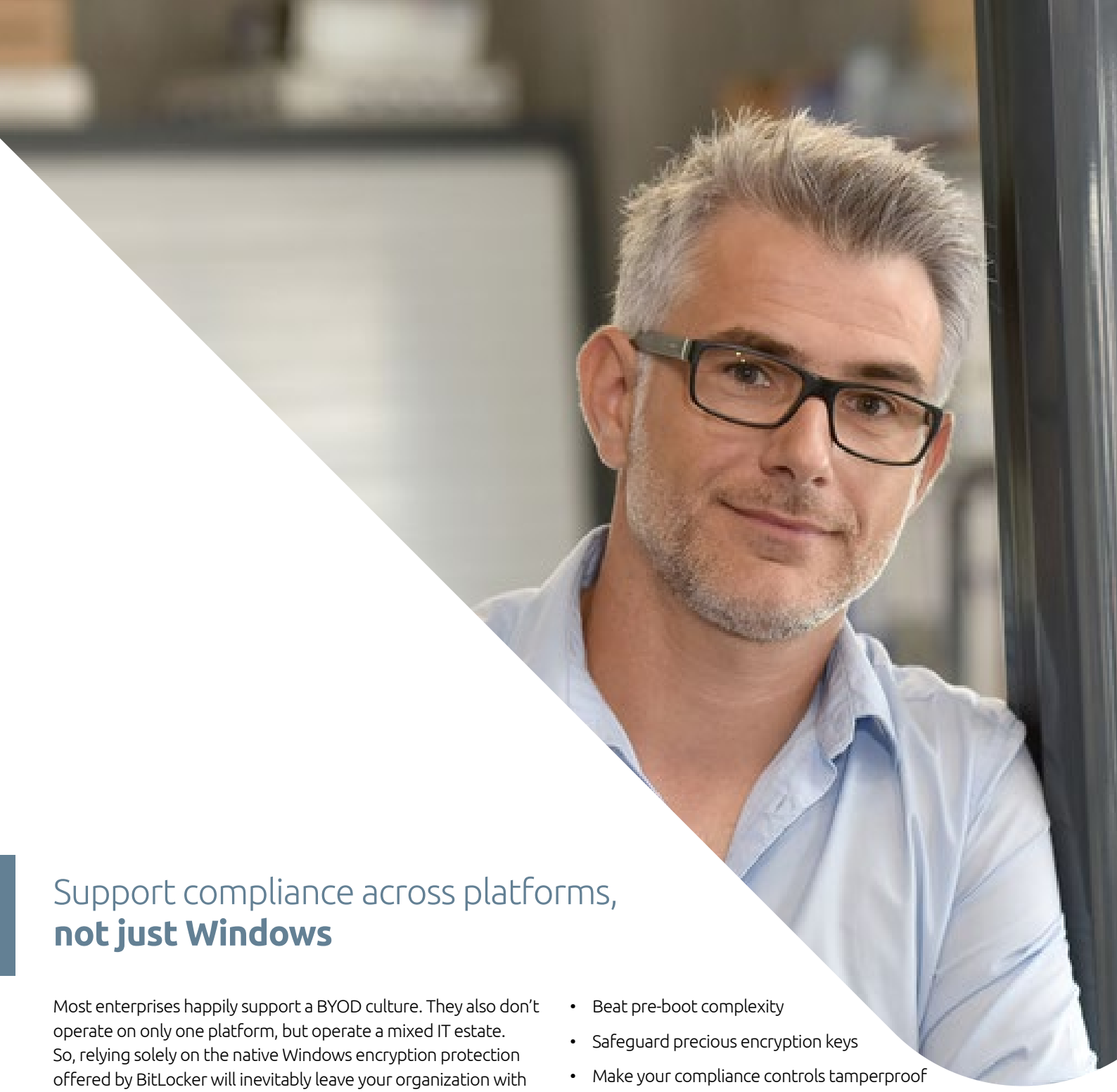
This picture is radically transformed just by adding SecureDoc from WinMagic. This visionary solution set is designed to rescue organizations from this compliance and productivity quicksand. It's the only encryption approach out there that can cover the management of encryption across any physical endpoint, virtual server or cloud instance: all from a single dashboard — simply unifying the intelligent management of encrypted data wherever it lives. Our pre-boot agent sits on top of BitLocker and other encryption solutions like FileVault for macOS and SEDs, enabling a single sign-on that's both fast and secure.

The result?

Businesses can enforce **secure and compliant authentication while also delivering a seamless user experience: no compromises. It's as simple as that.**

***https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/prepare-your-organization-for-bitlocker-planning-and-policies**

***https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/protect-bitlocker-from-pre-boot-attacks**



Support compliance across platforms, **not just Windows**

Most enterprises happily support a BYOD culture. They also don't operate on only one platform, but operate a mixed IT estate. So, relying solely on the native Windows encryption protection offered by BitLocker will inevitably leave your organization with significant security and compliance gaps.

While it's great that the WinMagic approach embraces FileVault2 for macOS and SEDs, managing them all from one unified and always-compliant dashboard, that's just the start. There are a whole number of other levels on which WinMagic's SecureDoc helps you bring additional clarity and control to compliance, helping you to govern and protect your whole workforce across your IT estate, not just Windows.

- Beat pre-boot complexity
- Safeguard precious encryption keys
- Make your compliance controls tamperproof
- Remove threats posed by removable media
- Achieve real-time, historical, and comprehensive reporting

In the next pages, we'll take you through these — one by one.

Beat pre-boot complexity

BitLocker device-based PINs can become a compliance liability, particularly when you offer shared workstations as so many businesses these days do. Often, users are left to print out or write down their PINs, which they then end up storing in close proximity to their device for easy access. It's only human, but it's also not tolerated by regulators in the new compliance era.

- Password sharing gets you a cross in the compliance box. PCI DSS forbids the use of generic or shared passwords (Req. 8.5), but the reality is that BitLocker PINs must be shared between users on shared workstations, often leaving them to write down or print the PIN and keep it near the device – which conflicts with PCI requirements.
- Password complexity is another challenge. Many regulations, including PCI DSS, also require password complexity (Req. 8.2.3), but the very basic MBAM controls that come with BitLocker cannot enforce PIN complexity, only PIN length, which can lead to the creation of easy-to-crack passwords that are also easy to remember.

One recent Gartner Peer Insights review of SecureDoc from WinMagic puts it well, saying: "Excellent integration with BitLocker" . WinMagic agrees.

Gartner peerinsights™

Simply deploy SecureDoc for BitLocker and your IT admins will be able to enforce password complexity rules and eliminate the need for users to share problematic PINs. Now each user will have their own password – either linked to Active Directory or not, as you choose. This helps businesses drastically simplify compliance enforcement and eliminate the potential gaps in security caused by shared PINs. That's one easy win.

Safeguard precious encryption keys

Regulators have quickly woken up to the need to not just protect data using encryption, but to also protect the encryption key itself. In fact, HIPAA, PCI DSS and other Breach Notification Laws now demand that businesses document and implement procedures to protect the encryption keys used to secure data against disclosure.

Critically, and quite rightly, if encryption keys are lost with the data, that is now considered a compliance breach. That leaves your organization vulnerable to reputational damage as well as all sorts of stiff penalties — in the case of GDPR, up to 4% of global annual turnover.

Your IT management team may not realize that Active Directory (AD) stores recovery keys and information in plain text, which leaves them open to unauthorized access, loss or exposure. The MBAM controls that come with BitLocker can store keys in an encrypted database, but a reliance on AD and Group Policy (GPO) can really complicate the separation of duties between AD admins and security teams, and create more IT headaches than it solves.

Put WinMagic's SecureDoc Enterprise Server in place and all key-related material will be stored in an encrypted database.

In fact, our unique PBConnex features can ensure that keys are never stored on devices at all. Instead they deliver the encryption key over the network at pre-boot and then discard it when the device shuts down or reboots.

Role-based Access Controls (RBAC) also allow businesses to isolate certain controls to specific named admins, thereby reducing the potential for rogue administrators or malicious insiders. Take it to the cloud, and SecureDoc CloudVM for BitLocker ensures that Enterprise controlled authentication stops keys and data from exposure to your Cloud Service Provider or other tenants without your knowledge – so you stay in charge of your data, at all times. It also helps you safeguard against error or attack from privileged insiders. These can be the most dangerous threat agents, working either within your Cloud Service Provider or within your own admin team, capable of causing huge damage through human error or through malice.

Make your compliance controls tamperproof

It's an open secret amongst IT admins that BitLocker can easily be disabled or suspended. Of course, the regulators have caught on. Certain users and applications can disable or suspend BitLocker protection completely, placing your devices or even worse, your cloud workloads in a non-compliant state, leaving them entirely vulnerable to unauthorized access.

This level of uncertainty is overwhelming for security teams and can place your business at significant risk. Worse yet, tampering or modifications to BitLocker settings can be carried out in Control Panel, Command Prompt, and PowerShell, leaving multiple security gaps.

There is NO option in BitLocker to prevent users from disabling the protection, but WinMagic has the answer.

SecureDoc Tamper Protection monitors your BitLocker-enabled devices in real-time. If it detects that encryption has been disabled or suspended, it automatically blocks and reverses the action, keeping devices in an always-compliant state and eliminating uncertainties as well as regulatory non-compliance. Problem, solved.

Remove threats posed by removable media

Despite new cloud and network file sharing solutions, nothing beats a classic USB. Users are accustomed to extracting and exporting data at will, sharing it with team members, moving it around devices and then often just leaving it languishing in a desk drawer. That makes removable media a huge compliance risk, largely unsupported by BitLocker To Go which offers protection only for Windows devices with no portability between Windows and macOS users. The basic BitLocker control suite MBAM also doesn't monitor or enforce encryption on removable media devices, leaving gaps in audit trails and difficulties in accurately reporting on data protection status.

SecureDoc from WinMagic includes OS-agnostic removable media protection.

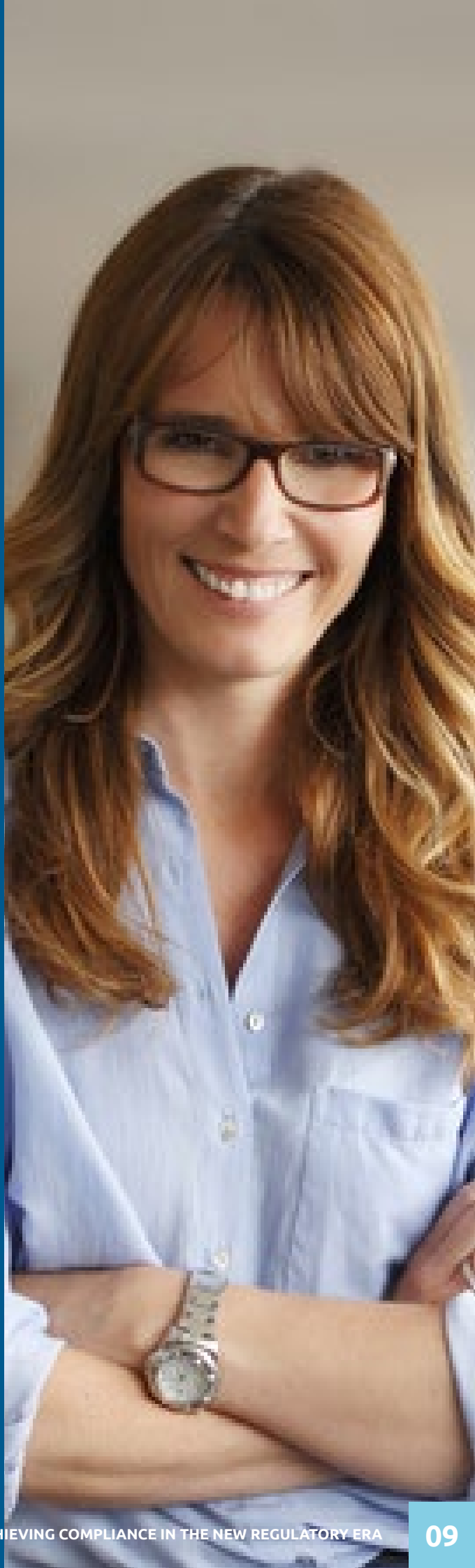
This ensures that access to data is secure and seamless between Windows and macOS devices. The SecureDoc Enterprise Server can enforce access policies and port controls, and delivers granular reporting, even for removable media. Job done.

Achieve real-time, historical, and comprehensive reporting

While BitLocker's encryption status can be checked using GPO or MBAM, neither option offers the historical reporting that is essential for a successful compliance audit. Even worse, macOS and Linux devices require a separate solution, creating gaps in compliance reporting and management complexity. No-one needs that.

WinMagic's SecureDoc Enterprise Server offers a single dashboard to monitor and report compliance status across virtually any workload – whether Windows, macOS or Linux.

Administrators have access to real-time and historical reports, ensuring that audits are comprehensive and consistent across endpoints, datacentre and cloud. Our customers have proven reduced reporting time by as much as to cut reporting time by as much as 60% while detailing failed log-in attempts as well as successful ones. Double win.



Beyond products to true partnership

Clearly, achieving compliance isn't an isolated technical challenge, but an ongoing operational priority. So you need a partner that offers you more than a one-stop solution. You need a strategic advisor who can offer you an approach aligned to your challenges and the evolving realities of today's tough regulatory climate.

As respected industry leaders in intelligent encryption management, WinMagic always works ahead of the curve. Our home base in software encryption has evolved over the last two decades to now embrace endpoint devices, data centres, hybrid cloud, virtual workloads and, most recently, hyper-converged infrastructures.

Partner with us and you get 'roadmaps to reality' designed for ambitious enterprises that know where they're heading and need the right, progressive IT support to get there.

Want to know more about going from protection to proof, strategically managing BitLocker and making your encryption environment simple, user-friendly and inherently compliant? We'd love to hear from you. Simply get in touch.

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**