Whitepaper

SecureDoc™
by WinMagic

4 ways to radically simplify BitLocker management and optimize business productivity

WINMAGIC®

Why smart IT Pros are choosing a new unified encryption management approach

BitLocker is built to encrypt Microsoft Windows 10 workloads and it does that job well. But as an IT pro, Windows workloads are only one part of the security universe for which you're responsible. You need to protect all your enterprise workloads across macOS and Linux platforms too, as well as self-encrypting drives — and manage security across platforms while maintaining compliance. And you need to do it all with budgets that aren't necessarily enough for the sheer levels of IT complexity and governance scrutiny that you're expected to navigate.

That's why IT pros are increasingly finding that BitLocker alone won't solve their encryption or audit and compliance issues. What's needed is a more complete approach that can unify encryption management across platforms. A way to discover protect and manage access to all your encrypted devices from a single console — and prove it to auditors, in real-time.

Most importantly, all this needs to be achieved without investing in more hardware and services.

This whitepaper shows you why enterprise IT teams are opting for the uniquely unified encryption management approach that only the SecureDoc Enterprise Server from WinMagic offers. It helps you unlock all the great benefits of BitLocker while simplifying, streamlining and supporting your encryption needs across the entire business.

The end-result isn't just lower IT costs, reduced help-desk workloads and satisfied auditors. User experience and productivity are also transformed with a simple, single sign-on to replace BitLocker PIN complexity — eliminating security friction points and supporting collaborative working.

We will now explore the 4 key ways that

SecureDoc revolutionizes BitLocker success.

How SecureDoc revolutionizes BitLocker success

1. Delivering a low-cost IT operation

BitLocker is a solid starting point for any data protection strategy, but it's not enough to meet compliance requirements. For that, you need a management tool capable of delivering management and reporting for audits.

Your organization has three options for managing BitLocker: manually via Active Directory Domain Services (AD DS), via cloud-based management with Azure Active Directory (Azure AD) and Microsoft Intune, or the Microsoft-recommended way, with Microsoft BitLocker Administration and Monitoring (MBAM). MBAM is typically the go to option for SMB and enterprise-level customers. While it offers more advanced functionality and protection than managing via Active Directory (AD) alone, it cannot deliver the level of visibility and control your enterprise needs to both achieve and prove compliance. The cost implications of this are serious.

Overcoming the challenges with SecureDoc

1. High OpEx and licensing costs

If you are using MBAM to manage BitLocker, you may find the solution is not as 'free' as it seems. Take a look at how the costs quickly start to escalate as layers of control are added.

- **BitLocker Drive Encryption** — Available (without additional purchase) for Professional, Business, Enterprise, Education and Mobile licenses of Windows 10.
- **AD DS** – No cost for Active Directory Domain Services.
- **MBAM** – You'll need a Microsoft Enterprise Agreement with a minimum 500 users/devices to access MBAM. It's only available as part of the Microsoft Desktop Optimization Package (MDOP) for Software Assurance Volume Licensing customers.
- **Intune/Azure AD** – Microsoft Intune offers basic BitLocker management and reporting options, but at a cost not affordable to many IT budgets today – additional costs for Intune and Azure AD licenses and lack of contract flexibility can make it a less than ideal solution for BitLocker.

The WinMagic Solution

- By deploying WinMagic's SecureDoc Enterprise Server (SES), organizations can eliminate the need to purchase, maintain and support complex contracts and licenses. For those without Enterprise Agreements, WinMagic offers a cost-effective, enterprise-level alternative designed with managing BitLocker-enabled devices at a low-cost in mind.
- One console to manage, monitor and protect all BitLocker-enabled devices – no need for Enterprise Agreements, commitment-based Microsoft subscriptions or additional servers.
- Enjoy the same protection and policies for all devices, regardless of your Windows 10 license type.

2. CapEx – Extra hardware outlay

However you choose to run BitLocker, you'll quickly come up against increasing costs for extra hardware investments that you'll need to make.

- **Basic BitLocker** – Pre-boot authentication with BitLocker requires either the use of a Trusted Platform Module (TPM) or for the user to input a PIN, or sometimes both, depending on the hardware and operating system configuration. TPM on its own does not provide enough protection: in fact, Microsoft says it offers the "lowest level of data protection" without additional hardware and OS-level security configurations. Alternatively, you have to add in PIN authentication, which Microsoft also admits "inconveniences users and increases IT management costs."
- **MBAM** – MBAM can be deployed in two different ways: Stand-alone or Configuration Manager Integration. Either way, your organization needs to standup and configure a complex infrastructure with more than one server and multiple software agents.
- **Network Unlock** – This is a core functionality that allows BitLocker-protected devices to startup without user intervention, similar to WinMagic's PBConnex Autoboot. This is particularly helpful for back-end servers that are always connected to the corporate network. However, with BitLocker alone, this requires a complex and costly set-up, including two additional servers – a WDS server and a DHCP server – and multiple configuration requirements.

The WinMagic Solution

SecureDoc Enterprise Server (SES) lets you unify all the disparate components of encryption management, including BitLocker, creating one simplified solution.

- Install all the components you need on a single server or multiple servers, depending on your business scale, reducing hardware costs and consolidating management tasks into one console.
- Advanced pre-boot authentication enables fast, secure and user-friendly device access, regardless of your underlying hardware. If TPM is available, SecureDoc can detect and automatically provision what's needed, but without TPM, SecureDoc still offers robust pre-boot protection.
- Integrated PBConnex technology offers all the advantages of 'Network Unlock' and much more – without additional hardware, firmware or server expense. You can securely authenticate or auto-boot devices over a wired or wireless network and let IT admins remotely enforce policy updates, password changes or remote wipe commands before a device even boots.

3. High OpEx management costs

Your business is probably already running Active Directory. Trouble is, it's neither secure, nor compliant for managing keys, plus you'll need to manage it manually, with no tools or automation to reduce time spent on provisioning, management or recovery. Meanwhile devices joined to Azure AD in the cloud require a Mobile Device Management (MDM) policy such as Microsoft Intune. Here, you'll find BitLocker policies are very limited. Even advanced options only available with Windows 10 Business or Enterprise (via BitLocker CSP) are limited, making it difficult and costly for businesses to control and manage devices.

Managing BitLocker with MBAM? Although this is better than AD-DS for domain-joined devices on-premises, you'll still need to manage BitLocker with multiple Microsoft applications, including Group Policy Objects (GPO). Management time and costs can quickly mount up to significant levels.

The WinMagic Solution

WinMagic SES gives IT a simple, centralized tool for deploying, managing, and reporting on BitLocker-enabled devices: from one dashboard.

- Drastically simplify management, with a clear administrative interface for deployment and on-the-fly policy changes, with no reliance on GPO.
- SecureDoc Active Directory Sync (ADSync) enables quick and simple import of all or select users and groups, with real-time synchronization to ensure passwords and policies are always up to date. That way, organizations can leverage AD, without depending on GPO.
- Isolate security management from device management, reducing the risk of insider threats.

4. Spiralling CapEx

Windows workloads are only part of your IT protection story. So what about all your other devices and data pools? Do you need to invest in too many solutions to keep on top of it all?

- **Linux devices** – Not supported with MBAM or Intune. Businesses will need to purchase an additional solution to manage encryption on Linux devices.
- **macOS devices** – Not fully supported by MBAM or Intune. Microsoft Intune can query whether macOS devices are encrypted or not, but cannot enforce or manage policies for encryption, so again a separate solution needs to be purchased.
- **Self-Encrypting Drives (SEDs)** – BitLocker – with or without MBAM – cannot manage standard self-encrypting drives. It only supports "Encrypted Hard Drives" which have specific requirements – including TCG Core Spec 2.0, Opal SSC 2.10, IEEE 1667 Support, and more. Practically, most businesses will already have hardware that doesn't meet these requirements, leaving them unable to leverage their existing investments.

The WinMagic Solution

SES offers a one-stop shop for all device-level encryption: simply manage and protect all your devices – Windows, macOS and Linux — with a drastically reduced dependence on knowing specific hardware configurations.

- The approach is less dependent on hardware, so devices can be secured with enterprise-level protection regardless of their hardware-level security features.
- Replaces multiple solutions, consolidating key management across Windows, macOS and Linux devices with market-leading support for a long list of certified Opal SEDs.

How SecureDoc revolutionizes BitLocker success

2. Maintaining a compliant data state without disrupting users.

BitLocker offers FIPS 140-2 compliant full drive encryption for Windows 10 devices. But with increasing regulatory pressure, businesses don't just need to protect data; they need to prove that they have protected it. However delivering governance is difficult and expensive with disparate management tools — and BitLocker encryption can be tampered with, , unless you add complex PIN authentication, which is disruptive to your users and IT staff.

Overcoming the challenges with SecureDoc

1. Delivering pre-boot protection

BitLocker leaves IT with a tough compromise – user productivity or robust security? If security is a priority, adding PIN authentication to TPM is the way forward, but it means users have to log in twice, handle lengthy recovery processes and remember multiple PINs for different devices. The alternative is TPM-only access which requires no user interaction, but also cannot guarantee adequate protection of data. WinMagic believes that security teams shouldn't have to make this fundamental compromise.

- **TPM + PIN** – Microsoft states that TPM + PIN "inconveniences users and increases IT management costs";
- **TPM-Only** –Microsoft also states that TPM-only offers "the lowest level of data protection," potentially vulnerable to weaknesses in hardware components.
- **MFA** – BitLocker does not support Multi-Factor Authentication (MFA) with industry-standard smartcards and tokens, required by regulations including PIV for federal government.

The WinMagic Solution

- Our SecureDoc pre-boot agent sits on top of BitLocker, enabling a fast and secure Single Sign-On (SSO) – plus integration with hundreds of industry standard smartcards and tokens.
- That means IT can deliver vital encryption protection without user disruption: no more choosing between security and productivity. Simply enforce a secure and compliant authentication while supporting easy workflows and business productivity.

2. Password Requirements

Shared workstations present a real problem if you're using BitLocker alone. Device-based PINs can become a compliance liability, with users left to print out or write down the PIN and store it in close proximity to the device to allow everyone easy access. You need to be clear about what compliance looks like

- **Password Sharing** – PCI DSS does not allow the use of generic or shared passwords (Req. 8.5). However, BitLocker PINs inevitably need to be shared between users with shared access.
- **Password Complexity** – Many regulations, including PCI DSS, also require password complexity (Req. 8.2.3), but MBAM cannot enforce PIN complexity, only PIN length.

The WinMagic Solution

- SecureDoc lets IT admins enforce password complexity rules. It also eliminates the need for users to share pre-boot passwords, since they can now each have their own – whether these are linked to Active Directory or not.
- This helps you drastically simplify compliance enforcement and eliminate the potential security risks that shared PINs create.

3. Key Protection

Protecting the keys used to encrypt the data is becoming increasingly important to regulators. HIPAA, PCI DSS and other Breach Notification Laws all state that businesses must document and implement procedures to protect the keys used to secure data. If keys are lost with the data, that is rightly now considered a data breach. Active Directory stores recovery keys and information in plain text, which leaves them open to unauthorized access, loss or exposure. MBAM can store keys in an encrypted database, but reliance on Active Directory (AD) and Group Policy (GPO) often complicates the separation of duties between AD admins and security teams.

The WinMagic Solution

- The SecureDoc Enterprise Server (SES) stores all key-related materials in an encrypted database. In fact, PBConnex ensures keys never need to be stored on devices, by delivering them over the network at pre-boot and discarding them when the device shuts down or reboots.
- Role-based Access Controls (RBAC) also allow businesses choose which admins get which controls, thereby reducing potential harm from rogue administrators or malicious insiders.

4. User Tampering

Strange but true: BitLocker can easily be disabled or suspended. Certain privileged users and applications can disable or suspend BitLocker protection, leaving your devices vulnerable to unauthorized access and therefore non-compliant. This can place your security team under great stress and 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.

The WinMagic Solution

- SecureDoc Tamper Protection monitors all your BitLocker-enabled devices in real-time.
- If it detects BitLocker has been disabled or suspended, it will automatically block and reverse the action, keeping devices in an always-compliant state.

5. Removable Media

Removable media can be a huge hazard area, letting users extract and share data at will. BitLocker To Go offers protection for Windows devices alone, but with no portability between Windows and macOS users. Beyond that, MBAM "does not monitor or enforce encryption" (MBAM 2.5 Deployment Guide) on removable media devices, leaving gaps in audit reporting.

The WinMagic Solution

- SecureDoc delivers OS-agnostic removable media protection, ensuring that access to data is secure and seamless between Windows and macOS devices.
- SES can enforce access policies and port controls, and delivers granular reporting even for removable media to log data movement.

6. Compliance Reporting

BitLocker's encryption status can be checked using GPO or MBAM, but neither offers the historical reporting essential for compliance audits. Of course, macOS and Linux devices also require a separate solution, which can create huge gaps in visibility and audit control.

The WinMagic Solution

- SES gives IT teams a single dashboard to monitor and report on compliance status across virtually all devices – whether they are Windows, macOS or Linux.
- Administrators have access to real-time and historical reports, ensuring that audits are comprehensive and consistent.

How SecureDoc revolutionizes BitLocker success

3. Simplifying IT complexity

Protecting your Windows workloads with BitLocker is simple, but managing users, encryption keys and passwords becomes chaotic without the right, centralized tools. Conducting OS upgrades and migrations also forces you to suspend BitLocker, which leaves data exposed and compromises your compliance stance. Rather than just focusing on BitLocker, invest in SecureDoc instead and you'll be supported by one truly future-proof encryption solution that's designed and continually developed to help you meet your evolving security realities.

Overcoming the challenges with SecureDoc

1. Complex deployment

Microsoft designed BitLocker to lock down Windows devices, but deploying it securely relies on you carrying out multiple hardware and firmware configurations. You need to check all devices for an available TPM chipset, then provision each TPM for use with BitLocker. For devices without a TPM, you need to check your BIOS or UEFI firmware for compatibility with USB at pre-boot and invest in a compatible USB to store the startup key. Want to use advanced features like Network Unlock? That takes an additional WDS server, DHCP server, DHCP drivers and all the configuration that comes with them. In short, you need to know the hardware and firmware on *each and every device* you provision.

The WinMagic Solution

- SecureDoc enables IT to leverage available Windows 10 features – such as TPM, Secure Boot, Device Guard and Credential Guard – without relying on them to provide strong pre-boot protection. That means BitLocker can be deployed without compromising security.
- It also doesn't require any heavy new hardware investments.
- The SecureDoc client will automatically detect and leverage the best available encryption – whether that's a self-encrypting drive, built-in OS encryption, or our own industry-leading drive encryption.
- It quickly detects the make and model of each device and automatically applies the best-known configuration too, with no IT intervention — plus it automates TPM provisioning.

2. Managing Users

BitLocker is built on a device-based model, using device-based PINs for authentication. The result?

IT has a difficult time managing which users are allowed access to which devices and managing multi-user workstations becomes really complex.

The WinMagic Solution

- SecureDoc puts the user back at the centre. IT can simply add or remove user access to any device with Intelligent Key Management and AD Sync, simplifying user management.
- Security teams also gain more insight into which users are accessing each device, allowing them to detect unauthorized attempts to access data.

3. Password Management

Remembering passwords is a constant headache in the digital era. Users already have so many accounts and services, now you're giving them one more password to remember. Chances are, they'll forget it, which quickly becomes the IT helpdesk's problem. Teams have to spend hours annually helping users recover their devices with 48-character BitLocker recovery keys. Centrally storing and recovering all of this information is tricky too. Manual spreadsheets are slow and vulnerable. MBAM stores recovery keys in an encrypted database, but that doesn't help IT helpdesk teams reset passwords.

The WinMagic Solution

- Our approach is proven to help businesses reduce their encryption-related IT helpdesk workloads by up to 75%.
- SecureDoc Enterprise Server centralizes all management tasks into a single console, with Role-Based Access Controls (RBAC) to help your IT helpdesk quickly and simply reset passwords.
- You're not stuck with one recovery method either, SecureDoc allows users to recover passwords without any IT intervention by leveraging a Self-Help or pre-boot browser recovery for organizations with an Identity Access Management (IAM) solution.
- Better yet, to retain jurisdiction over password resets, your helpdesk can enable pre-boot access over the network in seconds, giving the user access and letting them reset their password.

4. Diverse Infrastructure

Your enterprise today operates beyond Windows. It probably embraces a mobile, flexible work environment that has scaled beyond the four walls of the datacenter into the cloud in a bid to become more agile. While BitLocker is a solid starting point for protecting your Windows endpoint devices, it's a fraction of the bigger security picture you need to consider. Operating multiple encryption solutions across your IT infrastructure creates siloes in visibility and control – and doesn't give you the flexibility to protect data wherever it's stored across your business.

The WinMagic Solution

- SecureDoc Enterprise Server gives your businesses a scalable, centralized, enterprise-wide key management approach that can support your diverse data security needs.
- It's proven to help our customers significantly reduce encryption audit times by up to 60%
- SecureDoc provides businesses with a single platform to manage the encryption of data-at-rest, from diverse endpoint and IoT devices to workloads running across private, public and hybrid cloud infrastructures.
- You can quickly view and audit the encryption status across virtually any platform or device, via one dashboard.

How SecureDoc revolutionizes BitLocker success

4. Ending User Disruption

Like all Full Disk Encryption solutions, BitLocker depends on strong pre-boot authentication to ensure that only authorized users can access encrypted data. BitLocker offers multiple options for pre-boot authentication but with one major issue: users need to enter PIN authentication for every device they use, which can mean multiple sign-ons in a day. This is not a viable option in today's user-centric workplace. The trade-off for business security is user experience. Businesses are forced to decide what's more important: data protection or user productivity — but they shouldn't have to choose. Essentially, WinMagic's SecureDoc solution can be customized to deliver the perfect balance between the two.

Overcoming the challenges with SecureDoc

1. Slow startups and lost productivity

The most secure BitLocker deployment method is TPM + PIN, but even Microsoft states that this is "inconvenient to users…"[1]. Pre-boot authentication can cause significant downtime for day-to-day activity unless the right management solution is in place. User time spent on dual logins and troubleshooting can quickly add up to many hours of lost productivity every week.

The WinMagic Solution

- Simplify and speed up BitLocker authentication by augmenting it with a secure, user-based Single Sign-On (SSO).
- Just sync up Active Directory with SecureDoc and users can login quickly with a familiar username and password — within seconds, over the network.
- It's ideal for BitLocker-encrypted servers in the datacenter, allowing them to automatically boot on secure networks, without any IT interaction.
- Unlike a TPM-only approach, if the device is taken off the network it will not boot, which keeps your data secure and encrypted.
- It doesn't require a wired network connection for mobile workstations and laptops either.

2. Forgotten passwords

With BitLocker, users always have to remember at least two passwords – a PIN for pre-boot and a password for Windows login. If users have access to more than one device, they have to remember different PINs, and for shared workstations, they'll need to share a common PIN – unacceptable in today's compliance rules.

The WinMagic Solution

- No more PINs means significantly reduced forgotten or lost passwords.
- If users need a separate login at pre-boot for PCI DSS compliance, you can allow them to have a separate user-based login, not connected to Active Directory.

3. Password Recovery

If a user does forget their password, BitLocker requires them to call the IT helpdesk and receive a 48-digit challenge-response recovery key to gain access to their device. This is a lengthy and error-prone process. Even if they use the Self-Service Portal offered by MBAM, the user then has to access the web from a separate device and still needs to enter a 48-digit recovery key. Either way, it's time-consuming and pretty complex.

The WinMagic Solution

- SecureDoc pre-boot authentication sits on top of BitLocker encryption, giving users multiple ways to get back up and running, quickly.
- If a user forgets their password, they can leverage Self-Help, Challenge Response or even an IAM web browser – similar to the MBAM Self-Service Portal, but right at pre-boot.
- They'll never need another device or a 48-character string to gain access to their locked devices.
- With ADSync, any password changes made in Active Directory are automatically synchronized with SecureDoc, so users can change their password ay anytime, with no knock-on issues.

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

4. Disruptive Deployment

Deploying BitLocker encryption can be complex for both IT and users. Whether you're using AD or MBAM to deploy and manage BitLocker with TPM + PIN, users will need to register their PIN before encryption starts. In the real world, that leads to them repeatedly postponing the process and leaving devices unprotected. MBAM can force PIN registration, but it's bad practice to force users through a process in today's workplace.

The WinMagic Solution

- SecureDoc makes the deployment process invisible to users and ensures devices are protected from the moment they are provisioned, before reaching the user.
- For BitLocker-protected devices, users need only sign into Windows as usual and SecureDoc will automatically register them as the device owner and synchronize the pre-boot login password.
- The user will never even know that their device has been provisioned with encryption.
- SecureDoc pre-boot on top of BitLocker is fully customizable and able to deliver a skinned branded corporate user experience, end to end.

5. Sharing Data

BitLocker is a Windows-only solution designed to protect Windows OS and user data. No cross-platform compatibility means macOS and Linux users cannot access any portable media encrypted with BitLocker To Go. In today's mobile, multi-platform environment, users expect complete workflow transparency and mobility with zero disruptions. Restrictions to information sharing have become unacceptable.

The WinMagic Solution

- SecureDoc Removable Media Encryption (RME) works with BitLocker to enable the simple, transparent encryption of removable media devices.
- The SecureDoc Reader allows users to share encrypted information across virtually any device, all with the high level of security you'd expect.
- Encryption can be enforced at the IT or user level, with the options for key sharing or password protection to enable users to flexibly protect and share their data, their way.

SecureDoc™ by WinMagic

Do the right thing for your business — and your IT team

The SecureDoc Enterprise Server (SES) is proven to cut helpdesk time spent on tasks like password resets by as much as 75% . That makes BitLocker much simpler and more cost-effective for your team to manage. It also eases deployment and transforms IT management visibility and control.

SES can help you speed associated jobs such as OS migration too, and embrace and manage your diverse endpoint and hybrid cloud encryption environment as one unified, low-cost, always-compliant whole. That's great for your business as well.

Alongside a fast ROI and a low overall encryption management TCO, SecureDoc solves encryption-based compliance concerns in one, mitigating the risk of expensive financial penalties and creating a transparent user experience that supports uptime and collaboration. So your hard-worked IT admin staff win — and so do your line of business teams.

Why wait to start working smarter?

Contact the team at WinMagic and we'll walk you through solution and discuss how to quickly get you up and running — and your business benefitting.