

Microsoft might be terminating its support for MBAM, but SecureDoc has businesses covered with the industry's best BitLocker Management solution

Recently, Microsoft announced that, as of July 2019, mainstream support for Microsoft BitLocker Administration & Monitoring (MBAM) would end. While 'Extended Support' will continue to July 2024, providing critical security patches, no new feature development will occur. With MBAM's mainstream support ending, businesses really need to take a hard look at alternatives for their BitLocker management. And, at the same time, determine whether or not BitLocker itself can meet the universal data security needs required by their organizations. And that's what we do best. With WinMagic's SecureDoc BitLocker management solution, organizations can take advantage of Microsoft's native OS encryption, while tightening security through improved authentication and integration with [SecureDoc PBConnex](#).

Customers need an encryption expert for their data security

Microsoft is a leader in the operating system development; that's their core service. While they offer security services with their products, Microsoft is not a security expert. That is not their specialty. At WinMagic, data security is our sole focus. 100% of our effort goes to developing the encryption products and solutions businesses need to protect their business data and that of their customers. We've been in the encryption business for 21 years, and encrypt over 8 million endpoints in 90+ countries.

BitLocker has always needed a better management solution

While BitLocker is a great foundation for Windows security, trusting in MBAM or Azure Key Management and its lack of centralized management can leave you struggling. We've always stated - [READ OUR PREVIOUS BLOG](#) - that MBAM was never sufficient for managing BitLocker. Microsoft's decision to step away from mainstream support for MBAM is evidence of just that.

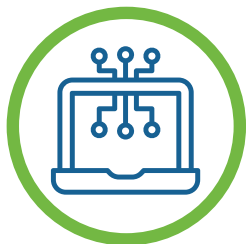
Why BitLocker and MBAM are not secure enough

- **Single Platform Support:** Most businesses don't operate on only one platform, or restrict data access to corporately owned devices. BitLocker only protects Windows-enabled devices or Azure VMs, forcing them to purchase additional solutions to manage Linux or macOS devices
- **Not Tamper Resistant:** BitLocker – with or without MBAM – can easily be disabled or 'suspended' by certain users and applications, so it can't be used on its own to demonstrate devices are in a compliant state after deployment.
- **Inferior Pre-Boot Authentication:** Lack of pre-boot network authentication
- **Cloud-Based Keys Aren't Secure:** Moving to cloud-based key control is not an option for security classified environments, as risks of security control are just too high to outsource to third party cloud vendors

SecureDoc should be your first choice in encryption and key management

Thousands of organizations worldwide use and trust WinMagic's SecureDoc to manage not only their BitLocker-encrypted devices, but any software-based, native or hardware-based encryption solution that they're using – including Windows, Mac and Linux OS – and across any endpoint, data center, virtualized or cloud environment. When customers are serious about data security, they need a partner that specializes in encryption.

- We are fully dedicated to data security – It's our only priority
- We unify encryption to remove security silos
- We let you maintain exclusive control of your encryption keys
- We tighten security through improved authentication and integration with SecureDoc PBConnex
- We provide a single pane of glass to simplify your compliance efforts



Maintain Exclusive Control of Your Encryption Keys

Businesses currently using MBAM or are planning to deploy MBAM soon will be left to utilize Active Directory, or move to Microsoft's preferred solution – its cloud-based Azure Active Directory – for key escrow. Moving to cloud-based key control is not an option for security classified environments, as risks of security control are just too high to outsource to third party cloud vendors. Many applications won't even accept cloud-based key management as safe. With SecureDoc BitLocker Management customers can:

Ensure keys are always stored on-premises:

Stored within a secure database, and under the control of the organization, so that they are not at the risk of third party discovery, undisclosed government access, or breach failure

Enable detailed, real-time reporting:

Proven to cut reporting time by as much as 60%, while providing the details needed for audits like historical data and user login activity



Prevent Compliance Gaps

BitLocker – with or without MBAM – can easily be disabled or 'suspended' by certain users and applications, so you can't use it on its own to demonstrate devices are in a compliant state after deployment.

An easy fix comes with integrating BitLocker with the SecureDoc Pre-Boot Protection and Monitoring solution from WinMagic – SecureDoc on Top. With SecureDoc BitLocker Management customers can:

Ready support: WinMagic is committed to supporting the Microsoft release cadence for Windows 10 and works closely with Microsoft to ensure that SecureDoc software solutions are fully compatible with all Windows releases

Prevent tampering: Block users from accidentally or maliciously disabling BitLocker protection

Reinforce protection: Stop BitLocker being thwarted by passware and hardware vulnerabilities with robust pre-boot protection and MFA smartcard support



Unify Encryption to Remove Security Silos

Your business doesn't operate on only one platform or restrict data access to corporately owned devices. So, it makes sense that relying solely on the native encryption protection offered by BitLocker will leave you with significant security and compliance gaps. With SecureDoc BitLocker Management, businesses can reduce operational workload and expenditures through:

One centralized console: Discover, protect and manage all your devices and virtual machines, including those running BitLocker, FileVault 2 for macOS, Linux, and even hardware-level encryption with OPAL SEDs. This includes unified encryption management for endpoints, data center and cloud environments

Unified view of company-wide data encryption: All the visibility without extra server, driver or upgrade expense

Simplified deployment: Transform slow TPM activation, device provisioning, and user registration with automated deployment, and transparent user adoption

Managing users, not devices: Simply add or remove Active Directory users to BitLocker-enabled devices, eliminating the needless user disruption caused by PINs

Want to know more about better managing BitLocker and your whole encryption environment with WinMagic? We'd love to hear from you. Simply get in touch: Sales@winmagic.com

Authenticate. Encrypt. Achieve.