A Guide to Managing Microsoft BitLocker in the Enterprise

WINMAGIC®
DATA SECURITY

TABLE OF CONTENTS

Introduction

Whole disk encryption, or full disk encryption (FDE) is becoming standard practice in the enterprise as organizations look to safeguard the lifeblood of their business: mission-critical data on a myriad of devices.

For enterprises dominated by the Windows Operating System, Microsoft's BitLocker would appear at first blush to be the logical choice to encrypt user devices, including PCs and laptops. But in a Bring-Your-Own-Device (BYOD) world, it simply won't address every device being used by your employees, such as smartphones and tablets running iOS and Android that connect to your network for convenient access to corporate data by a mobile workforce. In addition, many organizations have workstations and servers running Mac and Linux.

BitLocker is a solid starting point for device encryption, but enterprises need more if they are to have a true comprehensive strategy for securing all devices. WinMagic can manage your BitLocker deployment, leverage your existing investment and layer additional security functionality to fully realize the benefits of FDE on all platforms.

Why You Can't Ignore Effective FDE

Whether you're pondering the merits of BitLocker or have already deployed it, you can't ignore the benefits of effective FDE that combines security with ease of use and management. Every organization has confidential information that must be protected. The larger the organization and the more platforms in use, the greater the need.

Data breach incidents occur on an almost weekly basis. Since 2013, more than 660 million records have been compromised in data breaches according to The Privacy Rights Clearinghouse Chronology of Data Breaches (www.privacyrights.org, December 2013). It's a staggering number; more than a half a billion records and those are only the breaches that have been made public.

Even if you employed FDE across your organization, either with BitLocker or another solution, it only takes one stolen laptop to have not been properly secured and encrypted to make all of your FDE efforts irrelevant.

BYOD heightens the risk of data breaches and is likely to hamper your FDE efforts, since employees may access corporate data on personal Windows devices not included in a BitLocker deployment or an iOS or Android device not supported by BitLocker. If these devices are lost or stolen, whatever personal security setting the users have implemented are insufficient to truly safeguard information; having your corporate devices locked down with FDE becomes fruitless if all it takes is one device to compromise sensitive corporate information.

Securing data is becoming a requirement of doing business, and while passwords, biometrics, smart cards and other tokens do offer a high level of security, they aren't infallible; they can be cracked, thereby exposing sensitive business data.

The challenge faced by IT departments is how to keep costs low, while ensuring IT administrators are efficient and end user experiences are unaffected – all while keeping corporate data secure and complying with data privacy legislation, such as the United States' Health Insurance Portability and Accountability Act (HIPAA), Personal Information Protection and Electronic Documents Act (PIPEDA), or the United Kingdom's Data Protection Act.

Organizations need to ask some pointed questions in order to understand what BitLocker can do and more importantly what it can’t do so they can deploy a solution that addresses all devices and all FDE requirements:

Does BitLocker support multi-factor authentication in pre-boot?

Can I have multiple user logins available in pre-boot?

Can I use Active Directory credentials for pre-boot authentication?

Can BitLocker support non-Windows environments?

How do I share encrypted removable media on non-Windows systems?

Does BitLocker support Windows XP?

Does BitLocker work with Opal Self-Encrypting Drives (SEDs)?

Can Microsoft BitLocker Administration and Monitoring (MBAM) manage any other systems or only Vista, Win 7 and Win 8?

What infrastructure do I need to have at the back end to support MBAM?

Is a dedicated SQL server required for MBAM?

How much will that Windows Server and SQL server cost?

All of these questions are critical when evaluating BitLocker’s effectiveness and what you may require to fully support FDE across your organization.

BitLocker by Default

BitLocker is commonly used for FDE because it’s included with the Ultimate and Enterprise editions of Windows 7, and with the Pro and Enterprise editions of Windows 8 desktop operating systems, as well as Windows Server 2008, Windows Server 2008 R2 and Windows Server 2012.

Because BitLocker is a free feature in commonly used flavors of the Windows OS, it’s not surprising that enterprises opt to make use of it rather than invest in a third-party encryption solution. However, in the IT world, there’s no such thing as free. Standardizing on BitLocker brings with it hidden costs, and they’re not just financial, which is why BitLocker can be a great starting point for organizations that want to benefit from the peace of mind of FDE, but ultimately it’s only one piece of an overall data security strategy.

BitLocker's Total Cost of Ownership

The cost of maintaining technologies is often not understood until it is fully implemented. So while BitLocker may seem appealing because it comes baked into Windows OS PCs, laptops and servers, there are administration and management factors that determine BitLocker’s Total Cost of Ownership (TCO).

Hardware: A key unforeseen cost when standardizing on BitLocker can be additional hardware requirements. For example, even if you already have deployed a Windows OS that includes BitLocker, each system requires a Trusted Platform Module (TPM) chip in order to access all of BitLocker’s features. Adding a TPM chip to every devices in an organization to fully realize BitLocker’s benefits is a significant investment at roughly $30 per machine. In addition, that chip will need to be configured and enabled, which means each device has to be touched at least once by an IT Admin. Depending on the number of devices you wish to secure with BitLocker, that’s a great deal of time and resources that could be used elsewhere, assuming you even have the IT staff to support it.

Software: Standardizing on BitLocker may require you to upgrade some of your enterprise Windows licenses or make sure you have additional Microsoft software to support Microsoft BitLocker Administration and Monitoring (MBAM). This includes a dedicated Windows and SQL server, which is no small expense. Windows Server requires volume licensing agreements as well, either on a per client basis or a per core basis. For example, SQL Server Enterprise edition licensing can cost $6,874 per core, and given most servers run systems with multiple cores, it’s a very expensive proposition on an annualized basis.

Legacy, BYOD and beyond Windows: The larger problem is that BitLocker doesn’t support workstations running older versions of Windows, although most organizations have likely migrated from XP by now or have begun the process as Microsoft support for the OS comes to an end. But the problem of non-Windows devices remains. BitLocker does not support Linux, Mac OS X or Android, all of which are likely to exist in some shape or form within the enterprise, especially on mobile devices. And all it takes is a single unprotected system to offset all of your full disk encryption efforts. Unless you can ensure that only supported Windows OS devices will be used in your organization or connect with your enterprise network, you will have to enhance BitLocker with third-party FDE software to adequately manage non-Windows devices alongside those encrypted by BitLocker.

Management: When using BitLocker alone, users and administrators are able to take advantage of strong native encryption, but authentication is device-based, not user based, as today’s businesses require. Solutions that have the ability to manage devices running various platforms help fill a key gap in this native encryption offering. More importantly, the requirement would be to have a centralized management console to support all devices and orchestrate FDE, including Windows devices using BitLocker and devices on other platforms such as Mac OS, Linux and Android. This will offset the cost of having multiple tools in place to manage encryption, not just from the upfront cost of purchasing and deployment, but also from an ongoing operations perspective as it means requiring more IT skills to understand these various solutions and developing communications protocols so that all administrators are collaborating effectively.

SecureDoc Simplifies BitLocker Management

SecureDoc, WinMagic's core offering, secures data at rest by managing how it is encrypted, regardless of where it resides and on any operating system. SecureDoc gives enterprises a comprehensive data security solution that supports compliance with security and privacy regulations without increasing IT costs significantly and compromising end user productivity. SecureDoc is not limited to Windows-based devices, and protects sensitive data residing in laptops, desktops, mobile devices, servers, removable media and SEDs.

Designed with the heterogeneous IT environment in mind, SecureDoc organizes all security-related management under one centralized enterprise server including policies, password rules, and the manageability of encryption across PC, Mac and Linux platforms. Using SecureDoc, enterprises can manage BitLocker within this single umbrella.

SecureDoc improves upon BitLocker's encryption capabilities by providing IT administrators with tools to manage it, while also securing non-Windows devices and addressing BYOD and cloud computing. Administrators can leverage existing network log-in credentials (instead of only a PIN) in addition to multi-factor authentication with smart cards or other tokens to lock down system access and guarantee high-level security of devices. This multi-factor authentication approach is critical for many government institutions and organizations with high security requirements.

PBConnex Adds Pre-Boot Network Authentication to BitLocker

SecureDoc further enhances BitLocker by being the only data encryption and management solution that supports pre-boot network authentication (PBNA) through its PBConnex technology, which uses network-based resources to authenticate users, enforce access controls, and manage end point devices before the operating system loads.

PBConnex enhances security through authentication at pre-boot rather than at the Windows login and improves policy protection by making it easy for administrators to push system updates. Users enjoy an improved experience with simplicity of single password access as well as straightforward reset and recovery options. PBConnex's TCO for organizations is low because it's easy to provision thanks to simple, effective Active Directory integration and remote management capabilities that can enable encryption and revoke users in real-time. PBNA provides a means for authenticating encrypted devices to the network before the operating system ever loads. Before any data on a device is decrypted and a user granted access, the user must input their credentials in the form of a password that is verified by a network connected server and then allow the user to log-on to a device and start the operating system (OS) log-in process. It means data is never exposed until the user credentials are verified before the standard OS log-in process.

Standard device encryption is fallible regardless of the solution deployed. PBNA mitigates risk because instead of relying solely on user credentials stored locally on a given device which can be out of date, the authentication process leverages the most current policies available from that server to manage user access. This means an administrator could remotely lock out an employee that just left the company without having direct access to his/her device, which is both more secure and more cost-effective.

But PBNA provides much more than end point security. It also allows businesses to manage groups and really control how, what, when and where users access information via policy controls. In conjunction with BitLocker, end users can access any approved systems using only one password. Upon successfully logging in, they can use all authorized applications with virtually no impact to the speed and performance to their work station. PBConnex takes user credentials and validates them against the SecureDoc Enterprise Server (SES). SES is constantly syncing with the Microsoft Active Directory to ensure the most up to date information is available. Once SES authenticates the user by verifying credentials the system is allowed to continue the log-in process. Finally the system boots and the user has access to the system.

SES is available via the internet - authorized users around the world can connect to a wireless network and authenticate against SES and Active Directory. Meanwhile a wireless version of PBConnex offers organizations all the benefits of PBConnex without the need of a network cable by enabling authenticated users to boot their device without a local key file and to access the internet with a pre-boot browser.

SecureDoc Simplifies Data Security

In addition to PBNA, SecureDoc offers a number of features that enhances a BitLocker deployment by making it more secure, easier to manage and more user-friendly.

Secure and Self-Help Password Recovery: SecureDoc enables the use of self-help recovery questions so that users can recover access in the event of forgotten passwords without burdening the help desk. SecureDoc enhances the security of the recovery process by generating a onetime sequence of characters for remotely assisted recovery which is never reusable. It also sends encryption keys directly to the SQL Server database and provides the option not to continue with the encryption until the key is safely delivered.

Simplified Password Recovery: BitLocker requires AD Domain Administrators to retrieve the recovery passwords. By requiring the help desk or general IT staff to support password recovery, it means providing access to every encrypted drive to far too many staff. SecureDoc's Challenge Response password recovery process for remote password recovery can easily be outsourced to the help desk and other general IT staff as it is not providing access to any password which could later be used to access encrypted data.

Password Synchronization, Single Sign-on and Multi-Factor Authentication: SecureDoc enhances BitLocker by adding password synchronization which enables a user to have the same password for pre-boot authentication and for Windows log-on. This reduces the instances of forgotten passwords and therefore reduces support costs. SecureDoc also supports Single Sign-On so users can log-on once at Pre-Boot and then be automatically authenticated right through to the user's Windows desktop. Because the user only needs to enter their password once, the possibility of user error and support calls are less likely and users are more accepting of the security process. SecureDoc can also support multi-factor pre-boot authentication, including UPEK fingerprint readers, smart cards, USB tokens, trusted platform modules and CAC/PIV cards.

Support for Self-Encrypting Drives: SecureDoc maintains compatibility with the latest secure hard drives which are being carried or introduced by most leading laptop manufacturers. Called Self-Encrypting Drives (SEDs), they feature better performance, faster set-up, and more security than traditional drives (by removing the risk of vulnerabilities such as COLD RAM/Boot Attacks) with software encryption. WinMagic has been working with the Trusted Computing Group (TCG), a not-for-profit organization formed to foster interoperable trusted computing platforms, and supporting its Trusted Platform Module (TPM) and Opal SED specification since its inception. WinMagic offers unparalleled Opal SED management with SecureDoc. No other product in market has a solution that is as robust in its integration. Additionally, to meet the demands of servers, larger storage is required that can be supported by TCG Enterprise drives, which offer the best, most secure and efficient way to encrypt data on a disk. With OSA (Operating System Agnostic) for Servers, WinMagic has removed a key pain point for IT administrators and enabled remote unattended booting/rebooting of departmental servers via our pre-boot network authentication, something traditionally impossible for encrypted servers.

No TPM Chip Required: SecureDoc bypasses the need for a TPM Chip or a USB to store the key, which avoids a number of problems and limitations, such as:

1. The need for users to contact support when they can’t authenticate.
2. System status confusion as a result of docking or undocking a portable computer.
3. Moving the hard drive to a new computer where the original TPM chip is absent.
4. The need for the function keys (F1 through F10) for inputting the user’s TPM PIN, which is not intuitive.

In addition to not requiring the TPM chip, SecureDoc supports the use of keyboard passwords and passphrases which are easier to remember, resulting in fewer user authentication issues and fewer support calls. When a hard drive is moved to a new machine, the same authentication as was required on the previous machine can be leveraged.

Multiple Platform Support: While BitLocker supports your Windows devices, SecureDoc can encrypt and support other devices that run on Mac OS X or Linux operating systems (using SEDs), all from the same console.

Enterprise organizations that are heavily invested in Microsoft environment are sure to gravitate to BitLocker given that it is already baked into the Windows 7 and 8 OS, but in the era of BYOD, it's impossible not to have other platforms accessing your network and your data. These devices, whether Mac or Linux, will negate all of your FDE efforts if they are not properly secured and encrypted.

SecureDoc with its PBConnex functionality can enhance your BitLocker deployment with additional features that both improve security and provide ease of management by bringing the device management in a centralized console. Both end users and IT staff will see productivity gains, and overall you will realize a far better cost of ownership with WinMagic's SecureDoc as your primary interface for managing device encryption.

WinMagic's SecureDoc with BitLocker support in combination with its PBConnex technology reduces the cost of ownership by being easy to provision through simple, effective Active Directory integration and support for remote encryption and real-time user revocation, improve user experience with single password access, increased and enhanced security with PBNA and easy policy protection that allows administrators to push system updates and policies.

Today's businesses are increasingly working in hybrid security environments that include a combination of hardware and software encryption and multiple operating systems on a broad array of devices. With the addition of BitLocker management support in SecureDoc, customers no longer have to choose how and what to do for data encryption within their organization. Whether it's SecureDoc on mobile devices such as laptops, SED management and BitLocker on desktops that are less prone to loss and theft, SecureDoc can offer a single console to manage everything.

Deploying WinMagic's SecureDoc to manage BitLocker-encrypted devices as well as encrypt and manage devices on other platforms such as Mac and Linux means enterprise organizations can be assured their mission-critical data is safeguarded while addressing the compliancy and regulatory requirements in their industry. FDE can be achieved without negatively affecting existing processes and being transparent to the users. The end result for the organization is increased security, improved end-user experience and ease of management, all at lower IT costs.

WinMagic provides the world's most secure, manageable and easy-to-use data encryption solutions. With a full complement of professional services, WinMagic supports over 5 million SecureDoc users in approximately 84 countries. We can protect you too.

For more information on SecureDoc Enterprise Server contact **sales@winmagic.com** or visit our website to access a number of valuable resources:

PRODUCT PAGE
http://www.winmagic.com/products

WHITE PAPERS
http://www.winmagic.com/resource-centre/white-papers

CONTACT

WinMagic Inc.
Phone: 905. 502. 7000
Fax: 905. 502. 7001

Toll Free: 888. 879. 5879

sales@winmagic.com
www.winmagic.com

WINMAGIC
SECUREDOC FOR SERVERS
SecureDoc FOR SERVERS
SECUREDOC ENTERPRISE SERVER MANAGEMENT CONSOLE
SecureDoc ENTERPRISE SERVER
SECUREDOC FOR WINDOWS - STANDALONE
SecureDoc

SOCIAL MEDIA

http://blog.winmagic.com/

http://www.facebook.com/WinMagicInc

http://www.linkedin.com/company/winmagic

http://twitter.com/winmagic

http://www.youtube.com/user/winmagicinc

WANT TO TRY OUR SOFTWARE?

CLICK HERE TO REQUEST A FREE EVALUATION ›