Whitepaper

# *Enhancing BitLocker Deployment and Management with SimplySecure*

Addressing the Concerns of the IT Professional

Rob Weber

February 2015

# Table of Contents

## What is BitLocker?

Microsoft’s BitLocker is a volume-based encryption feature included with the Ultimate and Enterprise editions of Windows Vista and Windows 7 and the Pro and Enterprise editions of Windows 8 and Windows 8.1. It is designed to protect data by providing encryption for entire volumes. BitLocker encryption has been deemed FIPS 140-2 compliant and by default, it uses the AES encryption algorithm in cipher block chaining (CBC) mode with a 128-bit or 256-bit key.

In order for BitLocker to operate, at least two NTFS-formatted volumes are required: one for the operating system (usually C:) and another with a minimum size of 100 MB from which the operating system boots. BitLocker requires the boot volume to remain unencrypted. For devices running Windows 7 or greater, the operating system creates the secondary boot volume by default even if BitLocker is not used initially.

Once an alternate boot partition has been created, the Trusted Platform Module (**TPM**) needs to be initialized (assuming that this feature is being used).

## What is the Trusted Platform Module (TPM)?

TPM is an international standard for a secure cryptoprocessor, which is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices. TPM's technical specification was written by a computer industry consortium called the Trusted Computing Group (TCG). After the TPM is initialized, the required disk encryption key protection mechanisms such as TPM, PIN or USB key are configured. The volume is then encrypted as a background task, something that may take a considerable amount of time with a large disk as every logical sector is read, encrypted and rewritten back to disk. The keys are only protected after the whole volume has been encrypted, when the volume is considered secure. BitLocker uses a low-level device driver to encrypt and decrypt all file operations, making interaction with the encrypted volume transparent to applications running on the platform.

## What is Microsoft’s Recommended Best Practice for Encryption?

To ensure maximum protection, Microsoft recommends that BitLocker be used in conjunction with Microsoft’s file and folder encryption schema, the Encrypting File System (EFS). As described above, BitLocker encrypts all personal and system files on the operating system drive, and fixed and removable data drives. It does not depend on the individual user accounts associated with files, and is either on or off for all users or groups. It essentially protects data when the computer is off.

On the other hand, EFS works after Windows boots up, and encrypts files based on the user account associated with it. If a computer has multiple users or groups, each of them can encrypt their own files independently such that no user (or administrator) can access another user’s files (i.e. data isolation). **EFS encryption also protects user data from network-borne attacks.**

## Assessing Native BitLocker

Although it can be deployed by individual users using the BitLocker drive encryption control panel, if an organization were to deploy BitLocker via Active Directory, a command line utility must be used.

Without any enhancements, BitLocker enables an organization to specify in some form the following features on its domain machines:

- Choice of encryption strength
- Back up of recovery key to a specific location
- Specification of the type and complexity of authentication mechanisms
- Choice of whether or not to allow write access to drives not protected by BitLocker

On its own, BitLocker provides less functionality than most enterprise software full disk encryption solutions.

## BitLocker With SimplySecure

SimplySecure enhances native BitLocker by providing a set of added benefits centered around ease of deployment and streamlined management. These benefits include:

1) **SimplySecure Manages BitLocker on Non-Domain Machines and Remote Domain Machines With Little or No Access to the Domain.**

   Native BitLocker requires that all machines be on the domain. This simply is not practical in many organizations. SimplySecure only requires that the machine can check in with the SimplySecure server. This affords non-domain machines and remote domain machines with sporadic access to the domain the same protection as domain devices.

2) **SimplySecure Auto-Enables BitLocker on Devices With TPM (v1.2) Chips Without User Interaction**

   Deployment of native BitLocker can be quite time consuming. Without SimplySecure, each machine must be physically touched by IT in order to enable BitLocker. IT is responsible for making sure each of the following steps occur:

   - The TPM chip must be enabled. Many computer manufacturers ship their products with the chip disabled. To enable the chip, the machine must be rebooted and a hot key (usually F12) must be held down to access the BIOS. System menus are then used to enable the chip.
   - The TPM chip must then be initialized. Even if the TPM chip is already enabled on a device, IT will still have to initiate initialization. This is accomplished by accessing the TPM Management console on the computer where a TPM Management password will be assigned. The computer must then be rebooted and the new TPM Management password entered in a separate BIOS window in order to complete the reboot.
   - Finally, BitLocker can be enabled through the BitLocker Management Console. This will begin the BitLocker encryption pass. Advanced IT departments may be able to accomplish this task using a script.

   SimplySecure can remotely enable and initialize the TPM chip on most Dell, HP and Lenovo computers. The SimplySecure console allows IT to automate the entire deployment process.

3) **When BitLocker is Enabled on the System Drive, SimplySecure Can Auto-Enable BitLocker For All Other Internal Fixed Drives**

   As stated before, many organizations encounter all matter of configurations when assessing their computing environment. Many computers have multiple drive configurations. The data on these extra drives must also be encrypted and protected. If BitLocker is enabled on the system drive of a computer, SimplySecure can enable it on all other fixed drives. Previously it was noted that SimplySecure can auto-enable BitLocker on machines with TPM chips. Therefore, if a device contains a TPM chip and a multiple drive configuration, it is possible for your organization to encrypt the entire device without physically touching the device.

**4) SimplySecure Provides a Key Escrow Service for all BitLocker Key Protectors (not just recovery/numerical passwords)**

BitLocker has several different key protector types and key protector combinations. They are:

- Trusted Platform Module (TPM)
- External key
- Numerical password
- TPM And PIN
- TPM And Startup Key
- TPM And PIN And Startup Key
- Public Key
- Passphrase
- TPM Certificate
- CryptoAPI Next Generation (CNG) Protector

Keys are added/changed even when machines are not in the domain environment. As long as there is an internet connection, those keys are sent to the SimplySecure administrative server.

**5) Operational Benefits of BitLocker with SimplySecure**

Administrators of any BitLocker deployment are bound to encounter operational issues after the initial roll out. Incidents such as failed hard drives or motherboard swaps could leave BitLocker protected devices unusable. If your organization is using SimplySecure, any needed keys are available on the console and restoration is quick and easy.

**6) Remote Secure Decommissioning via SimplySecure**

Decommissioning a BitLocker device is akin to removing access to the drive. To securely decommission the drive so that prying eyes cannot retrieve data from it, an administrator must remove all the BitLocker key protectors from the drive. Without these, the data is not readable. SimplySecure allows the administrator to perform this task remotely from the SimplySecure administration console. The Secure Decommission command set includes the following:

- Elimination of all known BitLocker key protectors
- Creation of a recovery password that only the SimplySecure Server has
- Shutting down the computer to prevent access

### 7) Key Restoration via SimplySecure

SimplySecure employs two methods to protect a device in the event it is suspected to be lost or stolen. First, an administrator can manually delete the keys from a device using the administration console. Second, many versions of SimplySecure will also monitor and automatically respond to certain conditions deemed to be of sufficient security risk. These automatic responses can include key deletion from an affected device.

But what happens when the device is recovered or it is determined that the device was not lost or stolen or there is a hardware failure? Since the keys are escrowed on the SimplySecure server, an administrator has the ability to use the console to push the keys back down to the machine to restore the device to its original state upon its next check-in.

### 8) Auditing and Monitoring of Encryption Activities via SimplySecure

SimplySecure can help an organization to deploy and manage BitLocker devices, but it can also provide logging information about these devices which can help an administrator troubleshoot problems and complete audit reports. Encryption helps protect an organization's assets, but the real reason many people deploy encryption is to ensure they are in compliance with government mandated rulings. The logging reports that SimplySecure provides shows when encryption is deployed upon a device and when it completes. This information can be used to prove to an auditor that a device is within compliance.

### 9) BitLocker Can Be Suspended From the SimplySecure Console

Sometimes when a device is having a system issue, it is necessary for BitLocker to be disabled before the issue can be addressed. For example, when a BIOS update is needed, BitLocker must be disabled before the BIOS update can be applied. Failing to do so would lock the end user out of the machine and put the device into recovery mode. With SimplySecure, an administrator can suspend BitLocker on a device directly from the SimplySecure console. Once the problem is addressed, the device can be taken out of suspension from the console.

### 10) Persistent BitLocker Enforcement

Once BitLocker has been deployed on a device, it may be possible for a savvy user to disable the protection. If your organization is using SimplySecure, the client device will be instructed to re-enable BitLocker and resume protection.

### 11) SimplySecure Provides Single Console Management for all Security Activities

Many organizations have to manage computing devices that run the gamut when it comes to operating systems, memory, storage, and horse power. The SimplySecure platform allows an organization to manage security on all of its devices from one consolidated administration console. SimplySecure provides support for encryption on PCs (EFS, BitLocker, or both), Macs (FileVault), iOS devices, Android devices, and USB flash drives. In addition, SimplySecure's rule and trigger based scheme provides protection beyond that associated with encryption.

BitLocker provides encryption security for your devices, but managing those devices will almost certainly be problematic for an IT department.  SimplySecure offers ease of use along with added features intended to take advantage of the BitLocker platform.

Beachhead Solutions Inc.
1955 The Alameda
San Jose, CA 95126
Question, comments? Write Rob Weber
rweber@beachheadsolutions.com