BEACHHEAD

Whitepaper

Using BeachheadSecure™ to Deploy, Enforce & Manage BitLocker

Organizational management plus access control managed through the cloud

November 2019

What is BitLocker?

Microsoft's BitLocker is a volume-based encryption feature included with the Enterprise and Ultimate editions of Windows 7, the Enterprise and Professional editions of Windows 8 and 8.1, and the Education, Enterprise, and Professional editions of Windows 10. In addition, it is also a feature of both Windows Server 2012,2016 and 2019. BitLocker is designed to protect data by providing encryption for entire volumes. BitLocker encryption has been certified 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)

The Trusted Platform Module (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 them. 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 where BitLocker does not.**

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

BitLocker by itself provides less functionality than even out-of-date software-based full disk encryption in large part because there is no organizational management component. The organization must place trust in their users to ensure persistent operation (e.g. any logged-in administrator can turn BitLocker off on a machine) and often, for backup and safekeeping of mission-critical encryption keys. Reliance on users to manage any component of data security, particularly a tool as complex as BitLocker is a poor practice. Compliance, and perhaps more importantly, *proof of compliance* is neither guaranteed, reported, nor provable under an audit or a breach.

BeachheadSecure-Managed BitLocker

BeachheadSecure is an entirely cloud-managed platform that gives an IT professional the ability to remotely deploy, enforce and manage native BitLocker throughout an inventory of PCs. Further, BeachheadSecure provides a host of additional security features (including remote access-control capabilities) that will protect PII and sensitive business data under threats when BitLocker alone cannot. Perhaps most importantly, the platform removes user involvement for BitLocker efficacy. Encryption must be organizationally managed both to ensure true data security and as evidence of effective compliance practices.

A comprehensive list of these benefits are included in Appendix A at the end of this whitepaper, but the following benefits are written specifically for the IT Professional and underscore the value of the BeachheadSecure Platform.

EASY, REMOTE INSTALLATION

BeachheadSecure Remotely Auto-Enables and Initializes BitLocker Devices with TPM Chips (Versions 1.2 and 2.0)

Deployment of native BitLocker can be quite time consuming. Without BeachheadSecure, each machine must be physically touched in order to enable BitLocker. An IT staff 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, your IT staff 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 then 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.

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

BeachheadSecure Remotely Auto-Enables and Initializes BitLocker Devices on PCs without TPM Chips)

Although thought to be standard on all modern computers, not all PC hardware ship with TPM Chips making the deployment of BitLocker even more challenging.

Such customer environments having a mixture of older and new PCs, some with and others without TPM chips make it difficult for the centralized rollout and remote servicing of BitLocker by IT departments and MSP's alike. Windows 8 and above allows for the use of a password on computers without a compatible TPM in order to enable BitLocker, however this requires manual configuration changes including users editing the group policy on the local PC to allow for the use of the password-based authentication mode for BitLocker. Without BeachheadSecure, each machine must be physically touched in order to enable BitLocker. IT staff is responsible for making sure each of the following steps occur:

For non-TPM PCs, users need to edit the computer local group policy and then manually enable BitLocker, prepare the drive for encryption, create a password for unlocking the drive on start-up in order to encrypt the OS volume with BitLocker, manually backup the keys and then encrypt the drive.

BeachheadSecure can remotely allow for the password-based authentication mode on computers without TPM Chips or fallback to the password authentication mode when the TPM cannot be initialized in the BIOS in order to remotely enable BitLocker. Users need only to enter a password for BitLocker when automatically prompted to. The BeachheadSecure console allows your IT staff to automate the entire deployment process, even on non-TPM computers.

When BitLocker is Enabled on the System Drive, BeachheadSecure Can Auto-Enable BitLocker For All Other Internal Fixed Drives

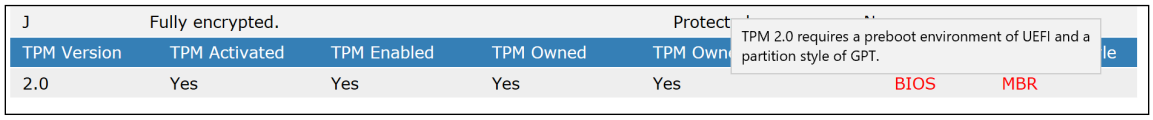
As stated before, many organizations encounter all matter of configurations when assessing their computing environment. Many computers have multiple drive configurations. The data on these extra drives must also be encrypted and protected. If BitLocker is enabled on the system drive of a computer, BeachheadSecure can enable it on all other fixed drives. Previously, it was noted that BeachheadSecure 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.

BeachheadSecure Tracks TPM Chip Status, Pre-Boot Environment, and Partition Style; Are There Any Compatibility Issues?

Deploying BitLocker in your environment can be a challenge at times. Incompatibilities between the bios, the operating system, and the hardware configuration can create roadblocks to a successful deployment. For troubleshooting purposes, BeachheadSecure provides administrators with information about the TPM chip, the pre-boot environment and the partition style along with warnings about any incompatibilities that might be causing problems.

The BeachheadSecure BitLocker tab for each deployed device lists several pertinent pieces of information. Two columns, Preboot and Partition Style, call out issues when they are encountered. These columns will display in black if everything is okay. However, they will display in red if there is a compatibility issue. If you mouse over either of the columns when the display is red, a box will display with an explanation. See examples of each screen below:

TPM Version	TPM Activated	TPM Enabled	TPM Owned	TPM Ownership Allowed	Preboot	Partition Style
2.0	Yes	Yes	Yes	Yes	BIOS	MBR



Deployment Status and Tracking; What Is the Current State of BitLocker Installations?

Not all BitLocker deployments are created equal. The proper combination of operating system and hardware can lead to a relatively easy process with little downtime for the end user. However, other operating system and hardware combinations may call for user intervention, multiple reboots, and / or IT help.

The BeachheadSecure administration console tracks and reports the current state of a BitLocker setup for each machine under its purview. Once the initialization and drive encryption is fully completed for a device, the console will report that the "System is BitLocker Protected" on the device's BitLocker tab. Administrators can view the BitLocker status for multiple devices from the Computers listing.

In addition, BeachheadSecure provides a BitLocker Status Report for each account. 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 produced by the BeachheadSecure platform can be used to prove to an auditor that a device is compliant.

Reporting and Management of TPM PCR Values; What Triggered a BitLocker Recovery?

Another BitLocker deployment 'gotcha' can occur after encryption has completed. Without warning, a device may go into BitLocker Recovery mode. This is frustrating for both the end user and the IT staff. Why did it happen and how can it be prevented from happening again?

The TPM PCR (Platform Configuration Register) value can be used to determine why a device went into recovery mode. For example, sometimes a BIOS update may be in conflict with BitLocker. That issue may trigger a recovery event.

The BeachheadSecure BitLocker tab for each deployed device features a Platform Validation Profile. Within the profile are the possible TPM PCR values. If you mouse over a number, it will provide a short definition of the value as provided by Microsoft. The display will indicate which value(s) triggered the BitLocker Recovery. Without this knowledge, administrators would never know why a recovery event occurs. As the administrator, you have the ability to correct the issues which triggered the BitLocker Recovery or bypass them right on the BeachheadSecure administration console. Now you can complete your deployment without worrying about the same issue cropping up on other devices.

CENTRALIZED CLOUD-BASED MANAGEMENT

BeachheadSecure 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. BeachheadSecure only requires that the machine can check in with the BeachheadSecure server. This affords non-domain machines and remote domain machines with sporadic access to the domain the same protection as domain devices.

BeachheadSecure Backs Up 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 can be added or changed even when machines are not in the domain environment. As long as there is an internet connection, those key protectors are sent to the BeachheadSecure administrative server.

BitLocker Can Be Suspended from the BeachheadSecure Console

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 BeachheadSecure, an administrator can suspend BitLocker on a device directly from the BeachheadSecure console. Once the problem is addressed, the device can be taken out of suspension from the console.

Automated BitLocker Suspension Triggered by Windows Updates

The multitude of Windows updates can provide a problem for an IT staff that is supporting devices protected by BitLocker. Each time the decision is made to allow for an update, BitLocker must be manually suspended on the devices in question. After the update is applied, BitLocker must be manually taken out of suspension on each device.

With BeachheadSecure, each client device will recognize when Windows updates are available and automatically suspend BitLocker. Once the update is complete, BeachheadSecure will automatically take the device out of suspension. Other than making the initial decision to allow for automatic Windows updates via BeachheadSecure, the IT staff does not have to be involved.

COMPLIANCE REQUIREMENTS

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 BeachheadSecure, the client device will be automatically instructed to re-enable BitLocker and resume protection.

Reporting

BeachheadSecure provides a variety of reports to choose from that can be automatically generated on prescribed dates (e.g. weekly, monthly) and automatically emailed to your designates, or on-demand as/when required. Security risk assessments, regulation compliancy and audits require evidence of strong data security practices of which encryption is included. Easy export of any screen within the administration console is available should the organization choose to build custom reports.

SECURITY ENHANCEMENTS (BEYOND ENCRYPTION)

Remote Secure Decommissioning via BeachheadSecure

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 unreadable. BeachheadSecure allows the administrator to perform this task remotely from the BeachheadSecure 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 BeachheadSecure Server has
- Shutting down the computer to prevent access

Key Protector Restoration via BeachheadSecure

BeachheadSecure provides two methods to protect a BitLocker device in the event it is suspected to be at risk. First, administrators can manually mark the device lost or stolen on the administration console. This will trigger the action to delete the key protectors from the device. Second, BeachheadSecure can also monitor and automatically respond to certain conditions deemed to be of a sufficient security risk. For example, making a hardware change on a device may be deemed as a security risk. This may cause BeachheadSecure to initiate the deletion of key protectors on the device.

But what happens when the device is recovered or it is determined that the device was not at risk? Since the key protectors are escrowed on the BeachheadSecure server, an administrator has the ability to use the console to push the key protectors back down to the device. After the end user goes through the recovery process, the device will be restored to its original state.

CROSS-PLATFORM ENCRYPTION MANAGEMENT

BeachheadSecure 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 BeachheadSecure platform allows an organization to manage security on all of its devices from one consolidated administration console. BeachheadSecure provides support for encryption on PCs (EFS, BitLocker, or both), Macs (FileVault), iOS devices, Android devices, and USB flash

drives. In addition, BeachheadSecure's rule and trigger-based scheme provides protection beyond that associated with encryption.

Beachhead Solutions Inc.
1150 S. Bascom Avenue
San Jose, CA 95128

Question, comments?
408.496.6936info@beachheadsolutions.com

APPENDIX A. BEACHHEADSECURE BITLOCKER FEATURES

(features in bold italic discussed in whitepaper)

Easy, Remote Installation

Automatically enable TPM on Lenovo, HP and Dell PCs

Automatically provision PCs for BitLocker enablement on non-TPM PCs

Auto-enable BitLocker for all internal drives

Tracks Compatibility issues with TPM, Pre-Boot Environment, and Partition Styles

Deployment Status and Tracking

Reporting and Management of TPM PCR Values; What Triggered a BitLocker Recovery?

Remote and silent web-based installation

Automatic client- or account-wide installation

Centralized Cloud-Based Management

Manages BitLocker on Non-Domain Machines and Remote Domain Machines

BeachheadSecure Backs Up All BitLocker Key Protectors

BitLocker Can Be Suspended From the BeachheadSecure Console

Automated BitLocker Suspension Triggered By Windows Updates

Persistent and organizationally enforced encryption (user or thief can't disable)

Centralized key management

Entirely web-managed console

Multi-tenanted client account management (from one administration console)

Graphical user interface alerts administrator of at-risk device(s) across all accounts

Easily navigate to devices requiring attention from graphs

Does not require user/employee involvement to install or manage

Key day-to-day management functionality & licensing available through Datto/Autotask RMM (Feb '19)

Manage BitLocker and/or EFS on non-domain PCs

Password and lockout polices for non-domain PCs

Nested access control policy setting by client account (sub-account, sub-sub account etc.)

Compliance Requirements (e.g. HIPAA, GDPR etc.)

Persistent BitLocker Enforcement

Comprehensive reporting, automated reports

Snapshot evidence from administration console

Full assortment of reports (including computer status, audit log, mobile and others)

Security Enhancements (in addition to BitLocker)

Remote Secure Decommissioning via BeachheadSecure

Key Protector Restoration via BeachheadSecure

Remote data wipe

Remote access control (deny & restore access to device)

EFS Encryption for additional encryption security layer

Prevents, reports and thwarts network-borne attacks

Persistency user/employee cannot disable

Automatic responses to invalid login attempts (including access denial)

Automatic responses to time-based excesses (including access denial)

Cross-Platform Encryption Management

Encryption for Windows OS 10 Computers (Pro or above)

Encryption for Windows OS 8 Computers (Pro or above)

Encryption for Windows OS 7 Computers (Pro or above)

Remote access control for Windows OS 10 Computers (Pro or above)

Remote access control for Windows OS 8 Computers (Pro or above)

Remote access control for Windows OS 7 Computers (Pro or above)

Encryption and remote access control (including full wipe) for USB Drives

Authentication policy setting (including optional 2-factor) for encrypted USB Drives

Encryption and remote access control for iOS Phones & Tablets (same console)

Encryption and remote access control for Android Phones & Tablets (same console)

Encryption for Windows Servers (same console)