Microsoft bitlocker is a full disk encryption tool/software to help protect data that is saved on the hard drive that has Microsoft windows installed on the system.

Microsoft first released the first version of Bitlocker with Windows Vista, and Windows Server 2008. It is available on all current windows operation systems, from client to servers. Microsoft has added and enhanced the features of bitlocker over the years making it more secure. Bitlocker is Microsoft's solution to full desk encryption. Bitlocker works at its strongest when it is paired up with a Trusted Platform Module (TPM) version 1.2 chip. A TPM chip is a hardware component installed in most newer computers. It allows the recovery key for bitlocker to be stored in the chip securely so the system's hard drive can be unlocked when it the system is booted up. When using the TPM chip your, you have to have password set on the BIOS, if you do not set up a BIOS password it will not let you use the TPM chip. If the computer does not have a TPM chip, you can use either a PIN/Password. If you use a PIN/Password, the system will require you to enter the PIN before the system will boot up and load the operating system. A USB drive may be used if the system does not have a TPM chip.

When a PC boots up it will look for the either the TPM chip or the USB key. There are several different ways to setup bitlocker at startup of a pc. The startup options are TPM, TPM + PIN, TPM + USB key, PIN + USB key or just PIN. If one of the ways is not present when the system tries to boot, it will ask you for the recovery key. The recovery key is a 25-digit key, without this key all the data on the drive will be lost.

The recovery key is created when you enable bitlocker. When bitlocker is enabled, it will ask you where you would like to store the recovery key. You can store it

on a network drive, another hard drive that is in the system or even an usb drive with the last option to print it off. The print it off option is the least secure. This is because if someone finds the paper, they will be able to access your data, as they will have the recovery key. If the system is part of an Active Directory Domain, there is a way also to store the recovery key in active directory itself. The key to recovery keys is to keep them safe. You don't want your end users having access to them unless they really need access to them. The more people that have access to them, the less secure the drives and data you have on them are.

There are different ways in which you can setup bitlocker. If it is a standalone system and you have admin rights, if you right click on the drive you want to enable bit locker on, and select enable bitlocker, a wizard will appear. As you run through the wizard it will ask you some questions, for example, where do you want to store the recovery key. It will also ask you to setup a PIN, but if the system has a TPM chip in it you can initialize it using the TPM management console (tpm.msc) before you run the wizard. In order for you to enable bitlocker on a system drive and/or partition, the system also has to have a special partition on the drive. In most cases the partition it uses to store information about how to unlock the drive and boot information is in the system reserve partition. This partition is created when you load the operation system It use to only be 100 MB in size but as newer versions of windows have been released this size has not increased. This partition will not be encrypted, as a system cannot boot from an encrypted drive and this partition will allow you to unlock.

If you are deploying bitlocker in a bit organization, it can be deployed via group policy settings. When you enable the right bitlocker group policy objects. The group

policy settings are located using the group policy management console (GPMC), all setting for bitlocker are under Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption. If you enable bitlocker in your origination using group policy, you may have to have some custom scripting to go along with it. Some things you may have to script are, the creation of the reserved partition on the hard drive if the partition is not big enough to hold all the info that bitlocker requires. BIOS setting, if your bios is not up-to-date, you may have to update the bios to get bitlocker to work. Also in the BIOS scripting you will need to set the TPM chip to active/on, set the BIOS password. These are just a few of the thing you may have to script to get bitlocker working.

BitLocker supports two levels of cipher strength for BitLocker: 128-bit and 256-bit. Both use the Advanced Encryption Standard (AES) to perform encryption. By default, it uses 128-bit. In most enterprises, the companies opt to go with the 256. Bitlocker uses block cipher encryption algorithm. Block cipher encryption, divides the data into fixed block size and encrypts the data.

When you need to recovery drive that has been encrypted you cannot just slave the drive to a working pc unless you have the recover key. When you slave the drive that have been encrypted into a windows system, it will ask you for the bitlocker recovery key. When you enter the key, the drive will mount just like any other drive that you connect to your system.

Microsoft has a server to help keep track of all the recovery keys and will only allow the people that need access to recover the key when needed. The software is called MBAM. The client computers have the mbam agent installed on the system.

When Bitlocker is installed and the mbam agent is on the client, it sends the recovery key to the mbam server, then the laptop is encrypted. When the system requires the recovery key, you go to the mbam website that you have setup and enter the challenge key, and it will give you the recovery key. After you use the recovery key to unlock the system in a recovery mode, the mbam client regenerates a new recovery key and then saves the key to the TPM chip and to the mbam server. This is done to tighten the security. When the key has been used it will not be able to be used again.

What can prompt you to need to use the recovery key? There are some items that if you do to the computer will require the recovery key. If the BIOS is upgraded, or memory added, it will prompt you to enter the recovery key. Also if any hardware is changed in the system. There is a way around this by suspending bitlocker before you do the hardware or bios upgrade. You will want to suspend bitlocker and not disable it. The difference is when you disable bitlocker it will fully decrypt the drive. Where if bitlocker is suspended it will resume after you reboot the system. There are two ways to suspend bitlocker, both require you to have admin right to the system. One way is to go into bitlocker options in the control panel and click suspend, this is nice if you are in front of the system, but not so much if you are pushing a change to the bios via the network. The second way is to use the command line. When you use the command line you can script it in as part of the deployment.

Bitlocker has a lots of pros to use this technology in your organizations. It helps protect your computer data so if your laptop is lost or stolen, the person that finds it cannot access any data. With more and more information going digital in today's world, you want to keep all your data as secure as possible. Bitlocker can be setup so the end

user doesn't really know that the system has been encrypted as well, until something goes wrong with the system. Also it does not have much over head on the performance of your computer after it has fully been encrypted. This is due to the entire drive being encrypted and not just files that are on the drive itself.

The main problem with using bitlocker is, it makes the systems harder to troubleshoot when there is a problem. For example: when you're the system can't find the right boot files, and it try to auto fix the problem. Windows recovery cannot access the hard drive until the recovery key is entered. If this happens when the user is out of the office, the user may not be able to work with the system until they are back in the office. Another problem is with the newer hard drives; data recovery is even harder to do when the drive is encrypted. There are times when you need to recover data, and it would have been easy if the drive was not encrypted, but with it encrypted, you have to either decrypt the drive or have a way to unlock the drive.

All in all, bitlocker is a great tool to use to keep your data in your systems secure. It comes as part of the windows operating systems so there is not more cost to the companies in order to use the technology.

Resources:

Microsoft Technet

https://technet.microsoft.com/en-us/library/cc732774(v=ws.11).aspx

Microsoft Technet BitLocker Group Policy Reference

https://technet.microsoft.com/en-us/library/ee706521(v=ws.10).aspx

Microsoft Technet How Strong Do You Want the BitLocker Protection

https://technet.microsoft.com/en-us/library/ee706531(v=ws.10).aspx