

Considerations for BitLocker™ in Microsoft® Windows® 7

by

Kevin Beaver, CISSP

Independent Information Security Consultant

Principle Logic, LLC



Principle Logic

Your Answer to Information Security®

November 2009

This paper outlines the factors you need to consider related to BitLocker when moving to Microsoft Windows 7 in the enterprise. Understanding the facts and thinking long term about how emerging technologies such as this will impact your business are key to running an efficient and productive IT shop. From operations to compliance to usability you'll learn about potential shortcomings and obstacles with BitLocker so you can make informed decisions on enterprise data encryption technologies moving forward.

Copyright © 2009 – All Rights Reserved.

Page 1 of 8

THE VALUE OF ENCRYPTION IN TODAY'S BUSINESSES

No matter what the regulators demand, the auditors recommend, or the naysayers rail against, the reality is that data encryption matters. When you think about the growing information system complexities, the risks associated with mobile computing, and the privacy/security regulations most businesses are faced with, the importance of protecting sensitive data with drive encryption technologies becomes clear. It's a critical piece of layered security and an excellent way to help ensure that sensitive data isn't exposed in the event of loss, theft, or other attack.

Ensuring reasonable data protection to meet the demands of doing business today requires well thought out security controls. Even with the prevalent regulatory requirements and the obvious benefits of data encryption there are still many organizations that haven't adopted encryption as a core component of information risk management. Many in management say things like "Anything of importance is on our servers and doesn't need to be encrypted". This couldn't be further from the truth. In any given organization there are literally hundreds if not thousands of islands of data scattered about on workstations, removable storage, smartphones and more. This is creating business risks that traditional controls or written policies could never reasonably protect against.

Businesses create, acquire, and end up storing more sensitive data than most people realize. Every record that's stored insecurely is a data breach waiting to happen.

Based on what I see in my security assessment work, it's extremely simple to compromise any given mobile workstation or storage device that does not have drive encryption enabled. Computers that were assumed to be secured but end up in the wrong hands can be compromised in matter of a few minutes using freely-available tools. The assumption that controls such as power-on passwords, operating system (OS) passwords, and user awareness are all that's needed to keep everything secure is not a sustainable strategy. In fact, it can be argued that many of the data breaches listed at Web sites such as Privacy Rights Clearinghouse's *Chronology of Data Breaches* (www.privacyrights.org/ar/ChronDataBreaches.htm) and Open Security Foundation's DataLossDB (<http://datalossdb.org>) could've been a moot point had drive encryption been used.

Based on what's happening in and around this space I can confidently say that drive encryption should be mandatory on mobile devices and other workstations deemed physically unsecure. Enter Microsoft's BitLocker.

OVERVIEW OF BITLOCKER IN WINDOWS 7

Until recently, the choices for enterprise-level security were third-party point solutions. You buy one product from one vendor to provide for specific controls in your environment. Microsoft has entered the picture over the past several years with various management and anti-malware products competing with third-party vendors. BitLocker drive encryption is no exception.

Microsoft first introduced BitLocker in Windows Vista back in 2007. Wrought with usability issues and other complaints in its initial release, BitLocker has since been revamped. The latest version of BitLocker ships with Windows 7 Enterprise and Ultimate editions as well as Windows Server 2008 R2. BitLocker supports encryption of the OS volume as well as other fixed and removable drives.

Since many enterprises opted to skip Windows Vista, odds are that Windows 7 is going to be the next big step at the desktop similar to the proliferation Windows XP has had to this point. This means you've got to start preparing for Windows 7 deployment and management at both strategic and tactical levels to ensure you implement it the right way. With BitLocker being bundled with the two different versions of the OS it's going to be tempting to use it – especially given the compliance pressures to encrypt data. After all, it's "free". It seems like a no-brainer. I've always been a big advocate of using the security controls you've already paid for from OS vendors as long as they reasonably address your business risks. But is BitLocker enough to meet your needs? Read on and decide for yourself.

OPERATIONAL CONCERNS

As a manager of IT and security operations there are several things you need to know before you go down the BitLocker path. These are issues that may fit into your current environment or only prove to be a bump in the road. However, they could also require a complete information systems overhaul or retooling of key IT processes that you may not be willing to take on.

Hardware Support

The first thing you have to consider with BitLocker are its minimum hardware requirements. In order to access all of BitLocker's features each system has to have a Trusted Platform Module (TPM) version 1.2 chip. If your business is relatively new or you've recently acquired new computers that support TPM this may be a moot point. However, if you have diverse systems scattered all over the country – or around the world – and these systems can't run Windows 7 then you may have a problem. If you don't have a good inventory of every workstation make and model this could create a lot of extra work.

Furthermore, in order to be able to read encryption keys stored on USB drives the system BIOS must be Trusted Computing Group-compliant. BIOS upgrades may be necessary in order to support this. If the hardware is old enough, it may not be upgradeable at all. Another issue is that the TPM passwords (referred to as PINs) must be entered using the keyboard's function keys (i.e. F1, F2, F3, and so on) because they're processed prior to localized keyboard support being available at boot time. Therefore, smart cards, tokens, and biometrics are not an option for boot-time authentication. There's also no support for non-U.S. keyboards.

Sure, you could say from this point forward every new system we acquire is going to be running a version of Windows 7 that supports BitLocker, have TPM support, have a U.S. keyboard and we'll integrate drive encryption over time. But is that good enough for your business right now?

Operating System Support

BitLocker is only available in the Enterprise and Ultimate editions of Windows 7. This may be an appropriate product marketing approach but what about all the other users with Windows 7 Professional, Home Premium, Home Basic, and Starter – versions that'll no doubt end up being used in your business? If you've already started acquiring new systems with Windows 7 Enterprise or Ultimate

BitLocker's latest drive encryption capabilities

- Simplified configuration and administration
- Separate system partition is standard and hidden from users
- Encryption capabilities outside of the OS volume
- BitLocker To Go™ for removable drives
- Additional management and recovery options

and plan to keep it that way this may not be a problem. However, it is an additional expense to take on and you may lock yourself into a specific Windows platform moving forward.

If your legacy hardware and operating systems are going to be around for a while, perhaps indefinitely, deploying BitLocker on new systems only may not be a viable risk mitigation strategy – at least in the eyes of the auditors and regulators. Even if you believe there's no sensitive data on these older systems odds are it does exist in some form.


The real gotcha is that consistent encryption protection across the board with BitLocker is not possible for legacy Windows XP and 2000 systems or even Linux and Mac OS X. This may be fine for the long haul but what about during the interim months or years when you've got other, unsupported, systems without protection?

Deployment

BitLocker is turned off by default. That's fine in and of itself. The problem is that it can turn into a security after-thought like what originally happened with WEP and WPA controls in 802.11-based wireless networks. It's out of sight and out of mind and not available unless and until you actually enable it. The best approach is to deploy drive encryption up front rather than making it a "nice to have" that you'll get to later. This requires some well thought out preparation on the part of IT staff along with the backing of management.

Initial preparation for BitLocker includes:

1. Verifying BIOS support for TPM and USB access during boot on every computer
2. Verifying the TPM version on every computer (version 1.2 or later is required)
3. Enabling the TPM since most computers have it disabled by default
4. Configuring Active Directory schema extensions for backing up BitLocker recovery data
5. Writing scripts for pushing out BitLocker

 *Certain deployment tasks such as TPM and USB initialization and setup require you to be at the computer. Doing this for a few dozen systems may not be a big deal as the costs for deployment would be minimal. However, reaching out to hundreds if not thousands of systems is, at best case, daunting if not completely impractical.*

Once you're ready for actual BitLocker deployment you'll need to do the following:

1. Configure recovery options for the OS volume (i.e. TPM only, TPM + PIN, TPM + PIN + USB key, or USB key only)
2. Configure recovery options for removable drives (i.e. auto unlock, password, or smart card only)
3. Configure BitLocker To Go™ for removable drives
4. Share PIN and password information with each user
5. Tweak Group Policy settings for additional security such as smart card and recovery options and additional settings for OS, fixed, and removable drives
(<http://technet.microsoft.com/en-us/library/dd875532%28WS.10%29.aspx>)

These steps may be a bit much for medium and larger-sized organizations to take on. Even Microsoft had its own BitLocker deployment challenges during its rollout on Vista machines (<http://technet.microsoft.com/en-us/library/dd126731.aspx>). Some of these problems still affect Windows 7 environments.

Optionally, you can write step-by-step instructions that walk each user through setting up BitLocker on their own systems. I prefer to stay away from getting users involved in security decisions. Sure, users are a great last line of defense but depending on them to do the right thing all the time – especially configuring technical controls and ensuring they remain enabled – is an incident waiting to happen. Depending too much on users also creates some serious responsibility and accountability issues. Furthermore, not knowing the status or being able to easily confirm the configuration settings users have chosen will likely create more work and ultimately sets everyone up for failure. In my opinion, a well-designed BitLocker deployment in all but the smallest of organizations could very well be downright painful.

Key management

It's hard enough for network operations managers and IT administrators to keep up with encryption key management across their networks. Adding another unique layer on top with BitLocker and having to adjust or augment existing key management processes can easily make things worse. The thing with managing keys is that if the processes are poorly implemented and not managed well, it can very well defeat the purpose of encryption.

Additional points to consider regarding key management are:

- Storing keys on USB devices creates an additional cost if you'll be using a separate USB drive for each computer.



USB drives can not only be used to store the startup key but also the recovery key. Such drives are easily misplaced and lost which can lead to increased usage of IT resources and a decrease in employee productivity. Odds are this *will* happen negating any encryption benefits.

- Active Directory integration is recommended for enterprise-level key management which may be too much of a burden for small businesses or branch offices that have limited resources.
- Encryption keys cannot be revoked.
- In environments where Active Directory is not used for centralized BitLocker management, the original media must be available to access recovery keys.
- Recovery keys can be stored in hard copy printout but this may not be a viable option.

Finally, you can use BitLocker in a system without TPM support if the BIOS can read USB drives at bootup (in order to access the startup key). However, you won't have access to the system integrity verification which can determine if a system has been changed or otherwise manipulated. Is it worth the risk?

USABILITY

In addition to the operational issues you've got this other big thing that tends to cause problems: your users. Usability and user management are both things you need to consider before going down the BitLocker path. A big underlying contributor to user management dilemmas is the fact that today's workforce is both unique and demanding. Compared to just a few years back, users are now working

with multiple computing devices, they're more tech-savvy, and they tend to want more control. Combine this with the fact that many users are often on the go, exposing sensitive data in various areas along the way, and you've got yourself a big responsibility to deal with. BitLocker in Windows 7 has features that cater to a mobile workforce. From user-controlled encryption settings to BitLocker To Go, there's nothing an average user can't do to help protect their systems and your business' sensitive data. But is this what you want?

When it comes to managing users and BitLocker there are 10 things that you need to take into account – things that may prove to be deal breakers:

1. Users have to remember their TPM PIN so true single sign-on is not an option.
2. BitLocker is either enabled or disabled – on or off – regardless of the user or computer function which can create confusion about authorized usage.
3. Multiple users of a single system will have to share the same PIN since multiple PINs are not supported by the TPM. This can lead to accountability problems proving who did what. It also leads to user provisioning and PIN revocation problems. For example, in a situation where you need to block a specific user's access by changing the PIN (i.e. after a firing), there's no realistic way for this to not affect other users of the system.
4. If users are given administrative rights in Windows 7 they can do what they want when they want with the encryption. This may not be as big of a deal with User Access Control but many applications still require direct administrative rights. Furthermore, network administrators don't want to constantly have management and users on their backs so users may very well be given administrative rights just to keep them quiet.
5. Any user with administrative privileges can manage the Windows 7 Local Security Policy via *gpedit.msc* and "tweak" BitLocker to his or her heart's content.
6. Within the local policy (*available via Administrative Tools/Local Security Policy/Local Computer Policy /Computer Configuration/Administrative Templates/Windows Components/BitLocker Drive Encryption*) the user has access to 24 different policy settings in Windows 7. That's enough to make a network administrator balk and a user's head spin. Do you want them to have that much control?
7. If a TPM PIN or USB key is not used, a weak password in Windows 7 is all that's keeping a would-be attacker out of the system. Based on what I see in my work, even with local or group policy-based password complexity requirements, weak passwords can and often do exist in Windows environments.
8. Files are copied in an unencrypted fashion to other drives. Once data leaves the "protected" area there's no way to prove it's still secure. No matter how many times you remind users where to store sensitive data, they're still going to store it in other places which could be a unprotected fixed drive – or removable drive – and still end up exposing the data.
9. When TPM PINs and encryption keys get lost, there's no self-service option for users thus creating even more work for IT staff. Keys cannot be revoked either.
10. Recovery passwords are stored in clear text which can expose them to abuse. It's like the stereotypical "sticky note" syndrome where users put their passwords in plain view thus negating any benefits. They can also be stored on a removable drive – big problem!

When it comes to users, balancing security with convenience and usability is quite a task. Finding a happy medium is key. Just don't take it too far and lose control of your systems – for that's what good security is made of.


POTENTIAL COMPLIANCE GAPS AND SECURITY CONCERNS

With compliance being the driving force behind many security initiatives these days it's certainly something we have to pay close attention to. The privacy and security regulations are evolving and tend to have more teeth. For instance, the recent HITECH Act which tightens down on the controls and enforcement for HIPAA covered entities and business associates in the healthcare industry. There are also the state breach notification laws that mandate the protection of sensitive data and subsequent reporting of data breaches. Currently there are only five states that do not have something in place for this in the U.S.

Looking beyond the well-known privacy and security regulations are another of set of compliance issues you likely have internally in your business. That is customer and business partner requirements as well as your own internal policies that need to be complied with. Understanding what's necessary requires checking internal security standards and policies and working with legal counsel to review business partner and customer contracts to ensure your protection mechanisms are appropriate.

When it comes to balancing compliance with BitLocker in Windows 7, there are several things you need to think about:

1. The different types of protection mechanisms BitLocker offers (i.e. TPM, PIN, and USB drive) may or may not meet your specific compliance needs.
2. There's limited audit logging and reporting with BitLocker so it may be difficult for to prove encryption status. It may also prove difficult to establish if and when drives were actually encrypted and contribute to general key management oversights. Logging and reporting may seem boring and trivial now but in the event of an audit, or worse, a breach or unauthorized disclosure it's going to be difficult to prove what was done.
3. There's no support for optical media with BitLocker To Go which may be an issue if protecting sensitive data on CDs and DVDs falls within the scope of your business's compliance responsibilities. There's no Mac support with BitLocker To Go either. Furthermore sharing BitLocker To Go-protected media may prove problematic when sharing the data with users who don't have Windows 7 Ultimate or Enterprise. They'll only be able to read the data since no writes are allowed in this situation. This could lead to misplaced and unprotected data on these unsupported systems and end up negating any benefits of mobile encryption.
4. With the limited support of BitLocker on older versions of Windows, you're going to have a mix of encrypted and unencrypted systems. This lack of consistent security may create compliance gaps and risks that your business cannot afford to take on.
5. BitLocker may be used to encrypt the system volume but it doesn't automatically encrypt everything – including removable storage devices – which could create gaps in coverage and a false sense of security.
6. Lack of integration with additional security controls such as tokens, biometrics, and PIV cards for Federal HSPD-12 compliance may go against policy and create compliance gaps.
7. Using Active Directory to store BitLocker recovery keys makes them accessible to domain administrators and others who've been assigned the necessary privileges. This creates a separation of duties issue and accountability concerns when a BitLocker-protected system is compromised. Considering keys are stored in an unencrypted fashion, it could also be argued that someone gaining unauthorized access to a Windows server running Active Directory – such as exploiting a missing patch and gaining remote access – could retrieve these keys without ever having to login to the system.

 The argument has been – and continues to be – made that relying on the OS vendor for all security controls may not provide an adequate level of “layered” security. This lack of vendor separation of duties can be viewed as the fox guarding the henhouse.

Compliance is about knowing what the regulations and contracts say, understanding what’s truly at risk, implementing reasonable technical controls, and then enforcing policies consistently across the organization. In many situations, these may be difficult to do with BitLocker.

SUMMARY

The most important thing to take away from this is to know the facts. Understand how BitLocker in Windows 7 is going to impact your organization’s overall information risks. I encourage people to use built-in security controls you’ve already paid for but *only if* it makes good business sense. Throughout my IT career I’ve found that the adage *you get what you pay for* rings true for information security time and again. “Free” doesn’t always mean it’s a good fit.

Managing IT and information security effectively means using products and tools that work for you rather than against you. With the growing information systems complexities we face, increased mobility, and users who don’t want security to get in their way, you have to choose your security controls wisely. Increasing your IT headaches is something you obviously want to avoid but it’s always an option if you don’t think things through.

With limited adoption of Windows Vista in the enterprise, BitLocker has yet to prove itself in the marketplace. Windows 7 is new and will likely become the next big OS we’ll be using but, still, the scrutiny of BitLocker has just begun. You may be able to argue that BitLocker is “good enough”. Maybe it is, maybe it isn’t. When will you know? When you get the results of a security assessment? Maybe when an auditor tells you? Or perhaps when a forensics expert delivers his investigation report? The reality is “good enough” security for the short term can create long-term issues that can cost you dearly if you’re not careful.

BitLocker does have a place in today’s market. Is it the right choice for your enterprise? That’s for you to decide.

About the Author

Kevin Beaver, CISSP, is an [independent information security consultant, expert witness, author, and keynote speaker](#) with Atlanta, GA-based Principle Logic, LLC. He has over two decades of experience in IT and specializes in performing information security assessments revolving around compliance and minimizing business risks. Kevin has authored/co-authored seven books on information security including *Hacking For Dummies* and *Laptop Encryption For Dummies* (Wiley) as well as *The Practical Guide to HIPAA Privacy and Security Compliance* (Auerbach). He is also the creator and producer of the *Security On Wheels* audio books providing security learning for IT professionals on the go ([securityonwheels.com](#)). Kevin can be reached at his Web site [www.principlelogic.com](#).

All trademarks are the property of their respective owners.

Copyright © 2009 – All Rights Reserved.