



Windows[®] 7

EXECUTIVE OVERVIEW

BitLocker[™] Drive Encryption

February 9, 2009

Abstract

This paper provides an overview of BitLocker[™] Drive Encryption in Windows[®] 7 and introduces BitLocker To Go[™]. Introduced in Windows Vista[®], BitLocker Drive Encryption helps protect data by preventing unauthorized users from breaking Windows file and system protection on lost, stolen or inappropriately decommissioned computers. New for Microsoft[®] Windows 7, BitLocker To Go is a natural extension of BitLocker Drive Encryption that addresses theft or unwanted disclosure of data made available through physical loss of removable storage devices (e.g., USB Flash Drives, USB Portable Hard Drives).

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, BitLocker, BitLocker To Go, Windows, the Windows logo and Windows Vista, are trademarks of the Microsoft group of companies.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

Introduction

A recent consumer security and privacy survey reveals that 79 percent of consumers cite loss of trust and confidence, damage to reputation, and reduced customer satisfaction as consequences of major security and privacy breaches suffered by the business that they deal with¹. When coupled with the over 12,000 laptops that are estimated to be lost or stolen in U.S. airports each and every week², it is plain to see why protecting customer data is a top priority for business executives today. Organizations that have deployed Windows Vista with BitLocker Drive Encryption know that company data, including customer data, is well protected on these devices.

However, data leakage is not just a lost laptop issue. The ubiquity of USB Flash Drives provides another potent avenue for data to fall into the wrong hands. Today, more than twice as many USB Flash Drives enter the marketplace than PC's. In 2011, a leading analyst forecasts that the most popular USB flash drive will hold 32 GB of data, for less around 25 US Dollars³. The scary part for an organization: unlike losing a laptop, a user never seems to report, or sometimes even notice, the loss of a USB flash drive!

The importance of protecting sensitive information on removable storage devices is driven home with the July 2008 revelation that the *UK Ministry of Defence* admitted to parliament that it has lost, or had stolen, eighty seven USB sticks in recent years which stored data that was marked as classified⁴.

Windows Vista introduced granular USB port controls that can block the utilization of USB removable storage devices while still allowing other USB devices such as keyboards, mice, and printers. Unfortunately, the ability to block removable storage devices does not provide the flexibility and control necessary to adequately protect most organizations. There are valid business requirements that necessitate the need to store data on removable USB devices: from sharing large files with a trusted partner to taking work home.

Windows 7 addresses the continued threat of data leakage with manageability and deployment updates to BitLocker Drive Encryption and the introduction of BitLocker To Go: an exciting new feature that helps protect data stored on portable media (e.g., USB Flash Drives, USB Portable Hard Drives) such that only authorized users can read the data, even if the media is lost, stolen, or misused.

Windows 7 BitLocker

BitLocker Drive Encryption (BitLocker for short) helps prevent a thief who boots another operating system or runs a software hacking tool from breaking Windows 7 file and system protections or performing offline viewing of the files stored on the protected drive. Windows 7 BitLocker shares many of the same core benefits of Windows Vista BitLocker:

¹ Computer Associates, "CA 2008 Security and Privacy Survey", July 16, 2008

² Ponemon Institute, "Airport Insecurity: The Case of Lost & Missing Laptops", July 29, 2008

³ Gartner, "Forecast: USB Flash Drives, Worldwide, 2001-2011", September 24, 2007

⁴ The Register, "MoD: We lost 87 classified USB sticks since 2003", July 18, 2008

- Helps prevent unauthorized users from breaking Windows file and system protection on lost, stolen or inappropriately decommissioned computers. This includes the operating system volume and fixed data volumes.
- Integrity checking of early boot components to help ensure that the system has not been tampered with and that the encrypted drive is located in the original computer.
- Protection against cold boot attacks by requiring the user to supply a startup PIN or USB flash drive that contains keying material before the computer will boot or resume from hibernation.
- Active Directory® Domain Services integration to remotely escrow recovery keys to aid in field recovery in instances where a user forgets their PIN or loses their keying material stored on a USB flash drive.
- Simple, efficient hardware recovery processes that include moving a protected hard drive containing the operating system volume to another computer or replacing the systems motherboard.

The core functionality in Windows 7 BitLocker has been enhanced to provide a better experience for IT Pros and for end users. From simple enhancements like the ability to right-click a drive to enable BitLocker protection to the automatic creation of the required hidden boot partition. For customers who did not deploy Windows Vista systems with the BitLocker required two partition disk configuration, repartitioning the drive to enable BitLocker protection for the OS was more cumbersome than it needed to be. As a result, Windows 7 automatically creates the necessary disk partitions during installation to greatly simplify BitLocker deployments.

Windows 7 BitLocker adds Data Recovery Agent (DRA) support for all protected volumes. A big ask from customers, DRA support allows IT to dictate that all BitLocker protected volumes (OS, fixed, and the new portable volumes) are encrypted with an appropriate DRA. The DRA is a new key protector that is written to each data volume so that authorized IT administrators will always have access to BitLocker protected volumes.

BitLocker To Go provides enhanced data protection against data theft and exposure by extending BitLocker support to removable storage devices. By extending support for BitLocker to FAT data volumes, a broader range of disk formats and devices can be supported, including USB Flash Drives and portable disk drives. This will allow users to deploy BitLocker for a broader range of data protection needs.

BitLocker To Go gives administrators control over how removable storage devices can be utilized within their environment and the strength of protection that they require. Administrators can require data protection for any removable storage device that users want to write data upon; while still allowing unprotected storage devices to be utilized in a read-only mode. Policies are also available to require appropriate passwords, smart card, or domain user credentials to utilize a protected removable storage device.

BitLocker To Go can be utilized on its own, without requiring that the system partition be protected with the traditional BitLocker feature. Although you will need a premium Windows 7 SKU to enable

protection of removable storage devices with BitLocker, any SKU can be utilized to unlock and use a protected device. Finally, BitLocker To Go provides read-only support for removable devices on older versions of Windows allowing you to more securely share files with users who are still running Windows Vista and Windows XP.

Summary

Forty two percent of respondents in the Computer Security Institute's 2008 Computer Crime and Security Survey reported having a laptop or mobile device stolen in the previous year⁵. The critical consequences of losing sensitive corporate data include decreased brand reputation, lawsuits, regulatory penalties, and possible criminal prosecution. Now is the time to encrypt your mobile data, whether stored on laptops or removable drives, for the risks of unencrypted data are too great to be ignored.

Windows 7 addresses the continued threat of data leakage with manageability and deployment updates to BitLocker Drive Encryption and the introduction of BitLocker To Go: data protection for removable storage devices. So whether traveling with your laptop, sharing large files with a trusted partner, or taking work home, BitLocker protected devices help ensure that only authorized users can read the data, even if the media is lost, stolen, or misused. Best of all, BitLocker protection is easy to deploy and intuitive for the end user, all the while leading to improved compliance and data security.

⁵ Computer Security Institute, "CSI Survey 2008", 2008