Business Brief

SecureDoc™

BitLocker - A Strong First Step in Data Security

> If BitLocker is not adequate, then SecureDoc should be seriously considered
>
> IT Personal Technology Supervisor, Energy & Utilities Sector, **Gartner Peer Insights (2016)**

90%

Percentage of data breaches that could have been prevented using available technologies, or adherence to basic processes and procedures.

The Online Trust Alliance (OTA) 2015 Data Protection Best Practices and Risk Assessment Guide

43%

Percentage of respondents who say DEVICE ENCRYPTION is currently a part of their mobile device management policy

Crowd Research Partners BYOD and Mobile Security Spotlight Report. (2016)

Microsoft BitLocker

Consider the shear damage a data breach can cause – stolen proprietary documents and data, bad publicity, lost business, and potentially massive fines that ultimately cripple your business. 90% of these breaches could easily have been avoided with some very simple precautions. As the simplest way to mitigate risks, many companies are opting to deploy the full disk encryption (FDE) capabilities built into their operating systems as an enterprise standard. For enterprises dominated by the Windows Operating System, Microsoft's BitLocker has been naturally adopted to encrypt user devices, including PCs and laptops. BitLocker is supplied with select editions of Microsoft Windows, and offers excellent performance and compatibility with the widest range of hardware, plus a good integrated user experience.

Microsoft BitLocker Administration and Monitoring (MBAM)

In many enterprise deployment scenarios, centralized management of BitLocker is provided by Microsoft BitLocker Administration and Monitoring (MBAM). MBAM allows administrators to quickly determine the compliance state of individual computers. It also enables administrators to automate the process of encrypting volumes on client computers, enforces the BitLocker encryption policy options, monitors the compliance of client computers with those policies, and reports on the encryption status of enterprise and individuals' computers – so long as they are on a Windows Operating System, and the company has proper mobile device management policies in place.

Adopting Bring Your Own Device policies…and their challenges

Bring-Your-Own-Device (BYOD) policies add a further layer of complexity to data security. Smartphones and tablets running Windows, iOS and Android are increasingly used by a mobile workforce to connect to your network - opening and sharing your files and folders – exposing your data to risk. These devices are also more easily lost or stolen than desktop computers, heightening the risks. This proliferation of mobile devices has made it necessary for many organizations to find ways to integrate and secure the endpoints, without layering in complexities.

Harnessing BitLocker's Full Potential

SecureDoc™ WinMagic engineers speak with IT and security professionals every day. Many are evaluating BitLocker, or preparing for its deployment. During these conversations, we are often provided feedback on a number of common areas where the encryption solution could benefit from additional functionality. By adding a third-party encryption solution as a management tool, organizations can:

- Benefit from a central management solution, allowing for better control over key storage, escrow, and policy, avoiding replacing current methods which are both time-consuming and problematic
- Extend multi-factor user-based authentication, providing the ability to add keys for personal or confidential files.
- Provide and heterogeneously manage encryption on devices, workstations, and servers on non-Windows platforms, such as Mac or Linux. And, can better manage challenges introduced by BYOD and mobile workforces
- Provide a simpler user experience by taking onus off end-user for compliance, and by providing easier password recovery processes.

BitLocker Strengths

- Comes with most enterprise Windows Operating systems
- Provides seamless end-point encryption
- Can encrypt the entire drive
- Permits token authentication
- Supports a wide range of hardware
- Offers compliance monitoring
- Enforces encryption policy, and provides status reports
- Uses Trusted Platform Module (TPM) for its secure cryptoprocessor

Why Should You Use WinMagic's SecureDoc on Top for BitLocker?

- **Increased User Friendliness** Disk encryption can be a disruptive and confusing process for end users. SDOT allows for user-based single sign-on, and the encryption is transparent to the end-user
- **Simplified Deployment** Allows for secure provisioning, transport, and deployment of machines using temporary key files
- **Next Level Functionality** Offers Centralized Intelligent Key Management supporting Windows, Linux and Mac OS, BYOD and virtualized environments
- **Enhanced Security** Prevents accidentally (or intentionally) disabling BitLocker
- **Stronger Recovery** Provides Multiple password reset methods to get end users up and running quicker
- **Better Auditing** Provides the audit records and reports you need to establish compliance with data protection regulations such as HIPAA, PCI DSS, and SOX

Better together: **BitLocker + SecureDoc**

SecureDoc on Top(SDOT) for BitLocker delivers the best of both worlds by combining the seamless encryption of BitLocker with WinMagic's sophisticated and comprehensive enterprise key management. SDOT for BitLocker enables user-based policies, which allow the administrator to better-manage who gains access to data, what level of access is granted, and when or how they access it.

SecureDoc on Top (SDOT) for BitLocker enhances BitLocker's native encryption capabilities by providing IT administrators with the tools to better manage it. SecureDoc organizes all security-related management such as policy and password rules under one centralized server console – the SecureDoc Enterprise Server.

Under this single umbrella, enterprises can manage BitLocker, protecting data residing in laptops, desktops, mobile devices, and servers operating on nearly any platform. It also easily supports removable media and SEDs. This ultimately allows for better compliance, more expansive functionality, and enhanced remote management capability.

The Power of Unified Key Management

WinMagic's SecureDoc Enterprise Server (SES) provides organizations total control over their data security environment, ensuring maximum security and transparency in the regular work flow.

SecureDoc, WinMagic's core offering, secures data at rest by managing how it is encrypted, regardless of where it resides, or on what operating system. SecureDoc provides enterprises a comprehensive data security solution that supports compliance with security and privacy regulations, without increasing IT costs significantly, or compromising end user productivity.

Designed with the heterogeneous IT environment in mind, SecureDoc organizes all security-related management under one centralized enterprise server, including policies, password rules, and the manageability of encryption across PC, Mac and Linux platforms.

SecureDoc offers organizations two different ways to manage BitLocker:

SDOT for BitLocker

Using SecureDoc on Top for BitLocker, enterprises can manage BitLocker within a single security umbrella, protecting data residing in laptops, desktops, mobile devices, servers, removable media and SEDs.

Administrators can leverage existing network login credentials (instead of only a PIN) in addition to multi-factor authentication with smart cards or other tokens. This guarantees a lock down of system access and a high-level security of devices – critical for many large organizations or institutions.

SDOT for BitLocker with PBConnex

SecureDoc further enhances BitLocker by being the only data encryption and management solution that supports pre-boot network authentication (PBNA) through its PBConnex technology. PB Connex uses network-based resources to authenticate users, enforce access controls, and manage end point devices before the operating system loads.

PBNA provides much more than end point security. Its policy control engine allows businesses to manage groups and control how, what, when and where users access devices and data.