Product Brief

SecureDoc by WinMagic

SecureDoc on Top for BitLocker

What you never believed BitLocker could do

- Simplified Deployment and Key Management
- Frictionless Authentication
- Cost and Time-Effective Recovery Processes

WINMAGIC

The Need for Native Encryption Management

For enterprises dominated by the Windows Operating System, Microsoft's BitLocker has been naturally adopted to encrypt user devices, including PCs and laptops. Integration of BitLocker into the operating system is a good first step in improving data security. However, to expose the full capability of BitLocker, organizations require a comprehensive key management tool that enables user-based policies, allowing the administrator to better-manage who gains access to data, what level of access is granted, and when or how they access it.

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 the operating system or where the data resides. SecureDoc provides enterprises a comprehensive data security solution that supports compliance with security and privacy regulations. SecureDoc simplifies the IT administrator role, while maintaining an easy-to-use end user experience.

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

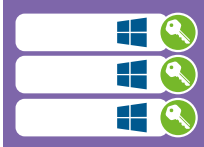
Download BitLocker toolkit

> More than 90 percent of the data breaches 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

BetterTogether: **BitLocker + SecureDoc**

SecureDoc offers organizations two different features for managing BitLocker:

SecureDoc on Top for BitLocker



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

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

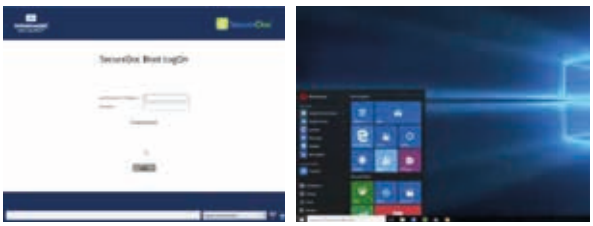
SecureDoc on Top for BitLocker with PBConnex

SecureDoc further enhances BitLocker by being the only data encryption and management solution to support 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.

Increased User-Friendliness

Leveraging WinMagic's Intelligent Key Management, SecureDoc on Top (SDOT) for BitLocker simplifies the authentication and compliance process for IT Administrators and end-users.



SDOT for BitLocker allows for true single-sign on. From the SecureDoc pre-boot login users can be taken directly to their desktop once connected, thanks to PBConnex, WinMagic's Pre-Boot Network Authentication.

Authentication credentials are based on the user, so there is no need to share or to find a matching PIN, allowing for many users to share one device.

Enhanced Security

SecureDoc on Top for BitLocker permits more granular control of user and administrator rights – further protecting against internal threats or errors

SecureDoc on Top for BitLocker prevents admins from accidentally or intentionally disabling BitLocker. In the event of improper disablement, SDOT re-encrypts automatically.

SDOT for BitLocker supplements the pre-boot environment, **reinforcing the TPM startup process via PBConnex**. This enhances security through authentication at pre-boot, rather than at the Windows login, improving policy protection and automatic system update capability.

Simplified Deployment

SecureDoc on Top allows admins the ability to deploy end point devices in a compliant and secure provisioning state, without relying on an unknown end-user.

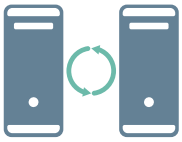
End devices may be deployed containing a temporary key file – not specific to the user-ensuring security of the device. Only basic set-up operations are enabled on the device until the actual end-user takes control.

Using multi-factor authentication, the security key file for the user is transferred when the end-user takes control using their AD credentials. This also permits multiple users on a single device. Access to files and folders can be controlled at the user level.

Advanced Recovery

Your data security solution should be freeing up productivity, not depleting it. SecureDoc on Top for BitLocker simplifies password resets, saving users valuable time, and you money.

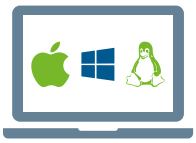
In the case of an OS crash, SDOT for BitLocker requires only a username and password, reducing the need for the help desk support required with Microsoft's BitLocker Administration and Monitoring (MBAM) tool.



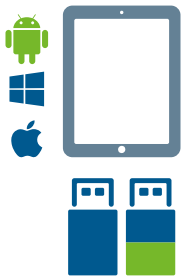
With SDOT for BitLocker, there are multiple methods of password reset, including self-help, challenge-response and PBConnex password reset through AD sync.

Enhanced Functionality

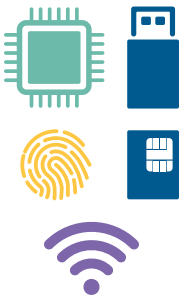
SecureDoc is platform agnostic, not limited to Windows-based devices, and protects sensitive data residing in laptops, desktops, servers, removable media and SEDs



Provides support for Microsoft's BitLocker (Win 10, Win 8, Win 7 and Vista), Mac OS X and FileVault 2, and Linux.



Policy-driven management for removable media (RME & RMCE) and virtualized and cloud environments.



Supports integration with multi-factor authentication using TPM, tokens, smartcards and biometrics – plus Pre-Boot Network Authentication.

SecureDoc by WinMagic

Enhancing Microsoft **BitLocker** Administration Monitoring (MBAM) with **SecureDoc**

	OPTIMAL	STRONGER	STRONG	GOOD
	SES Opal Management	SecureDoc Enterprise Server BitLocker Management	MBAM	
		With SecureDoc Pre-boot	With BitLocker Pre-boot	BitLocker
Pre-Boot Authentication				
Unique user authentication at pre-boot	■	■	✖	✖
Pre-boot network user authentication (AD)	■	■	✖	✖
Multifactor authentication (tokens, smartcards, biometrics)	■	■	✖	✖
Secure network auto unlock	■	■	✖	■
Offline self-help password recovery option	■	■	✖	✖
Single use challenge and response password recovery	■	■	✖	✖
Customizable pre-boot Screen	■	■	✖	✖
Multilingual Support	■	■	✖	✖
Windows Secuity Features				
Single Sign on	■	■	✖	✖
Password Synchronization	■	■	■	✖
Policy driven removable media encryption with key management	■	■	■	✖
Policy driven File and Folder encryption with key management	■	■	■	✖
Single use challenge/ response password recovery for removable media encryption	■	■	■	✖
Port control	■	■	■	✖
Auditing and Reporting				
Client pre-boot login auditing	■	■	✖	✖
BitLocker Recovery key access auditing	■	■	■	✖
Installation and Deployment				
Single location to configure BitLocker policies (No need to configure GPO)	■	■	■	✖
Automatic TPM Provisioning	■	■	■	✖
Ability to secure and manage OS that do not support BitLocker	■	■	■	✖
Supports Self Encrypting drives (TCG OPAL drives)	■	■	■	✖
Supports Self Encrypting Drives (E-Drive)	■	■	■	■
Supports importing of standalone BitLocker enabled machines into centralized management	■	■	■	✖
Silent deployment with no user interaction	■	■	■	✖
Security and Performance				
Protected against Cool RAM attack	■	✖	✖	✖
Protected against brute force attacks	■	✖	✖	✖
Permanent and secure erasure of data	■	✖	✖	✖
No performance degradation	■	✖	✖	✖
Supports any operating system	■	✖	✖	✖
Near Zero time required for encryption when staging/preparing users' machines	■	✖	✖	✖

info@winmagic.com | www.winmagic.com

WINMAGIC®

US & Canada +1 888 879 5879 | United Kingdom +44 0148 334 3020 | Germany +49 69 175 370 530 | Japan +03 5403 6950 | India +91 124 4696800 | APAC-Singapore +65 9634 5197