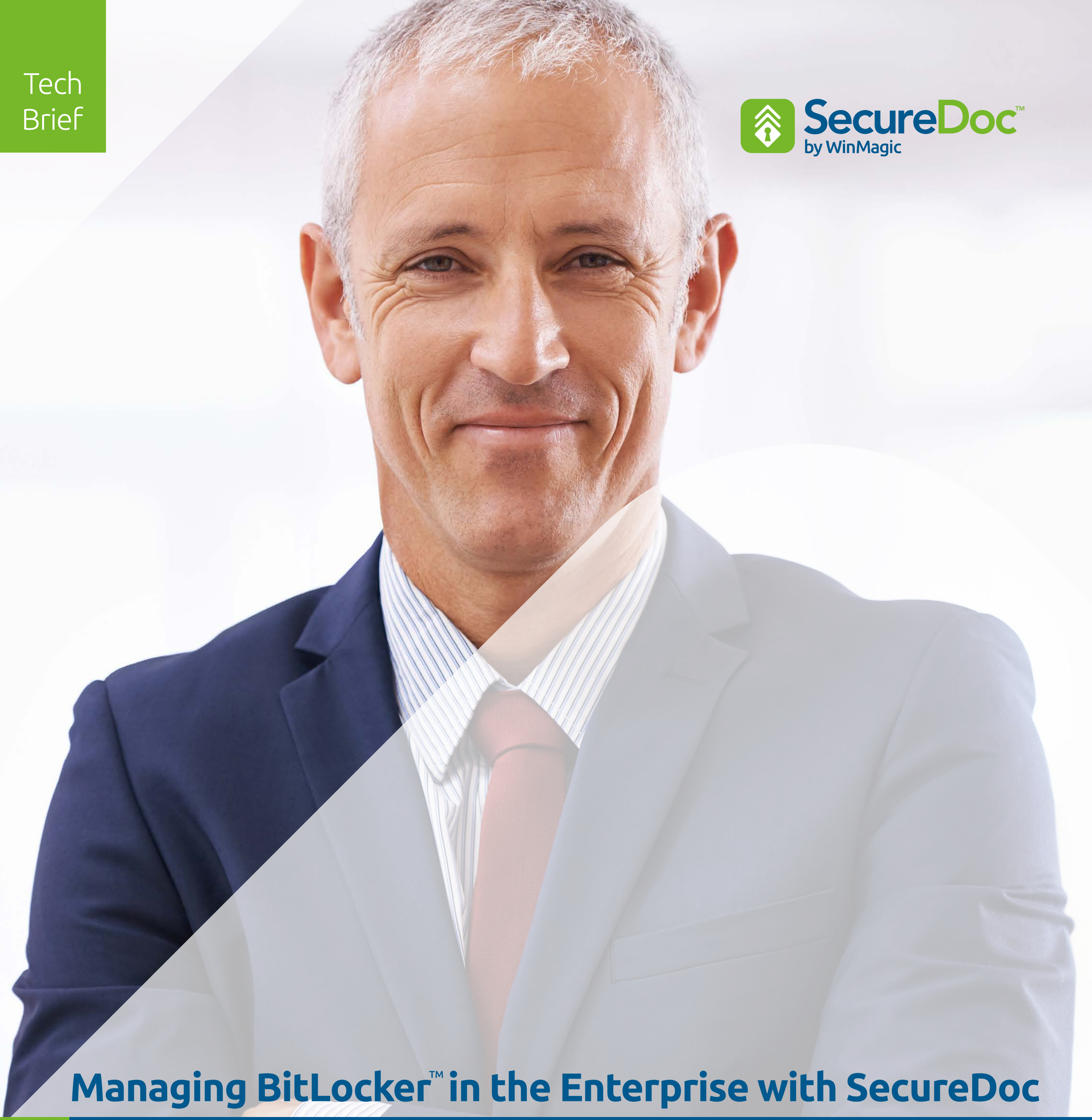
Tech
Brief



Managing BitLocker™ in the Enterprise with SecureDoc

What you never believed BitLocker could do

- Simplified Management and Authentication
- Demonstrated Compliance, Audit and Reporting
- Increased Security and User Productivity

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

Microsoft BitLocker

Microsoft offers built-in encryption software designed to protect data on a system drive from loss, theft or unauthorized access. Microsoft BitLocker is a solid starting point for your data protection strategy, offering secure, OS-embedded encryption. However, the question with BitLocker is often less about security and more about manageability, which in the end matters most to the total cost of ownership in today's multi-OS, multi-platform enterprise.

Microsoft BitLocker is available with:

Windows 7	Ultimate, Enterprise
Windows 8/8.1	Pro, Enterprise
Windows 10	Pro, Enterprise, Education

Windows Server 2008 and later

One Platform, Two Flexible Solutions

SecureDoc BitLocker Management
Known as SDBM

A traditional management solution for BitLocker, leveraging BitLocker's pre-boot protection and security that is centrally managed by SecureDoc Enterprise Server for essential key management, access controls, reporting and recovery.

SecureDoc On Top for BitLocker
Known as SDOT

An enhanced management solution for BitLocker, leveraging SecureDoc's advanced pre-boot protection and PBConnex technology that enables more flexible, scalable deployment and management. Advanced features like PBConnex Network-brokered Authentication, Wireless Auto Boot, and Password Resets reduce downtime and increase user productivity.

A Solid Starting Point for Data Protection

Enterprises dominated by Windows OS have quickly adopted BitLocker to protect Windows Desktops, Laptops, Surface Tablets, and Servers. After all, why shouldn't they? BitLocker Drive Encryption and Device Encryption are OS-embedded, and they do one thing very well – encrypt system drives.

BitLocker is a simple and effective way to protect your data, but management of encryption keys becomes complex when you add the scale and diversity of IT infrastructure in today's enterprises.

You need the flexibility to deploy encryption across your business without creating security gaps or roadblocks to user productivity. To support the scale and diversity of your enterprise, device encryption is only the beginning.

The Power of Unified Data Protection and Compliance

SecureDoc Enterprise Server (SES) offers unified, intelligent key management to centrally protect data where it resides, control who can access that data, and how it is protected – with the flexibility to leverage SecureDoc Drive Encryption, BitLocker, FileVault 2 or hardware-level encryption with OPAL SEDs on your workstations.

Beyond drive encryption for your devices, SecureDoc CloudVM protects your public, private or hybrid cloud deployment with persistent, platform-agnostic encryption. For an additional layer of protection, SecureDoc File Encryption and SecureDoc CloudSync deliver file-level encryption across local folders, network shares and Cloud file shares.

All the while, SecureDoc Enterprise Server delivers one unified platform to enforce consistent protection, policies and compliance across all of these solutions in your unique mix of physical, virtual and cloud infrastructure. That's the power of unified, intelligent key management.

Managing BitLocker with SecureDoc Enterprise Server

The widespread availability of Microsoft BitLocker has resulted in a growing number of BitLocker management tools available in the market – including WinMagic's SecureDoc BitLocker Management (SDBM) solution. SDBM provides essentials for BitLocker deployment, management and compliance, but your particular user habits, business needs and risks sometimes demand a greater level of security and manageability.

SecureDoc On Top for BitLocker (SDOT) – our industry-first solution for next-level BitLocker management – integrates BitLocker's built-in encryption with SecureDoc pre-boot technology, enabling more advanced features designed to eliminate roadblocks to user productivity and enhance security across your Windows clients.

With SecureDoc, you have the flexibility to choose the solution that best suits your enterprise, whether you choose the simplicity of SDBM for basic management and compliance reporting, or the advanced management and client features with SDOT for BitLocker. Enterprises can also upgrade at any time without interruption to operations.

It's the Best of Both Worlds!

SecureDoc™
by WinMagic

Best of Both Worlds: SecureDoc On Top for BitLocker

With Unified Key Management and Policy Control via SES

Why choose between security and manageability? Now, you don't have to. With SecureDoc On Top for BitLocker (SDOT), you can leverage BitLocker's powerful OS-integrated encryption with state-of-the-art SecureDoc pre-boot protection and intelligent key management. It's secure, manageable, and doesn't stand in the way of user productivity. With SecureDoc and BitLocker together – you can have the best of both worlds.

Improved User Experience

Simple User-Based Authentication

Leveraging SecureDoc pre-boot technology, SDOT simplifies authentication for the end user, reducing downtime and increasing productivity. No need to sign in twice with BitLocker device-based PINs or reduce devices to baseline protection with TPM-only. SDOT and Active Directory Sync (ADSync) enable users to login with the same set of credentials across your network, and share devices without having to share passwords.

Seamless SSO and Network Auto boot

Better yet, mobile or remote users can leverage Password Sync to Single-Sign-On (SSO) while off the network, and users on the network can take advantage of WinMagic's PBConnex technology to bypass pre-boot when connected to authorized wired or wireless networks for ultimate flexibility in your mobile work environment.

Enhanced Security

Secure Network Authentication and Key Management

BitLocker with SecureDoc pre-boot enables network-brokered authentication, where user access policies and credentials are verified over the network at pre-boot before the keys are delivered to the device – that's the power of pre-boot networking with PBConnex. SDOT also adds support for MFA with smartcards and tokens, Disk Access and Port Control, as well as policy-driven Removable Media Encryption (RME) and SecureDoc File Encryption (SFE).

Tamper Protection for BitLocker

SDOT for BitLocker enhances protection across your enterprise with more granular controls over user and administrator rights. Tamper Protection for BitLocker can automatically detect and reverse unmanaged Suspend or Turn Off BitLocker commands, ensuring that your devices are always in a compliant state. For a more preventative approach, BitLocker settings via Control Panel or Manage-bde can be blocked altogether.

Simplified Management

Zero-Touch Deployment

With SDOT for BitLocker, IT Admins can deploy BitLocker-protected devices without any user interaction, transparently designating the user as the device owner when they login to Windows and automatically initializing encryption silently in the background.

Quick Password Recovery and Sync

Reduce helpdesk downtime with simplified password changes and recovery, eliminating the need for 48-character BitLocker recovery passwords. If a user forgets their password, they can use Self-Help Recovery or 16-character Challenge-Response locally. IT admins can also reset passwords at pre-boot remotely from the SES Console via PBConnex. All password changes are seamlessly synced with Active Directory and locally with Windows on the device.

Simplified Patch Management

SDOT enables Pre-boot Networking (PBN) via WinMagic's PBConnex technology so IT admins can rollout unattended software updates and patches in scenarios such as Wake-On-LAN (WOL) without having to temporarily Suspend BitLocker, and without any costly or complex hardware configurations such as DHCP, WDS server and a wired network connection.

Key Benefits of SDBM:

- Upgrade Windows OS without having to decrypt and re-encrypt your devices
- Create, Deploy and Manage BitLocker policies directly from SES Management Console
- Intelligent Key Management securely creates, stores and delivers user-specific key files
- Recovery keys are also stored in a secure, central database
- Strengthen compliance with centralized logs and reports
- Prevent users from suspending or decrypting BitLocker with Tamper Protection
- Sync with AD/LDAP services to enforce policies against changing users and groups
- Prevent data leakage with Disk Access Control, Port Control and OS-Agnostic RME (full or container-based)
- Protect local folders and network shares with the optional policy-driven SFE

Advanced features with SDOT enabled:

- PBConnex Authentication
- PBConnex Auto Boot via Wired or Wireless Network
- User Single Sign-On
- Password Sync with Windows
- Zero-Touch Deployment
- Self-Help Password Recovery
- Web Browser Support for Identity Management Systems (IdM) at Pre-boot
- Multi-Factor Authentication with Smartcards and Tokens
- Customizable Boot Logon – including splash screen, text and color scheme