Data Sheet

SecureDoc by WinMagic

SecureDoc Enterprise

Endpoint Encryption | Device Control

> "Full disk and file system encryption will always play the first line of defense"
>
> Market Guide for Information-Centric Endpoint and Mobile Protection, **Gartner (2017)**

Protect

- Endpoint Devices – Desktops, Laptops, Tablet PCs and VDI
- Removable Media – USB, CD/DVD, SD and portable drives
- Files, Folders and Network Shares

Prevent

- Data Loss or Theft
- Improper Disposal
- Unauthorized Access
- Compliance/Audit Failure

Passwords alone cannot protect your business. Endpoint encryption is the essential first line of defense to protect sensitive or confidential information, prevent costly data breaches, and achieve key compliance objectives.

That said, the proliferation of data and devices across your business has increased the complexity of deploying encryption – a challenge further amplified by constantly evolving hardware, OS updates, and increasingly mobile users. Securing data in the event of a lost or stolen device has never been more challenging.

WinMagic SecureDoc Enterprise offers a single, unified console to manage data and device protection – combining industry-leading endpoint encryption with robust device and port controls to significantly reduce the threat of data loss. That way, you can apply persistent encryption to protect virtually any hardware or OS platform, even as you shift from physical to virtual desktops.

Data Security Challenges. Solved.

Maximize Protection with Enterprise-wide Coverage

Protect data and devices with flexible, multi-OS encryption support.

- Protect devices with industry-leading FIPS 140-2 compliant full drive encryption
- Leverage built-in OS encryption with BitLocker or FileVault 2
- Manage hardware-embedded encryption with the most expansive Opal SED support
- Prevent data loss with OS-agnostic removable media encryption and granular device and port controls

Simplify Data Security & Compliance

Centrally deploy, manage and monitor encryption from a single console.

- Deploy encryption faster with compatibility automation tools and transparent user provisioning
- Manage users, keys, and policies with Active Directory integration
- Reduce compliance reporting time by up to 60% with a single dashboard for all devices
- Protect remote users and devices with network-aware pre-boot authentication

Lower TCO with Improved User & IT Helpdesk Uptime

Don't compromise productivity for security – get the best of both.

- Reduce IT helpdesk time spent on password resets by up to 75% with multiple user recovery options
- Maximize user uptime with faster and more secure single sign-on or network-aware unlock
- Quickly respond to lost or stolen device scenarios with remote lock, reset or "kill" commands
- Streamline operations with role-based access to management, recovery and reporting tools

Technical Specifications

Client Support
- Windows 7 and later (32/64-bit)
- Windows-Embedded for IoT
- macOS 10.10 and later
- Linux OS versions (SED Only)

Encryption Support
- SecureDoc Drive Encryption
- SecureDoc File Encryption
- Microsoft BitLocker for Windows
- Apple FileVault 2 for macOS
- TCG Opal 1.0/2.0 SEDs

VDI Support
- Citrix XenDesktop
- VMware Horizon

Validations
FIPS 140-2, OPSWAT Gold

Management Server
- Windows Server 2008 or later (32/64-bit)

See System Requirements for more information.

Key Features.

Unified Key Management & Compliance

SecureDoc Enterprise Server (SES) lets you enforce consistent protection, policies and compliance reporting across all data and devices in your mixed IT environment.

- Unify key and policy management under a single platform, synchronized with Active Directory for a user-centric approach
- Enable industry-leading PBConnex technology for significantly faster recovery, policy updates, and user authentication over secure wired or wireless networks
- Manage remote devices outside of the network, ensuring that your most vulnerable data is protected from breaches

Industry-leading Drive Encryption

- Protect all data – including the Operating System – with FIPS 140-2 validated SecureDoc Full Drive Encryption (FDE)
- Enforce robust pre-boot protection with support for Active Directory, Multi-Factor and Network-Based Authentication
- Leverage OS-agnostic, agentless management of Opal Self-Encrypting Drives (SED) with the most comprehensive compatibility program in the industry

Advanced Native Encryption Management

- Centrally enforce encryption on BitLocker or FileVault 2-enabled devices, ensuring consistent compliance and audit trails
- Don’t just manage native OS encryption, enhance it with the SecureDoc pre-boot client for faster and more secure authentication, customizable pre-boot and MFA support
- Turn on Tamper Protection to automatically block privileged users and applications from disabling or suspending encryption for always-on protection form deployment to decommission

Robust Removable Media Encryption & Device Controls

- Enable automatic, enforced encryption of removable media devices – including portable drives, USB, CD/DVD and SD Cards
- Share and access encrypted data across any endpoint device without the need for any additional software installation
- Apply trusted device and port controls to prevent data loss or offline malware injection via external media

Transparent, Persistent File Encryption

- Upgrade your SecureDoc Enterprise clients with automatic and transparent file-level encryption, protecting access to individual files and folders
- Never interrupt workflow – encryption, decryption and access to information is automated and transparent to the end user
- Centrally enforce automatic encryption or allow users to manually encrypt individual files and folders, with persistent protection even when shared

	SecureDoc Enterprise	SecureDoc Essentials	SecureDoc Standalone
Key Management			
Centralized Key and Policy Management	x	x	
Advanced Reporting and Auditing Tools	x	x	
Active Directory User Integration	x	x	
Remote Device Management	x	x	
Endpoint Encryption			
FIPS 140-2 Validated Full Drive Encryption	x		x
Manage BitLocker for Windows	x	x	
Manage FileVault 2 for macOS	x		
Leverage Opal Self-Encrypting Drives	x		x
Upgrade with File and Folder Encryption	x		x
Access Controls			
Network-Aware Pre-Boot Authentication	x	x	
Network-Aware Auto-Unlock	x	x	
Wireless Pre-Boot Networking	x		
Granular Device and Port Controls	x		x
Removable Media Encryption	x	x	x
Multi-Factor Authentication Support	x		x

How Can You Protect Your Data Everywhere?

If you already have SecureDoc Enterprise Endpoint Encryption, consider building out an enterprise-wide data security strategy beyond your endpoints. Simply add new license modules to your SecureDoc Enterprise Server, including:

- **SecureDoc File Encryption** – Protects data stored in local files and folders, as well as network file shares
- **SecureDoc CloudSync** – Encrypts data stored in Cloud-based Enterprise File Sync and Share (EFSS) solutions
- **SecureDoc for Servers** – Ensures your backed physical servers infrastructure is protected from offline attacks
- **SecureDoc CloudVM** – Protects virtual and cloud workloads from a range of known threat vectors

SecureDoc Enterprise Server offers the flexibility to protect data across physical, virtual and cloud infrastructure. Combining modules enables a defense-in-depth strategy to deliver persistent encryption of data wherever it resides across your organization.