

SecureDoc OSA for Servers

OS-Agnostic Encryption & Protection for Enterprise Servers

- Enhance security by managing TCG Opal & TCG Enterprise Self-Encrypting Drives (SEDs)
- Assure security of server through startup and authentication
- Centrally manage all servers and devices with SecureDoc Enterprise Server
- Eliminate the need for OS-specific software installation
- Support any distribution of Linux*



The key selling point for self-encrypting drives isn't just that they encrypt data, but that it's carried out in the firmware of the drive."

Ashton Mills, CSO Online

OSA for Servers Benefits

Enhanced Compatibility

Pre-boot authentication eliminates the need to create an OS-specific installation package helping avoid bothersome compatibility issues, and reducing the risk of boot attacks.

More Secure Authentication

Enables secure remote unattended booting/rebooting of servers by implementing pre-boot network authentication.

Increased Compliance Assurance through Leading Technology

Managing Self-Encrypting Drives adhering to the Trusted Computing Group Opal or Enterprise Specifications with SecureDoc OSA for Servers increases the ability to meet industry or regulatory requirements for data security.

Reduced Risk from Physical Theft

Protects the organization from the data breach risk associated with the physical theft of the system storage devices – devices are rendered useless without being able to authenticate over the network.

Full Disk Encryption for your back-end infrastructure

Organizational servers should always be encrypted. Encryption is the bedrock of strong data security. If your servers are not properly encrypted, critical information could be at risk of being exposed, leaving an organization susceptible to regulatory violations, personal lawsuits, and damage to corporate reputation.

In an environment where organizations have a need to deploy combinations of multiple operating systems including Windows and Linux, taking an OS-neutral approach to managing these systems is extremely efficient compared with deploying and managing multiple encryption solutions. With organizations subject to more compliance and data controls than ever before, the need for one solution to manage all servers has never been greater.

OS-Agnostic Protection for Servers

WinMagic's SecureDoc OSA (Operating System Agnostic) for Servers helps businesses lock down their infrastructure investment, offering hardware full disk encryption and a host of other features to seamlessly manage and secure the data residing on a company's servers, regardless of the operating system.

SecureDoc OSA manages the SEDs with no OS-present. Installation is performed at pre-boot which eliminates the need to create an OS-specific installation package, and helps avoid bothersome compatibility issues.

SecureDoc OSA is ideal for organizations that require the ability to run Linux in their environment, and still be able to manage and audit the security of systems.

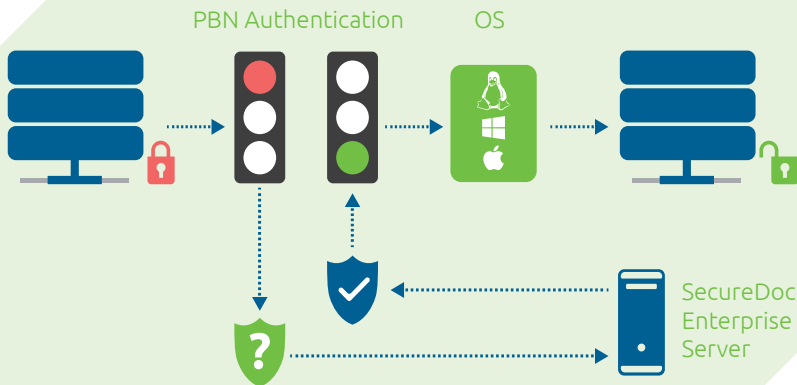
Robust Authentication

With so much focus today being on identity and access control; it is important to have an encryption solution in place that can provide more robust authentication of servers to ensure that your data is safe from harm. WinMagic provides organizations total control over their data security environment through our **SecureDoc Enterprise Server (SES)**, ensuring maximum security and transparency in the regular work flow.

With SecureDoc OSA, WinMagic has also removed a key pain point for IT administrators by enabling secure remote unattended booting/rebooting of servers via PBConnex – WinMagic's Pre-Boot Network Authentication, before the operating system ever loads – something traditionally impossible for encrypted servers.

Enabling PBConnex also ensures that should a server or hard drive ever leave the premise, or was lost or stolen, the data residing on those devices would be inaccessible.

Automated Network-Based Authentication for Servers



SecureDoc OSA for Server features include:

- Enhanced Policy & User Control
- Centralized Auditing
- PBN Auto-boot
- Multi-Factor Authentication
- Crypto Erase

How it works

WinMagic's PBConnex delivers the power behind SecureDoc OSA for Servers solution. PBConnex utilizes network-based resources to authenticate and enforce access controls before the operating system loads. From the point of initial boot, restart, or unattended reboot, PBConnex authenticates the Trusted Computing Group (TCG) Opal or Enterprise drive against the SecureDoc Enterprise Server, validating the existence of all controls and authentication requirements. If successful, SecureDoc then allows the OS to load, unlocking the server.

This unique and ground-breaking approach to Full Disk Encryption (FDE) management results in significant cost savings for organizations by streamlining IT management.

What are the other benefits in partnering with WinMagic?



User & Device-Based Authentication

Utilizes wired and wireless pre-boot network authentication to enforce access controls and manage end point devices before the operating system loads.

Reduces the total cost of IT ownership: Cuts password reset time by 75% and PC staging time by 75%.



Cross-Enterprise, Multiplatform

Easy to use in multi-platform environments, supporting Windows, Mac and Linux.

Synchronizes user credentials across hardware platforms and device types.



Cloud IaaS Encryption & Key Control

For enterprises adopting or working in a virtualized or Cloud IaaS Environment who need to protect their data, demonstrate compliance, and want greater control and certainty over the security of their data (strengthening security and reputational posture), SecureDoc CloudVM is a data security solution that protects against undisclosed government access, malicious insiders, or external breach by separating encryption management from the hypervisor, which unlike CSPs, provides enhanced high performance data protection using enterprise-controlled key management; ultimate flexibility in deployment; and eliminates vendor lock-in.



BitLocker Management

SecureDoc manages BitLocker with the benefits of lower IT costs and increased IT efficiency.

SecureDoc is platform agnostic, and capable of managing Windows, macOS, Linux and any other current available operating systems, unlike MBAM.

*OSA supports any type of software RAID, but does not support hardware RAID. The HBA must support pass-thru of the TCG management commands.

Notes:

1. At least 1 Opal drive is required to boot from the Shadow MBR. Other drives may be TCG Opal or TCG Enterprise drives, selected from WinMagic's compatibility list
2. OSA for Servers is for applications where multiple drives are required. When only one Opal drive is used, customers should use OSA for Workstations.

Authenticate. Encrypt. Achieve.

