SecureDoc For Servers
WinMagic

Full disk encryption for your back-end infrastructure

Departmental servers should always be encrypted - even if they only run a process as simple as print services - as they often reside in unsecured environments. Any server that manages data related to a business and its customers needs to be secured from prying eyes.

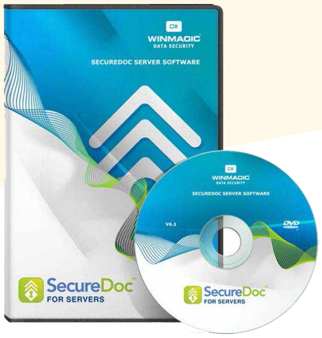
Just because servers reside in some of the most secure areas of a business this doesn't preclude them from being at risk to data loss or theft. Something as simple as an IT manager swapping storage drives in a server and misplacing them could lead to a data loss. If that drive isn't encrypted, its information is at risk of being exposed, leaving an organization at risk of regulatory violations, personal lawsuits and damage to corporate reputation.

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

KEY FEATURES

- Ideal for departmental servers
- Support for TCG Enterprise Drives
- Only full-disk encryption solution to offer pre-boot network authentication via PBConnex
- Certifications: FIPS 140-2, AES validation
- Can be centrally managed by SecureDoc Enterprise Server (SES)
- RAID Support*

WINMAGIC®
DATA SECURITY



SecureDoc
FOR SERVERS

SecureDoc is ready to support all of your encryption needs now and well into the future.

SecureDoc for Servers and OSA for Servers allows administrators to fully encrypt, secure and manage their server environments.

With the knowledge that a server has different demands placed on it versus a traditional PC, WinMagic has worked to optimize SecureDoc for Servers to address items such as RAID arrays, Disk and Port access control and remote management.

- SecureDoc for Servers uses a FIPS 140-2 validated AES-NI 256-bit cryptographic engine to encrypt data and easily integrates with industry-standard technologies.

- SecureDoc places all security-related management under one centralized enterprise management server. This includes the management of policies, password rules, and the manageability of encryption across all platforms within an organization.

SecureDoc OSA for Servers

WinMagic has been working with the TCG and supporting the Opal SED specification since its inception. WinMagic's leadership in this space is evident by its market-leading support of Opal-compliant drives as well as through the innovative use of PBConnex in combination with SED management – SecureDoc OSA.

WinMagic has taken a similar approach to TCG Enterprise drives. In order to meet the demands of servers, larger storage is required that can be supported by TCG Enterprise drives. Enterprise Drives offer the best, most secure and efficient way to encrypt data on a disk. With OSA for Servers, WinMagic has removed a key pain point for IT administrators and enabled remote unattended booting/rebooting of departmental servers via our pre-boot network authentication – something traditionally impossible for encrypted servers.

PBConnexTM

SecureDoc with PBConnex is the only data encryption and management solution that allows for pre-boot network authentication. The ability to enable secure boot-up in a server environment, where unattended reboot of a machine is common, adds a layer of security that helps ensure business continuity. This means that if a server ever has to restart due to failure or other causes, it can easily be restarted and authenticated without any onsite management. PBConnex utilizes network based resources to authenticate and enforce access controls before the operating system loads. This unique and ground-breaking approach to Full Disk Encryption (FDE) management results in significant cost savings for organizations by streamlining IT management.

The other key benefit to this approach is the limited liability exposure due to physical loss or theft of a server or hard drive. If a server or hard drive ever left the premises and was lost or stolen, the data residing on those devices would be unreadable; there would be no key on the machines or hard drives that would enable an attacker to decrypt the data.