WINMAGIC®
DATA SECURITY

SECUREDOC FOR SERVERS

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 a company at risk of regulatory violations, personal lawsuits and damage to corporate reputation.

FEATURES AT A GLANCE:

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

SecureDoc™

*Not all RAID controllers are supported.

SecureDoc for Server enables administrators to fully encrypt, secure and manage their server environments.

WinMagic's SecureDoc for Servers helps businesses lock down their infrastructure investment, offering full disk encryption and a host of other features to seamlessly manage and secure the data residing on a company's servers.

- SecureDoc for Servers uses a FIPS 140-2 certified AES 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.

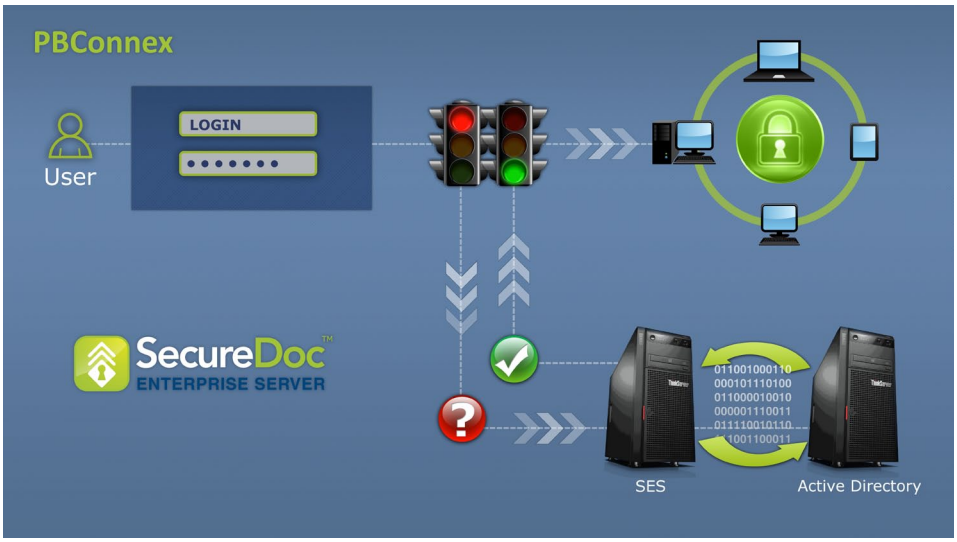
With the knowledge that a server has different demands placed on it versus a traditional PC, WinMagic has worked to optimize SecureDoc for Servers to address things such as RAID arrays, Disk and Port access control and remote management.

PORT & DISK ACCESS CONTROL

Data leakage is an ongoing concern in any business. With Port Control, administrator can lock down a server and prevent the transfer of data to an external storage device. Alternatively, through Disk Access Control, the ability to read/write to any external media can be limited only to encrypted drives to ensure the security and integrity of the data being transferred or stored.

PBCONNEX

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, was lost or stolen in transport to a storage facility etc., 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.

AWARDS & CERTIFICATIONS

WINMAGIC DATA SECURITY

sales@winmagic.com | www.winmagic.com