Solution Brief

SecureDoc Linux for Servers

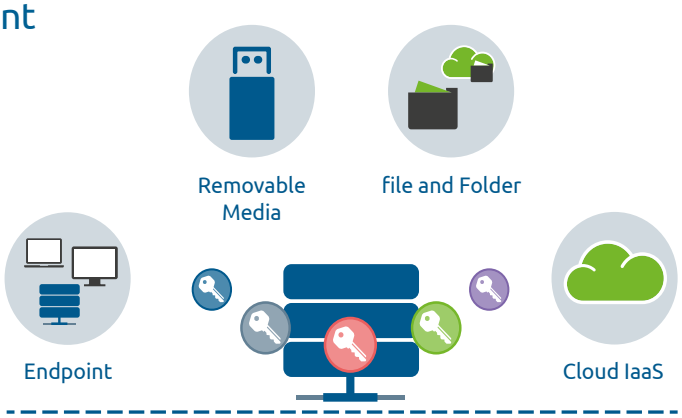
SecureDoc Linux for Servers, the only enterprise-class Full Disk Encryption software on the market for Linux Servers works on top of dm-crypt, rather than replacing it, to better manage encryption – taking Linux encryption management to the next level and solving the real world needs of large global technology organizations.

When it comes to server protection, many enterprises overlook physical security risks. The common myth is that because the servers are in a data center, or otherwise behind lock and key, and because the data is in perpetual use, encrypting the drives is unnecessary as the data is never at-rest. Add in the complexities required to encrypt Linux devices, and it's no wonder that so many organizations simply avoid it all together. That's particularly troublesome. All drives eventually leave the data center for repair or disposal and having them encrypted is the best way to protect you and your data from unintentional exposure.

Separation of Encryption and Key Management

To be most effective, an encryption product should be separated into two components – encryption and key management because the expertise to deliver these two components is quite different. That's the magic behind SecureDoc Linux for Servers, the only enterprise-class Full Disk Encryption software on the market for Linux Servers. The solution layers on top of dm-crypt rather than replacing it to better manage encryption – taking Linux encryption management to the next level and solving the real world needs of large global technology organizations.

- Secure your Linux environment, and still be able to manage and audit the security of systems
- Manage any operating system native software encryption (Linux, Windows, or Apple) or Self-Encrypting Drive
- Compatible with the most advanced storage approaches



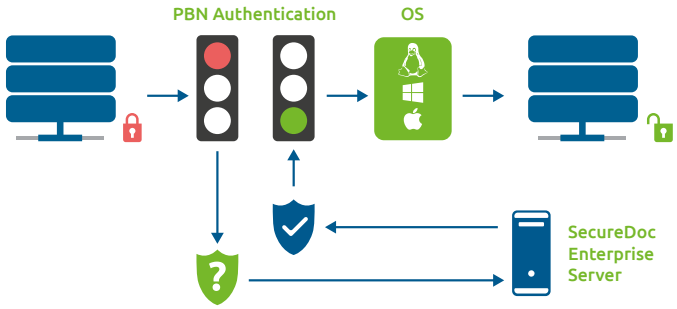
Robust Authentication

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. Together, dm-crypt and LUKS, Linux' current encryption capabilities, form the basis for a simple "standalone" password authenticated FDE application. However, is not an enterprise grade solution especially for servers where it is very inconvenient to have to have an admin present...

With SecureDoc Linux for Servers, WinMagic has 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.

- Improve authentication security with Pre-boot Network-based authentication – ensuring security before the OS boots
- Allow Active Directory username and passwords to authenticate at pre-boot, unlike Linux which requires having a pre-boot password or different passwords for each volume, and doesn't support AD

Automated Network-Based Authentication for Servers



SecureDoc™ by WinMagic

Full Disk and Root Volume Encryption

Root volume encryption, data volume encryption and encrypting swap partitions are all required within most organizations. However, protecting the root volume with Linux native FDE is very complex. SecureDoc Linux for Servers provides an improved mechanism for encrypting Linux servers.

- Optimized to address RAID arrays, Disk and remote management

Live Conversion on initial encryption

Minimizing downtime is critical to organizations operating in a fast-paced market. Taking down servers for hours or days to encrypt them is a disruptive and painful practice. That's why SecureDoc Linux for servers provides customers the ability to:

- Encrypt pre-installed Linux servers without having to wipe the disk or re-install Linux with encryption enabled before commencing encryption
- Save valuable time and money from avoided disruptions

Centralized password & key management of encrypted system

Simple password recovery, operations & management of encrypted Linux devices is essential. What's more important is providing this from a centralized console, that should also be able to provide central backup of the encryption keys and recovery info.

- Centrally manage all servers and devices with SecureDoc Enterprise Server (SES)
- Cryptographically erase keys when a device is compromised or is to be repurposed. (This operation should also be recorded for compliance reasons) encryption enabled before commencing encryption

Strengthened Compliance

For enterprises facing potentially crippling penalties for a compliance failure under data protection regulations like GDPR and HIPAA, having a seamless and integrated key management solution for Linux- and Windows-based servers is essential. With SecureDoc, operation, management and recovery of the servers are all possible within a single console. The encryption status of each server is tracked to ensure its data is in a protected state and is viewable in a single pane of glass – giving auditors and business leaders the certainty they need to pass a compliance audit.

- Strengthen compliance posture by encrypting the data itself
- Gain instant visibility of server, endpoint, or virtual machine encryption status through an easy-to-read single pane of glass
- Quickly meet compliance needs with easy audit and reporting tools

SD Linux for Servers Features

- **Live Conversion** allowing admins and users to log-in and work on the machine while encryption occurs
- **Encryption Simplicity** removing the need to clear the disk and re-install the OS before commencing encryption
- **Pre-boot network-based authentication** – the additional security measures needed to keep data safe
- **Enterprise Manageability** making operation, management and recovery of Linux devices possible within a single console

Client System Requirements

redhat

SUSE

CentOS

ubuntu

WINMAGIC®

US & Canada +1 888 879 5879 | EMEA +49 69 175 370 530 | Japan +03 5403 6950