Customer Case Study

# Encrypting Linux Servers

## Why You Can't Trust 'Good Enough' in the Age of Compliance

When the staff within the data center of a large financial services institution recently packaged up a few drives and servers to send to IT for repairs, they really didn't consider the ramifications of doing so. What could really go wrong, right? Unfortunately, during shipping, the packages were stolen. The servers were not encrypted, and the personal data of customers was exposed.

## Business Challenge

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.

This was the case with a regional financial services institution (FSI) that has hundreds of servers spread across hundreds of branches. There were no IT personnel at each individual branch capable of analyzing and repairing the servers. These resources are based at headquarters. Therefore, when there are issues with the server, including drives, the components were required to be shipped via postal service of courier service to headquarters to be analyzed, repaired, or replaced. Sometimes these drives even became misplaced internally during the process.

So where did it all go wrong? For one, the FSI struggled with complexity in managing data security across its server portfolio. They were operating both Windows- and Linux-based servers, and had different management means for both operating systems. While native encryption solutions were considered – with no enterprise solution even being available for Linux – they were not applied due to the false sense of security of having servers behind lock and key, and a desire to keep systems unencumbered and transparent. Secondly, they had also no detailed plan/assurance of persistent encryption during movement of devices. When they shipped drives with data on them, they were assuming the risk that it could be lost or stolen in transit, and this was exactly what happened. The FSI mistakenly assumed a level of trust and security with its staff, its transport methods, and its reliance on External 3rd party IT support - which they now identify as a risk, too.

## Compliance Challenge

Being in the financial industry, the FSI was very cognizant of the potentially facing crippling penalties for a compliance failure under data protection regulations like GDPR or PCI-DSS. Unfortunately, a decision not to encrypt the devices was made due to a combination of both misjudgment of costs and risks. GDPR even recommends encryption. Encryption is explicitly cited throughout GDPR documentation and other similar data privacy regulations as a 'recommended best practice'. The GDPR has significantly raised the bar on the "minimum requirement" making encryption one of the most sensible uniform security solutions available. The transparent operations and security behind data-at-rest make it a wise choice for organizations to apply FDE to their servers.

SecureDoc™ by WinMagic

## CUSTOMER OVERVIEW

### Industry
Financial Services

### Challenges

- Customer required encryption due to a recent internal data breach where drives were lost during shipping to IT for repair
- Customer mistakenly assumed a level of trust and security with transport methods
- Customer was reliant on external 3rd party IT support, which they now identify as a risk

### Pain Points

- Complexity in managing data security across its server portfolio
- Fear of failing compliance if devices breached or lost
- No plan/assurance of persistent encryption during movement
- Linux Encryption was too complex, leading to customer avoiding it
- Costs: Customer is extremely OPEX sensitive, and more comfortable with CAPEX

### WinMagic Solution

• SecureDoc for Servers
• SecureDoc Linux for Servers

### SecureDoc for Servers (Windows & Linux) 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

## Technical Solution

The solution to the FSI's challenges with managing server security throughout its network of branches was simple; encrypt all the remotes servers. Then, if lost in transit, the risk is limited to the replacement cost of the drive, which is order of magnitude less than dealing with the legal and financial consequences of a breach.

Many organizations rely on native platforms like Linux or Windows for their flexibility and robustness to deliver an enterprise's workloads. This includes a reliance on built-in tools like dm-crypt or BitLocker. While these native encryption toolkits are the best at encrypting either Windows- or Linux-based devices, the operating systems can further benefit from independent encryption management solutions to manage and unify encryption efforts across an enterprise.

That's the magic behind the SecureDoc for Servers (including the only enterprise-class Full Disk Encryption software on the market for Linux Servers). The solution can work independently as standalone FDE solutions or, can take over the native encryption solutions with our pre-boot intelligence, rather than replacing them, to better manage encryption – taking native encryption management to the next level.

With SecureDoc's Server solutions, WinMagic removes a key pain point for IT administrators by enabling secure remote unattended booting/rebooting of servers via PBConnex – WinMagic's Pre-Boot Network Authentication. PBConnex improves authentication security, – ensuring security before the OS boots. It also allows Active Directory username and passwords to authenticate at pre-boot. When it comes to password recovery, operations & management of encrypted devices, SecureDoc makes it simple providing this from a centralized console, that also serves as a central backup of the encryption keys and recovery info.

With SecureDoc, operation, management and recovery of the FSI's servers are all now 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 the FSI's auditors and business leaders the certainty they need to pass a compliance audit.

## Business Results

WinMagic's encryption software was deployed to nearly 1000 servers through SecureDoc's seamless deployment process. All devices were encrypted in a very short time period, with no downtime, and not a single support ticket being opened, resulting in significant cost savings. With WinMagic's SecureDoc encryption software and intelligent key management solution the financial services institution was able to significantly reduce its security concerns around data protection on its servers, easily integrating the solution within their business environment, without compromising the user or customer experience.

While the servers remain behind lock and key, the customer now has the peace of mind in knowing that their data is safe on their servers whether they are in a rack, or on the road – and the confidence in knowing that their encryption solution conforms to their compliance requirements.