Customer Case Study

Full Disk Encryption

The right preventative measure for large healthcare provider

When the staff of a large regional healthcare provider recently discovered a gap in its data breach protection during a regular control audit, they started building their revised data security plan. All too quickly though, they were faced with the reality of trying to coordinate the deployment of encryption to tens of thousands of devices, in hundreds of branch offices, with their current set of mismatched solutions.

Business Challenge

Regional Healthcare Providers (RHPs) are the stewards of significant volumes of sensitive data including the names, healthcare numbers, address, gender, race, date of birth and medical history of patients. With the ease in which data flows across networks of healthcare centers, and the risk inherent in allowing such a large audience of personnel to have access to highly sensitive data, organizations need to be confident that a patient's record is secure whenever it is being transported or stored. And, with increasing data privacy compliance requirements and the fines attached with a compliance failure, there is no justifiable reason not to encrypt data at every point within the business it's simply a healthy data security practice. Unfortunately, for some organizations, trying to cohesively manage data security over a branch network is a trialing challenge, often leaving gaping holes in protection.

This was the case with a nation-wide healthcare provider that had tens of thousands of endpoints across hundreds of offices. There was simply no unified strategy or solution deployed across the network. Thousands of devices had insufficient encryption, or worse, none at all.

So, what were the customer's main challenges? For one, the RHP struggled with complexity in managing data security across its laptop and desktop portfolio. They were operating a Windows-based environment. While BitLocker, a native encryption solution, was considered were considered, it nor other solutions were not applied due to a desire to keep systems unencumbered and transparent. Secondly, the RHP had no detailed plan/assurance of persistent encryption during movement of devices. When laptops moved with sensitive data on them, they were assuming the risk that it could be lost or stolen in transit. The auditing team identified this as a serious risk to the team, that could land them in contravention of a number of data security regulations.

Compliance Challenge

Data security has become especially critical to the healthcare industry as the frequency of breaches continues to rise. Patient privacy hinges on data security regulations, like the Health Insurance Portability and Accountability Act (HiPAA) to drive compliance. However, compliance is not a one-time project – rather, it's an ongoing effort requiring regular risk assessments, compliance monitoring and workforce training. Unfortunately, an earlier decision by the RHP not to encrypt the devices was made due to a combination of both misjudgment of costs and risks in their data security strategy.

Customer Case Study

SecureDoc™ by WinMagic

CUSTOMER OVERVIEW

Industry
Healthcare

Pain Points

- Complexity in managing data security across its device portfolio
- Many devices were left accessible in open public spaces
- Fear of failing compliance if devices breached or lost
- No plan/assurance of persistent encryption during data movement
- Many devices had multiple users sharing PINs

Challenges

- No current continuity in encryption solutions (where existing) across the organization
- Customer required to encrypt tens of thousands of devices in short order
- Customer is extremely OPEX sensitive, and more comfortable with CAPEX

WinMagic Solution

- SecureDoc Enterprise (FDE)
- SecureDoc File Encryption

SecureDoc Features

Industry-leading Drive Encryption: Protect all data and the OS with FIPS 140-2 validated SecureDoc Full Drive Encryption (FDE)

Robust RME & Device Controls: Enable automatic, enforced encryption of removable media devices – including portable drives, USB, CD/DVD, SD Cards

Advanced Native Encryption Management: Centrally enforce encryption on BitLocker or FileVault 2-enabled devices

Transparent, Persistent File Encryption: automatic and transparent file-level encryption, protecting access to individual files and folders

Pre-Boot Network Authentication: Keep data safe by ensuring devices are booted only when on your network

Enterprise Manageability: Operation, management and recovery of encrypted devices possible within a single console

Technical Solution

In a device-sharing environment, it was imperative that the healthcare provider's data not only be protected in the event devices are stolen, but that individual user data residing on the same devices be protected from unauthorized access. **One truth exists when it comes to data protection – encryption is the bedrock of any data security strategy**, and it's the most effective way to protect electronic Personal Health Information (ePHI) and significantly reduce the risk of breach notification.

After discussing WinMagic's solution set, the Regional Healthcare Provider opted to use WinMagic's time-tested full disk encryption product – SecureDoc Enterprise, in addition to SecureDoc File Encryption. WinMagic SecureDoc Enterprise offered the customer a single, unified console to manage data and device protection – combining industry-leading endpoint encryption with robust device and port controls to significantly reduce their threat of data loss. With SecureDoc, the RHP was able to apply persistent encryption to protect virtually any hardware or OS platform they may bring into the organization, even as they you shift look to shift from physical to virtual desktops.

SecureDoc is known for its protection of ePHI. With FIPS 140-2 validated encryption across nearly any device or server. For organizations with shared devices, like mobile laptop carts and USBs, SecureDoc provides organizations the required methods to partition access across its user base, well beyond a simple password or PIN.

WinMagic's SecureDoc Enterprise Server (SES) manages everything encryption within the enterprise, whether it's FDE, removable media or individual files and folders. It places all security-related management under one centralized enterprise server, including policies, password rules, and the manageability of encryption across PC, Mac and Linux platforms alike. It also easily integrates with industry-standard technologies such as Opal-compliant Self-Encrypting Drives (SEDs) while also managing native OS encryption solutions such as Microsoft BitLocker, FileVault2, and dm-crypt. Regardless of the OS or platform, WinMagic is poised to meet any of the customer's growing needs.

When it came to access management, SecureDoc's Intelligent Key Management checked off all the RHP's wish list items. For one, it provided secure, centralized management of encryption keys and access policies. SecureDoc does so via its web-based console with role-based access to ensure separation of duties. And with SecureDoc's Pre-Boot Network Authentication feature – PBConnex – WinMagic was able to provide a unique way of ensuring that devices would not boot if they were off the network. Transition is quick and painless, without compromising security. To unify it all, SecureDoc's single pane of glass was able to provide the customer with detailed audit logs and monitoring for all endpoints, removable media, files and folders, and cloud instances across the organization, providing accountability and assurance with audit control requirements.

Business Results

WinMagic successfully encrypted tens of thousands of endpoints of the nation-wide healthcare provider; protecting highly sensitive personally identifiable information (PII) of its patients against breach. With WinMagic's SecureDoc encryption software and intelligent key management solution, the RHP was able to address both its device and file security concerns. And this was all accomplished through a transparent deployment that had minimal impact on the operational processes or daily workflow of the organization's healthcare professionals.

Interested in learning more about WinMagic's encryption solutions for healthcare? Visit **winmagic.com**, or email **info@winmagic.com**

Authenticate. Encrypt. Achieve.

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

WINMAGIC®