ENDPOINT ENCRYPTION EQUATES TO COMPLIANCE

IT Risk Management

Client Profile

A large nonprofit health system providing the highest quality care to all, with special attention to the poor and vulnerable.

Challenges

Like all healthcare providers, the client faces daunting regulatory compliance issues that continue to evolve as technological advances are made. With the prevalence of mobile devices in medical facilities today, full disc encryption is required to meet HIPAA and HITECH requirements. For this healthcare provider, implementing full disc encryption posed a significant challenge because the health system is actually a group of over 30 hospital organizations located across the country.

While there were standards in place for administrative functions throughout the organization, they hadn't taken hold in the IT department, resulting in a nonstandard environment with multiple servers and differing policies. With multiple servers in varying geographic locations comes the need for several IT management teams, creating inefficiencies in both deployment of personnel and utilization of hardware. In addition, inconsistent policies can lead to further compliance violations.

In addition to the logistical struggles that led to IT inconsistencies throughout the network, it was determined that client's equipment didn't support the necessary software.

Solution

After systematically exploring the needs and technical capabilities of each hospital organizations' environment, CBI recommended that the client consolidate to a single point of control with a small group of management servers that would generate generic policies overall, while implementing specific policies for each ministry based on individual findings.

In order to meet the full disc encryption requirement, CBI implemented the Symantec Endpoint Encryption product—a data at rest encryption software that secures locally saved information. The product comes with a pre-boot authentication system, which is a HIPAA/HITECH requirement. The removable storage encryption functionality played a key role in this decision as well, as it protects valuable data that is transferred to portable storage devices that can leave the health system's facilities.

The policies were created during implementation of Symantec Endpoint Encryption. CBI designed a custom installation package that reported back to each ministry endpoint with policies that would work best for each environment based on security and compliance needs. Hospitals that required multiple logins for each machine, for example received different policies than the hospitals that had individual machines with sole access.

Finally, CBI addressed the incompatible hardware issues by working with Symantec to re-code the unsupported equipment. After six code rewrites, the hardware was able to support the endpoint encryption re-booting process.

Results

First and foremost, the CBI encryption solution enabled the client to meet regulatory compliance requirements, avoiding costly fines and public scrutiny. The removable storage aspect of Symantec Endpoint Encryption has recovery certification, meaning that the client's IT team can recover any encrypted data—a real failsafe from data loss. In fact, CBI implemented the product across nearly 100,000 machines without losing any data.

In addition to the compliance and data protection benefits, the consolidated system, along with centralized monitoring and reporting, delivered a major convenience factor to the client. The healthcare provider's original plan for addressing their compliance needs would have required a team of 32 IT professionals. The CBI solution delivered four servers in one central location managed by just three IT experts…a better use of personnel and hardware resources that generated measureable cost savings for the client.

OVERVIEW

Industry
Healthcare

Solution
Endpoint Encryption

CBI Generated Results

- Ability to satisfy compliance requirements
- Encrypted data recovery, mitigating data loss
- Four servers in one central location managed by just three IT experts

CBI CASE STUDY