EndoChoice, Inc.

Deploying workplace data security solutions across remote locations

EndoChoice® is a global medtech company focused on the manufacture and commercialization of platform technologies for specialists treating a wide range of gastrointestinal diseases. It is based in Atlanta, Georgia but has offices in various corners of the world, subjecting the company to disparate laws and regulations, including those related to personal data protection. In addition, the company needs to secure data related to product designs and other confidential, sensitive company documents. EndoChoice needed a disk encryption solution that would meet or exceed data privacy regulation requirements; allow centralized command and control of encryption beyond geographic boundaries; and complement and match the company's phenomenal growth.

Challenge: Data Privacy and Security Compliance, Managing International Growth

EndoChoice knows the importance of protecting data on laptop computers. As a medtech company, it is subject to some of the most strenuous and aggressively enforced data privacy laws that govern commercial interests in the US, Europe, and beyond. In addition, the company needs to protect proprietary information that allows it to be at the forefront of their industry: in 2013, *Inc. Magazine®* recognized EndoChoice as one of the fastest growing companies in America, for the fourth year in a row.

This phenomenal growth, however, brought its own challenges, as the IT leadership realized that their approach to deploying and managing data security needed to keep pace with the Company's extraordinary growth. EndoChoice needed a solution that offered the following, among other features:

- **FIPS 140-2 Validation**: Solutions that comply with NIST (National Institute of Standards and Technology) requirements are recognized as providing respectable levels of security under most data privacy laws and regulations.
- **Proof of Compliance**: The ability to provide documented proof of encryption is as important as the act of encrypting devices with sensitive data, especially if Safe Harbor provisions are present.
- **Easy and fast setup across the world**: Solutions that require months of pre-planning, followed by months of implementation, is not an option for a dynamic, growing company like EndoChoice.
- **Flexibility**: As a growing international company, EndoChoice needed a solution that was easily scalable, has a global reach, and frees up as much of its resources as possible so that these can go towards maintaining the company's momentum.

Solution: Web-Based Data Security Solution Deployment for Mobile Endpoints and their Management

AlertBoot, a provider of cloud-based mobile device management (MDM) and full disk encryption (FDE) was an excellent match for EndoChoice. Its massively scalable and easy-to-deploy solution is centrally managed through a secure enterprise-grade web-based console, and offers mobile device management, mobile antivirus, remote wipe and lock, device auditing, and hard disk encryption with integrated customizable reporting.

Benefits: Cloud-based Central-Management of NIST-Validated FDE Saves Resources

Benefit #1 FIPS 140-2 Core Validated By NIST

The FDE core used by AlertBoot is ***validated*** by NIST; that is, it has been reviewed by NIST and granted a certificate, proving it satisfies FIPS 140-2 requirements. Solutions that claim ***FIPS 140-2 compliance***, on the other hand, may mean that the solution provider has followed NIST guidelines without actually having it verified. It is not unusual to find at a later date that "FIPS-compliant" solutions are rejected by NIST[1] due to incorrect implementation.

In addition, security best practices expected under NIST guidelines – such as backing up encryption keys and storing them safely; managing them so that they're correctly paired up with the correct machines; centralizing the installation on endpoints; and establishing and enforcing authentication like multiple IDs on the same endpoint – are also built into AlertBoot.

Benefit #2 Cloud-Based Management: Global Outreach, Proof of Compliance

AlertBoot leverages the internet to encrypt endpoint devices, so EndoChoice is able to deploy and manage devices remotely, even if the endpoint is in another continent, while keeping everything centralized. AlertBoot's reporting engine, an integral part of the solution and factored in during the preliminary design stages of the service, not only provides conclusive proof of a device's encryption status, it has been successfully used to prove compliance with encryption requirements to regulators.

Benefit #3 Saves Resources: Lowest Total Cost, IT Dept Time Freed Up

AlertBoot's cloud-based management has other benefits as well. First, the cost of installing and managing FDE becomes transparent to decision-makers because hidden costs are non-existent – such as the deployment of management servers, the licenses required to run such servers, and securing the data center space.

Second, the cloud frees IT personnel. Instead of researching and bargaining with data center providers or dealing with the required regular maintenance issues of operating a server, the AlertBoot cloud already takes care of such expenditures. Not having to support private infrastructure not only saves money but also saves less tangible resources.

Third, the ability to add only as many licenses as necessary frees up resources that could be tied up as "shelf-ware," software that just sits on a shelf because they were purchased as part of fulfilling the vendor's quota.

About AlertBoot

AlertBoot offers a cloud-based data and mobile device security service for companies of any size who want a scalable and easy-to-deploy solution. Centrally managed through a secure web based console, AlertBoot offers mobile device management, mobile antivirus, remote wipe & lock, device auditing, USB drive and hard disk encryption managed services.

EndoChoice®, Inc. Magazine®, and other product or service names mentioned herein are the trademarks of their respective owners in the United States and/or other countries.

[1] http://www.phiprivacy.net/dentrix-claims-it-encrypts-their-data-but-does-it/