Phoenix Enterprises

Empowering and Protecting a Non-Profit Social Enterprise

Phoenix Enterprises (Swindon) Ltd. is a not-for-profit social enterprise based in Rotherham, United Kingdom. Charged with the mission "to increase employability and overcome social exclusion," a devoted team of specialists aid unemployed people get back to work. Since 1998, Phoenix has helped over 37,000 people to participate in their communities. In 2013, Phoenix helped someone back into work every two and a half hours of every working day.

Employees at Phoenix use computers in the workplace and, due to the nature of their operations, personal information is stored in these devices. Full disk encryption (FDE) is used on their machines to ensure data privacy and to meet information security standards like the UK Data Protection Act (DPA).

The Challenge: Meet ICT Security Regulations

The Information Commissioner's Office (ICO), responsible for enforcing the DPA mandate, started delivering heavy penalties for data breaches starting December 2011. The ICO has continually emphasized the importance of encryption wherever sensitive personal data is stored in digital format, especially on portable data devices like laptops and external hard disk drives.

In order to avoid data exposure to unauthorized third parties, Phoenix has to comply with strict information and communication technology (ICT) security regulations, such as encrypting the hard-drives of all PCs and laptops. While there are many facets to said regulations, data protection for computers demands that an officially FIPS 140-2 validated encryption solution be used to secure digital information.

Recognizing the potential risk of not following such guidelines, Phoenix searched for a solution that would meet recommended best practices while making life easier for its IT personnel.

An Extra Challenge: Small IT Staff and Mobile Devices

In addition to regulations, there are certain private challenges that Phoenix has to meet. Unlike most SMEs who outsource their IT needs, Phoenix has a small but dedicated in-house staff that support the multiple Phoenix offices, requiring trips from one location to another as problems arise or upgrades are needed.

It is not uncommon to see IT issues arise at different locations at the same time. The outfit has to deal with many IT issues, and any solution that makes their life easier and makes them more efficient is not only welcome but critical. The ability to remotely install and manage the FDE solution would be handy as well.

In addition, Phoenix is introducing devices like smart phones into the workplace. It would be ideal to incorporate a solution that can protect traditional work devices like laptops and modern ones like smart phones and tablets.

IN BRIEF

Industry

- Non-profit

Challenges

- FIPS 140-2 validated encryption
- Remote encryption management
- Easing small IT staff burden

Solution

- AlertBoot cloud-based mobile device management (MDM) and full disk encryption (FDE).

Benefits

- Ease of use
- 24/7 administrative support
- Low administrative overhead
- Web-based console allows management from anywhere, from any device connected to the internet
- Endpoint solution is deployable anywhere an internet connection is available

The Solution: AlertBoot Cloud-Based Endpoint Data Security and Management

After investigating the market for FDE solutions, Phoenix chose AlertBoot, which offers, in the form of a cloud-based service, mobile device management (MDM) for smart phones and tablets as well as laptop disk encryption. AlertBoot uses a NIST FIPS 140-2 certified technology at its core with a powerful AES-256 encryption algorithm, satisfying DPA requirements associated with laptop computer data security.

In addition, the cloud-based service means Phoenix's busy IT staff can eliminate the need to separately manage and monitor a central server – required if there is a need to keep logs for auditing purposes, or if one needs to deploy encryption and push policy updates – saving them time and headaches, and lowering cost associated with in-house hosted infrastructure models.

Additional Benefits: Growing Features and Cost Effective

While Phoenix chose AlertBoot because of its ease of use and the powerful cloud-based management system, there are a number of AlertBoot features that make it shine over the competition.

Extra features such as remote wipe and lock, device auditing, customized reports, password policy management, mobile antivirus, and external USB drive encryption come included to enhance the robustness of the AlertBoot security solution.

One single, unified console is used for the management of different device platforms, lowering the operational learning curve.

The solution is cost effective. Savings can be found not only in the increased efficiency of IT personnel but also in the decreased expenditures associated with server management (such as purchasing hardware; securing data center space, operating systems, and database software licenses; and routine maintenance), because the AlertBoot cloud replaces it. Downtime is also minimized thanks to AlertBoot's globally redundant nature.

Finally, endpoint protection licenses are purchased on an as-needed basis. No longer does a company have to purchase more than necessary just to fulfill the sellers' quota, leaving shelved licenses collecting virtual dust. Unnecessary impacts to the bottom line are eliminated, allowing resources to be diverted where they are most needed.

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.