

Myscience.co Limited

Safeguarding A Company's Dispersed Workforce On The Move

Myscience.co Limited was established in 2004 by the White Rose University Consortium, (comprising the Universities of Leeds, Sheffield, and York), and Sheffield Hallam University. Myscience operates the National Science Learning Centre as a centre of excellence for science teachers' continuing professional development and the National STEM Centre (Science, Technology, Engineering, and Maths) which brings together key national organisations working within the STEM communities, and are co-located at the University of York.

The company's activities have expanded to include the operation of the full network of Science Learning Centres which are situated within each of the government's regional areas, as well as a wide range of national and international projects in the field of STEM education. The organisation installed full disk encryption (FDE) on all of their laptops to ensure data privacy and to adhere to compliance standards like the United Kingdom's Data Protection Act (DPA).

Challenge: Secure Laptops, Prevent Data Breaches

It is Myscience policy that employees do not hold sensitive data on their laptops. However, it was imperative that Myscience have encryption in place as a backup to prevent potential data breaches. Because all employees are provided with laptops, it is important that devices feature proper data protection, just in case devices are lost or stolen while Myscience carries out its mission.

The security solution's impact on operations, which can affect both IT staff and endpoint users, was also of significance to Myscience. A traditional, centralised encryption solution requires the procurement and installation of management servers, deployment planning and scheduling, and supporting users during and after installation.

Endpoint users may also be adversely impacted by the installation of encryption on their computers. They may have to wait for the computer to finish installation before using it, and during normal use may be locked out of the computer. For example, they may have problems remembering the password.

Extra Challenge: UK & European Privacy Laws

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

Recognising the potential risk, Myscience searched for a solution that would meet recommended best practices.

IN BRIEF

Industry

- Education

Challenges

- Minimal impact to IT staff
- Fair price / budget constraints

Solution

- AlertBoot cloud-based mobile device management and disk encryption

Benefits

- 24/7 support
- Low administrative overhead
- Web-based console allows management from anywhere
- Solution deployable anywhere an internet connection is available



Solution: Cloud-Based Data Security and Management of Endpoints

AlertBoot cloud-based mobile device management and disk encryption was an excellent match. This massively scalable and easy-to-deploy solution is centrally managed through a secure enterprise-grade web-based console, and not only offers disk encryption for laptop computers that has integrated customizable reporting, but also mobile device management, mobile antivirus, remote wipe and lock, device auditing, USB drive, and hard disk encryption.

The solution is also available for deployment to private clouds.

Benefits: Easy Central Management, Scalability, All-In-One Solution

"A big reason for using AlertBoot was that it didn't require us to support it with our own infrastructure," said Alan Oakden, User Services Assistant at Myscience. "Other pros and cons would have been to do with ease of use and the effect on the user. Both would have had to be of minimal impact."

A cloud-based security solution like AlertBoot leads to minimal impact on operations. First, IT staff are not burdened because the setup and maintenance of extraneous hardware like management servers is absent from the beginning. Due to AlertBoot's hosted nature, Myscience is able to obtain and deploy encryption licences by logging into their account and *purchasing them when needed*. This budgetary flexibility is an additional benefit in the hosted model as upfront licence purchases are not required.

Second, AlertBoot leverages the internet to encrypt endpoint devices, allowing the remote deployment and management of devices. This is beneficial when considering the mobile nature of Myscience employees: the organisation has approximately 90 employees at the centre, all of whom have encrypted Laptops. Choosing AlertBoot spares Myscience from multiple issues associated with handling future growth.

Finally, AlertBoot proved to be very easy to use: an automated installer, sent via email to the end user, is essentially all it takes to install encryption on a laptop computer. The solution's integration with the cloud-based management console ensures that all devices are tracked to show installation and operational status.

But the benefits of choosing AlertBoot do not end there. AlertBoot not only offers FDE for laptops but an entire range of mobile security solutions that extend to smartphones and tablets, which are making inroads into the workplace in the form of BYOD (bring your own device) or COPE (corporate owned, personally enabled) programs.

Myscience, in addition to laptop computers, has also begun to adopt these smaller devices as part of their workflow, and, if Myscience chooses to do so, it will be able to further extend security to all mobile devices with the same level of security, convenience, and responsiveness it has come to expect from AlertBoot.

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.