

Ignis Case study

Background

Ignis Asset Management is a dynamic, privately owned investment management company with offices in Glasgow and London. This ambitious firm manages around £65 billion† on behalf of a large client base of UK and overseas retail and institutional investors.

Ignis has grown into a market-leading organisation providing investment services to individuals and institutions across a wide spectrum of sectors. Fostering an entrepreneurial approach, Ignis has a multi-boutique structure, consisting of four proprietary teams and four joint venture partnerships. This allows the business to have a diverse investment capability across key asset classes.

Challenge

More than ever before, companies offering financial services expertise are impacted by increasingly stringent regulation and legislation of data security as imposed by the industry regulator, the Financial Services Authority (FSA). The FSA's primary role is to promote efficient, orderly and fair financial markets. But it is also required to ensure that financial institutions meet their statutory obligations regarding consumer protection and crime prevention.

There has been a long list of high profile breaches of IT security in public and private organisations in recent years. As a result of this, one particular area that the FSA are keen to improve is the storage and transportation of sensitive data.

Bruce Paterson, IT Manager, at Ignis Asset Management recognised that the company would have to adopt certain technology in order for the company to be totally compliant. "An audit from the FSA reinforced our belief that our IT department should know exactly who is using, or accessing, what device at any given time. We had an endpoint security policy in place, but we realised that in order to effectively support our staff in all locations, we needed something more robust."

Originally, there were basic security barriers in place to stop people bringing in USB sticks. Considering the amount of USB devices and smartphones that were in operation among the Ignis employees, it became necessary to re-evaluate our precautionary measures that could be adopted to better protect the company's endpoints, which could be vulnerable to data theft and virus infiltration through the uncontrolled use of removable storage devices. With this in mind, Ignis decided to implement an endpoint security system that could offer straightforward functionality at a competitive cost.

Bruce Paterson says, "With a tighter regulatory environment, coupled with the fact that managing the use, or misuse, of removable devices was becoming very time consuming we decided that it was essential for us to further develop our IT security barrier."

Solution

After evaluating the various alternative solutions available on the market, Ignis chose DeviceLock endpoint security as it could provide the level of security the company were looking for at the right price.

Bruce explains the decision, "DeviceLock was the ideal product for us. I was primarily looking for a solution that required minimal supervision, allowing me to focus on managing our IT estate and supporting our asset managers. DeviceLock was simple to roll out and it was very competitive on cost. We have just renewed our contract and price is naturally an increasingly important consideration in the current environment. Until we purchased DeviceLock, our policy was to disable USB totally. With the advent of newer PCs with only USB mice and keyboards, this was clearly not a sustainable situation."

Ignis adopted DeviceLock to cover 500 of their employees. DeviceLock has placed Ignis in a better position to enforce its security policies, and allows it to perform audits of activity at end-user computer ports and peripheral devices including Windows Mobile® and Palm® -based personal mobile devices, as well as any type of local, network and virtual printers.

The Ignis IT department is now able to log and shadow-copy any uploaded or downloaded data and define a DeviceLock "approved list" of USB devices, ensuring user

access to specific devices regardless of any other restrictions that would otherwise be imposed based on device class or model.

“You want to be secure in the knowledge that your endpoints are protected and that it gets on with the job without excessive management,” explains Bruce. “The recent addition of a dynamic email delivery of event and shadow log reports is very useful as well.”

Benefits

Paterson believes that the implementation of DeviceLock has brought about a significant and positive change to the business. “From a financial services perspective, knowing that we are compliant with the FSA’s data security regulations is obviously very important. As an IT manager, I am certainly more aware of the amount of USB devices that are in operation in our business. Naturally, this opens up some serious security concerns. But, whereas in the past we had a blanket ban on USB devices, we can now be more flexible without compromising security, because of the DeviceLock software,” concludes Paterson.

- Ends -

†Source: Internal, Ignis and Axial total assets under management at 31 Mar 09.