

Case Study

DeviceLock® secures lighting specialist Weblight

Established in 1993, Weblight is one of the leading providers of lighting maintenance solutions. Currently employing over 135 people nationwide with a turnover in excess of £12m it is a large company with a rich and wide spread client base that includes the likes of Marks and Spencer and Somerfield.

With a large remote workforce the senior management at Weblight were keen to implement a system that would help to protect their IT systems from unforeseen circumstances. “We were concerned that unauthorised devices could be connected to the IT Systems (especially our laptops) allowing confidential information to be lost or stolen. Our sales team work right across the country, so the concern was that confidential customer and company information could be at risk,” said Matthew Cole, IT Systems Administrator at Weblight.

As well as the issue of theft, the IT department also had to take into account the fact that viruses, spyware and other similar malware programmes can easily be transmitted via the large amount of USB devices in use. USB memory sticks, mobile phones and PDAs are the tools of the trade for most remote workers so the company needed to know what devices their staff were using. “Every staff member filled out a request form so that we could allow them access for their specific devices. This meant that we knew what devices were being used on our hardware, which gave us much more control,” explained Matthew.

Staff certainly had to get used to the new software, “Naturally, sales staff get given USB memory sticks from customers, and this can be a risk to our systems. Once we explained to them why we needed to control this, they were much more understanding and willing to support the roll-out.”

Weblight looked at a selection of end-point security solutions and decided that DeviceLock's software was the most suitable technology for their business needs and provided the best value for money.

DeviceLock is a flexible, policy-based endpoint security solution that enables network administrators to centrally control uploading and downloading activity through local computer devices. With DeviceLock, Weblight is now able to lock out un-authorized users from USB and FireWire devices, WiFi and Bluetooth adapters, PDAs and many other plug-and-play devices.

Weblight deployed the software across all company Servers, PC's and Laptops but did not activate it initially, choosing to allow staff to get familiar with the technology on their desktops before going live.

The benefits of the system have shone through since implementation, according to Matthew; "We are still finding out very useful functions of DeviceLock, for example adding specific devices to the USB database is very valuable to us. You can also do a remote install without the user being involved, which saves huge amounts of time as it doesn't require us to visit each PC, or reboot, which again is very efficient."

Weblight has also taken advantage of the management console that enables PCs to be managed individually, or in groups. The user-friendly nature of the software means that IT managers can choose to integrate it with Microsoft's Active Directory, allowing them to work with groups of PCs rather than one at a time.

Ultimately, DeviceLock gives the company more control over the devices that their staff uses on their IT systems, significantly reducing the risks of data leaks and the uncontrolled use of locally connected devices. "We have approx 70 users across 5 different sites, from Livingston to Bristol, many working remotely, so the ability to access and control all our hardware remotely is very important," says Matthew.