

## *Is your data walking out the door??*



What data is valuable to a company? While some people may say emails, contacts and pricing, often it's not that simple. For an engineering firm it may be CAD drawings, for a marketing company it may be their CRM and for you it might be your latest upgrade proposals or an RFP you have been working on for several months. One solution is to encrypt any shared file partitions but you still need to give access to your employees and that's when data can literally walk out the door.

According to the data protection, 59% of people who lost their job admitted to taking confidential company information with them either on DVD or using USB drives. The proliferation of consumer devices such as iPods, USB devices, Smart Phones and more, has dramatically increased the risk of intentional and unintentional data leaks and other malicious activity. While most companies have anti-virus software, firewalls, email and web content security to protect against external threats, few realize how easy it is for an employee to simply walk in and copy large amounts of sensitive data onto an iPod or USB stick.

Of course your administrator could lock down all ports, an ill-advised, difficult and unsustainable solution. The only really effective solution to counter portable device threats is by deploying a software solution that protects the corporate network perimeter against unauthorized device usage – a solution that allows you to discriminate between legitimate and illegitimate use of devices, in compliance with the custom security policies set up by the company.

Controlling access, can be as simple as installing a small footprint agent on a user's machine. This agent is only 1.2 MB in size and a user will never know it is there. After installation, the agent queries Active Directory when the user logs on and sets permissions to the different nodes accordingly. If the user is not a member of a group that allows access to a particular device or set of devices, then access is blocked.



You can:

- **Manage User Access and Protect Your Network From Portable Devices:** You can centrally disable access to any portable device, preventing both data theft and the introduction of data or software that could be harmful to your network.

- **Real-time Status Monitoring and Alerts:** Alerts can be sent to one or more recipients by email, network messages, and SMS notifications sent through an email-to-SMS gateway or service when specific devices are connected to the network



- **Blocking by file type:** File security policies can be defined by file type. For example allow the user to read \*.doc files but block access to all \*.exe files.
- **Blocking at physical port level:** Devices can be blocked by the physical port on which they are connected, for example USB, Firewire, Bluetooth, Infrared, Wi-Fi, PCMCIA, Parallel, Serial, S-ATA, SD.



- **Blocking by device serial number:** Besides being able to set permission for a whole device class, it is now also possible to set permission for a single device based on the unique device Hardware ID.

- **Device white list and blacklist:** The administrator can define a list of particular devices which are allowed and others which are permanently banned. For example an administrator might want to allow only company-owned USB drives to be used on the network, whilst banning all other devices.



- **Permit Temporary Device Access:** Temporary access can be granted to users for a device (or group of devices) on a particular computer for a particular timeframe.
- **Log the Activity of Portable Device Access to your Network:** USB sticks present a significant threat to your business environment. They are small, easily hidden and can store up to 4 GB of data. Even plugging a digital camera into a USB port gives users access to storage on an SD card; SD cards are available in 2 GB capacity and more. A list of files that have been accessed on a given device is recorded every time an allowed user plugs in.



- **Detailed Reports on Device Usage:** A powerful reporting package can be scheduled to automatically generate graphical IT-level or higher level management reports based on data collected, giving you the ability to report on devices connected to the network, user activity, endpoint files copied to and from devices (including actual names of files copied).
- **Custom messages:** When users are blocked from using devices, they can be shown custom popup messages explaining the reasons why the device was blocked.

To find out more and to have a trial installed, don't hesitate to contact our sales team on [sales@lantech.co.nz](mailto:sales@lantech.co.nz) or phone 04 494 9670