

# Case Study | Endpoint Encryption & Remote Data Wipe | Mobile Data Security

## The Challenge

With the emergence of mobile computing, the risk of loss or theft of sensitive data is as high as ever. This risk is widely recognised with Central Government, the Criminal Justice Secure Email system, Treasury Solicitors and the NHSLA all making stringent data security demands of its users. The requirements for laptop encryption and mobile data security must now be taken as seriously as any other part of a Solicitors' or Chambers' network.

## The Solution

Sprout's layered and complementary solution is refreshingly simple. There is almost zero end user interaction and no additional passwords to remember. Even so, the solution meets the strict FIPS-2 compliance requirement (that the widely used 'Truecrypt' product does not), is centrally managed and highly scalable.

- In order to secure the data on a mobile computer, the entire drive is encrypted. To access the machine, a user must log in – this authentication takes place before the traditional Windows login (pre-boot) and requires just one password entry for the entire logon process. If the computer is lost or stolen, there is simply no way to access the data without the password. Even removing the computer's hard drive and installing in a new machine will not allow access.
- If your computer and its sensitive data is lost or stolen, you now have the option to remotely wipe the entire machine. Remotely delete sensitive data on missing computers and produce an audit log of the deleted files to prove compliance with Government and corporate regulations. Device Freeze allows you to freeze a computer and display a custom message to the user instructing them to comply with specific requests for action (return for servicing, validate user identity, etc.).
- Remote File Retrieval allows you to obtain files from a device even if it is not within your control.
- Encrypt USB devices and CDs to the same level of compliance, quickly and easily.



sprout **IT**  
Legal IT Specialists

# The Results

## Protection

- In the event of loss or theft, remotely delete all sensitive information and generate reports to prove your compliance with Government and corporate regulations
- Use internationally recognised encryption standards for full hard-disk encryption
- Prevent unauthorised users from reading lost or stolen media

## Recovery

- Report a theft and engage our Theft Recovery Team who will work with local law enforcement to recover your property
- Send a 'freeze' command to a lost/stolen device rendering it useless, with just an on screen message to encourage its return

## Simplicity

- Convenient and secure with single sign-on (SSO) — there's just one password for users to remember for encryption and their OS
- Allows multiple users to share encrypted computers without sharing their passwords
- Encrypts data in the background so that protection doesn't interrupt your users' work

**“ For peace of mind and regulatory compliance, use Sprout’s full disk encryption and remote track and wipe products. Easy to use, highly secure, inexpensive and completely scalable.”**

**Matt Torrens**  
Director - SproutIT



## Contact Us

**Call Matt Torrens or Danny Killeen**

**020 7036 8530**

**[www.sproutit.co.uk](http://www.sproutit.co.uk)**

**[info@sproutit.co.uk](mailto:info@sproutit.co.uk)**

**Quadrant House,**

**10 Fleet Street, London, EC4Y 1AU**