

How to Make ‘Mission Impossible’ Memory Sticks a Reality

Latest webinar from Network Defence demonstrates how new Secured eUSB enables businesses to manage flash drive security, helping prevent data leaks by remotely wiping data from lost and stolen USBs

25 June, 2010 – Leading IT and data security specialists Network Defence is making ‘Mission Impossible’ memory sticks, where the data on the device can be destroyed remotely, a reality for businesses.

Network Defence demonstrates in its latest webinar how new Secured eUSB allows businesses to manage flash drive security, letting them instantly wipe data from lost and stolen USBs, preventing damaging data loss and leaks.

Recent studies show that lost or stolen USB sticks are the most common method of data loss. Of the 1007 security breaches reported to the Information Commissioner’s Office in the last three years, 740 were due to lost or stolen hardware. It is estimated that over half of these devices were USB sticks. Secured eUSB software, developed by Cryptzone, helps protect intellectual property, sensitive and confidential information by enabling IT administrators to remotely send a “kill pill” to any lost or stolen USB flash drive which is connected to the server, instantly erasing any data.

It also makes it possible for management to roll out security policies for all USB flash drives in the organisation, providing a comprehensive level of protection against threats.

Dave Beesley, Managing Director for Network Defence, said: “Portable storage devices such as USB flash drives are increasingly popular in most enterprise environments as they are convenient and enhance productivity. But they present new security risks as they can be easily lost or stolen and the data stored on them may be sensitive and confidential.

“Our latest webinar provides businesses with a simple and easy, though best-in-class approach to USB security. It gives an overview of how new Secured eUSB empowers IT administrators by providing them the tools to manage the security of portable storage devices; tracking data content stored on these devices, user access control and enforcing end point encryption. The unique new software with its data ‘self destruct’ feature, really does make ‘Mission Impossible’ possible for business!”

Among other topics, Network Defence explored Active Directory integration, management of user rights and authentication methods, and automatic controls to lock out access of lost USB flash drives. Included in the discussion was a live demonstration of the end user application as well as the SEP Enterprise manager.

To see the webinar please visit:

<https://www1.gotomeeting.com/register/113293296>

Ends/

Press contact

Priya Mistry
Context Public Relations
01625 511 966
www.contextpr.co.uk

About Network Defence

Based in the North West, Network Defence is a leading IT and Data security consultancy that works with a range of companies in different markets to improve overall IT security and business efficiency saving time and money.
www.networkdefence.com