

## BACKGROUND FOR SECURITY

The overall IT infrastructure of an organization, in the majority of cases, involves an expansive enterprise network connecting computer resources at headquarters with those of individuals from smaller companies, partners and independently owned agencies who access data by dialing in from outside a firewall via a PC, laptop, PDA or smartphone. This can result in security gaps through which all of the organization's data becomes vulnerable. The data stored on equipment, and the access the equipment provides to servers at headquarters, is far more valuable than the equipment itself.

Viruses, worms, hackers and other security threats are becoming more sophisticated and more frequent. Attacks aimed at theft of customer records and other core business data are on the rise, according to a recent study by Network Associates, and damages resulting from the theft of data are costly. The best estimate of the impact of security breaches on a single organization can be found in the 2004 CSI-FBI survey of over almost 500 organizations. They concluded that the average cost impact of security breaches on each organization is over \$526,000 per year.

Combine a malicious attack with the distributed environment of the typical company and the results could be devastating. A security breach can result in:

- Loss of customer confidence
- Loss of shareholder confidence
- Liability claims
- Extortion
- Errors and omissions litigation
- Network security failures
- Loss of property
- Business interruption

## DATA SECURITY NO LONGER OPTIONAL: LEGISLATION DEMANDS

It is incumbent upon IT management to respond to today's higher expectations for security by developing policies, procedures, and action plans that are easily implemented within their existing organizational structures. The key is to find a means of guaranteeing that encryption and access control have been implemented on each and every machine as well as having evidence that security has been provided on each and every machine.

### SAFEBOOT: VENDOR-OF-CHOICE FOR LAPTOP ENCRYPTION

SafeBoot designs, develops, supports, and markets leading-edge mobile data security solutions for mobile devices and network systems. In use at nearly 170 Fortune® 500 companies, SafeBoot® is the vendor-of-choice for mobile data security solutions that protect data, devices and networks against the risks associated with loss, theft, and unauthorized access, anytime and anywhere. SafeBoot solutions offer powerful encryption and strong access control technologies that seamlessly integrate with existing enterprise systems. SafeBoot's centralized management capabilities provide enterprises of all sizes with operational efficiency and ensure the lowest possible total cost of ownership. Founded in 1991, SafeBoot operates in the U.S., The Netherlands, United Kingdom, Sweden, France, Germany, Brazil, Belgium, and Australia — and hosts a worldwide network of more than 50 certified distributors. SafeBoot is privately held and consistently demonstrates growth and profitability.

## THE SOLUTION: SAFEBOOT FOR DEVICE ENCRYPTION

SafeBoot<sup>®</sup> is a PC security system which prevents any data stored on a PC, Tablet, Palm, Pocket PC or any other portable device's hard disk from being read or used by an unauthorized person. With SafeBoot, users must identify themselves each time the device or PC is booted. If users fail to identify themselves, or if an unauthorized person attempts to use the PC, SafeBoot prevents access to both the machine and the data stored on it.

To gain access to a SafeBoot-protected PC, users must "boot" the PC and enter their user ID, password and/or token such as a smart card or USB key at a pre-operating system logon screen (pre-boot-authentication, or PBA). Only when SafeBoot has verified that the details presented are correct, is a user granted access to the PC and the data stored on it.

## SAFEBOOT PRINCIPLES & BENEFITS

- Lowest Possible Total Cost of Ownership
- Highest Return on Investment
- Quality Assurance
- High Level Support
- One Central Solution
- One Identity
- Seamless Integration into Enterprise Systems
- Mandatory & Enforcable Security Policies
- Transparent to the User
- Fail-Safe Recovery
- Extensive Audits

## HOW DOES SAFEBOOT WORK?

SafeBoot Device Encryption works by encrypting the data stored on a PC, PDA or any other portable device. Encryption is a process whereby information is 'scrambled' using a mathematical function (the encryption algorithm) and a numerical value known as the encryption key. SafeBoot encrypts the information stored on the PC's hard disk using a unique encryption key generated when SafeBoot is installed. No more or less data is generated, but the result is different from the source, and is unintelligible.

Once SafeBoot has been installed, there is no noticeable difference in the operation of a PC, other than the user having to identify themselves at 'log on' before the operating system starts. The encryption and decryption of data happens both automatically and transparently. All data on the hard disk is protected, including temporary and swap files, and "sector slack". As data is read from the disk, it is decrypted into memory; conversely as data is written, it is encrypted in memory before being written to the disk itself. This simple process ensures that all the data on the disk is encrypted consistently: there is never a moment where plain data is exposed on the hard disk.

If an unauthorized person attempts to retrieve data from the PC, that person will find that the data stored on the hard drive is unintelligible. To the casual "hacker," the hard drive will appear to be blank, but to the more persistent, they will find the hard disk is totally encrypted; even the filenames are unintelligible.

Administration of SafeBoot is extremely easy. Each time a protected machine boots, it attempts to access a central configuration database where it synchronizes its local configuration with that which is specified in the database. This transfer occurs over an encrypted TCP/IP network link with no reliance on any special network shares or user permissions. Only specially privileged administrators are able to make changes in the central configuration repository.