



SafeBoot® Device Encryption™

Security Solutions for PC, Laptop, and Tablet PC

THE PROTECTION OF DATA ASSETS IS A PRIMARY ISSUE FACING TODAY'S ORGANIZATIONS. SAFEBOOT® DEVICE ENCRYPTION™ IS A SCALABLE, ENTERPRISE-WIDE SECURITY SOLUTION THAT USES STRONG ACCESS CONTROL AND POWERFUL ENCRYPTION TO PREVENT UNAUTHORIZED ACCESS TO OR USE OF PCs, LAPTOPS, AND TABLET PCs, AS WELL AS DATA ON THEIR HARD DISK STORAGE DEVICES.

In today's organizations, mission-critical data travels freely across networked environments and the Internet, and it is stored and accessed on PCs, laptops, tablet PCs, a variety of mobile devices, and even removable storage devices such as discs. SafeBoot Device Encryption for PCs, laptops, and tablet PCs uses strong access control, and pre-boot protection to authenticate users, and it supports Single Sign-On (SSO). It uses algorithms such as RC5-1024 and AES-256 to encrypt data on all storage drives. Encryption and decryption are transparent to the user and performed on the fly, with virtually no performance loss.

In addition to industry-leading, award-winning authentication and encryption technologies, SafeBoot Device Encryption for PCs, laptops, and tablet PCs offers, central management capabilities, extensive mandatory security policies, and secure recovery.

STRONG ACCESS CONTROL, PRE-BOOT PROTECTION AND CERTIFICATE INTEGRATION

The SafeBoot Device Encryption solution offers secure hibernation and authenticates both users and machines prior to the system ever booting (it also offers pre-boot event logging). In addition to password authentication, SafeBoot Device Encryption supports two-factor pre-boot authentication (F2-PBA), which requires users to both "know something" and "have something" before PCs, laptops, and tablet PCs are allowed to start. SafeBoot Device Encryption also offers multiple options for two-factor security, including numerous Smart Cards and USB token technology. SafeBoot Device Encryption supports authentication via PKI certificates and provides access to SafeBoot and the machine's PKI infrastructure.

CENTRAL MANAGEMENT CAPABILITIES FOR LOWER TCO

Via SafeBoot Management Center, SafeBoot Device Encryption offers administrators a unique, powerful, and cost-effective method of maintaining enterprise security. Central management capabilities include central deployment, remote upgrades, policy management, a scripting tool, hot revocation, audit facilities, secure centralized recovery, and policy synchronization with Active Directory, Novell, PKI, and others. These capabilities enable today's businesses to increase ROI and lower TCO.

EXTENSIVE MANDATORY SECURITY

SafeBoot Device Encryption's central management system provides an administrator with the tools to easily set and enforce extensive mandatory security policies. Users have no control over the SafeBoot security policies, because these policies are transparently enforced. Also, administrators will find great ease-of-use in setting mandatory security policies for users.

SECURE RECOVERY

If a user forgets a password, loses a token, or leaves the organization, SafeBoot Device Encryption's tools safely recover the protected systems, without using an unsafe master password as a "backdoor." Password and token recovery is only a phone call or a Web page away. The Web-based, SafeBoot® WebHelpdesk recovery tool permits the Helpdesk to reset user passwords remotely after the user successfully passes a verbal challenge & response verification and authentication with the administrator Helpdesk via telephone.



BENEFITS OF SAFEBOOT DEVICE ENCRYPTION

SafeBoot Device Encryption for PCs, laptops, and tablet PCs offers users and organizations the following features and benefits:

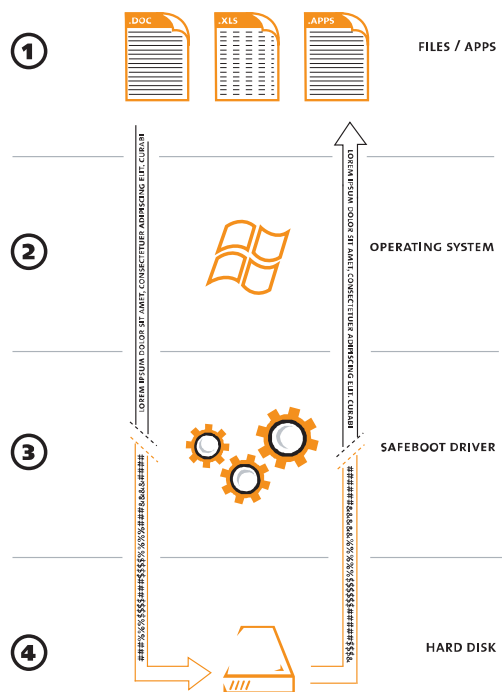
- Protects PCs, laptops, tablet PCs against unauthorized access
- Offers full encryption of data on hard disks
- Eliminates the need for hard drive shredding
- Helps achieve compliance with legislation (i.e. Sarbanes-Oxley, HIPAA, etc.)
- Helps enforce mandatory, company-wide security policies
- Offers boot protection, pre-boot authentication, pre-boot event logging, and protects against master boot viruses
- Encrypts data on-the-fly and is transparent, requiring no end-user training
- Supports Single Sign-On (SSO) and all popular Smart Cards and tokens
- Supports all common languages, keyboards, and Windows® OSs
- Uses multiple standardized algorithms such as RC5-1024 and AES-256

- Offers easy centralized management for administration, deployment, upgrades, auditing, hot-revocation, recovery, synchronization, and more
- Offers a worldwide support network including 24/7 support

In addition to all SafeBoot Device Encryption features available for PCs, users of tablet PCs can authenticate during pre-boot using a stylus.

CERTIFIED, AWARD-WINNING TECHNOLOGY

With more than 2 million users, SafeBoot has the largest installed base of any device and data security solution. SafeBoot has achieved consecutive 4- or 5-star ratings from SC Magazine, as well as the SC Magazine 2004 Reader Trust Award for Best Encryption Product. SafeBoot holds several certifications, including FIPS 140-2 - ensuring that SafeBoot solutions employ true strong encryption and secure key management. The solution is widely used by organizations worldwide, including banks, insurance companies, consultancy firms, governmental bodies, and health care organizations.



HOW SAFEBOOT WORKS

- ① Files are in plain text and fully viewable by the authorized user(s) and application(s)
- ② Files are translated into sectors. Sectors are assembled into files.
- ③ Sectors are encrypted in memory. Encrypted sectors are decrypted in memory.
- ④ Sectors are stored on the hard disk. Sectors are read from the hard disk.