



# SafeBoot® Device Encryption™

## Soluções de segurança para PCs, laptops e tablet PCs

A PROTEÇÃO DO PATRIMÔNIO DE DADOS É UM DOS PRINCIPAIS DESAFIOS ENFRENTADOS PELAS EMPRESAS NOS DIAS DE HOJE. O SAFEBOOT® DEVICE ENCRYPTION™ É UMA SOLUÇÃO DE SEGURANÇA QUE ENVOLVE TODA A EMPRESA E USA CONTROLE DE ACESSO REFORÇADO E CRIPTOGRAFIA ROBUSTA PARA IMPEDIR A UTILIZAÇÃO E O ACESSO NÃO-AUTORIZADO A PCs, LAPTOPS E TABLET PCs, ASSIM COMO A DADOS EXISTENTES NOS DISPOSITIVOS DE ARMAZENAMENTO DE SEUS DISCOS RÍGIDOS.

Nas empresas de hoje, dados críticos trafegam livremente em ambientes de rede e na Internet, e são armazenados e acessados em PCs, laptops, tablet PCs, em diversos tipos de dispositivos móveis, e mesmo em dispositivos de armazenamento, como discos. O SafeBoot Device Encryption para PCs, laptops e tablet PCs usa controle de acesso reforçado e proteção pré-inicialização para autenticar usuários, e conta com suporte para logon único (SSO). Usa algoritmos como RC5-1024 e AES-256 para criptografar dados em todas as unidades de armazenamento. Os processos de criptografia e descriptografia são transparentes para o usuário e executados sem necessidade de interrupção dos trabalhos, praticamente sem perda de desempenho.

Além das premiadas tecnologias de autenticação e criptografia líderes do mercado, o SafeBoot Device Encryption para PCs, laptops e tablet PCs oferece recursos de gerenciamento central, amplas diretivas de segurança compulsórias e recuperação segura.

### CONTROLE DE ACESSO REFORÇADO E INTEGRAÇÃO DE PROTEÇÃO E CERTIFICAÇÃO ANTES DA INICIALIZAÇÃO

A solução SafeBoot Device Encryption oferece hibernação segura e autentica tanto usuários quanto computadores antes da inicialização do sistema (também oferece log de eventos anteriores à inicialização). Além da autenticação da senha, o SafeBoot Device Encryption é compatível com a autenticação de dois fatores antes da inicialização (F2-PBA), exigindo que os usuários "saibam alguma coisa" e "tenham alguma coisa" para poder inicializar PCs, laptops e tablet PCs. Também oferece várias opções de segurança de dois fatores, inclusive diversas tecnologias de token USB e Cartões Inteligentes. O SafeBoot Device Encryption é compatível com autenticação por certificados PKI (infra-estrutura de chave pública) e fornece acesso ao SafeBoot e à infra-estrutura PKI do computador.

### RECURSOS DE GERENCIAMENTO CENTRAL PARA REDUZIR O CUSTO TOTAL DE PROPRIEDADE

Usando o SafeBoot® Management Center™, o SafeBoot Device Encryption oferece aos administradores um método único, potente e econômico de manter a segurança da empresa. Entre os recursos de gerenciamento central destacam-se: implantação central, atualizações remotas, gerenciamento de diretivas, uma ferramenta de criação de scripts, revogação a quente, recursos de auditoria, recuperação central segura e sincronização de diretivas com Active Directory, Novell NDS, PKI e outros. Com essas funcionalidades, as empresas de hoje podem aumentar o retorno sobre o investimento e reduzir o custo total de propriedade.

### AMPLA SEGURANÇA COMPULSÓRIA

O sistema de gerenciamento central do SafeBoot Device Encryption oferece ao administrador as ferramentas necessárias para definir e aplicar diretivas de segurança compulsórias de modo simples. Os usuários não controlam as diretivas de segurança do SafeBoot porque a aplicação das diretivas é transparente. Além disso, os administradores terão grande facilidade em definir diretivas de segurança compulsórias para usuários.

### RECUPERAÇÃO SEGURA

Se um usuário esquecer a senha, perder um token ou sair da empresa, as ferramentas do SafeBoot Device Encryption recuperarão com segurança os sistemas protegidos, sem usar uma senha mestre pouco segura para contornar a situação. A recuperação de senhas e tokens pode ser feita por telefone ou em uma página da Web. A ferramenta de recuperação SafeBoot® WebHelpdesk, baseada na Web, permite que o suporte técnico redefina senhas de usuário remotamente, após o usuário ter sido verificado e autenticado pelo administrador, por telefone, por meio de uma pergunta verbal e da resposta correta.



## VANTAGENS DO SAFEBOOT DEVICE ENCRYPTION

O SafeBoot Device Encryption para PCs, laptops e tablet PCs oferece aos usuários e empresas os seguintes recursos e vantagens:

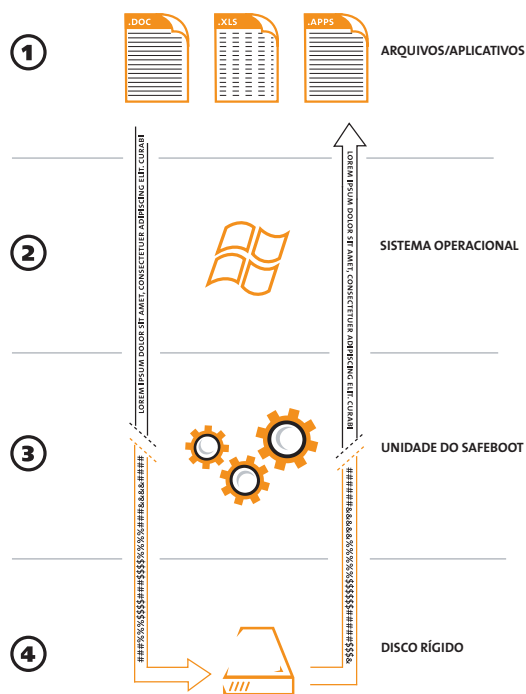
- Protege PCs, laptops e tablet PCs contra acesso não-autorizado.
- Oferece criptografia de dados integral em discos rígidos.
- Elimina a necessidade de divisão de discos rígidos.
- Ajuda a manter a conformidade com a legislação (por exemplo, Sarbanes-Oxley, HIPAA etc.).
- Ajuda a aplicar com êxito as diretivas de segurança globais da empresa.
- Oferece proteção de inicialização, autenticação e log de eventos anteriores à inicialização, e proteção contra vírus que afetam a inicialização mestre.
- Criptografa dados sem interromper os trabalhos e de modo transparente, sem necessidade de treinamento do usuário final.
- É compatível com SSO e todos os tokens e cartões inteligentes mais usados.
- É compatível com todos os idiomas, teclados e sistemas operacionais Windows® mais comuns.
- Usa vários algoritmos padronizados, como RC5-1024 e AES-256.

- Oferece gerenciamento central facilitado, para administração, implantação, atualizações, auditorias, revogação a quente, recuperação, sincronização e muito mais.
- Oferece uma rede de assistência internacional, inclusive suporte de 24 horas, 7 dias por semana.

Além de todos os recursos do SafeBoot Device Encryption disponíveis para PCs, os usuários de tablet PCs podem fazer a autenticação antes da inicialização usando um stylus.

## TECNOLOGIA CERTIFICADA E PREMIADA

Com mais de 2 milhões de usuários, a SafeBoot conta com a maior base instalada entre todas as soluções de segurança de dispositivos e dados. A SafeBoot obteve avaliações consecutivas de 4 ou 5 estrelas da SC Magazine, além do prêmio SC Magazine 2004 Reader Trust Award como Melhor Produto de Criptografia. Possui várias certificações, inclusive FIPS 140-2 - garantindo que as soluções SafeBoot de fato empregam criptografia reforçada e gerenciamento de chave seguro. A solução é amplamente usada por instituições do mundo inteiro, incluindo bancos, companhias de seguro, empresas de consultoria, agências governamentais e instituições de saúde.



## COMO FUNCIONA O SAFEBOOT

- 1 Os arquivos, em formato de texto simples, são totalmente visíveis para usuários e aplicativos autorizados.
- 2 Os arquivos são convertidos em setores. Os setores são reunidos em arquivos.
- 3 Os setores são criptografados na memória. Os setores são descriptografados na memória.
- 4 Os setores são armazenados no disco rígido. Os setores são lidos do disco rígido.