



SafeBoot Content Encryption

Proteja dados confidenciais com criptografia no nível de arquivos e pastas

AGORA EXISTE UM MODO DE MANTER OS DADOS CONFIDENCIAIS PROTEGIDOS SEMPRE QUE FOREM MOVIDOS NA EMPRESA E GRAVADOS EM QUALQUER OUTRO LUGAR. TOTALMENTE INTEGRADA COM O WINDOWS, A CRIPTOGRAFIA DE CONTEÚDO SAFEBOOT NÃO REQUER INTERVENÇÕES DO USUÁRIO FINAL E É COMPLETAMENTE TRANSPARENTE. OS ARQUIVOS CONFIDENCIAIS NÃO PODERÃO SER VISTOS MESMO PELA EQUIPE DE TI.

Com a Criptografia de Conteúdo SafeBoot, os administradores podem determinar que sejam criptografados todos os arquivos de um determinado tipo, por exemplo do Excel, ou todo o conteúdo de pastas específicas, como Meus Documentos. Os usuários podem pertencer a grupos que compartilham direitos de acesso aos mesmos arquivos.

CRIPTOGRAFIA TRANSPARENTE DE ARQUIVOS E PASTAS

Depois que o administrador designa as pastas e tipos de arquivo a ser criptografados, tudo se passa de modo transparente. Os usuários nem notam os processos de criptografia e descriptografia, pois o desempenho não é afetado e nenhuma intervenção de sua parte é necessária. A Criptografia de Conteúdo SafeBoot é totalmente integrada ao Windows para facilitar as coisas para os usuários. Para criptografar um arquivo específico, o usuário pode clicar com o botão direito do mouse no arquivo e a opção de criptografia aparecerá para ser selecionada.

COMPARTILHE E MOVA ARQUIVOS SEM RESTRIÇÕES

Grupos de usuários com os mesmos direitos de acesso podem compartilhar arquivos na rede. Com a Criptografia de Conteúdo SafeBoot, os dados particulares armazenados na rede não podem ser visualizados inclusive pelo administrador. Arquivos confidenciais, como minutas de uma reunião da diretoria, podem ser vistos somente pelos membros do grupo que tenha a chave de criptografia correspondente. Os indivíduos que possuem direitos de acesso aos arquivos



podem visualizá-los imediatamente, da mesma forma como veriam um arquivo não-criptografado.

A CRIPTOGRAFIA ACOMPANHA OS ARQUIVOS SEJA QUAL FOR O DESTINO

Com a Criptografia de Conteúdo SafeBoot, reforçada com a tecnologia PET (Persistent Encryption Technology) SafeBoot, os arquivos permanecem criptografados independentemente do local em que venham a ser salvos. Mesmo um arquivo aberto e visível em um laptop estará criptografado e não poderá ser lido em uma mídia removível na qual o usuário tentar gravá-lo. Somente um usuário autorizado poderá visualizar o arquivo criptografado.

IMPLANTAÇÃO E ADMINISTRAÇÃO CENTRAIS

SafeBoot é a única solução de segurança do setor projetada com administração central desde o início. Com a implantação



SafeBoot Content Encryption

central, é possível realizar a implementação de 1.000 usuários em apenas um dia, e o número de usuários gerenciados do ponto de administração central é praticamente ilimitado. A implantação da Criptografia de Conteúdo SafeBoot é um processo simples, principalmente porque a solução é totalmente integrada aos ambientes de TI existentes. O administrador pode especificar os direitos de acesso para grupos de usuários ou indivíduos, de acordo com as diretivas de segurança da instituição. Uma vez implantada a Criptografia de Conteúdo SafeBoot, a solução é administrada com facilidade por meio da interface gráfica da SafeBoot Management Center ou da interface baseada na Web.

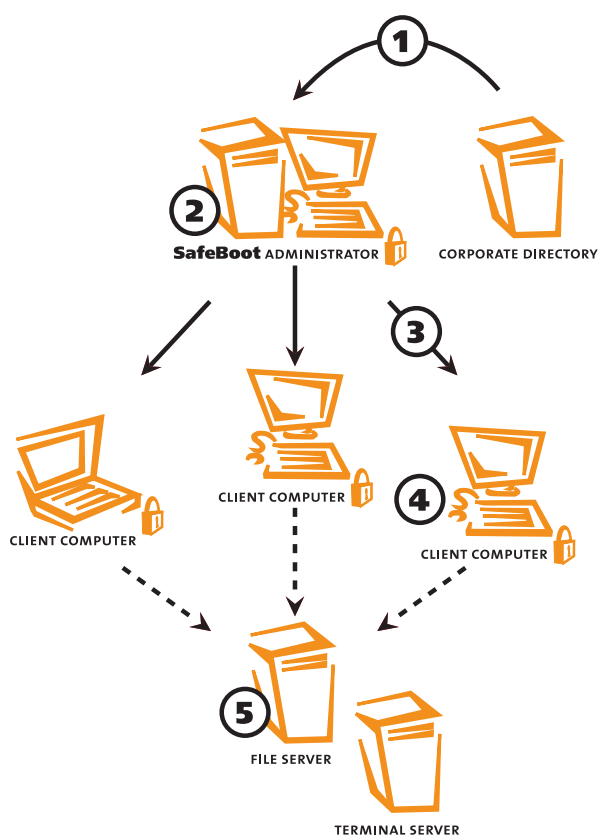
SEGURANÇA COMPULSÓRIA POR MEIO DE DIRETIVAS OBRIGATÓRIAS

Com a Criptografia de Conteúdo SafeBoot, as diretivas de segurança são obrigatórias e compulsórias, pois os usuários

não têm como esquivar-se delas. Os administradores configuram uma Criptografia de Conteúdo SafeBoot de modo que tipos de arquivos ou pastas específicos sejam criptografados sem a intervenção do usuário.

CARACTERÍSTICAS PRINCIPAIS

- Suporte para todos os tokens e cartões inteligentes mais usados para oferecer um nível adicional de proteção.
- Mecanismos exclusivos de compartilhamento de chave para que os usuários compartilhem com segurança o acesso aos arquivos.
- Integração com Active Directory, Novell, PKI e outros.
- Mecanismos de recuperação seguros com suporte internacional.
- Um único ponto de administração.
- Suporte para vários algoritmos, inclusive AES-256.



COMO FUNCIONA A CRIPTOGRAFIA DE CONTEÚDO SAFEBOOT

1. O administrador do SafeBoot cria grupos de usuários ou os importa de diretórios corporativos como Active Directory, Novell NDS ou um ambiente de infra-estrutura de chave pública (PKI).
2. Chaves de criptografia, privilégios de criptografia e diretivas de segurança são criados na Central de Gerenciamento SafeBoot e atribuídas a usuários e grupos. Também podem ser configurados tokens de usuário.
3. As chaves e diretivas de criptografia são distribuídas para os computadores conectados à rede. Elas são armazenadas localmente para permitir que se trabalhe offline com os dados criptografados.
4. Os arquivos e pastas são criptografados automaticamente no computador local e em mídia removível como memory sticks (cartões de memória) USB. A criptografia é totalmente transparente para o usuário final.
5. Os arquivos e pastas são criptografados automaticamente nos recursos da rede, de acordo com as diretivas de criptografia da instituição. Também podem ser criptografados em ambientes de Servidor de Terminal.