

ProtectDrive

Criptografia de disco rígido

O ProtectDrive protege notebooks, computadores pessoais e servidores com criptografia total do disco rígido, controle das portas de conexão e autenticação antes do boot

ProtectDrive & iKey 2032

O ProtectDrive realiza criptografia total de discos rígidos para proteger informações sensíveis em desktops, laptops e servidores contra furtos de informação, acessos indevidos ou hacking. O iKey 2032 adiciona ao ProtectDrive uma total segurança na autenticação, uma vez que, para iniciar o sistema, é necessário inserir o iKey na porta USB e digitar o seu PIN (Número de Identificação Pessoal).

A autenticação pré-boot do ProtectDrive utilizando iKey 2032, previne acessos indevidos ao fechar o acesso ao sistema operacional. Com o iKey o disco rígido da máquina protegida permanece criptografado.

Além disso, durante o uso normal, basta desconectar o iKey da porta USB para que o sistema seja bloqueado, até que se insira o iKey novamente e digite seu PIN.

Criptografia de discos, autenticação forte e proteção de dispositivos

Os registros mestres de boot (MBR) não podem ser modificados e todos os setores de boot são particionados com chaves acessíveis apenas após a autenticação do usuário. Todos os dados são criptografados e decifrados com transparência total, isto é, sem a interação do usuário.

Gerenciamento local ou centralizado, integrado à política de uso das estações

Poder optar entre um gerenciamento centralizado, no servidor, ou descentralizado (local) garante à administração da rede liberdade de escolha para adequar o produto à política da empresa, e não o contrário. O ProtectDrive é flexível para se integrar a qualquer arquitetura padrão de rede.

Integração transparente às funcionalidades existentes no Windows

Integrar-se de forma transparente às práticas de gerenciamento do Windows simplifica muito o processo de implementação do produto. Usuários locais e de domínio podem ser automaticamente integrados ao ambiente de pré-boot do ProtectDrive independentemente da forma de autenticação, sejam simples senhas, smart cards ou tokens USB com certificados padrão X509v3.

Integração transparente com Active Directory

O ProtectDrive integra-se totalmente ao Console de Gerenciamento Microsoft (MMC), o que agiliza a implementação e reduz esforço de instalação. Não se trata de evitar apenas o trabalho repetitivo de instalar uma solução de segurança, mas também de reduzir o custo de aquisição e treinamento.

Implementação automática pela rede

O ProtectDrive prevê deployment automático pela rede, através do Microsoft Group Policy Object. A configuração inicial do sistema e a política de uso são definidas antes da instalação nas estações dos usuários.

Criptografia de discos, autenticação forte e proteção de dispositivos

O ProtectDrive prevê deployment automático pela rede, através do Microsoft Group Policy Object. A configuração inicial do sistema e a política de uso são definidas antes da instalação nas estações dos usuários.

Os registros mestres de boot (MBR) não podem ser modificados e todos os setores de boot são particionados com chaves que só são acessíveis após a autenticação bem sucedida do usuário.

Todos os dados são criptografados e decifrados com transparência total, isto é, sem a interação do usuário.

Benefícios

Fácil de usar

Criptografia de disco transparente e “on-the-fly” Single Sign-on usando senha, smart cards e tokens USB

Mecanismos fortes de segurança

Autenticação transparente ao usuário antes e depois do boot

Smart cards e tokens USB (duplo fator de autenticação)

Autenticação do usuário com cartão ou token (PIN)

Criptografia total do disco

Pode ser usado em conjunto com hardware acelerador de operações de criptografia

Algoritmos criptográficos

3DES, IDEA, AES 128, AES 192, AES 256

Requisitos mínimos de sistema

10Mb de espaço em disco

Plataformas suportadas

Microsoft Windows NT, 2000

Cliente e Servidor, XP, Server 2003

Citrix Winframe/Metaframe

Certificações

O ProtectDrive tem certificado Common Criteria EAL2 e ITSEC E1 e está sendo atualmente avaliado para Common Criteria EAL4

Ferramentas de gerenciamento de software RIS, SMS, Tivoli, TNG, Active Directory e outros

Smart Cards e Tokens

O ProtectDrive é compatível com todos os cartões e tokens padrão X509v3

Uma lista de todos os fabricantes suportados pode ser solicitada sob demanda

Administração fácil e poderosa

Gerência simples de usuários Instalação via rede (interativa e automatizada) Distribuição via Tivoli, SMS, TNG Recuperação através de disco de diagnósticos de posse do usuário

Mínima perda de performance

Nenhum delay é notado durante o trabalho normal

Baixa utilização de memória RAM

Apenas 3.2 MB de disco são utilizados pelo produto

O ProtectDrive gerencia automaticamente as chaves de criptografia durante todo o processo de implementação

A atividade criptográfica se dá sem interferência dos usuários e dos gerentes da rede

Características Técnicas

Criptografia de disco de alta performance com suporte a múltiplos algoritmos: DES, 3DES e IDEA

Criptografia de disco configurável

Chave do usuário derivada das credenciais PKCS#5 v.2.0 PBE

Utiliza certificados para autenticação pré-boot

Criptografia assimétrica da chave que protege o disco

Gerência segura de chaves

Previne o sistema de arquivos contra acessos não autorizados

Proteção de boot

Certificações

- iKey 2032

FIPS 140-1 nível 3

- ProtectDrive

ITSEC-E1

Common Criteria EAL-2

Em avaliação para EAL-4

Requerimentos do Sistema

10Mb de disco

Requerimentos

Autoridade certificadora (CA) Microsoft, Entrust ou RSA, para emissão de certificados de logon no Windows

Plataformas Suportadas

Windows NT® SP6a

Windows® 2000 SP2

Windows® 2000 Server

Windows® XP