



## Proteção exclusiva de dados confidenciais contra acesso por qualquer invasor interno ou externo não autorizado

A maioria das medidas de proteção são voltadas para combater o perigo de fora de uma empresa, enquanto que a maioria dos riscos internos são geralmente ignorados. No entanto, o potencial para danos causados pelo uso indevido de dados confidenciais é exatamente o mesmo. Em praticamente qualquer organização, informações valiosas tais como relatórios de negócios, documentação de RH, dados dos clientes e resultados de pesquisas são salvos eletronicamente sem serem protegidos. A prática atual de salvar os dados centralmente em servidores, redes de comunicação no local de trabalho de vários sites e o uso de mídia de dados móveis significa que os riscos de segurança estão se tornando cada vez maiores. À medida que mais organizações terceirizam seus departamentos de TI em um esforço para reduzir custos, suas preocupações quanto à confidencialidade dos dados aumenta do mesmo modo.

O que é necessário é uma solução de segurança que permite que somente grupos de usuários autorizados acessem dados sigilosos em uma organização. Até mesmo os administradores internos de sistema ou funcionários da empresa terceirizada não devem ter permissão para visualizar os dados confidenciais. Essa é exatamente a questão de segurança que o SafeGuard LAN Crypt foi desenvolvido para resolver.

Ela usa uma criptografia de arquivo completamente automatizada para fornecer uma proteção eficaz para arquivos confidenciais.

No SafeGuard LAN Crypt as funções de Administrador de sistema e Administrador de segurança são estritamente definidas, oferecendo uma vantagem única no tratamento da segurança de dados. O Administrador do sistema ainda pode gerenciar o sistema como de costume, mas não tem como decodificar nenhum arquivo.

Isso se deve ao fato de as chaves serem gerenciadas pelo Administrador de segurança que, por sua vez, não pode acessar os arquivos criptografados armazenados.

O Administrador de segurança define os direitos de acesso individuais para grupos de trabalho ou usuários individuais de acordo com as diretrizes de segurança da empresa. Esses direitos de acesso são, em seguida, reunidos em perfis de criptografia. Isso significa que cada usuário recebe um „grupo chave“ exclusivo com base em seu perfil, com o qual ele pode ler os arquivos divulgados em texto puro da de modo normal. Pessoas não autorizadas só podem ver um string ilegível e cifrado de caracteres.

O **SafeGuard LAN Crypt** não obriga os usuários a alterar o modo como eles trabalham. O processo de criptografia é transparente e é executado de modo invisível em plano de fundo. O SafeGuard® LAN Crypt pode ser usado por tipos diferentes de mídia de memória, unidades de rede de comunicação ou servidores de arquivos, discos rígidos e mídia removível, bem como em servidores terminais.

O **SafeGuard LAN Crypt** fornece proteção completa para todos de uma empresa. Ele é escalável, portanto, pode ser usado em pequenas equipes temporárias, em departamentos e grupos de projeto ou em organizações completas.

**SafeGuard LAN Crypt** – Criptografia inteligente de arquivos. Proteção exclusiva de dados confidenciais contra acesso por invasor interno ou externo não autorizado

**SafeGuard® LAN Crypt Criptografia multi-usuário transparente e baseada em grupos**

### Benefícios

#### Maior segurança

- Segurança de dados transparente para grupos de usuário e usuários individuais
- Criptografia em toda tipo de mídia padrão em ambientes heterogêneos
- Divisão de poder entre a administração do sistema e da segurança
- Implementação simples de uma política de segurança para toda a empresa
- Definição flexível de regras para grupos de usuários
- Integração PKI descomplicada e suporte para certificados, smartcards e tokens de USB

#### Fácil de implementar

- Fácil integração com infra-estruturas heterogêneas de TI
- Administração central descomplicada, usando diretórios ou domínios existentes
- Não são necessárias atualizações adicionais à infra-estrutura de TI existente
- Escalável a partir de grupos de usuários até o lançamento completo em toda a empresa

#### Fácil de usar

- Simples de usar por se integrar aos ambientes de trabalho mais comuns
- Transparência para usuários
- Funcionalidade auto-explicatória, o que significa níveis elevados de aceitação pelo usuário

### Sobre a Utimaco – A Empresa de Segurança de Dados.

Utimaco é uma importante fornecedora global de soluções de segurança de dados, permitindo que organizações de médio a grande porte protejam seus ativos de dados contra perda de dados intencional ou acidental, e cumpram com as leis de privacidade. A linha completa de soluções de segurança de dados da Utimaco fornece uma proteção de dados integral de 360 graus, para dados parados, dados em movimento e dados em uso. A Utimaco oferece aos seus clientes um suporte integral através de uma ampla rede de parceiros certificados e subsidiárias. A Utimaco Safeware AG, com sede em Oberursel, próximo a Frankfurt, Alemanha, está listada na Bolsa de Valores de Frankfurt (ISIN DE0007572406). Para maiores informações, acesse [www.utumaco.com](http://www.utumaco.com)

## Requisitos do sistema

### Hardware

- PC com um processador Intel Pentiu ou um processador compatível

### Sistema operacional

- Microsoft Windows XP
- Microsoft Windows 2000

### Sistemas operacionais de servidor de arquivos suportados

- Microsoft Windows
- Novell Netware
- Linux, Unix (Samba)

## Certificações

- FIPS 140-2
- Algoritmos de criptografia sofisticados e eficientes



## Interoperabilidade

- Integração Microsoft Crypto API: o uso de Fornecedores de serviços criptográficos (CSPs) significa que quaisquer componentes RSA ativados de outros fornecedores (tais como smartcards ou tokens USB) podem ser implementados para autenticação do usuário
- Interface de banco de dados para Oracle e Microsoft SQL Server
- Integração do Microsoft Active Directory e Novell eDirectory

## Mídia suportada

- Discos duros, disquetes, CD, DVD, USB y muchos otros

## Interfaces

- ODBC (banco de dados)
- Crypto API
- Microsoft Cryptographic Service Provider (CSP – Token e smartcards)

## Padrões/Protocolos

- Autenticação: autenticação do usuário via certificados X.509v3
- PKCS#12
- LDAP
- Criptografia: 3DES 168-bit, IDEA 128-bit, AES 128-bit e 256-bit
- Hash: MD5, SHA-256
- Tokens: smartcards e tokens USB via Crypto API

## Versões de idiomas

- Inglês, francês, alemão

## Principais recursos/funcionalidade

### Segurança

- Solução de dados completa para evitar o acesso não autorizado a dados
- Protege os dados de valor da empresa e as informações pessoais confidenciais
- Separara estritamente as responsabilidades de administrações de sistema e segurança
- Melhor proteção possível se a TI for terceirizada porque, embora os funcionários terceirizados possam gerenciar os arquivos, não poderão lê-los em texto plano
- Usa algoritmos de segurança testados e comprovados
- Criptografia e decodificação automática em plano de fundo
- Protege dados em discos rígidos, unidades de rede e mídia portátil, tais como disquetes, CD-ROMs, DVDs, USB e cartões de memória flash
- Autenticação de usuário através de certificados X.509
- Suporta smartcards e tokens USB

### Administração do sistema

- Instalação simples e central, configuração e administração através da integração com ambientes de TI existentes e usando serviços de diretórios atuais (LDAP, Active Directory) ou domínios
- Integração descomplicada em sistemas PKI
- Nenhuma redução do desempenho do servidor. A criptografia e decodificação só são realizadas por um driver de filtro nos dispositivos
- Solução eficaz e de rápida implementação que não precisa de nenhuma infra-estrutura adicional
- Menos tempo e dinheiro necessário para serviços de suporte
- Estratégia de recuperação para que dados criptografados também possam ser acessados em uma situação emergencial

### Fácil de usar

- Usuários autorizados podem salvar suas informações compartilhadas com segurança usando sua mídia de memória comum sem nenhum risco de acesso não autorizado por invasores externos
- Criptografia persistente
- Não há necessidade de alterações aos ambientes e hábitos de trabalho comuns
- Alto nível de aceitação dos usuários: não é necessário treinamento adicional

### Maiores informações

- Para maiores informações, acesse: [www.utimaco.com/SG-LANcrypt](http://www.utimaco.com/SG-LANcrypt)



## Parceiro Utimaco Safeware:

Informações de direitos autorais  
© 2004-2009, Utimaco Safeware AG  
SafeGuard® LAN Crypt Versão 3.51

Todos os produtos SafeGuard são marcas comerciais registradas da Utimaco Safeware AG. Todas as outras marcas comerciais mencionadas pertencem aos seus respectivos proprietários. Funções individuais podem ter características individuais de acordo com os diferentes recursos dos sistemas operacionais).

[www.utimaco.com](http://www.utimaco.com)