

McAfee Total Protection for Data

Proteção abrangente para dados essenciais

O comprometimento com as informações confidenciais de clientes ganhou as manchetes inúmeras vezes nos últimos anos. Muitas vezes, os dados simplesmente saíram pela porta da frente em um laptop ou outro dispositivo móvel. As empresas que sofrem esse tipo de perda de dados se arriscam a graves consequências, inclusive multas previstas em lei, divulgação pública, prejuízos à marca, desconfiança do cliente e prejuízos financeiros. Em 2008, o custo médio para as empresas em virtude de violações de dados foi de US\$6.65 milhões.¹

No ambiente atual, com a Internet onipresente e o número cada vez maior de dispositivos móveis, a proteção das informações confidenciais e da propriedade intelectual dos clientes deve ser uma prioridade.

Principais vantagens

Prevenção contra perda de dados

- Aplicar políticas gerenciadas de maneira centralizada para controlar como os funcionários acessam, usam e transferem dados confidenciais

Criptografia de dispositivos para grandes empresas

- Criptografia completa de disco combinada com um controle de acesso de alta segurança para proteger dados confidenciais em todos os terminais

Criptografia persistente de arquivos e pastas

- Criptografia automática e transparente de arquivos e pastas no momento da gravação, antes que eles trafeguem pela organização

Console centralizado de gerenciamento

- Definir políticas corporativas de segurança que controlem como os dados confidenciais serão criptografados, monitorados e protegidos contra a perda
- Reduzir o trabalho, o tempo e o treinamento gerenciais, aumentando o ROI e reduzindo o TCO

Emissão de relatórios e auditoria avançados

- Monitorar eventos de forma rápida e imediata, além de gerar relatórios detalhados
- Comprovar o cumprimento das normas internas e legais para auditores, diretores e outras partes envolvidas

McAfee Total Protection for Data

Para proteger dados confidenciais, o McAfee® Total Protection for Data é a solução mais completa disponível no mercado. Ele possui criptografia de alta segurança, autenticação, prevenção de perda de dados e controles de segurança por políticas para evitar o acesso e a transferência ilegais de informações confidenciais, em qualquer lugar e a qualquer hora.

Data Loss Prevention

Evitar a perda de dados começa com o aumento da visibilidade e do controle dos dados, mesmo quando eles estão disfarçados. O McAfee Total Protection for Data permite a implementação e a fiscalização de políticas de segurança em toda a empresa, controlando e restringindo como os funcionários usam e transferem dados confidenciais por meio de canais comuns, como e-mail, mensagens instantâneas, impressão e drives USB. Não importa se eles estão no escritório, em casa ou em deslocamento. A empresa mantém o controle.

Criptografia de dispositivos para grandes empresas

Proteja os dados confidenciais com uma solução de segurança de grande porte. O Total Protection for Data utiliza criptografia de disco completo, com controle de acesso de alta segurança por meio de autenticação bifatorial antes da inicialização, evitando o acesso ilegal a dados confidenciais em todos os terminais, inclusive desktops, laptops, handhelds, smartphones e outros dispositivos.

Criptografia persistente e transparente de arquivos e pastas

Garantia de que arquivos e pastas específicos sejam sempre criptografados, independentemente de onde os dados sejam editados, copiados ou salvos, inclusive desktops, laptops, handhelds, smartphones e outros dispositivos. O Total Protection for Data oferece criptografia de conteúdo, que codifica automaticamente e de maneira imperceptível, durante o processo, os arquivos e as pastas selecionados, antes que eles trafeguem pela organização. É possível criar e fiscalizar políticas de forma centralizada com base em usuários e grupos, exigindo a criptografia de determinados arquivos e pastas, sem envolvimento do usuário.

Gerenciamento centralizado de segurança e emissão avançada de relatórios

O McAfee Total Protection for Data se integra com o McAfee ePolicy Orchestrator® (McAfee ePO™) para reduzir os custos permanentes de gerenciamento, instalação, emissão de relatórios e auditoria. Essa integração ajuda a cumprir efetivamente as exigências de privacidade em constante mudança, garantir proteção contínua e demonstrar a conformidade a auditores internos e externos e outras partes envolvidas. Além disso, ele permite o gerenciamento centralizado de segurança com base em políticas. Essa integração também oferece recursos de emissão avançada de relatórios para ajudar a cumprir exigências rigorosas do poder público e do mercado, garante uma proteção "Safe Harbor", e demonstra o cumprimento de exigências de auditores internos e externos, diretores e outras partes envolvidas importantes.

¹ Estudo do custo da Violação de Dados do Ponemon Institute, 2008

Requisitos do sistema

ePO Server

Sistemas operacionais

- Microsoft Server 2003 SP1, 2003 R2

Requisitos de hardware

- Espaço em disco: 250 MB
- RAM: 512 MB
1 GB RAM (recomendado)
- CPU - Intel Pentium II ou superior – mínimo de 450MHz

Terminais de desktops e laptops

Sistemas operacionais

- Microsoft Vista* (todas as versões de 32 e 64 bits)
- Microsoft Windows XP Professional SP1 ou posterior
- Microsoft Windows 2000 SP4 ou posterior
* Disponível para o DLP em 20082

Requisitos de hardware

- CPU: Pentium III 1 GHz ou superior
- RAM: 512 MB recomendáveis
- Espaço em disco: 200 MB no mínimo
- Conexão de rede: TCP/IP para acesso remoto

Terminais Windows Mobile

Sistemas operacionais

- Microsoft Windows Mobile 6.0 for Smartphone
- Microsoft Windows Mobile 6.0 for PDA
- Microsoft Windows Mobile 5,0 for Smartphone
- Microsoft Windows Mobile 5.0 for Pocket PC

Requisitos de hardware

- CPU: Mínimo de 195 MHz
- RAM: 64 MB
- Conexão de rede: TCP/IP para administração remota e Activesync 4.5 ou posterior para instalação/atualizações de políticas pela rede interna

Recursos

Prevenção de perda de dados

- Controlar a maneira como os usuários enviam, acessam e imprimem dados confidenciais pela rede, por meio de aplicativos e para dispositivos de armazenamento. e-mail, webmail, aplicativos P2P, mensagens instantâneas, Skype, HTTP, HTTPS, FTP, Wi-Fi, USB, CD, DVD, impressoras, fax, e armazenamento removível
- Impedir a perda de dados confidenciais causada por cavalos de Troia, worms e aplicativos de troca de arquivos que roubam as credenciais dos funcionários
- Proteger todos os dados, formatos e derivados, mesmo quando os dados são modificados, copiados, colados, compactados ou criptografados, sem perturbar as atividades diárias legítimas

Criptografia de dispositivos para grandes empresas

- Criptografar automaticamente dispositivos inteiros, dispensando a ação ou o treinamento dos usuários finais, além de não afetar os recursos do sistema
- Criptografar completamente o disco com vários algoritmos padrão, entre eles AES-256 e RC5-1024
- Identificar e verificar usuários autorizados, utilizando uma autenticação multifatorial de alta segurança

Criptografia persistente de arquivos e pastas

- Garantir que os arquivos permanecerão sempre criptografados quando não estiverem sendo usados, por meio da inclusão automática de um cabeçalho que acompanha os arquivos protegidos
- Os arquivos e as pastas são mantidos em segurança independentemente de onde foram salvos, inclusive discos rígidos locais, servidores de arquivos, mídias removíveis, até mesmo anexos de e-mail

Console centralizado de gerenciamento

- Utilizar o ePO para especificar a filtragem, o monitoramento e o bloqueio detalhados, por conteúdo, do acesso não autorizado a dados confidenciais
- Gerenciar a criptografia de discos completos, arquivos e pastas; controlar o gerenciamento de políticas e patches; recuperar chaves perdidas e demonstrar o cumprimento das normas
- Sincronizar as políticas de segurança com o Active Directory, Novell NDS, PKI, e outros

Recursos avançados de emissão de relatórios e auditoria

- Comprovar que os dispositivos estão criptografados, com amplos recursos de auditoria
- Registrar as transações de dados para gravar informações, como remetente, destinatário, data e hora e evidências de dados, data e hora do último login bem-sucedido, data e hora de recebimento da última atualização, e sucesso/falha da criptografia

Para saber mais sobre Proteção de Dados, visite http://www.mcafee.com/data_protection.

