



McAfee Complete Data Protection — Essential

Solução básica de criptografia para endpoint

Os dados confidenciais estão sob risco constante de perda, roubo e exposição. Muitas vezes, os dados simplesmente saem pela porta da frente, em um laptop ou dispositivo USB. As empresas que sofrem esse tipo de perda de dados podem sofrer consequências sérias, incluindo penalidades regulatórias, divulgação pública, danos à marca, desconfiança do cliente e prejuízos financeiros. De acordo com um relatório do Ponemon Institute, 7% de todos os laptops corporativos serão roubados ou perdidos em algum momento de sua vida útil.¹ A rápida proliferação de dispositivos móveis com grande capacidade de armazenamento e acesso à Internet está abrindo ainda mais canais para perda ou roubo de dados, de modo que proteger informações confidenciais, proprietárias e de identificação pessoal deve ser uma prioridade principal. O McAfee® Complete Data Protection — Essential soluciona todos esses problemas e muitos outros.

Principais recursos

- Management of Native Encryption
- File and Removable Media Protection

Principais vantagens

- Detenha a perda de dados causada por malware sofisticado, que sequestra informações pessoais e sigilosas
- Proteja os dados armazenados em desktops, laptops, tablets e sistemas de armazenamento na nuvem
- Gerencie o recurso de criptografia nativa oferecido pelo Apple FileVault e pelo Microsoft BitLocker diretamente a partir do software McAfee® ePolicy Orchestrator® (McAfee ePO™)
- Comprove a conformidade com recursos avançados de auditoria e emissão de relatórios
- Monitore eventos e gere relatórios detalhados para demonstrar conformidade com requisitos de privacidade internos e normativos a auditores e outras partes envolvidas

Management of Native Encryption

O Management of Native Encryption permite que os clientes gerenciem o recurso de criptografia nativa oferecido pelo Apple FileVault no Mac OS X e pelo Microsoft BitLocker nas plataformas Windows, diretamente a partir do software McAfee® ePolicy Orchestrator® (McAfee ePO™). O Management of Native Encryption oferece compatibilidade de dia zero com patches, upgrades e atualizações de firmware do OS X e do Windows fornecidos pela Apple e pela Microsoft, além de suporte de dia zero para hardware novo da Apple. O Management of Native Encryption permite que os administradores importem de forma manual as chaves de recuperação para os locais em que os usuários já habilitaram o FileVault e o BitLocker.

Criptografia de mídias removíveis, arquivos, pastas e sistemas de armazenamento na nuvem

Tenha a certeza de que certos arquivos e pastas específicos estarão sempre criptografados, independentemente de onde os dados são editados, copiados ou salvos. O McAfee Complete Data Protection — Essential fornece criptografia de conteúdo, que criptografa de forma automática, transparente e dinâmica os arquivos e pastas escolhidos por você, antes que eles se movam pela sua empresa. Você pode criar e impor políticas centralizadas com base em usuários e grupos de usuários para arquivos e pastas específicos, sem interação com o usuário.

Especificações

Sistemas operacionais

Microsoft Windows

- Microsoft Windows 10
- Microsoft Windows 7, 8, 8.1 (versões de 32 e 64 bits)
- Microsoft Windows Vista (versões de 32 e 64 bits)
- Microsoft Windows XP (somente versão de 32 bits)
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003 (somente a versão de 32 bits)

Requisitos de hardware

- CPU: computadores desktop e laptop com Pentium III de 1 GHz ou superior
- RAM: mínimo de 512 MB (1 GB recomendado)
- Disco rígido: mínimo de 200 MB de espaço livre em disco

Sistemas operacionais

Apple Mac

- Mac OS X El Capitan, Yosemite, Mountain Lion e Mavericks

Requisitos de hardware

- CPU: laptop Mac baseado em Intel com EFI de 64 bits
- RAM: mínimo de 1 GB
- Disco rígido: mínimo de 200 MB de espaço livre em disco

Gerenciamento centralizado

- Consulte a data sheet da plataforma McAfee ePO para obter especificações técnicas

Gerenciamento centralizado da segurança e geração de relatórios avançados

Utilize o console centralizado do software McAfee ePO para implementar e impor políticas de segurança obrigatórias para toda a empresa, que controlam a forma como os dados são criptografados, monitorados e protegidos contra perda. Defina, distribua, gerencie e atualize de forma centralizada as políticas de segurança que criptografam, filtram, monitoram e bloqueiam o acesso não autorizado a dados sigilosos.

Recursos dos pacotes McAfee Complete Data Protection

Gerencie a criptografia nativa em Mac e Windows

- Gerencie o FileVault em qualquer hardware Mac que possa executar o Mac OS X Mountain Lion, Mavericks, Yosemite e El Capitan diretamente a partir do software McAfee ePO.
- Gerencie o BitLocker nos sistemas Windows 7, 8 e 10 diretamente a partir do software McAfee ePO, sem precisar de um servidor Microsoft BitLocker Management and Administration (MBAM) diferente.

- Comprove a conformidade com vários relatórios e dashboards do software McAfee ePO.

Criptografia de mídias removíveis

- Criptografia automática e dinâmica para praticamente qualquer dispositivo móvel de armazenamento, fornecido ou não pela empresa.
- Criptografe ou bloqueie a gravação nas mídias removíveis em estações de trabalho de infraestrutura de desktop virtual (VDI).
- Acesse dados criptografados em qualquer lugar, sem a necessidade de instalar software adicional ou de direitos de administrador local no host do dispositivo.

Criptografia de arquivos, pastas e sistemas de armazenamento na nuvem

- Mantenha arquivos e pastas protegidos independentemente de onde estejam salvos, incluindo discos rígidos, servidores de arquivos, mídias removíveis e sistemas de armazenamento na nuvem, como Box, Dropbox, Google Drive e Microsoft OneDrive.



Figura 1. McAfee Complete Data Protection — Essential.

Console de gerenciamento centralizado

- Use o gerenciamento de infraestrutura do software McAfee ePO para gerenciar a criptografia de pastas, arquivos, discos inteiros e mídias removíveis, controlar as políticas e o gerenciamento de patches, recuperar senhas perdidas e demonstrar a conformidade regulatória.
- Sincronize as políticas de segurança com o Microsoft Active Directory, Novell NDS, PKI e outros.
- Comprove a criptografia dos dispositivos com recursos extensivos de auditoria.

- Grave transações de dados para registrar informações como remetente, destinatário, data e hora do último login bem-sucedido, data e hora do recebimento da última atualização e se a criptografia foi realizada com sucesso ou não.

Para obter mais informações sobre o McAfee Data Protection, visite www.mcafee.com/br/products/dataprotection/index.aspx.

