McAfee Complete Data Protection

Solução abrangente de criptografia para endpoint

Principais recursos

- Drive Encryption
- File and Removable Media Protection
- Management of Native Encryption

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 McAfee ePO
- Comunique-se com seus endpoints e controle-os em nível de hardware, independentemente de eles estarem desligados, desativados ou criptografados, a fim de acabar com as chamadas intermináveis ao suporte e as visitas ao local por causa de incidentes de segurança, epidemias ou senhas de criptografia esquecidas
- Demonstre a conformidade com recursos avançados de auditoria e geração de relatórios; monitore eventos e gere relatórios detalhados que demonstrem aos auditores e a outras partes interessadas a sua conformidade com requisitos internos e normativos de privacidade

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, muitas vezes, acesso à Internet, está abrindo ainda mais canais para a perda ou roubo de dados, de modo que proteger informações confidenciais, proprietárias e de identificação pessoal deve ser uma prioridade principal. Os pacotes McAfee® Complete Data Protection solucionam todos esses problemas e muitos outros.

Criptografia de unidades em nível corporativo

Proteja seus dados confidenciais com uma solução de segurança de nível corporativo que possui os certificados FIPS 140-2 e Common Criteria EAL2+, acelerada com o conjunto Intel® Advanced Encryption Standard — New Instructions (Intel AES-NI). O McAfee Complete Data Protection usa criptografia de unidade combinada a um poderoso controle de acesso, executado por meio de autenticação de pré-inicialização de dois fatores a fim de impedir acesso não autorizado a dados confidenciais em endpoints, incluindo desktops, estações de trabalho de infraestrutura de desktop virtual (VDI), laptops, tablets Microsoft Windows, unidades USB e mais.

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 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 a interação do usuário.

Management of Native Encryption

O Management of Native Encryption permite que os clientes gerenciem o recurso de criptografia nativa oferecido pelo Apple FileVault no OS X, e pelo Microsoft BitLocker nas plataformas Windows, diretamente a partir do software McAfee® ePolicy Orchestrator® (McAfee ePO™). Assim, 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.

McAfee™
Together is power.

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.

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 do McAfee Complete Data Protection

Criptografia de unidades em nível corporativo

- Criptografe automaticamente dispositivos inteiros sem exigir treinamento ou ações do usuário e sem afetar os recursos do sistema.
- Identifique e verifique usuários autorizados usando uma autenticação multifator forte.
- Suporte para Intel® Software Guard Extensions (Intel® SGX).
- Compatibilidade com provedores de credenciais de terceiros.
- Suporte próprio de upgrade para a Atualização de aniversário do Windows 10.

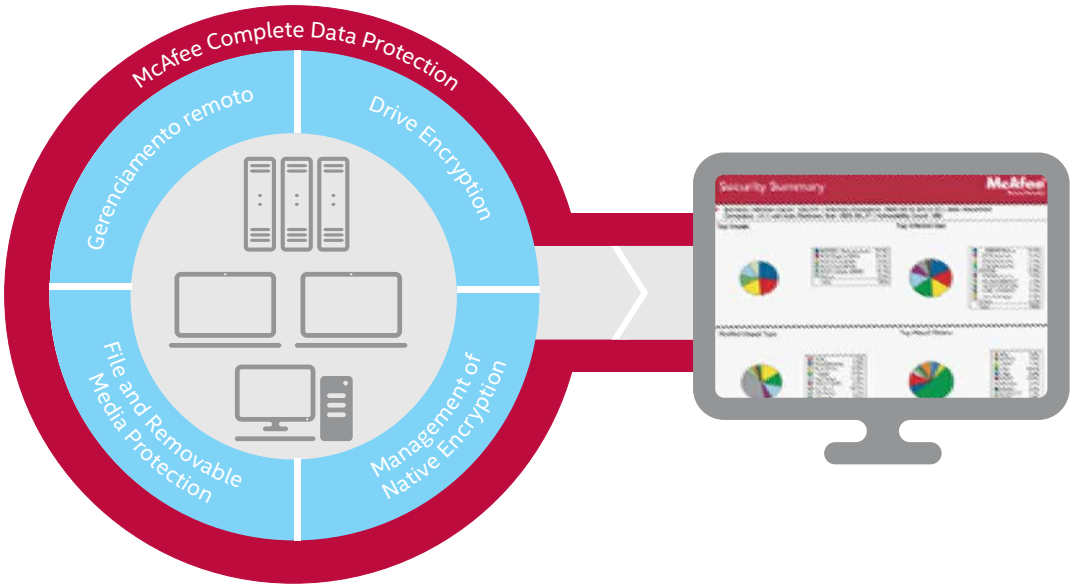

Figura 1. McAfee Complete Data Protection

Especificações do McAfee Complete Data Protection

Sistemas operacionais Microsoft Windows

- Microsoft Windows 7, 8 e 10 (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

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.

Gerencie a criptografia nativa nos Macs 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.

Console de gerenciamento centralizado

- Use o gerenciamento de infraestrutura do software McAfee ePO para gerenciar a criptografia de arquivos, pastas, discos completos e mídias removíveis; controle as políticas e o gerenciamento de patches; recupere senhas perdidas e demonstre 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.
- As transações de dados de registro gravam informações como remetente, destinatário, carimbo de data/hora, evidência de dados, data e hora do último login bem-sucedido, data e hora do recebimento da última atualização e se a criptografia foi realizada com sucesso.

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

McAfee™
Together is power.

1. *The Billion Dollar Lost Laptop Problem Study* (O estudo do problema do laptop de um bilhão de dólares perdido), Ponemon Institute, setembro de 2010.

McAfee LLC
2821 Mission College Blvd.
Santa Clara, CA 95054 USA
www.mcafee.com/br