Segurança de dados simples, flexível e abrangente para toda a sua organização.

Dell Encryption

Hoje, além de proteger os endpoints e os dados armazenados, as organizações também precisam garantir a mobilidade das equipes de trabalho. As soluções de criptografia tradicionais tentam suprir essas demandas, mas são limitadas. É difícil implantar e gerenciar a maioria dessas soluções, que geralmente não cobrem todos os endpoints e acabam oferecendo aos usuários uma performance reduzida.

O Dell Encryption Enterprise oferece mais opções porque ele conta com tecnologias de criptografia flexível, como políticas centradas em dados e criptografia total de disco para proteger os dados. Essa solução foi projetada para:

- Facilidade de implementação

- Transparência para o usuário final

- Conformidade descomplicada

- Facilidade de gerenciamento com um único console

O Dell Encryption é um pacote flexível de soluções avançadas de segurança, incluindo: criptografia baseada em arquivos; criptografia total de disco; gerenciamento centralizado e aprimorado de criptografia nativa (Microsoft BitLocker e Mac FireVault). Além de oferecer proteção de dados em mídias externas, unidades de autocriptografia e dispositivos móveis.

Dell Encryption Enterprise

Com o Dell Encryption Enterprise, a TI pode aplicar as políticas de criptografia facilmente, com os dados na unidade do sistema ou na mídia externa, sem a intervenção do usuário final.

Uma solução perfeita para ambientes com vários fornecedores, o Encryption Enterprise permite:

- Implementação e provisionamento automáticos quando instalado de fábrica em dispositivos comerciais da Dell
- Implantação rápida e fácil em menos de 30 minutos em ambientes VMware usando assistente de instalação, banco de dados totalmente integrado e gerenciamento de chaves
- Possibilidade de eliminar a necessidade de desfragmentação antes da criptografia
- Criptografia de mídia externa e disco do sistema em uma única solução
- Escolha entre criptografia do software baseada em arquivos e criptografia total de disco
- Fácil auditoria e gerenciamento de conformidade usando modelos de política de conformidade definidos com um único toque, gerenciamento remoto e recuperação rápida do sistema
- Integração a processos existentes para fins de autenticação, aplicação de patches e muito mais
- Vendas e suporte para suas soluções de segurança e hardware em uma única fonte
- Criptografia de todos os dados, exceto os arquivos essenciais para inicializar o sistema operacional ou criptografia total de disco,dependendo de sua preferência
- Sistema de controle de porta aprimorado para impedir vazamento de dados
- Capacidade de criptografar de acordo com os perfis de usuários finais, dados e grupos na sua organização
- Gerenciamento centralizado de todas as políticas de criptografia, inclusive unidades com criptografia automática, criptografia total de disco e criptografia do Microsoft BitLocker
- Autenticação avançada de dispositivos padrão OPAL, incluindo logon único no sistema operacional por meio de autenticação pré-boot (PBA) usando Smart Cards e senhas

A vantagem do Dell Encryption

Proteção abrangente e alto nível de segurança

- Protege os dados em qualquer dispositivo e mídia externa
- As chaves e os registros mestre de boot nunca são expostos

Produtividade e simplicidade para TI e usuários finais

- Escolha o Security Management Server Virtual para obter implantação simplificada ou o Security Management Server se quiser ajustar a escala para milhares de usuários
- Integração perfeita a processos de autenticação e gerenciamento de sistemas existentes
- A criptografia é transparente para os usuários finais e os ajuda a manter a produtividade

Criptografia flexível

- Baseada no perfil do usuário final, confidencialidade de dados, necessidades de performance ou conformidade
- Criptografe dados na mídia externa ou desative portas de uma só vez e viabilize também o funcionamento de dispositivos não relacionados a armazenamento
- Gerencie e faça auditoria do Microsoft BitLocker e das unidades com autocriptografia para ajudá-lo no processo de conformidade

Dell Security Management Server Virtual

Com uma implantação simplificada, que utiliza um servidor de gerenciamento virtual criado sob medida e o aplicativo de console para VMware, a Dell mostra como a solução de criptografia de endpoint Dell Encryption está em outro patamar. Ela pode ser implantada com mais rapidez e facilidade na maioria dos ambientes empresariais de médio porte com até 3.500 endpoints.

O Dell Security Management Server Virtual faz com que o Dell Encryption seja a escolha perfeita para SMEs que já têm soluções da VMware e buscam uma plataforma de gerenciamento simples e rápida de implantar para suas políticas de criptografia e autenticação. Ele contém os mesmos recursos e benefícios da versão padrão, inclusive suporte completo à ampla variedade de cobertura de criptografia disponível para laptopts, desktops e mídias externas.

Gerenciamento de unidades de autocriptografia usando o Dell Encryption Enterprise

As organizações que usam as unidades de autocriptografia (SEDs) também precisam de gerenciamento cuidadoso se quiserem reduzir o risco de perda de dados e atender às metas de auditoria e conformidade.

O Dell Encryption Enterprise fornece gerenciamento centralizado e seguro para todas as unidades de autocriptografia da organização, tanto local como remotamente. Todas as tarefas de política, autenticação e gerenciamento, além de armazenamento e recuperação de chaves de criptografia, ficam disponíveis em um único console, reduzindo o trabalho de proteção dos dados críticos e, ao mesmo tempo, minimizando o risco de os sistemas ficarem desprotegidos em caso de perda ou acesso não autorizado.

O mais importante é que o gerenciamento de dispositivos padrão OPAL é totalmente integrado à mesma plataforma de proteção de dados como criptografia baseada em arquivo, Microsoft BitLocker e criptografia de mídia removível.

Os recursos de gerenciamento remoto incluem a capacidade de:

- Desativar logins e limpar caches de usuários para proteger dados e garantir que apenas um administrador autorizado possa reativar o acesso aos dados protegidos
- Desativar o dispositivo para que nenhum usuário faça login no sistema enquanto um comando de desbloqueio não for emitido
- Ativar o dispositivo para que os usuários possam fazer login e usar a SED
- Executar o desbloqueio remoto e automático no disco, permitindo que os administradores executem tarefas essenciais, como aplicação de patches, sem precisar deixar o dispositivo desbloqueado durante a noite
- Realizar autenticação pré-boot completa, incluindo autenticação usando o Active Directory
- Definir políticas de resposta automática a ataques (inclusive ataques de força bruta)

Gerenciado a criptografia total de disco com o Dell Encryption Enterprise

As organizações que usam a criptografia total de disco podem proteger 24x7 os dados confidenciais armazenados no PC e em outros endpoints. A criptografia total de disco é o mais recente recurso do Dell Enterprise Encryption e ajuda a suprir efetivamente as necessidades de proteção de dados. A criptografia total de disco:

- Complementa nossa oferta atual de criptografia e torna nossa solução de criptografia uma das mais robustas do setor
- Oferece autenticação pré-inicialização de classe empresarial para a implementação corporativa
- Usa a tecnologia TPM (Trusted Platform Module) para proteger chaves. Isso evita que invasores removam o disco rígido da plataforma e realizem um ataque off-line nas chaves ocultas que estão armazenadas na unidade

- Criptografa todos os discos rígidos locais em uma implementação simplificada e uma estrutura de gerenciamento remoto
- A criptografia total de disco oferece também uma tecnologia de criptografia fácil de gerenciar que pode ser ativada e mantida com intervenção mínima
- Uma experiência transparente e de alta performance para os seus usuários
- Com a autenticação empresarial pré-inicialização, a criptografia total de disco oferece:
  - Logon único no sistema operacional e na rede
  - Suporte a um único cliente e vários usuários
  - Recuperação simples de chaves de criptografia orientada por administrador e acesso aos dados

Nota: atualmente, a criptografia de disco total da Dell é compatível com os PCs comerciais da Dell (X7 e posterior) no modo de inicialização UEFI com o fator de autenticação por senha. Os PCs que não são da Dell com modo de inicialização preexistente e autenticação via Smart Card serão compatíveis nas versões subsequentes.

Recursos e benefícios do Dell Encryption

Implementação e gerenciamento simplificados

Como você precisa de uma solução fácil de implementar e gerenciar, que não interfira nos processos de TI existentes, o Dell Encryption pode ajudar a:

- Implementar e provisionar automaticamente os usuários quando o Dell Encryption vier instalado de fábrica em determinados dispositivos comerciais da Dell
- Implantar a solução em menos de trinta minutos[1] em ambientes VMware com um banco de dados totalmente integrado e gerenciamento de chave em comparação com soluções típicas da concorrência que exigem vários servidores, um banco de dados separado e várias licenças
- Implantar sem o longo processo de desfragmentação total de disco e com implantação completa
- Eliminar a preocupação com processos de TI preexistentes usando uma solução que funciona imediatamente e não exige reconfigurações
- Integrar a solução a processos de autenticação existentes, inclusive senha do Windows, RSA, impressão digital e Smart Card
- Corrigir, proteger e controlar: detectar rapidamente dispositivos, aplicar e fazer auditoria da criptografia
- Criptografar os arquivos ou dados confidenciais dos usuários mesmo quando a TI precisar acessar o endpoint
- Ter o gerenciamento de dispositivos padrão OPAL totalmente integrado em um único console para todos os endpoints
- Proteger endpoints em ambientes heterogêneos, independentemente do usuário, dispositivo ou localização

Conformidade mais fácil

O Dell Encryption vem com modelos de política predefinidos para ajudar os clientes interessados em cumprir as normas de conformidade, como as citados a seguir:

- Normas do setor: PCI DSS, Sarbanes Oxley (SOX)
- Normas estaduais e federais dos EUA: HIPAA e a Lei HITECH, Lei Gramm Leach Bliley, Califórnia — SB1386, Massachusetts — 201 CMR 17, Nevada — NRS 603A (que exige PCI DSS) e mais de 45 outras leis estaduais e de jurisdições dos EUA
- Normas internacionais: Safe Harbor EUA–Europa, Diretiva de Proteção de Dados da UE 95/46/EC, Lei de Proteção de Dados do Reino Unido, BDSG (Bundes-daten-schutz-gesetz) Alemão e leis semelhantes em vigor para todos os países membros da União Europeia, Canadá — PIPEDA

Especificações técnicas

O Dell Encryption Enterprise está disponível para ambientes que usem soluções de vários fornecedores e atendam às especificações abaixo.

Sistemas operacionais de cliente com suporte:

- Microsoft Windows 7 Ultimate, Enterprise e Professional Editions
- Microsoft Windows 8 e 8.1 Enterprise e Professional Editions
- Microsoft Windows 10 Education, Enterprise e Pro Editions
- macOS X El Capitan, Sierra

O Dell Security Management Server foi validado nos seguintes ambientes operacionais:

- Windows Server 2008 R2 SP0-SP1 de 64 bits Standard e Enterprise Editions
- Windows Server 2012 R2 Standard e Datacenter Editions
- Windows Server 2016 Standard e Datacenter Editions
- VMware ESXi 5.5, 6.0 e 6.5
- VMware Workstation 11 e 12.5

O acesso ao console de gerenciamento remoto e relatórios de conformidade é compatível com os seguintes navegadores:

- Internet Explorer 11.x ou posterior
- Mozilla Firefox 41.x ou posterior
- Google Chrome 46.x ou posterior

Produtividade do usuário final

Entendemos a importância de operar em capacidade máxima, sem interrupções nem atrasos. Por isso, implantamos nossa solução de forma transparente, ajudando a eliminar interrupções durante a criptografia de dispositivos. Na verdade, como ela é tão discreta, as pessoas podem nem perceber que seus dispositivos foram criptografados.

Deployment Services

Permita que a Dell implemente sua solução. Fornecemos um portfólio completo de serviços para implantar soluções de segurança em seu ambiente. Primeiro, nossa equipe de especialistas em cibersegurança avalia seu ambiente para identificar áreas onde é possível aprimorar a segurança dos dados em endpoints, servidores, dados na nuvem e dispositivos móveis. Depois, implementamos, otimizamos e gerenciamos sua solução.

Ampla proteção por criptografia

Conte com o Dell Encryption para proteger dados valiosos em qualquer dispositivo, mídia externa e armazenamento em nuvem pública sem atrapalhar a produtividade. Essa é mais uma maneira de permitir que você vá ainda mais longe. Para obter mais informações sobre a segurança de dados da Dell, acesse Dell.com/DataSecurity.