



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

## Dell Data Protection | Encryption

As organizações precisam encontrar uma forma de garantir a segurança dos dispositivos de endpoint e dos dados contidos neles e, ao mesmo tempo, adotar as tendências de computação, como a política "Traga seu próprio dispositivo" e a mobilidade da força de trabalho. As soluções de criptografia tradicionais tentam atender a essas necessidades, mas a maioria delas é difícil de implantar e gerenciar, não oferece cobertura para todos os endpoints e também reduz a performance para os usuários.

O Dell Data Protection | Encryption fornece uma abordagem de criptografia centralizada nos dados e baseada em política que protege os dados em qualquer dispositivo ou mídia externa. Projetado para fácil implantação, transparência para o usuário final e conformidade livre de transtornos, o Dell Data Protection | Encryption oferece um alto nível de proteção, preenche as lacunas críticas de segurança e permite que você gerencie políticas de criptografia para vários endpoints e sistemas operacionais a partir de um único console de gerenciamento.

O Dell Data Protection | Encryption é um pacote flexível de soluções de segurança avançada que inclui criptografia baseada em software, gerenciamento avançado do Microsoft® BitLocker, proteção de dados em mídia externa, unidades com criptografia automática e dispositivos móveis, além de dados em serviços de armazenamento em nuvem pública.

## Dell Data Protection | Enterprise Edition

O Dell Data Protection | Enterprise Edition inclui criptografia baseada em software e voltada para dados que protege seus dados sem interromper os processos de TI ou a produtividade do usuário final. Ele permite que a TI aplique facilmente as políticas de criptografia, estejam os dados na unidade do sistema ou na mídia externa, e não exige a intervenção do usuário final. Uma solução perfeita para ambientes com vários fornecedores, o Enterprise Edition permite:

- Implantação e provisionamento automáticos quando instalado de fábrica nos dispositivos comerciais da Dell
- Implantação rápida e fácil em menos de trinta minutos<sup>1</sup> em ambientes VMware com instalação baseada em assistente, além de banco de dados totalmente integrado e gerenciamento de chave
- Desfragmentação desnecessária antes da criptografia
- Criptografia de mídia externa e disco do sistema em uma única solução
- Cobertura para ambientes com vários fornecedores, incluindo sistemas operacionais Windows e Mac
- Auditoria e gerenciamento de conformidade com facilidade com modelos de política de conformidade definidos com um toque, gerenciamento remoto e rápida recuperação do sistema
- Integração com processos existentes para 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 arquivos essenciais para realizar o boot do sistema operacional ou criptografia de todo o disco, dependendo da sua preferência
- Sistema de controle de porta aprimorado para impedir vazamento de dados
- Capacidade de criptografar com base em perfis de usuários finais, dados e grupos na sua organização
- Gerenciamento centralizado de todas as políticas de criptografia, inclusive unidades de criptografia automática e criptografia Microsoft BitLocker
- Autenticação avançada para dispositivos padrão OPAL, incluindo Smart Cards e logon único

## A vantagem do Dell Data Protection | Encryption

Proteção abrangente e nível mais alto de segurança

- Protege os dados em qualquer dispositivo, mídia externa e serviços de armazenamento em nuvem pública, como Box e DropBox
- Chaves e registros mestre de boot nunca são expostos

Produtividade e simplicidade para TI e usuários finais

- Escolha o Virtual Edition Server para implantação simplificada ou o Enterprise Edition Server para ajustar a escala para milhares de usuários
- Modelos de política predefinidos criados para fácil conformidade
- Integração perfeita com 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 dos dados, necessidades de performance ou conformidade
- Criptografe dados na mídia externa ou desative portas de uma só vez e permita, ao mesmo tempo, que dispositivos não relacionados a armazenamento funcionem
- Gerencie o Microsoft BitLocker e as unidades com criptografia automática e faça auditoria nos mesmos para obter ajuda no caminho para a conformidade

incluindo suporte completo à mais ampla variedade de cobertura de criptografia disponível para notebooks, desktops, dispositivos móveis, mídia externa, BYOD e armazenamento em nuvem pública.

## Gerenciamento de unidades com criptografia automática com Dell Data Protection | Enterprise Edition

As organizações que usam as unidades com criptografia automática (SEDs) também exigem gerenciamento cuidadoso se desejarem reduzir o risco de perda de dados e atender às metas de auditoria e conformidade.

O Dell Data Protection | Enterprise Edition fornece gerenciamento centralizado e seguro para unidades com criptografia automática em toda a organização, tanto local como remotamente. Todas as tarefas de política, autenticação e gerenciamento, além do armazenamento e da recuperação de chaves de criptografia, ficam disponíveis em um único console, reduzindo o trabalho de proteção dos dados críticos e reduzindo também o risco de os sistemas ficarem desprotegidos em caso de perda ou acesso não autorizado. O mais importante é que o gerenciamento dos dispositivos padrão OPAL é totalmente integrado à mesma plataforma de proteção de dados, como a criptografia baseada em arquivos, Microsoft BitLocker, criptografia de mídia removível, segurança de smartphones e criptografia de dados no armazenamento em nuvem pública.

Os recursos de gerenciamento remoto incluem a capacidade de:

- Desativar logons 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 impedir que qualquer usuário faça logon no sistema até que um comando de desbloqueio seja emitido
- Ativar o dispositivo para que os usuários possam fazer logon e usar a SED

## Dell Data Protection | Enterprise Server – Virtual Edition

A implantação de qualquer aplicativo em toda a empresa pode ser uma tarefa desafiadora, e os produtos de criptografia normalmente não têm sido uma exceção, até agora. Ao utilizar um servidor de gerenciamento virtual criado sob medida e o aplicativo de console para VMware, a Dell conseguiu colocar em execução a solução de criptografia de endpoint, Dell Data Protection | Encryption, com mais rapidez e facilidade na maioria dos ambientes empresariais de médio porte com até 3.500 endpoints.

O Dell Data Protection | Virtual Edition Server torna o Dell Data Protection | Encryption a opção ideal para organizações de pequeno a médio porte que já tiverem investido em VMware e estiverem em busca de uma plataforma de gerenciamento simples e que possa ser implantada rapidamente para suas políticas de criptografia e autenticação. Ela contém os mesmos recursos e benefícios do DDP Server padrão,



- 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 completa pré-boot, incluindo autenticação usando o Active Directory
- Definir políticas de resposta automática a ataques (inclusive ataques de força bruta)

## Recursos de benefícios do DDP | Encryption

Implantação e gerenciamento simplificados

Como você precisa de uma solução fácil de implantar e gerenciar sem interferir nos processos de TI existentes, o Dell Data Protection | Encryption ajuda você a:

- Implantar e provisionar automaticamente os usuários quando o Dell Data Protection | Encryption vier instalado da fábrica em dispositivos comerciais selecionados da Dell
- Implantar a solução em menos de trinta minutos<sup>1</sup> 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 de disco completa e com implantação total
- Eliminar a preocupação com processos de TI preexistentes, com uma solução que funciona imediatamente e não exige reconfigurações
- Integrar a solução a processos de autenticação existentes, como 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 do usuário mesmo quando a equipe de TI precisar acessar o endpoint
- O gerenciamento de dispositivos padrão OPAL é totalmente integrado em um único console para todos os endpoints
- Proteger endpoints em ambientes heterogêneos, independentemente do usuário, dispositivo ou local

Conformidade mais fácil

O Dell Data Protection | Encryption vem com modelos de política predefinidos para ajudar os clientes interessados em atender aos regulamentos de conformidade, como os citados a seguir:

- Regulamentações do setor: PCI DSS, Sarbanes Oxley (SOX)
- Regulamentações 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 jurisdição dos EUA
- Regulamentações internacionais: US-European Safe Harbor, EU Data Protection Directive 95/46/EC, UK Data Protection

## Especificações técnicas

O Dell Data Protection | Enterprise Edition está disponível para ambientes com vários fornecedores que atendem às especificações abaixo.

Sistemas operacionais de cliente com suporte:

- Microsoft Windows XP Professional<sup>1</sup>
- 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<sup>2</sup>
- Microsoft Windows Server 2008 SP2 e 2008 R2 SP1 Foundation, Standard, Datacenter e Enterprise Editions
- Microsoft Windows Server 2012 e R2 Foundation, Essential, Standard e Datacenter Editions
- Mac OS X Mavericks, versões Yosemite e El Capitan

O Dell Data Protection | Enterprise Edition foi validado nos seguintes ambientes operacionais:

- Windows Server 2008 R2 SP0-SP1 de 64 bits, Standard e Enterprise Editions
- Windows Server 2008 SP2 de 64 bits, Standard e Enterprise Editions
- Windows Server 2012 R2 Standard Edition
- VMware ESXi 5.1, 5.5 e 6.0
- VMware Workstation 9, 10 e 11

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

Act, German BDSG (Bundes-daten-schutz-gesetz) e leis semelhantes em vigor para todos os países membros da União Europeia, Canadá – PIPEDA

### Produtividade do usuário final

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

### Proteja seus dados em qualquer lugar

Confie no Dell Data Protection | Encryption para ajudar a proteger dados valiosos em qualquer dispositivo, mídia externa e armazenamento em nuvem pública, mantendo também a produtividade. É apenas mais uma forma de proporcionar a você a capacidade de fazer mais. Para obter mais informações sobre o pacote de soluções Dell Data Protection, acesse [Dell.com/DataProtection](http://Dell.com/DataProtection).

Saiba mais em [Dell.com/DataProtection](http://Dell.com/DataProtection)

<sup>1</sup>. Suporte para DDP | E v 8.5 ou anterior

<sup>2</sup>. Suporte para DDP | E v 8.6.1 ou posterior