



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

Dell Data Protection | Encryption

À medida que as organizações lutam para proteger dispositivos de endpoint, a consumerização, a globalização e a mobilidade da força de trabalho criam novos desafios. Enquanto isso, você só precisa ler as notícias para saber que as ameaças estão mais coordenadas e rápidas. A Dell pode ajudar você a alcançar a confiança nos negócios, proporcionando um caminho mais fácil até a proteção de dados, conformidade e continuidade empresarial.

O Dell Data Protection | Encryption oferece a você a garantia de que seus dados e os dados de seus clientes estão seguros, com uma solução desenvolvida para proteção simples, abrangente e flexível. É uma solução baseada em políticas que protege os dados armazenados na unidade do sistema e/ou na mídia externa. Criado para fornecer fácil implantação, transparência para o usuário final e conformidade livre de transtornos, o portfólio de produtos do 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, tudo 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, dispositivos e em serviços de armazenamento de 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 instalados de fábrica nos dispositivos comerciais da Dell
- Implantação rápida e fácil em menos de trinta minutos¹ em ambientes VMware com instalação baseada em assistente, além de banco de dados totalmente integrado e gerenciamento de chave
- Não é necessária a desfragmentação da base de instalação
- 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 fáceis 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 de uma única fonte
- Criptografia de todos os dados, exceto arquivos essenciais para o boot do sistema operacional
- Controle de porta aprimorado para gerenciar o vazamento de dados em smartphones com Android ou iOS
- 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 autcriptografia
- Autenticação avançada para unidades de autcriptografia, inclusive Smart Cards e logon único



Dell Data Protection | Server Encryption

A conformidade e a segurança do endpoint são fundamentais para todas as organizações, não importa o tamanho. As organizações devem proteger todos os dispositivos de endpoint, independentemente do tipo de endpoint e de onde estejam localizados. Além disso, devem atender aos requisitos do usuário final e manter a conformidade com os requisitos de segurança. As soluções de proteção de endpoint tradicionais tentam atender a essas necessidades, mas o gerenciamento de vários clientes e consoles é difícil para equipes de TI com recursos restritos, especialmente aquelas sem especialistas em segurança internos, como pequenas e médias empresas. A maioria das soluções de proteção de endpoint são difíceis de implantar e gerenciar, não oferecem cobertura para todos os endpoints e reduzem a performance para os usuários.

O Dell Data Protection | Server Encryption oferece proteção de endpoint eficiente para servidores Windows que podem estar localizados em ambientes de filiais ou escritórios remotos. Esses servidores podem armazenar dados confidenciais, mas podem sofrer invasões. A proteção dos dados nesses servidores poderia significar a proteção da reputação de uma organização. Há muitos servidores que estão localizados em locais como escritórios remotos, escritórios de advocacia, lojas de varejo ou escritórios do governo estadual e local que não estão protegidos por muros e, ainda sim, armazenam informações confidenciais do cliente como informações pessoais e financeiras que devem ser protegidas. O produto Server Encryption oferece proteção abrangente para dados que pode ser gerenciada centralmente através de um único console para ajudar as empresas a reduzirem a complexidade e os custos com o gerenciamento da TI. Com o relatório de conformidade consolidado, as empresas podem facilmente aplicar e comprovar a conformidade para todos os servidores de endpoint. A segurança integrada com recursos como política predefinida e modelos de relatório é especialmente útil para organizações de médio porte com equipes de TI menores e menos especializadas.

Dell Data Protection | External Media Edition

Muitas organizações já estão protegendo dados em unidades de sistema de endpoint, mas talvez não tenham uma solução para resguardar os dados armazenados

em mídia externa. Isso cria uma importante lacuna de segurança que poderia comprometer a propriedade intelectual, além de dados de clientes e funcionários. O External Media Edition oferece proteção de mídia externa e acesso a portas baseados em políticas. Incluído com o Dell Data Protection | Enterprise Edition ou disponível por conta própria, o External Media Edition oferece gerenciamento e implantação simples, aplicação eficiente de políticas e proteção flexível para redução de interrupções do fluxo de trabalho:

- Gerencie, criptografe e gere relatórios em qualquer tipo de mídia removível e USB (inclusive dispositivos ópticos)
- Gerencie o vazamento de dados em smartphones com Android ou iOS conectados a uma porta externa
- Todas as chaves de criptografia são controladas para facilitar a recuperação
- A equipe de TI pode definir políticas de proteção sem depender de sua aplicação por usuários finais
- As regras de criptografia estão vinculadas ao perfil do usuário nas ferramentas do Microsoft® Windows Server® Active Directory®
- Nenhuma formatação especial nem "contêineres" são criados na unidade removível e nenhuma cópia, remoção ou destruição forçada de dados preexistentes é realizada
- Sem longos períodos de espera até que a unidade USB seja formatada
- Criptografa apenas os dados confidenciais na mídia externa (como cartões SD e XD) sem alterar a operação fundamental do dispositivo para que dados pessoais e os dados protegidos da organização possam coexistir
- Logon único, seja em um sistema único ou múltiplo

Dell Data Protection | Cloud Edition

Hoje em dia, funcionários, fornecedores e parceiros movem, compartilham e armazenam de maneira rotineira arquivos em serviços de armazenamento de nuvem, como Box, Dropbox e Microsoft® SkyDrive. A pura facilidade e conveniência com que as pessoas podem colaborar entre elas aumenta a produtividade, mas, ainda assim, os serviços de armazenamento em nuvem pública também introduziram uma lacuna de segurança de dados. Assim que os usuários salvam arquivos em uma nuvem pública, a TI perde o controle sobre a segurança dos dados. O Dell Data Protection | Cloud Edition ajuda a colocar a TI no controle, protegendo os dados enquanto eles se movem para dentro e para fora das nuvens públicas, com um processo transparente de criptografia e descriptografia que permite que as pessoas utilizem o armazenamento em nuvem como sempre fizeram, sem interrupções.

O Dell Data Protection | Cloud Edition permite que os administradores de TI:

- Criem listas brancas de endereços de e-mail que os usuários estão autorizados a utilizar para o compartilhamento de arquivos
- Monitorem todos os endereços IP conhecidos para os serviços de armazenamento de nuvem e os combinem com o processo do aplicativo.

- Controlem dados por meio da criptografia transparente, criptografem e descriptografem o tráfego capturado conforme ele se movimenta para dentro e fora da nuvem
- Gerenciem criptografia, chaves de criptografia, recuperação de acesso, políticas e perícia centralmente
- Façam auditoria e gerem relatórios sobre atividade de arquivos, arquivos sincronizados, arquivos acessados por quem, onde e quando, além de compilar relatórios de conformidade
- Acessem dados criptografados na nuvem de plataformas iOS e Android
- Apliquem políticas para acesso a serviços de nuvem, pastas públicas, aplicativos, expirações de chaves e períodos de pesquisa

Dell Data Protection | Mobile Edition

Smartphones e tablets pessoais, como desktops e notebooks, tornaram-se uma ferramenta de trabalho padrão. Consequentemente, a maioria das organizações estão aderindo à estratégia de Traga seu próprio dispositivo, reconhecendo que isso ajuda a reduzir os custos com equipamentos e a aumentar a produtividade. Mas, sem a aplicação de senha e a criptografia adequada, os dados acessados em dispositivos móveis, seja de um servidor corporativo ou uma nuvem pública, ficam desprotegidos. Um dispositivo perdido ou roubado coloca as empresas em risco de violações de segurança e violações de conformidade. O Dell Data Protection | Mobile Edition protege os dados acessados em smartphones e tablets que executam sistemas operacionais iOS ou Android.

O Dell Data Protection | Mobile Edition permite que os administradores de TI:

- Definam políticas pela empresa, como exigir um PIN ou desativar backups
- Emitam comandos rapidamente, como a Limpeza remota e a Redefinição de senha
- Detectem automaticamente dispositivos não registrados
- Removam o acesso de um dispositivo ao Exchange Server se ele for perdido ou roubado, ou se precisar ser desprovisionado
- Compilem relatórios de conformidade e atendam aos requisitos do auditor

Dell Data Protection | BitLocker Manager

Se você busca por uma forma de gerenciar a criptografia Microsoft BitLocker, o Dell Data Protection | BitLocker Manager permite que você veja, gerencie e faça auditorias nos recursos e no software. Os recursos do gerenciamento de nível empresarial do BitLocker Manager incluem:

- Controle centralizado de chaves e senhas de recuperação
- Auditoria e geração de relatórios centralizados
- Gerenciamento centralizado de políticas
- Controle total sobre todas as políticas sem o uso do Active Directory **nativo**
- Aplicação aprimorada de usuários que sejam administradores locais

A vantagem do Dell Data Protection | Encryption

Proteção abrangente, nível superior 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

- Não exige um banco de dados separado, vários servidores ou várias licenças durante a implantação em ambientes VMware
- Modelos de política predefinidos criados para fácil conformidade
- Integração perfeita com processos de autenticação e gerenciamento de sistemas existentes
- O mecanismo de 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 os dados de portas ou desative-os totalmente, sem que os dispositivos que não são de armazenamento parem de funcionar
- Gerencie o Microsoft BitLocker e faça auditorias no mesmo para obter ajuda no caminho para a conformidade

- Inicialização e gerenciamento automatizados do TPM
- Integração à criptografia de outras plataformas

Recursos e benefícios do Dell Data Protection | 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 minutos¹ 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 os processos de TI pré-existentes com uma solução que funciona imediatamente e não requer reconfigurações²
- Integrar a solução a processos de autenticação existentes, como senha do Windows, RSA, impressão digital e Smart Card²

- Definir automaticamente a política de criptografia usando o console remoto, dependendo dos requisitos regulamentares
- Corrigir, proteger e controlar: detectar rapidamente dispositivos, aplicar e fazer auditoria da criptografia
- Criptografar os arquivos ou dados confidenciais dos usuários mesmo quando o suporte da TI for necessário
- 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 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.

Com o Dell Data Protection | Encryption, você pode ter menos erros do sistema na infraestrutura e uma chance menor de perder dados durante a implantação.

Proteja seus dados em qualquer lugar

Confie no Dell Data Protection | Encryption para ajudar na proteção de seus dados mais valiosos em qualquer dispositivo, mídia externa e em 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.

Especificações técnicas

DDP | Enterprise Edition, DDP | External Media Edition, DDP | Cloud Edition e DDP | BitLocker Manager estão disponíveis para ambientes com vários fornecedores que atendam às especificações abaixo.

Sistemas operacionais com suporte:

- Microsoft Windows XP Professional¹
- 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 Editions²
- Mac OS X Mavericks, versões Yosemite e El Capitan

Sistemas operacionais com suporte para Server Encryption

- 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

DDP | Enterprise Edition, DDP | External Media Edition, DDP | Cloud Edition e DDP | BitLocker e DDP | Server Encryption foram validados 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

Saiba mais em Dell.com/DataProtection

¹. Suporte para DDP | E v 8.5 ou anterior

². Suporte para DDP | E v 8.6.1 ou posterior