



Panda Full Encryption

A primeira linha de defesa para proteger os dados de forma simples e eficaz



De acordo com o Gartner¹, um laptop é roubado a cada 53 segundos, e parece claro que a quantidade crescente de dados armazenados nos endpoints aumentou o interesse nele e o risco de sofrer uma violação de segurança de dados devido a perda, roubo ou acesso não autorizado a informações.

Isso resultou em regulamentos como o GDPR² na União Europeia e o CCPA³ nos Estados Unidos, entre outros, tornando-se mais exigentes em um esforço para reduzir a probabilidade crescente de perda, roubo ou acesso não autorizado a dados e o sério impacto econômico que pode ter nas organizações.

FORTALECER A SEGURANÇA CONTRA O ACESSO NÃO AUTORIZADO DE FORMA CENTRALIZADA

Uma das maneiras mais eficientes de minimizar a exposição a dados é criptografar automaticamente os discos rígidos de desktops, laptops e servidores, impedindo que usuários não autorizados acessem as informações criptografadas sem a chave apropriada. Essa política fornece uma camada adicional de segurança e controle para as organizações, embora também possa levar a problemas de controle e recuperação de dados se a chave for perdida.

O Panda Full Encryption⁴ utiliza o BitLocker, a tecnologia comprovada e estável da Microsoft, para criptografar e descriptografar discos sem afetar os usuários finais e fornecer às organizações o valor agregado de controlar e gerenciar centralizadamente as chaves de criptografia armazenadas na plataforma de gerenciamento baseada em nuvem da Panda Security: Aether.



Painel do Panda Full Encryption no console de gerenciamento web do Aether com indicadores principais do status de criptografia dos endpoints em toda a organização.

BENEFÍCIOS

- **Evite perda, roubo e acesso não autorizado a dados sem afetar os usuários**

Criptografe seus discos e proteja o conteúdo deles contra roubo, perda acidental e insiders maliciosos. A criptografia, a descriptografia e o acesso a dados é automático, imediato e transparente para os usuários.

Para sua conveniência, as chaves de recuperação são armazenadas e recuperadas de forma segura a partir da plataforma em nuvem e seu console da web.

- **Nenhuma implantação ou instalação. Nenhum servidor ou custos adicionais. Zero problemas**

O Panda Full Encryption gerencia centralizadamente o BitLocker, uma tecnologia Windows comprovada e amplamente utilizada.

O BitLocker está incluído na maioria dos sistemas operacionais Windows e, com o console Web do Aether Platform, você terá um único local centralizado para gerenciar seus dispositivos.

Você não precisará implantar ou instalar outro agente.

As soluções baseadas em Aether compartilham o mesmo agente leve. A capacidade de gerenciar centralizadamente as chaves de recuperação a partir da nuvem, significa que você não precisa instalar ou manter servidores para gerenciá-las. O Panda Full Encryption pode ser ativado imediatamente e é fácil ser gerenciado através da interface amigável do Aether Platform

- **Conformidade regulatória, relatórios e gerenciamento central**

O Panda Full Encryption ajuda e simplifica a conformidade com os regulamentos de proteção de dados, monitorando e impondo a ativação do BitLocker em dispositivos Windows.

Todas as soluções baseadas em Aether fornecem painéis intuitivos, relatórios detalhados e auditorias de alterações.

Além disso, seu gerenciamento baseado em funções permite que os administradores implementem diferentes níveis de autorização e diferentes políticas para grupos e dispositivos a partir de um único console Web centralizado.

¹ Gartner: http://www.dell.com/content/topics/global.aspx/services/prosupport/en/us/get_connected?c=us&l=en

² GDPR - Regulamento Geral de Proteção de Dados: obriga as organizações a garantir que as informações pessoais processadas sejam protegidas. O não cumprimento pode resultar em multas severas e danos indiretos.

³ CCPA - Lei de Privacidade do Consumidor da Califórnia de 0,8: Esta é a primeira lei dos Estados Unidos seguindo os passos do GDPR da União Europeia. Aplica-se a empresas com sede na Califórnia e empresas com sede fora do estado.

⁴ O Panda Full Encryption é um módulo integrado na plataforma de gerenciamento de nuvem Aether.

PRINCIPAIS FUNCIONALIDADES

O Panda Full Encryption, é um módulo adicional para a proteção de endpoints da Panda Security e soluções de segurança avançadas adaptáveis, projetado para gerenciar centralizadamente a criptografia completa de disco e fornecer os seguintes recursos:

Criptografia e descriptografia completa da unidade

O Panda Full Encryption aproveita o BitLocker para criptografar totalmente as unidades de seus laptops, desktops e servidores Windows⁵. O painel do Panda Full Encryption fornece visibilidade global dos endpoints de rede compatíveis com o recurso, seu status de criptografia e o método de autenticação usado e permite que os administradores atribuam configurações de criptografia e restrinjam as permissões de criptografia.

Gerenciamento centralizado e recuperação de chaves de criptografia

Se a chave de criptografia for esquecida ou houver alterações no hardware do computador, o BitLocker solicitará uma chave de recuperação para inicializar o sistema afetado. Se necessário, o administrador da rede pode obter a chave de recuperação por meio do console de gerenciamento e enviá-la ao usuário do computador.

Listas e relatórios. Aplicação de política centralizada

A lista de computadores no console permite que os administradores apliquem vários filtros com base no status de criptografia. Essas listas podem ser exportadas para análise de dados com ferramentas externas.

Defina políticas de criptografia a partir do console e visualize alterações de políticas por meio de relatórios de auditoria que você pode apresentar a órgãos reguladores e instituições, se necessário.

Computer ID	Group	Operating system	Encryption status	Disk encryption	Authentication method	Last connection
WIN_DESKTOP_1	ion	Windows 10 Pro (Version 1807) (Build 18363.893)	Encrypted	Encrypted disks	Security processor (TPM)	3/26/2018 8:55:23 AM
WIN_DESKTOP_2	ion	Workstat Windows 8.1 Enterprise 64 SP2 (Build 9200)	Encrypted (partially)	Encrypted (partially)	Security processor (TPM)	3/26/2018 8:55:23 AM
WIN_DESKTOP_3	ion	Workstat Windows 7 Ultimate 64 SP1	Encrypted by the user (partially)	Encrypted by the user (partially)	Security processor (TPM)	3/26/2018 8:55:24 AM
WIN_DESKTOP_4	ion	Workstat Windows 7 Ultimate 64 SP4	Not encrypted	Not encrypted	Password	3/26/2018 8:55:24 AM

Lista de computadores mostrando os computadores, os grupos a que pertencem, o sistema operacional, o status de criptografia e o método de autenticação usado.

Requisitos do Panda Full Encryption e plataformas suportadas:
<http://go.pandasecurity.com/full-encryption/requirements>

Prêmios e certificações

A Panda Security participa e é regularmente premiada em avaliações comparativas independentes de proteção e desempenho realizadas por instituições como o Virus Bulletin, o AV-Comparatives, o AV-Test e o NSS Labs. O Panda Adaptive Defense ganhou a Certificação Common Criteria EAL2 +.



A Panda Security é reconhecida como "Visionária" no Quadrante Mágico da Gartner para Plataformas de Proteção de Endpoint (EPP) 2018.

PLATAFORMA DE GESTÃO EM NUVEM



A plataforma baseada em nuvem da Aether é comum a todas as soluções de endpoint da Panda Security, simplificando a segurança, a avaliação de vulnerabilidades e o gerenciamento de patches. Isso, combinado com o Panda Full Encryption, facilita o monitoramento, a conformidade e o gerenciamento de criptografia e descriptografia do endpoint a partir de um único console da web. Este módulo permite que as organizações gerenciem centralizadamente todas as chaves e recursos de recuperação, ajudando a gerenciar os discos criptografados de laptops, desktops e servidores do Windows.

Gera maior valor em menos tempo. Implementação rápida e fácil

- Gera maior valor em menos tempo. Implementação rápida e fácil
- Único agente leve para todos os produtos e plataformas (Windows, Mac, Linux e Android).
- Descoberta automática de endpoints desprotegidos. Instalação remota.
- Tecnologias proprietárias de proxy e repositório / cache. Comunicação otimizada mesmo com endpoints sem conexão com a Internet.

Simplifica as operações. Adapta-se à sua organização

- Console da web intuitivo. Gerenciamento modular flexível que reduz o custo total de propriedade.
- Usuários com permissões totais ou restritas e visibilidade. Auditorias de atividades
- Políticas de segurança para grupos e endpoints. Funções predefinidas e personalizadas.
- Inventários de hardware /software e registros de alterações.

Fácil dimensionamento de recursos de segurança e gerenciamento ao longo do tempo

- Adicione módulos sem infraestruturas adicionais ou custos de implantação.
- Comunicação em tempo real com endpoints de um único console de gerenciamento da web.
- Painéis e indicadores para cada módulo

⁵ Para ver as plataformas suportadas, clique em <http://go.pandasecurity.com/full-encryption/requirements>