

Panda Full Encryption

Primeira linha de defesa para proteger os dados de forma simples e eficaz

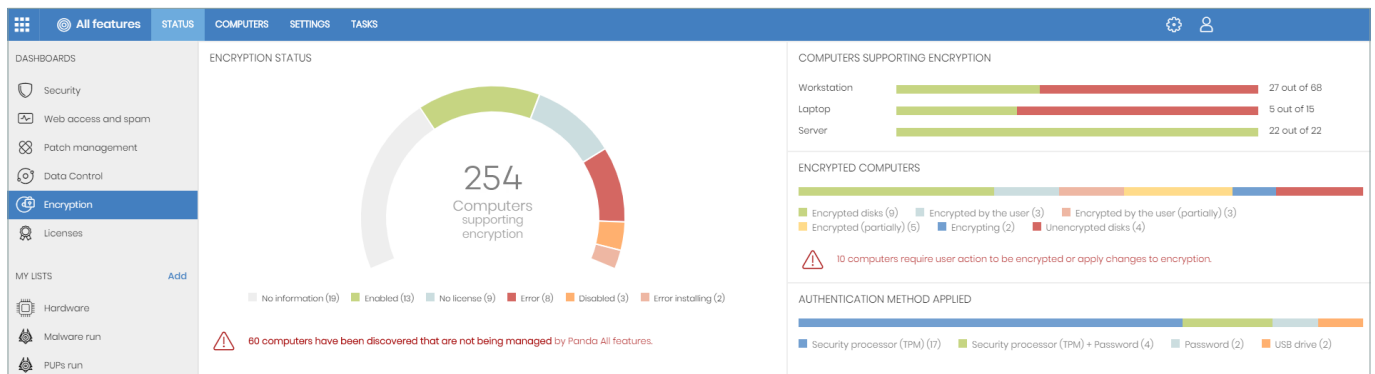
De acordo com o Gartner,¹ **um laptop é roubado a cada 53 segundos. A crescente quantidade de dados armazenados em endpoints aumentou o interesse por essas informações, assim como o risco de violações por meio de perda, roubo ou acesso não autorizado.**

Como consequência, houve uma elevação na exigência de regulamentos, como o GDPR² na União Europeia e o CCPA³ nos Estados Unidos, em um esforço para reduzir a crescente probabilidade de perda, roubo ou acesso não autorizado aos dados e o grande impacto econômico causado por esse tipo de evento.

FORTALECER CENTRALMENTE A SEGURANÇA CONTRA O ACESSO NÃO AUTORIZADO

Uma das maneiras mais eficazes de minimizar a exposição dos dados é criptografar automaticamente os discos rígidos de desktops, laptops e servidores. Dessa forma, o acesso aos dados é **seguro e cumpre com os mecanismos de autenticação estabelecidos**. A definição de políticas de criptografia 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 Encryption**⁴ aproveita o BitLocker, uma tecnologia comprovada e estável da Microsoft, para criptografar e descriptografar discos sem afetar os usuários finais. Fornece às organizações o valor agregado para controlar e administrar **centralmente as chaves de recuperação armazenadas na plataforma de gerenciamento baseada na nuvem da Panda Security: Aether**.



Painel do Panda Full Encryption no console de gerenciamento web do Aether, que inclui indicadores-chave do status de criptografia dos endpoints em toda a organização.

BENEFÍCIOS

- **Evite perdas, roubos e acesso não autorizado a dados sem afetar os usuários**

Criptografe seus discos e proteja seu conteúdo contra roubo, perda acidental e insiders maliciosos. A criptografia de dados, a descriptografia e o acesso são automáticos, imediatos e integrados para os usuários.

Para aumentar a praticidade, as chaves de recuperação são armazenadas e recuperadas com segurança na plataforma em nuvem e no console na web.

- **Sem implantação ou instalação. Sem servidores ou custos adicionais. Sem problemas**

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

O BitLocker está incluído e pronto para uso na maioria dos sistemas operacionais Windows e, **com o console da web da plataforma Aether, você pode gerenciar seus dispositivos em um só lugar.**

Não é preciso implementar nem instalar outro agente. Todas as soluções baseadas em Aether **compartilham o mesmo agente leve.**

Com a capacidade de gerenciar centralmente as chaves de recuperação da nuvem, você **não precisa instalar nem manter servidores para** fazer esse controle.

O Panda Full Encryption **pode ser ativado imediatamente** e é fácil de gerenciar por meio da interface simplificada da plataforma Aether.

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

Com o Panda Full Encryption, fica mais fácil se manter em **conformidade com as regulamentações de proteção de dados**, monitorando e reforçando a ativação do BitLocker em dispositivos Windows.

Todas as soluções baseadas no Aether fornecem **painéis intuitivos, relatórios detalhados e auditorias de alteração.**

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

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

² GDPR – Regulamento de Proteção de Dados Gerais: Força as organizações a garantir que as informações pessoais processadas sejam protegidas. O não cumprimento pode resultar em muitas severas e danos indiretos.

³ CCPA - Lei de Privacidade do Consumidor da Califórnia de 2018: Esta é a primeira lei dos Estados Unidos que segue os passos do GDPR da União Europeia. Aplica-se a empresas sediadas na Califórnia e a organizações sediadas fora do estado.

⁴ Panda Full Encryption é um módulo integrado na plataforma de gerenciamento Aether Cloud: Aether.

PRINCIPAIS RECURSOS

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 centralmente a criptografia completa de disco. A ferramenta fornece os seguintes recursos:

Criptografia e Descriptografia Completa da Unidade

O Panda Full Encryption aproveita o BitLocker para criptografar totalmente as unidades de seus notebooks, desktops, servidores e armazenamento removível do Windows. O painel do Panda Full Encryption fornece visibilidade global sobre os endpoints de rede compatíveis, o status de criptografia e o método de autenticação usado. Além disso, permite que os administradores atribuam configurações e restrinjam permissões de criptografia.

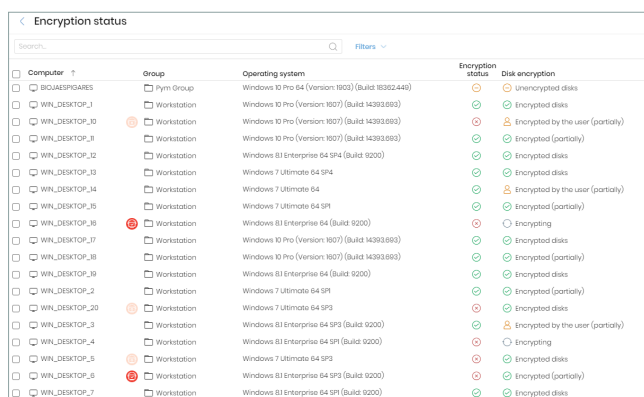
Gerenciamento Centralizado das Chaves de Recuperação

Se a chave de acesso for esquecida ou houver alterações na sequência de inicialização, o BitLocker pedirá uma chave de recuperação para iniciar o sistema afetado. Se necessário, o administrador da rede pode obter a chave de recuperação através do console de gerenciamento e enviá-la para o usuário.

Listas e Relatórios. Política Centralizada de Aplicativos

A lista de computadores na 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 as políticas de criptografia da console e visualize as mudanças de políticas por meio de relatórios de auditoria que podem ser apresentados aos órgãos e às instituições reguladoras, se necessário.



Computer	Group	Operating system	Encryption status	Disk encryption
BIOAESPIGARES	Pym Group	Windows 10 Pro 64 (Version: 1803) (Build: 18302.449)	Unencrypted disks	Unencrypted disks
WIN_DESKTOP_1	Workstation	Windows 10 Pro (Version: 1807) (Build: 18363.893)	Encrypted disks	Encrypted disks
WIN_DESKTOP_3	Workstation	Windows 10 Pro (Version: 1807) (Build: 18363.893)	Encrypted by the user (partially)	Encrypted (partially)
WIN_DESKTOP_8	Workstation	Windows 10 Pro (Version: 1807) (Build: 18363.893)	Encrypted disks	Encrypted disks
WIN_DESKTOP_12	Workstation	Windows 8.1 Enterprise 64 SP4 (Build: 9200)	Encrypted disks	Encrypted disks
WIN_DESKTOP_13	Workstation	Windows 7 Ultimate 64 SP4	Encrypted disks	Encrypted disks
WIN_DESKTOP_14	Workstation	Windows 7 Ultimate 64 SP4	Encrypted by the user (partially)	Encrypted (partially)
WIN_DESKTOP_15	Workstation	Windows 7 Ultimate 64 SP4	Encrypted disks	Encrypted disks
WIN_DESKTOP_16	Workstation	Windows 8.1 Enterprise 64 (Build: 9200)	Encrypting	Encrypting
WIN_DESKTOP_17	Workstation	Windows 10 Pro (Version: 1807) (Build: 18363.893)	Encrypted disks	Encrypted disks
WIN_DESKTOP_18	Workstation	Windows 10 Pro (Version: 1807) (Build: 18363.893)	Encrypted (partially)	Encrypted (partially)
WIN_DESKTOP_19	Workstation	Windows 10 Pro (Version: 1807) (Build: 18363.893)	Encrypted disks	Encrypted disks
WIN_DESKTOP_2	Workstation	Windows 7 Ultimate 64 SP4	Encrypted (partially)	Encrypted (partially)
WIN_DESKTOP_23	Workstation	Windows 7 Ultimate 64 SP4	Encrypted disks	Encrypted disks
WIN_DESKTOP_29	Workstation	Windows 7 Ultimate 64 SP4	Encrypted disks	Encrypted disks
WIN_DESKTOP_3	Workstation	Windows 8.1 Enterprise 64 SP3 (Build: 9200)	Encrypted by the user (partially)	Encrypted (partially)
WIN_DESKTOP_4	Workstation	Windows 8.1 Enterprise 64 SP3 (Build: 9200)	Encrypted disks	Encrypted disks
WIN_DESKTOP_5	Workstation	Windows 7 Ultimate 64 SP4	Encrypted disks	Encrypted disks
WIN_DESKTOP_6	Workstation	Windows 8.1 Enterprise 64 SP3 (Build: 9200)	Encrypted (partially)	Encrypted (partially)
WIN_DESKTOP_7	Workstation	Windows 8.1 Enterprise 64 SP3 (Build: 9200)	Encrypted disks	Encrypted disks

Lista do computador mostrando o status de criptografia, os grupos aos quais pertencem, o sistema operacional e o método de autenticação usado.

PLATAFORMA DE GERENCIAMENTO EM NUVEM

Plataforma Aether

A plataforma Cloud Aether é comum a todas as soluções de endpoint da Panda Security. Ela simplifica a segurança, a avaliação de vulnerabilidades e o gerenciamento de patches. Com tudo isso e mais a supervisão e o gerenciamento de criptografia do Panda Full Encryption em todos os endpoints, permite que as empresas reforcem a postura de segurança, ao mesmo tempo, que agregam valor às próprias operações.

Gera Maior Valor em Menos Tempo. Implementação Fácil e Rápida

- Implementação, instalação e configuração em minutos. Veja valor desde o primeiro dia.
- Agente único, leve para todos os produtos e todas as plataformas (Windows, Mac, Linux e Android).
- Descoberta automática de endpoints desprotegidos. Instalação remota.
- Tecnologias exclusivas 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 flexível e modular que reduz o custo total de propriedade.
- Usuários com permissões e visibilidade totais ou restritas. Auditorias das atividades.
- Políticas de segurança para grupos e endpoints. Funções predefinidas e personalizadas.
- Inventários de hardware e software e registros de alteração.

Fácil Escalonamento de Capacidades de Segurança e Gerenciamento Ao Longo do Tempo

- Implemente módulos sem infraestruturas e custos adicionais.
- Comunicação com endpoints em tempo real a partir de um único console de gerenciamento na web.
- Painéis e indicadores detalhados para cada módulo.

O Panda Full Encryption é um módulo compatível com Panda Endpoint Protection, Panda Endpoint Protection Plus, Panda Adaptive Defense e Panda Adaptive Defense 360.

Sistemas operacionais compatíveis: [Windows](#).

Lista de navegadores compatíveis: [Google Chrome](#), [Mozilla Firefox](#), [Internet Explorer](#), [Microsoft Edge](#) e [Opera](#).