CHECK POINT

Check Point
Harmony
Secure Users & Access

Harmony Endpoint

Configurando a função Media Encryption

Autor: Lorena Freitas
Security Engineering Brazil
Dez/23

Configurando a função Media Encryption no Harmony Endpoint

O recurso de Media Encryption faz parte do pacote Data Protection do Harmony Endpoint, e permite o controle granular do uso de mídias removíveis. Protegendo, assim, os dados armazenados nas máquinas corporativas.

Ao utilizar um dispositivo de mídia removível, o usuário precisa criptografar o dispositivo, que passará a ter duas partições, uma restrita para dados corporativos e outra não criptografada, destinada ao uso para dados não corporativos. É possível a criação de regras distintas para acesso a essas partições.

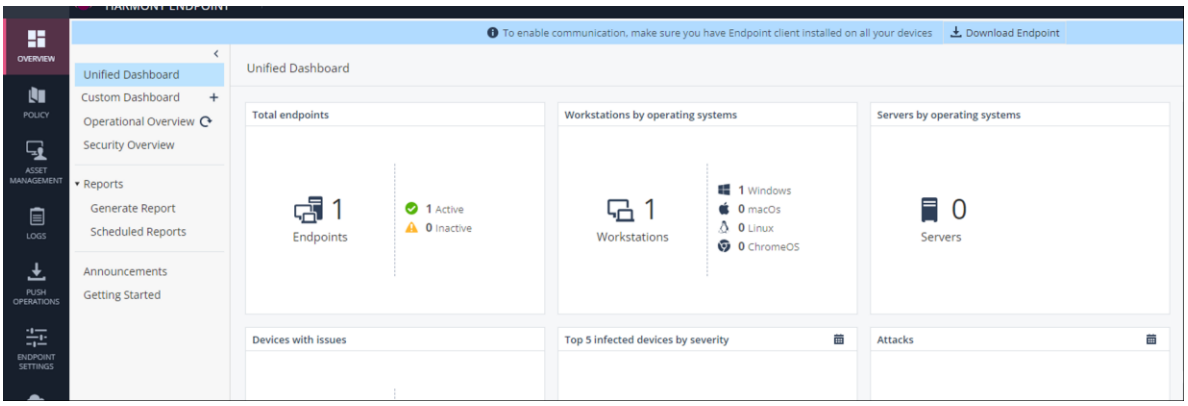
É recomendado não criptografar dispositivos removíveis que não sejam destinados a armazenamento, como: câmeras digitais, smartphones, MP3 e etc.

Para este tutorial foram utilizados os seguintes elementos:

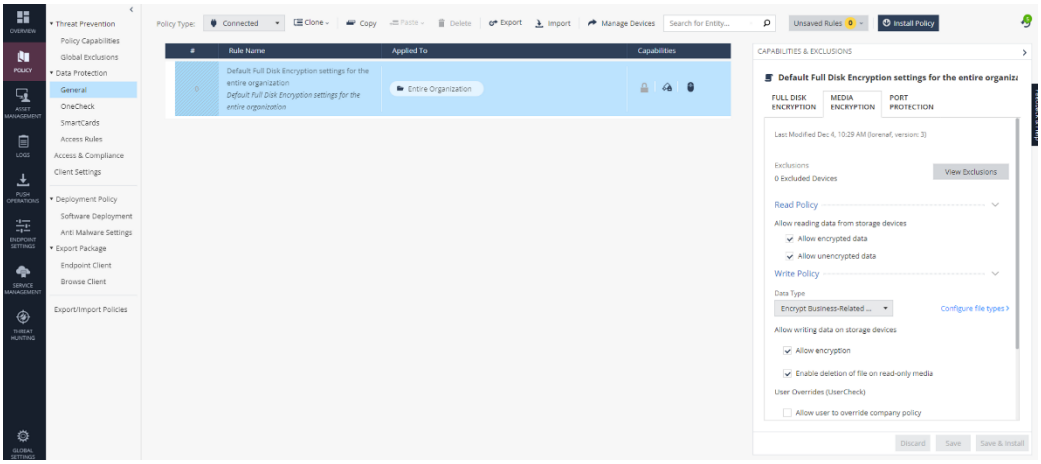
- Portal Infinity com licenciamento válido para o Harmony Endpoint;
- Desktop de usuário com Windows 11;
- Agente Harmony Endpoint versão 87.52.2005 (instalado no desktop de usuário);
- Pendrive Kingston 4GB;

A figura abaixo mostra o menu *Overview* do Harmony Endpoint, após a instalação do agente concluída.

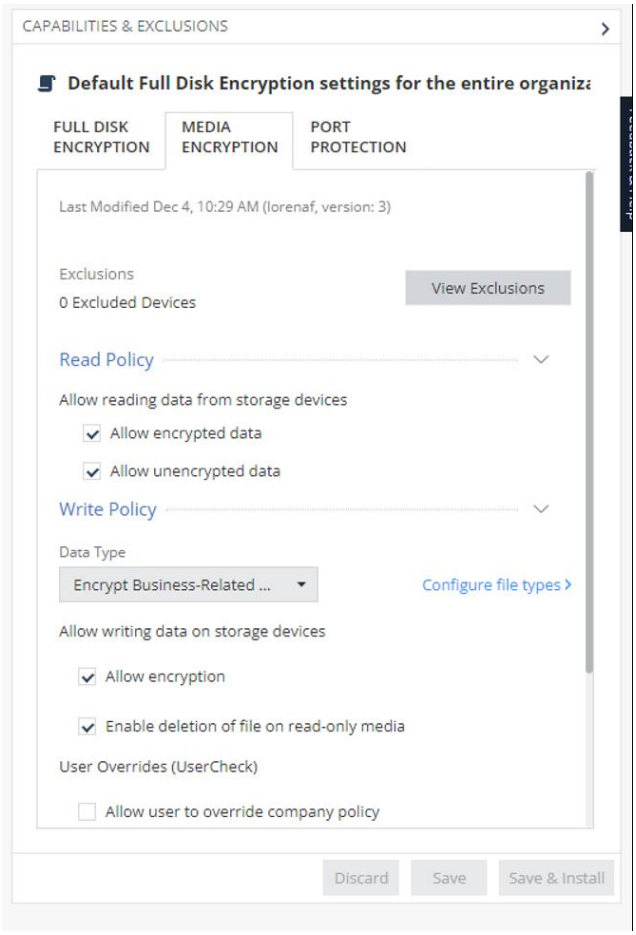
Mais detalhes em: https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Endpoint-Admin-Guide/Topics-HEP/Getting-Started.htm?tocpath=Getting%20Started%7C_____0



Para configurar a função Media Encryption, vamos acessar o menu *Policy* > *Data Protection*, conforme abaixo:



Acessar, então, a aba *Media Encryption* no menu *Capabilities & Exclusions* à esquerda.

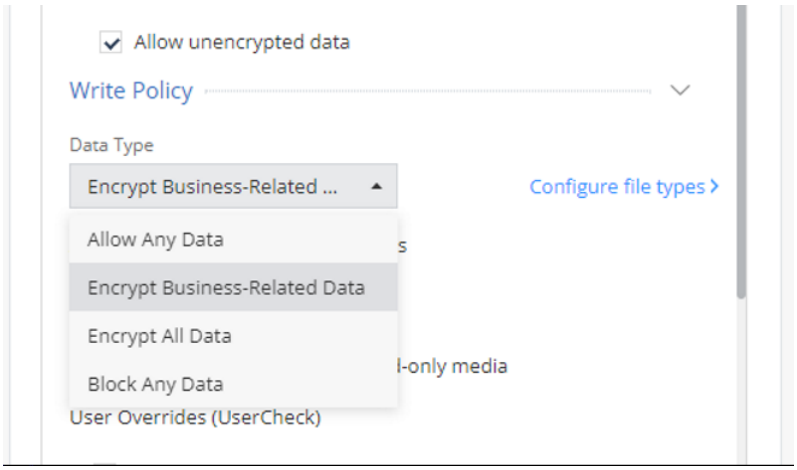


Neste menu, é possível configurar exclusões para as políticas de Media Encryption, além de permitir ou negar, a leitura de dados criptografados e não-criptografados nas mídias removíveis utilizadas na máquina do usuário.

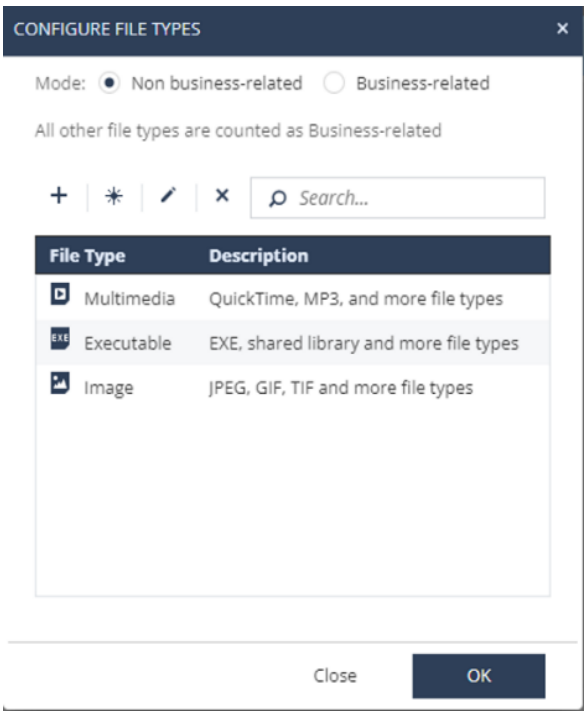
Para este tutorial, vamos configurar a função de escrita em mídias removíveis.

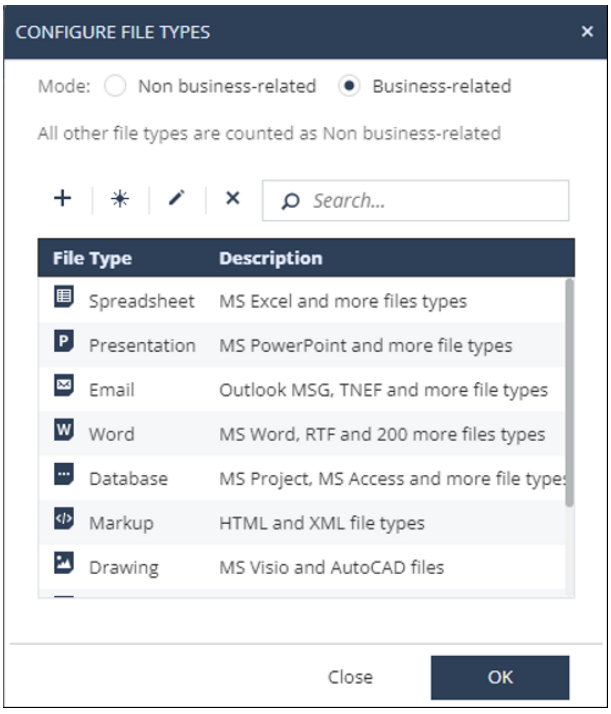
No campo *Data Type* em *Write Policy*, é possível definir as ações a serem tomadas quando o usuário fizer a escrita em uma mídia removível.

Vamos selecionar a opção *Encrypt Business-Related Data*, que permite a utilização de mídias removíveis, mas criptografa dados corporativos, impedindo que usuários não-autorizados tenham acesso a dados sigilosos.

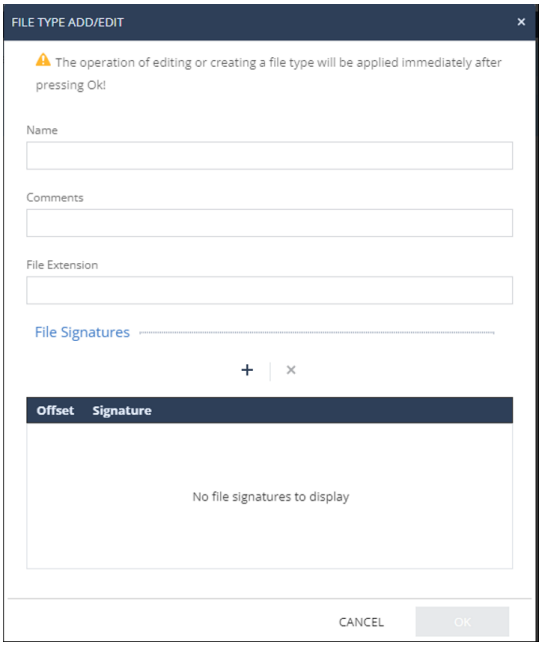


O campo *Configure file types* permite configurar quais tipos de arquivos serão considerados corporativos ou não-corporativos.

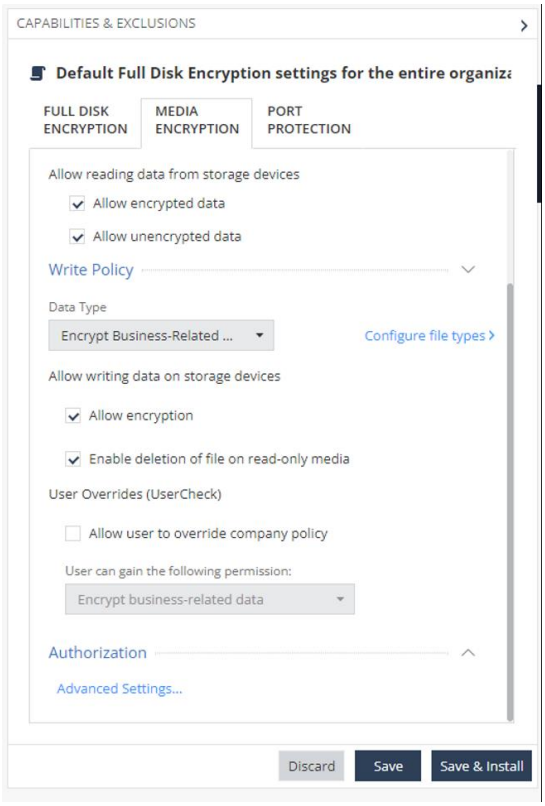




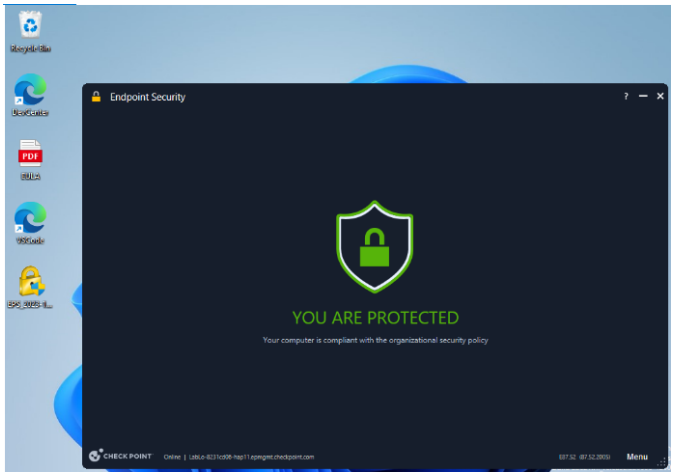
Em *Create a new file type* você pode criar um tipo de arquivo utilizando suas informações de extensão e assinaturas

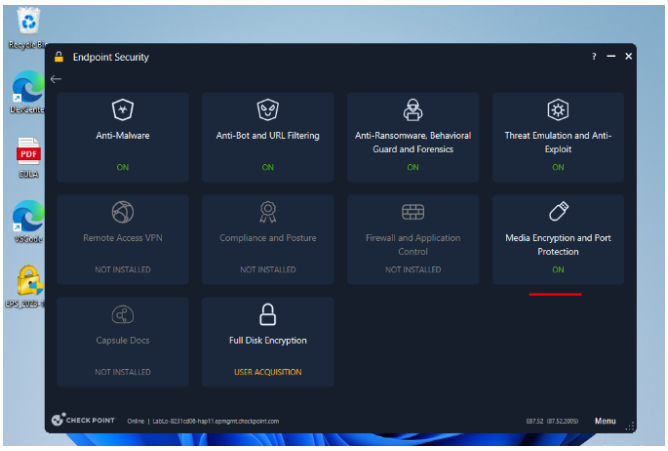


Vamos manter os file types padrão e clicar em Save & Install

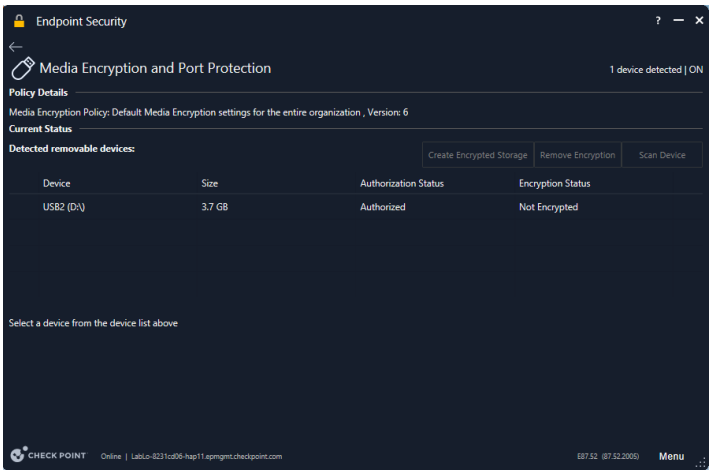


A seguir vamos utilizar o desktop de usuário com agente instalado, e verificar que a blade de Media Encryption está ativa.

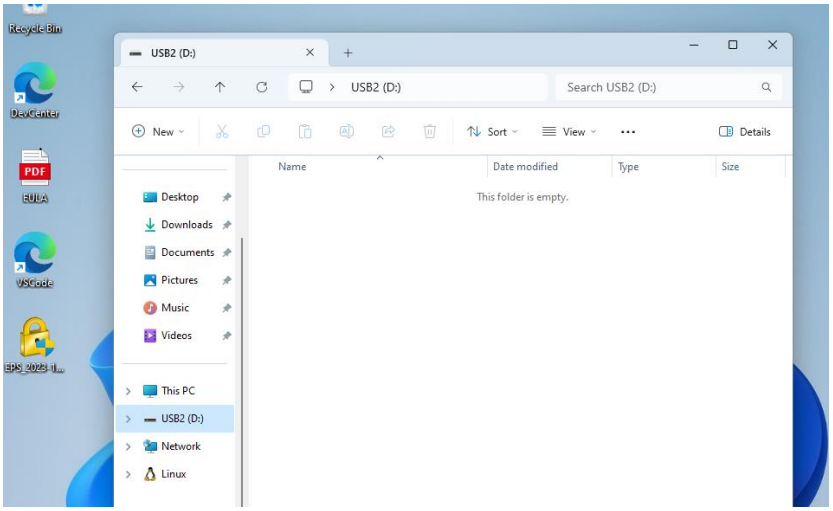




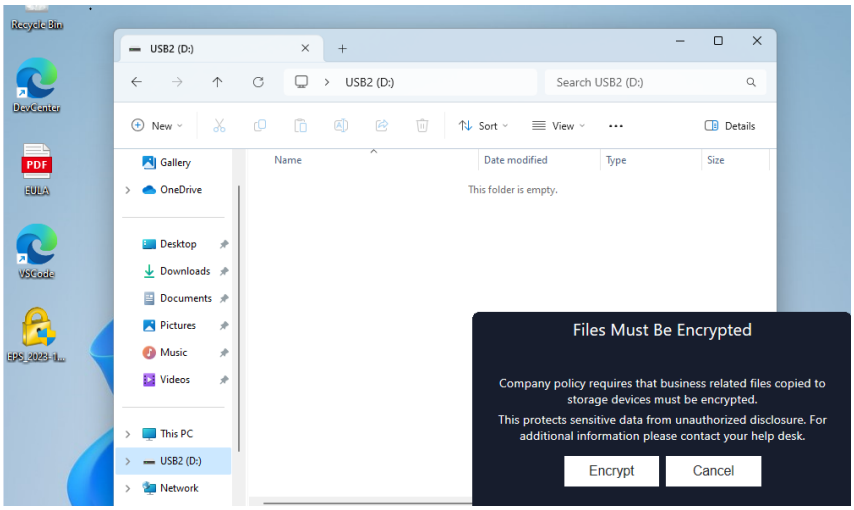
Ao acessar uma mídia removível, a blade de Media Encryption indica que o dispositivo precisa passar por um scan para liberar o acesso, note que o Encryption Status é não-criptografado.



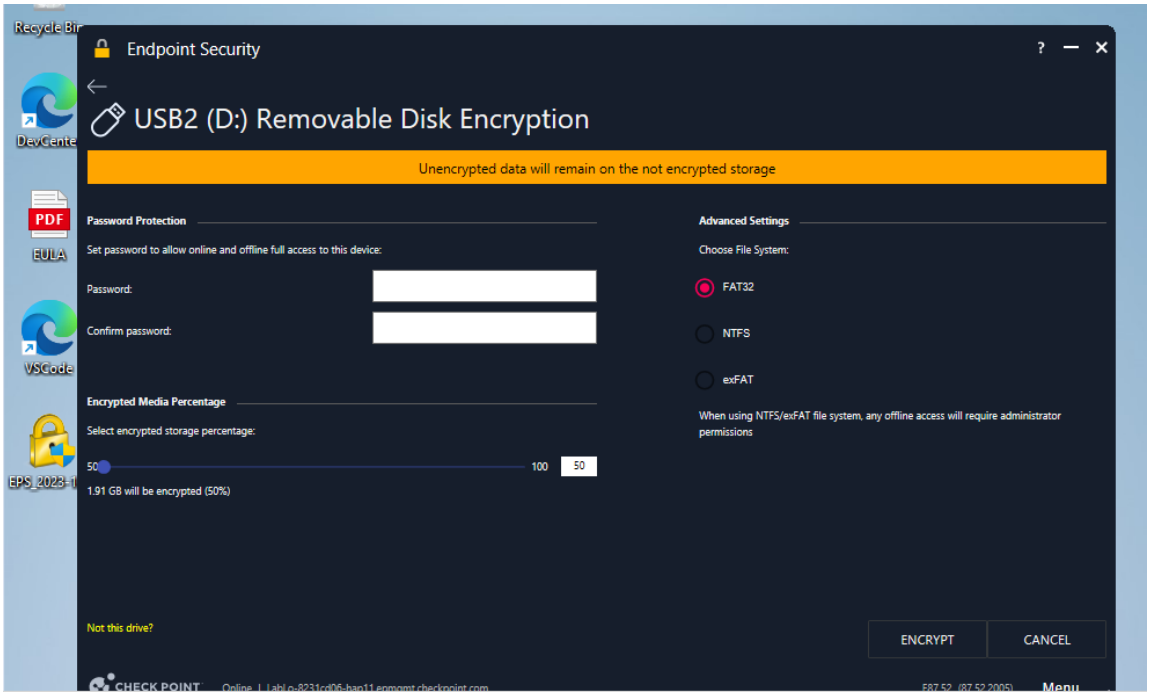
Na configuração da política, permitimos a leitura de dispositivos criptografados e não-criptografados. Assim, após o scan é possível abrir o pendrive.



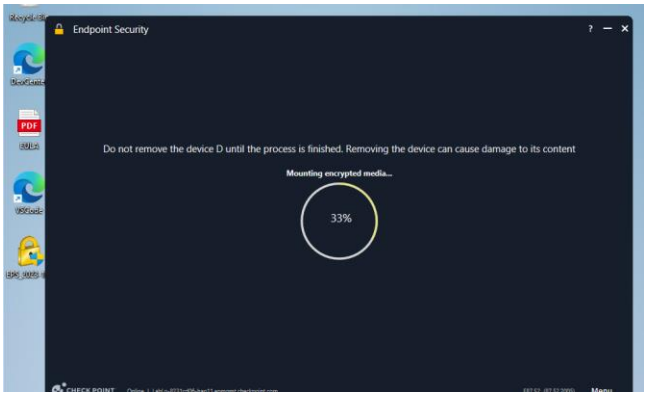
Porém, ao tentar copiar um arquivo do desktop para o pendrive, temos o trigger na política de escrita, que exige a criptografia da mídia removível.

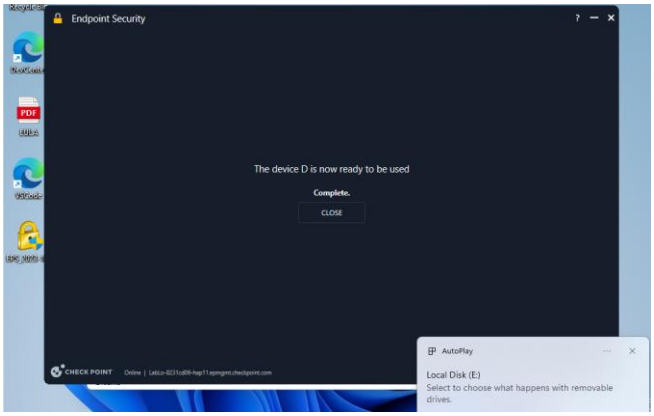


O usuário, então, precisa clicar em Encrypt e criar uma senha de acesso aos arquivos criptografados, que são os tipos de arquivos que indicamos com Business-Related na política.

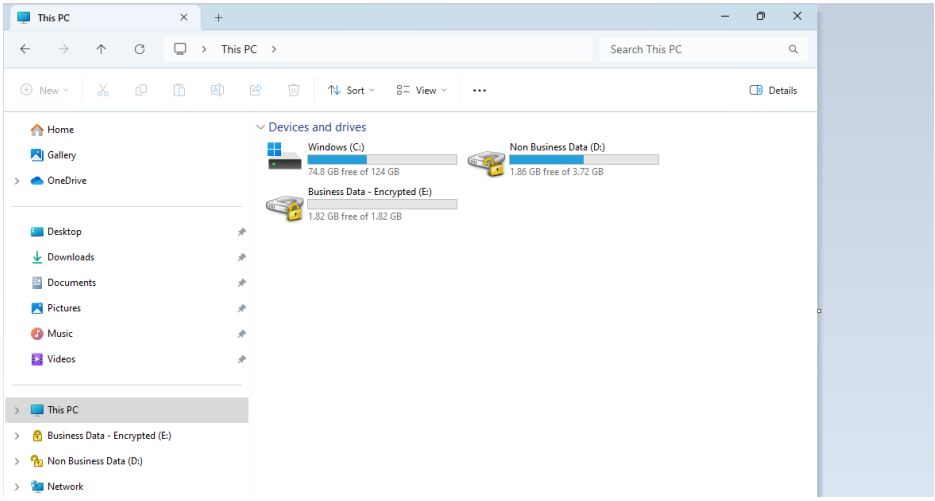


A partir desta configuração, a mídia removível será particionada em dois discos, e o usuário pode definir o tamanho do disco destinado aos dados corporativos, e o sistema de arquivo a ser utilizado. O usuário então, deve clicar em Encrypt e aguardar a finalização do processo.

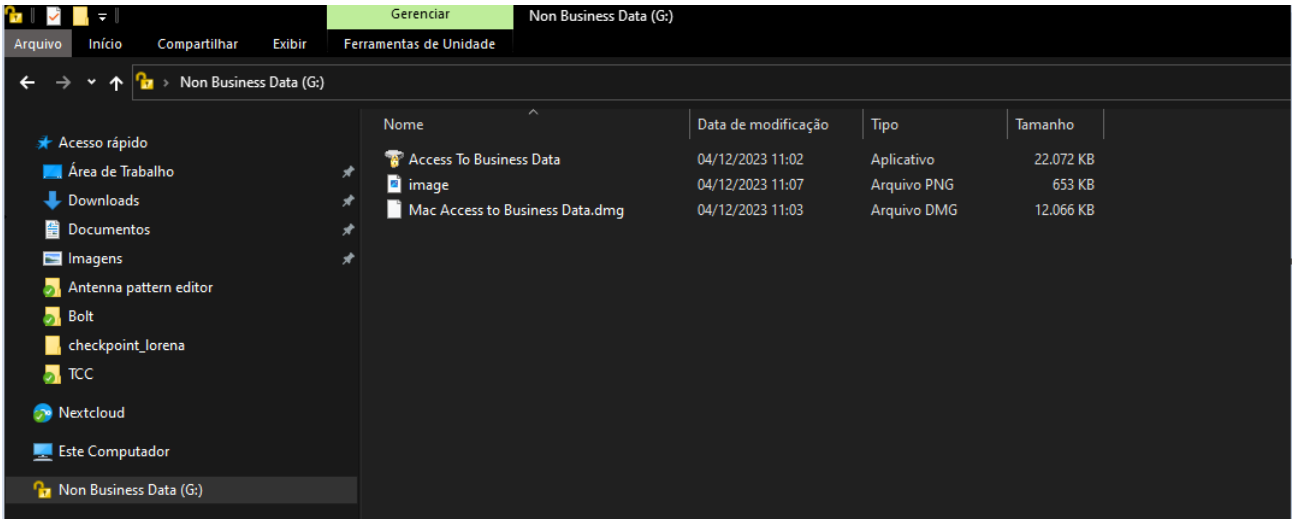




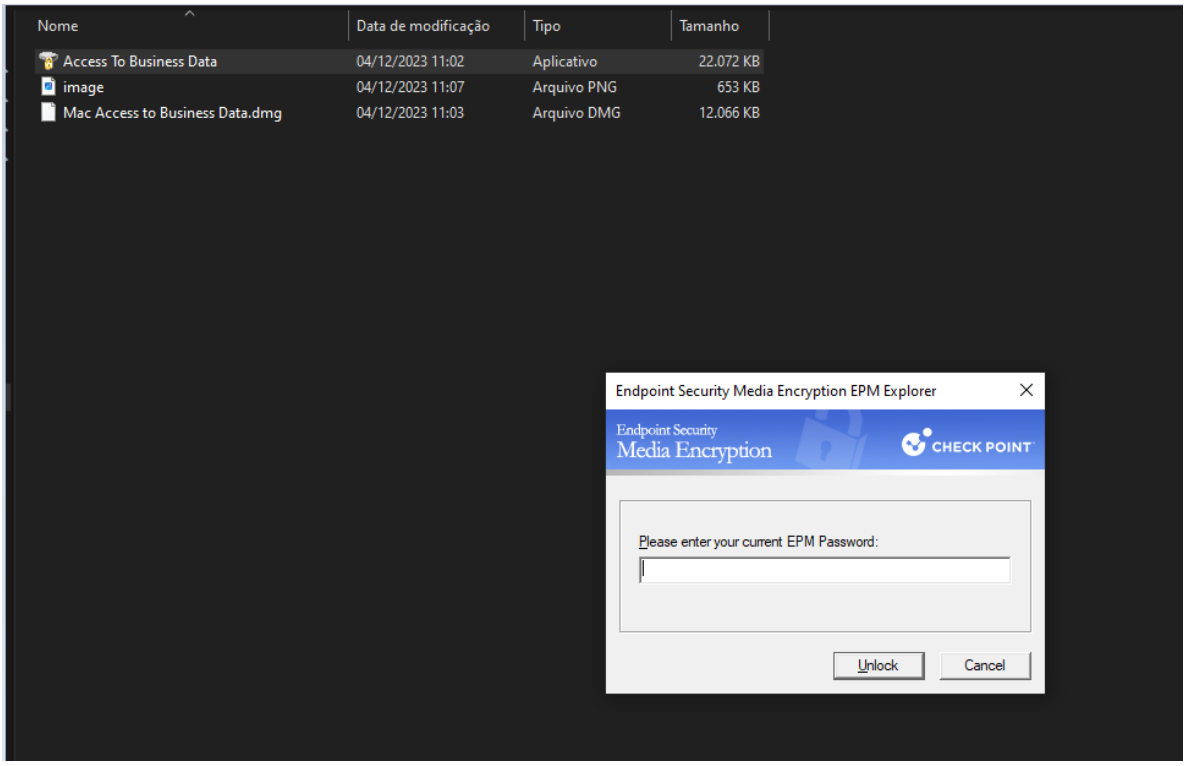
A partir disso, note que uma nova partição é criada.



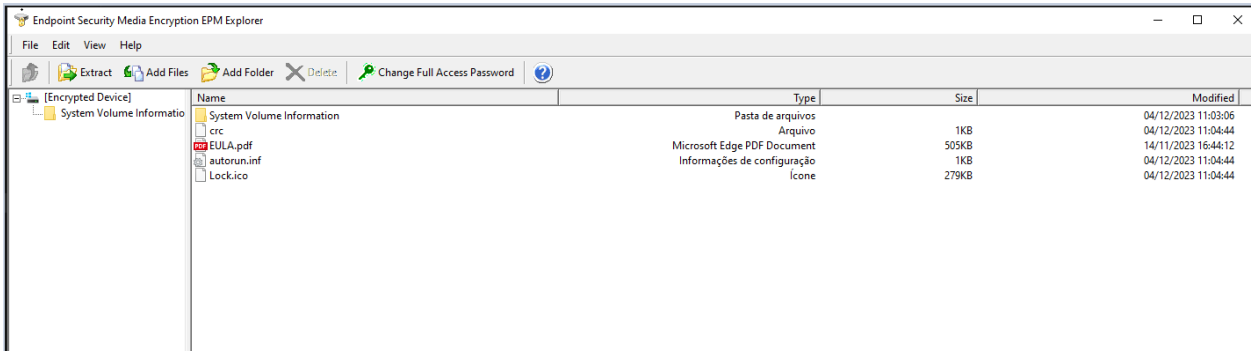
Ao abrir este pendrive em uma máquina sem o Harmony Endpoint, o acesso é liberado apenas para os arquivos não-corporativos, na imagem abaixo podemos ver um arquivo PNG com acesso liberado, já que o mesmo está classificado como non-business related na política.



Ao tentar acessar a partição criptografada, a senha configurada no momento da criptografia é solicitada.



Ao adicionar a senha e clicar em Unlock, a partição criptografada pode ser acessada normalmente. Neste exemplo temos um arquivo .pdf que estava classificado como corporativo em nossa política.



Este recurso do Harmony Endpoint, permite que o acesso a mídias removíveis seja liberado, porém com a proteção dos dados corporativos da companhia.

Este white paper foi escrito em dezembro de 2023, versões futuras estão sujeitas a alterações.