**Cybersecurity 401**

**Module 2 - Data Security**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# **Lab 08 - DLP and Classification**



### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

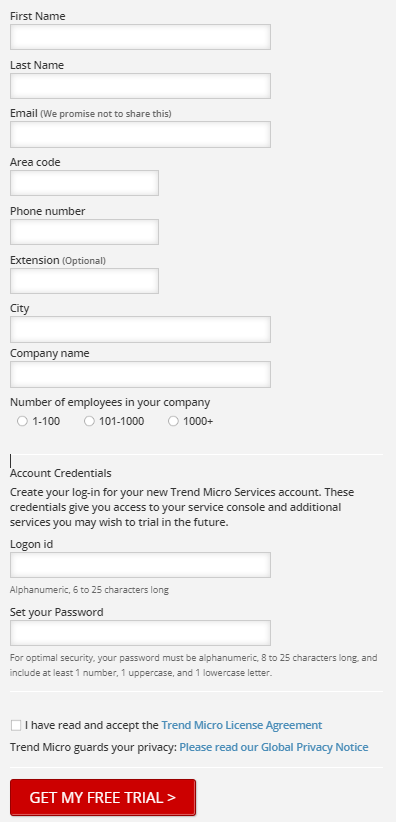
### 

### 

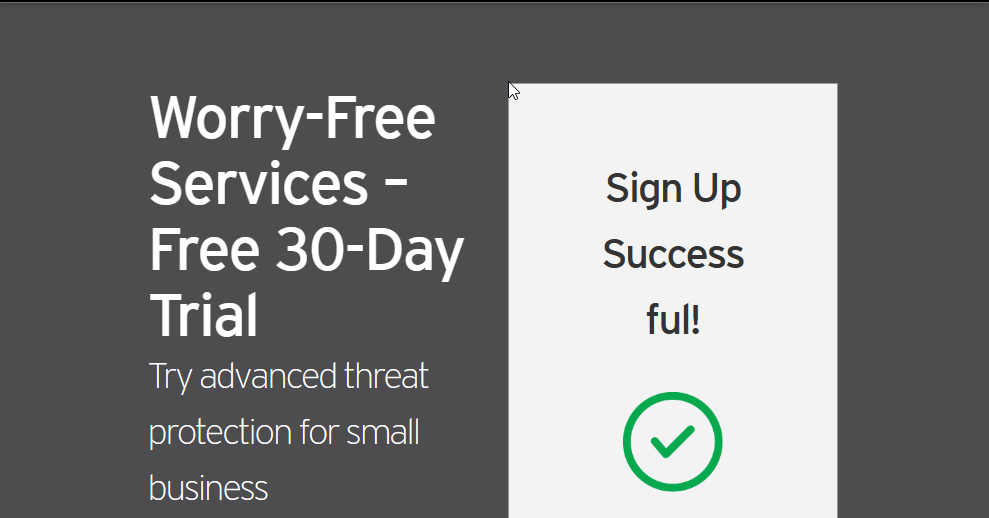
### 

### | Rodrigo Brasil 11/2023 |

### **Part 1: Staging**

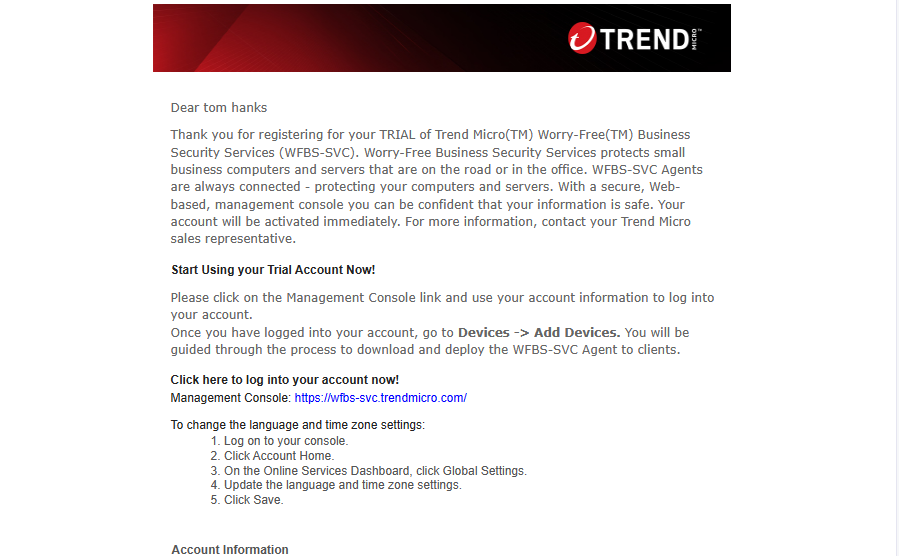


Sign up to a Free 30-day trial on trend micro.

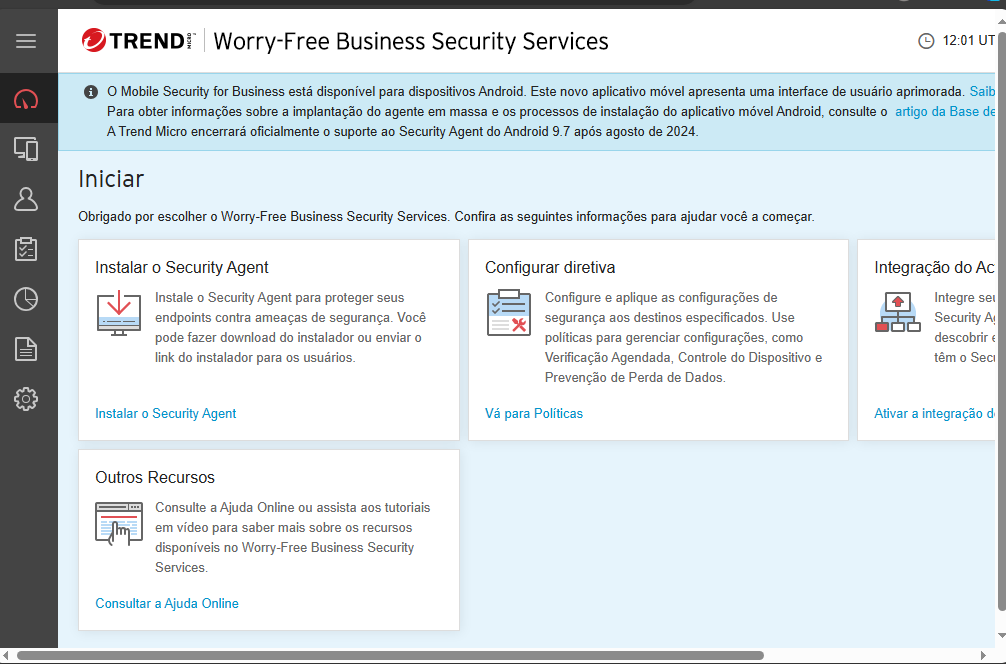


Free 30-day trial sign up done.

it was used a temporary email “[vilem86774@cabose.com](mailto:vilem86774@cabose.com)” to make a account



Email sent to the temporary mail



Trend Portal

### 

### 

### 

### 

### 

### 

### 

### 

### 

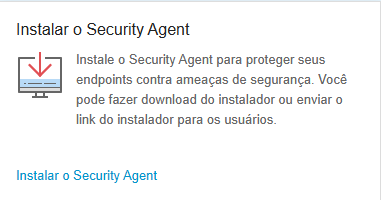
### 

### 

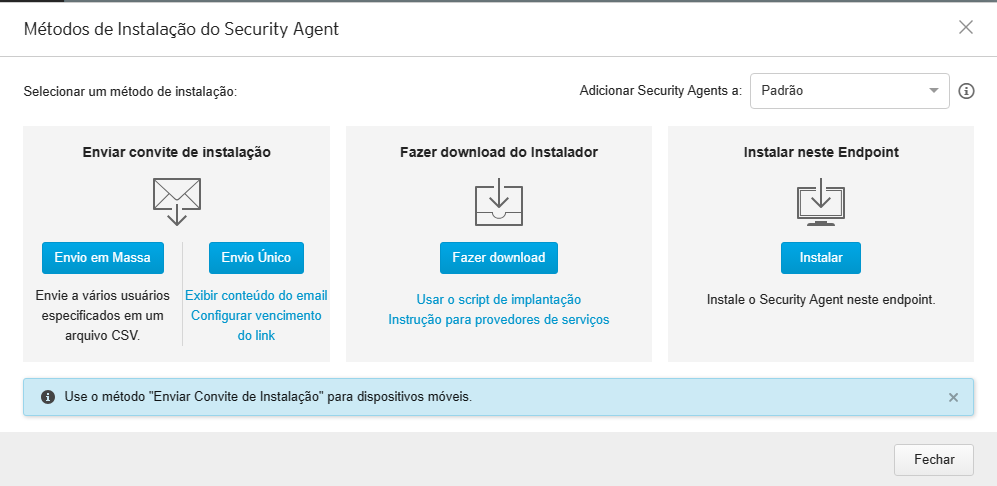
### 

### 

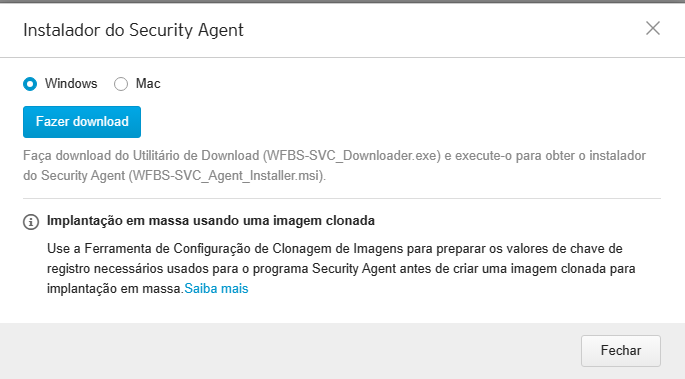
#### **Security Agent download and installation**



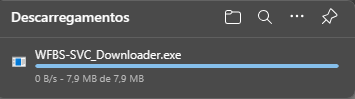
Inside the portal we will have an option to install the security agent



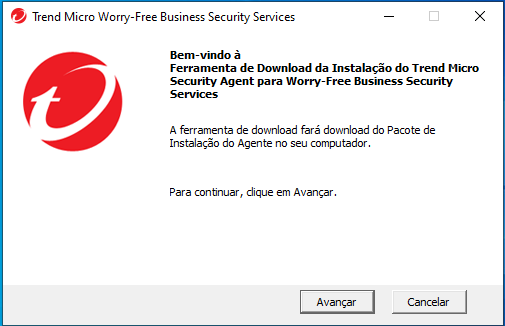
Inside this option It will ask what method we want do use, we will use the middle one to download



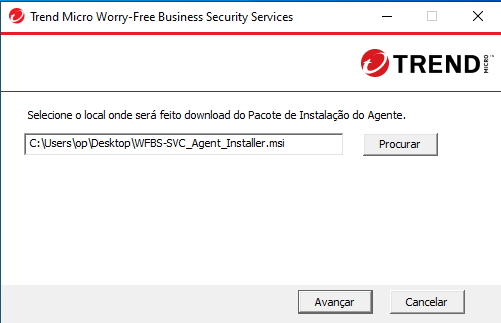
It will ask what operating system we want to download to, we will choose windows



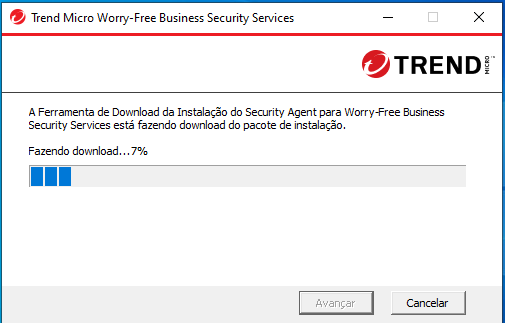
after clicking the blue download button, it will start to download



after downloading, we open the executable and will be welcomed with this message



after clicking next it will ask where do we want to store the installer, in this case it will store it in the desktop



after clicking next again it will start to download the installer

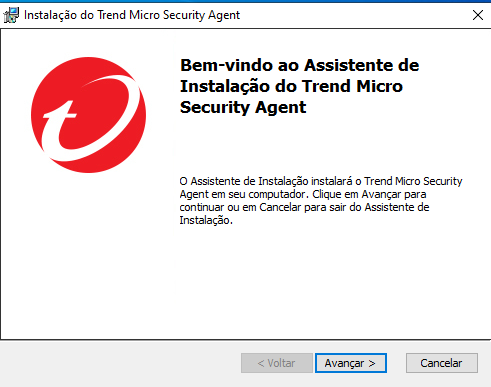
### 

### 

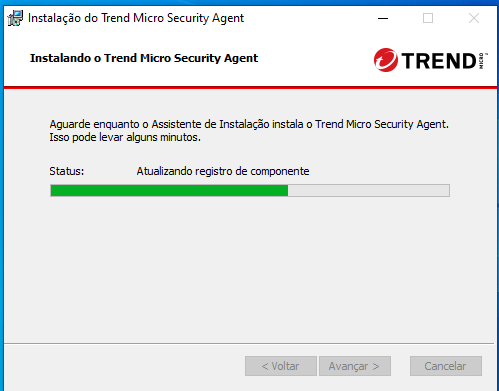
When the download ends it will show this message if we click the blue text it will open the folder where the installer was downloaded to

### 

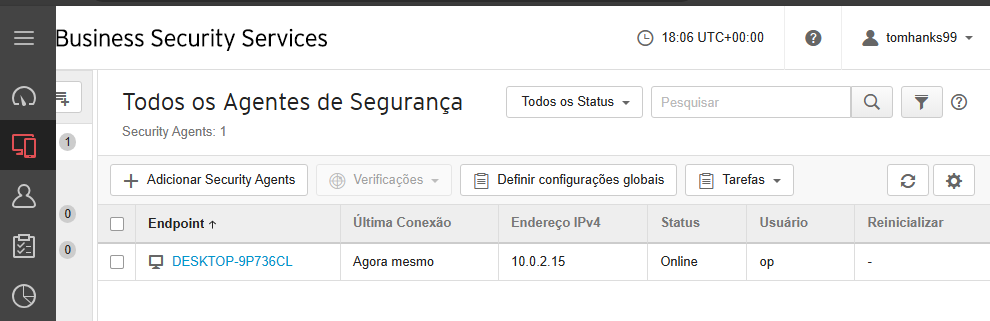
Now we must open the installer to finally install the agent



When we start the installer this will be the first message, click next to advance to the next step



after clicking next it will start installing the security agent, after it finishes it will close and it will be installed!



After installing the agent the VM will now appear on the portal under security agents

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

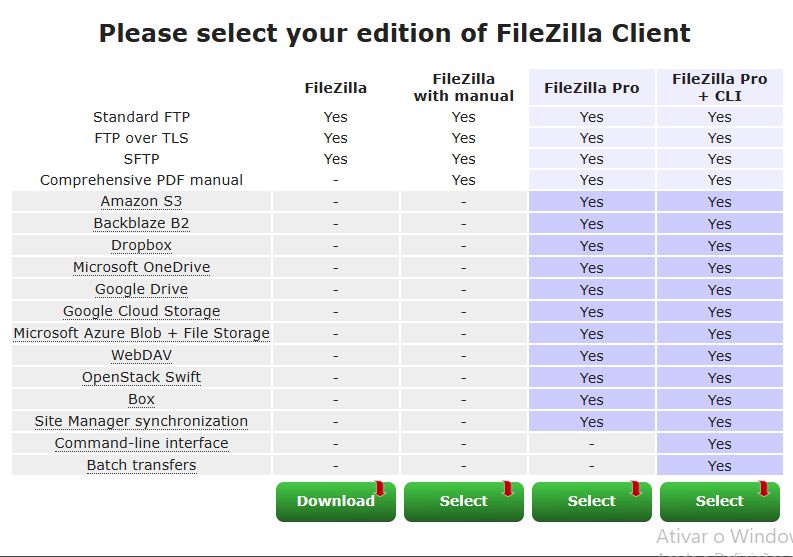
### 

### 

#### **FileZilla download and installation**



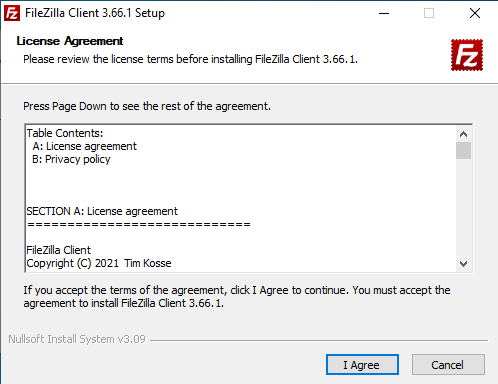
We will also need for this exercise FileZilla, it can be downloaded in this URL: <https://filezilla-project.org/download.php?type=client>



I will ask what version we want to download, we will simply download the first option for FileZilla by clicking on the green Download button



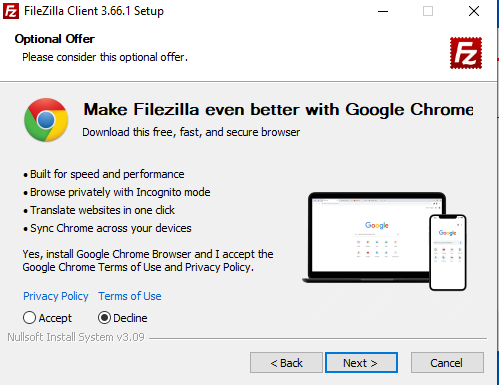
After clicking on the green button it will start downloading



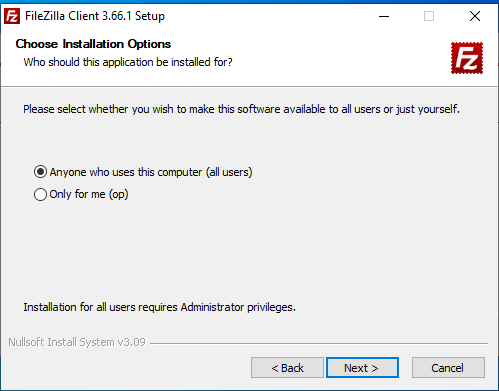
After downloading, start the executable to start the installation.

The license agreement will be the first thing that will appear when started.

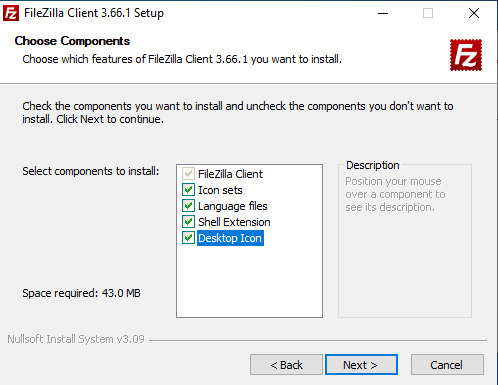
Click “I Agree” to start



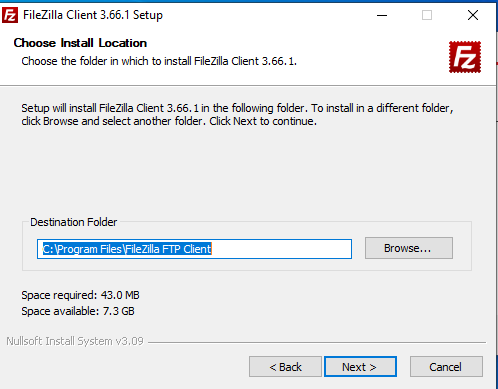
It will ask if we want to install google chrome as well, feel free to install it if you want to and click next.



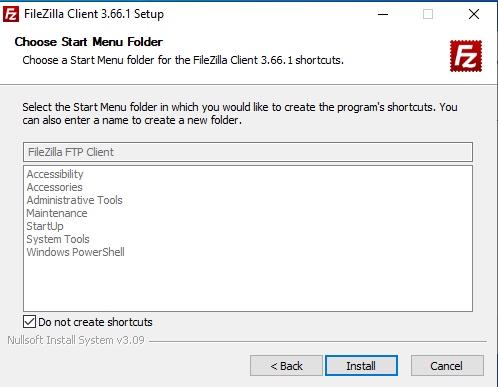
It will ask if you want to install filezilla for multiple users that are on the same machine or only the one you are currently using. In this case we only have one user so it makes no difference which option we chose.



Next it will ask to select components to install, we recommend selecting the desktop icon if it isn't already and click next.

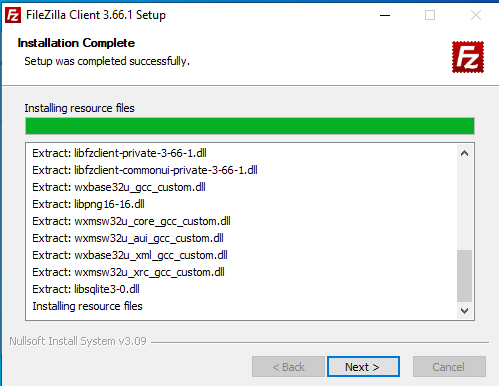


In this next step it will ask where you want to install it, for this exercise it will be left at its default destination.

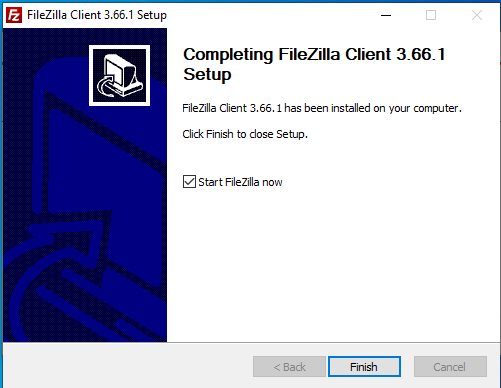


This step will ask if we want to create a start menu folder, its personal preference.

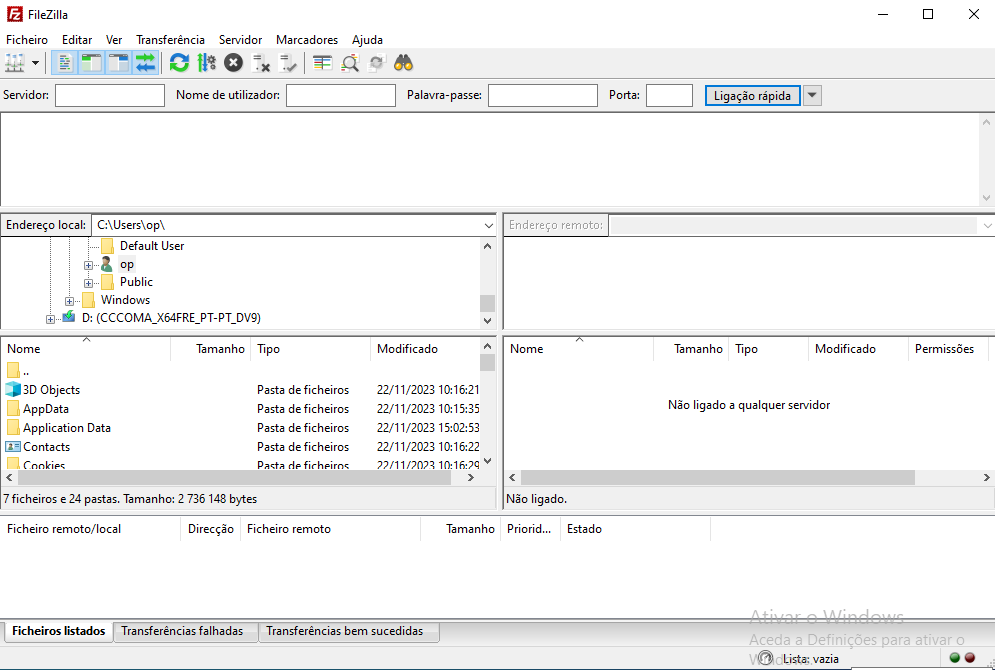
in this case the checkbox is checked to create.



After clicking next it will start installing filezilla



After installing it will say it is installed with a checkbox when clicking finish to open filezilla. we want to open filezilla so it will be left checked.



When filezilla opens it will look like this.

### **Part 2: Baseline Evaluation**

##### HTTP POST

##### HTTPS POST

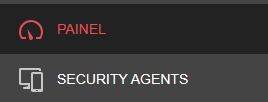
##### FTP Test using FileZilla

### 

### **Part 3: Endpoint DLP Policy Implementation with Trend Micro**

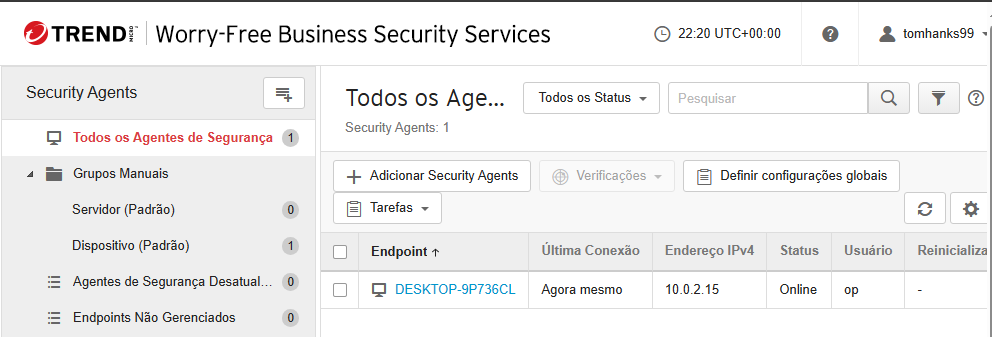


In the Trend Micro portal where we downloaded the security agent

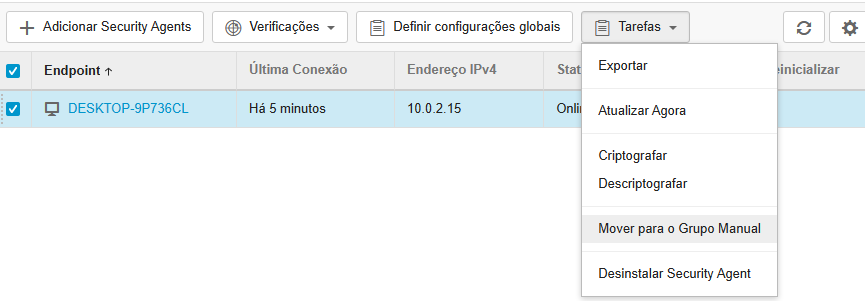


On the left side there will be multiple options to choose.

click on the security agents

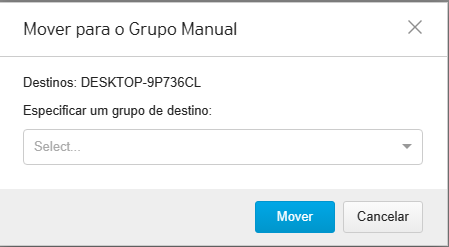


inside the security agents tab, it will look like this

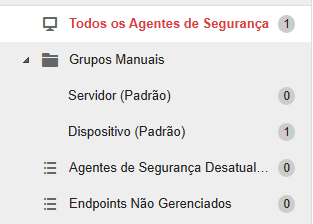


To configure its DLP policies we need to add it to a manual group first.

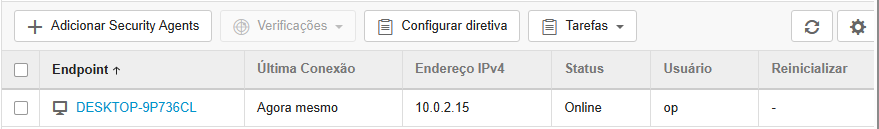
To do that select the right endpoint click on tasks and in the dropdown select move to manual group



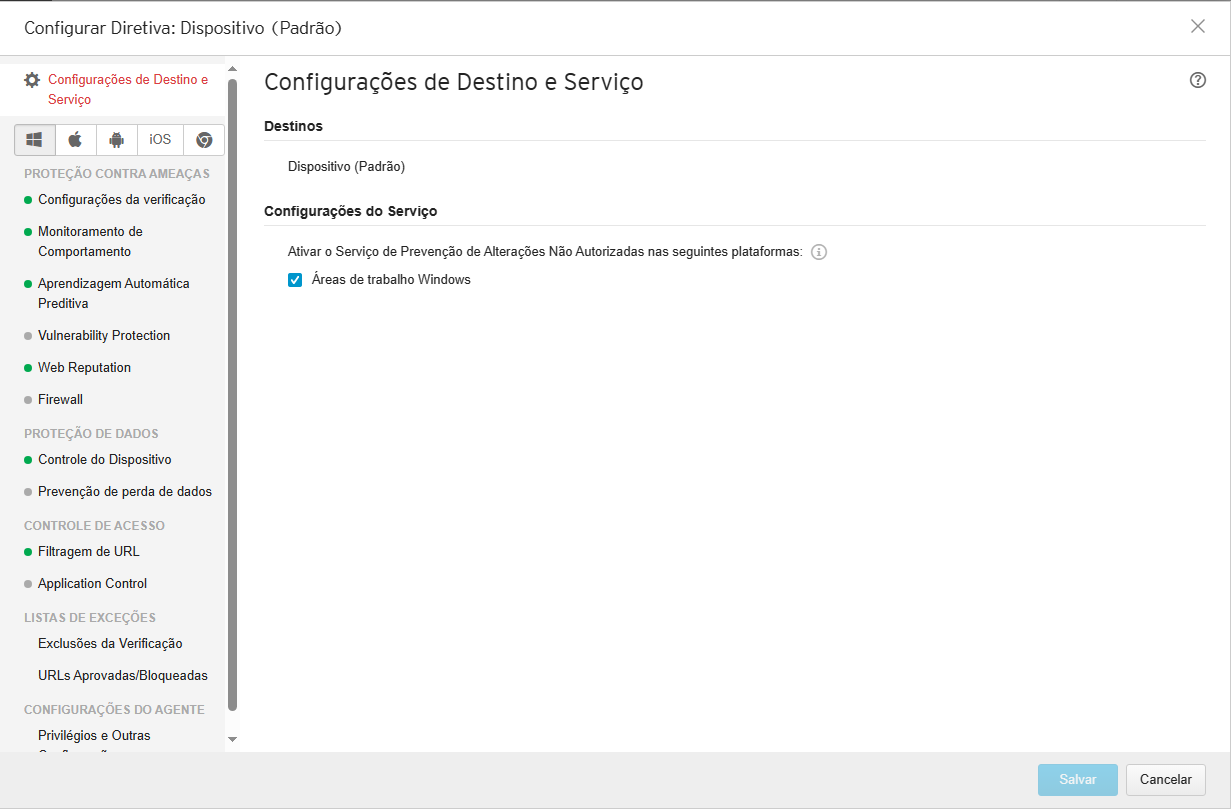
This message will pop up, simply click move, if you select a destination group it will be empty



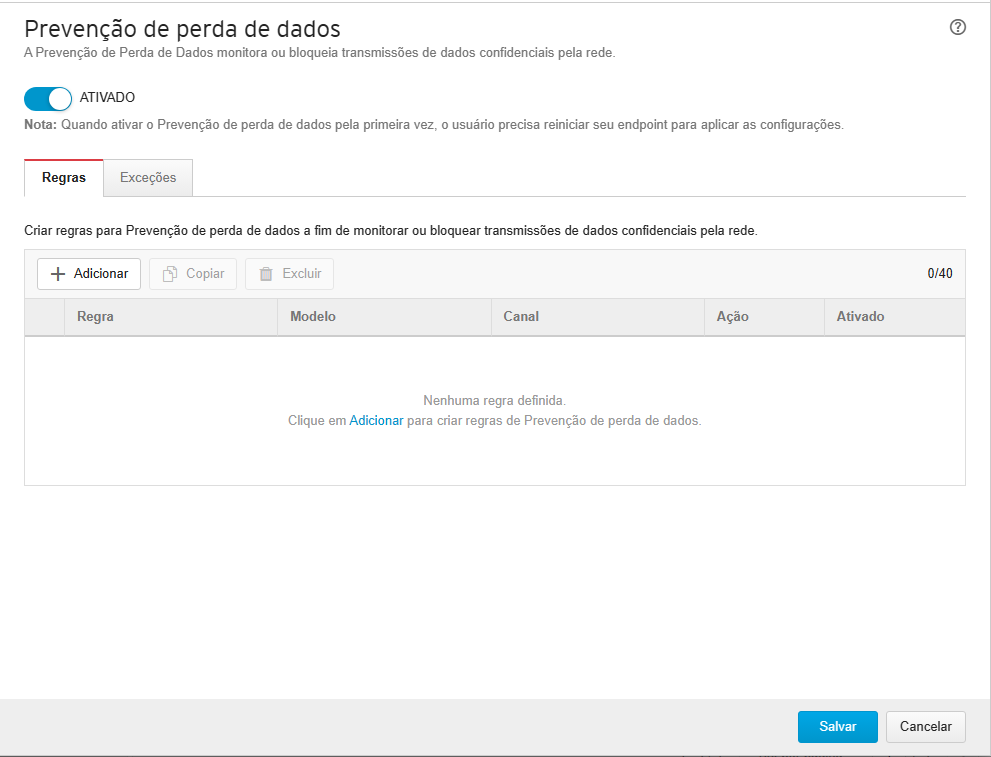
Now inside the manual groups there will be a endpoint inside the device



Inside it, it will look exactly like before but now there is a new option, select the endpoint and and click configure directive

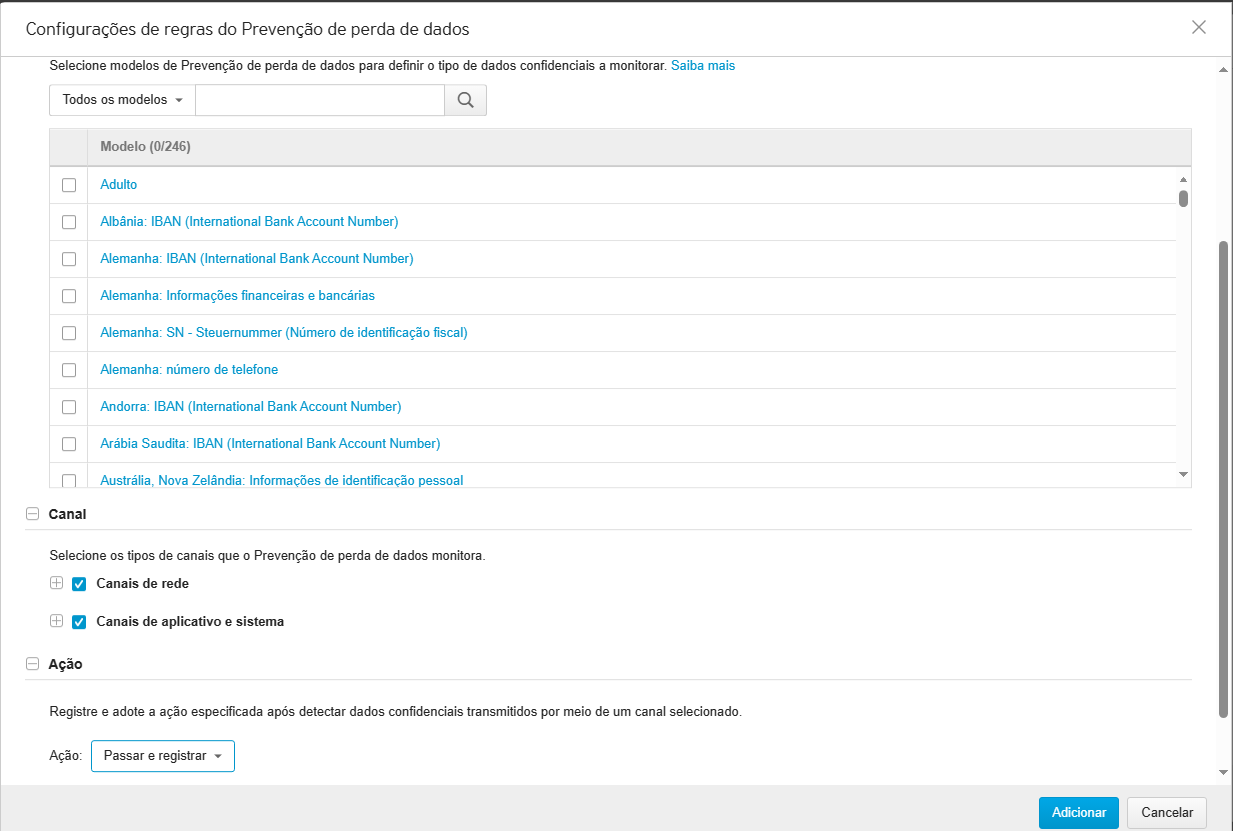


It will look like this, Under data protection there will be loss of data prevention

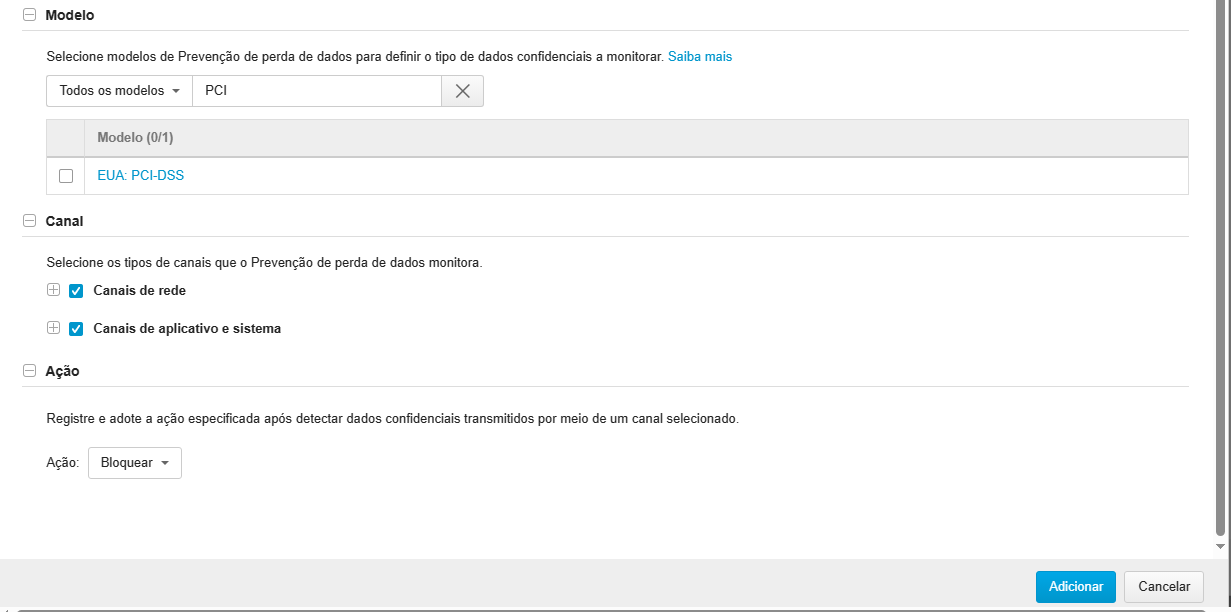


by default it’s turned off, turn it on.

To finally configure the policy we will create a new rule by clicking add



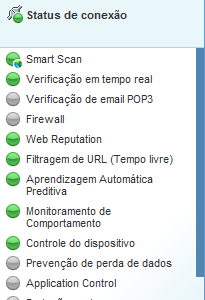
In the search bar type PCI-DSS, check the checkbox



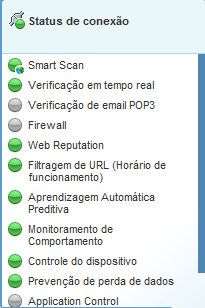
change the action to block, click add and save



After saving reboot the computer



For some reason after rebooting the computer, it refused to activate data loss prevention on the agent.



After leaving the VM on for a while it ended up finally activating data loss prevention on the agent.

Because of the policies I can not copy a credit card number or a social security number, so to test I will have to write them manually.

For some reason it still doesn't block any data

* HTTP POST
  + Test one sample SSN or CCN file
* HTTPS POST
  + Test one sample SSN or CCN file
* FTP Test using FileZilla
  + Test all sample SSN and CCN files