



CONSULTING



Malwarebytes

# SECURITY SUMMARY



<https://es.consulting>



[info@es.consulting](mailto:info@es.consulting)



+502 2375-7765

# Best Practices Review Malwarebytes Console

## CENDIS

### 1. Update Malwarebytes Agent

#### Endpoints

|   |
|---|
| DESKTOP-CR5IUNS.cendis.centrodistribuidor.com |
| GT_FSAL_TELE_05.cendis.centrodistribuidor.com |
| GT_FSAL_COOR_12.cendis.centrodistribuidor.com |
| GR_RETA_TELE_01.cendis.centrodistribuidor.com |
| GT_CUIN_AUXI_.cendis.centrodistribuidor.com   |
| DESKTOP-CR5IUNS.cendis.centrodistribuidor.com |
| GT_FSAL_TELE_05.cendis.centrodistribuidor.com |
| GT_FSAL_COOR_12.cendis.centrodistribuidor.com |
| GR_RETA_TELE_01.cendis.centrodistribuidor.com |
| GT_CUIN_AUXI_.cendis.centrodistribuidor.com   |
| DESKTOP-CR5IUNS.cendis.centrodistribuidor.com |
| GT_FSAL_TELE_05.cendis.centrodistribuidor.com |
| GT_FSAL_COOR_12.cendis.centrodistribuidor.com |
| GR_RETA_TELE_01.cendis.centrodistribuidor.com |
| GT_CUIN_AUXI_.cendis.centrodistribuidor.com   |
| DESKTOP-CR5IUNS.cendis.centrodistribuidor.com |

### Recommendation

Update the agent as it is the part of the software that is responsible for communicating with the Malwarebytes server and getting virus definition updates and other important updates. Make sure that the software has the latest version available to ensure optimal protection against malware threats and for this software to function properly on the system.





## 2. Assess Inactive Endpoints

Validate endpoint inactivity

| Inactive endpoints +2 weeks                   |
|---|
| DESKTOP-CR5IUNS.cendis.centrodistribuidor.com |
| GT_FSAL_TELE_05.cendis.centrodistribuidor.com |
| GT_FSAL_COOR_12.cendis.centrodistribuidor.com |
| GR_RETA_TELE_01.cendis.centrodistribuidor.com |
| GT_CUIN_AUXI_.cendis.centrodistribuidor.com   |

### Recommendation

Verify that the endpoint has an internet connection, and that the malwarebytes service is running, this to improve the connection between endpoint and console, this to have the detection record in real time.



<https://es.consulting>



[info@es.consulting](mailto:info@es.consulting)



+502 2375-7765

### 3. Perform scans

#### Endpoints

DESKTOP-CR5IUNS.cendis.centrodistribuidor.com

GT\_FSAL\_TELE\_05.cendis.centrodistribuidor.com

GT\_FSAL\_COOR\_12.cendis.centrodistribuidor.com

GR\_RETA\_TELE\_01.cendis.centrodistribuidor.com

GT\_CUIN\_AUXI\_.cendis.centrodistribuidor.com

### Recommendation

Run regular scans on Malwarebytes to detect and remove any malware threats that may have infected your computer. These scans can help identify and remove any malware that may be affecting your computer's performance or compromising your privacy and security.



<https://es.consulting>



[info@es.consulting](mailto:info@es.consulting)



+502 2375-7765

## 4. Remove threats that are in quarantine

| Threat name  | Category | Type          | Endpoint     | Location      | Date         |
|--------------|----------|---------------|--------------|---------------|--------------|
| PUP.Optio... | PUP      | Registry V... | GT_Dige_L... | HKU\S-1-5-... | 05/03/202... |
| Adware.Se... | Malware  | Registry V... | GT_CUIN_...  | HKU\S-1-5-... | 05/03/202... |
| Adware.Se... | Malware  | File          | GT_CUIN_...  | C:\USERS\...  | 05/03/202... |
| PUP.Optio... | PUP      | Registry V... | GT_Dige_L... | HK\S-1        | 05/03/202... |
| PUP.Optio... | PUP      | Registry V... | GT_Dige_L... | HK\S-1        | 05/03/202... |
| PUP.Optio... | PUP      | Registry V... | GT_Dige_L... | HK\S-1        | 05/03/202... |
| PUP.Optio... | PUP      | Registry V... | GT_Dige_L... | HK\S-1        | 05/03/202... |
| PUP.Optio... | PUP      | Registry V... | GT_Dige_L... | HK\S-1        | 05/03/202... |
| PUP.Optio... | PUP      | Registry V... | GT_Dige_L... | HK\S-1        | 05/03/202... |
| PUP.Optio... | PUP      | Registry V... | GT_Dige_L... | HK\S-1        | 05/03/202... |

## Recommendation

Delete quarantined files once you have confirmed that they are malware threats and you no longer need to keep them. This helps free up space on your hard drive and reduces the risk of files re-infecting your computer. For more information check the platform.





## 5. You have another antivirus or anti-malware installed

### Recommendation

Disable or remove an additional antivirus program to Malwarebytes since having these active at the same time in an endpoint can conflict since they constantly work to detect and eliminate malware and would be doing so at the same time, an antivirus can detect a file as malicious while that the other program marks it as safe. This can lead to slower system performance, file crashes, and other issues.

If in this case you want to leave the additional antivirus:

Turn off Windows Defender's on-access scanning feature because Malwarebytes works as the primary antivirus program on your computer.

Attached is how to create exclusions in windows for McAfee:  
<https://service.malwarebytes.com/hc/en-us/articles/4413789721235>

## 6. Perform resets required by Malwarebytes

### Recommendation

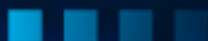
Malwarebytes may require a system reboot to install important software updates and also after a scan to complete the removal of any remaining malware files and fully clean your computer.

### General recommendations

Coordinate with the users that it is necessary to carry out these procedures so that the Malwarebytes protection can cover the endpoint and likewise will be protecting the information assets that they manage within the company.

Delete the agent in the endpoints that are not being used and add the agent to the endpoint that they are using, remembering that additional antivirus configurations must be made and in Mac devices give full access to the disk.

\*general recommendations depend on the client



## CONFIDENTIAL

This communication contains privileged, reserved and confidential information for the exclusive use of the recipient. Distribution, disclosure, dissemination, copying or other use by third parties is prohibited.



<https://es.consulting>



[info@es.consulting](mailto:info@es.consulting)



+502 2375-7765