Malwarebytes Cloud Server Report

Account: Malwarebytes SE Tenant
Group: All
Licensed Product: Endpoint Protection and Response (EPR)

Report period ● Start Monday, December 17, 2018 ● End Tuesday, January 15, 2019

Executive Summary

Active endpoints less than 80%

Active endpoints are those that have connected to the Malwarebytes Cloud within the last **72 hours**. The current percentage of active endpoints is low and should be investigated.

Consider removing old endpoints that might have been decommissioned or no longer valid.

Scan needed endpoints over 40%

48% of the endpoints have not performed a scan in more than 7 days. This is possible for different reasons. For example, they are not in a policy with a regular scan schedule. Another reason is that the endpoints are offline when a scheduled scan is due. The Excel Addin has a feature to initiate bulk scan under Endpoints Computers → Take Status Actions.

Detected threats for this period

These are the threats detected for the time period and endpoints selected.

Category	Detection Count
Malware	24
PUP	13
Ransomware	5
Website	4
Exploit	3
Grand Total	**49**

61
Installed Endpoints

39 / 64%
Active Endpoints

61 / 12%
Licenses Used of 500

517 Days
License Expires In

29 / 48%
Scan Needed

4 / 7%
Remediation Required

1 / 2%
Reboot Required

5 / 8%
Suspicious Activities

0%
Isolated/Quarantined

49
Total Detections

London UK >> Claudio Lab
Most At-Risk Group

clavictone
Most At-Risk Endpoint

Endpoints Action Status

These are endpoints with statuses requiring actions or additional investigations.

Scan Needed

These are endpoints that have not ran a Malwarebytes scan for more than 7 days.

Remediation Required

The endpoints have threats that were detected during scans that need to be remediated.

Reboot Required

These endpoints should be restarted to completely quarantine items found during scans, or to complete Malwarebytes software installations and updates, or to install Malwarebytes software updates.

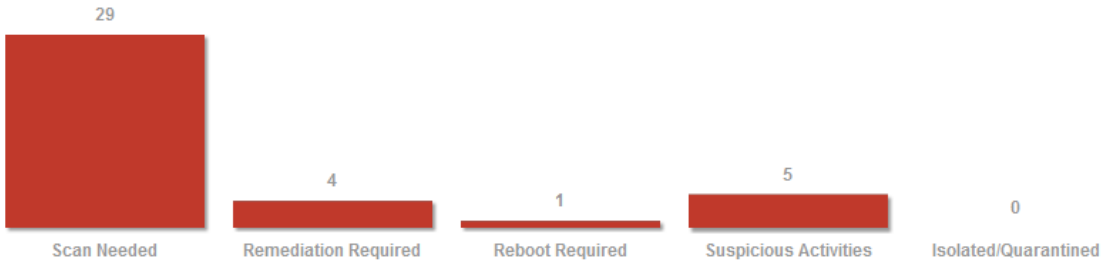
Suspicious Activities

Suspicious activities were detected on these endpoints. Note that this is only available if there is a subscription to the Endpoint Protection and Response (EPR) module.

Isolated/Quarantined

These endpoints are currently isolated (quarantined). Note that this is only available if there is a subscription to the Endpoint Protection and Response (EPR) module.

Action Needed Status	Endpoint Count	Endpoint Percentage
Scan Needed	29	48
Remediation Required	4	7
Reboot Required	1	2
Suspicious Activities	5	8
Isolated/Quarantined	0	0

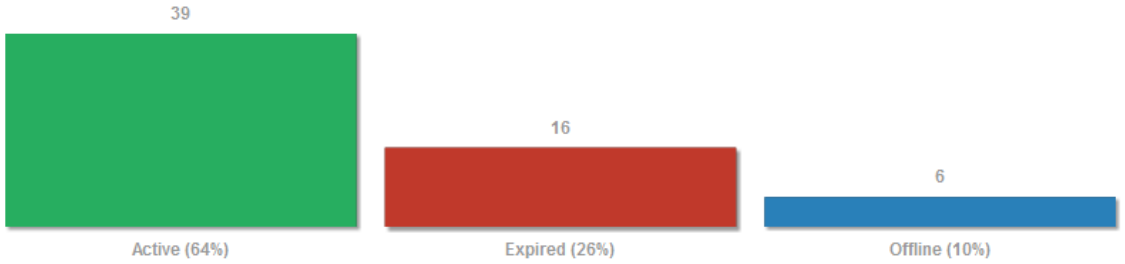


Endpoints Check-In Status

This is a report of all the check-in statuses of the endpoints.

- Endpoints that have checked in within the last **72** hours (**3** days) are considered **Active**.
- Endpoints that have not checked in in the last **720** hours (**30** days) are considered **Expired**.
- Endpoints checked in between these 2 thresholds are considered **Offline**.

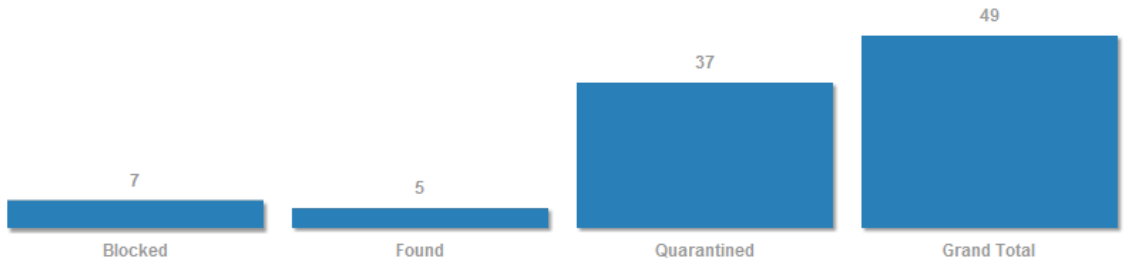
Endpoint Checkin Status	Status Count
Active (64%)	39
Expired (26%)	16
Offline (10%)	6
Grand Total	**61**



Statuses of Detected Threats

These are the detected threats and their statuses.

Blocked	Found	Quarantined	Grand Total
7	5	37	49

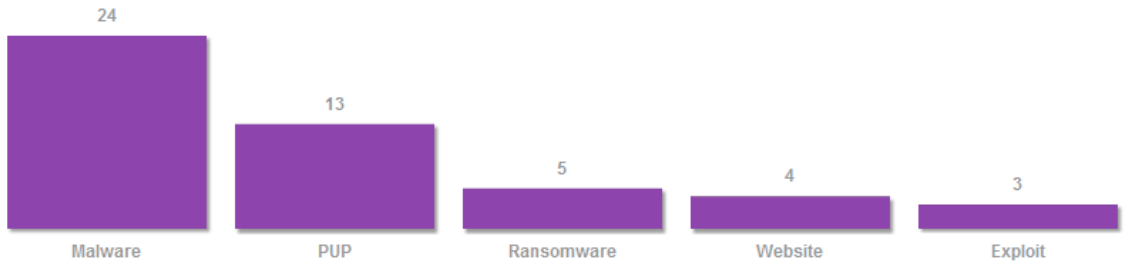


Threat Categories

Cybercriminals design threats to compromise computer functions, steal data, bypass access controls, and otherwise cause harm to the host computer, its applications or data.

Malwarebytes classifies the many types of threats into several different high level categories for easy overview.

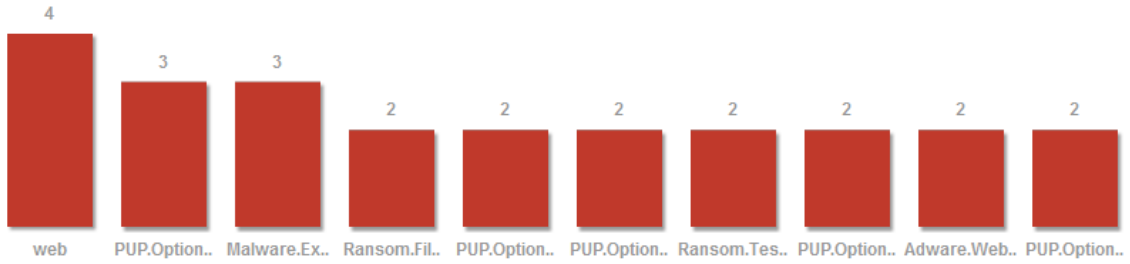
Category	Detection Count
Malware	24
PUP	13
Ransomware	5
Website	4
Exploit	3
Grand Total	**49**



10 Most Detected Threats

These are the top 10 most detected threats. The threats are either Blocked, Quarantined, Deleted, Restored, Cleaned, or simply Found with no remediation actions taken.

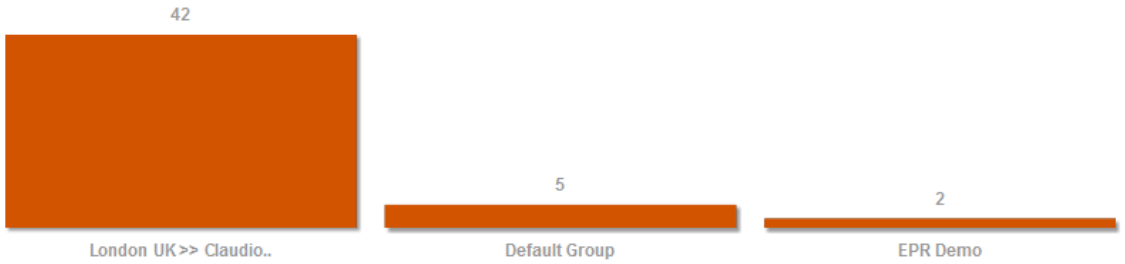
Threat Name	Detection Count
web	4
PUP.Optional.SearchManager	3
Malware.Exploit.Agent.Generic	3
Ransom.FileCryptor	2
PUP.Optional.SofTonic	2
PUP.Optional.Delta	2
Ransom.TeslaCrypt	2
PUP.Optional.InstallCore	2
Adware.WebCake	2
PUP.Optional.OpenCandy	2
Grand Total	**24**



10 Most At Risk Computer Groups

These are the top 10 computer groups with the highest incident counts, or number of detected threats. The report does not take into account threat severity and nature. Nonetheless, it is a good indication of groups that should be monitored closely.

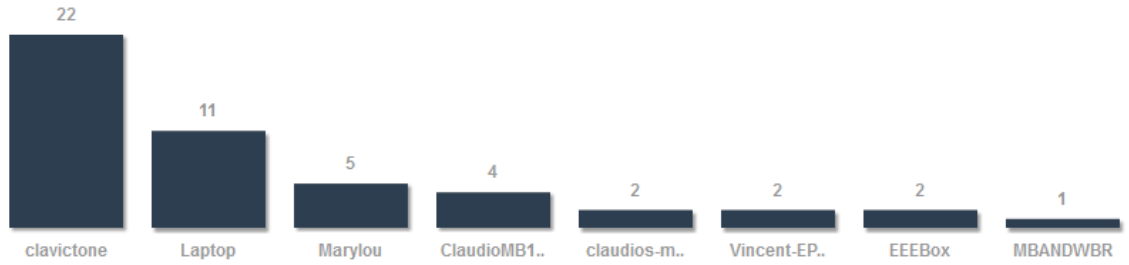
Group Name	Detection Count
London UK >> Claudio Lab	42
Default Group	5
EPR Demo	2
Grand Total	**49**



10 Most At Risk Endpoints

These are the top 10 endpoints with the highest incident counts, or number of detected threats. The report does not take into account threat severity and nature. Nonetheless, it is a good indication of endpoints that should be monitored closely.

Machine Name	Detection Count
clavictone	22
Laptop	11
Marylou	5
ClaudioMB1.claudiolab.local	4
claudios-macbook-pro.local	2
Vincent-EPR	2
EEEBox	2
MBANDWBR	1
Grand Total	**49**



Endpoints Online

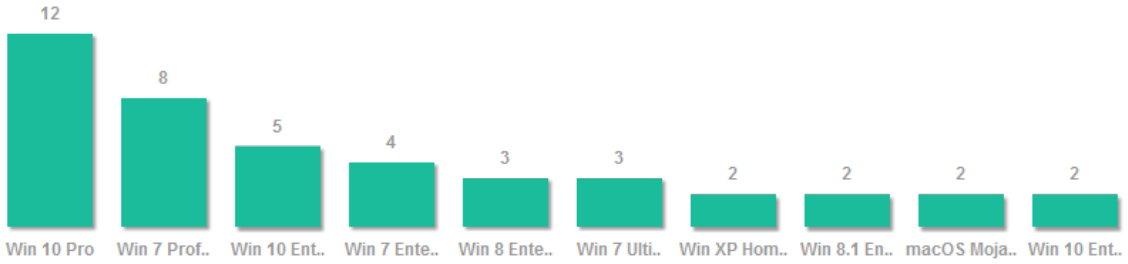
This is a report of all the endpoints that are currently active and online. These endpoints have communicated with the Malwarebytes server, or have sent a keepalive signal in the last few minutes.

Online	Endpoint Count
False (54%)	33
True (46%)	28
Grand Total	**61**

Endpoint Operating Systems

Malwarebytes supports Windows and macOS operating systems including the different variants and versions. The following operating systems and variants are being protected by this server.

Operating System	Endpoint Count
Win 10 Pro	12
Win 7 Professional	8
Win 10 Enterprise	5
Win 7 Enterprise	4
Win 8 Enterprise	3
Win 7 Ultimate	3
Win XP Home Edition	2
Win 8.1 Enterprise	2
macOS Mojave 10.14.2	2
Win 10 Enterprise N	2
Grand Total	**43**

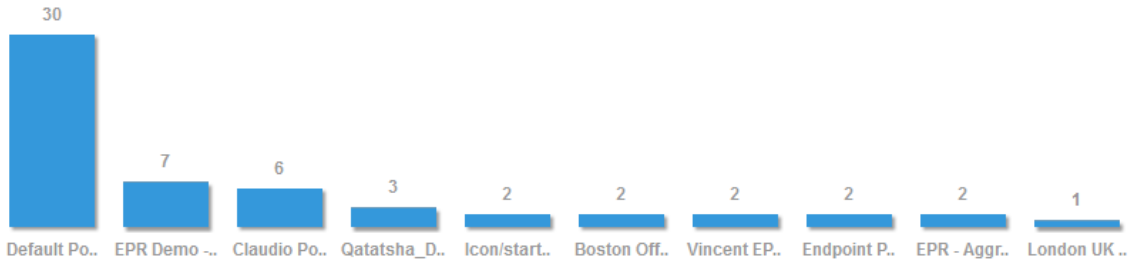


Top 10 Policies

The Malwarebytes endpoints are controlled through policies configured on the Malwarebytes Cloud server.

These are the policies associated with the most endpoints

Policy Name	Endpoint Count
Default Policy	30
EPR Demo - Realtime Protection OFF	7
Claudio Policy Test	6
Qatatsha_Demo	3
Icon/startup test policy	2
Boston Office	2
Vincent EP Layer Demo	2
Endpoint Protection	2
EPR - Aggressive Mode	2
London UK Default	1
Grand Total	**57**



End Report

Report generated on Tuesday, January 15, 2019 9:56 PM (Pacific Standard Time UTC-08:00)

Generated by lwei@malwarebytes.com