Getting Started with Your Malwarebytes Trial

1 Activate Your Account

a. Check for a Malwarebytes invitation email via the address you provided, and click **Verify**
b. When prompted, type in your name as you'd like it displayed in the management console, and create your password
c. Confirm your password, accept the terms of the End User License Agreement and click **Submit**
d. Login to the Malwarebytes cloud platform using your email address and password

2 Install Onto Your Endpoints

Manual Install (quick and easy, to help get your trial going fast)

a. Login to the Malwarebytes cloud platform (https://cloud.malwarebytes.com) using your email address and password
b. Click on **Endpoints** (left menu bar) ► **Add** (right hand side)
c. Download the correct version(s) for the OS of the target endpoint(s)
d. Save the file to a USB drive or network share
e. From the target endpoint, click on the installer that you downloaded and the agent will install
f. Once installed, the agent will reach out to the management console & will be listed on the Endpoints screen

Malwarebytes Discovery & Deployment Tool (best for larger numbers of endpoints)

a. Login to the Malwarebytes cloud platform (https://cloud.malwarebytes.com) using your email address and password
b. Click on **Endpoints** (left menu bar) ► **Add** (right hand side)
c. Scroll down to the "How to Install" section for the Malwarebytes Discovery & Deployment Tool link. *Tip: scroll down to the next item and you can download the full Malwarebytes Administrator Guide*
d. Click the link to download the Malwarebytes Discovery & Deployment Tool
e. Copy the file to a location where you would like to run it from. *Note: download the Malwarebytes Discovery & Deployment tool to the place where you will to run it from. This is a standalone tool that does not require installation*
f. Click on the file to run the tool (EndpointAgentDeploymentTool.exe)
g. Login to the tool using the same login (email address) and password you created in Step 1. *Note: requires Internet access*
h. Select **Network** if the endpoints are not part of a domain -OR- select **Active Directory** if endpoints are part of the domain and you have the appropriate credentials
i. If you have credentials to login to the target endpoints, check the box at the bottom of the screen for a more complete scan. Enter the credentials and click **OK**
j. Click **Scan**
k. Enter the network information. Acceptable syntax is noted at the top of the dialog box. Then click **Add**
l. Once all the network information is added to the lower box in the dialog, click **Scan Network**
m. Depending on the number of endpoints, the scan may take a while to run. Check the status column
n. Click the check marks on the left of the Host Name for the endpoints you wish to install the agent to. Then click **Install**
o. The endpoints will be added to the Task screen where you can see the status
p. Once the agent is successfully installed, it will appear in the Endpoints screen in the management console

Deploy Using Your Existing Tools (third-party tools e.g., Microsoft SCCM, Jamf, etc.)

a. Login to the Malwarebytes cloud platform (https://cloud.malwarebytes.com) using your email address and password
b. Click on **Endpoints** (left menu bar) ► **Add** (right hand side)
c. Download the correct version(s) for the OS of the target endpoint(s). *Note: select the version that works best with the software deployment tool you will be using. In the case of Windows clients, that might be .msi*
d. Follow your standard procedures for creating an install package for your third-party software deployment tool

3 Run Initial Scan

a. Login to the Malwarebytes cloud platform (https://cloud.malwarebytes.com) using your email address and password
b. Click on **Endpoints** (left menu bar)
c. Check the boxes of the endpoints you wish to scan. If you would like to scan the entire list, check the box in the header row to the left of the word Endpoints
d. Click the **Actions** button (right hand side)
e. **Select Scan + Report** if you want the scan results but do not want to make changes to the endpoint -OR- **Select Scan + Quarantine** to quarantine threats detected during the scan on the endpoint's local hard drive. Quarantined files are encrypted during the process to assure that they cannot become reactivated and cause damage on your endpoint

For complete, detailed instructions on the above steps and procedures, download the Malwarebytes Administrator Guide (https://www.malwarebytes.com/pdf/guides/MBQSG.pdf). You can also check out the links and FAQs on our Trial Support page https://www.malwarebytes.com/business/trial/.

Rev. Sept. 13, 2017