WEBROOT®

an opentext™ company

Endpoint Protection Best Practices Guide

Table of Contents

Introduction

Webroot SecureAnywhere® Business Endpoint Protection is very easy to deploy and manage, but, as with all things, there are a few tips and tricks to help you get the most out of your security solution. This guide offers details on a few of the topics new users frequently ask about.

Deploying With the Silent Audit Policy

When deploying SecureAnywhere Business Endpoint Protection in new environments, we recommend using the Silent Audit policy at the outset to avoid false positives and identify unknown files and programs. This policy means that the agent will detect but not remediate potential threats in order to help you adapt your protection to suit the environment. This is particularly important if your endpoints use any proprietary software.

After using the Silent Audit policy for a day or two, you can create overrides to address unknowns and work with support to correct any false positives you may have encountered.

Addressing Unknowns

Unknown files and programs are those that have not yet been encountered by Webroot® Threat Intelligence, and, as such, have not yet been classified as either benign or malicious. When discovered, these files are automatically monitored by the SecureAnywhere endpoint agent, which may impact an executable's performance. If a user reports that an application isn't running properly, it is likely to be an unknown that is currently under heavy monitoring.

In the case of performance impact due to monitoring, if you are certain the application in question is benign, or if it is proprietary software, you can create an override. Please be sure to contact our support team afterward to ensure that the application is classified accordingly.

To address an unknown:

1. Collect the hostname of the endpoint experiencing the issue, as well as the executable name, directory location, etc.
2. Open the SecureAnywhere management console.
3. Click the **Reports** tab.
4. Run the **All Undetermined Software Seen** report.
5. Sort the report by **Hostname** to locate the endpoint.

   Note: The report can also be exported to CSV.
6. Search for any undetermined files related to the software that is being monitored.
7. Select the **Selector** checkbox to select the files. This enables the Create Override button at the top of the report.
8. Click the **Create Override** button.
9. From the Determination drop-down menu, select **Good** and add a description.
10. To apply this override to all sites under management, select the **GSM** checkbox and click the **Save** button.
11. Once the override is saved, navigate to the Group Management tab and locate the endpoint's hostname.
12. Select the **Selector** checkbox to select the endpoint.
13. Select **Agent Commands > Files and Processes > Reverify all files and processes**.

    The reverification process takes place as soon as the agent receives the agent command, which will depend on the policy polling interval. The agent command can be monitored in the **Logs > Command Log** tab.

Submitting Logs and Opening Support Tickets

Support is automated and easy to access through the SecureAnywhere management console.

To submit a log and open a support ticket:

1. In your management console, click the Group Management tab.
2. Select the endpoint from which you want to gather and send logs.
3. Run **Agent Commands > Advanced > Customer support diagnostics**.

   This command automatically uses the email address from your console login as the identifier in our systems. If you prefer to use a different email, you may change it. The command and log collection timeframe will vary depending on your policy polling interval.
4. Once the agent command is submitted, in the upper right corner of the console window, from the drop-down menu beneath the email address, select **Support**.
5. This opens the Support page. Click **Open or View a Support Ticket**.
6. The wizard will guide you through creating a new support ticket. Be sure to mention that you ran the **Customer support diagnostics** command.
7. Support will review your logs and follow up on the ticket.

Detecting Toolbars and Other Potentially Unwanted Applications

Although potentially unwanted application (PUA) detection is not enabled by default, you can enable it manually in your policy settings.

To enable PUA detection:

1. In your management console, navigate to the Policy tab.
2. Evaluate the policies in use by double-clicking each policy and navigating to the **Scan Setting** tab.
3. The **Detect Possible Unwanted Applications (PUAs) as malicious** setting is off by default. Toggle the setting to **On** and save the change. The change is saved as a draft.
4. Click **Promote Draft Changes to Live** to propagate the change to your endpoints. Agents will receive the change during their next poll to the console.

   Reducing the polling interval accelerates the time it takes for an agent to receive policy changes and agent commands.
5. Return to the Policy tab.
6. Double-click the policy in use to display the Basic Configuration tab.
7. Repeat steps 3 and 4 in the Basic Configuration tab.

Recovering Seats That Are No Longer Used

If an endpoint no longer needs to be protected, you can deactivate it to free the license seat.

To deactivate an endpoint and recover license seats:

1. In your management console, click the **Group Management** tab.
2. From the Groups panel on the left, select the group that includes the endpoints you want to deactivate.
3. Select one or more endpoints, then click **Deactivate** from the command bar.
   A dialog warns you that a deactivated endpoint will no longer be able to report to the console.
4. Click **Yes** to send an Uninstall command to the endpoint. This removes the SecureAnywhere agent.
   Once SecureAnywhere is removed, the endpoint displays in the Deactivated Endpoints group in your management console. After seven days, the status changes to Not Seen Recently.