

Bookmark Fact Sheet

Waiving Bookmark Modules In Cylance

September 2024

This fact sheet applies to public schools in Victoria.

After updating, parts of Bookmark may not open, such as Circulation, Search, Reports, or any other part. This is usually due to the Cylance security system generating a false positive for a Bookmark app located on a server. If Cylance is suspicious about anything it does not understand – such as a complex program - then that file is quarantined. (The program is tossed into prison on suspicion.)

Once quarantined, a file cannot be opened, replaced, or removed.

Bookmark consists of over a dozen separate executable modules or “exe’s” (apps) – e.g., Circulation, Cataloguing, Search, Reports, Overdues, etc. Each button on Bookmark’s main menu launches a separate executable application program. Bookmark programs are regularly screened and do not contain malware. Unfortunately, security systems such as Cylance, generate false positives and take action.

Once a Bookmark file is quarantined, it must then be “waived” in Cylance. The waiving procedure tells Cylance the file is safe and can be released from quarantine. (Get out of prison for false arrest.)

Cylance may quarantine a Bookmark exe when it is updated, even if it has been quarantined previously.

Note: reducing the Cylance security level to 4 can prevent Bookmark exe’s being quarantined.

The Bookmark exe files (applications):

<u>Task/Button</u>	<u>EXE filename</u>
Main menu	BM.EXE and BMMainMenu.exe
Borrowers	BmBorrowers.exe
Cataloguing	BmCataloguing.exe
Circulation	BMCIRC.EXE and BmCirculation.exe
Controls	BmControls.exe
Webopac	BMOPAC.EXE
Overdues	BmOverdues.exe
Reports	BmReports.exe
Search	BmSearch.exe
Stocktake	BmStocktake.exe
Utilities	BmUtilities.exe
Webopac server	BMWEBSVR.EXE and BmWebserver.exe

In addition, the files Bmlha32.exe, Bm.com, Pa.com, Paw.exe, Bwmenu.exe, Wincirc.exe and Circl.com may also be quarantined. These old exe files are no longer used in Bookmark and do not have to be waived. If they are being used by a desktop shortcut, the Target should be changed to the correct file. Example: if Wincirc.exe or Circl.com is on the Target line of the icon's properties, change that part to BmCirculation.exe. Change Bm.com or Bwmenu.exe to Bm.exe. Change Pa.com or Paw.exe to BmSearch.exe.

(Note: Bookmark filenames may change in the future, but will always begin with BM.)

The following steps were kindly provided by David Sutcliffe, Specialist Technician.

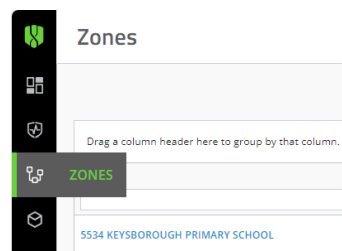
Opening Cylance

Log into Cylance. Go to <https://login-au.cylance.com/Login?from=VenueWeb>

Under the green "Sign In", select the blue writing saying "[Or sign in with your External Identity Provider](#)"

Now sign in with your eduSTAR details.
On the left select "Zones" to show your Schools.

In here Select your current School.

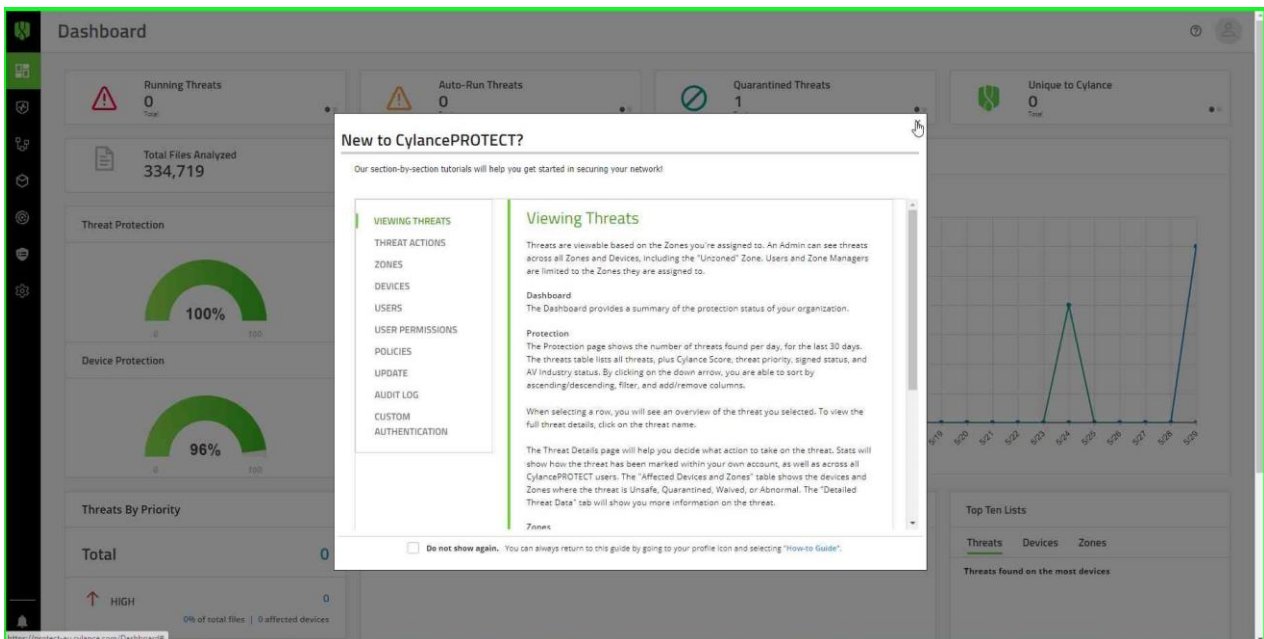


A list of Servers with Cylance is displayed.

Select the Bookmark Server from the list. It should show you Threats & Activities as well as Quarantined items. If Bookmark 'exes' are listed, they need to be 'Waived'. Most Bookmark filenames all begin with BM.

How to Waive Items in Cylance

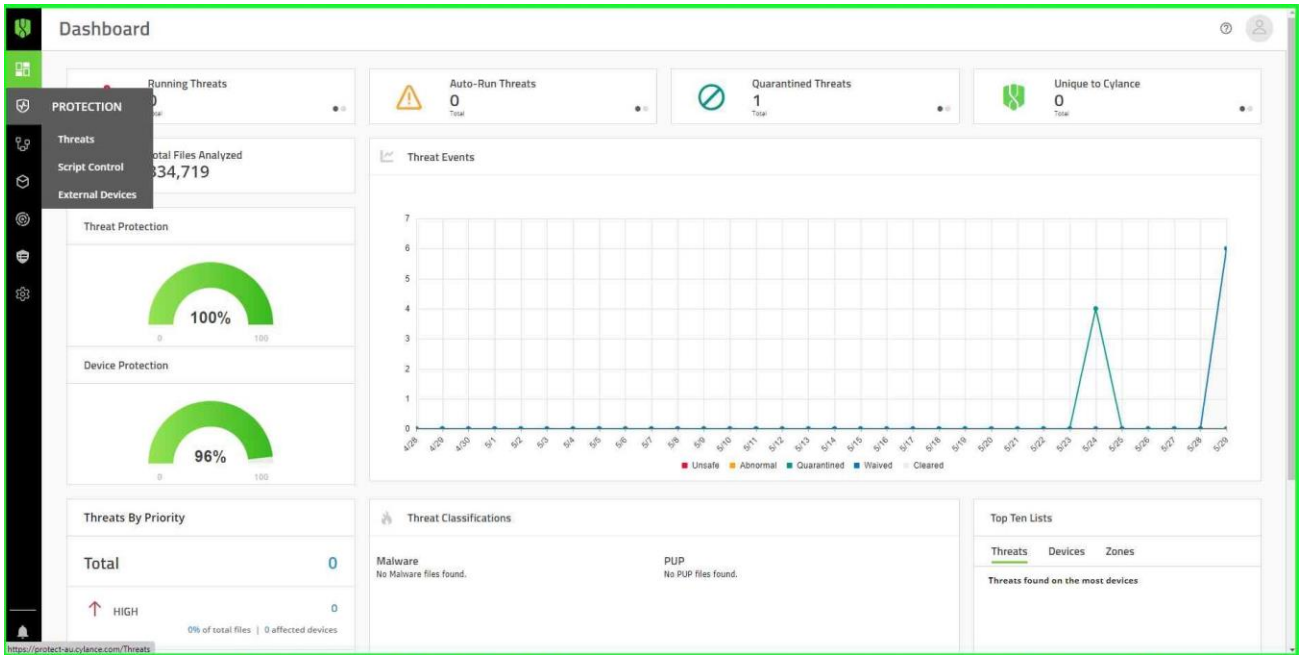
Step 1. Log into Cylance as above.



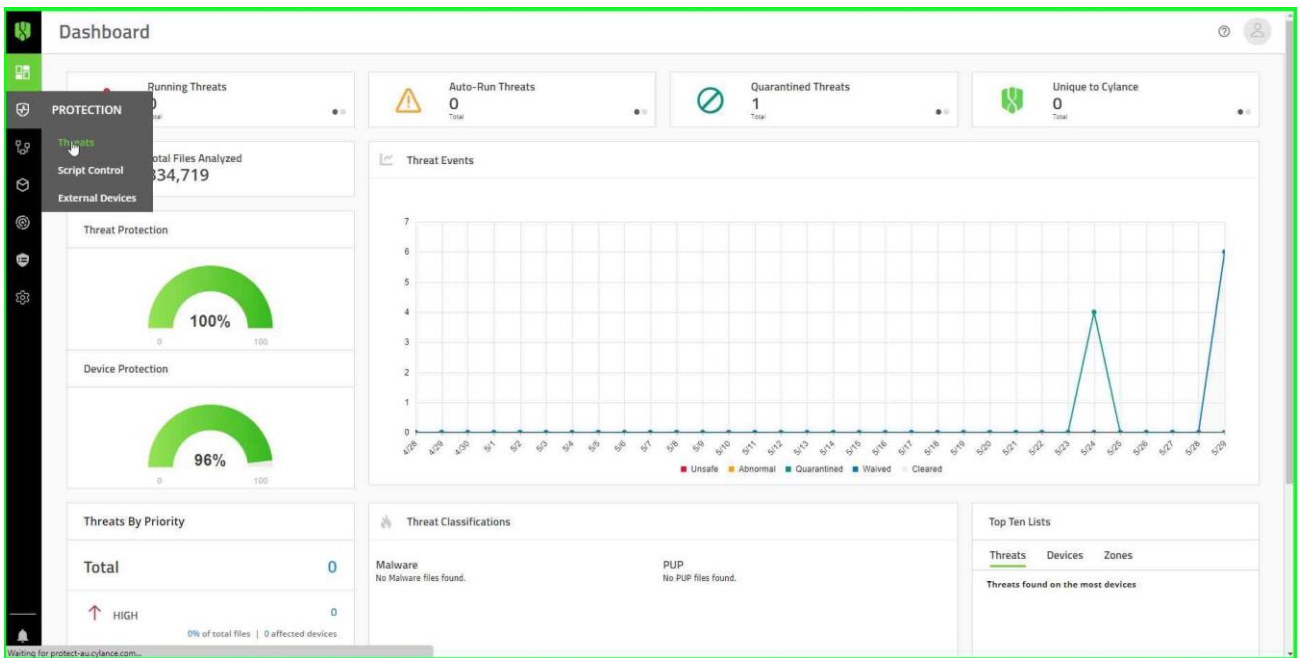
email
education.bookmark@sa.gov.au

website
<http://bookmark.central.sa.edu.au/>

Step 2. Click on 'PROTECTION' on the left menu.



Step 3. Select 'Threats'



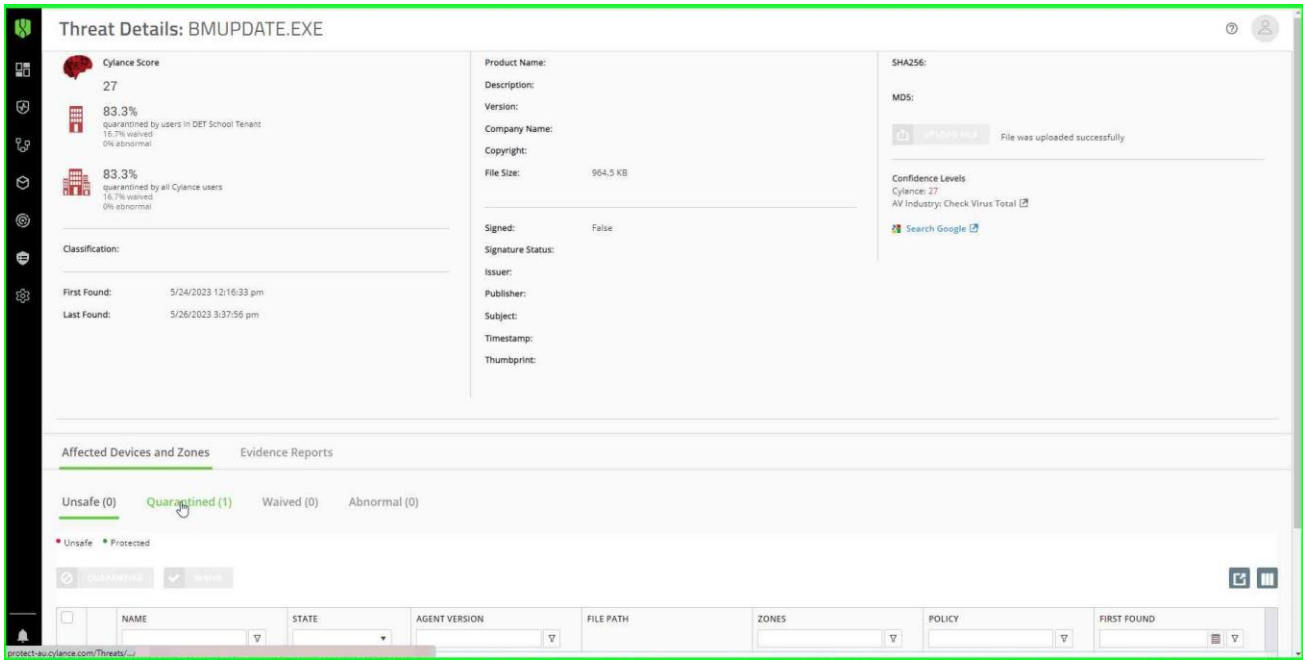
Step 4. On the left, select the number of 'Quarantined' items to list them.

The screenshot shows the 'Protection > Threats' interface. On the left, the 'Threat Filters' panel is open, showing 'Status: Last 24 Hours' with 'Quarantined' selected. The main table lists several threats, including BMCIRC.EXE, BMREPORT.EXE, BMSTK.EXE, BMUPDATE.EXE, Bmsha32.EXE, PA.COM, PAW.EXE, and WINCIRC.EXE. The 'Details: BMCIRC.EXE' panel is visible at the bottom, showing 'Overview' and 'Devices (1)' with a status of 'Quarantined (0)'.

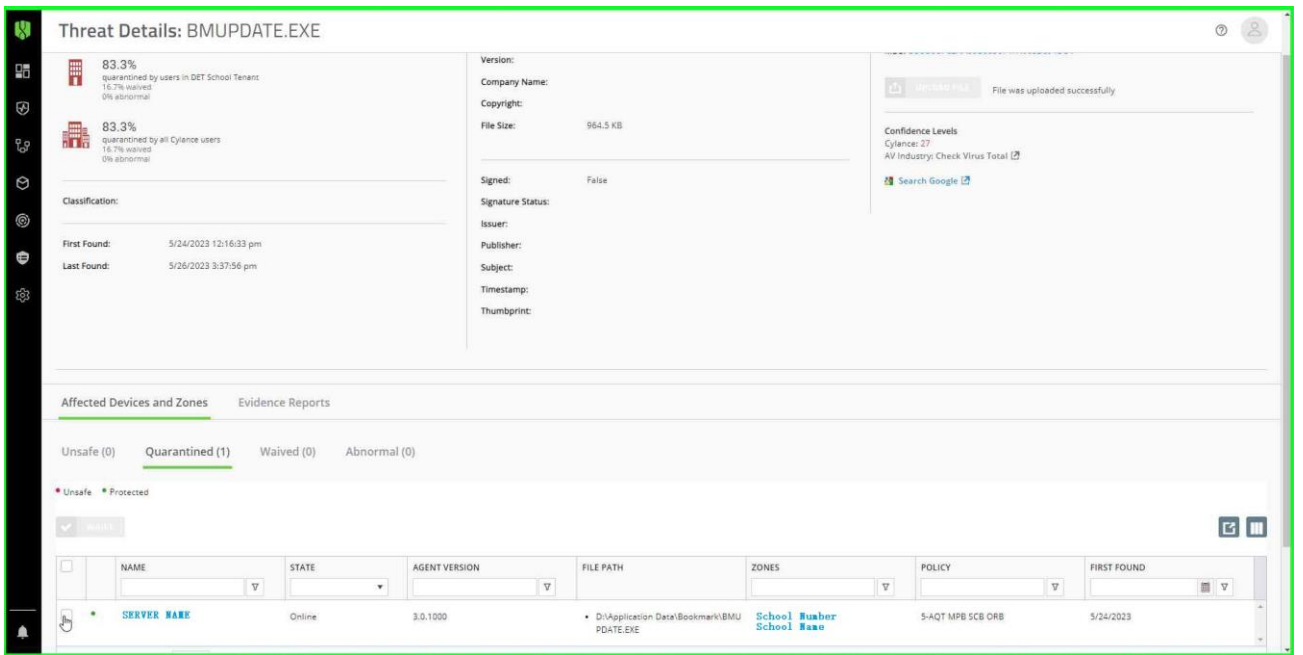
Step 5. Select a 'Quarantined' item.

The screenshot shows the 'Protection > Threats' interface with the 'Quarantined' status selected in the left-hand filter menu. The main table lists several threats, including BMUPDATE.EXE. The 'Details: BMUPDATE.EXE' panel is open, showing 'Overview' and 'Devices (1)'. The 'Devices (1)' section shows 'Quarantined (1)' and 'Protected'. The 'File Information' section shows the product name, description, version, company name, copyright, and file size (954.5 KB).

Step 6. Select the 'Quarantined' header.



Step 7. Tick the check box.



Step 8. Select 'Waive'

Threat Details: BMUPDATE.EXE

83.3% quarantined by users in DET School Tenant
16.7% waived
0% abnormal

83.3% quarantined by all Cylance users
16.7% waived
0% abnormal

Classification:

First Found: 5/24/2023 12:16:33 pm
Last Found: 5/26/2023 3:37:56 pm

Version:
Company Name:
Copyright:
File Size: 964.5 KB
Signed: False
Signature Status:
Issuer:
Publisher:
Subject:
Timestamp:
Thumbprint:

Confidence Levels
Cylance: 27
AV Industry: Check Virus Total

Affected Devices and Zones Evidence Reports

Unsafe (0) Quarantined (1) Waived (0) Abnormal (0)

Unsafe Protected

WAIVE

NAME	STATE	AGENT VERSION	FILE PATH	ZONES	POLICY	FIRST FOUND
Server 1	Online	3.0.1000	D:\Application Data\Bookmark\BMUPDATE.EXE	School Huber School 1	5-AQT MPB SCB ORB	5/24/2023

Step 9. Agree to the 'Action Confirmation'

Threat Details: BMUPDATE.EXE

83.3% quarantined by users in DET School Tenant
16.7% waived
0% abnormal

83.3% quarantined by all Cylance users
16.7% waived
0% abnormal

Classification:

First Found: 5/24/2023 12:16:33 pm
Last Found: 5/26/2023 3:37:56 pm

Version:
Company Name:
Copyright:
File Size: 964.5 KB
Signed: False
Signature Status:
Issuer:
Publisher:
Subject:
Timestamp:
Thumbprint:

Confidence Levels
Cylance: 27
AV Industry: Check Virus Total

Affected Devices and Zones Evidence Reports

Unsafe (0) Quarantined (1) Waived (0) Abnormal (0)

Unsafe Protected

WAIVE

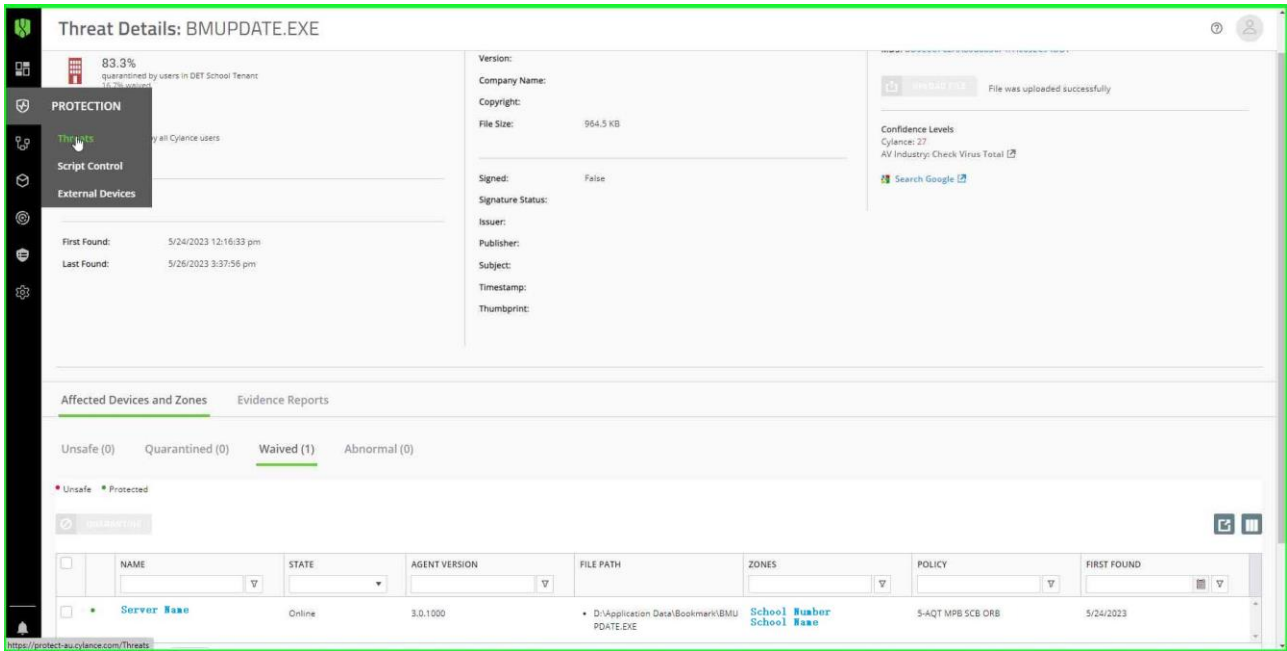
Action Confirmation

Are you sure you want to provide a waiver for this file on the selected device?

YES CANCEL

NAME	STATE	AGENT VERSION	FILE PATH	ZONES	POLICY	FIRST FOUND
Server 1	Online	3.0.1000	D:\Application Data\Bookmark\BMUPDATE.EXE	School Huber School 1	5-AQT MPB SCB ORB	5/24/2023

Step 10. Go back to 'PROTECTION' (step 2) and select 'Threats' for the next item.



Loop back to [Step 3](#).

Keep going till all items are Waived.

Unfortunately, waiving is not permanent. When Bookmark is updated again, Cylance can re-quarantine a file.

As an alternative to waiving, try setting the security level to 4 or excluding the entire Bookmark drive or folder.