Bookmark Fact Sheet

Waiving Bookmark Modules
In Cylance

February 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):

Task/Button	EXE filename
Main menu	BM.EXE and BMMainMenu.exe
Borrowers	BMBORRX.EXE
Cataloguing	BMCAT.EXE
Circulation	BMCIRC.EXE
Controls	BMCTRLS.EXE
Webopac	BMOPAC.EXE
Overdues	BMOVD.EXE
Reports	BMREPORTS.EXE
Search	BMSEARCH.EXE
Stocktake	BMSTK.EXE
Utilities	BMUTILX.EXE
Webopac server	BMWEBSVR.EXE
Update	BMUPDATE.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 BmCirc.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.

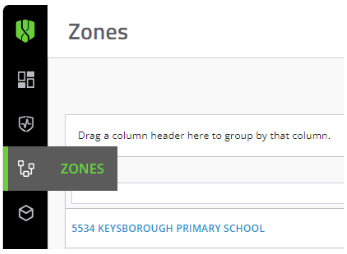
Opening Cylance

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.



Zones

Drag a column header here to group by that column.

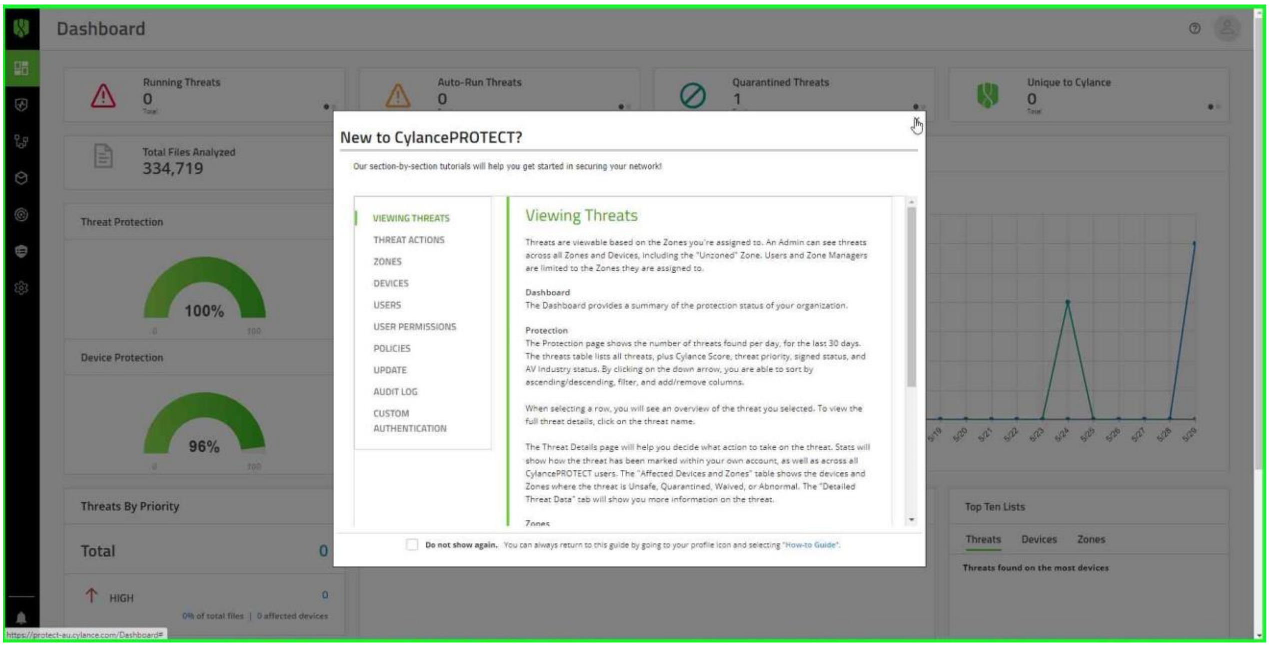
5534 KEYSBOROUGH PRIMARY SCHOOL

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.



New to CylancePROTECT?

Our section-by-section tutorials will help you get started in securing your network!

Viewing Threats

Threats are viewable based on the Zones you're assigned to. An Admin can see threats across all Zones and Devices, including the "Unzoned" Zone. Users and Zone Managers are limited to the Zones they are assigned to.

Dashboard
The Dashboard provides a summary of the protection status of your organization.

Protection
The Protection page shows the number of threats found per day, for the last 30 days. The threats table lists all threats, plus Cylance Score, threat priority, signed status, and AV Industry status. By clicking on the down arrow, you are able to sort by ascending/descending, filter, and add/remove columns.

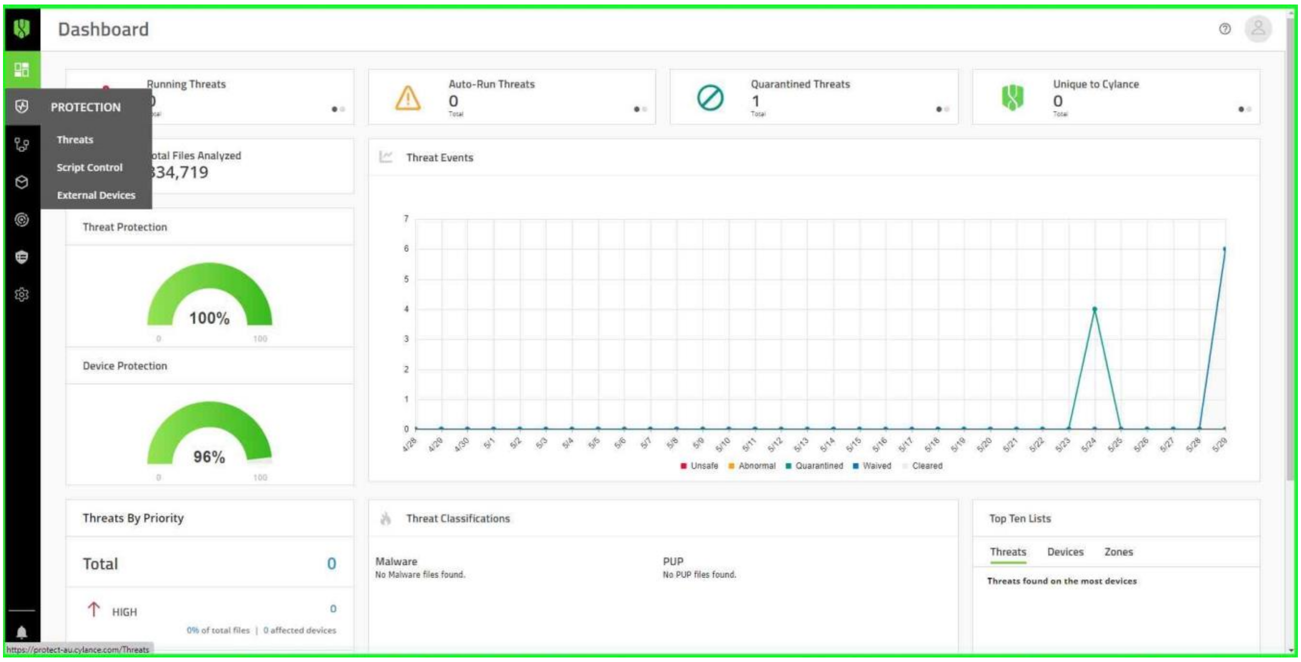
When selecting a row, you will see an overview of the threat you selected. To view the full threat details, click on the threat name.

The Threat Details page will help you decide what action to take on the threat. Stats will show how the threat has been marked within your own account, as well as across all CylancePROTECT users. The "Affected Devices and Zones" table shows the devices and Zones where the threat is Unsafe, Quarantined, Waived, or Abnormal. The "Detailed Threat Data" tab will show you more information on the threat.

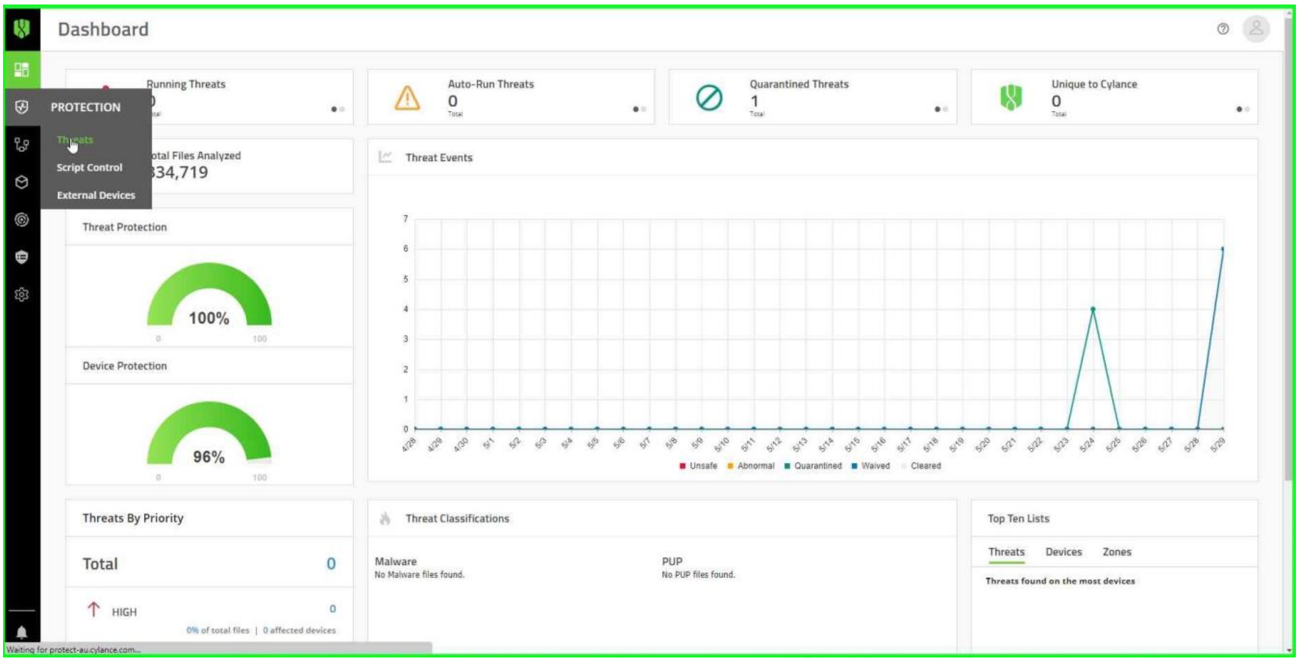
Zones

☐ **Do not show again.** You can always return to this guide by going to your profile icon and selecting "How-to Guide".

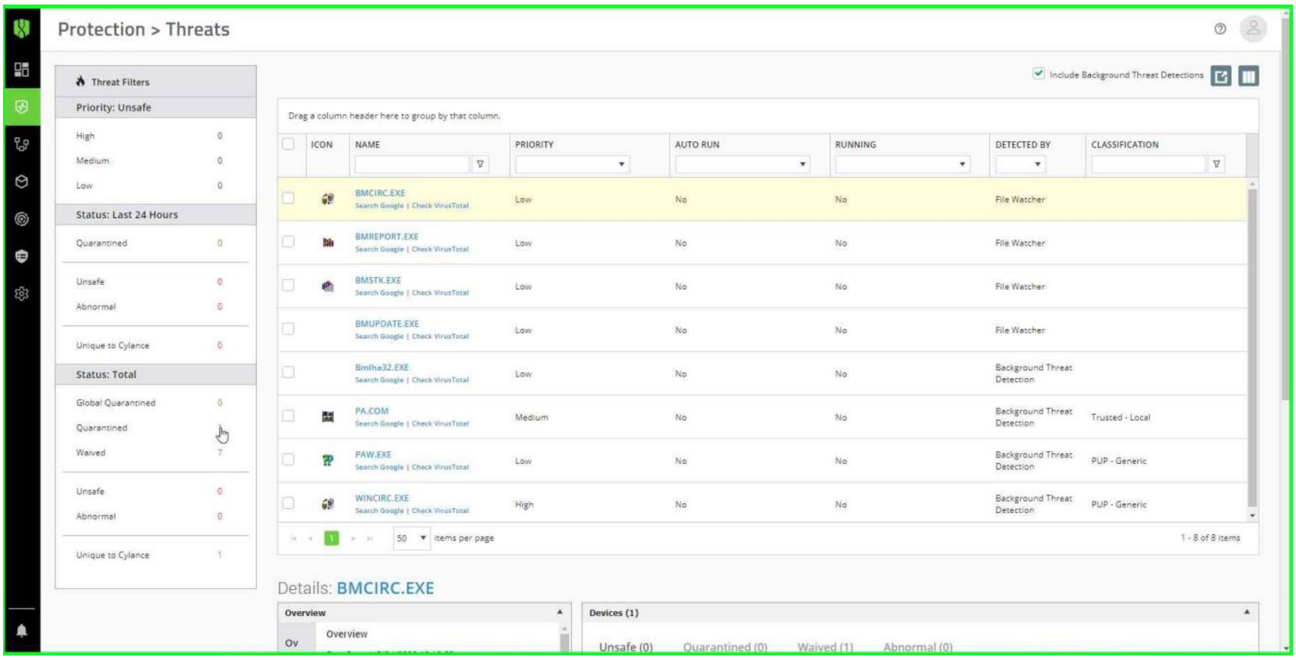
Step 2. Click on ‘PROTECTION’ on the left menu.



Step 3. Select ‘Threats’



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



Protection > Threats

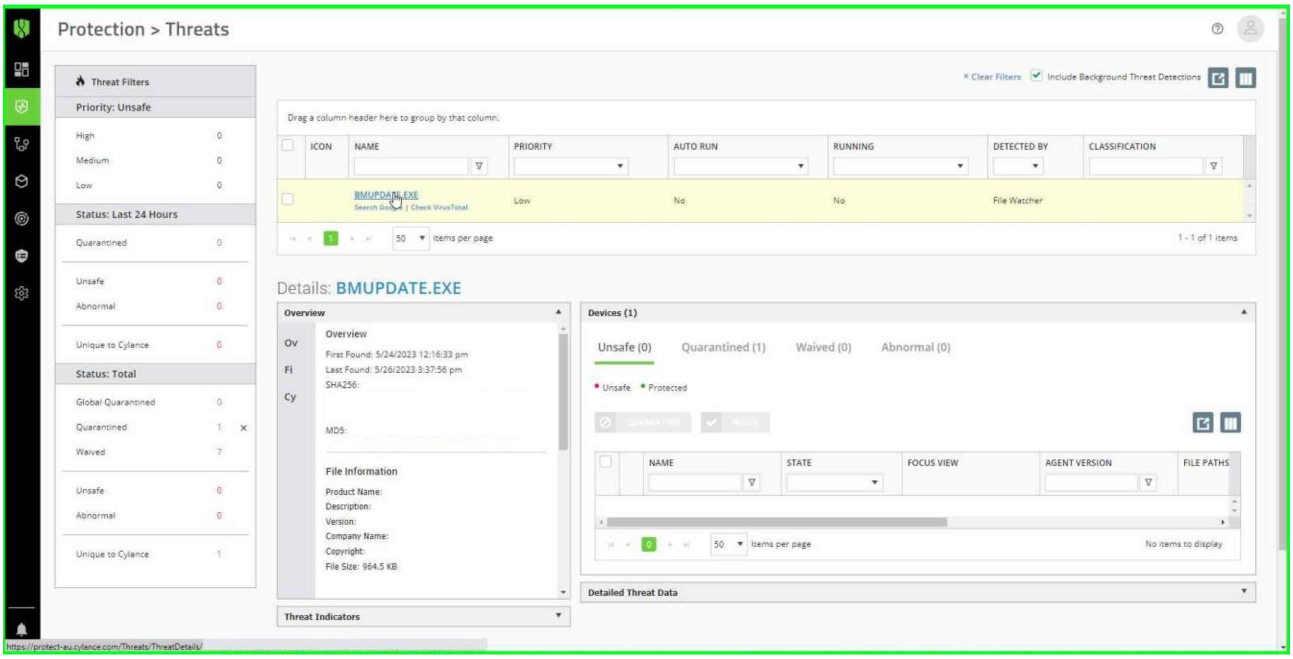
Threat Filters	
Priority: Unsafe	
High	0
Medium	0
Low	0
Status: Last 24 Hours	
Quarantined	0
Unsafe	0
Abnormal	0
Unique to Cylance	0
Status: Total	
Global Quarantined	0
Quarantined	
Waived	7
Unsafe	0
Abnormal	0
Unique to Cylance	1

Drag a column header here to group by that column.

ICON	NAME	PRIORITY	AUTO RUN	RUNNING	DETECTED BY	CLASSIFICATION
	BMCIRC.EXE Search Google | Check VirusTotal	Low	No	No	File Watcher	
	BMREPORT.EXE Search Google | Check VirusTotal	Low	No	No	File Watcher	
	BMSTK.EXE Search Google | Check VirusTotal	Low	No	No	File Watcher	
	BMUPDATE.EXE Search Google | Check VirusTotal	Low	No	No	File Watcher	
	Bmlha32.EXE Search Google | Check VirusTotal	Low	No	No	Background Threat Detection	
	PA.COM Search Google | Check VirusTotal	Medium	No	No	Background Threat Detection	Trusted - Local
	PAW.EXE Search Google | Check VirusTotal	Low	No	No	Background Threat Detection	PUP - Generic
	WINCIRC.EXE Search Google | Check VirusTotal	High	No	No	Background Threat Detection	PUP - Generic

Details: BMCIRC.EXE

Step 5. Select a ‘Quarantined’ item.



Protection > Threats

Threat Filters		
Priority: Unsafe		
High	0	
Medium	0	
Low	0	
Status: Last 24 Hours		
Quarantined	0	
Unsafe	0	
Abnormal	0	
Unique to Cylance	0	
Status: Total		
Global Quarantined	0	
Quarantined	1	×
Waived	7	
Unsafe	0	
Abnormal	0	
Unique to Cylance	1	

Drag a column header here to group by that column.

ICON	NAME	PRIORITY	AUTO RUN	RUNNING	DETECTED BY	CLASSIFICATION
	BMUPDATE.EXE Search Google | Check VirusTotal	Low	No	No	File Watcher	

Details: BMUPDATE.EXE

Overview

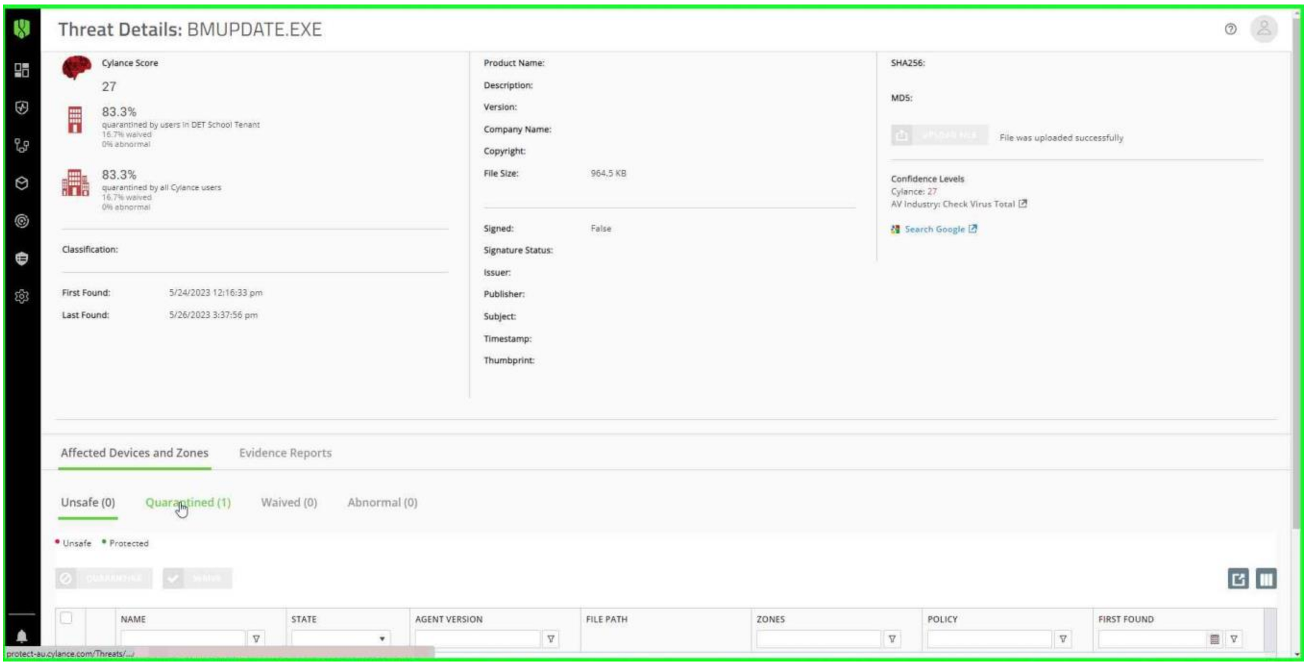
First Found: 5/24/2023 12:16:33 pm
Last Found: 5/26/2023 3:37:56 pm
SHA256:
MD5:

File Information

Product Name:
Description:
Version:
Company Name:
Copyright:
File Size: 964.5 KB

	NAME	STATE	FOCUS VIEW	AGENT VERSION	FILE PATHS

Step 6. Select the ‘Quarantined’ header.



Threat Details: BMUPDATE.EXE

Cylance Score
27

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

Product Name:
Description:
Version:
Company Name:
Copyright:
File Size: 964.5 KB

Signed: False
Signature Status:
Issuer:
Publisher:
Subject:
Timestamp:
Thumbprint:

SHA256:

MD5:

File was uploaded successfully

Confidence Levels
Cylance: 27
AV Industry: Check Virus Total

Search Google

Affected Devices and Zones | Evidence Reports

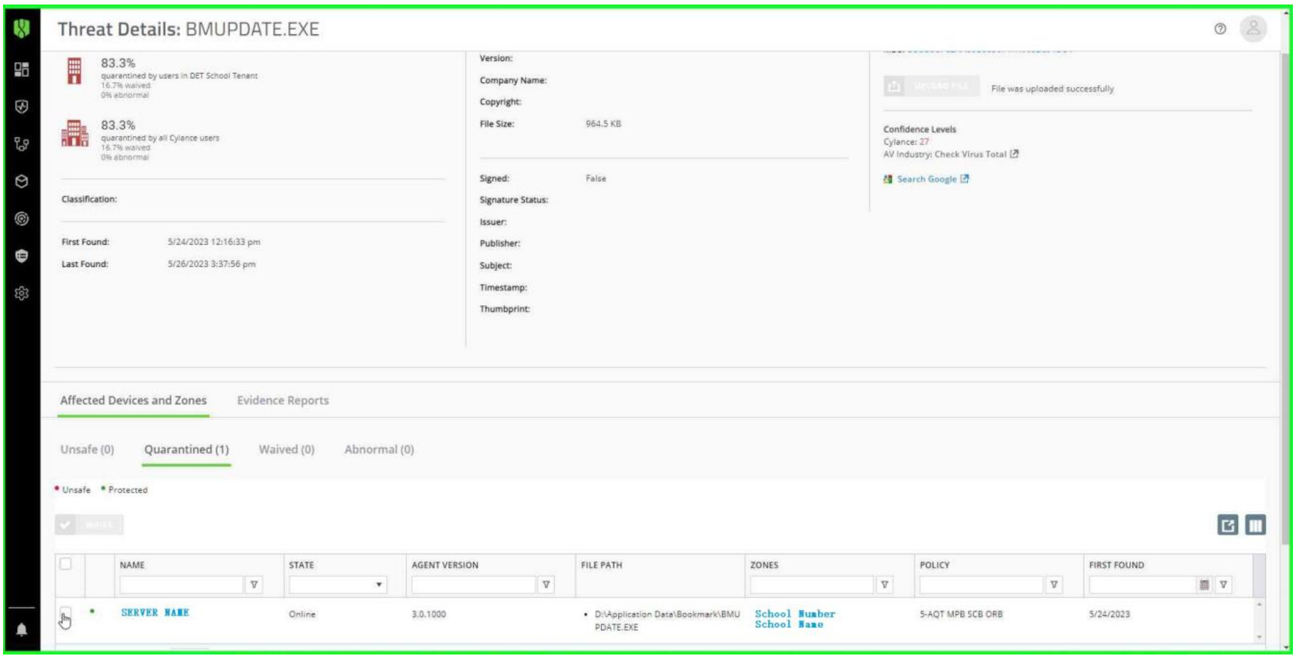
Unsafe (0) | Quarantined (1) | Waived (0) | Abnormal (0)

● Unsafe ● Protected

□		NAME	STATE	AGENT VERSION	FILE PATH	ZONES	POLICY	FIRST FOUND

protect-au.cylance.com/Threats/.../

Step 7. Tick the check box.



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:

File was uploaded successfully

Confidence Levels
Cylance: 27
AV Industry: Check Virus Total

Search Google

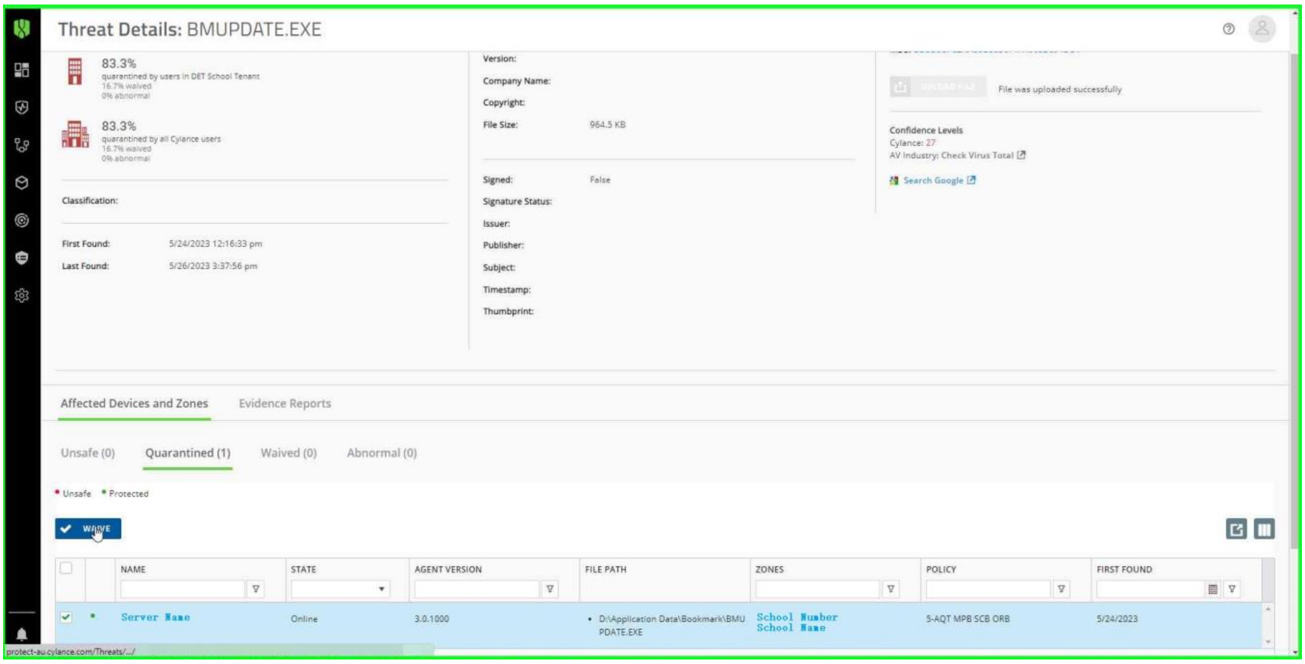
Affected Devices and Zones | Evidence Reports

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

● Unsafe ● Protected

□		NAME	STATE	AGENT VERSION	FILE PATH	ZONES	POLICY	FIRST FOUND
□	●	SERVER NAME	Online	3.0.1000	• D:\Application Data\Bookmark\BMUPDATE.EXE	School Number School Name	5-AQT MPB SCB ORB	5/24/2023

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:

File was uploaded successfully

Confidence Levels
Cylance: 27
AV Industry: Check Virus Total

Search Google

Affected Devices and Zones | Evidence Reports

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

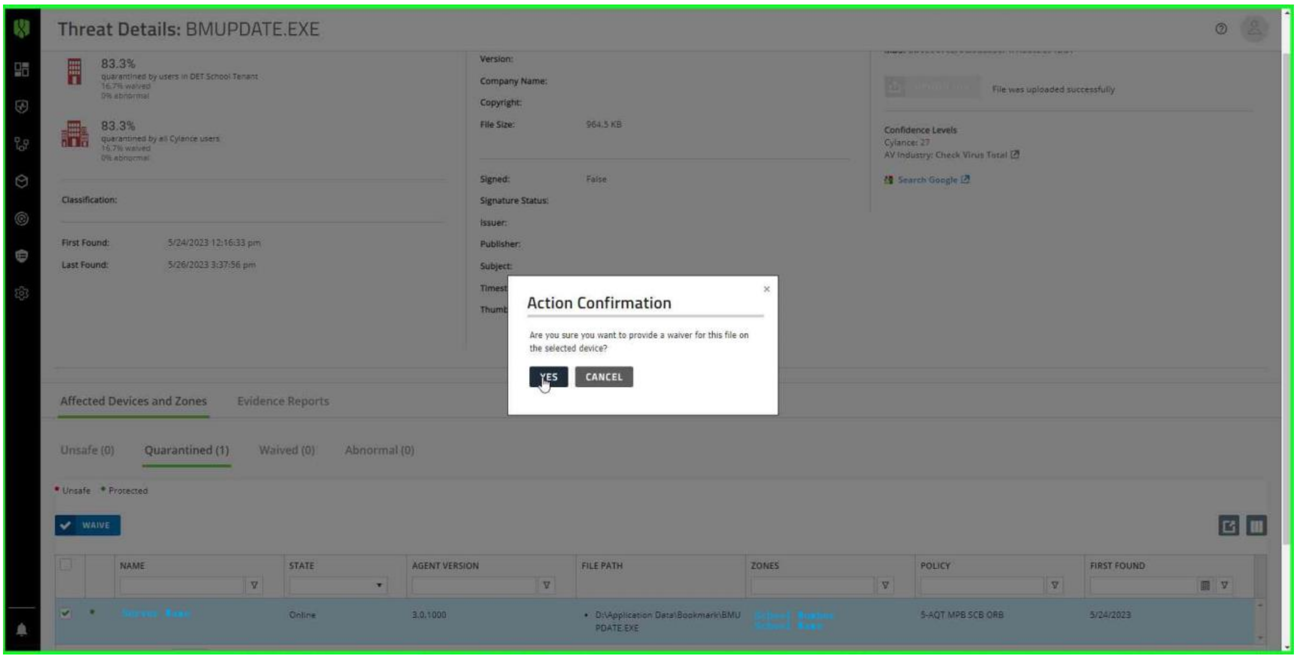
● Unsafe ● Protected

✓ WAIVE

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

protect-au.cylance.com/Threats/.../

Step 9. Agree to the ‘Action Confirmation’

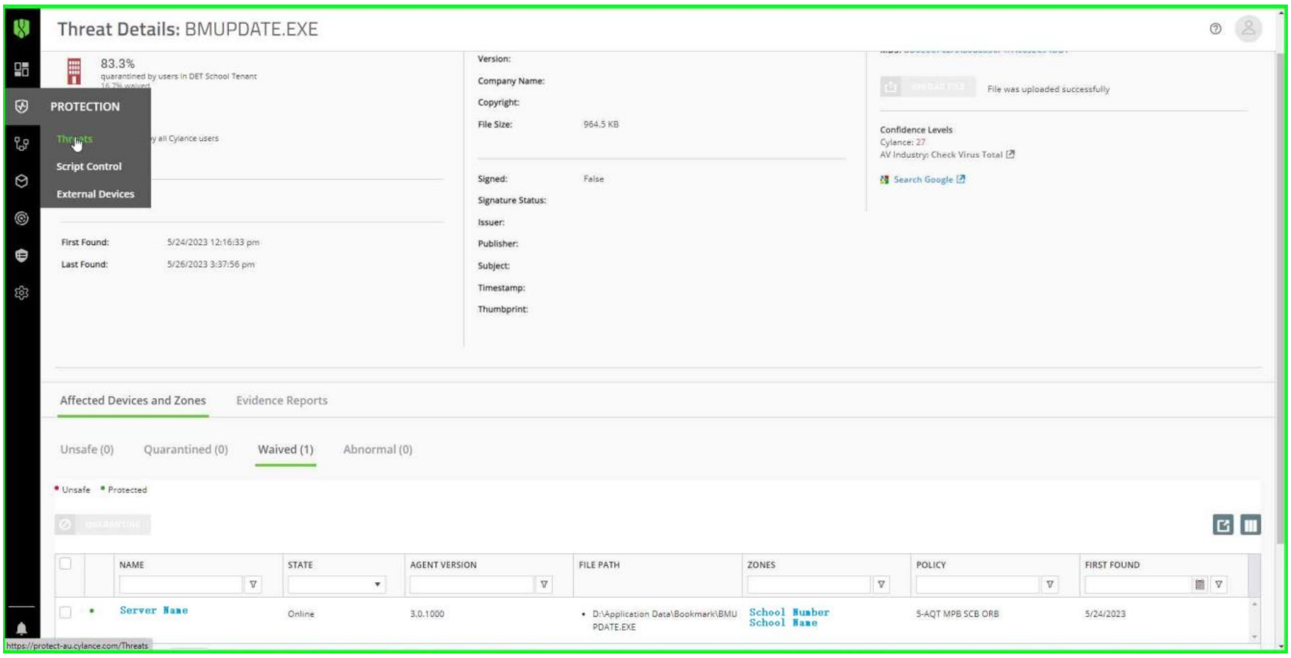


Action Confirmation

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

YES | CANCEL

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



Threat Details: BMUPDATE.EXE

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

y all Cylance users

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:

UPLOAD FILE File was uploaded successfully

Confidence Levels
Cylance: 27
AV Industry: Check Virus Total
Search Google

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

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.