

VMware Carbon Black Threat Remediation with Workspace ONE Intelligence

This lab is for the purposes of understanding the integration with Workspace ONE Intelligence and VMware Carbon Black Cloud. You will be required to do a little pre-work to setup the requirements for the integration. Once those are setup you will be able to demo carbon black policy enforce a blacklist policy virtual machine in to Workspace ONE and push out the VMware Carbon Black Sensor installer and connect it to the correct org. We will look at how a threat with it's various severities can be detected by policies we create inside VMware Carbon Black.

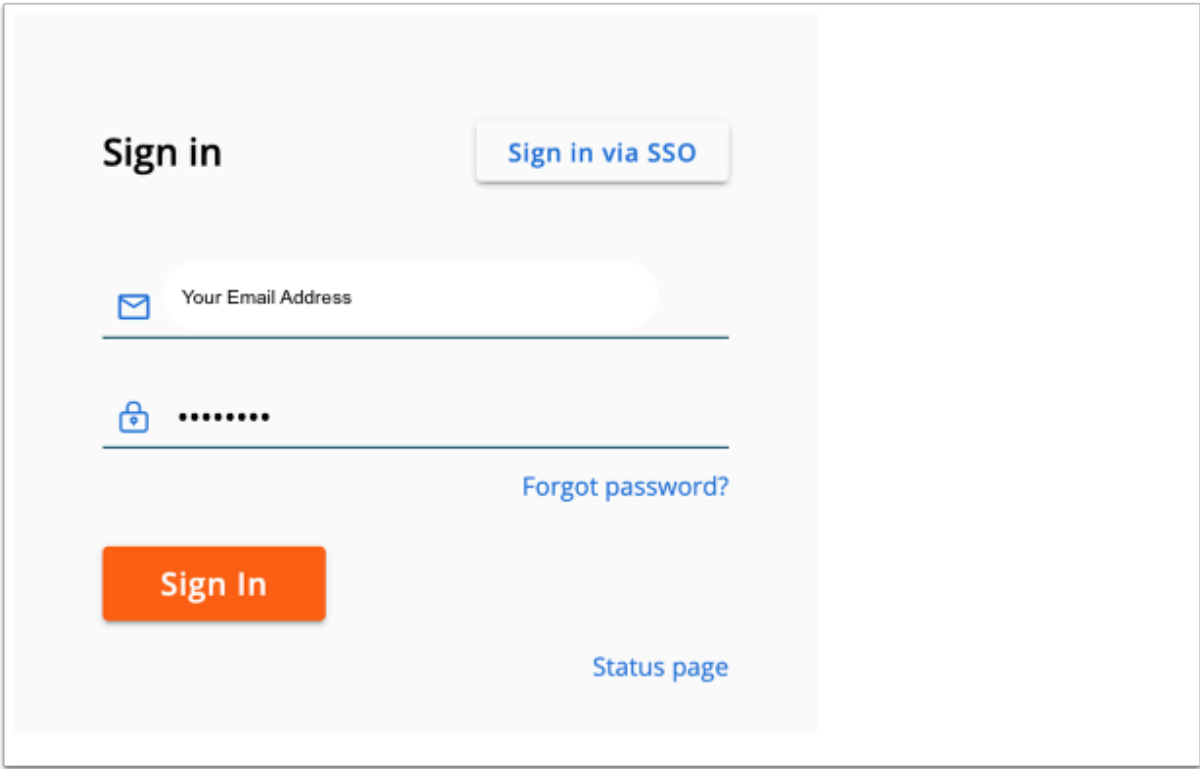
Next we will see how Workspace ONE Intelligence is ingesting this information and taking action to re-mediate an issue on that device.

There are four parts to this Lab

1. Downloading the VMware Carbon Black Sensor
2. Workspace ONE UEM & VMware Carbon Black Sensor Integration
3. Workspace ONE IntelligenceAPI integration & Automation
4. VMware Carbon Black Incident & Workspace ONE Intelligence Automation

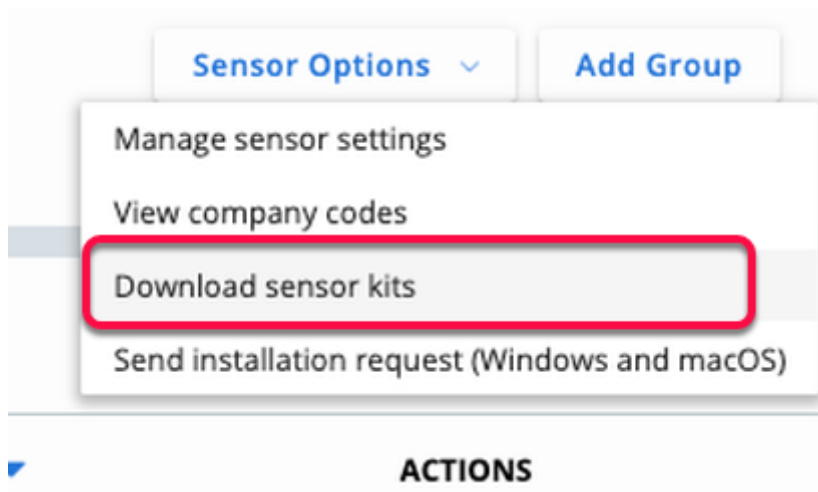
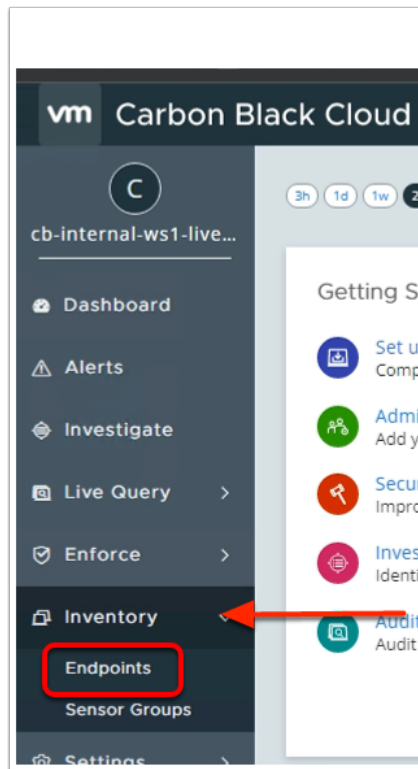
NOTE: Screenshot precedes Instructions in this lab

Part 1: Downloading the VMware Carbon Black Sensor

A screenshot of the VMware Carbon Black Sign in page. The page has a light gray background. At the top left, the text "Sign in" is displayed. To its right is a button labeled "Sign in via SSO". Below the "Sign in" text, there is a form with two input fields. The first field is labeled "Your Email Address" and has an envelope icon to its left. The second field is for a password, indicated by a lock icon and a series of dots. To the right of the password field is a link that says "Forgot password?". At the bottom left of the form is an orange button labeled "Sign In". At the bottom right of the form is a link that says "Status page".

1. On your ControlCenter server
 - **Open** your **Chrome** browser
 - Launch a web page to your Carbon Black tenant using the following URL
<https://defense-prod05.conferdeploy.net>
 - On the **Sign in** page. User your **email address** and the password **VMware1!**
 - Select **Sign In**

 Use the credentials created above to authenticate as administrator.



2. On your ControlCenter server
 - On the **VMware Carbon Black** Console
 - On the left navigation pane, expand **Inventory**
 - Select **ENDPOINTS**
 - On the top right-hand corner, select the **drop down** next to **Sensor Options**.
 - Select **Download sensor kits**



NOTE: If you do not see the options on the left pane, reduce the Page Zoom by Navigating to the menu options on top right and click on minus sign.

Learn more about sensors from: [Supported Operating Systems](#), [Sensor Release Notes](#), and the [Sensor Installation Guide](#)

OS	SENSOR VERSION	ACTION
Windows 64-bit	3.7.0.1503	Download Kit

3. In the **VMware Carbon Black** Console

- Select **Download Kit** next to **Windows 64-bit** from the **Download Sensor Kits** page.
 - (Be sure to download the latest)

! IF you do not see the Save File as shown above, come back to the **VMware Carbon Black Cloud** admin console and right-click on **Download Kit** next to **Windows 64-bit** and click **Save Link As...** and then click **Save**

Close your Carbon Black Cloud Administration Console

This concludes Part 1, please proceed to Part 2

Part 2: Workspace ONE UEM & VMware Carbon Black Sensor Integration

In this lab we will create a software distribution package to install VMware Carbon Black Sensor silently (unattended) using Workspace ONE UEM.

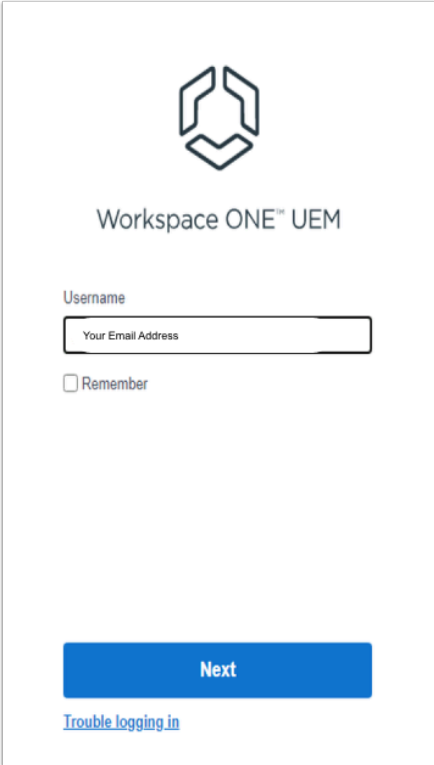
The lab parts are as follows:

2.1: Create VMware Carbon Black Sensor installation package through WorkspaceONE UEM

2.2: Change Windows 10 Name and IP Address

2.3: Observe Device behaviour in VMware Carbon Black console

2.1: Create VMware Carbon Black Sensor installation package through Workspace ONE UEM

The image shows the Workspace ONE UEM login interface. At the top is the Workspace ONE logo, a stylized hexagon composed of three interlocking shapes. Below the logo is the text "Workspace ONE™ UEM". Underneath is a "Username" label followed by a text input field containing the placeholder text "Your Email Address". Below the input field is a checkbox labeled "Remember". At the bottom of the form is a large blue button with the text "Next". Below the button is a link that says "Trouble logging in".

Workspace ONE™ UEM

Username

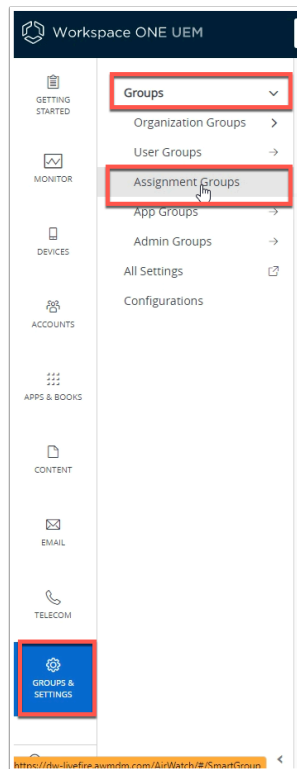
Your Email Address

☐ Remember

Next

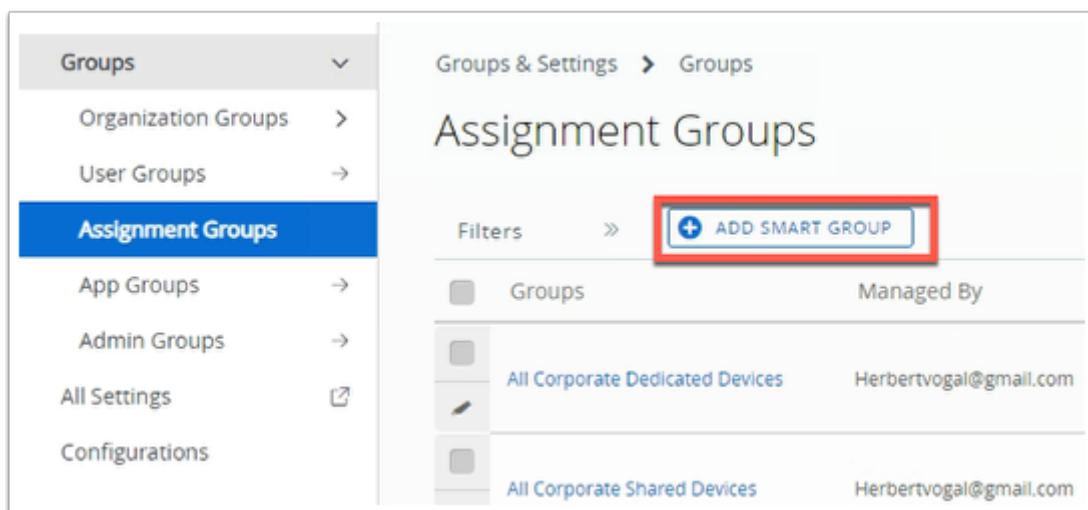
[Trouble logging in](#)

1. On the **ControlCenter** server
 - Open a **new tab** in Google Chrome
 - Navigate to your Workspace ONE UEM admin console with the following URL (<https://cn-livewire.awmdm.com>)
 - Enter your **custom Username**, select **Next**
 - In the **Password** area, enter your **custom password** select **Log in**
 - If prompted **close** the **Workspace ONE UEM Console Highlights** window



2. In the **Workspace ONE UEM** Console

- Navigate to **GROUPS & SETTINGS**
- Select **Groups**
- Select **Assignment Groups**



3. In the **Assignment Groups** window

- Select **+ ADD SMARTGROUP**

Create New Smart Group

Name

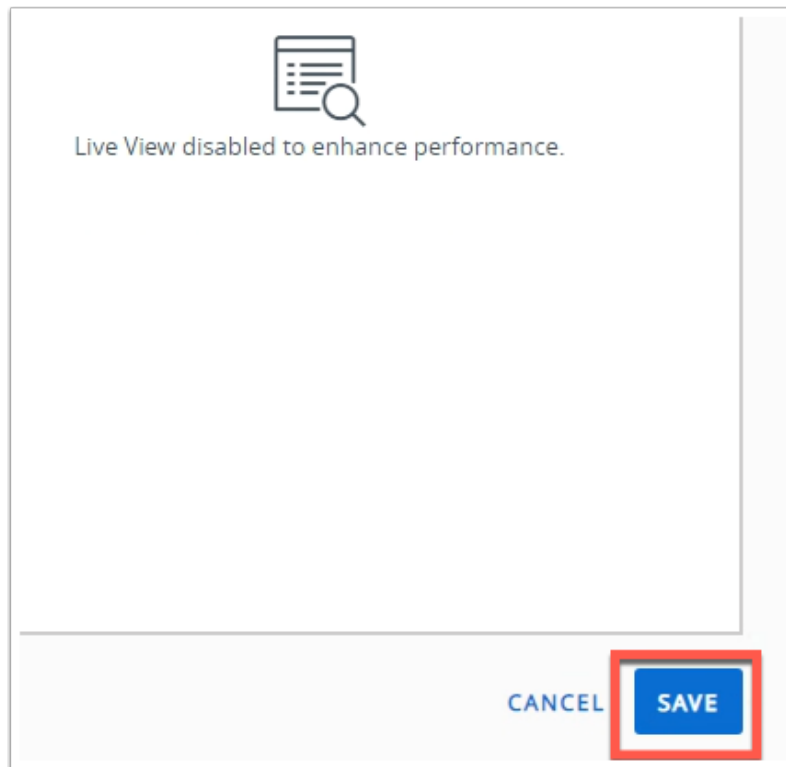
Managed By Herbertvogal@gmail.com

Choose Type

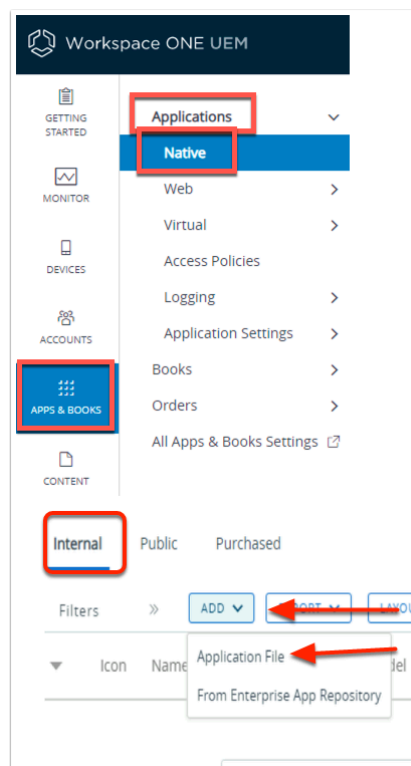
▼ Devices ⓘ

Herbertvogal@gmail.com VMware Virtual Platform 1 eeATTE	<input type="button" value="ADD"/>
Herbertvogal@gmail.com Android X1X0Android_Android SDK built for x86_64_358240051111110	
Herbertvogal@gmail.com VMware Virtual Platform 1 eeATTENDEE200	
Herbertvogal@gmail.com VMware7,1 5 e5W10EXT01A	<input type="button" value="ADD"/>

4. In the **Create New Smart Group** window
 - Next to **Name** enter: **W10Client01a**
 - Next to **Choose Type**, select **DEVICES OR USERS**
 - When prompted with a warning message, select **OK**
 - Under **Devices**:
 - Select the Device which you have re-named and enrolled in the introduction section
 - Select **ADD**

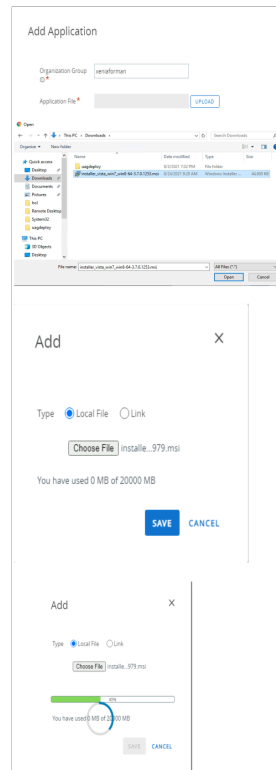


5. In the **Create New Smart Group** window
 - Select **SAVE** in the bottom right corner.



6. In the **Workspace ONE UEM** Console
 - Navigate to **Apps & Books > Application > Native**
 - Select **ADD** under the **Internal** tab

- Select **Application File**




7. In the **Add Application** window

- Next to **Organization Group ID**, leave this default
- Next to **Application File**, select **UPLOAD**
 1. Select **Choose File** and a new window will open,
 2. Navigate to the **Download Folder** in the left navigation bar and select the msi you downloaded earlier.
 3. Select the **installer.....msi** and select **Open**.
 4. Select **SAVE** on the final Add page this will upload the application.

8. In the **Add Application** window

- Select **CONTINUE** to verify the application file and that it is not a dependency
- In the **Add Application - Carbon Black Cloud Sensor 64-bit** window
 - On the **Details** tab
 - **Scroll down** to **Supported Processor Architecture**
 - Change it from **32 bit** to **64-bit**
 - Select the **Deployment Options** tab
 - **Scroll down** to the **Install Command** field
 - Paste the **install parameter** from below into the **Install Command** Field
 - Replace the existing install command in that field already. Ensure the version of Sensor is correct
 - If you typing in the COMPANY_CODE, the number 8 is followed by 'O' and not Zero. (Common Mistake)
 - **msiexec /q /i "installer_vista_win7_win8-64-3.7.0.1503.msi" /L*vx Log.txt COMPANY_CODE=S17NA79RWX!K8OJLXA3**
 - **Scroll** further down **Deployment options** tab
 - Next to **Device Restart** select "**User-engaged restart**"
 - Select **SAVE & ASSIGN**

 **NOTE:** The Company Code determine the VMware Carbon Black Cloud environment and can be retrieve from the VMware Carbon Black admin console. In an environment

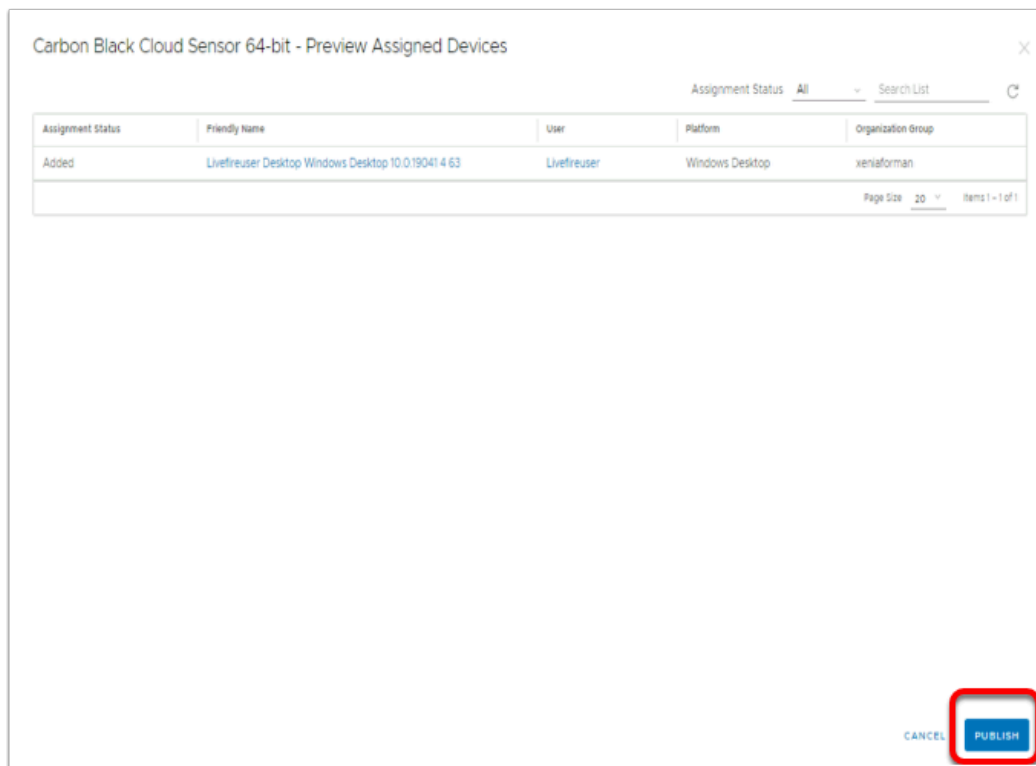
where you have Super admin rights, you can verify the company code by Navigating to **ENDPOINTS > SENSOR OPTIONS > COMPANY CODES** in the VMware Carbon Black portal. However, in this lab environment you have only read only access and so this option is not available.

The screenshot shows the 'Distribution' tab of the 'Carbon Black Cloud Sensor 64-bit- Assignment' page. The form includes the following fields and options:

- Name:** Carbon Black Sensor for Windows
- Description:** Assignment Description
- Assignment Groups:** To whom do you want to assign this app? (W10Client01a(grantZTRNEL) X)
- Deployment Begins:** 06/04/2021 12:00 AM (GMT-05:00) Eastern Time (US & Canada)
- App Delivery Method:** Auto (selected), On Demand
- Hide Installation Notifications:** (toggle off)
- Allow User Install Deferral:** (toggle off)
- Display in App Catalog:** (toggle on)

At the bottom right, there are 'CANCEL' and 'CREATE' buttons. The 'CREATE' button is highlighted with a red box.

9. On the **Carbon Black Cloud Sensor 64-bit- Assignment** page,
 - Under **Distribution** enter next to :
 - **Name:** Type **Carbon Black Sensor for Windows**
 - **Assignment Groups**, select the SMART Group you created earlier, starts with **W10Client0a1**
 - **Deployment Begins**, **Go back one day** (in terms of today's date)
 - **App Delivery Method**, select **Auto radio button**
 - Select **CREATE** at the bottom of the page



10. On the **Carbon Black Cloud Sensor 64-bit- Assignment**

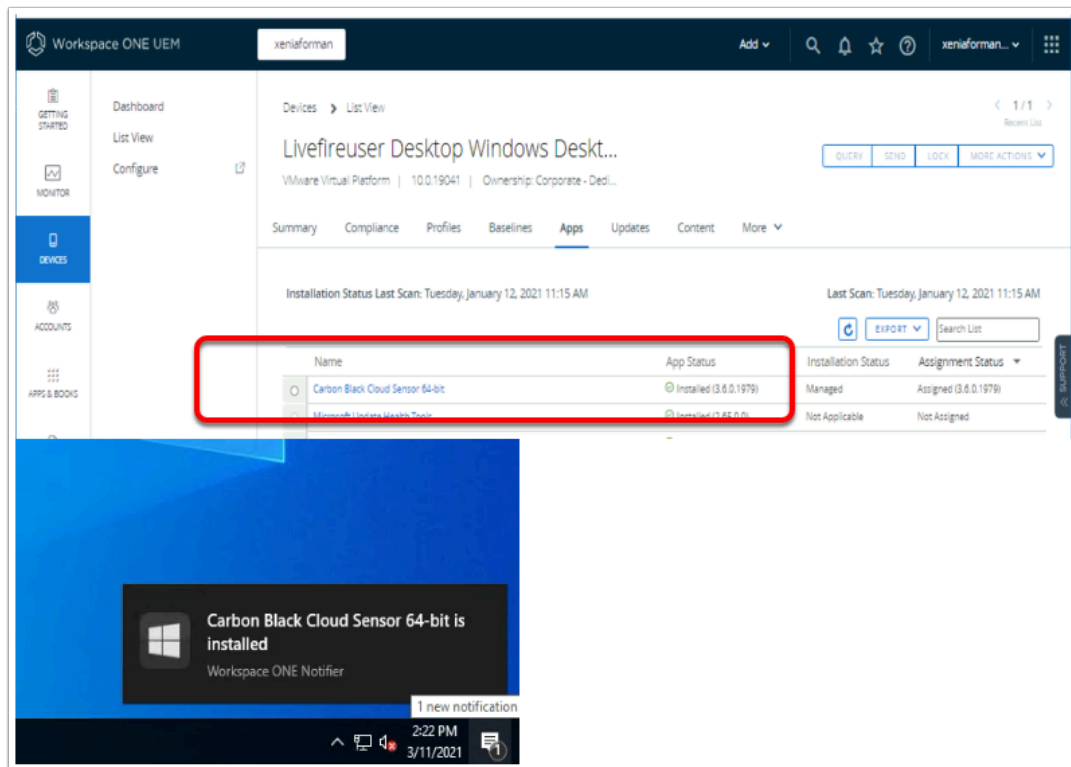
- Select **PUBLISH**

💡 The CB sensor package will be published to any Windows devices enrolled into this UEM organization group.

2.2: Observe device behaviour in VMware Carbon Black

Workspace ONE UEM will push the VMware Carbon Black MSI package and install the Sensor with the correct company Code.

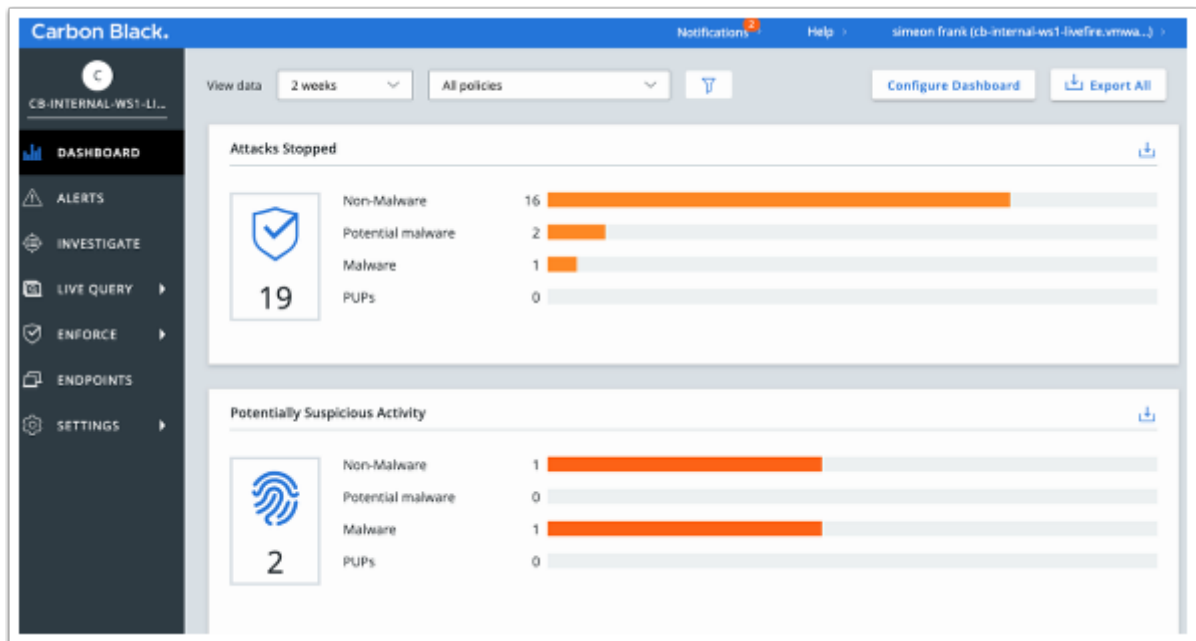
Note: This may take up to 5 minutes. Take a break!



1. On the ControlCenter server,

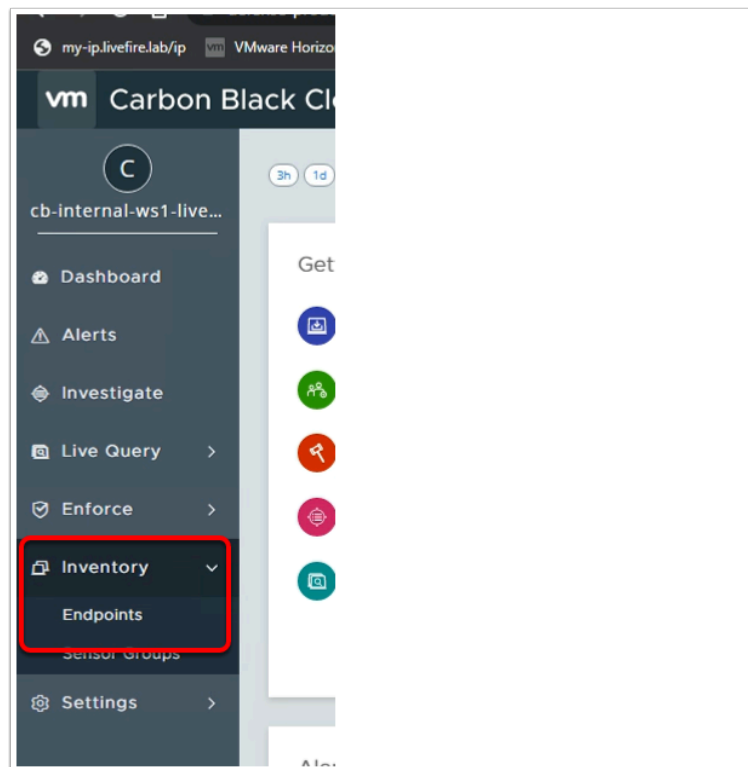
- If you aren't already signed into your Workspace ONE UEM console
 - Login to the cn-livefire.awmdm.com tenant
- Navigate to **Devices** > **List View**
- Select your **device**
- Select the **Apps** Tab
- Make sure the **VMware Carbon Black Cloud Sensor 64-bit** has a green Check box next to it.

❗ If you see the status as failed or Not Installed, re-trace your steps and double check the MSI install command in the previous chapter.



2. On the **ControlCenter** desktop

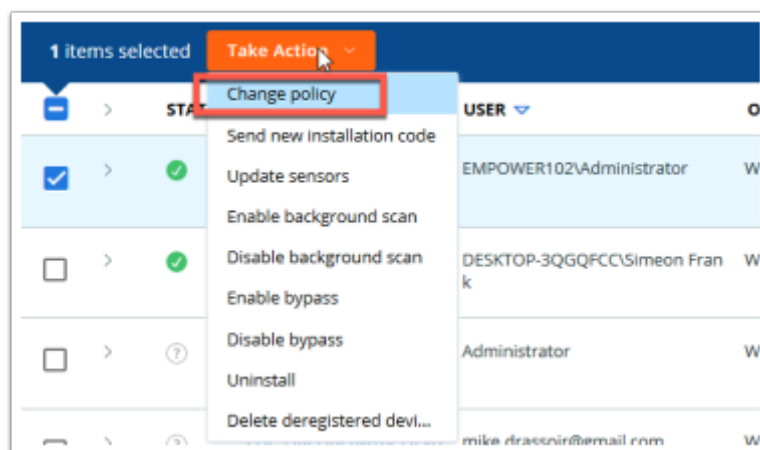
- Open a browser and navigate to <https://defense-prod05.conferdeploy.net/>
- Sign in with your **e-mail address** and **password** assigned to you.



3. In the **VMware Carbon Black Cloud** console

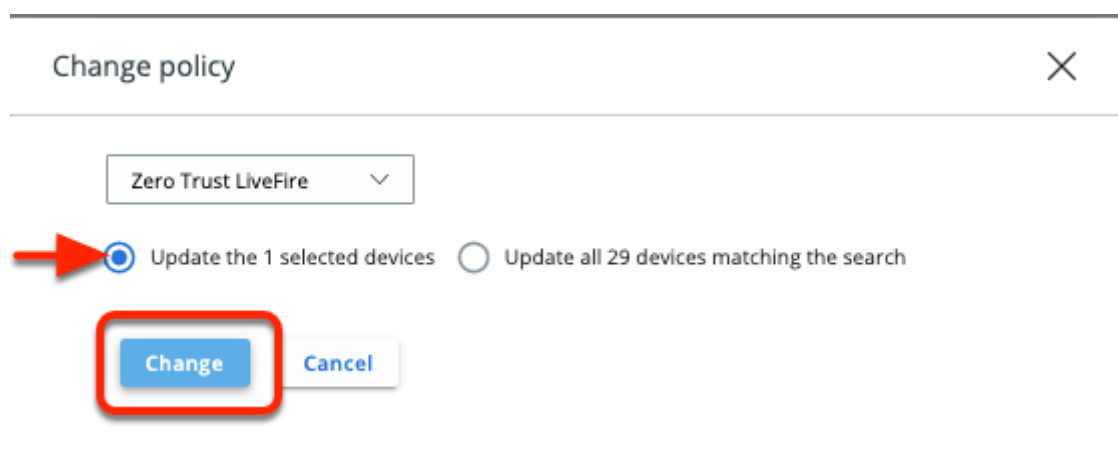
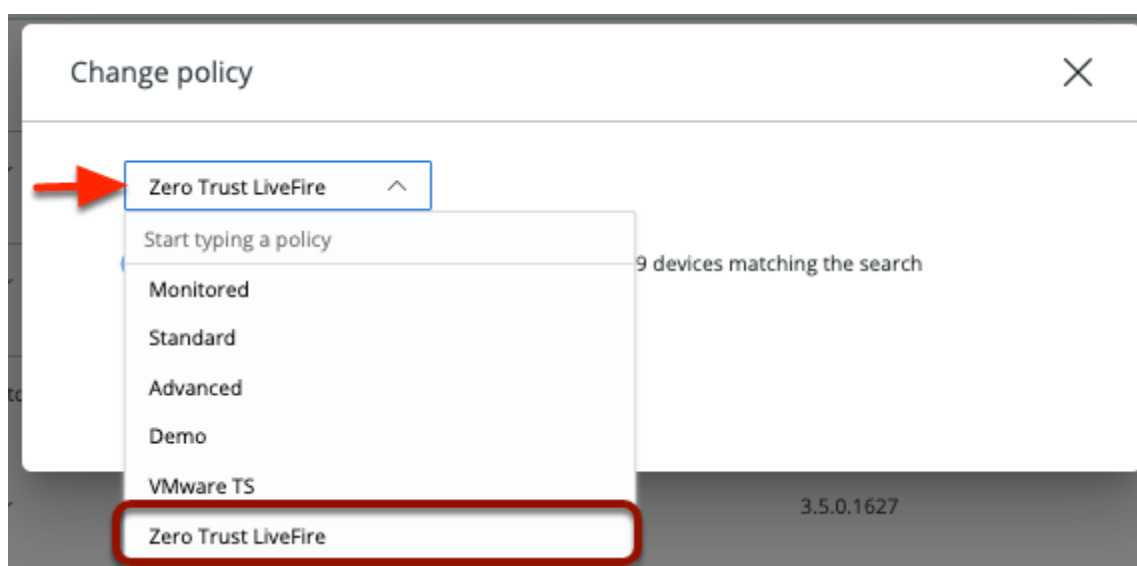
- In the left hand navigation, expand **Inventory**
 - Select **Endpoints**
 - Identify your Device with the computer name that you set. (i.e. AttendeeXXX)

- Click on the **Check Box** next to your device



4. In the Endpoints window

- Select **Take Action** drop down and click **Change policy**

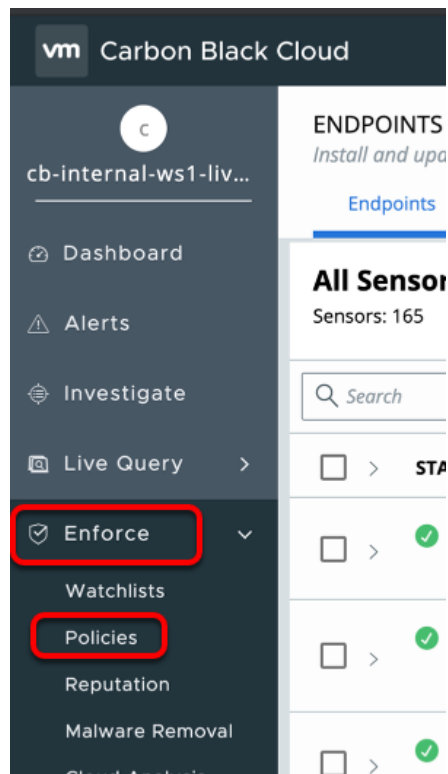


5. In the **Change Policy** window

- In the dropdown, select **Zero Trust LiveFire**

- Select **Change**. (NOTE: Ensure you have the selection set to '**Update the 1 selected devices**').

This will change the Endpoint policy to **Zero Trust Livefire** Policy. Lets look at what exactly this policy is enforcing on our endpoints.



6. In **Carbon Black Admin** console, in the left navigation panel,
- Navigate to **Enforce > Policies**

NAME	DEVICES
Monitored	0
Standard	4
Advanced	0
Demo	0
VMware TS	0
Zero Trust LiveFire	0

General | Prevention | Local Scan | Sensor

General

* Policy name

Monitored

Policy description

No prevention. Use to detect activity before moving endpoints into a prevention policy, or for mission critical endpoints.

Target value

Multiplier when calculating the threat level for detected issues and resulting alerts. Medium is the baseline/default.

Medium

Sensor UI: Detail message


- Under **NAME** for the list of available policies,
 - Select the **Zero Trust Livefire Policy**.

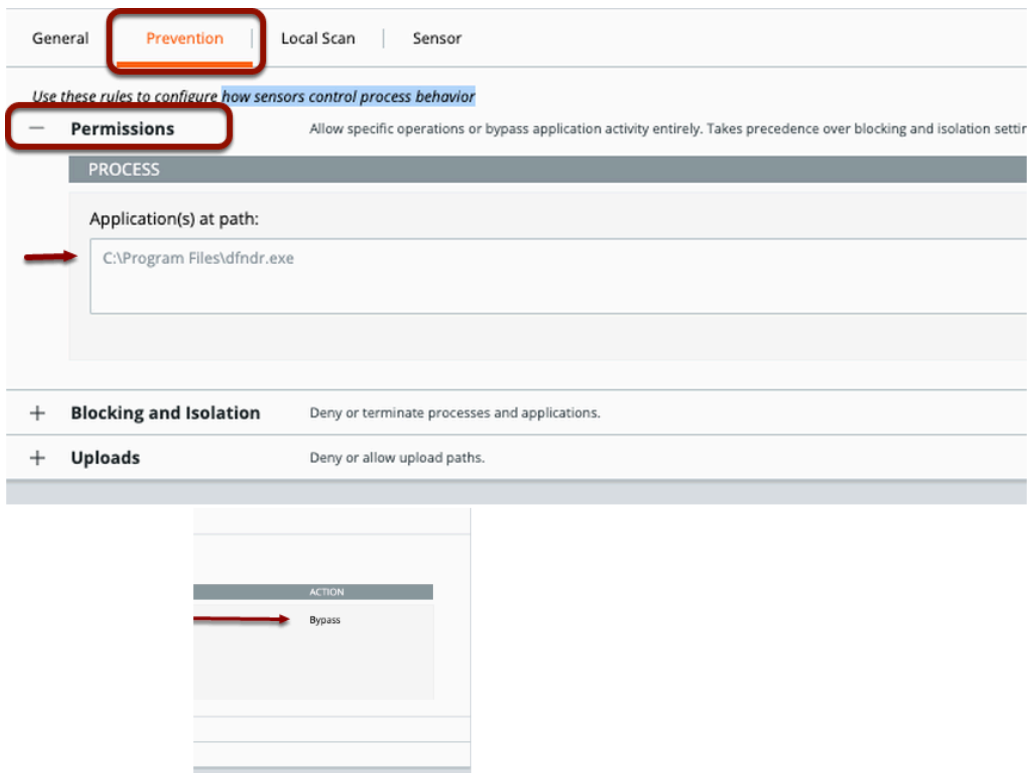
General | **Prevention** | Local Scan | Sensor

Use these rules to configure how sensors control process behavior

+ Permissions	Allow specific operations or bypass application activity entirely. Takes precedence over blocking and isolation settings below.
+ Blocking and Isolation	Deny or terminate processes and applications.
+ Uploads	Deny or allow upload paths.

- Click on the **Prevention** tab.

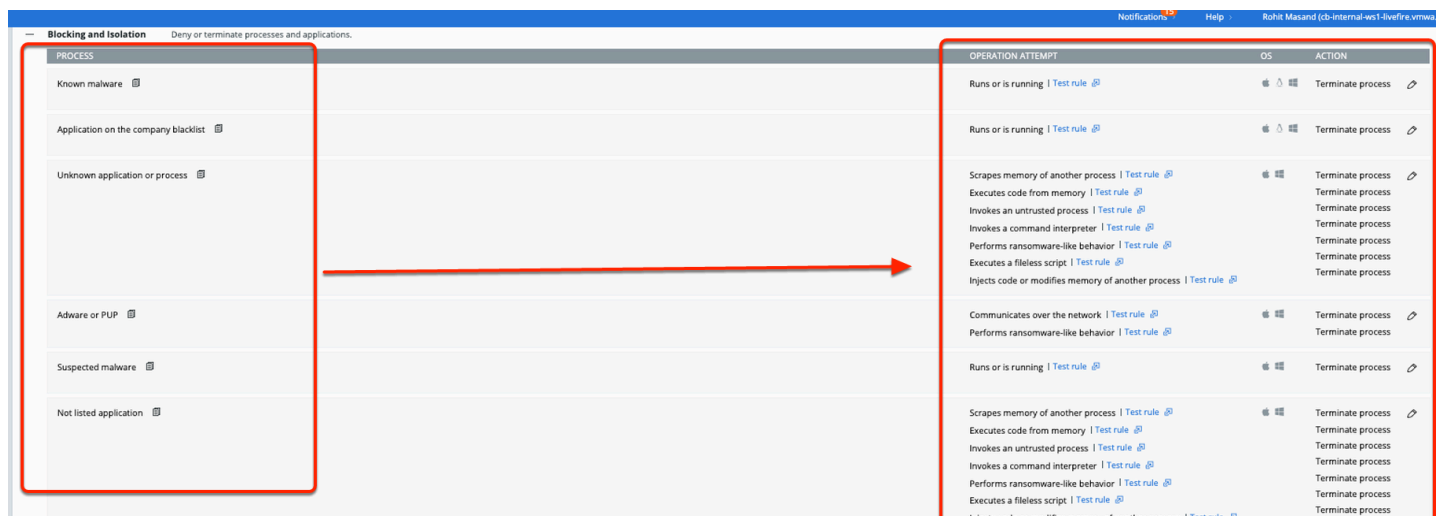
 You will see Permission, blocking & isolation and uploads rules to configure how sensors controls our endpoints.



9. Under the **Prevention** tab

- Expand **Permissions**,
- Notice, the **Application(s) at path: C:\Program Files\dfndr.exe** is set to **Bypass** for any operation.

💡 This can be an example of an internal application which needs to be excluded from any sensor actions.





10. Next, observe the **Blocking and Isolation** Rules,

- Notice it lists all the processes, their operation attempt and the actions this policy will take to prevent an attack.
- In our policy example, we have added **NOTEPAD.exe & Powershell.exe** as blacklisted applications,
 - Any executed processes will **TERMINATE** and any existing attempt to run will be **BLOCKED**

💡 In our LAB environment, you only have read only access and hence cannot make any changes to the policy. In real world, you can choose to perform a deny operation or terminate operation depending upon the use case.

You have successfully completed this section. Please proceed to the next section.

Part 3. Workspace ONE Intelligence API integration & Automation

In this lab you will create the integration between VMware Carbon Black Cloud and Workspace ONE Intelligence.

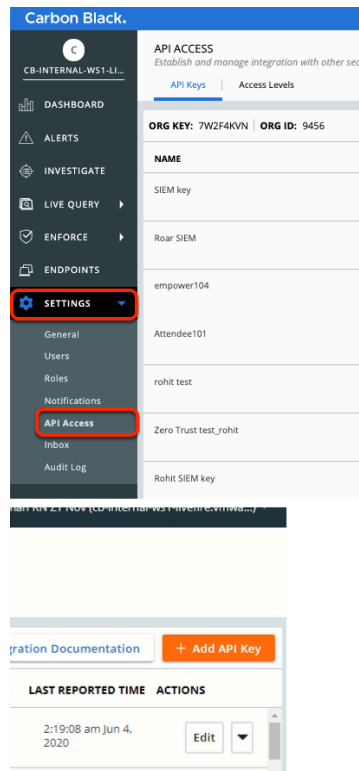
3.1: Create API & SIEM Notifications

3.2: Create VMware Carbon Black & Workspace ONE UEM Connectors

3.3: Create Dashboard and Widget

3.4: Create Automation

3.1: Create API Keys



1. Adding an API Key.

- On the left hand navigation pane. Expand **Settings** and select **API Access**
- In the top right corner of the Admin Console, select **+ Add API Key**

Add API Key [X]

1 * Name
Attendee222

Description

2 * Access Level type
Custom

3 * Custom Access Level
Zero Trust

Warning: This permission set may contain unversioned APIs. Visit developer.carbonblack.com for all currently supported/versioned APIs.

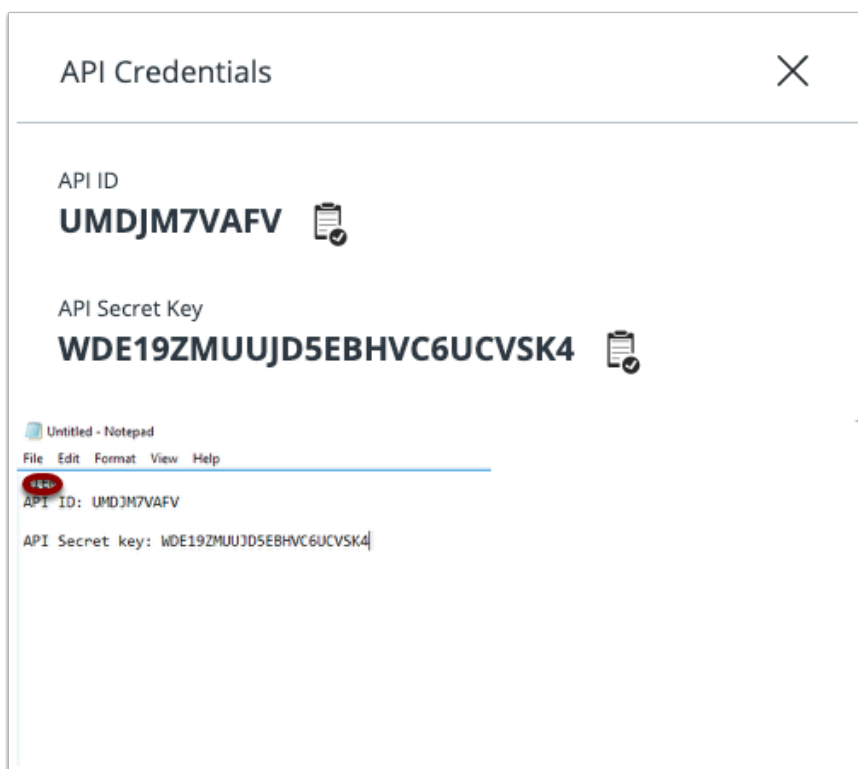
Authorized IP addresses
Specify a comma separated list of single IP address, or an IP address range in CIDR notation (for example, 203.0.113.5/32).

4 [Save] [Cancel]

2. Enter the below information,

1. Name the API key your **unique attendee Identifier**. EXAMPLE: **Attendee101**
2. Select **Custom** in the Access Level type
3. Select **Zero Trust** for Custom Access Level
4. Select **Save** at the bottom of the window.

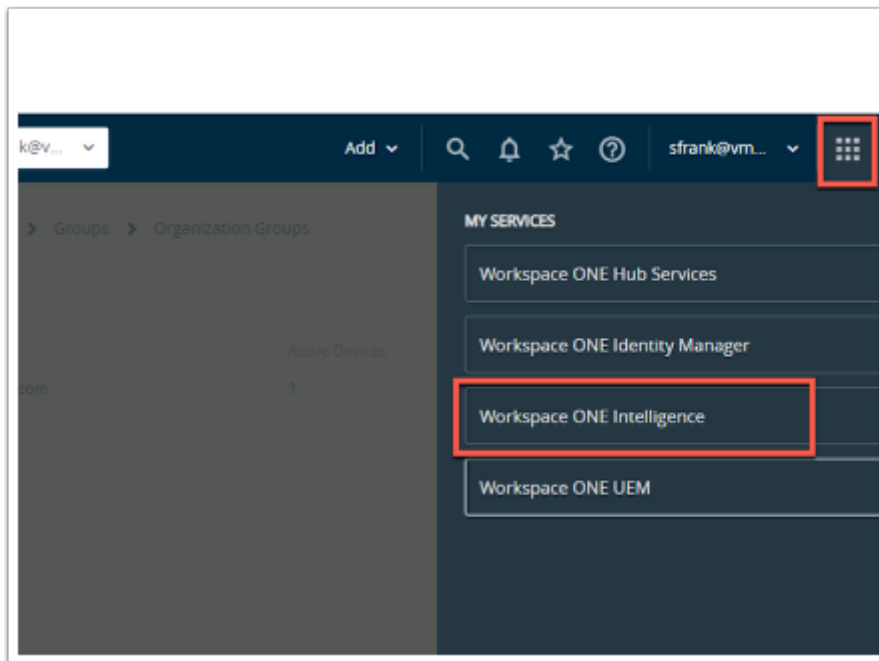
NOTE: For the integration with Intelligence the API Access Level must include the "Data Forwarder" settings



3. You will now be shown the **API Credentials**.
 1. **Copy** both the **API ID** and the **API Secret Key** to Notepad.
 2. Close out of the API Credentials windows by clicking **X**

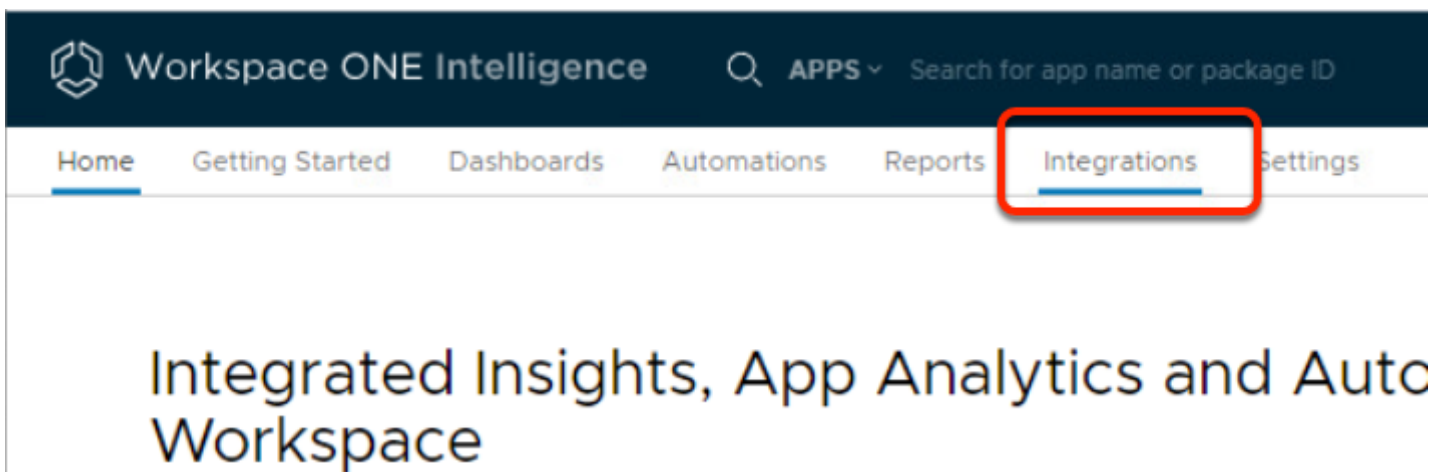
3.2: Configuring VMware Carbon Black & Workspace ONE UEM Connectors

In order to send Alerts received in VMware Carbon Black portal to Workspace ONE Intelligence, we will be configuring a VMware Carbon Black Connector in Workspace ONE Intelligence. This requires us to use both VMware Carbon Black console API Key & SIEM API Key. Security Information and Event Management (SIEM) API allows you to capture security events generated on the VMware Carbon Black platform in your Workspace ONE Intelligence console.



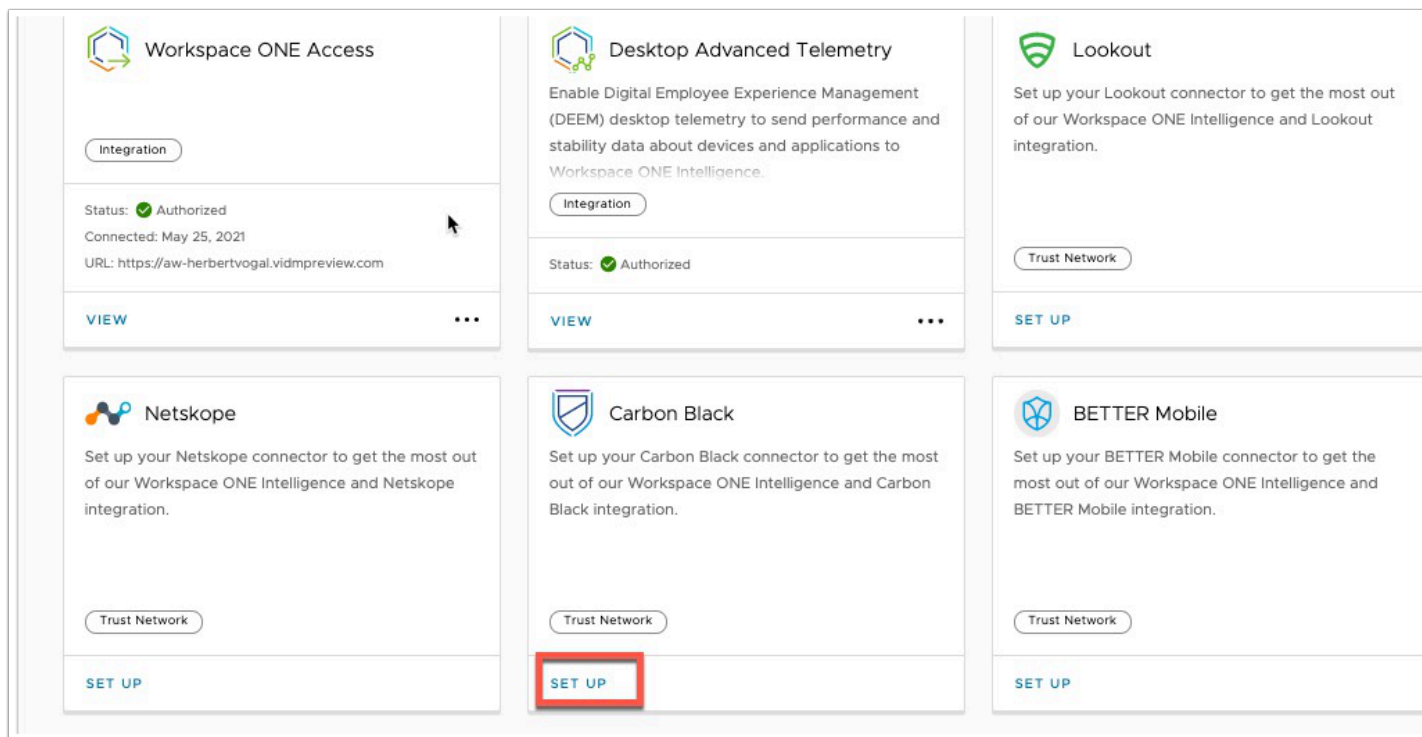
1. On the ControlCenter

- Switch to your Workspace ONE UEM console,
 - If necessary navigate to <https://cn-livewire.awmdm.com>.
 - Sign in using your admin credentials (E-mail used to attend the course)
- In the top right corner, select the **MY SERVICES** icon (9 squares)
 - Select **Workspace ONE Intelligence**



2. In the Workspace ONE Intelligence Admin console

- Select the **Integrations** tab



3. Under Integrations section

- **Scroll down** to find the **Carbon Black** tile,
- Select **SET UP**

Edit Connector: Carbon Black

Intelligence would like to get access to Carbon Black for the following:

> Connector Permissions

▼ Authorization Details

[Click here for more information on how to set up this connector.](#) [More information](#)

Payload Body

Base URL:

API ID:

API Secret Key:

Org Key:

[CANCEL](#) [SAVE](#)

4. In the **Authorize Connector: Carbon Black** console

- Expand the **Authorization Details** dropdown. Enter the following information, next to:-
 - **Base URL:** <https://defense-prod05.conferdeploy.net>

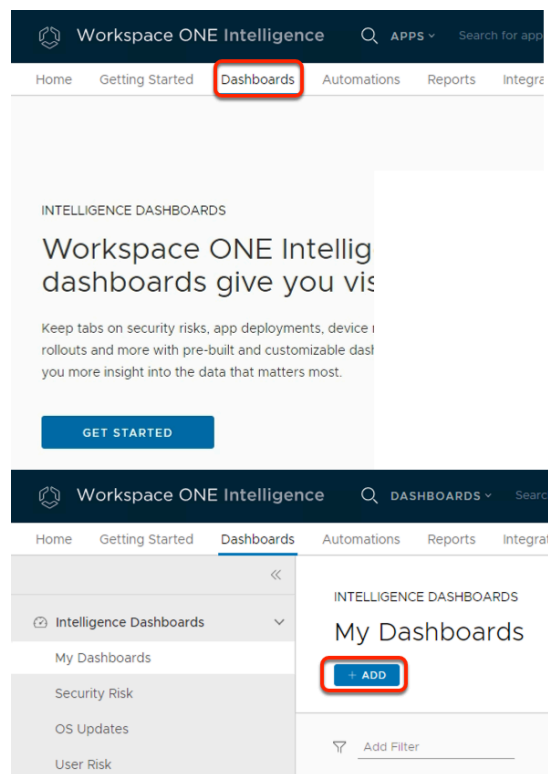
- **API ID:** {Paste the API ID from your notepad above}
- **API Secret Key:** {Paste the API secret Key from the notepad above}
- **Org Key:** 7W2F4KVN

- Select **AUTHORIZE**

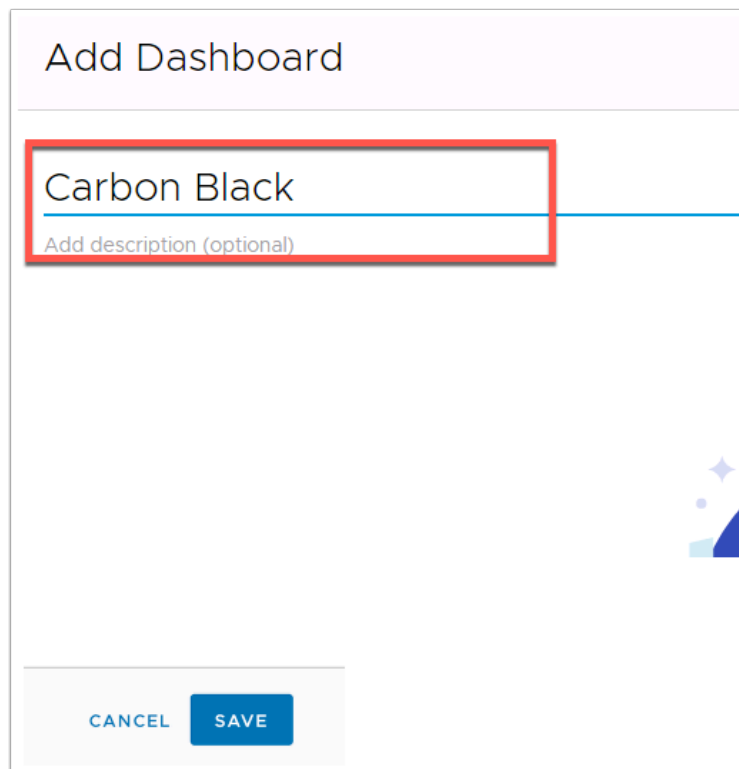
NOTE: The Org Key identifies the Carbon Black Tenant and is unique to each Carbon Black Cloud instance.

3.3: Create Dashboard & Widget

We will now create a Dashboard and a Widget for VMware Carbon Black



1. In the Workspace ONE Intelligence Console
 - In menu bar, select the **Dashboards** tab
 - In the **Dashboards** area
 - Select **Get Started**
 - In the **My Dashboards** section
 - Select **+ADD**



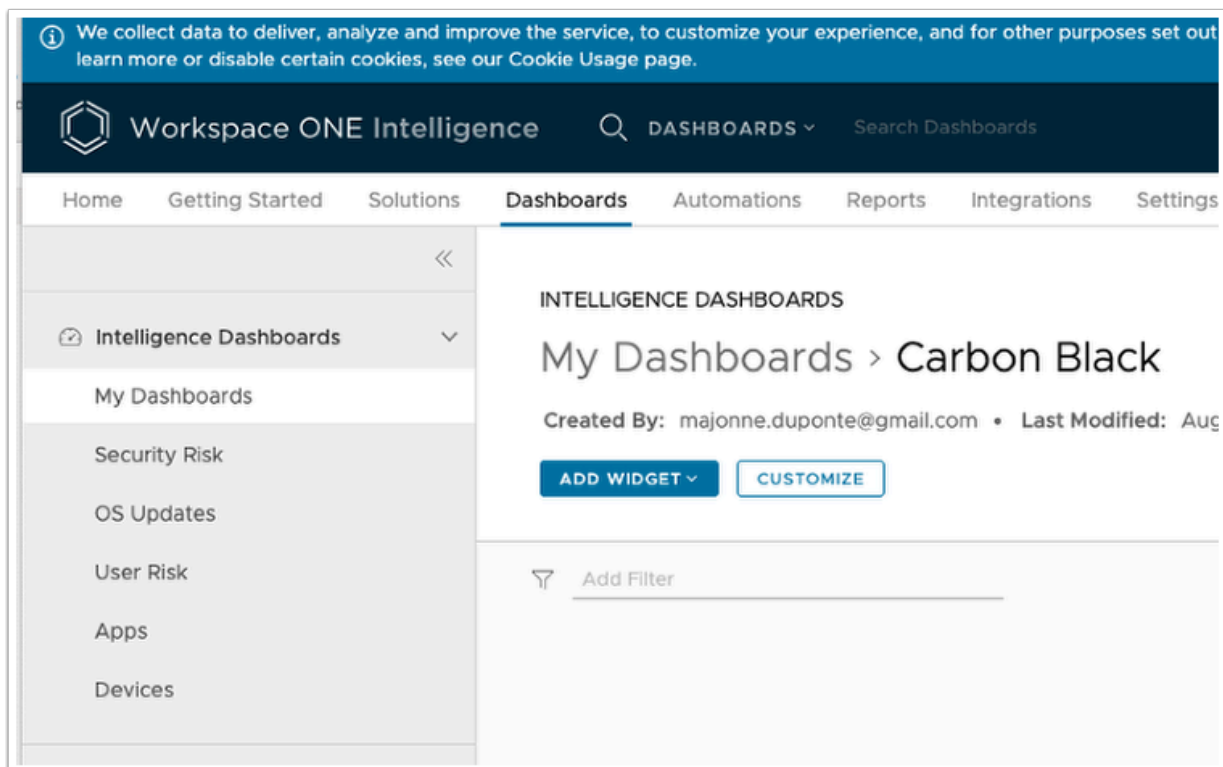
Add Dashboard

Carbon Black

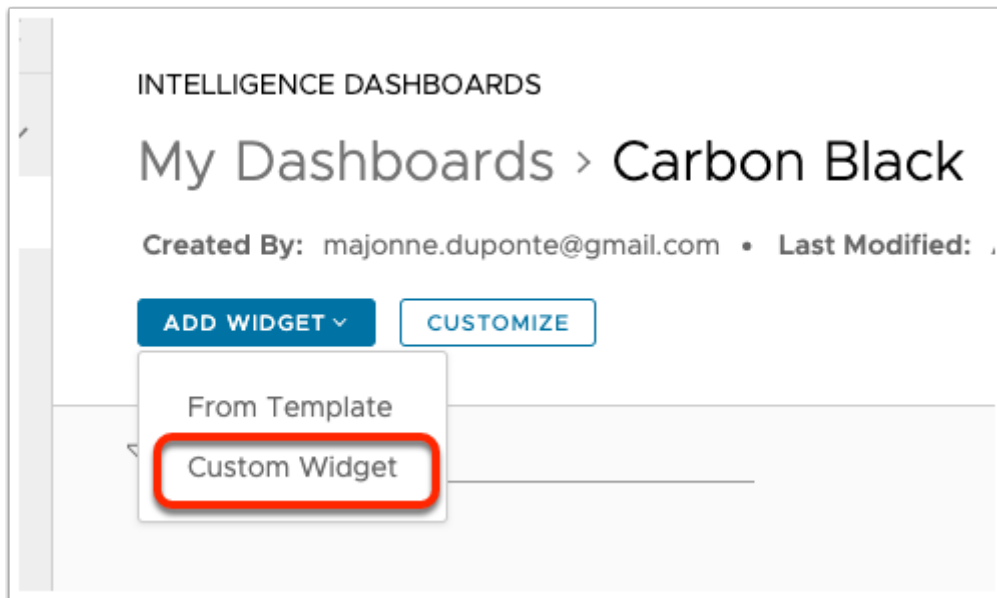
Add description (optional)

CANCEL SAVE

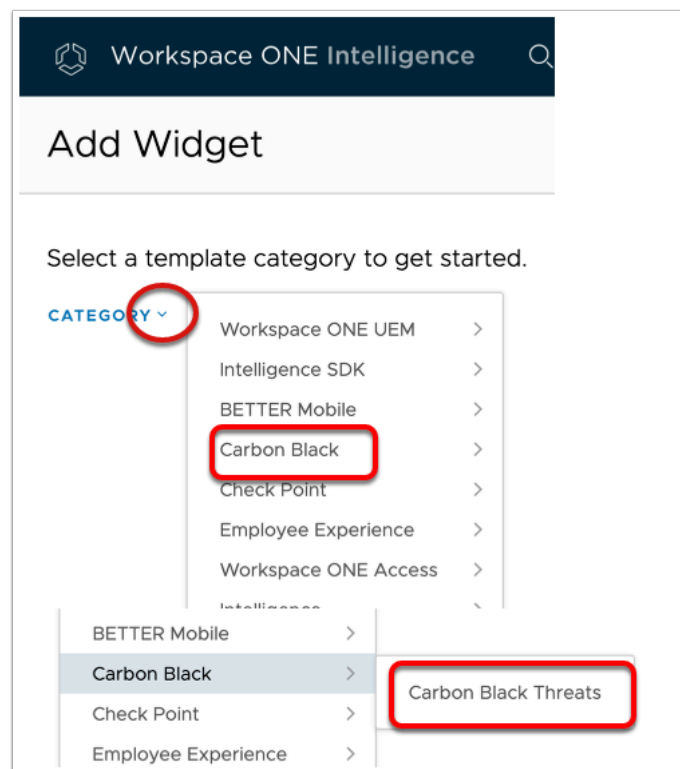
2. In the **Add Dashboard** window
 - Name the dashboard **Carbon Black**
 - In the bottom right of the page, select **SAVE**



3. In my **My Dashboards > Carbon Black** area
 - Select **ADD WIDGET**



4. In the MY Dashboards > Carbon Black
 - From the dropdown, select **Custom Widget**



5. In the Add Widget window
 - Select the **dropdown** next to **CATEGORY**
 - Select **Carbon Black > Carbon Black Threats**

Add Widget

Template: Custom Widget Category: Carbon I

Add description (optional)

Data Visualization ⓘ

SNAPSHOT HISTORICAL

6. In the **Add Widget** screen,
- Replacing the "Name your widget" with **Medium & High Severity**

Data Visualization ⓘ

SNAPSHOT HISTORICAL

Chart Type

VERTICAL AREA LINE METRIC TABLE HEAT MAP

Chart Type

VERTICAL
AREA
LINE
METRIC
TABLE
HEAT MAP

Measure Count of Carbon Black Device ID


Group by (Optional) Carbon Black Device E × Carbon Black External × Carbon Black Incident × Carbon Black Severity × Platform ×

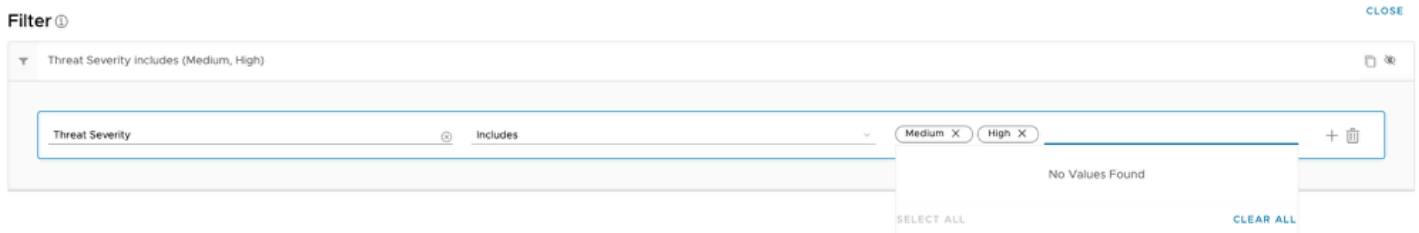
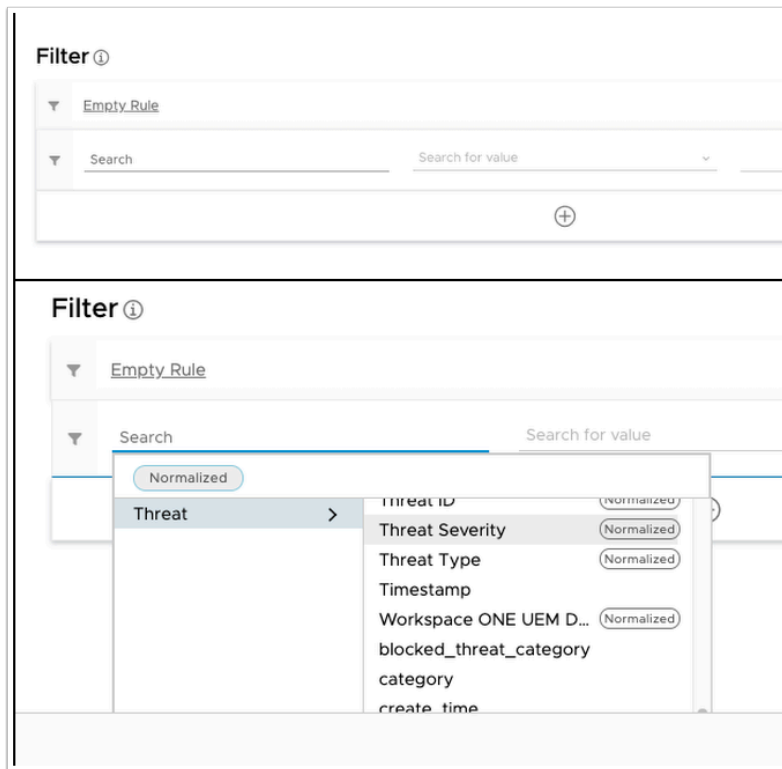
Results per group 10

Date Range (Optional) Last 28 days

7. In the Add Widget screen,

1. Under **Data Visualization > Chart Type**, Select **TABLE**.
2. Fill in the following fields: **Next TO**
 - **Measure:** **Count** of **Carbon Black Device ID**. (Choose from drop down)
 - **Group by (Optional):** select from the dropdown **Carbon Black Device Email**,
 - Next to **Carbon Black Device Email**, select **ADD SUBGROUP**
 - Select from the dropdown **Carbon Black Device External IP Address**
 - Next to **Carbon Black Device External IP Address**, select **ADD SUBGROUP**
 - Select from the dropdown **Carbon Black Incident ID**, select **ADD SUBGROUP**
 - Select from the dropdown add **Carbon Black Severity Score**, select **ADD SUBGROUP**
 - Select from the dropdown select **Platform**.
 - Next to **Date Range**, ensure that the **Last 28 days** is configured

 **Note:** These are mere suggestions, any given attribute coming from VMware Carbon Black could be selected to be displayed






8. In your Custom Widget


- Under **Filter**,
- In the **Search** area, under **Empty Rule**, select **Threat > Threat Severity**
- In the second drop down select **INCLUDES**
- In the third drop down type **Medium** and hit **ENTER on your Keyboard**
- In the same field, type **High** and hit **Enter** on your Keyboard.
- Select **SAVE** at the top of the page.

My Dashboards › Carbon Black

Created By: rmasand@vmware.com • Last Modified: Sep 5, 2021 • Last Modified By: rmasand@vmware.com • Last Modified Widget: Medium & High Severity


 Date Range 

 Device Organization Group Name includes All
2 AND Organization Group Hierarchy includes All

ADD WIDGET  **CUSTOMIZE**

 Add FilterMedium & High Severity  Platform   Date Range   Table 9. In **INTELLIGENCE DASHBOARDS**

- Select **SAVE**

 **NOTE:** If you are not seeing Medium in the dropdown, it means Workspace ONE Intelligence has not yet received any Medium Alerts from VMware Carbon Black Portal. You can simply type in **medium** and hit **enter**.

Part 4: Create Automation

We now will create an automation from the widget we have just created.

My Dashboards > Carbon Black

Created By: rmasand@vmware.com • Last Modified: Sep 5, 2021 • Last Modified By: rmasand@vmware.com • Last Modified Widget: Medium & High Severity

Date Range

Device Organization Group Name includes All
2 AND Organization Group Hierarchy includes All

ADD WIDGET CUSTOMIZE

Add Filter

Medium & High Severity

Platform Date Range Table

No Data Available

Info
Edit
Automate
Refresh
Export as .CSV
Copy to
Add to Bookmarks
Duplicate
Rename
Set as thumbnail
Delete

VIEW

1. In the **Carbon Black** Dashboard,
 - In the **Medium & High Severity** widget
 - At the bottom , right corner of the widget, select the **more options** icon (**three horizontal dots**).
 - Select **Automate**

NOTE: if you don't see the three dots, you may not have saved the dashboard at the top of the page

Workspace ONE Intelligence AUTOMATIONS Search Automation Name

Add Workflow

Category: Carbon Black: Carbon Black Threats

Name your workflow !

Generated from widget: Low&Medium Severity (Carbon Black)

Trigger (When) ⓘ

Cb Carbon Black: Carbon Black Threats Data

☒ Automatic ⓘ

Filter (If) ⓘ

Threat Severity equals (medium)

2. In the **Add Workflow** window

- In the **Name your workflow** area, give the Workflow a title: **Tag Malware Device & Notify Admin**

Filter (If) ⓘ CLOSE

Threat Severity includes (Medium, High)

Threat Severity Includes 2 selected X

+

Action (Then) ⓘ

3. Under the Filter (if) area

- In **Threat Severity** row, at the end select the **+ icon**

Filter (If) ⓘ CLOSE

1 Threat Severity equals (High medium) ⓘ

2 AND Carbon Black Device Name equals (EUC-LIVEFIRE\GrantFLZT29) ⓘ

AND

Threat Severity ⓘ Equals ▾ High medium ▾ + ⌵ ⌵

Carbon Black Device Name ⓘ Equals ▾ EUC-LIVEFIRE\GrantFLZT29 ▾ + ⌵ ⌵

4. Under the **Filter (if)** area

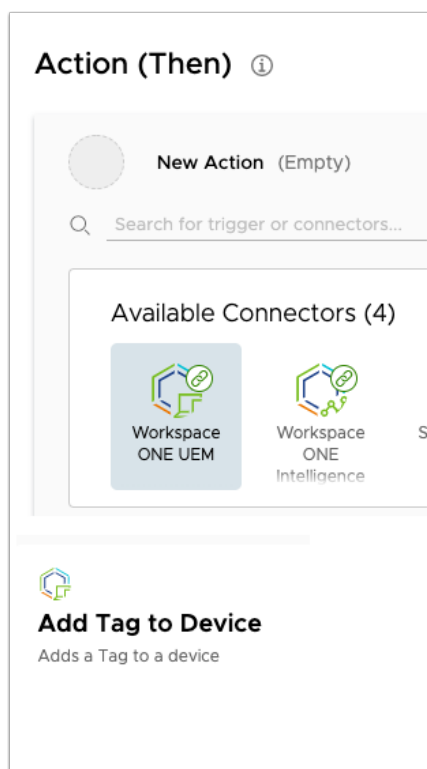
- Under **Threat Severity** in the **Search** area, select **Carbon Black Device Name**
- Next to **Carbon Black Device Name**, from the dropdown change **includes** to **equals**
- In the the third n choose your **device** (eg **Attendee22**)

Action (Then) ⓘ

+

3. In the **Add Workflow** window

- Scroll down to **Action (Then)** and select the ⊕



4. In the **Add Workflow** window
 - Under Available Connectors, select **Workspace ONE UEM**
 - Scroll down to the right and select **Add Tag to Device**

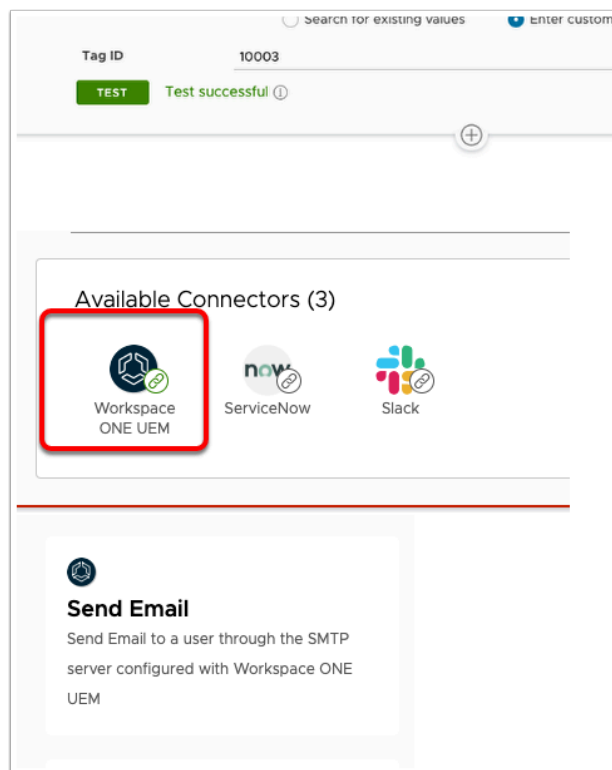
Action (Then) ⓘ

5. In the Tag ID field, Type **10000**. This sets the Tag "**Quarantine**" on the device. At the bottom of the **Action (Then)** area select **+**

i Note the Tag Name Quarantine is a custom TAG created in Workspace ONE UEM

To view the location,

- Go to Groups & Settings > Groups > All Settings > Device & Users > Advanced > Tags
- Note the Quarantine Tag has already been defined



6. In the Action (Then) area

- At the bottom select the **+ sign**
- Under **Available Connectors**,
 - Select the **Workspace ONE UEM** connector,
 - Select the **Send Email** Connector

Workspace ONE UEM → Send Email ⓘ

Body

To Address: rmasand@vmware.com

Subject: Malware detected

Message: The following threat is detected on your device:

Path Variables: Device ID: \${airwatch.de}

TEST

Normalized

Threat	Alert Category	Normalized
Carbon Black Device Name	Carbon Black CB Defense Event ID	
Carbon Black Device OS Version	Carbon Black Data Stream Type	
Carbon Black Device Priority Code	Carbon Black Device Email	
Carbon Black Device Priority Type	Carbon Black Device ID	
Carbon Black Event Description	Carbon Black Device Name	
Carbon Black Event Occurred Time		
Carbon Black External IP Address		
Carbon Black Group Name		
Carbon Black Incident ID		
Carbon Black Internal IP Address		
Carbon Black Main Process Hash (...)		

7. In the Workspace ONE UEM > Send Email

- In the Send Email, add the following next to
 - Address: **your e-mail address**
 - Subject: **Malware detected**
 - Message :
 - USE THE LOOKUP OPTION TO POPULATE THE BELOW INFORMATION OR MANUALLY TYPE IT IN, DONT COPY AND PASTE

The following threat is detected on your device :

Device ID - \${carbonblack.threat.threatinfo_threatcause_causeeventid}

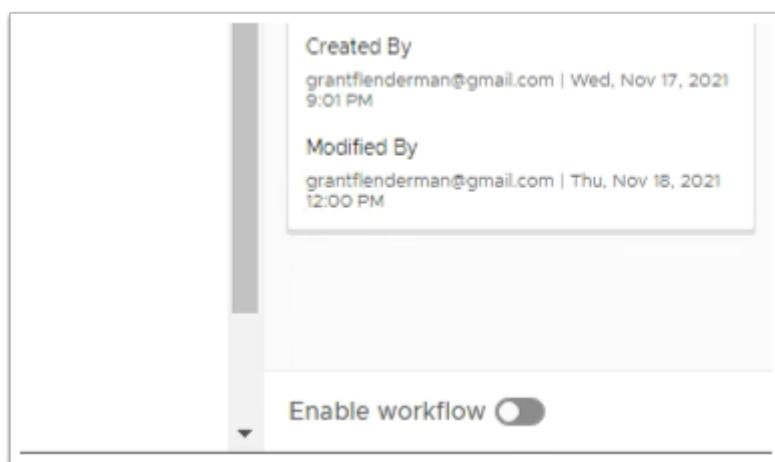
Device name - \${carbonblack.threat.deviceinfo_devicename}

Threat - \${carbonblack.threat.threatinfo_threatcause_actorname}

Threat Severity - \${carbonblack.threat._threat_severity}

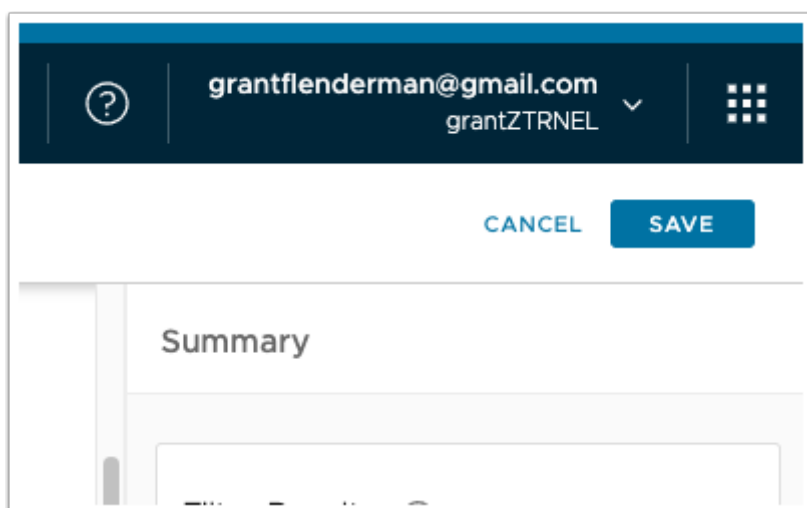
Threat time - \${carbonblack.threat.first_event_time}

Platform - \${carbonblack.threat._device_platform}



8. In the Workflow interface

- Look in the bottom right-corner and you will notice a toggle with **Enable workflow** next to it
- Move the **Toggle** to the right



9. In the Workflow interface

- In the top right corner, select **SAVE**


and refresh summary panel.

One-time Manual Run ☐ OFF

Do you want to save the workflow?

Save Workflow

This workflow will constantly monitor and run on new data that matches your criteria. To view how many filtered results may be affected, go back and refresh summary panel.


 Actions will immediately execute on filtered results.

One-time Manual Run ☒ ON

Do you want to save the workflow?

10. In the **Save Workflow** window

- Next to **One-time Manual Run**, move the **toggle** from an **OFF** position to the right to turn on
- Select **SAVE & RUN**

 Your automation should now be live. Let's trigger an event on your device to see this take effect.

Part 5. VMware Carbon Black Incident & Workspace ONE Intelligence Automation

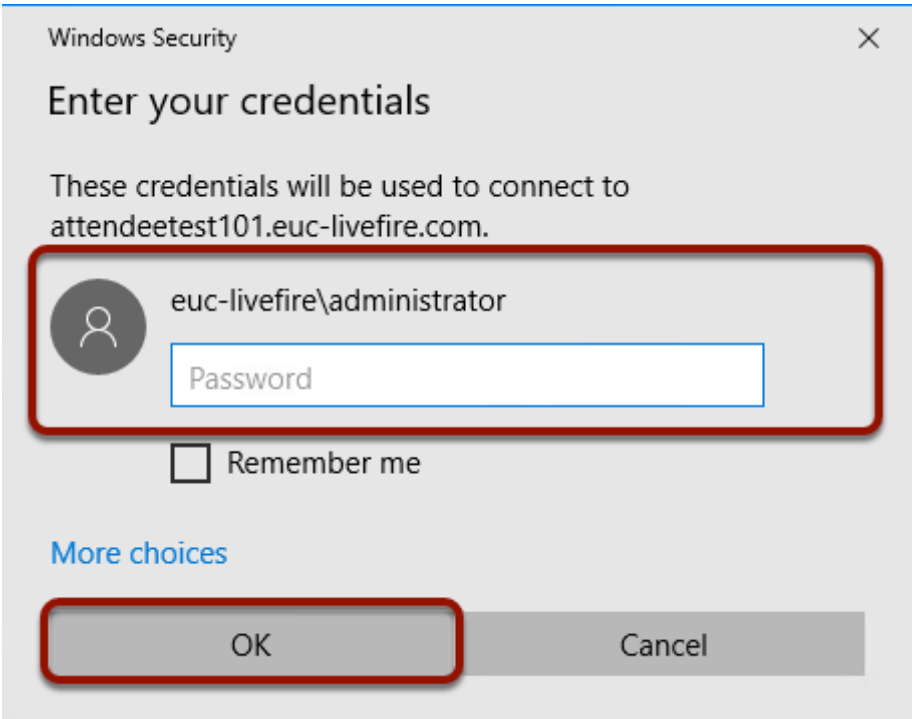
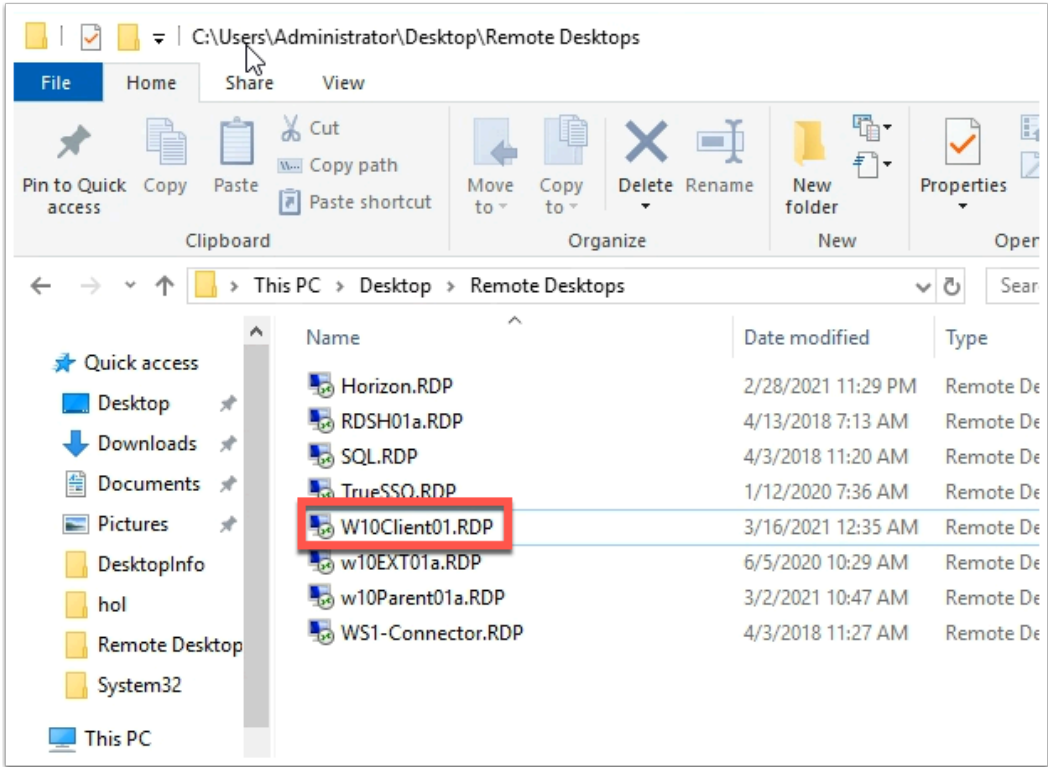
You are now ready to demo threat remediation using Workspace ONE intelligence and VMware Carbon Black. This section had two parts:

5.1: Incident

5.2: Notification

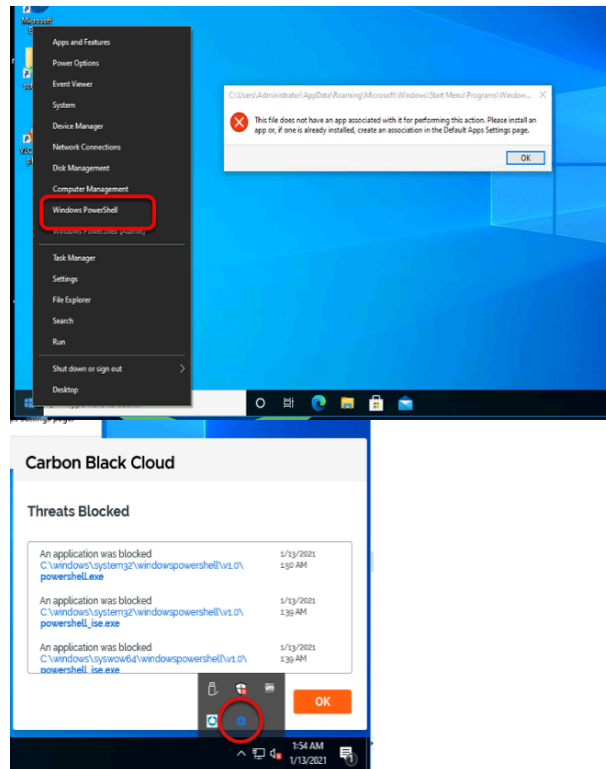
5.1: Incident

We will now create an incident. As we don't have the means to infect this vm with malware we will use Notepad++ as an example of a malicious application.

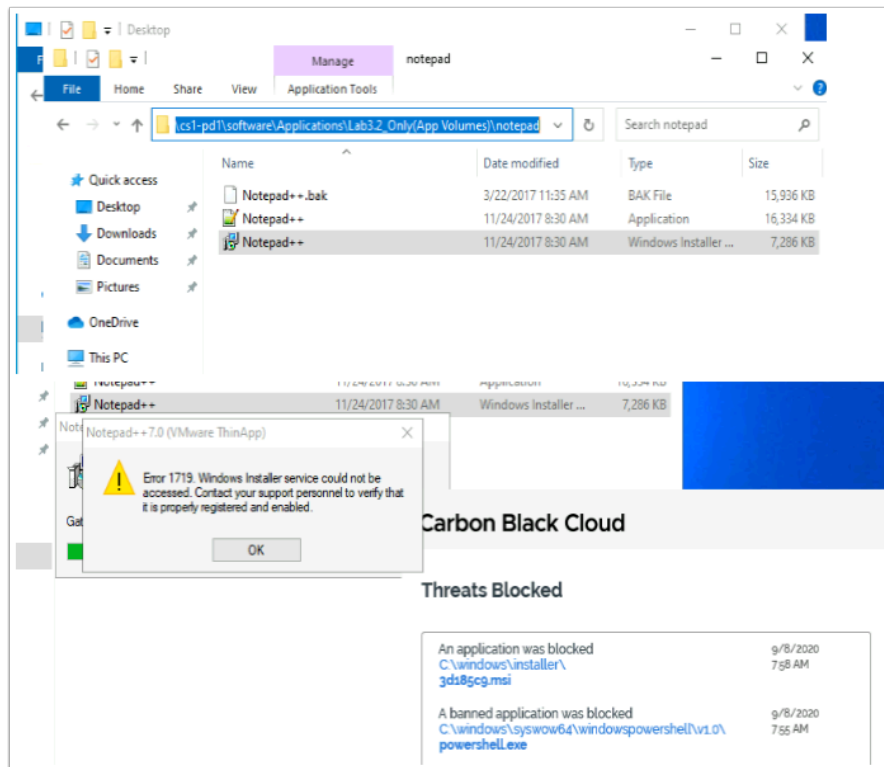


1. On the ControlCenter

- Open the **Remote Desktop** folder
- Connect to your **W10client01 RDP** virtual machine with your new hostname.



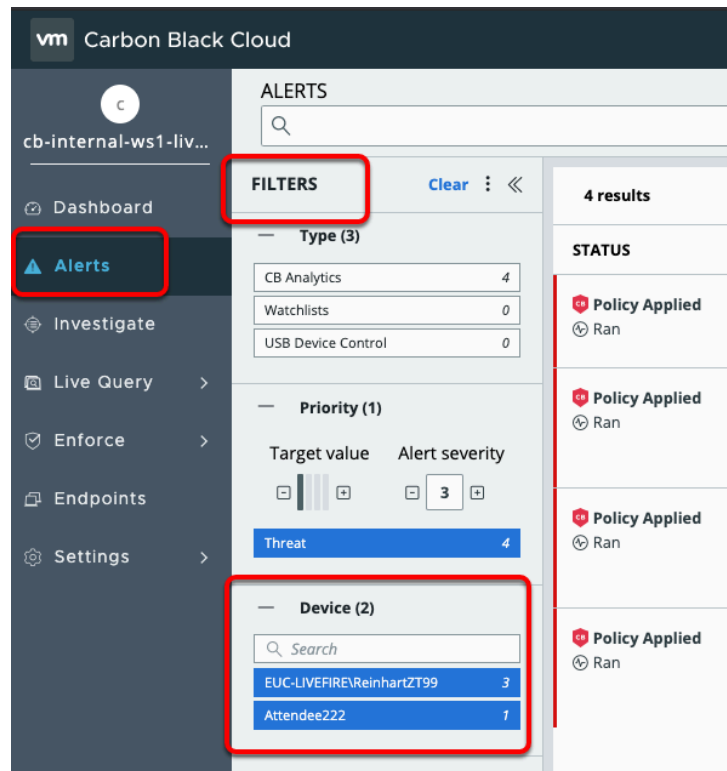
2. On the W10Client02 virtual machine
 - Right-click the **Start** button,
 - Select **Windows PowerShell**.
 - Notice the PowerShell message
 - Select the **Carbon Black** Sensor in the right-hand corner
 - Notice the configured Threats that have been blocked.
 - Select **OK** to close



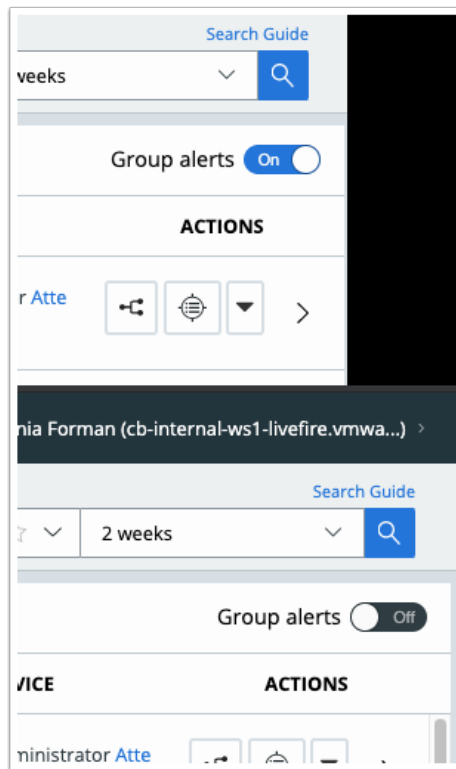
3. On your Windows Desktop

- Select **Start > Run**
- Enter the following UNC Path [\\horizon.euc-livefire.com\software\Applications\Lab3.2_Only\(App Volumes\)\notepad](\\horizon.euc-livefire.com\software\Applications\Lab3.2_Only(App Volumes)\notepad)
- **Copy** the **Notepad++ msi** to your Desktop
- Attempt to **execute** this MSI.
 - Notice the installation of Notepad++ is blocked
 - Note that this is not a standard Notepad++ msi package but a ThinApp package that offers application isolation and even with this, the sensor is able to block the installation and execution on the device.
- Attempt to **rename** the MSI and re-execute see what happens

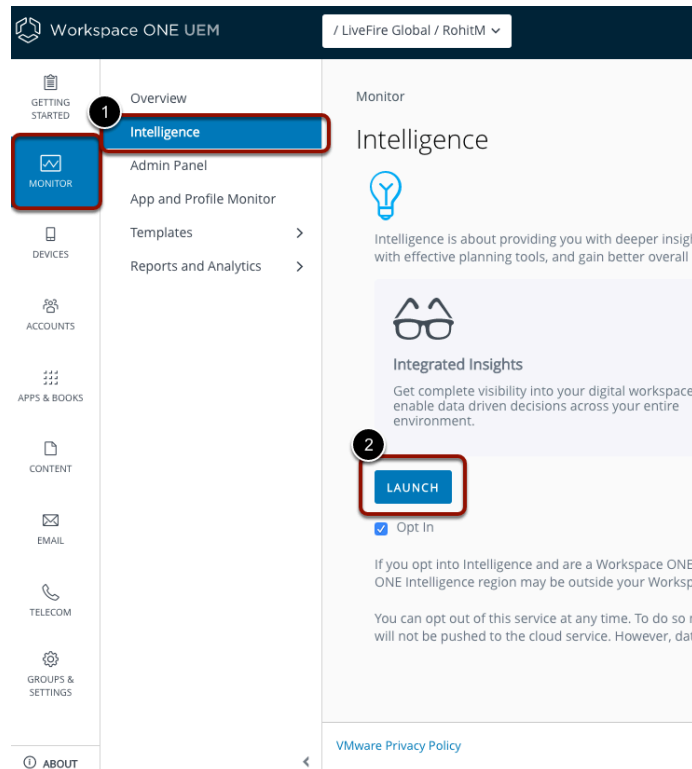
5.2: Alert & Automation



1. Log into the Carbon Black **Cloud Admin console**.
 1. Navigate to **Alerts** from the left menu bar.
 2. Under **FILTERS** menu, expand **DEVICE** and select your **endpoint** i.e. AttendeeXXX.
 - In the right-hand pane, observe **STATUS** of Alert as a Deny Policy Action and the Alert Severity.

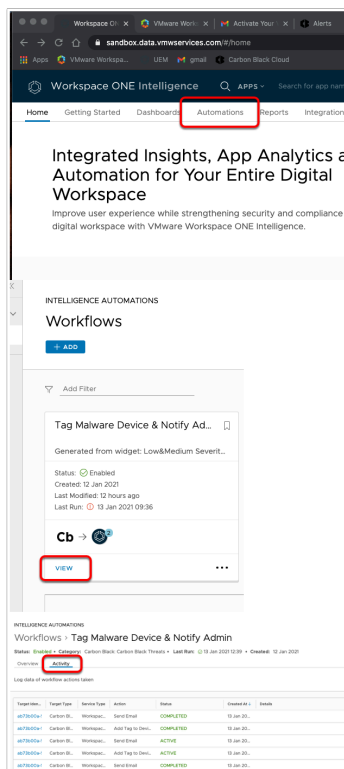


- ❗ NOTE: Ensure GROUP ALERTS is set to OFF. If not, ensure to set it to OFF to view your specific endpoint alert.
- Move the **Toggle** in the right-hand corner from **On** to **Off**



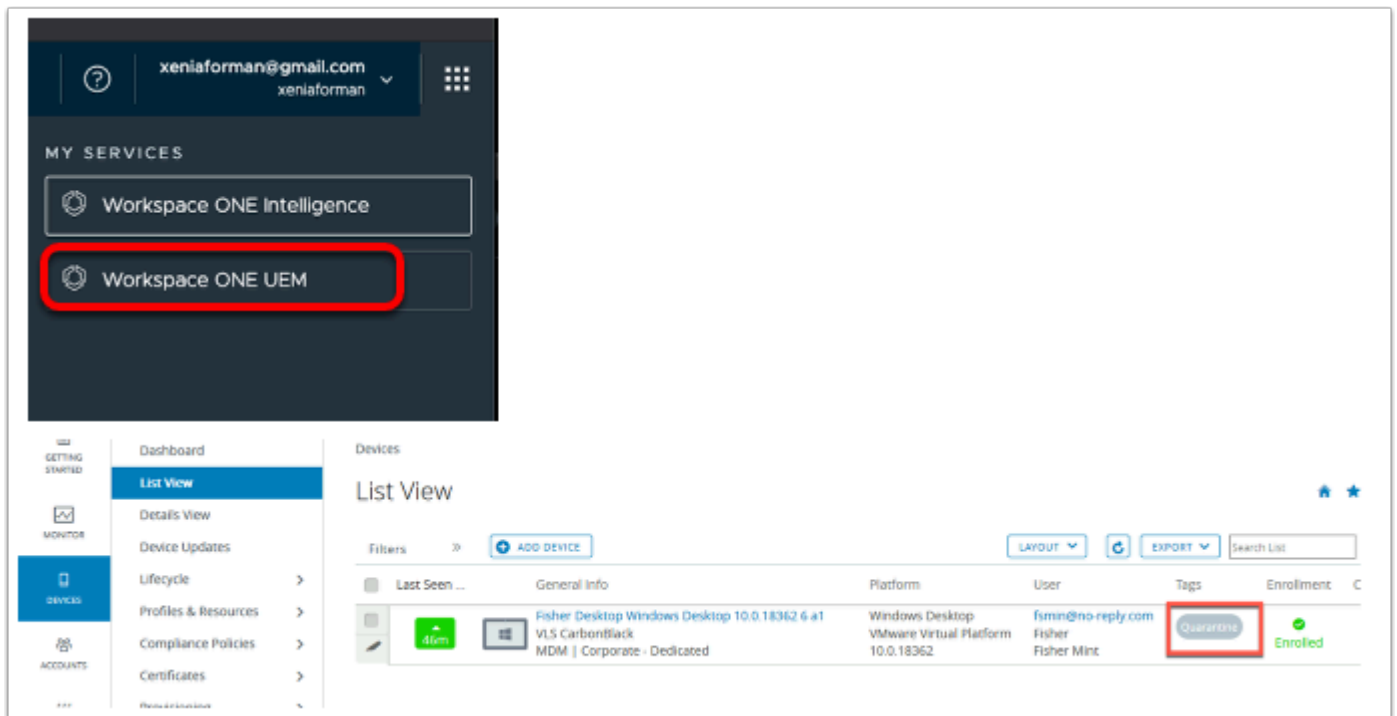
2. Switch to the **Workspace ONE Intelligence console.**

- Login to **cn-livewire.awmdm.com** with your admin credentials.
- Navigate to **Monitoring > Intelligence.**
- Select **LAUNCH**

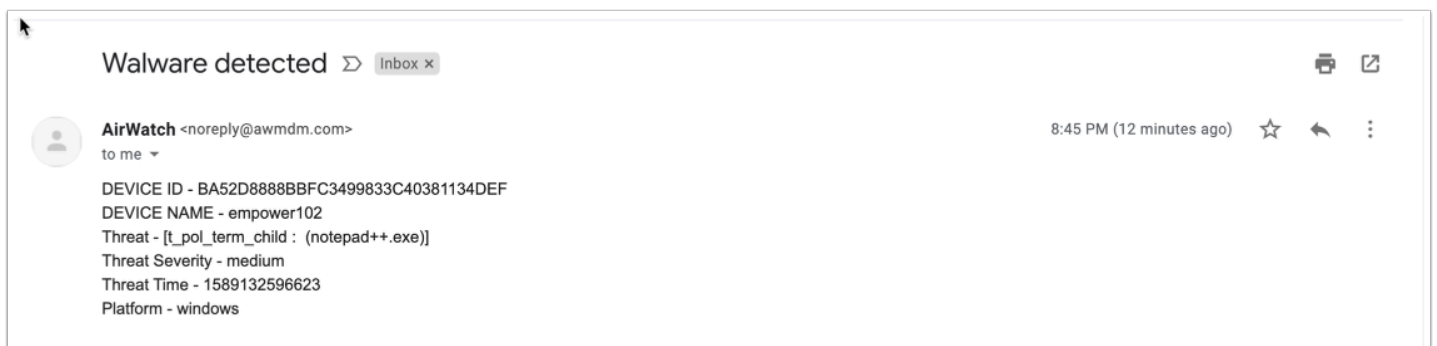
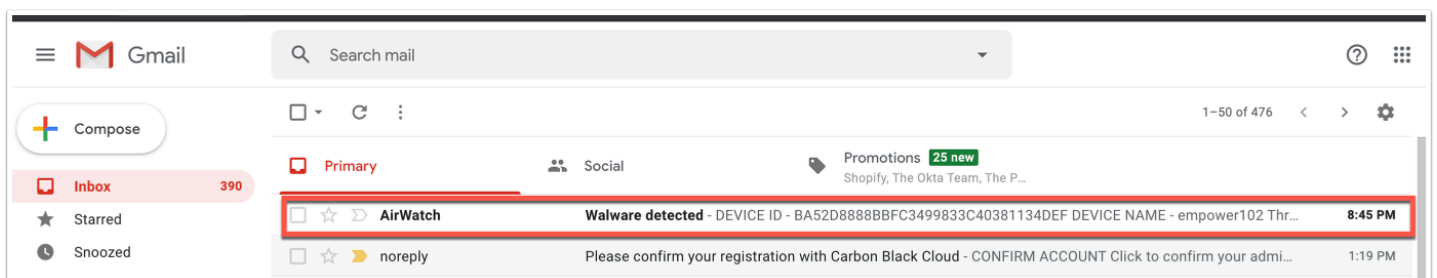


3. In the Workspace ONE Workspace ONE IntelligenceConsole,

1. Select **Automations**
2. Select **VIEW** on your Carbon Black automation
3. Next to Overview, select the **Activity** tab
 - You should see the events, the tag being assigned and the e-mail being sent to the admin.



4. Switch to the Workspace ONE UEM console,
 1. Navigate to **Devices > List View**
 2. You will notice the enrolled device has the **QUARANTINE** tag assigned to it



5. Now navigate to your e-mail and notice you have an e-mail from **AirWatch** that has the information for the device that has been compromised.

This ends the lab for VMware Carbon Black Integration with Workspace ONE Intelligence.