COMODO
Creating Trust Online®

Comodo EDR

Software Version 1.7

Administrator Guide

Guide Version 1.1.071619

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

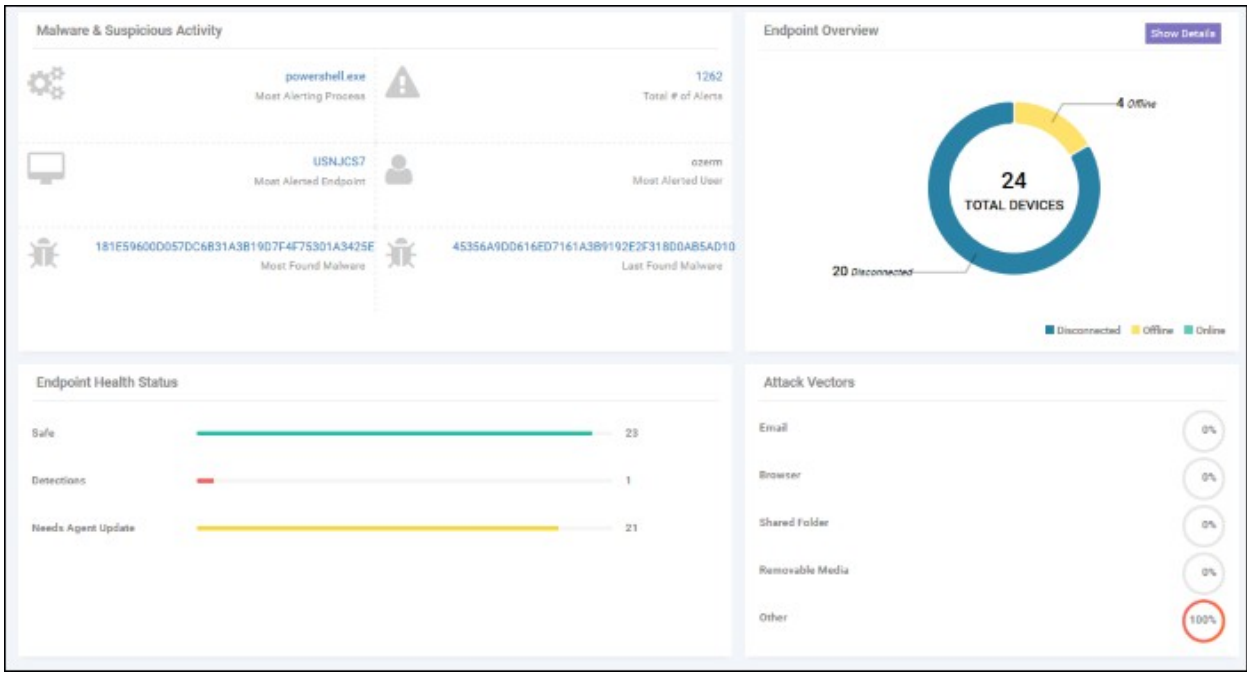
Table of Contents

1 Introduction to Comodo EDR

Comodo Endpoint Detection and Response (EDR) is a powerful event analysis tool that provides real-time monitoring and detection of malicious events on Windows endpoints. EDR allows you to visualize threats in a detailed timeline while instantaneous alerts keep you informed if an attack occurs.

EDR's cloud-based admin console can be accessed anytime using an internet browser.

- You can enroll for a free EDR account at **https://edr.cwatch.comodo.com**
- You can login to the EDR admin console at **https://edr.cwatch.comodo.com/login**
- You can also access EDR through your Comodo One/ Comodo Dragon / ITarian account. Login then click 'Applications' > 'cWatch EDR'.
- You must install the EDR agent on all endpoints you wish to monitor. After logging-in, click 'Download Agent' to get started.



Features

- Continuous threat monitoring of managed endpoints
- Advanced search capabilities for file hashes and detection
- Real-time visibility into what's happening in your environment
- Policy customization
- Unrivaled process timeline visualization
- Retrospective analysis of events
- Centralized cloud hosted architecture
- Human analysis of unknown file and event types
- Compatible with other endpoint security tools
- Multi tenancy Support

Guide Structure

This guide is intended to take you through the configuration and use of EDR and is broken down into the following main sections. The guide can also be navigated using the bookmarks on the left.

1.1 Purchase Licenses

There are two ways you can sign up for cWatch EDR.

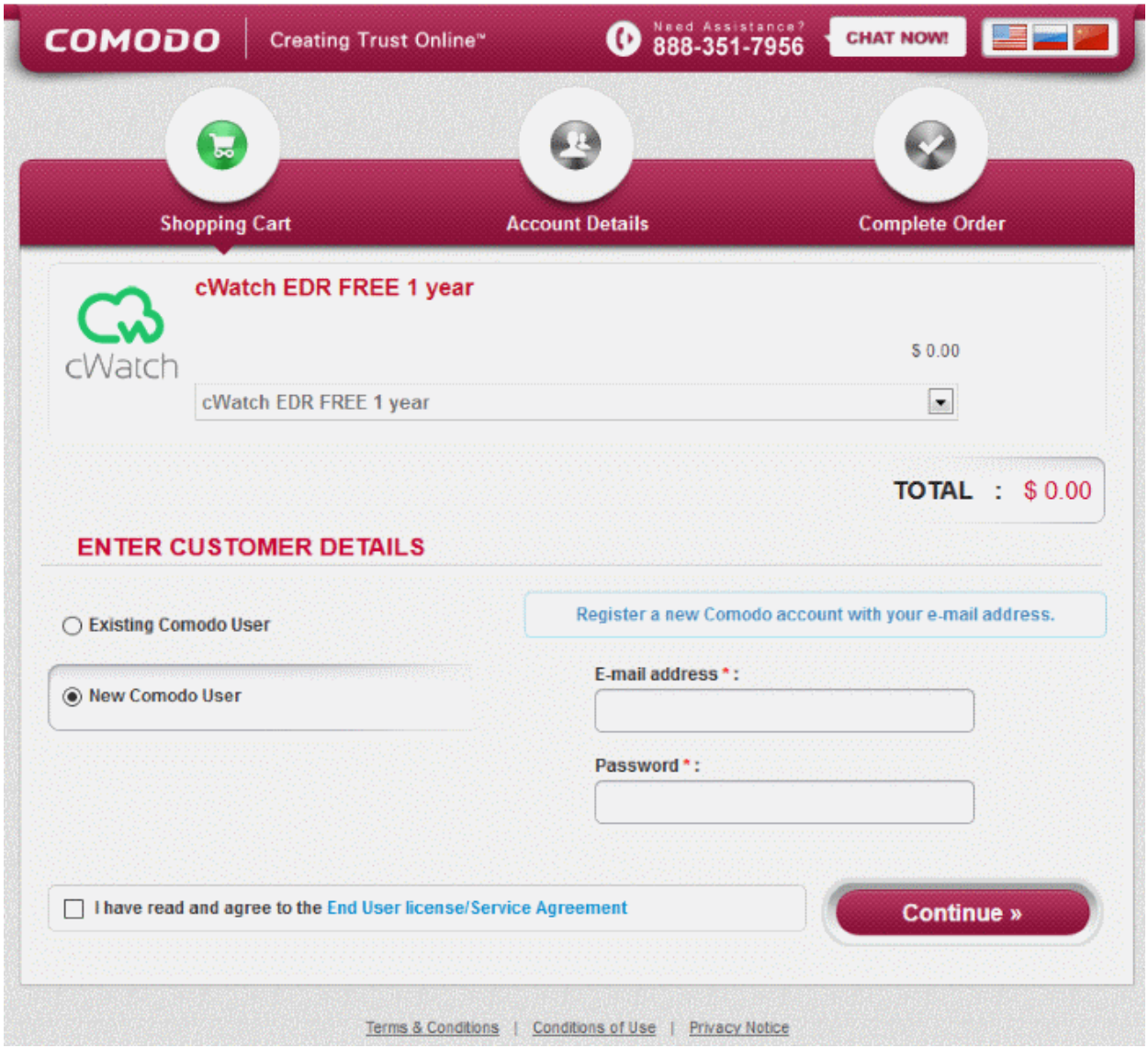
- From cWatch EDR website as stand-alone application
- From your Comodo One / Comodo Dragon / ITarian portal as an integrated application

Stand-alone application

It only takes a few steps to subscribe to the EDR service:

- Visit **https://edr.cwatch.comodo.com/**
- Select your plan and click 'Protect your Endpoints Now'

The purchase page will be displayed:

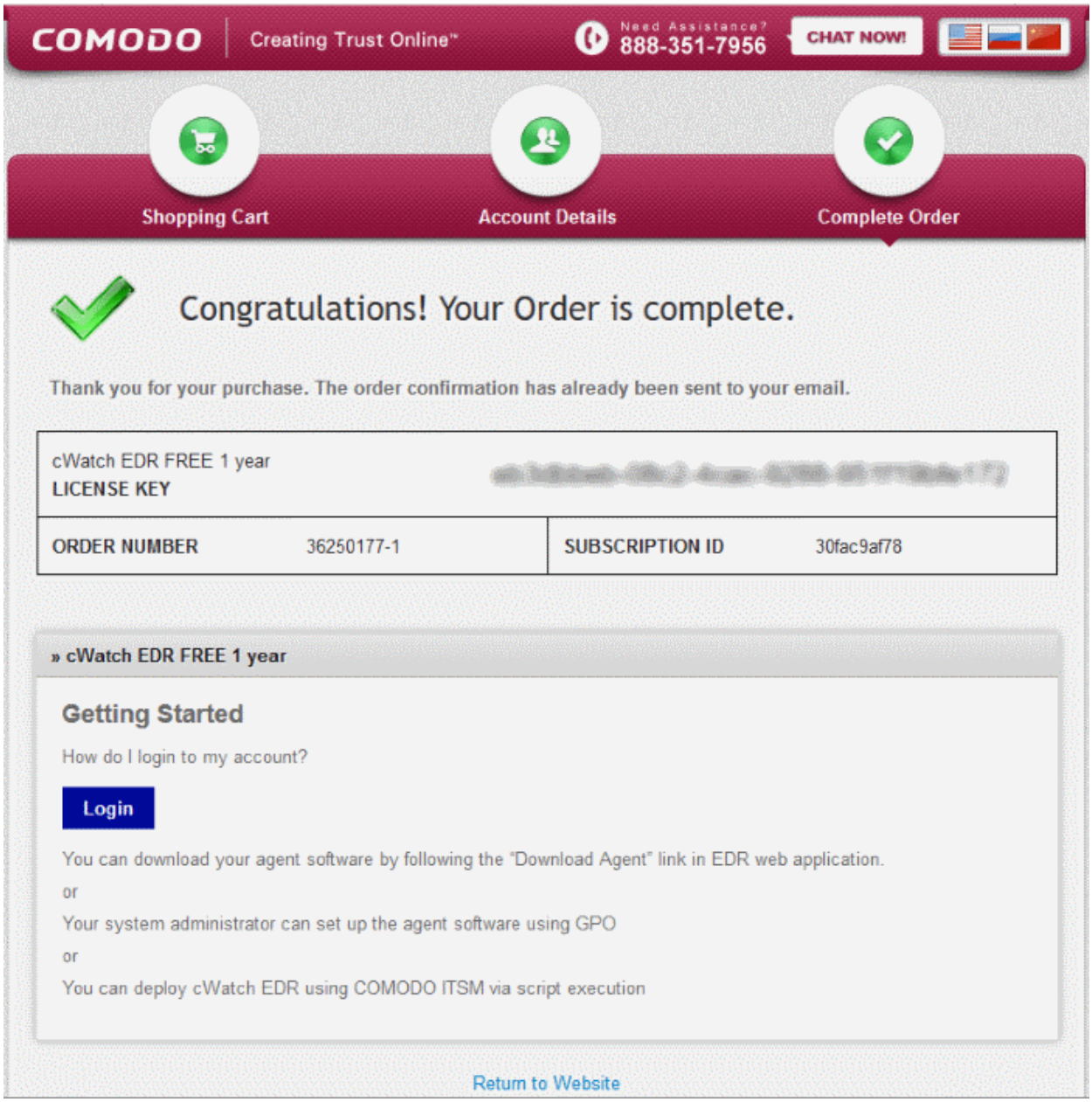


- Select a subscription plan. A free,1 year is also available. You have to provide your credit card details for a paid subscription.
    - **Subscribing for EDR without Comodo Account**
    - **Subscribing for EDR with Comodo Account**

If you do not have a Comodo account:

- Select 'New Comodo User'
- Enter your email address and password in the respective fields
- Provide credit card details if you select a paid subscription
- Click 'End User license / Service Agreement' link, read the EULA fully and select the check-box
- Click 'Continue'

Your order will be processed and a confirmation message will be displayed:



You will also receive a confirmation message to your email address. A new Comodo account (CAM) will be created for you at **https://accounts.comodo.com/**. You can subscribe to various Comodo products using this account. See '**Comodo Accounts Manager**' help guide for more details about how to manage your account.

If you have a Comodo account:

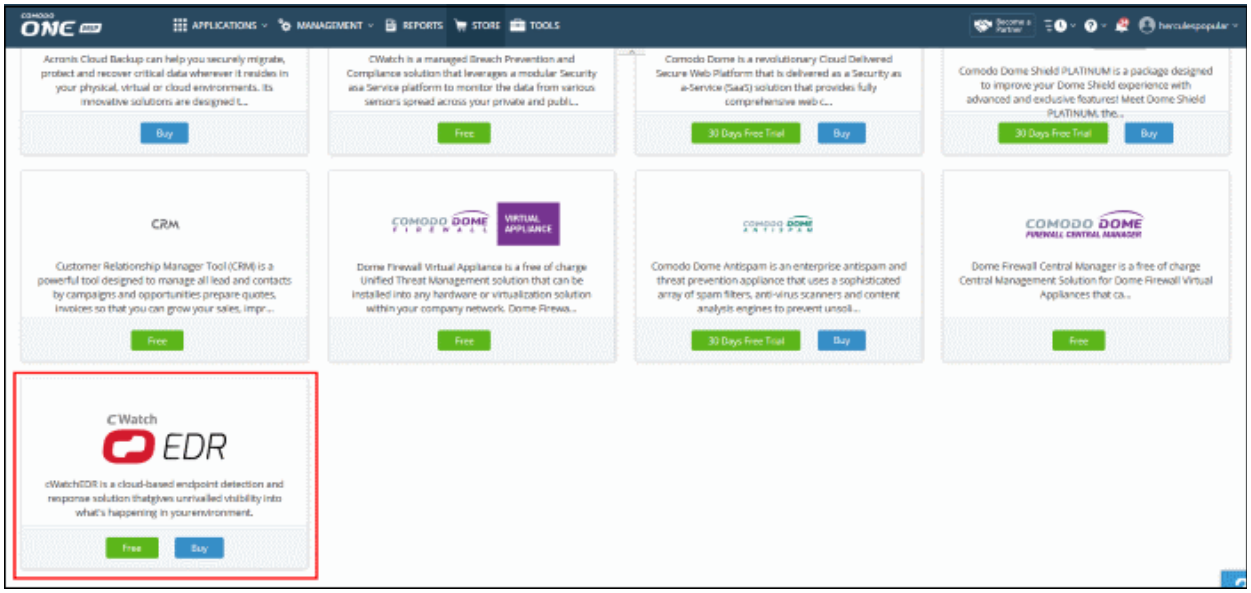
- Select 'Existing Comodo User'
- Enter your 'Comodo Accounts Manager' (CAM) username and password in the respective fields
- Provide credit card details if you chose a paid subscription
- Click 'End User license / Service Agreement' link, read the EULA fully and select the check-box
- Click 'Continue'

Your order will be processed and a confirmation message will be displayed and a notification sent to your registered email also. Comodo EDR will be added to your subscribed products list. See '**Comodo Accounts Manager**' help guide for more details about how to manage your account.

Comodo One / Comodo Dragon / ITarian customers

To subscribe for EDR via Comodo One / Comodo Dragon / ITarian portal

- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account
  - The purchase process is same for Comodo One / Comodo Dragon and ITarian. Comodo One portal is shown below as an example.
- Click 'Store' in the top-menu
- Click 'Buy' or 'Free' on the EDR tile.



- You will be taken to the respective subscription page.
- Complete the purchase process. See **https://help.comodo.com/topic-457-1-981-14357-Add-cWatch-EDR.html** for more details.

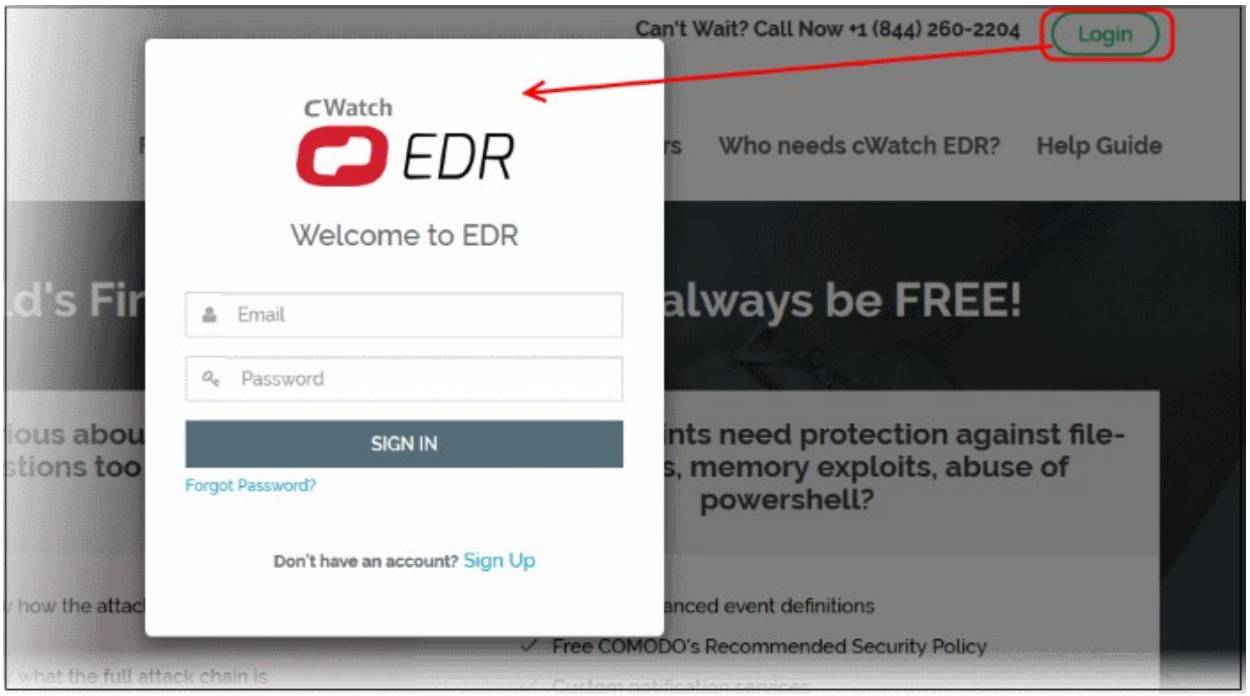
1.2 Login to the Admin Console

There are two methods to login to EDR:

- **Stand-alone EDR customers**
- **Comodo One / Comodo Dragon / ITarian portal customers**

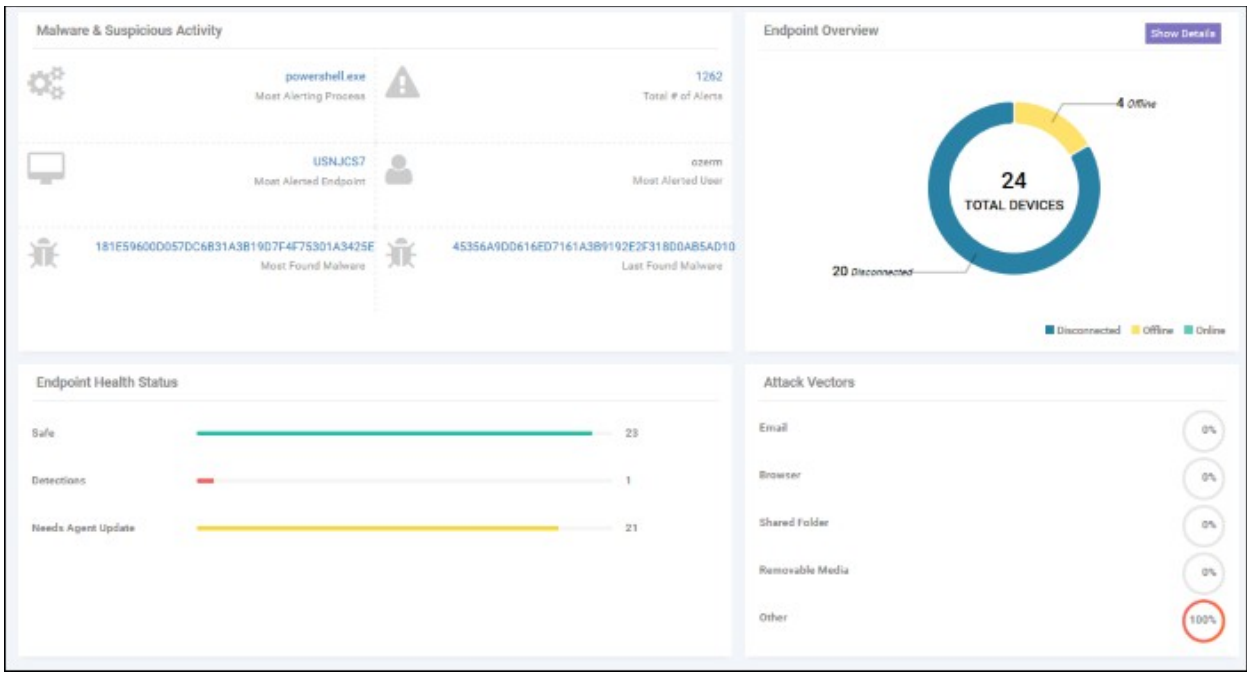
Stand-alone EDR portal

- Customers that subscribed for stand-alone EDR application should login at **http://edr.cwatch.comodo.com/**



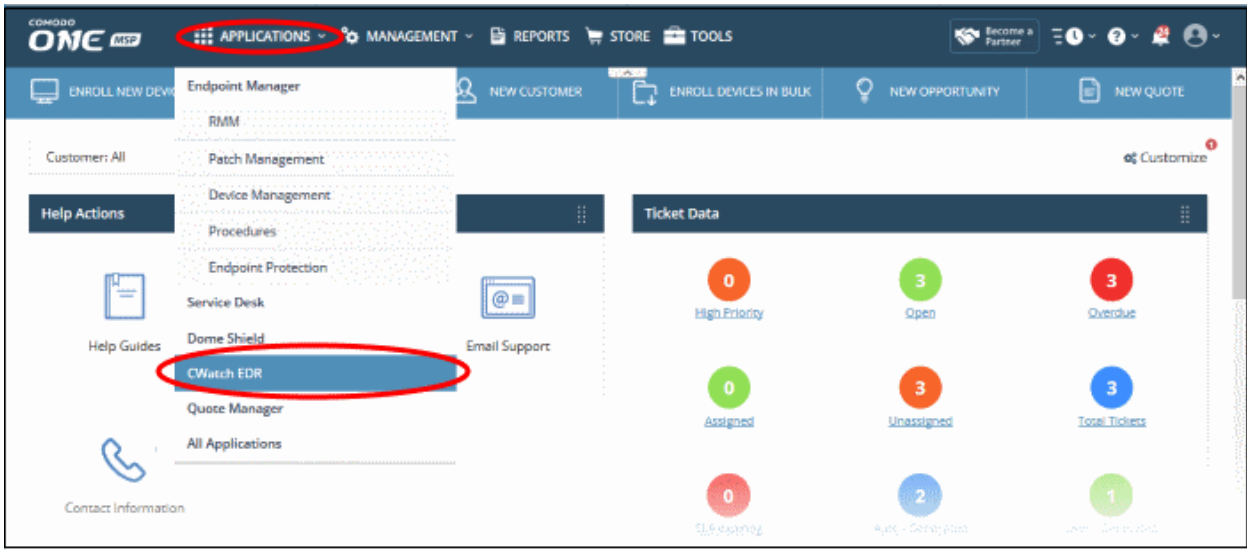
- Enter your credentials and click 'Sign in'. If you have forgotten your password, click 'Forgot Password' to reset it.

After successful verification, the 'EDR Dashboard' page will be displayed:



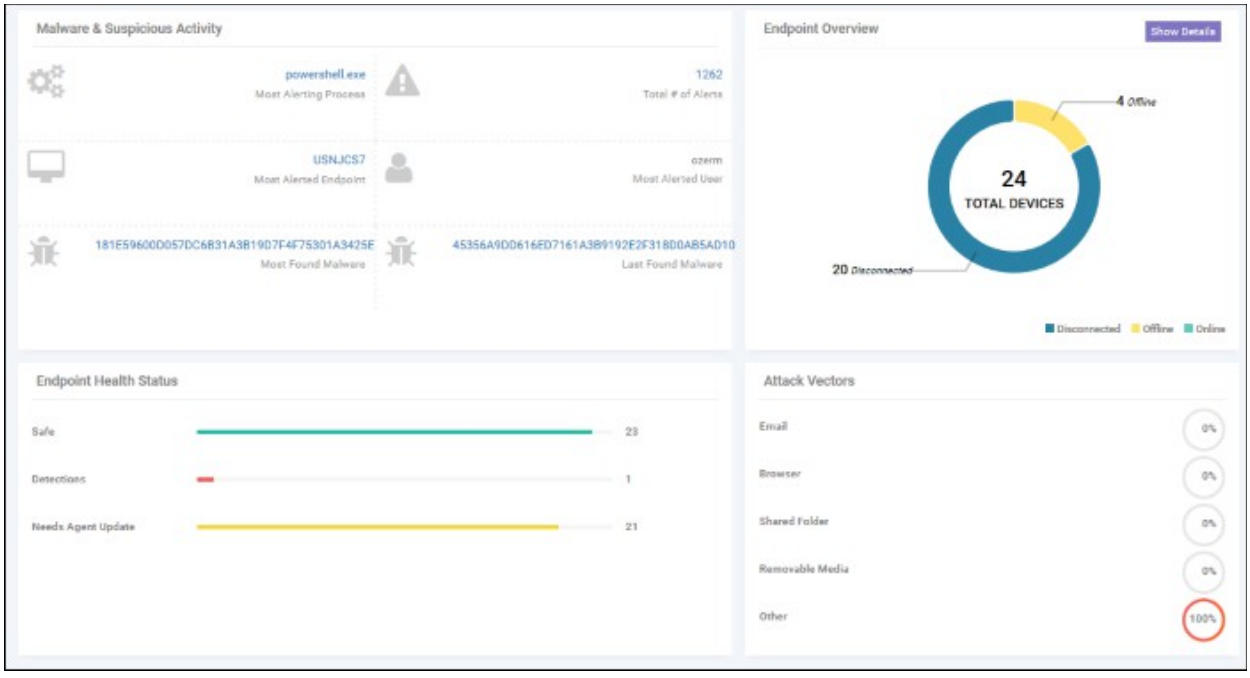
Comodo One / Comodo Dragon / ITarian customers:

- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account
- Click 'Applications' > 'cWatch EDR' to open the EDR interface



2 The Admin Console

- The EDR admin console allows you to enroll endpoints, create polices, view and analyze events and more.
- You need to install the EDR agent on all endpoints you wish to manage. Click 'Download Agent' to get started.



The buttons at the top of the interface allow you to:

Expand / collapse the left-hand menu.

Upgrade Now

Allows you to purchase a higher subscription plan. The available plans are:

- Free for 1 year - 3 days data retention/history
- Premium - 30 days data retention/history
- Platinum - 90 days data retention/history

Log out	Log out of the EDR admin console.

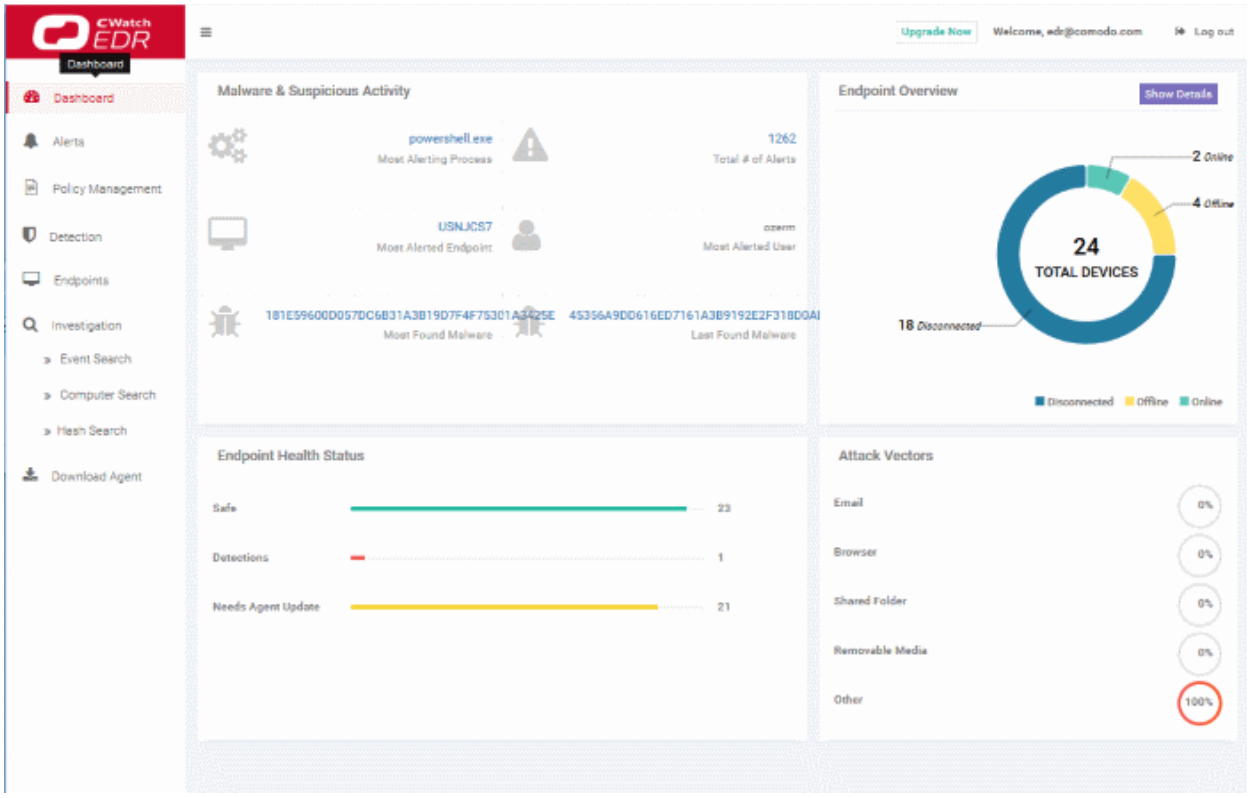
The menu on the left contains links to the main areas of the console:

- **Dashboard** - A top level overview of events on your managed endpoints. The dashboard shows the number of online, offline and disconnected devices, a summary of detected malware and the most attacked/ most recently attacked endpoints. See '**The Dashboard**' for more details.
- **Alerts** - A list of warnings generated by a policy breach. Alert details include name of the event, time of the breach and more. See '**Alerts**' for more details.
- **Policy Management** - EDR ships with default policy that will monitor and generate alerts for numerous attack types and activities. You can also configure custom policies according to your requirements. See **Manage EDR Policies** for more details.
- **Endpoints** - A list of Windows devices enrolled to EDR. Each row shows various details about the endpoint, including computer name, operating system, connection status and more. See '**Viewing Enrolled Endpoints**' for more details.
- **Detection** - Displays more detailed information about the malware found on your endpoints. See '**Viewing Event Details on Endpoints**' for more details.
- **Investigation** - Allows you to search for, identify and analyze events by event type, by computer or by hash value. See '**Investigation**' for more details.
- **Download Agent** - Download the endpoint agent. You need to install this agent on your target Windows machines in order for EDR to monitor them. See '**Adding Endpoints to EDR**' for more details.

3 The Dashboard

The dashboard is an at-a-glance summary of the security and connection status of enrolled endpoints. Each dashboard tile shows vital information about detected malware and allows you to drill-down further on areas of interest. Statistics include most the attacked endpoint, the quantity of malware found, the number of enrolled devices and so on.

- Click 'Dashboard' on the left to view the EDR dashboard



- Stand-alone and Comodo One / Comodo Dragon / ITarian enterprise customers – You can view endpoint statistics of your company.
- Comodo One / Comodo Dragon / ITarian MSP customers - You can view endpoint statistics of all companies managed by you. See **MSP Dashboard** to to learn more.

Dashboard Tiles

- **Malware & Suspicious Activity**
  - **Most Alerting Process** - Name of the application process that generated most alerts. Click the process name to open the 'Alerts' interface which shows more details. See '**Alerts**' for more information.
  - **Most Alerted Endpoint** - The name of the device for which the most number of alerts were generated. Click the name of the endpoint to open the 'Alerts' interface which shows more details. See '**Alerts**' for more information.
  - **Most Found Malware** - The hash value of the most prevalent malware on all your managed endpoints. Click the hash value to view malware details, including the endpoints that triggered the events, the date and time of the event and so on. See '**Hash Search**' for more details.
  - **Total number of Alerts** - The total number of alerts generated for all enrolled endpoints. Click the alert number to open the 'Alerts' interface. See '**Alerts**' for more information.
  - **Most Alerted User** - The device user for whom the most alerts were generated.
  - **Last Found Malware** - The hash value of the malware that was detected most recently. Click the hash value to view malware details, including the endpoints that triggered the events, the date and time of the event and so on. See '**Hash Search**' for more details.
- **Endpoint Overview**
  - **Total Devices** - The total number of endpoints you have added to EDR
  - **Online Devices** - The number of devices that are currently active.
  - **Offline Devices** - The number of endpoints that are currently shut down and not connected to EDR.
  - **Disconnected Devices** - Enrolled devices that are logged off. Disconnected devices includes endpoints that were not shut down properly or crashed.

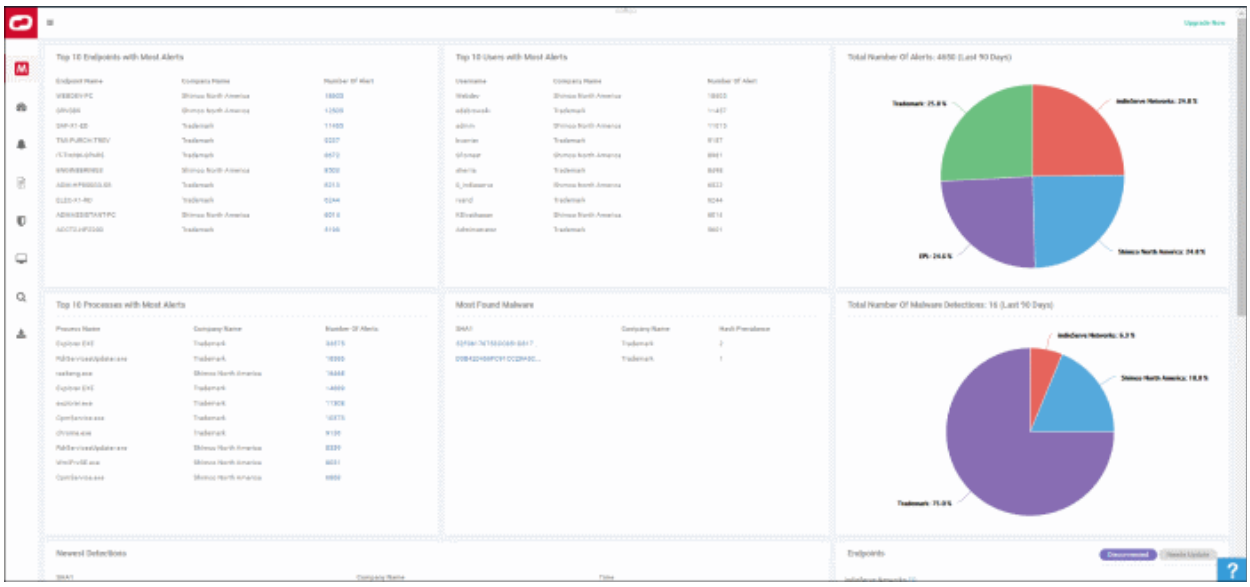
- Click 'Show Details' to open the 'Endpoints' interface to view information about the endpoint. See '**View Enrolled Endpoints**' for more details.

- **Endpoint Health Status**
  - **Safe** - The number of endpoints where no malicious activities were detected.
  - **Detections** - The number of devices on which malicious and suspicious activities were detected.
  - **Needs Agent Update** - The number of endpoints which are using an outdated version of the EDR agent. EDR supports auto-update. Whenever an endpoint with outdated agent version goes online, it gets the latest update.
- **Attack Vectors** - The channel via which malicious activities originated on the endpoints.

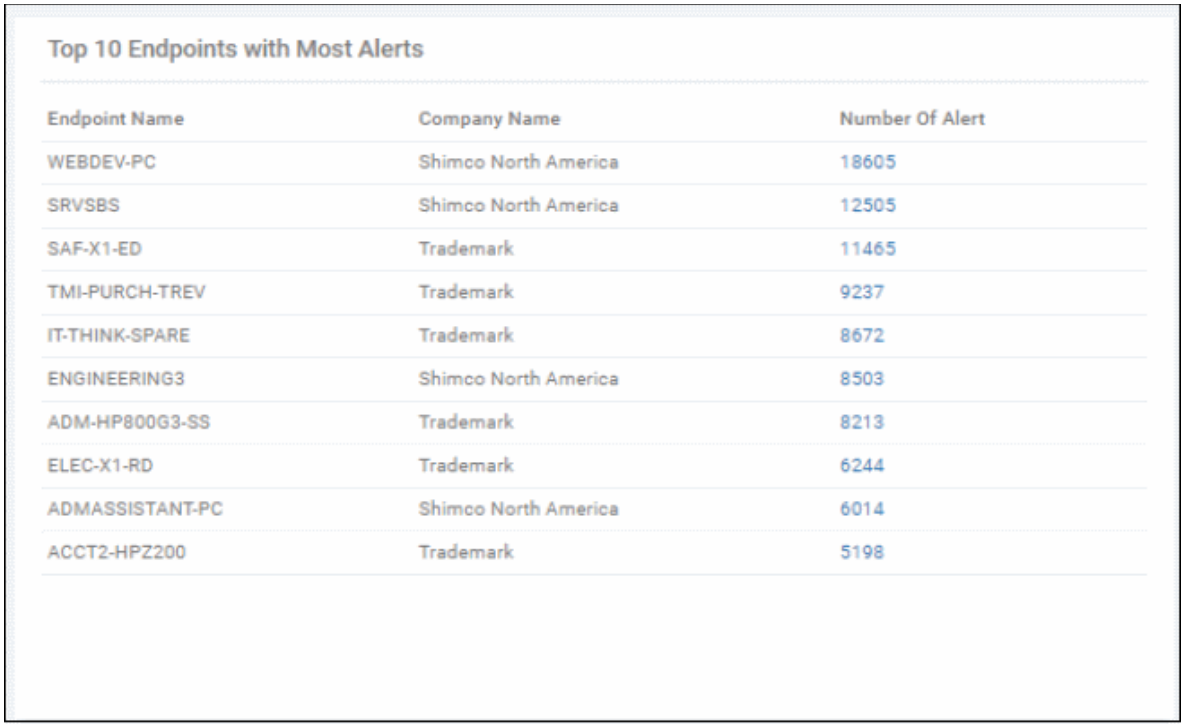
4 MSP Dashboard

Comodo One / Comodo Dragon and ITarian MSP customers can view endpoint statistics of all companies managed by them.

- Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account
- Click 'Applications' > 'cWatch EDR'
  - Click 'Store' if you haven't yet activated EDR. You can install the free version from the 'CWatch EDR' tile.
- Click 'MSP Dashboard' on the left of the EDR interface to view statistics for all companies on your account.



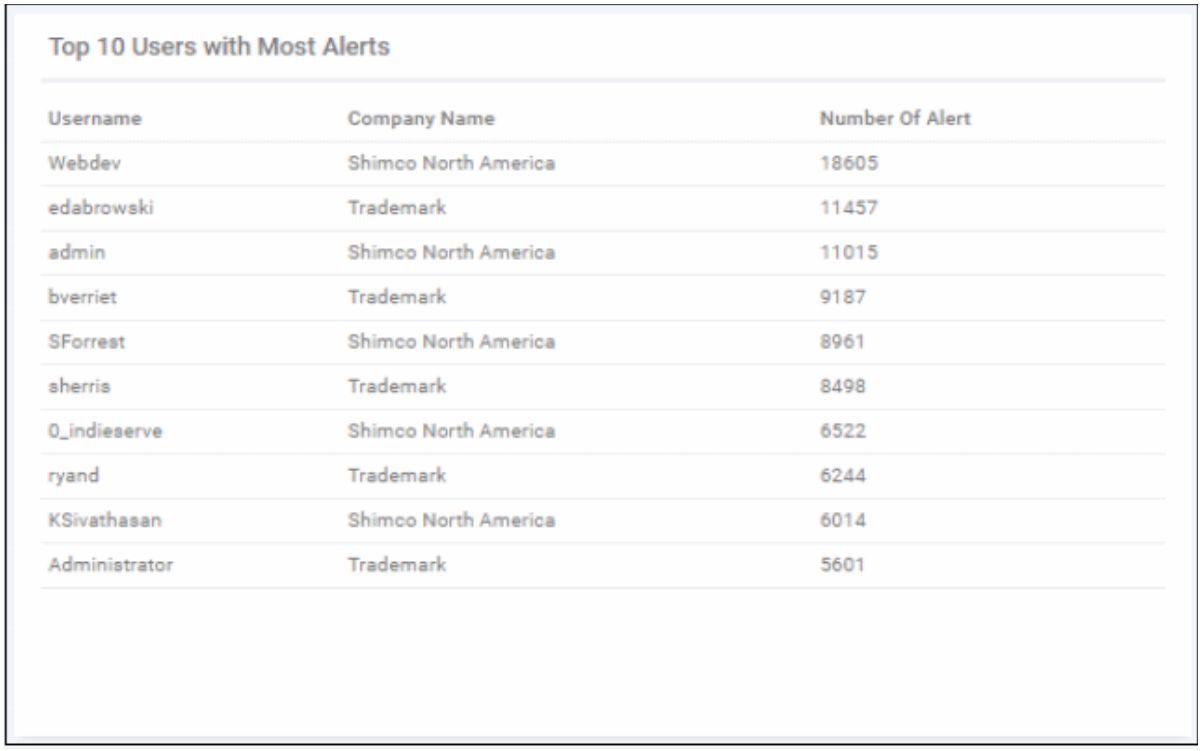
Top 10 Endpoints with Most Alerts - List of endpoints which caused the most alerts to be generated (all time).



Top 10 Endpoints with Most Alerts

Endpoint Name	Company Name	Number Of Alert
WEBDEV-PC	Shimco North America	18605
SRVSBS	Shimco North America	12505
SAF-X1-ED	Trademark	11465
TMI-PURCH-TREV	Trademark	9237
IT-THINK-SPARE	Trademark	8672
ENGINEERING3	Shimco North America	8503
ADM-HP800G3-SS	Trademark	8213
ELEC-X1-RD	Trademark	6244
ADMASSISTANT-PC	Shimco North America	6014
ACCT2-HPZ200	Trademark	5198

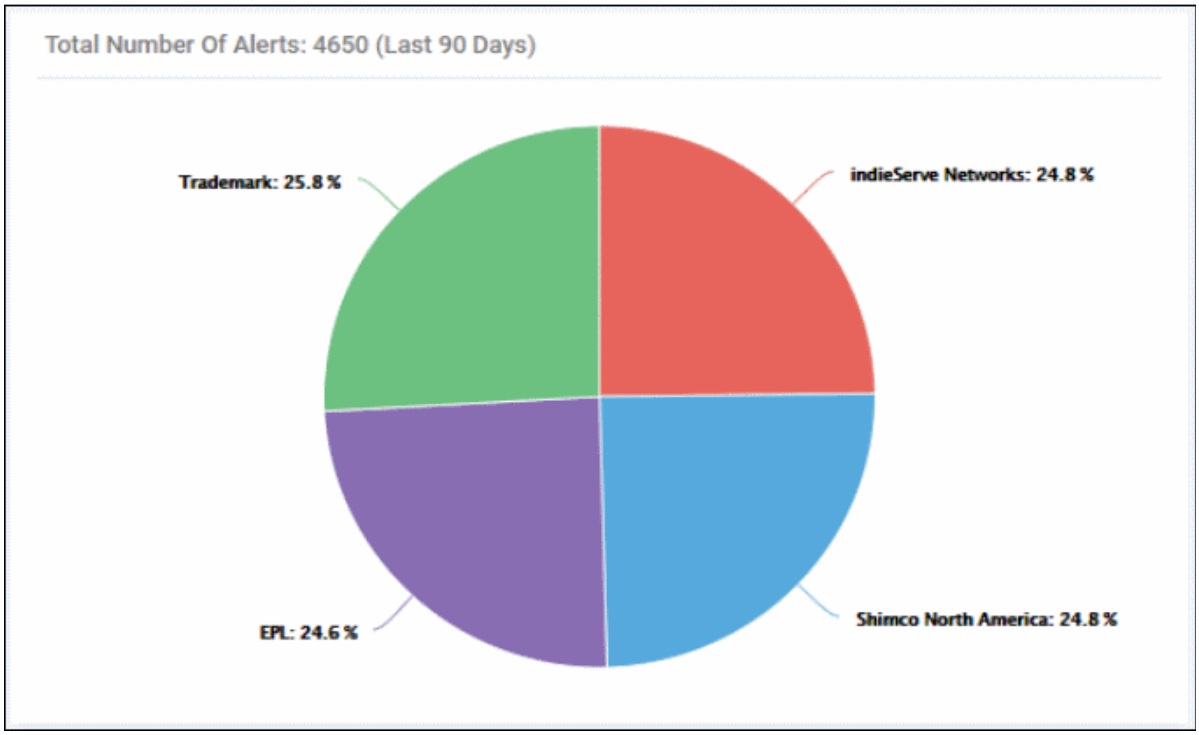
Top 10 Users with Most Alerts - List of users who caused the most alerts to be generated (all time).



Top 10 Users with Most Alerts

Username	Company Name	Number Of Alert
Webdev	Shimco North America	18605
edabrowski	Trademark	11457
admin	Shimco North America	11015
bverriet	Trademark	9187
SForrest	Shimco North America	8961
sherris	Trademark	8498
0_indieserve	Shimco North America	6522
ryand	Trademark	6244
KSivathasan	Shimco North America	6014
Administrator	Trademark	5601

Total Number of Alerts (Last 90 Days) - Amount of alerts generated by all users and all endpoints in the previous 90 days. Alerts are broken down by company responsible:



-

Top 10 Processes with Most Alerts -The 10 processes and applications that triggered the most alerts (all time).

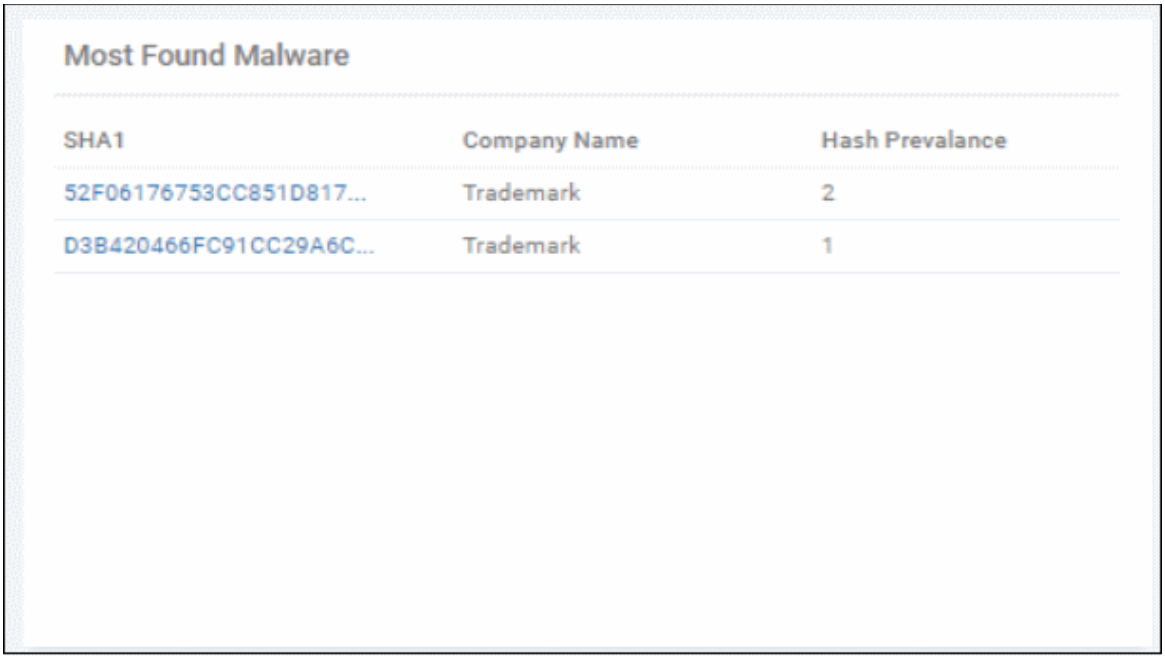
Top 10 Processes with Most Alerts

Process Name	Company Name	Number Of Alerts
Explorer.EXE	Trademark	33575
RdrServicesUpdater.exe	Trademark	18386
taskeng.exe	Shimco North America	16468
Explorer.EXE	Trademark	14889
explorer.exe	Trademark	11308
CpmService.exe	Trademark	10373
chrome.exe	Trademark	9136
RdrServicesUpdater.exe	Shimco North America	8339
WmiPrvSE.exe	Shimco North America	8031
CpmService.exe	Shimco North America	6868

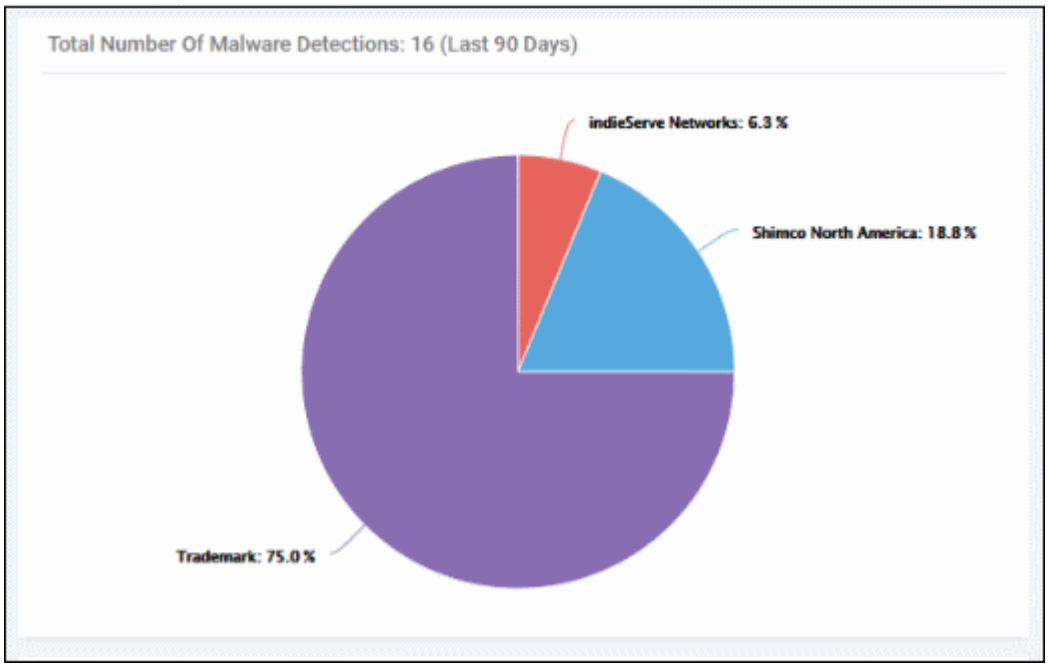
Most Found Malware - The most prevalent malware on your protected endpoints (all time).

- SHA1 = hash of the malware.
- Hash prevalence = how many instances of the hash were found on endpoints which belong to the company

shown in the middle column.



Total Number of Malware Detections:(Last 90 Days) - Quantity of malware found on your protected endpoints in the previous 90 days. Malware is broken down by company affected:



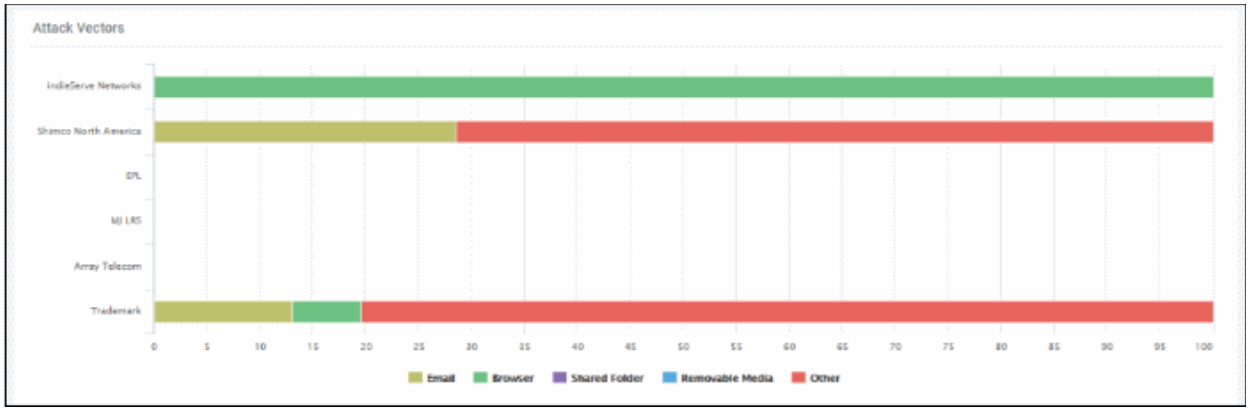
Attack Vectors -

Shows the methods by which threats were launched on your companies. Each bar shows the % of each type in relation to all threats.

Y axis - Company affected by the threat

X axis - Percentage of total threats

Legend - Method used to deliver the threat. Examples include 'Email', 'Browser' and 'Shared Folder'.



5 Add Endpoints to EDR

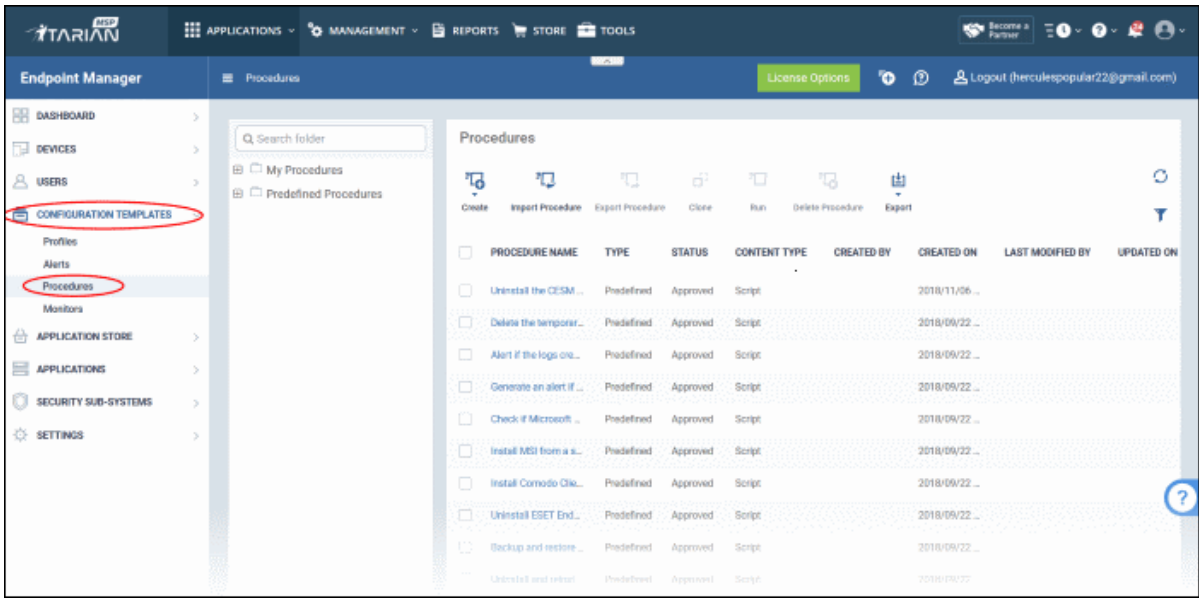
You need to install the EDR agent on all endpoints that you wish to monitor. There are two ways to do this:

1. **Individual Endpoints.**

   - Click 'Download Agent' at the bottom left of the interface
   - Install the agent on every target machine
   - **Click here** to view a tutorial on this process

2. **Use Group Policy Management (GPO)**. See **https://help.comodo.com/topic-444-1-910-11939-Introduction-to-Agent-Deployment-via-GPO.html** for help with this

3. **Use script execution via Endpoint Manager**. You can also deploy the .msi agent by executing scripts via procedures in Endpoint Manager. The script can be accessed from the link below: **https://scripts.comodo.com/frontend/web/topic/enroll-comodo-edr-agent**

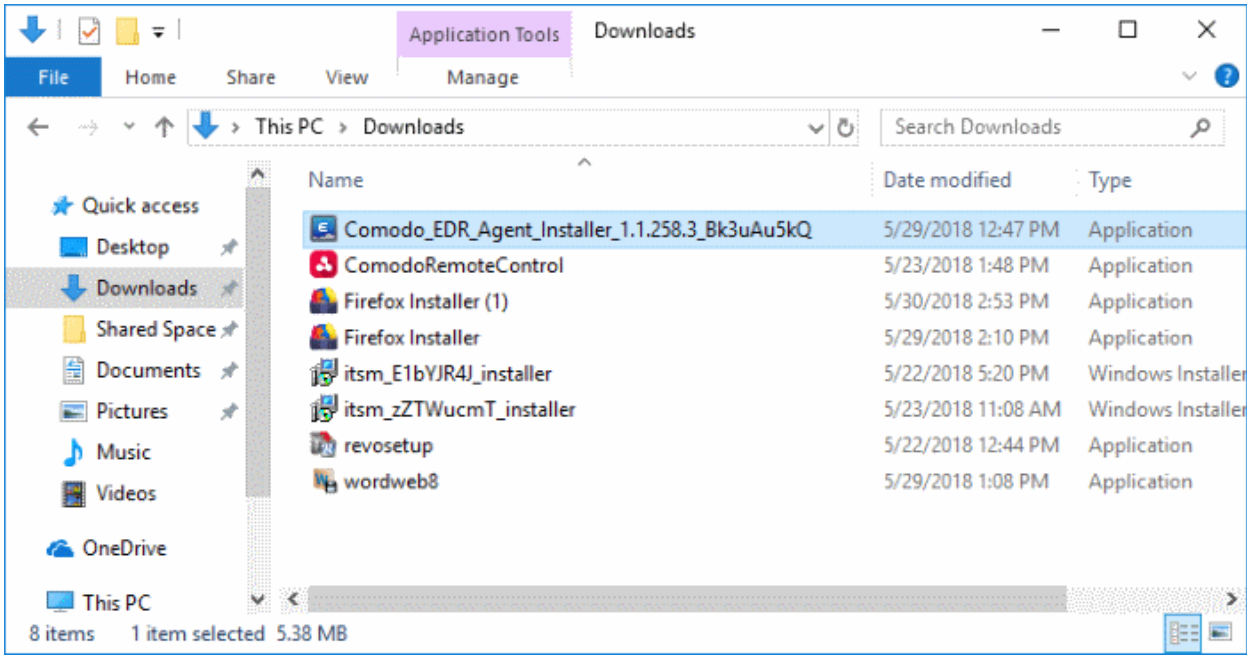


   - To run the script, create a custom procedure. Login to your **Comodo One** / **Comodo Dragon** / **ITarian** account
   - Click 'Applications' > 'Endpoint Manager'
   - Click 'Configuration Templates' > 'Procedures'

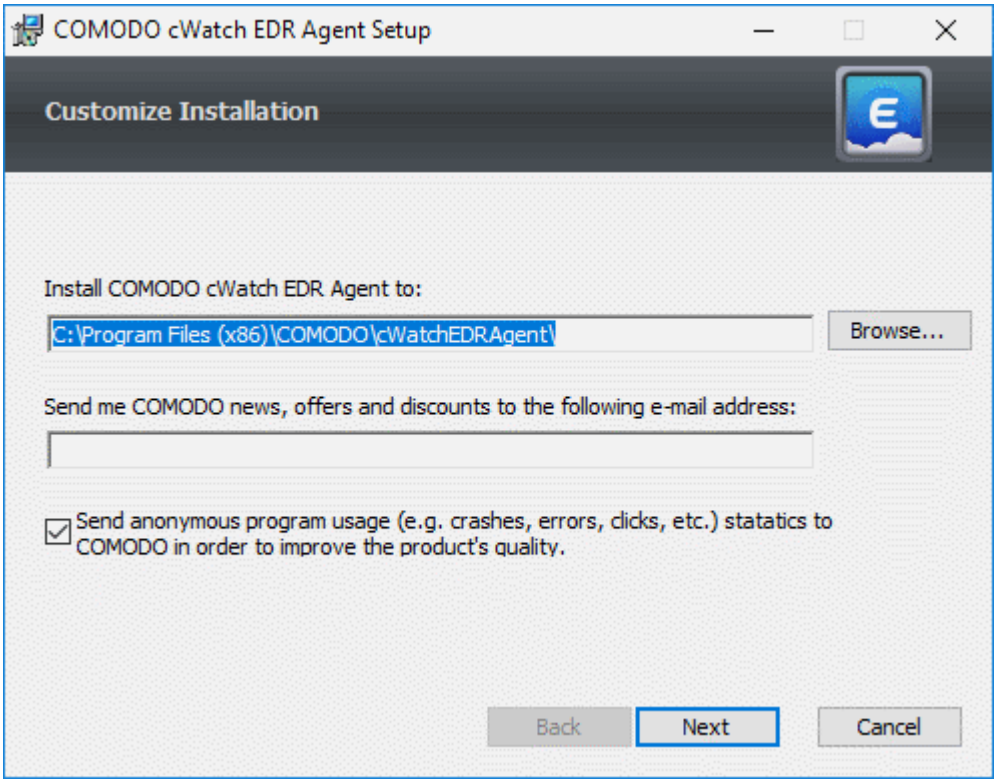
- To create script to install .msi package on multiple endpoints, see '**Create a custom Procedure**' in the 'Endpoint Manager – Administrator Guide' guide for help.

Add endpoints individually

- **Login** to your EDR account from each of these endpoints and download the agent from there.
- Click 'Download Agent' in the left menu.



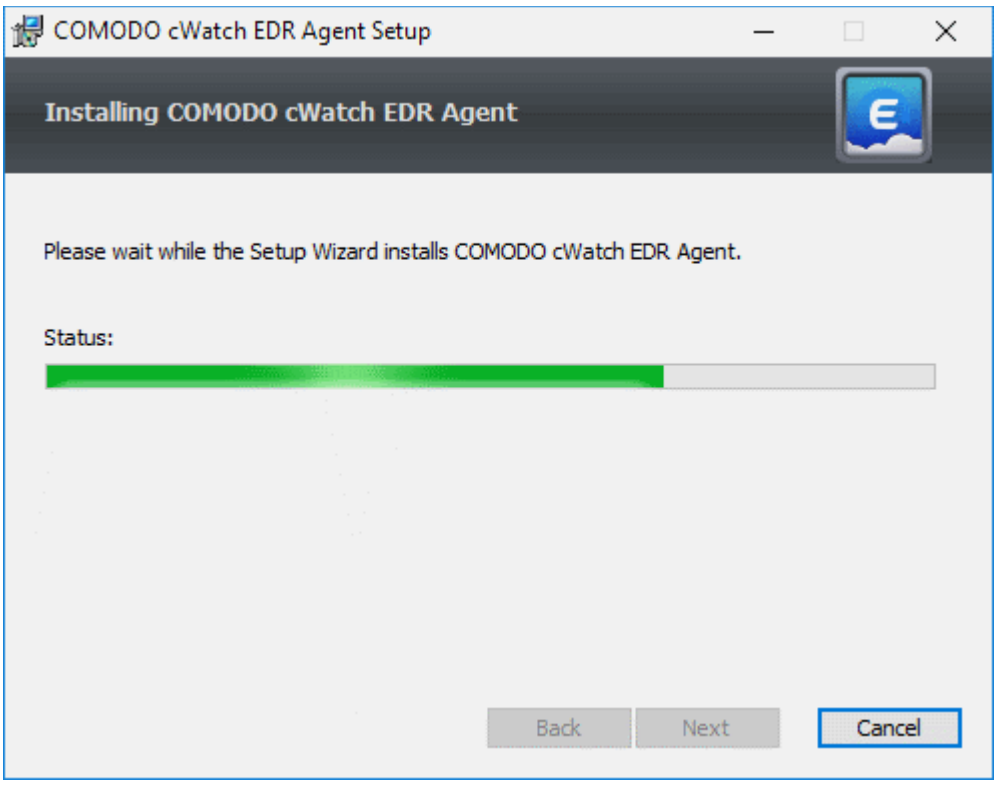
- Open the setup file to start the installer



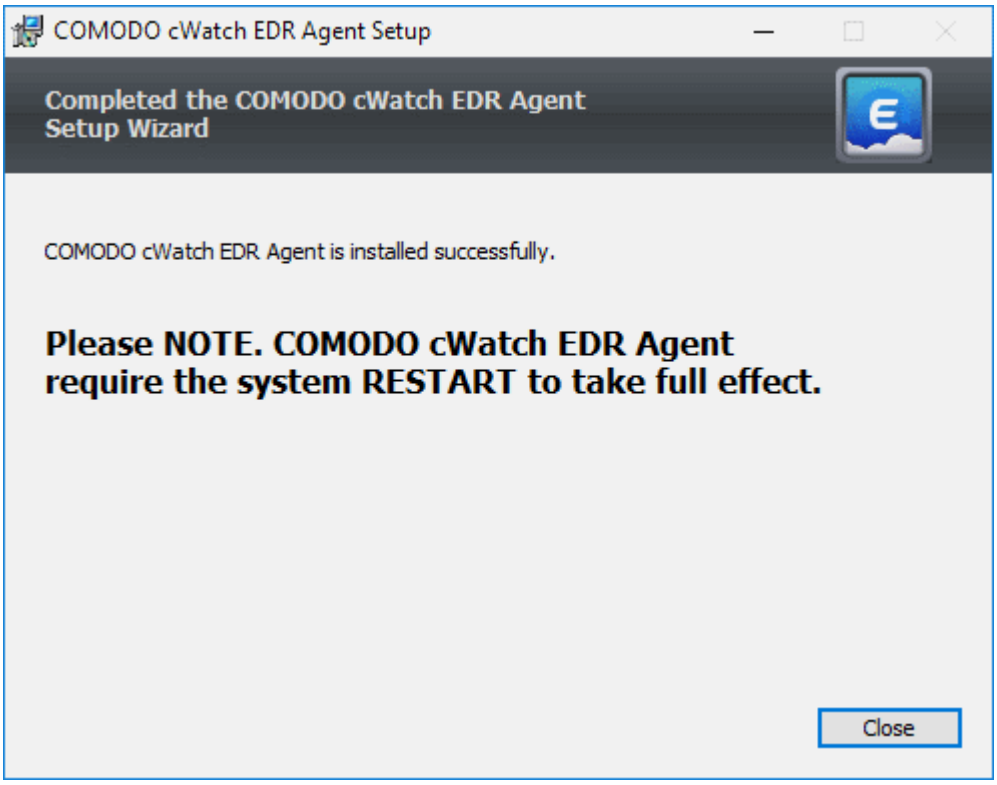
- The default installation location is C:\Program Files (x86)\COMODO\cWatchEDRAgent\. Click 'Browse...' to

choose a different installation location.

- Click 'Next' to continue the installation



You must restart the endpoint to complete the installation:

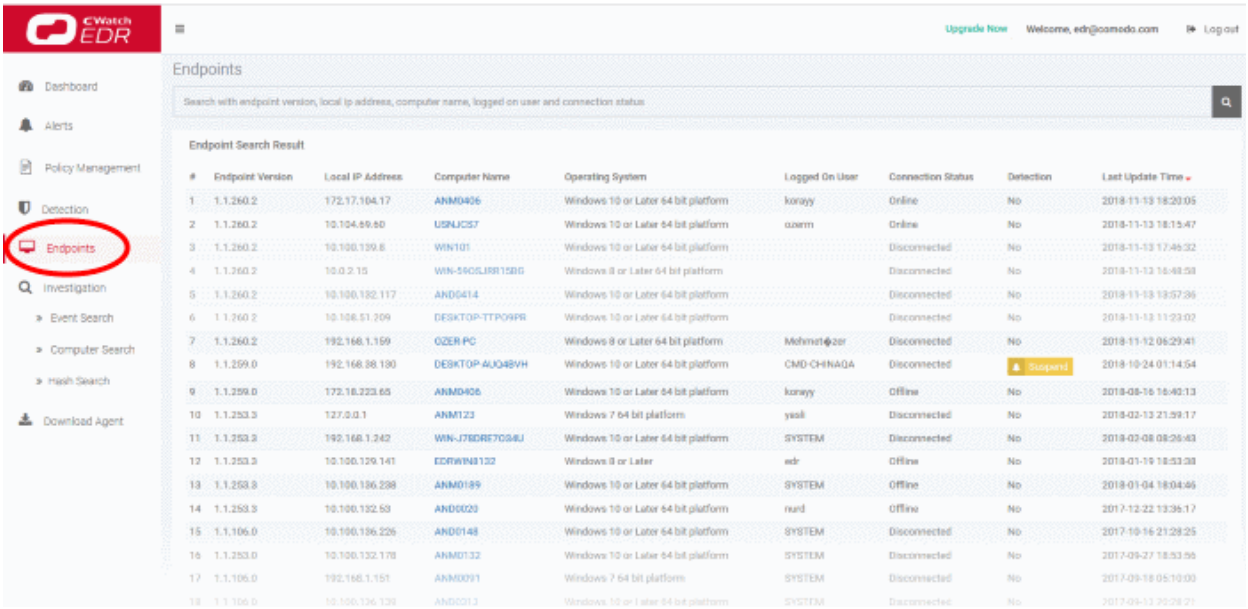


- Click 'Close'
- Restart the endpoint to finalize the installation.

That's it. The endpoint now is enrolled to EDR and can be monitored.

6 View Enrolled Endpoints

- Click 'Endpoints' on the left to view and manage all endpoints you have added to EDR
- Details include the endpoint name, connection status, IP address, operating system, alerts and more.



Endpoints - Table of Column Descriptions	
Column Header	**Description**
Endpoint Version	The version number of the EDR agent.
Local IP Address	The internal IP address of the endpoint
Computer Name	The endpoint label. Click this name to view events on the endpoint. See '**Computer Search**' for more information.
Operating System	The endpoint's OS
Logged On User	The user currently using the machine
Connection Status	Whether or not the endpoint is connected to EDR
Detection	Whether or not there have been malicious events on the endpoint. • A yellow bar indicates a malware event. Click 'Suspend Alarm' to remove the alert. You may want to do this if the event has been dealt with and no longer poses a concern.
Last Update Time	The most recent update sent from the endpoint agent to the EDR console.

- Use the search box above the table to find specific items. You can filter by agent version, local IP, active user, computer name and connection status
- Clear the data to view the full list again.

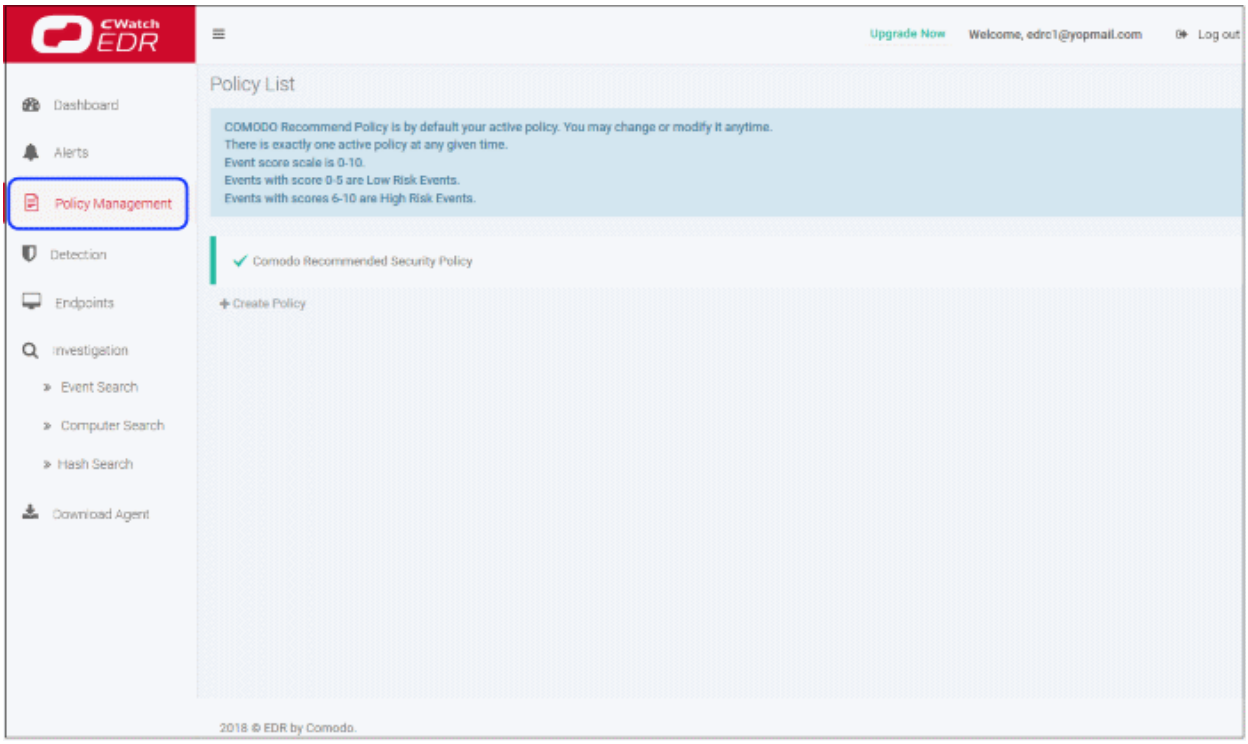
7 Manage EDR Policies

- An EDR policy determines which events will generate an alert for you.
- There are 7 event categories. You can define specific rules within each category.
- Comodo EDR ships with a default security policy that is applied to all enrolled endpoints.
- You can also create custom policies according to your requirements.
- Only one policy can be active at a time. You cannot delete the active policy.

Note. EDR policies do not determine which events are logged, they determine which events you *receive alerts* for. cWatch automatically logs all events and submits suspicious files to Valkyrie for analysis, regardless of EDR policy. This means cWatch will always catch zero-day malware, even if you prefer to disable some alerts in a policy.

You can search raw logs in the 'Investigation' screen.

- Click 'Policy Management' on the left to manage EDR security policies:



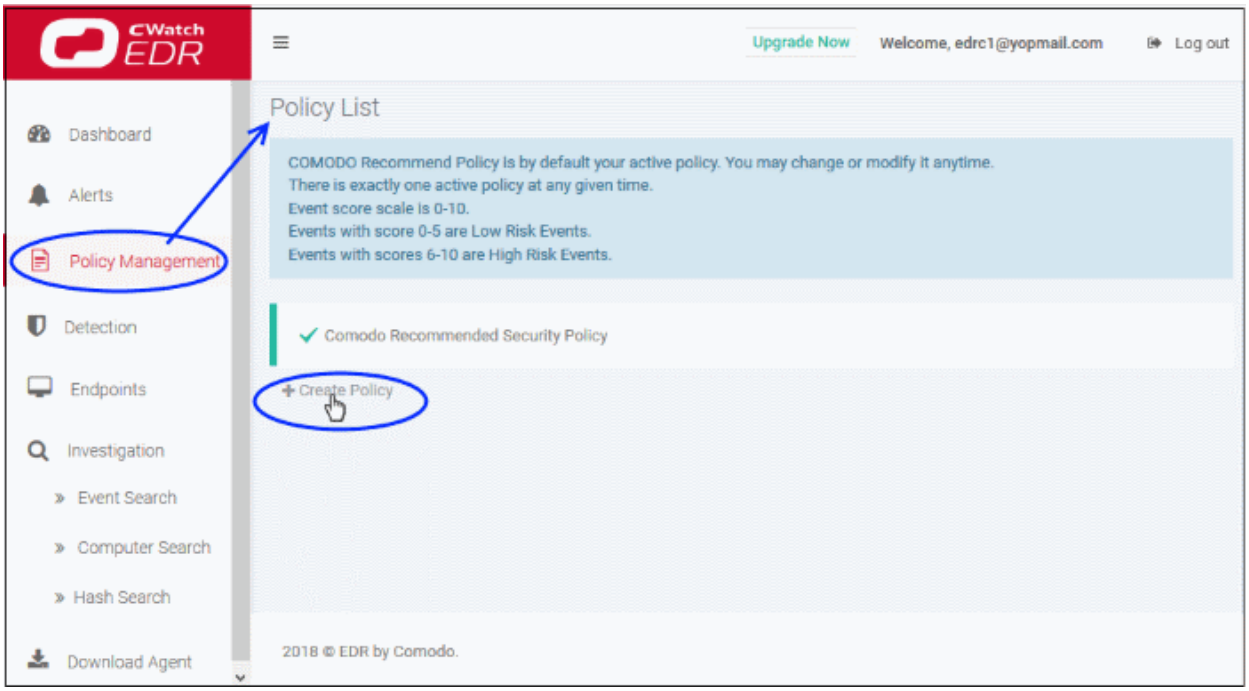
- The screen shows general information about policies and lists the default 'Comodo Recommended Security Policy'.
- A check-mark beside a policy indicates it is currently active.

From this interface you can:

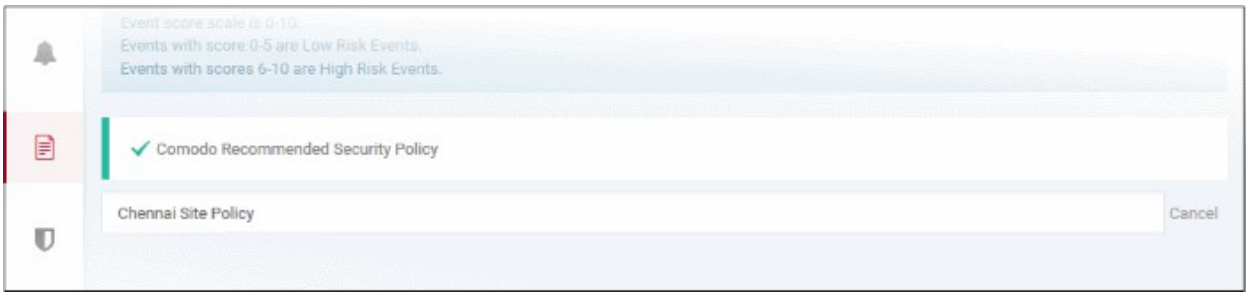
- **Create a new policy**
- **View and edit the default Comodo security policy**
- **Activate a policy**
- **Delete a policy**

Create a new policy

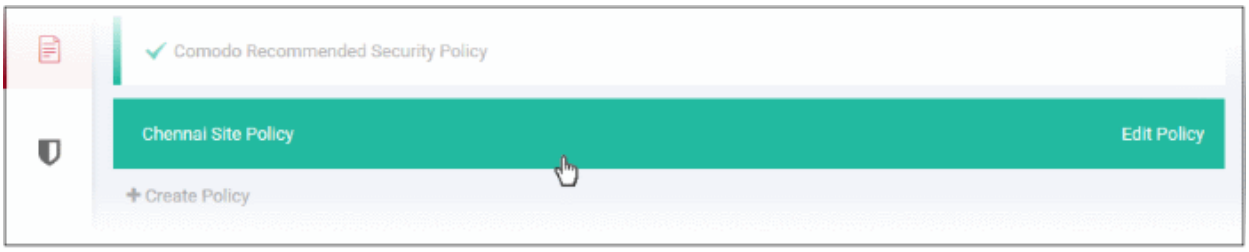
- Click 'Policy Management' on the left
- Click 'Create Policy':



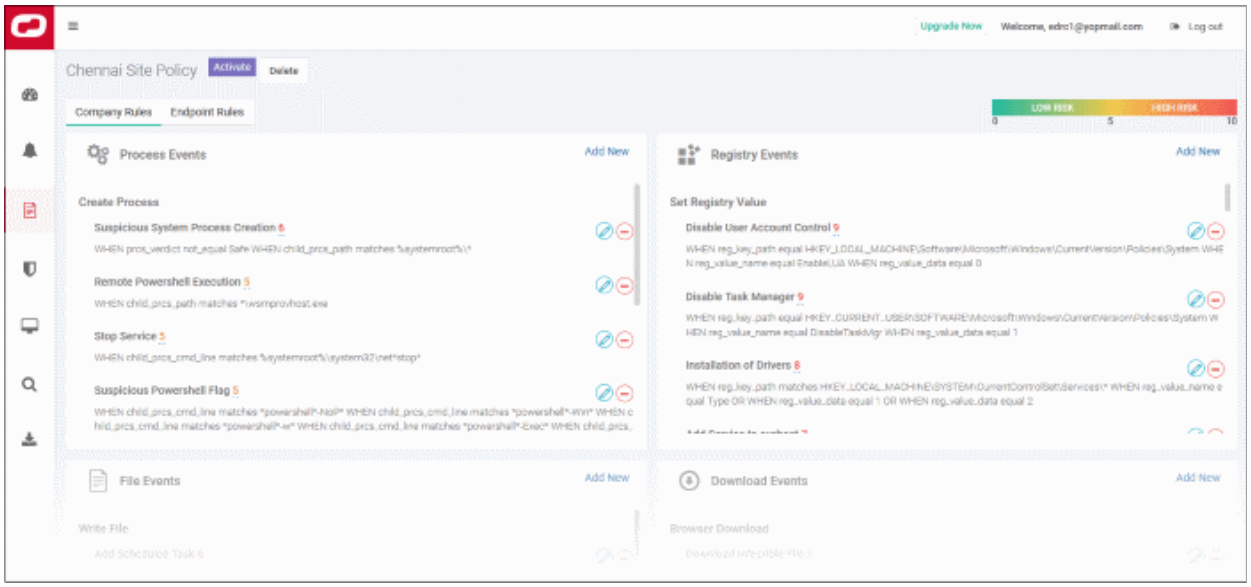
- Create a name for the policy and press enter:



- Now, click on the policy name to view and edit its current details:



- The new policy is automatically assigned a set of default rules.
- You can add new rules, edit or delete rules as required.



The policy interface has two tabs - 'Company Rules' and 'Endpoint Rules'.

- **Company Rules** - Create rules by event category. Company rules are applied to all protected endpoints. See '**Company Rules**' for more information.
- **Endpoint Rules** - Create additional conditions for each event category and apply to specific endpoints. See '**Endpoint Rules**' for more details.

Company Rules

There are seven event categories in the company rules section.

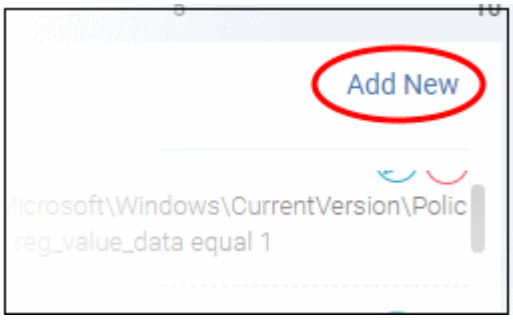
Each category has conditions or rules that can be implemented in your policy. You can create new conditions and edit or delete a condition from an category.

The built-in event categories are:

- **Process Events** - Rules to alert you when processes are invoked by an application
- **Registry Events** - Rules to alert you about changes to the Windows registry on your endpoints.
- **File Events** - Rules to alert you about modifications to system files.
- **Download Events** - Rules to alert you when files are downloaded via browsers, emails, shared folders or external drives.
- **Upload Events** - Rules to alert you when files are transferred to shared folders or external drives.
- **Defense+ Events** - Rules to alert you when processes attempt to access critical operating system functions or launch attacks.
- **Network Events** - Rules to alert you about any service listening to ports and network connections on your endpoints.

To create a new condition

- Click 'Add New' lat the top of an event category:



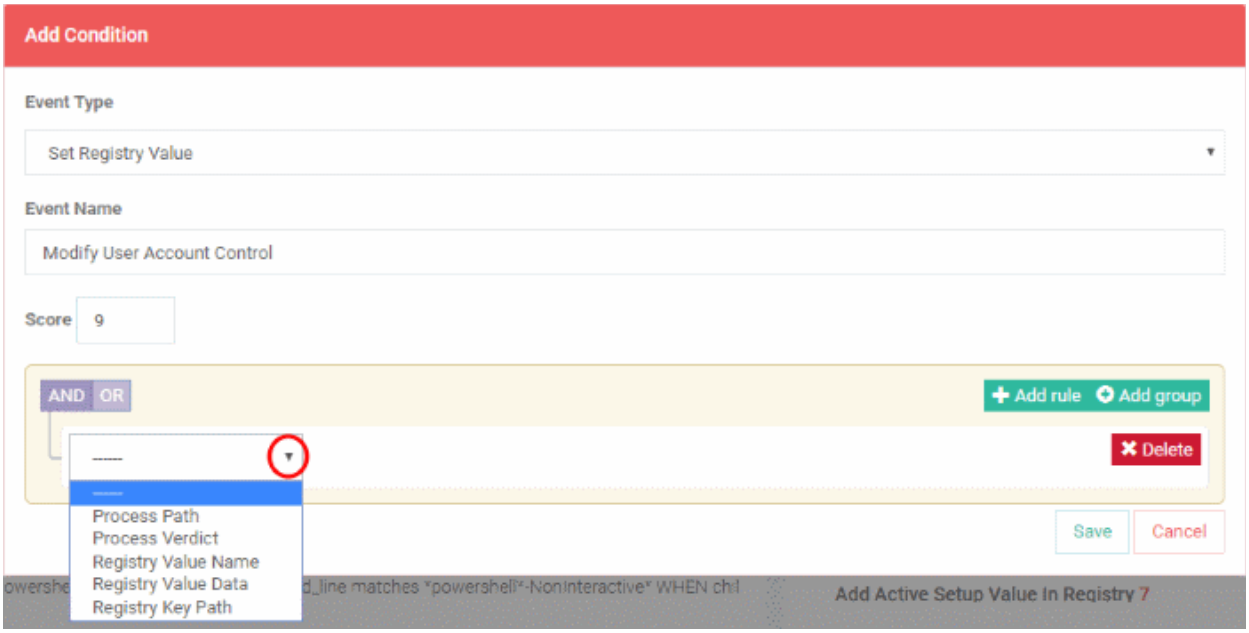
The 'Add Condition' dialog will open:

- **'Event Type'** - choose the type of incident that you want EDR to detect. The event types available depend on the event category chosen.
- In the example above, the category is 'Registry Events', so the available event types are 'Delete Registry Key', 'Delete Registry Value' and 'Set Registry Value'.
- After choosing a type, you must next construct your condition. You do this by choosing the specific criteria which should be monitored. Again, the criteria vary by event category and event type.
- In the example above we will chose 'Registry Events' > 'Set Registry Value'. The available criteria for 'Set Registry Value' let you specify which key names, values or paths should be monitored.

- Event Name - Create a label for your condition. This label will be shown as 'Alert Name' in the 'Alerts' interface.
- Score - Rate the event according to how seriously you judge the incident. Scores range from 0 to 10.
  - Scores 0 to 5 - Low risk events
  - Scores 6 to 10 - High risk events

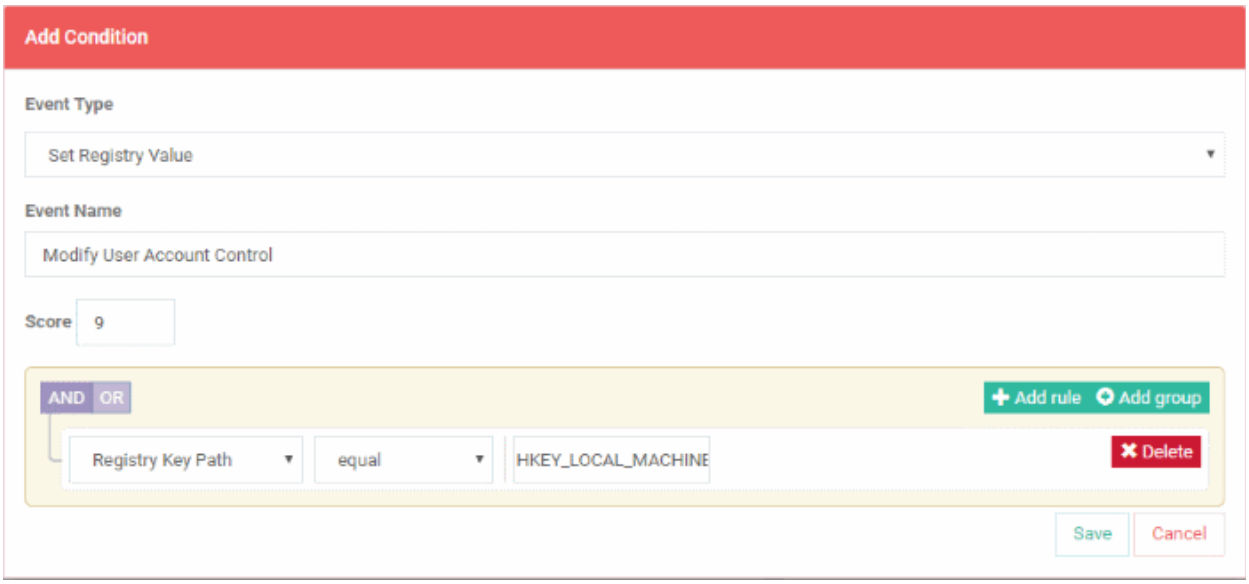
The next step is configure the parameters and conditions for the rule.

- Click the arrow below 'AND/OR'

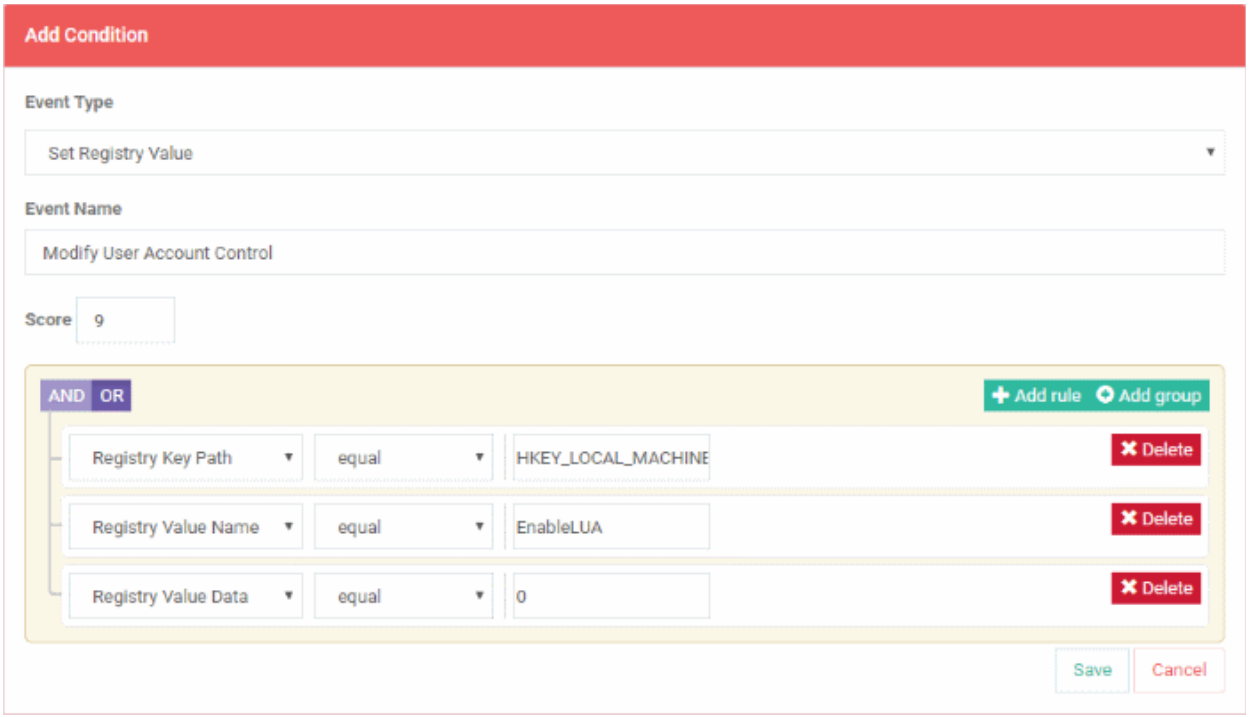


The parameters depend on the selected category and event type.

- Choose the parameter you wish to monitor
- In the second box select the condition. The conditions list varies for different parameters.
- In the third box, enter or select the value. You have to enter the value or select depending on the parameter.



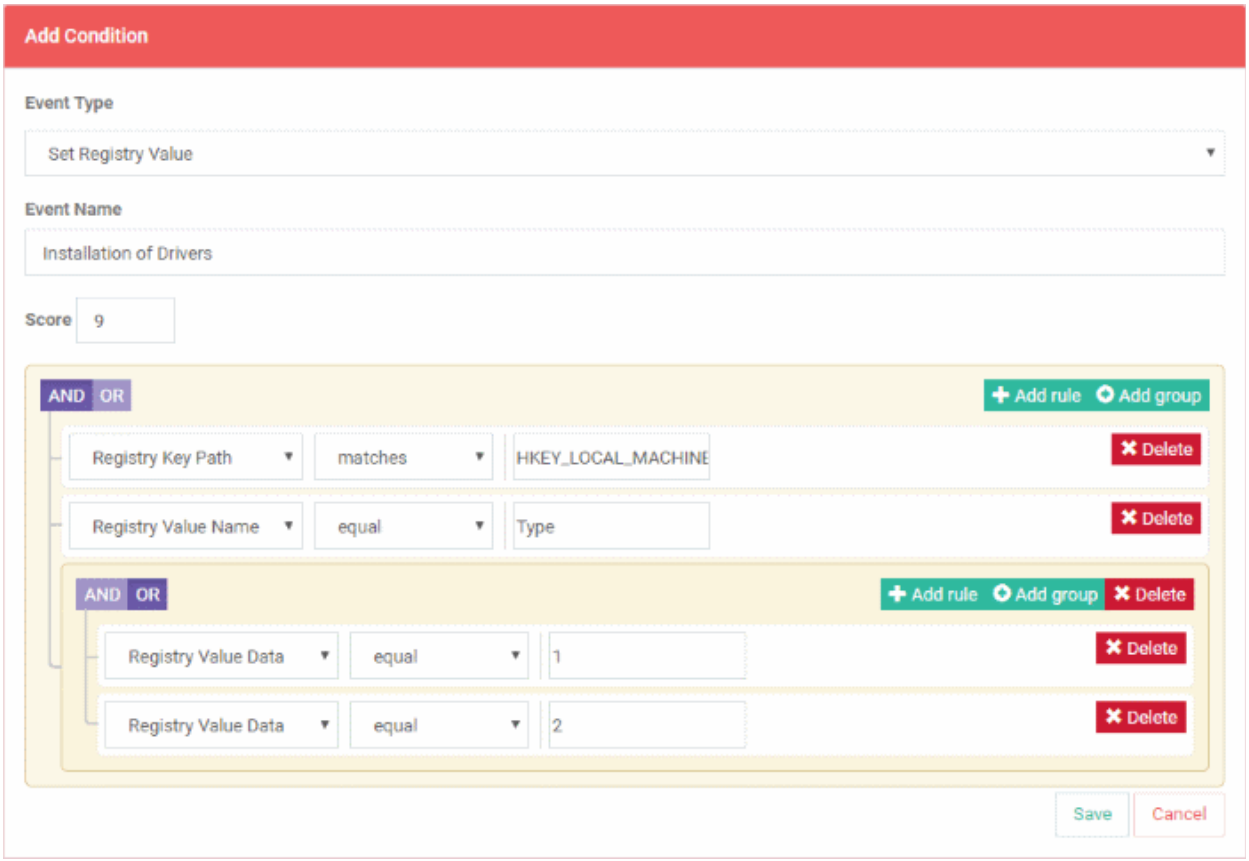
- Click 'Delete' to remove the rule
- Click 'Save' if the rule satisfies your requirement
- To add multiple rules, click 'Add rule'
- Define parameters and condition as explained above.



- Use 'AND' or 'OR' operators for the rule per your requirement

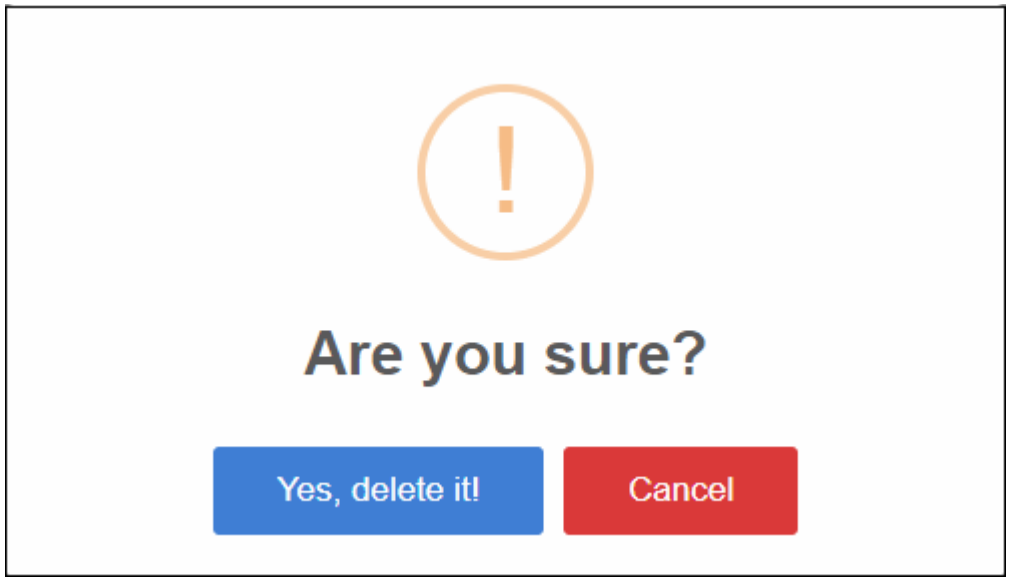
You can add multiple rules and define their relationship with 'AND', 'OR' operators.

- To add a group, click 'Add group'
- Define parameters and conditions as explained above.



- Use 'AND' or 'OR' operators for groups (and within a group for rules) per your requirements.
- Click 'Save' when done.

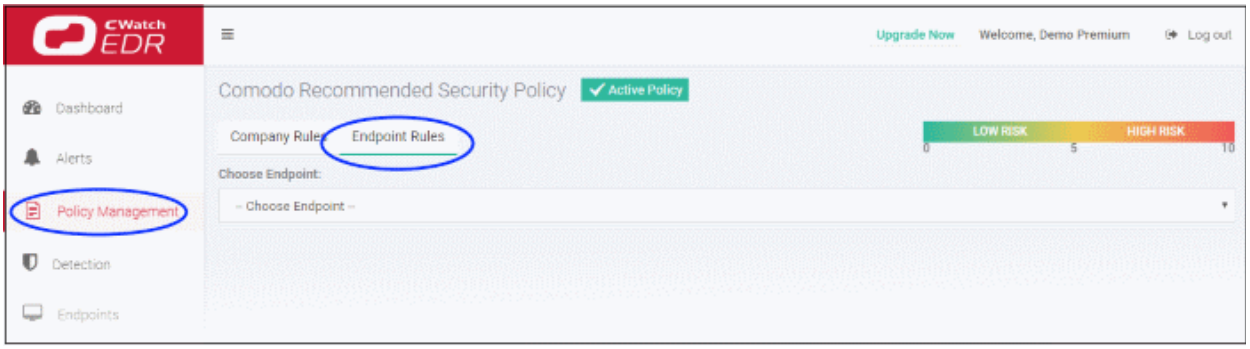
- An alert will be created if the rule condition(s) are met
- To edit a rule, click the pencil icon beside it and update as required. The process is same as explained above.
- To remove a rule, click the delete icon beside it.



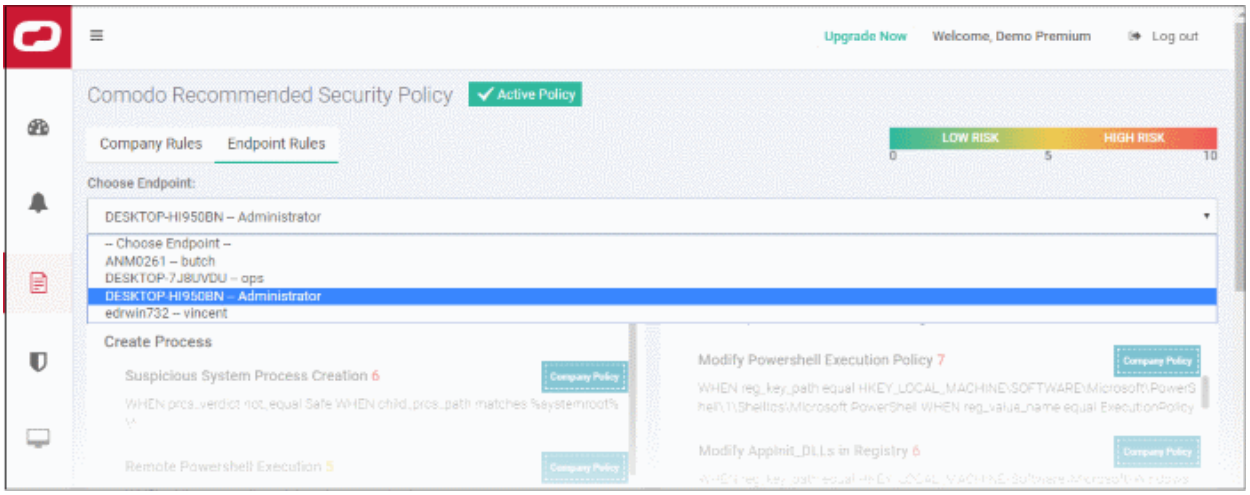
- Click 'Yes, delete it!' to confirm removal.

Endpoint Rules

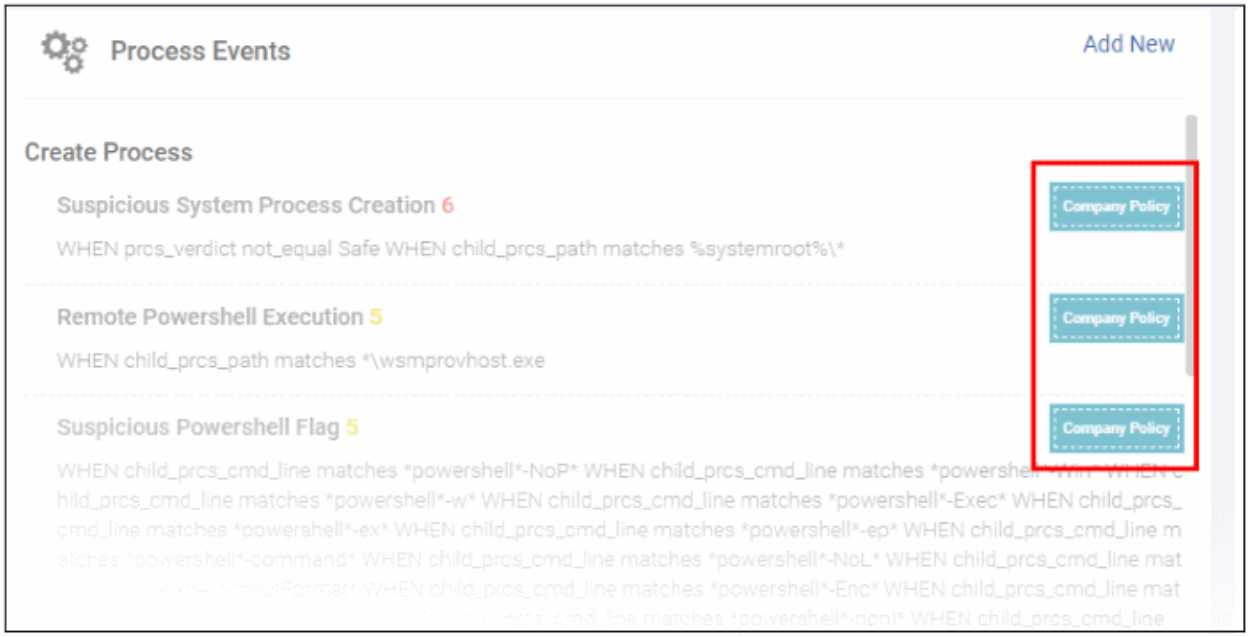
- Click 'Policy Management' on the left then the 'Endpoint Rules' tab



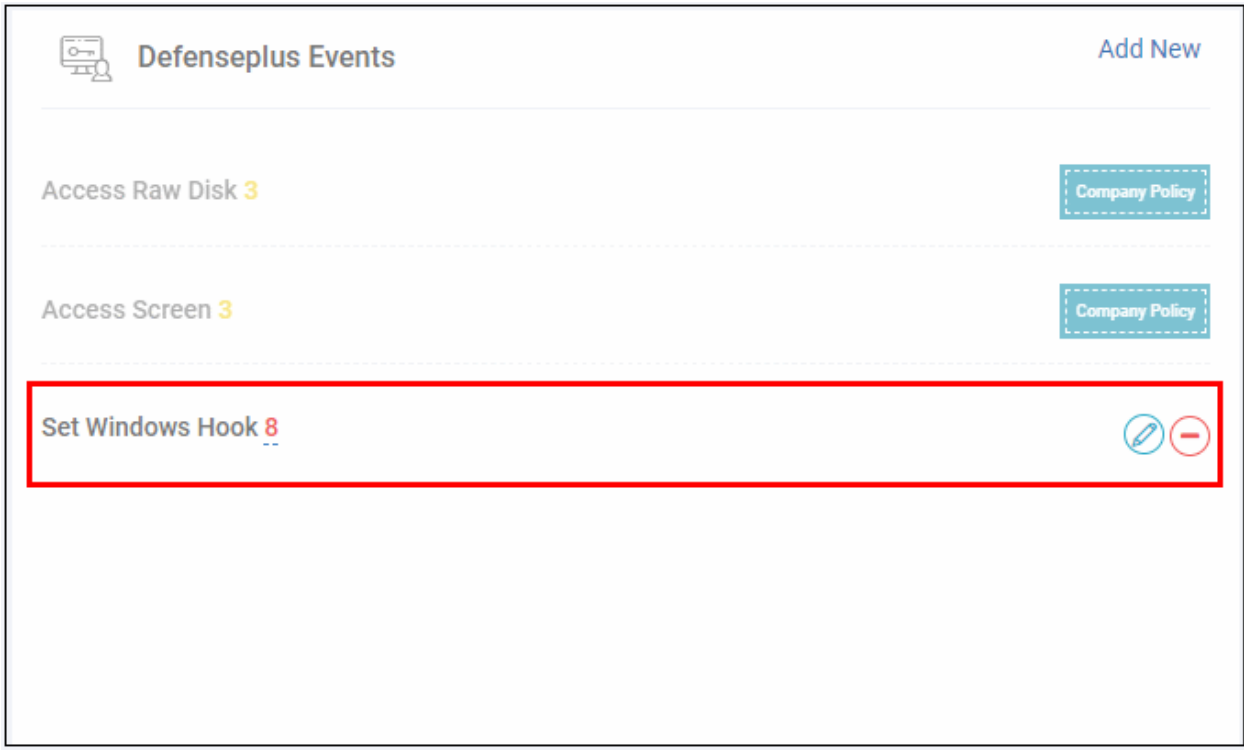
- Select the endpoint from the drop-down



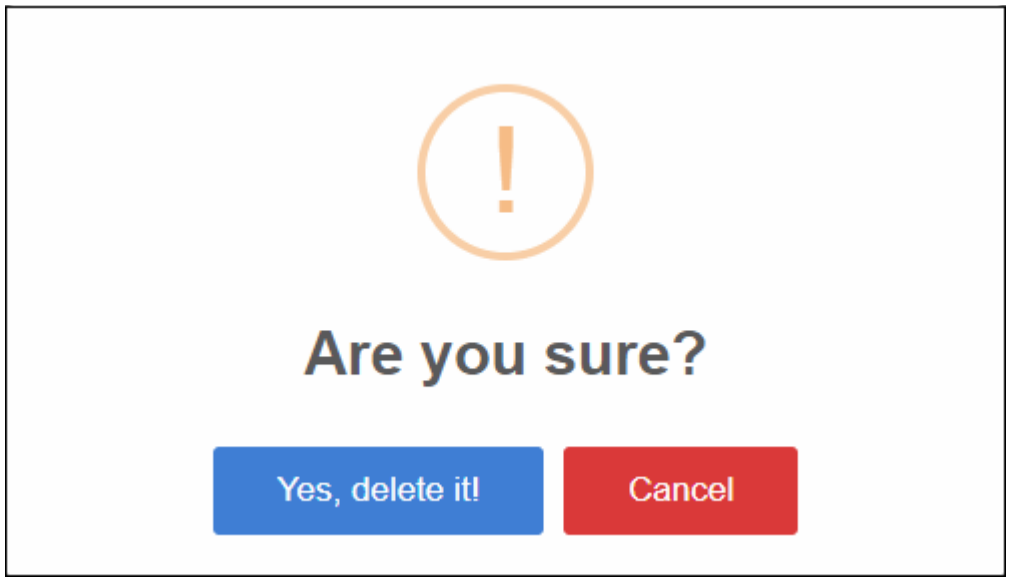
- All the event rules under 'Company Rules' will be applicable for the endpoint and shown as 'Company Policy', which cannot be edited or removed from here.



- Add new rules under event categories that will be applicable for the selected endpoint only
- Click 'Add New' link and follow the same process as explained under 'Company Rules'



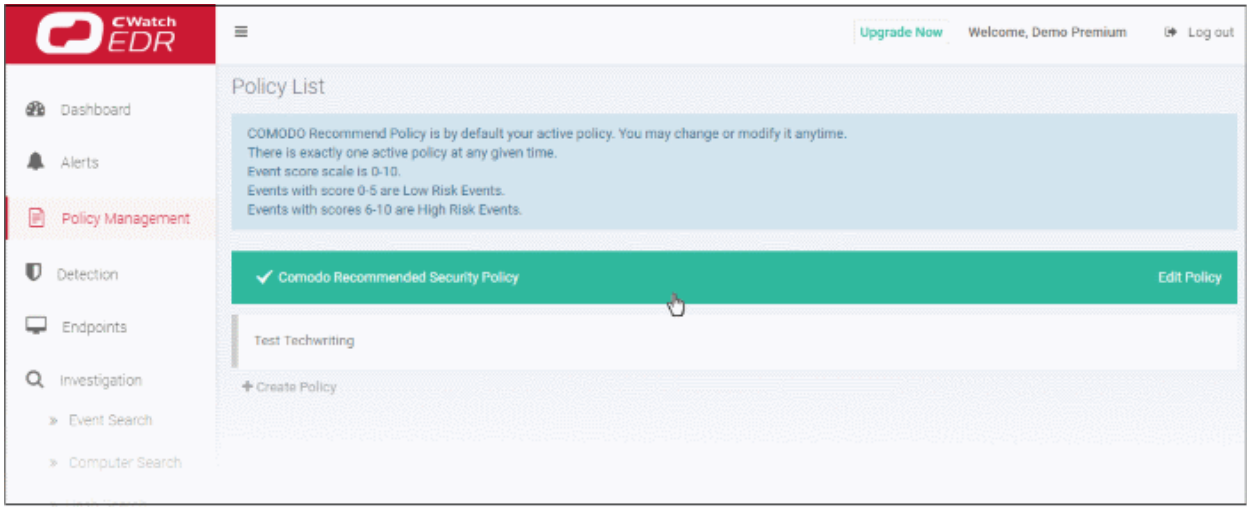
- The added rule can be edited or removed from the event category.
- To edit a rule, click the pencil icon beside it and update as required. The process is same as explained above.
- To remove a rule, click the delete icon beside it.



- Click 'Yes, delete it!' to confirm removal.

View and edit the default Comodo security policy

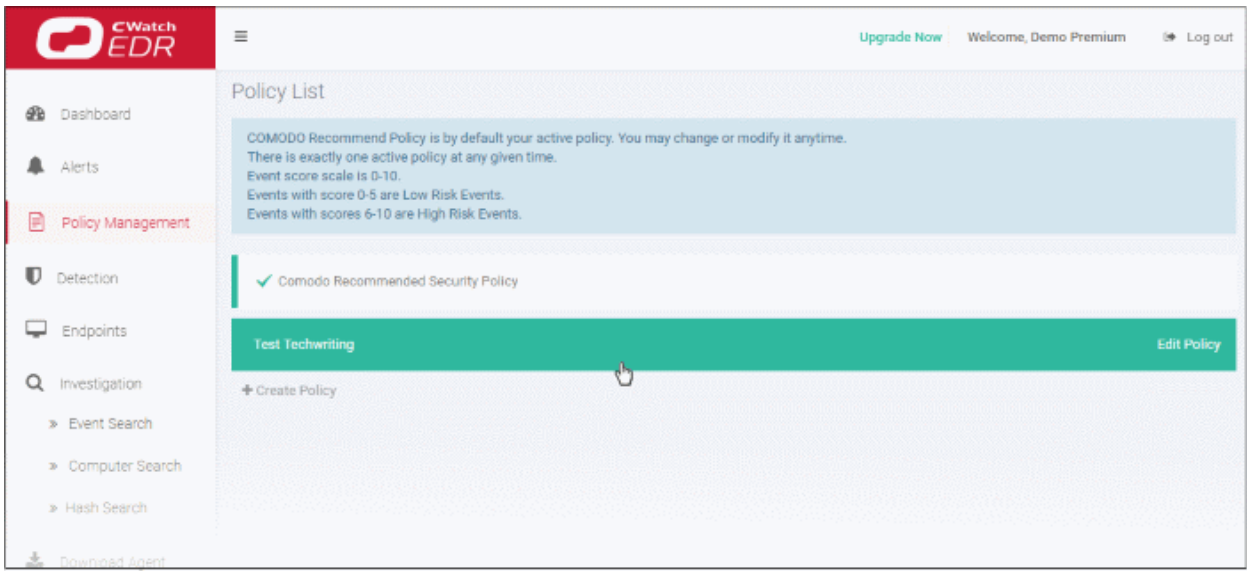
- Comodo EDR ships with a default security policy that is automatically applied to enrolled endpoints.
- Click 'Policy Management' on the left, then 'Comodo Recommended Security Policy'



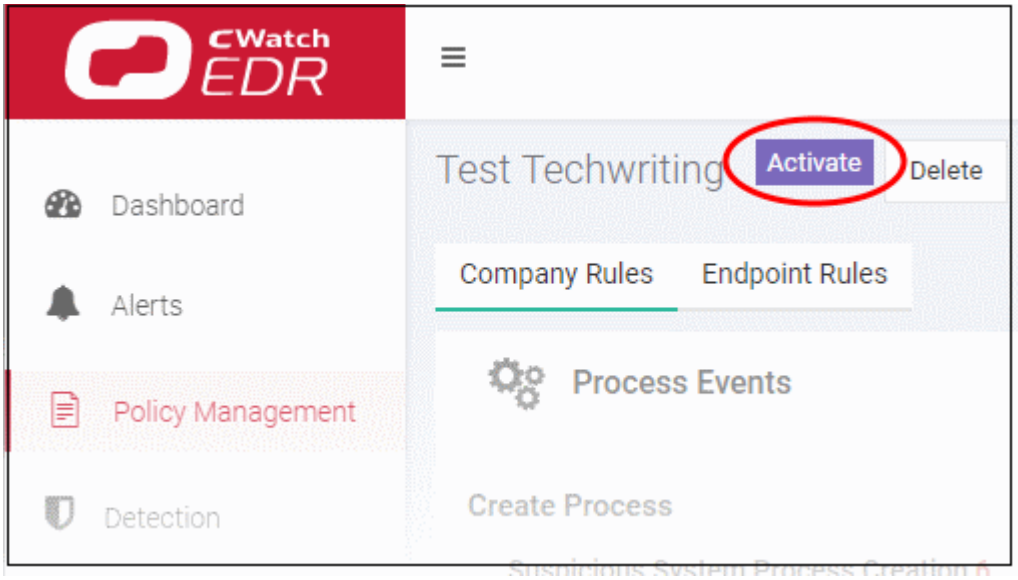
The policy interface is similar to the 'Create a new policy' interface. See '**Company Rules**' and '**Endpoint Rules**' under '**Create a new policy**' section.

Activate a policy

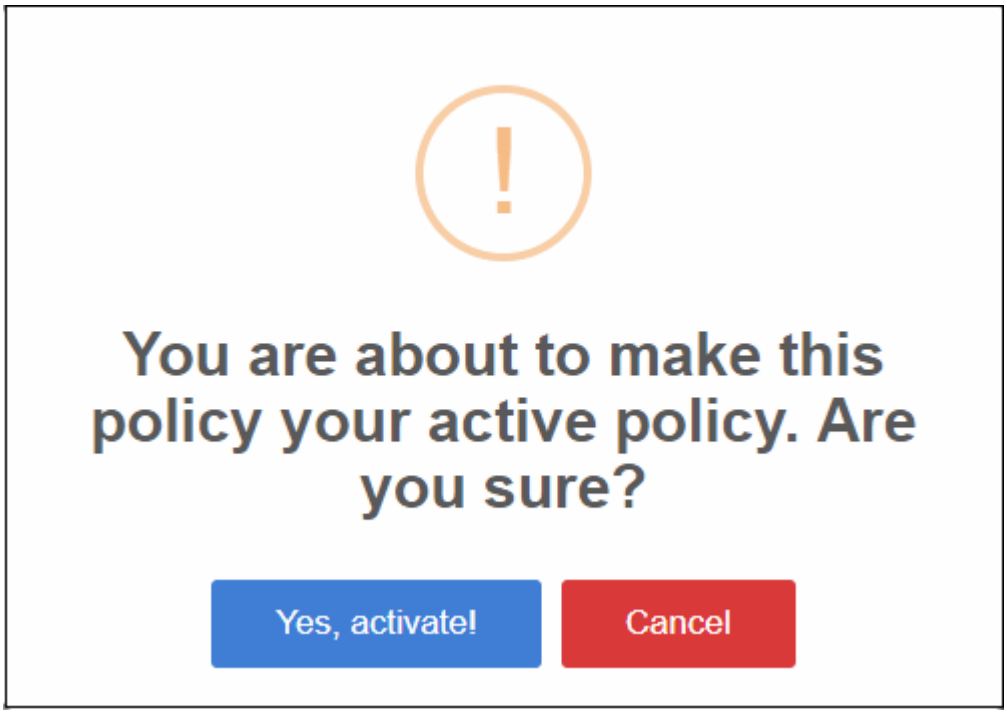
- You can add as many security policies as required but any one only can be active at a time.
- The active policy has a green check mark next to it.
- Click 'Policy Management' on the left then the security policy that you want to active.



- Click 'Activate' at the top



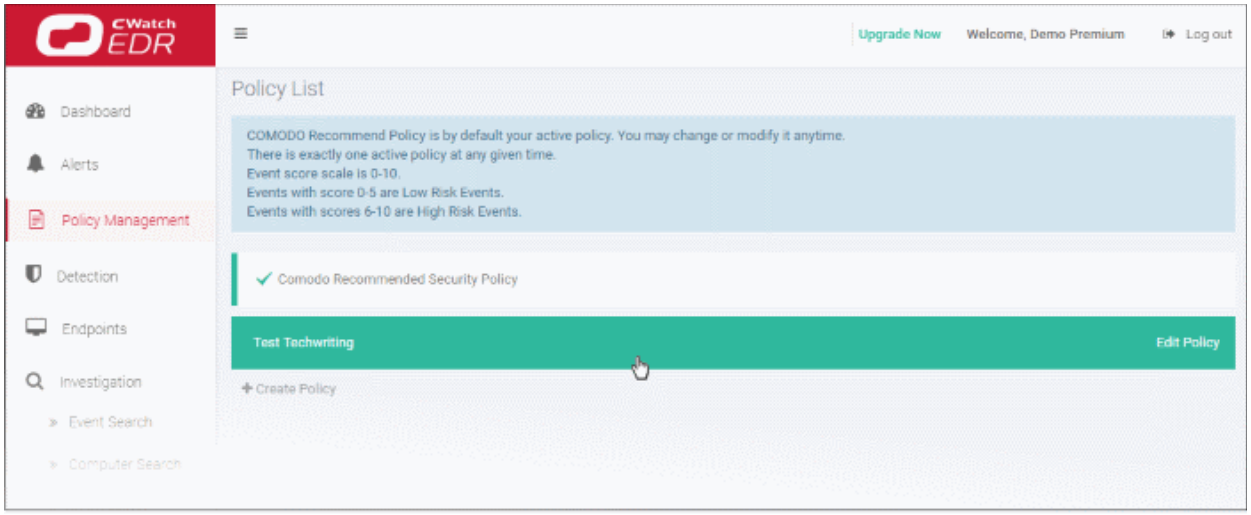
- Click 'Yes, activate' to confirm



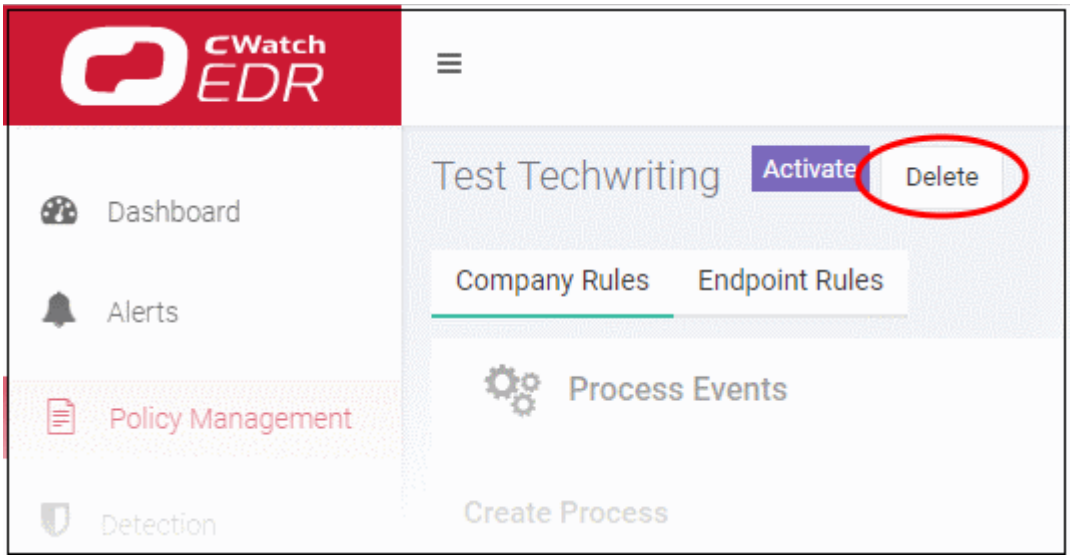
The policy will be activated and its rules will be applied to the enrolled endpoints.

Delete a policy

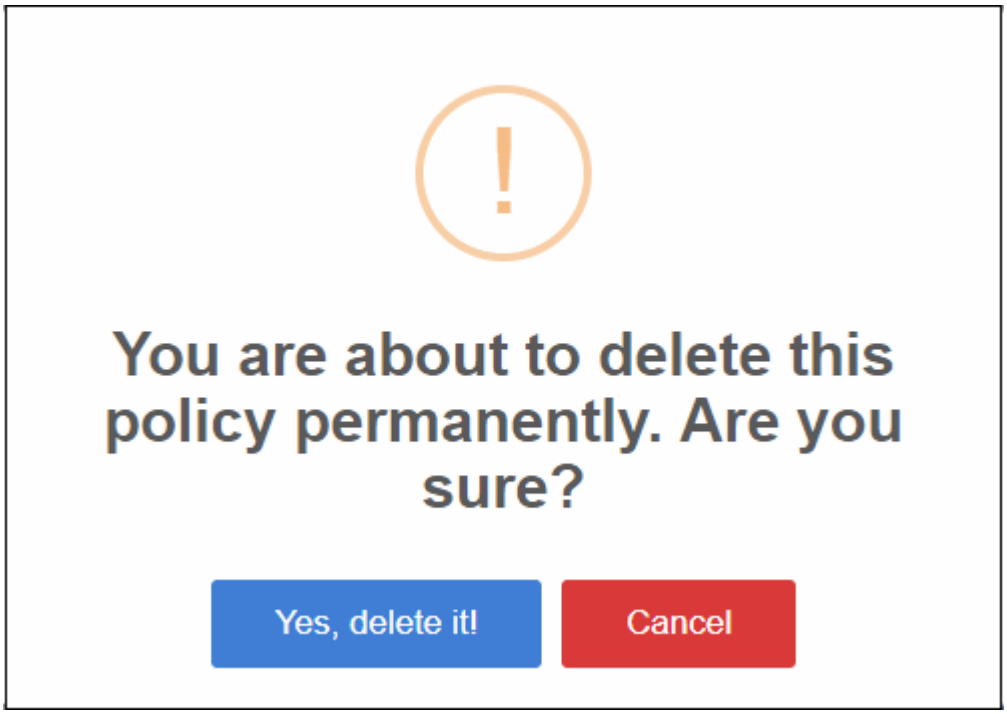
- You cannot delete an active policy
- Click 'Policy Management' on the left then the security policy that you want to delete



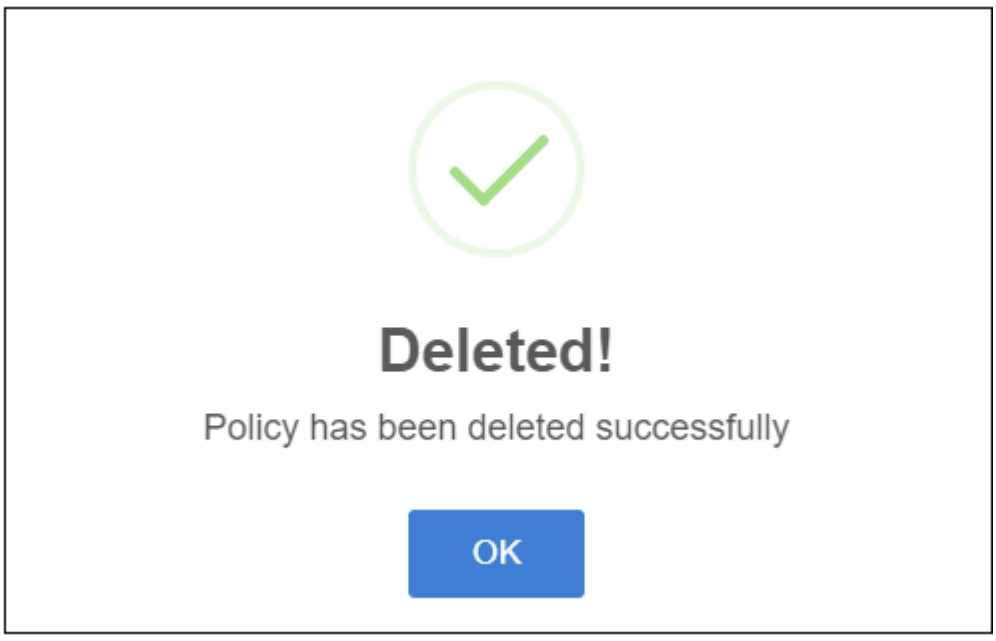
- Click 'Delete' at the top



- Click 'Yes, delete it!' to confirm



A confirmation dialog will be shown:

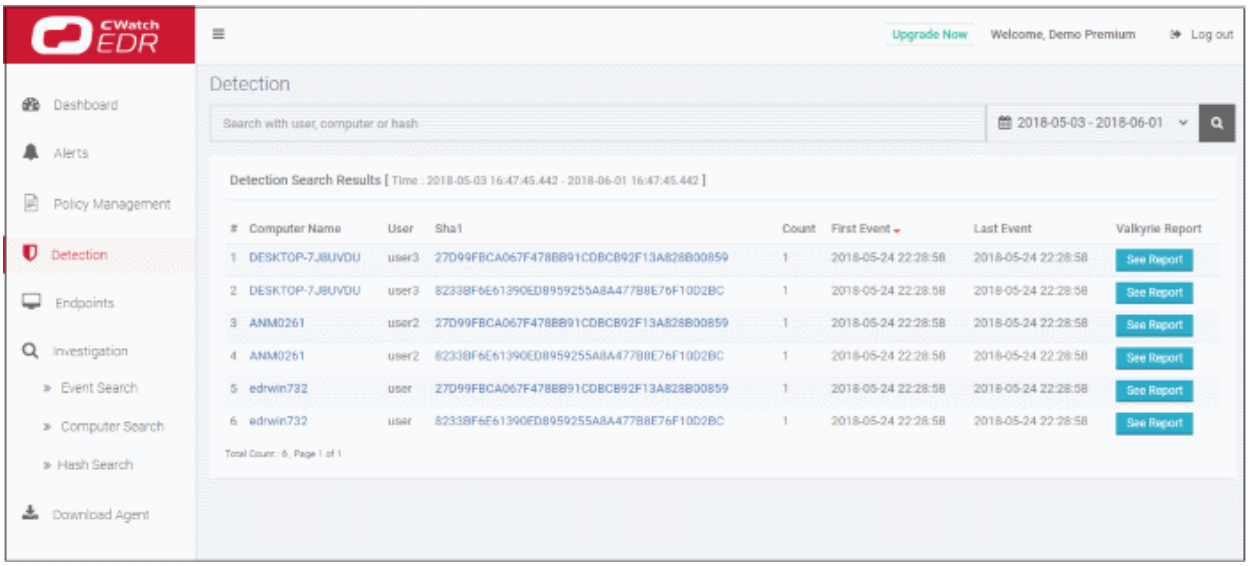


- Click 'OK' to close the dialog.

8 View Event Details on Endpoints

The 'Detection' screen provides an 'at-a-glance' summary of malicious events on your endpoints. The table shows detailed information about each malware incident.

- Click 'Detection' on the left to open the 'Detection' interface

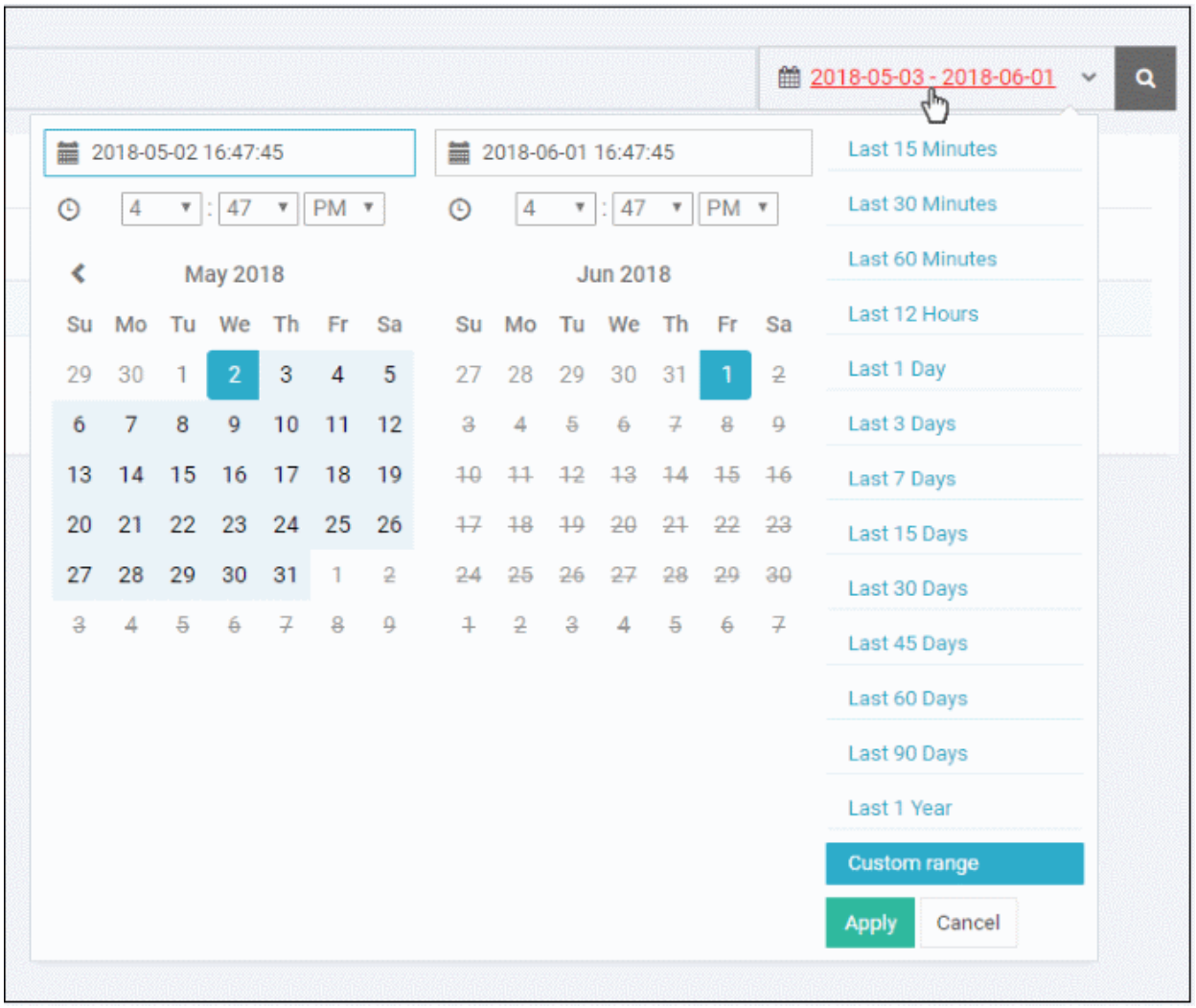


Detection Search Results - Table of Column Descriptions	
Column Header	**Description**
Computer Name	The name of the endpoint. Click the computer name to view its full details. See '**Computer Search**' for details.
User	The user who is logged in to the endpoint.
Sha 1	Hash value of the detected malware. Click the hash value to view its full details. See '**Hash Search**' for details.
Count	Number of times the malicious event was detected on the endpoint.
First Event	Date and time the event was first detected on the endpoint.
Last Event	Date and time the event was most recently detected on the endpoint.
Valkyrie Report	Unknown and suspicious files are analyzed by Comodo's Valkyrie, an advanced file analysis and file verdict system. Click 'See Report' to view full details of the file analysis. See **https://help.comodo.com/topic-397-1-773-9563-Introduction-to-Comodo-Valkyrie.html** for more information about Valkyrie.

Search and Sorting options

- **Search option** - The 'Search' boxes above the table allow you to filter the list.
  - Type full or partial search terms in the search box and press enter.
  - Matching results will be automatically displayed
  - Clear the search terms and click 'Search' again to reset the list.
- **Sorting option** - Click any column header to sort items in ascending/descending/alphabetical order.

Use the time-range drop-down to show event information for a specific date or date range.

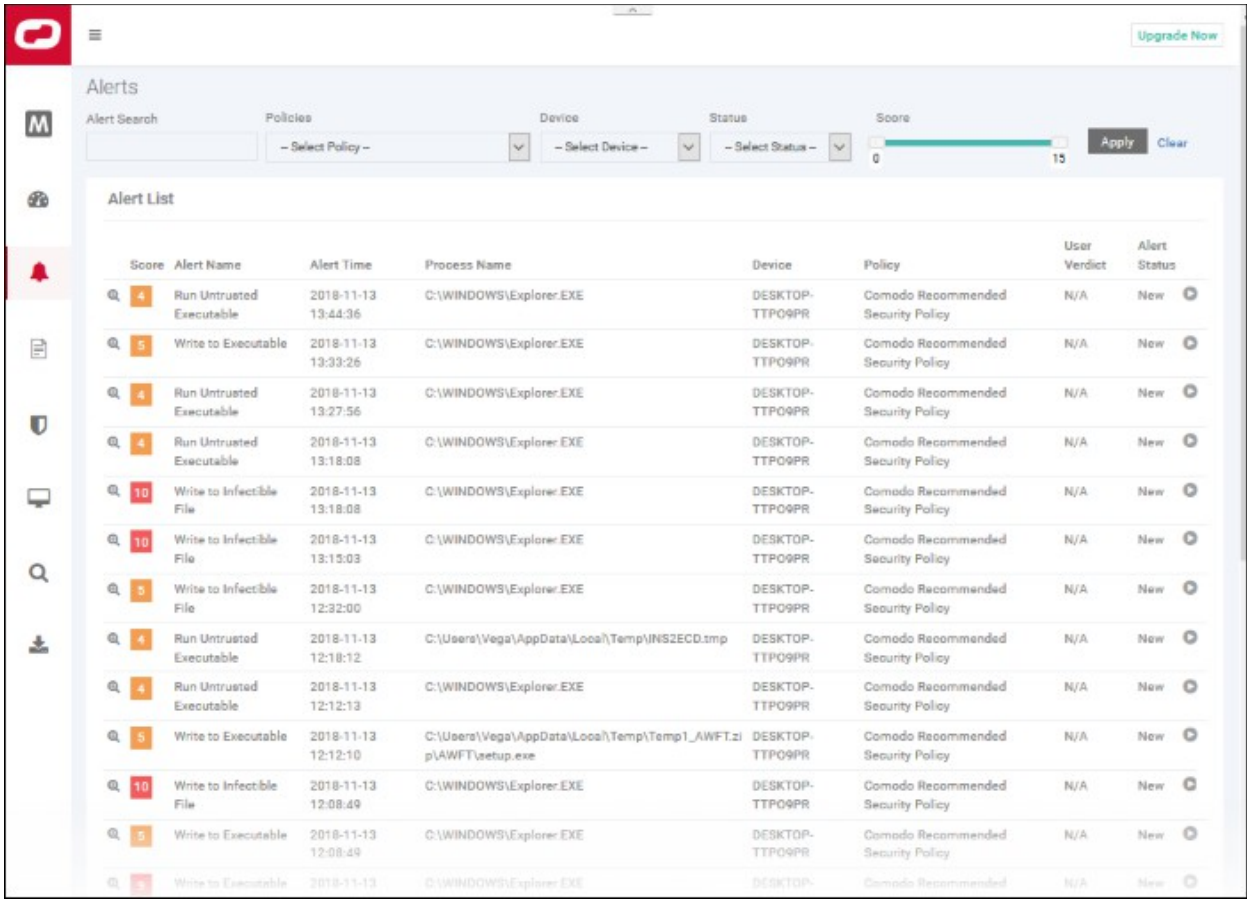


- Click 'Custom range' to choose specific dates:
- Click 'Apply'. The results for the selected period will be displayed.

9 Alerts

Alerts are generated when an event on your network matches a rule in your EDR policy. See '**Manage EDR Policies**' if you want to learn about policies and rules.

- Click 'Alerts' on the left to open the interface



Alerts - Table of Column Descriptions	
Column Header	**Description**
Score	The rating you specified for the event when creating the rule. You can apply a score between 0 and 10 based on the severity you place on the event. See '**Manage EDR Policies**' for more information.
Alert Name	The label you gave to the condition when creating the rule. Alerts are generated when rule conditions are triggered. See '**Manage EDR Policies**' for more information.
Alert Time	The date and time the warning was created.
Process Name	Path of the application that caused the event.
Device	The name of the endpoint from which the event was logged.
Policy	The name of the security policy that created the alert.
User Verdict	The status assigned to the alert by the admin who dealt with the issue. Options include: • False Positive - Admin does not consider the incident a security threat • True Positive - Admin confirms the incident occurred. The 'Score' attached to the

	incident should determine the response required. • Add comments. Note - The comments will not appear in the list of user verdicts
Alert Status	Progress of the alert. Statuses include: • New - Work has not yet started on the alert • In progress - An admin is attending to the alert • Resolved - An admin has submitted a verdict for the alert

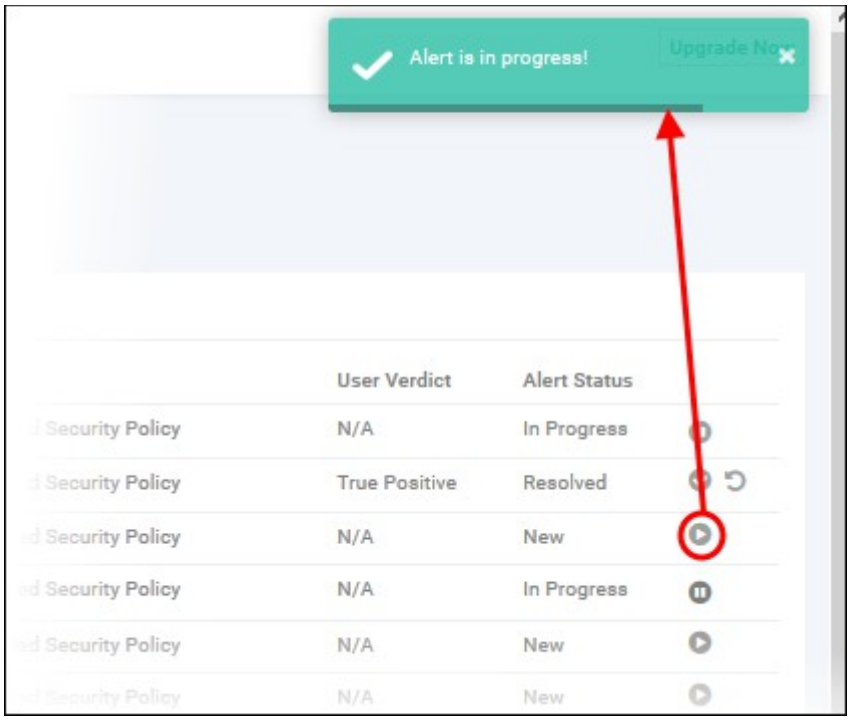
Filter options

You can search for particular alerts using the following filters:

- Alert Name - Search by alert label.
- Alert Time - Search by when the alert was generated.
- Process Name - Search by process name
- Devices - Select the device on which the event occurred
- Policy - Filter by policy that triggered the alert
- User Verdict - Filter by status awarded to the alert by an admin.
- Alert Status - Filter by any of the 3 progress levels - 'New', 'In progress' or 'Resolved'.
- Enter / select the filter and click 'Apply'
- Click 'Clear' to remove the search filters

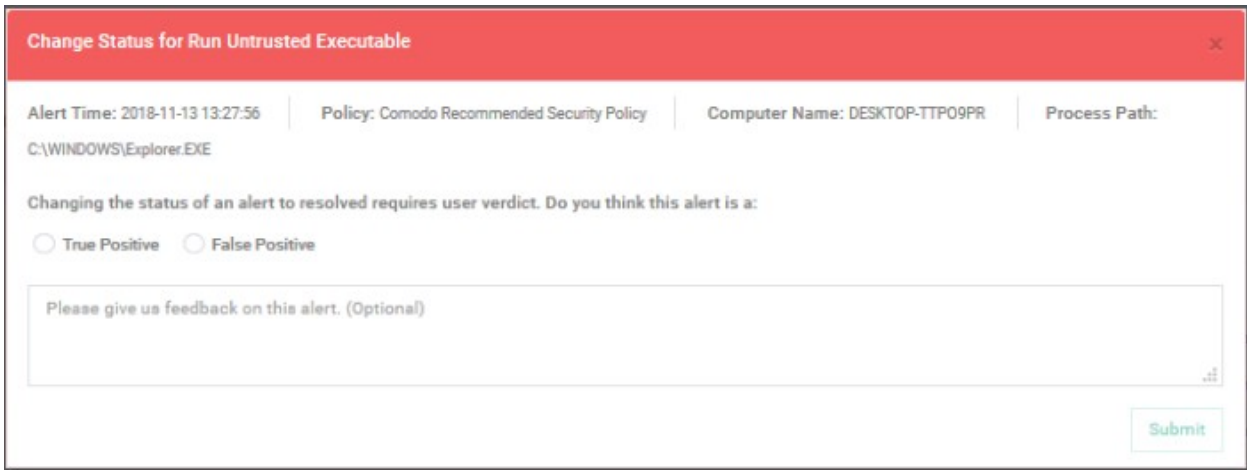
You can configure multiple filters to search for a particular alert. For example, you can search for an event by its alert name, policy and the endpoint.

- Click the play icon beside the 'New' alert status to submit the verdict.

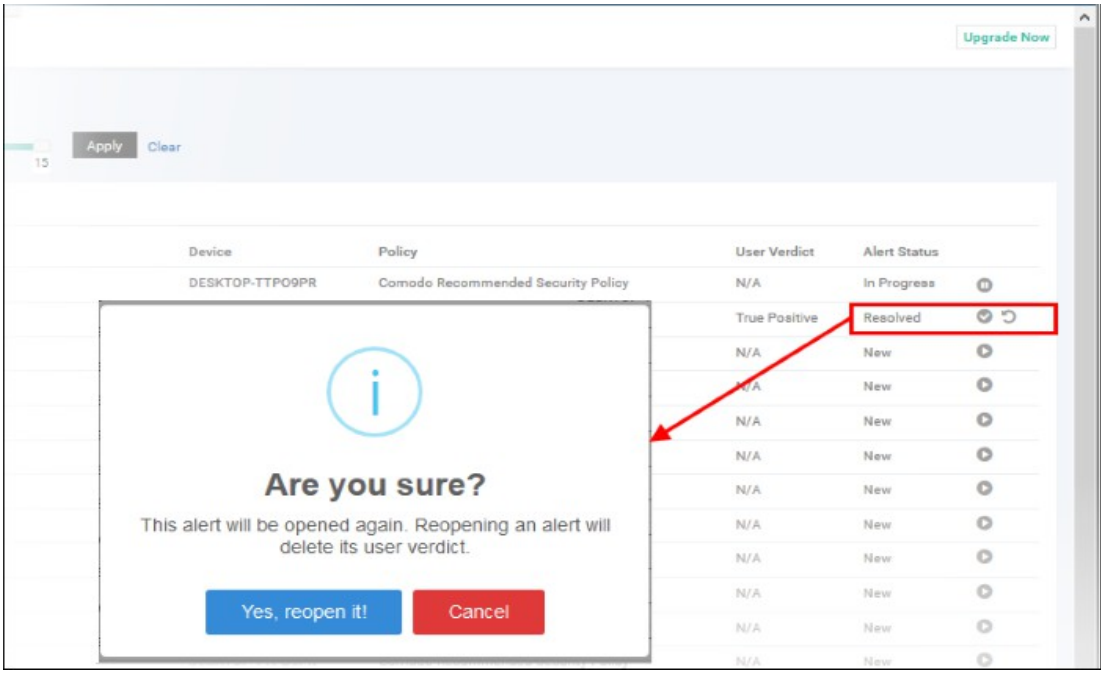


The alert status will change to 'In progress'

- Click the progress icon to submit the verdict



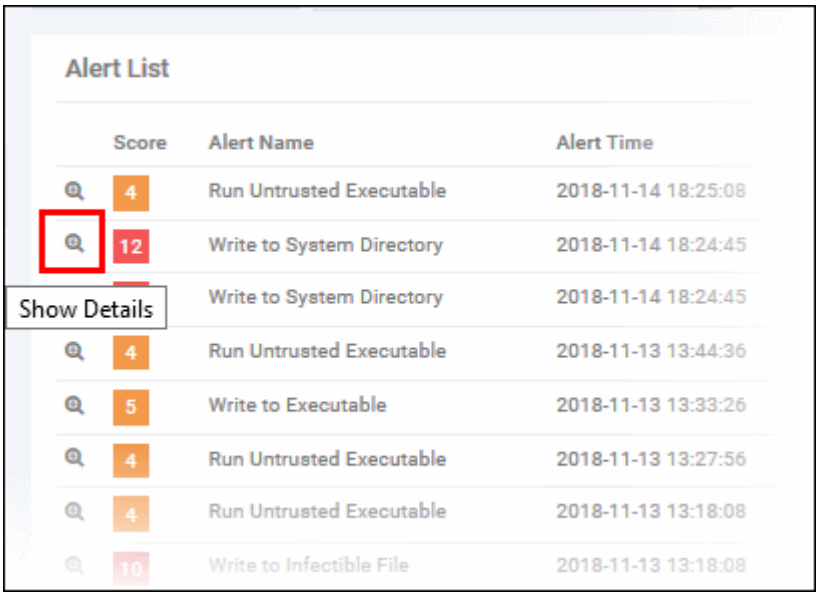
- Click 'Submit' to resolve the alert
- Click the reopen icon if you want to change the verdict.



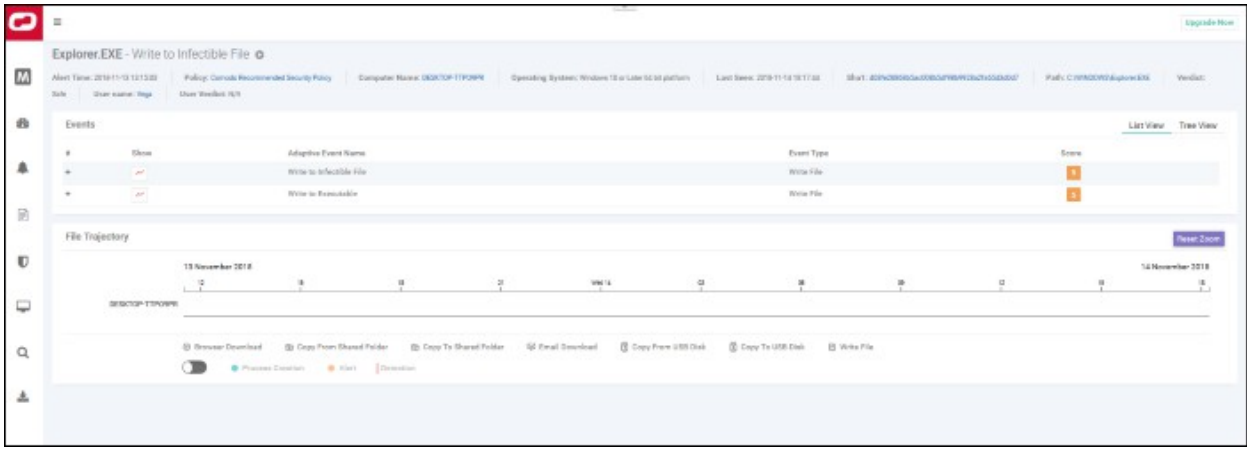
- Click 'Yes, reopen it!' to change the verdict
- Click 'Cancel' to keep the verdict unchanged

View Event Details

- Click 'Show Details' in the 'Score' column:



This open the information screen for that event:



The top part of the screen shows details such as the alert name and the application that generated the event:

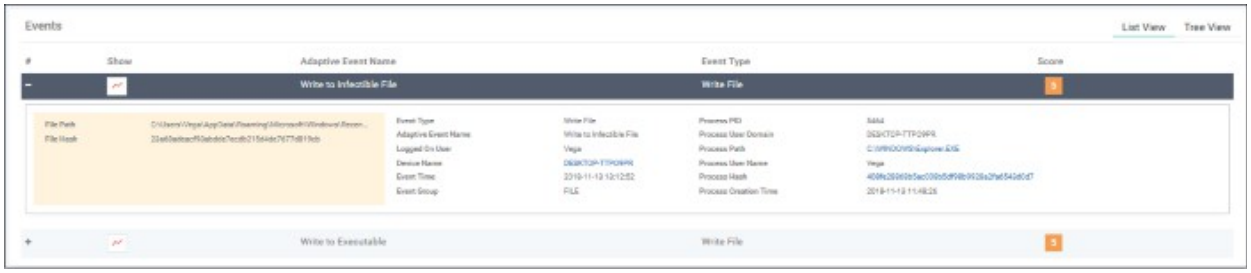
- Alert and application name is shown at the top
- Alert Time - Date and time of the alert
- Policy - Name of the security policy. Click the name of the policy to open the policy management screen. See '**Manage EDR Policies**' for more information.
- Computer Name - Name of the endpoint from which the event was logged. Clicking the endpoint will open the 'Computer Search' screen with the endpoint preselected. See '**Computer Search**' for more details.
- Operating System - Details of the endpoint's OS from which the event was logged.
- Last Seen - The last date and time the endpoint communicated with EDR.
- Sha 1 - The hash value of the file. Clicking the hash value will open the 'Hash Search' screen with the file preselected. See '**Hash Search**' for more information.
- Path - The full process path of the event that was logged. Clicking the process path will open the 'Event Search' screen with the event query auto-filled in the search field. See '**Event Search**' for more details.
- Verdict - Valkyrie results after the analysis.

- User name - The logged in user name of the endpoint. Clicking the name will open the 'Event Search' screen with the event query auto-filled in the search field. See '**Event Search**' for more details.
- User Verdict - The admin's conclusion on the nature of alert. The options given to declare the results are 'True Positive' and False Positive'.

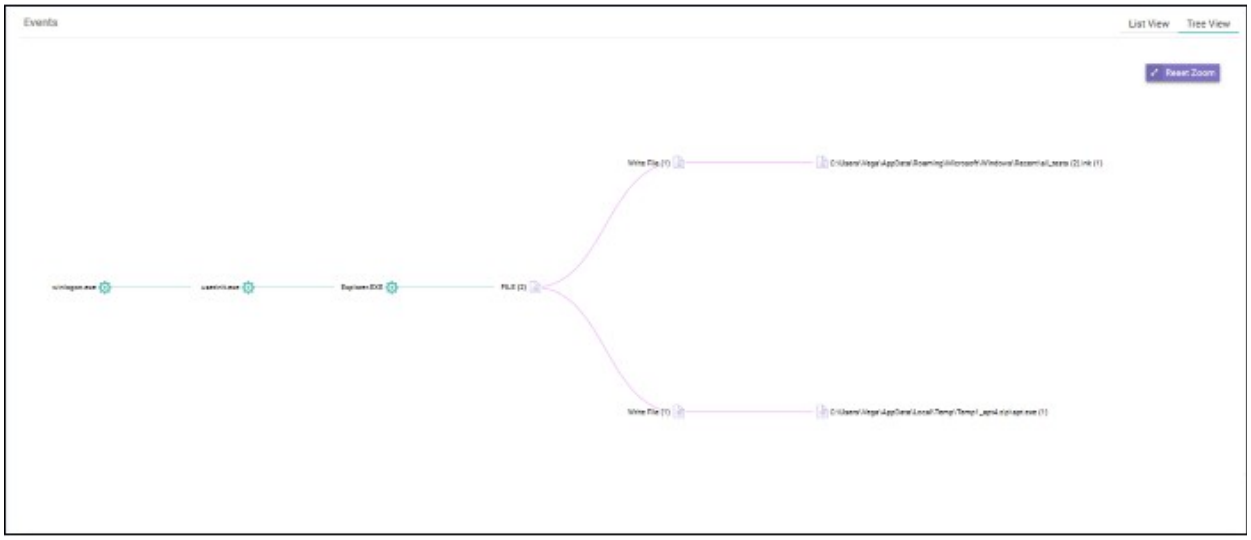
Events

Details of the event are shown in the main pane:

- **List View**
  - Show - Click  icon to view the event timeline. See '**Process Timeline**' for more details.
  - Adaptive Event Name - Label given to the event when creating the security rule.
  - Event Type - The category of event
  - Score - The event severity. This was specified when the rule was created.
  - Click anywhere in the row to view all event fields for that event type. The number of event fields shown depends on the event type.:



- **Tree View**
  - Click 'Tree View' link at top-right of 'Events' section



The screen shows the full process path of the event. Clicking any process label will open the 'Event Search' screen with the event query auto-filled in the search field. See '**Event Search**' for more details.

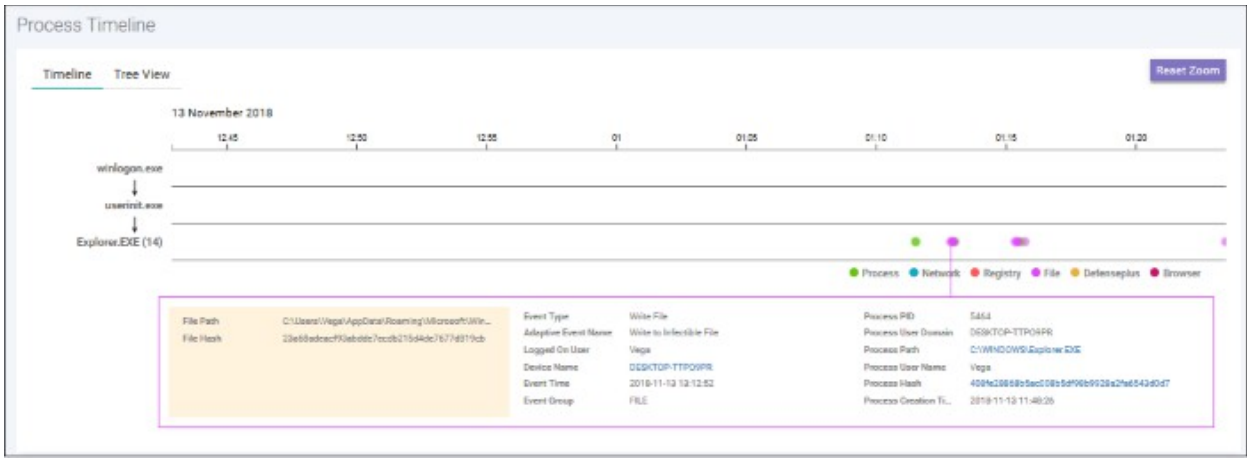
- Zoom in or out using your mouse. Right-click and move the chart left or right. Click 'Reset Zoom' to return to default view.

Process Timeline of the Event

Shows the various activities happening in an event for each file type

Timeline View

- Click the 'Show in Process Timeline' icon of the event

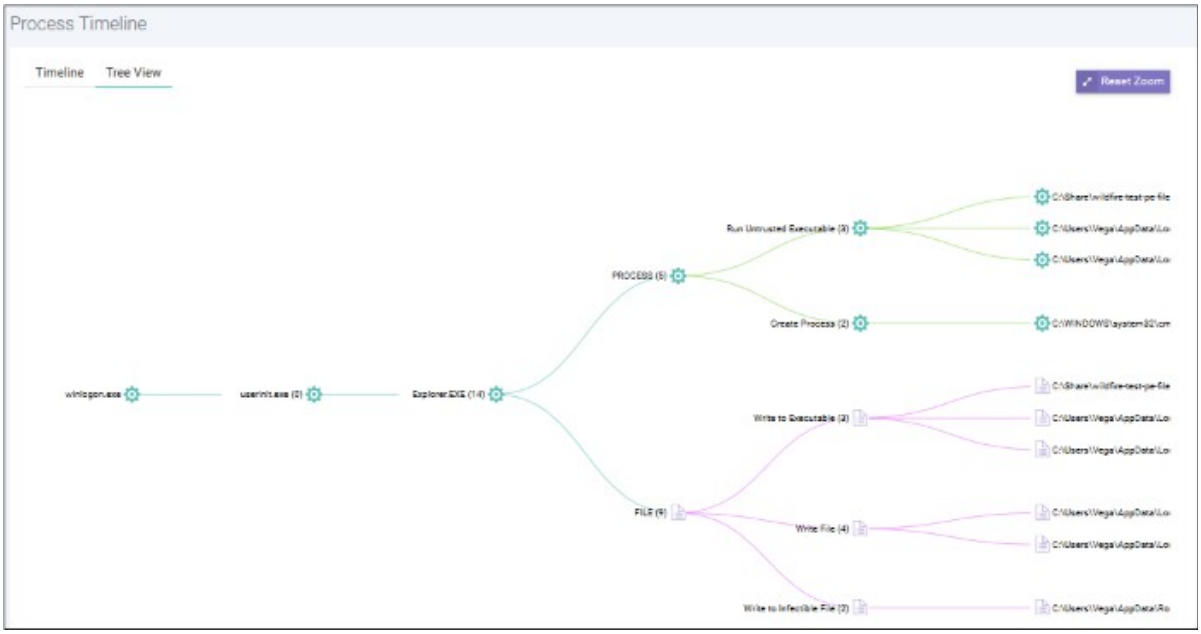


The 'Process Timeline' screen will open

The screen shows the time at which each event occurred. See '**Process Timeline** for more details.

Tree View

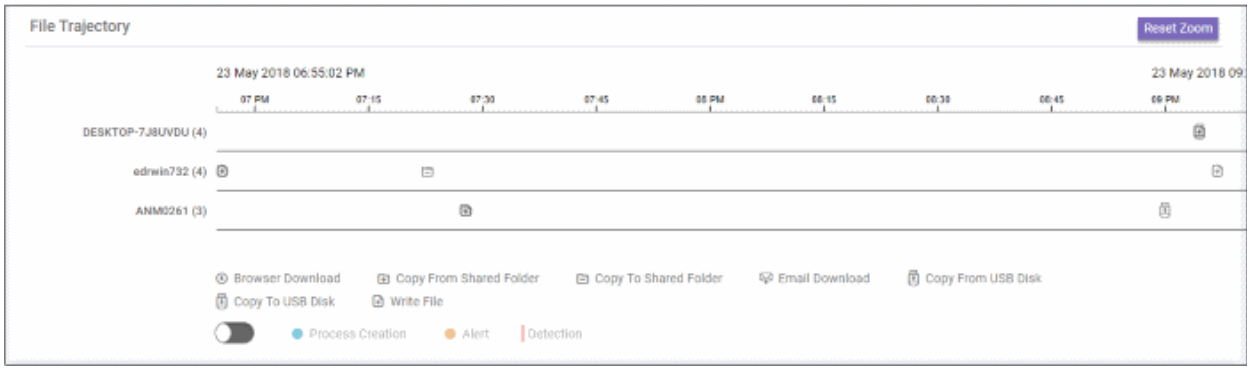
- Click the 'Show in Process Timeline' icon of the event
- Click 'Tree View'



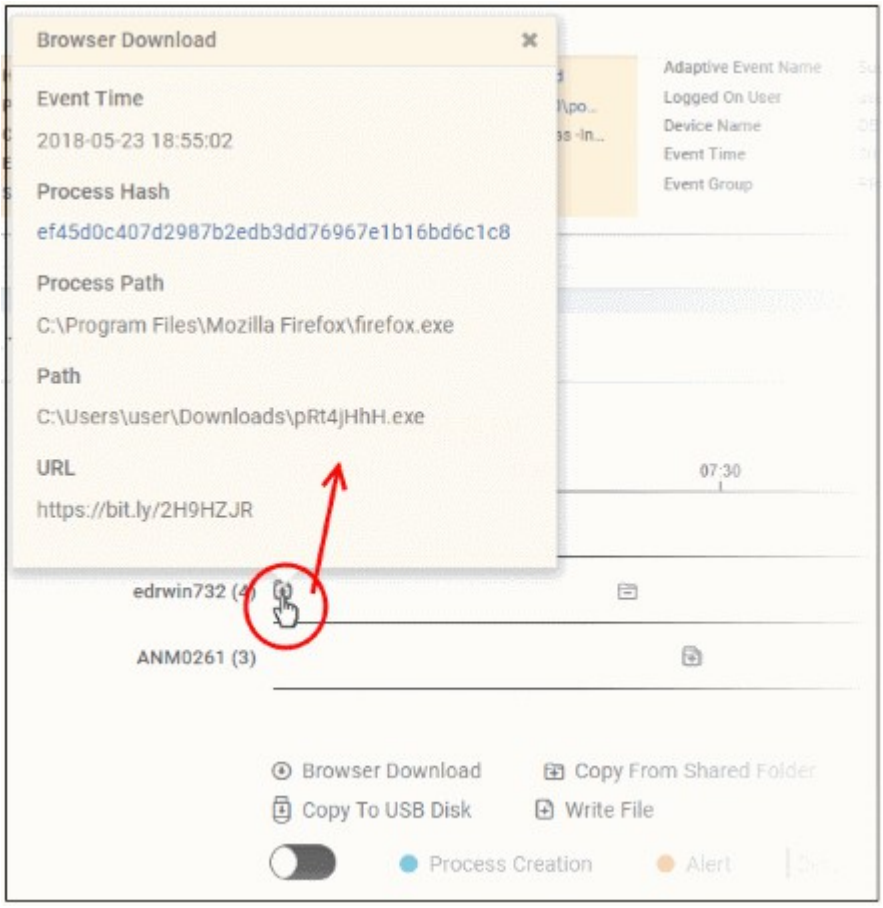
The screen shows the tree view of the event occurrences. See '**Process Timeline**' for more details.

File Trajectory

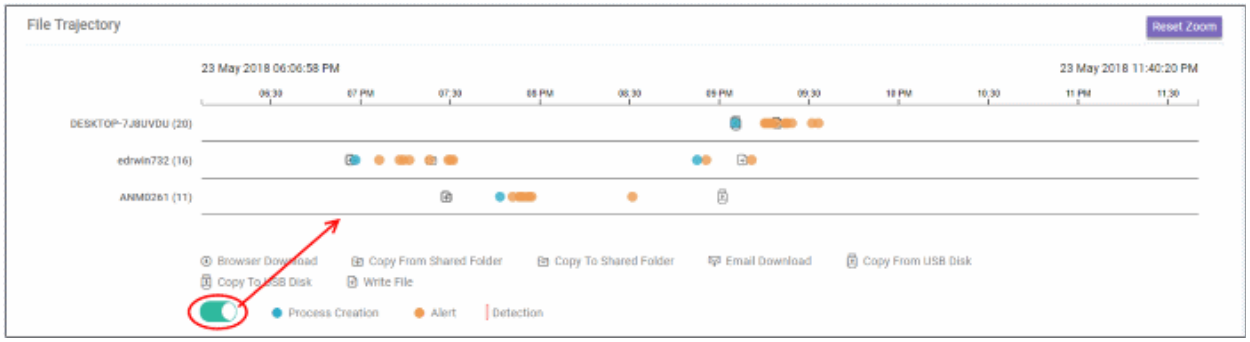
The bottom section of the screen displays the movement of the file, that is from where it was downloaded, copied to which endpoint and so on.



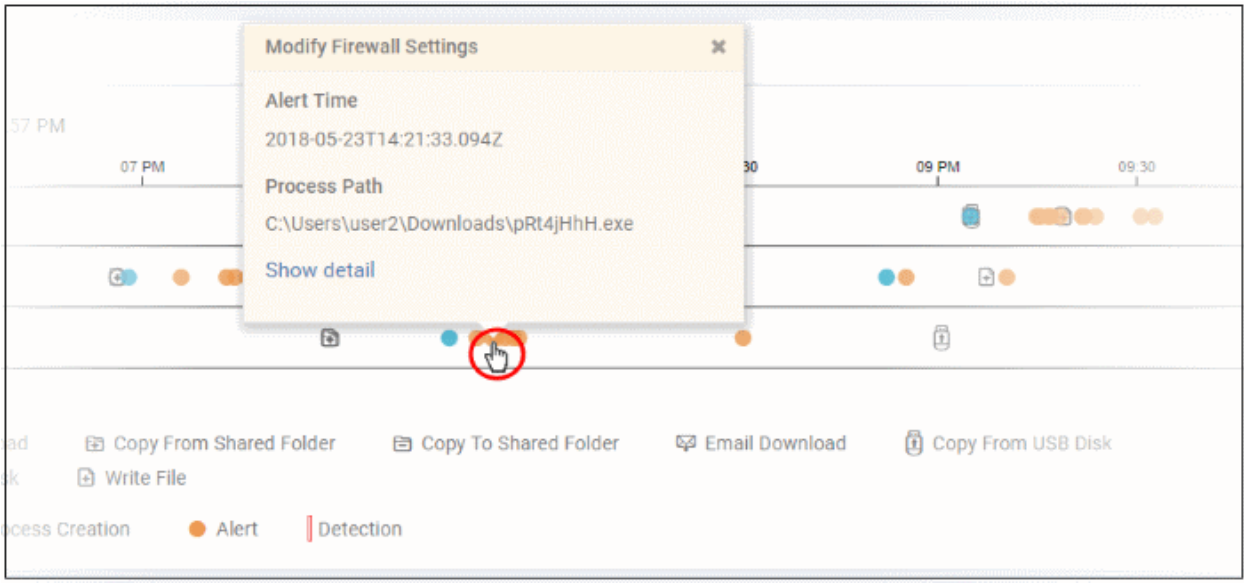
- Zoom in or out using your mouse. Right-click and move the chart left or right. Click 'Reset Zoom' to return to default view.
- Details of the icons is shown below the graph.
- Click an icon to view the trajectory details.



- Click 'X' to close the dialog.
- Click 'Process Creation' button to view time of process creation, event detected and alert generated.



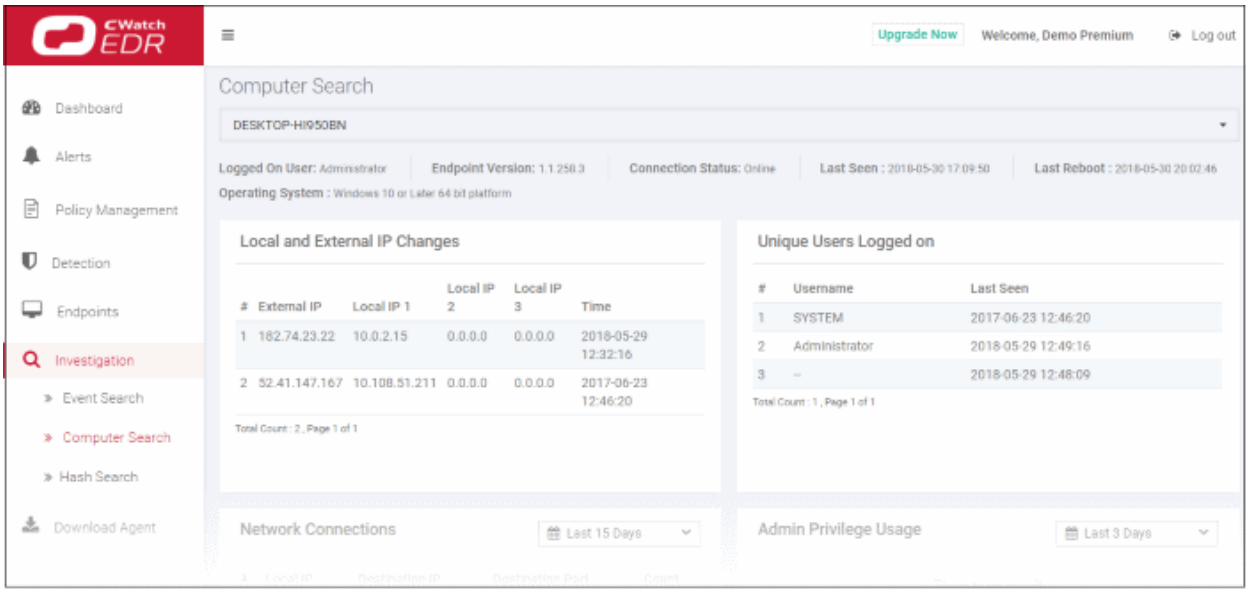
- Click an icon color code to view trajectory details.



- 'Show detail' link will be available for Alert dialog. Clicking the link will open the event details screen for which the alert was generated.
- Click 'X' to close the dialog.

10 Investigation

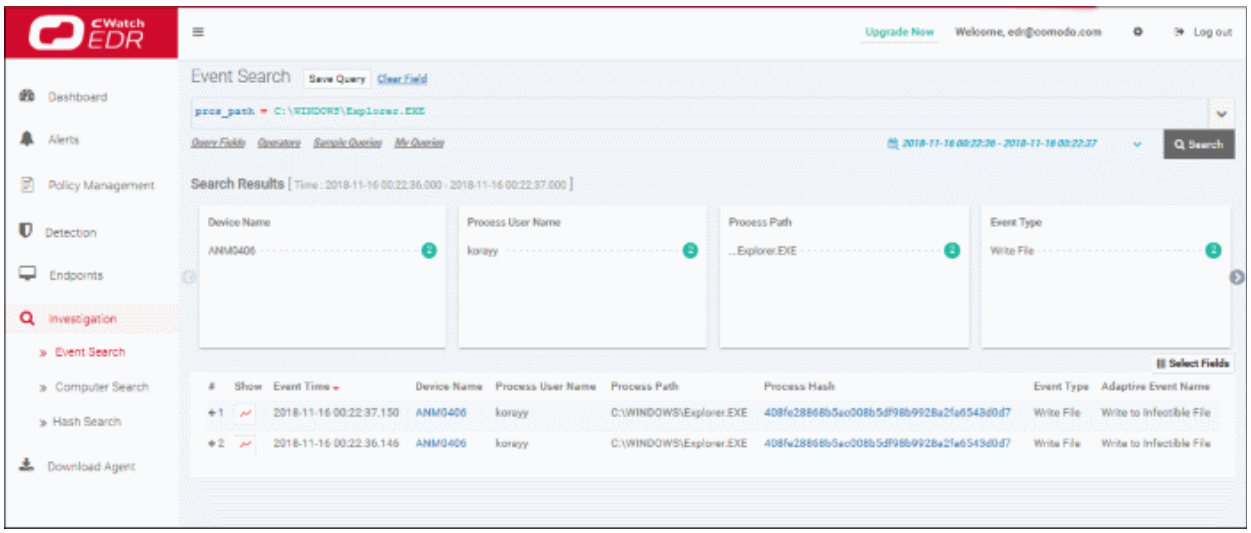
The 'Investigation' section allows you to identify analyze events by event type, computer or hash value. For example, you can query events generated by a certain browser on specific devices.



- **Event Search** - Search for events according to specific parameters. Parameters include event ID, device name, logged on user and so on. You can use operators to concatenate parameters and build granular queries. See '**Event Search**' for details.
- **Computer Search** - Search for events that were recorded on a specific endpoint. The search results include items such as network connections, malware detections, event trends and so on. See '**Computer Search**' for details.
- **Hash Search** - Search for events based on the hash value of the file. The search results include file name and type, point of entry, execution trend, file history and more. See '**Hash Search**' for details.
- **Process Timeline** - View a timeline of processes initiated by events. See '**Process Timeline**' for details.

10.1 Event Search

- The 'Event Search' interface lets you find specific events using built-in queries.
- cWatch ships with some useful sample queries, and you can construct your own queries.
- You have to create conditions for a search and configure the results table accordingly.
- You can also use the search results to construct another query.
- Click 'Investigation' on the left then 'Event Search' to open the interface:



- By default, no custom queries are defined, allowing you search for all events that occurred during the last 3 days.
- Use the 'Query Fields' and 'Operator' links on the upper-left to build a custom event query.
- The first query field you add will automatically have the '=' operator appended to it (you can change this if required). You will need to enter the criteria after the operator.
- Any subsequent fields you add to the query will automatically be prefixed with the 'AND' operator.
- All queries that you save will be listed under 'My Queries'
- 'Sample Queries' are pre-defined, example queries. These can be used as standalones, or adapted to produce a more complex search.
- 'Select Fields' on the right lets you configure the columns of the results table.
- You can change the date range using the link 2nd from the right.

Event Search Interface - Table of controls	
Select Fields	Allows you to configure the 'Results' table for the query results displayed at the lower pane.
Last 3 Days	Allows you choose the time period for which events are fetched. Periods range from 15 minutes to 1 month. You can also specify a custom period.
Search	Allows you to run a search operation based on the configured / general query.
Query Fields	Allows you to add query fields for a custom query
Operators	Allows you to add conditions for a custom query.
Sample Queries	Built-in sample event queries that are most often used.
Clear Field	Allows you to remove queries entered in the search field
Save Query	Allows you to save a custom query
My Queries	Saved custom queries will be listed here.

The interface allows you to:

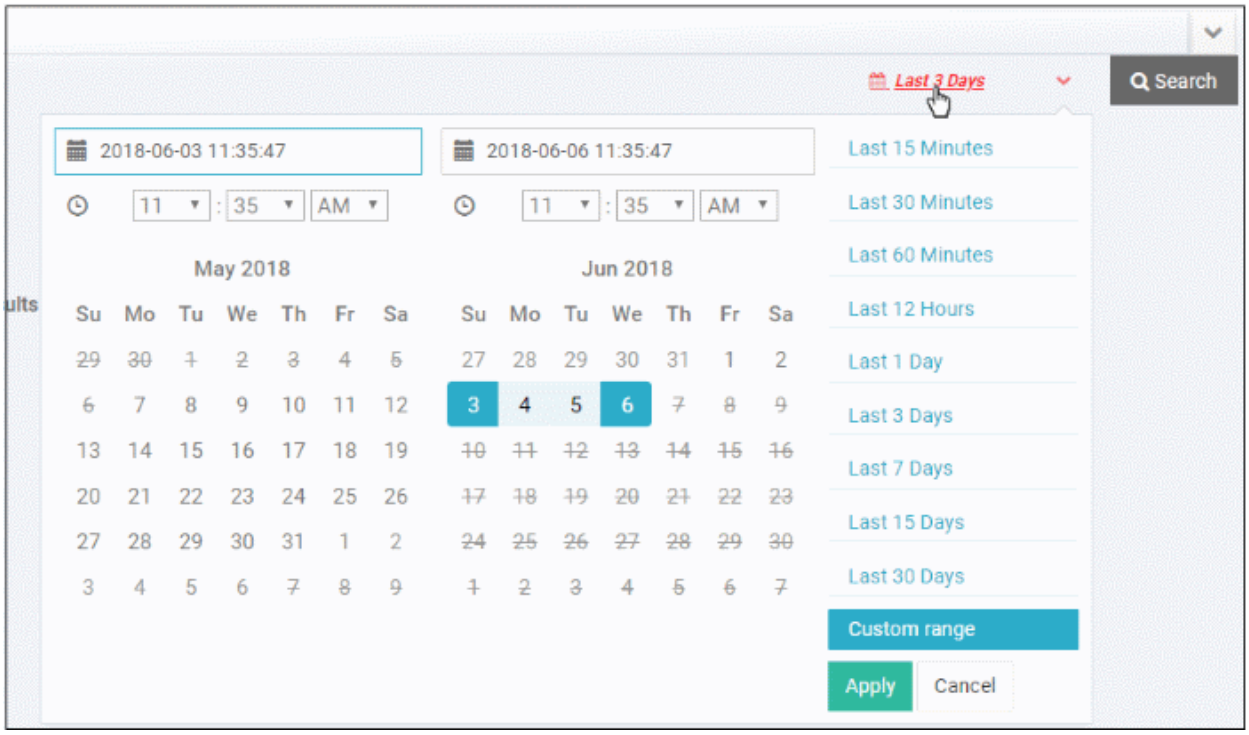
- **Run a general event search**
- **Configure and run a custom query search**
- **Use sample queries**
- **View query results**
- **Configure results table column headers for a query**

Run a general event search

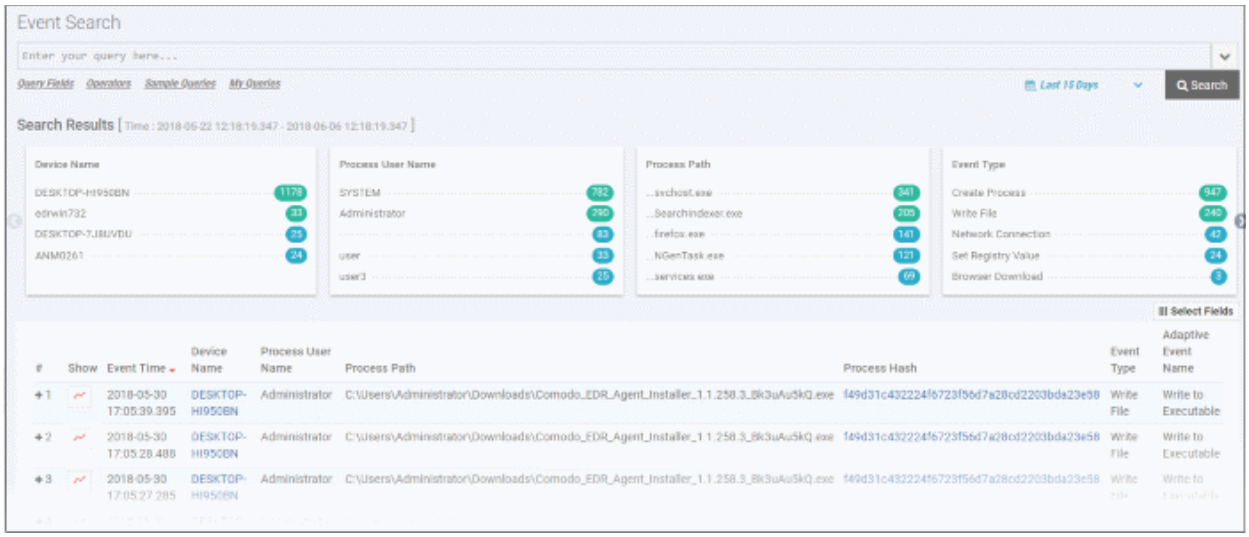
A general search returns all events recorded from all enrolled endpoints.

To run a general event search:

- Make sure the 'Search Box' field is blank.
- Use the time-range drop-down to pick a specific date or date range.



- Click 'Custom range' to choose specific dates
- Click 'Apply', then 'Search'



The results for the selected period will be displayed. See '**View Query Results**' for more information.

Configure and run a custom query search

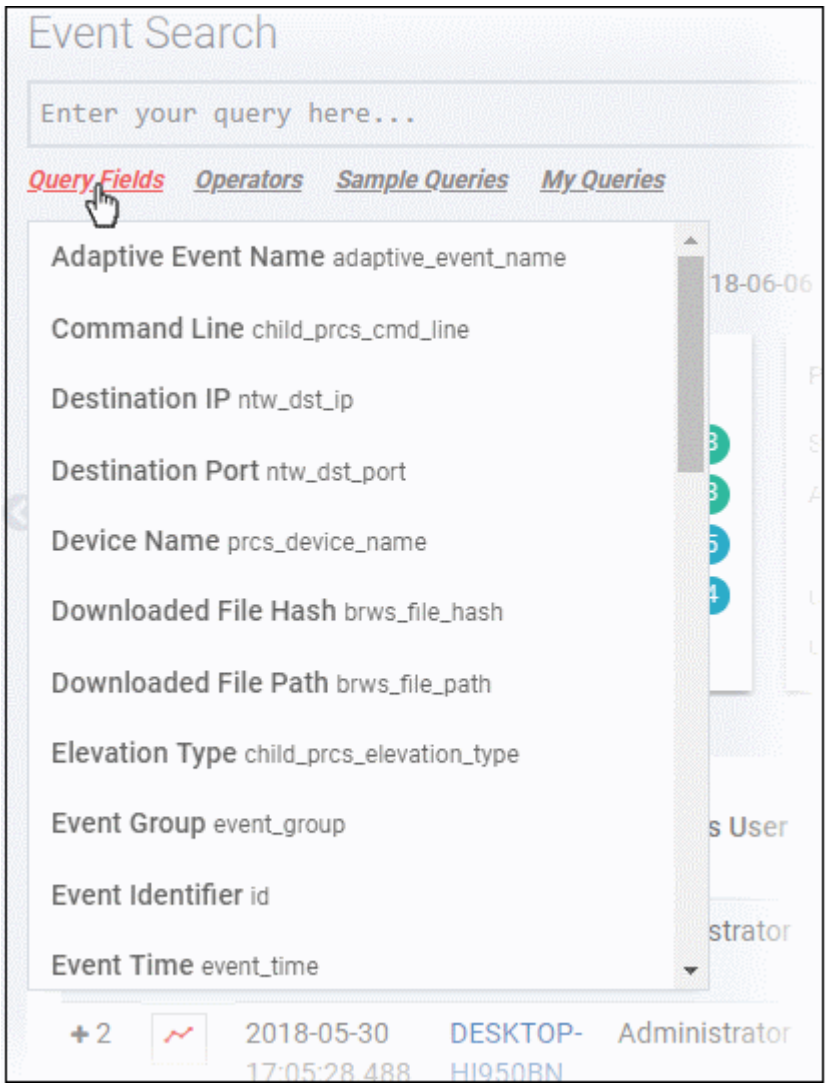
You can search for particular events by building custom queries. Custom queries can be configured in two ways:

- **Configure a custom event query manually**

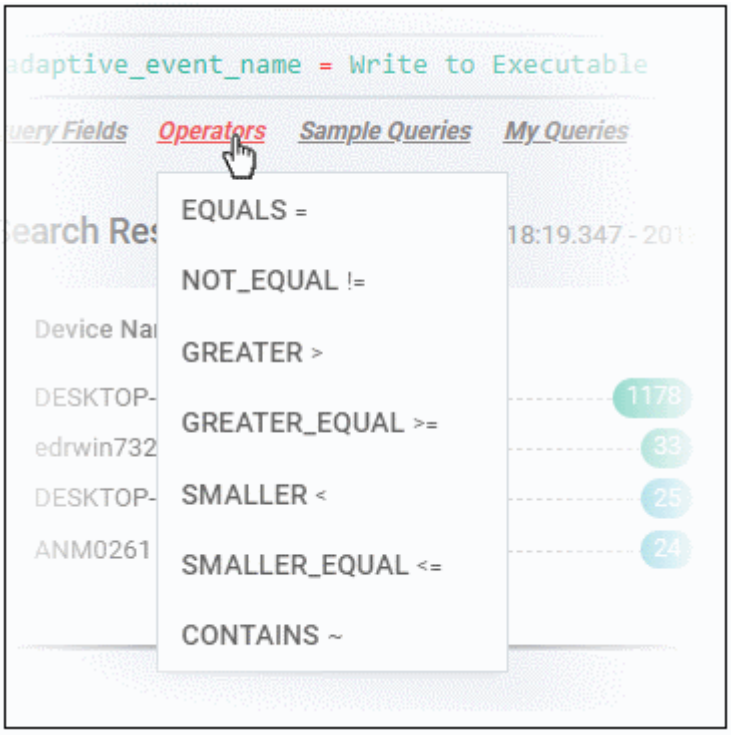
- **Using the search results**

To configure a custom event query

- Click 'Query Fields' below the search box and select an event from the list.



- Alternatively, click in the search box and use short cut keys 'Ctrl + space'. Select an event field from the list.
- Repeat the process to add more event fields for the query. The 'AND' operator will be automatically added to any subsequent fields you add.
- Click 'Operators' link and select the operator from the drop-down. You can also enter the operator manually.



- Enter the relevant details of the event fields.

The following example shows a search for 'Adaptive Event Name' = 'Run Untrusted Executable' AND 'Device Name' = 'DESKTOP-7J8UVDU':

- Next, select the time period for the custom query and click 'Search'

The search results for the custom query will be displayed:

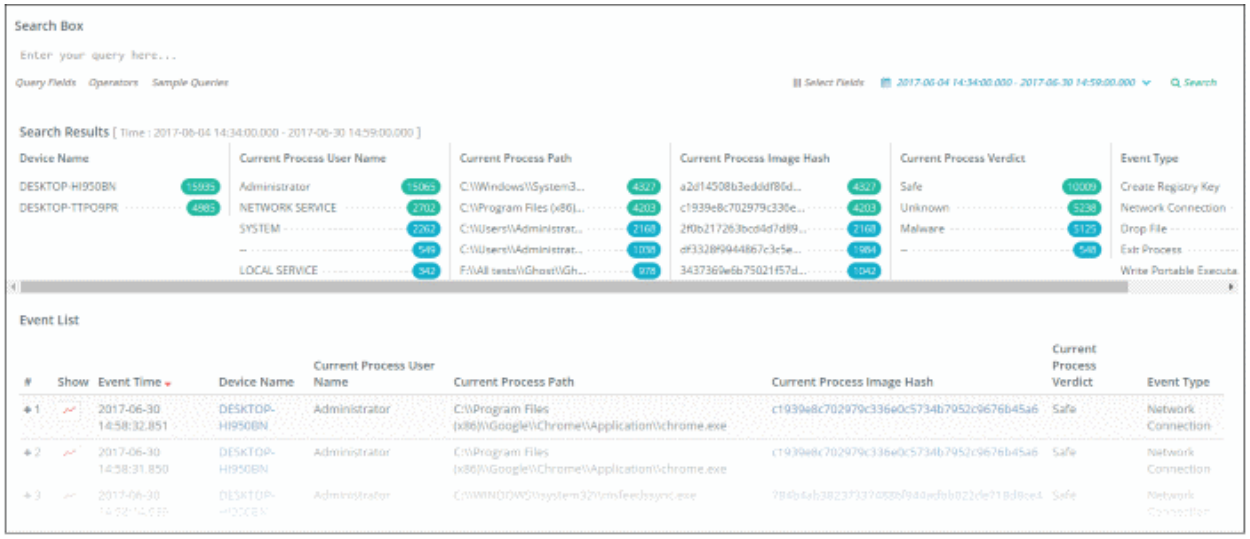
Please note the results for the query will also display details for other fields also. See '**View Query Results**' for more information.

- Click 'Save Query' for future use. The saved query will be listed under 'My Queries'.

To configure a custom query using the search results

In addition to manually providing the event field details for creating a custom query, you can also query for a particular event from the search results.

The following example shows the general search results for a selected time-period.

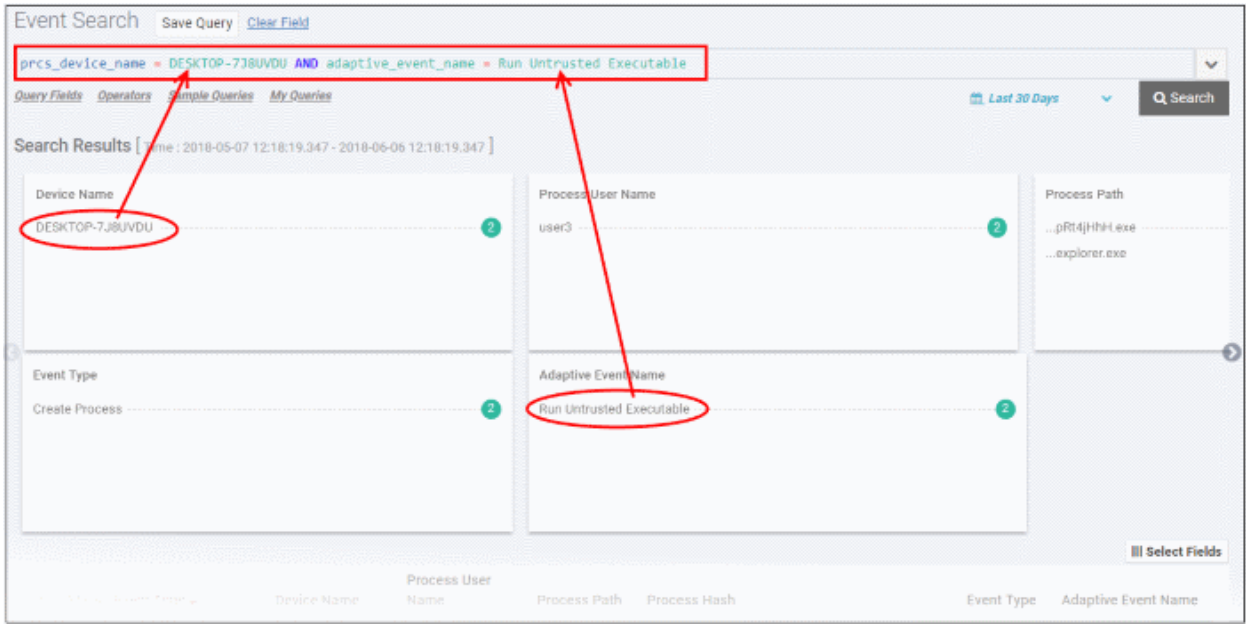


Summary Results section

The results summary section at the top shows results for all endpoints and events. You can select particular fields to build a custom query from the results.

The result columns depend on the **selected event fields**. For example if you want to search for run untrusted executable events for an endpoint:

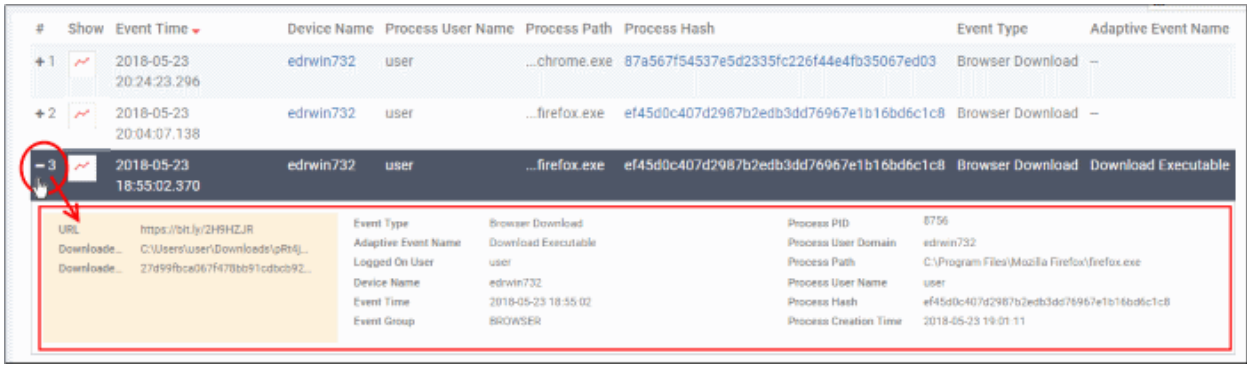
- First, click the endpoint under 'Device Name'. The query will be automatically entered in the 'Search Box' and EDR will provide all results for the endpoint.
- Click 'Run Untrusted Executable' under 'Adaptive Event Name'. The query will be automatically updated in the 'Search Box' and the results for the untrusted executable events on the endpoint will be displayed:



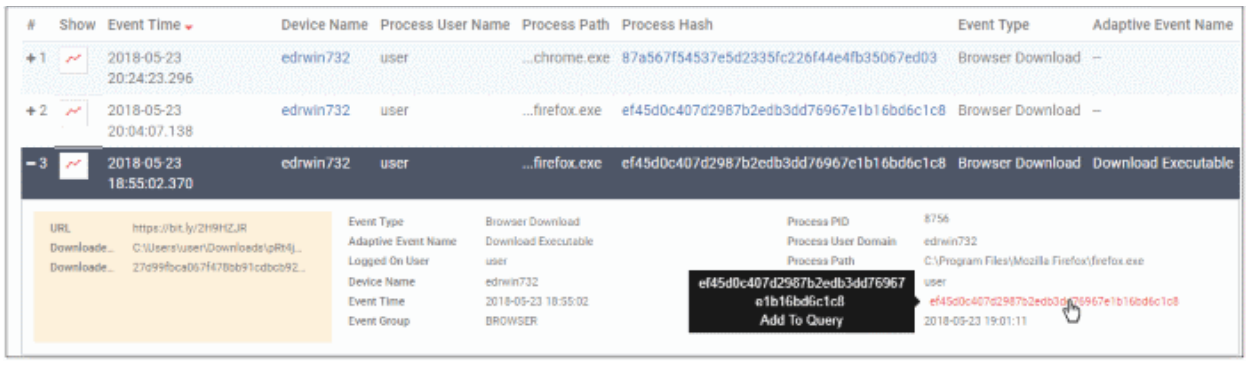
Event List section

The details shown in the summary results depend on the **selected event fields**. You can, of course, also choose fields from the 'Event List' section.

- Click the number beside a event list row from which you want to build a custom query



- Click the event field(s) details that you want to use to build a custom query.



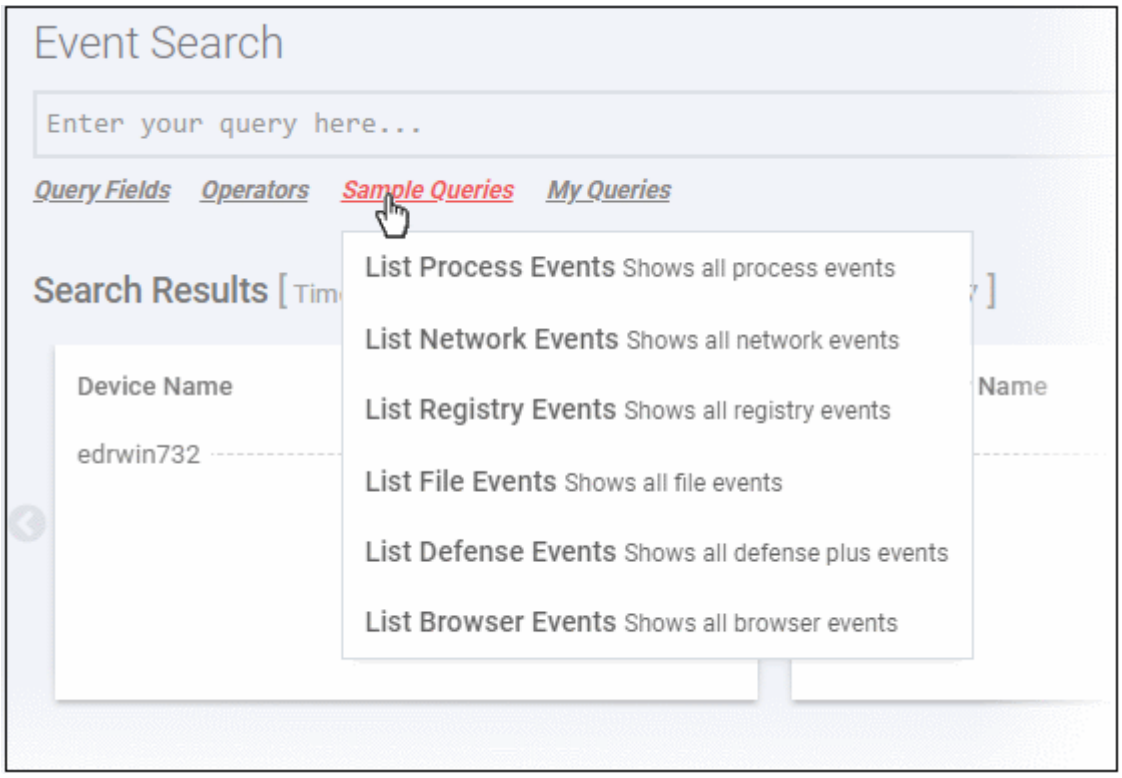
The query fields will be automatically updated in the 'Search Box'.

- Select the time-period and click 'Search'

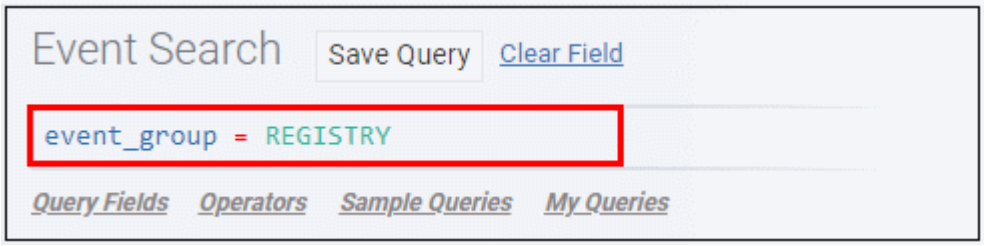
Events matching the custom query will be displayed. See '**View Query Results**' for more information.

Run Sample Queries

EDR ships with built-in sample queries that are often used for data analysis by administrators. This also serves as examples for administrators to create more complex queries.



The sample query will be automatically updated in the 'Search Box'.



- Select the time-period and click 'Search'

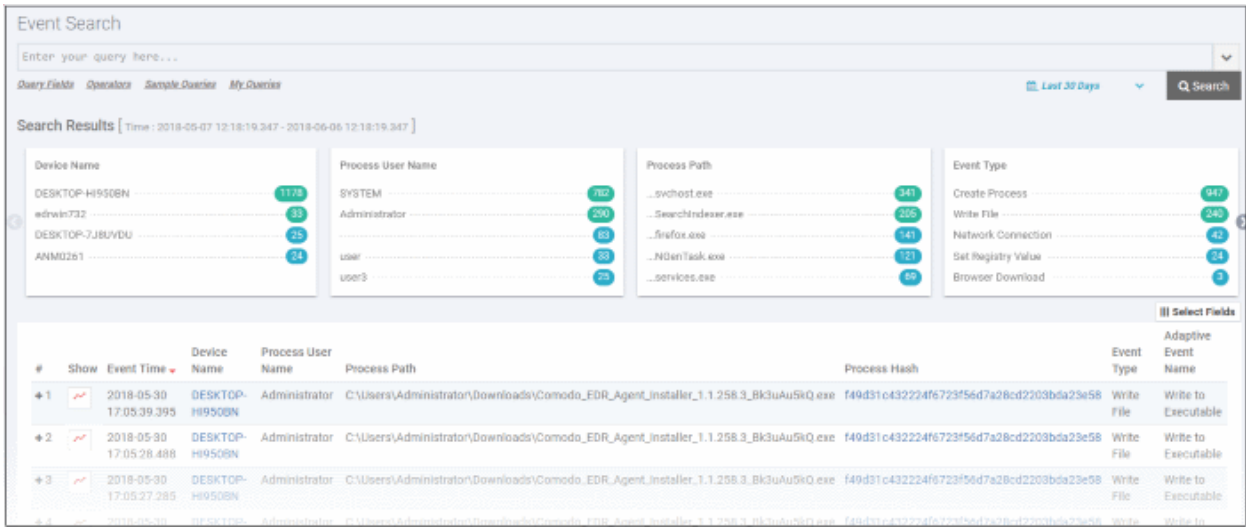
Events matching the sample query will be displayed. See '**View Query Results**' for more information.

View Query Results

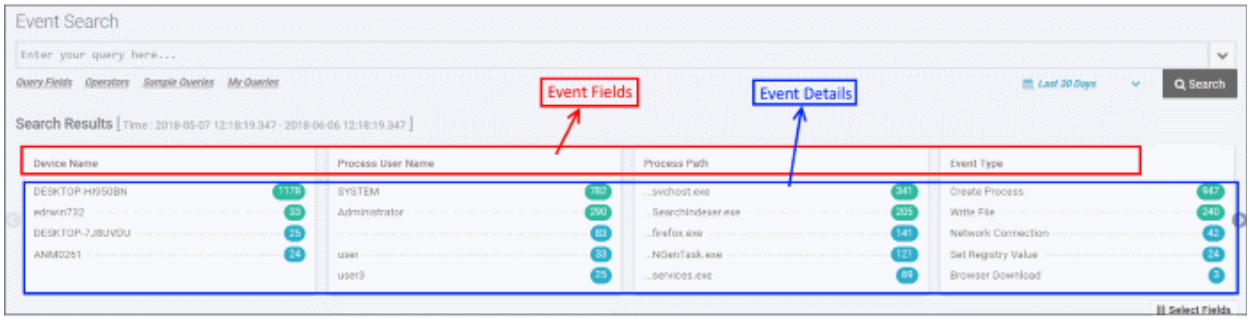
EDR stores the generated events on the cloud and these can be fetched anytime from anywhere using an internet browser. Administrators can use these events for data analysis and take remedial actions on endpoints.

The query results will be displayed depending on the type of query search. See '**Configure results table column headers for a query**', '**Run a general event search**', '**Configure and run a custom query search**' and '**Use sample queries**' for more details.

A summary of the search results is shown on separate tiles at the top. Results for each event are displayed below.



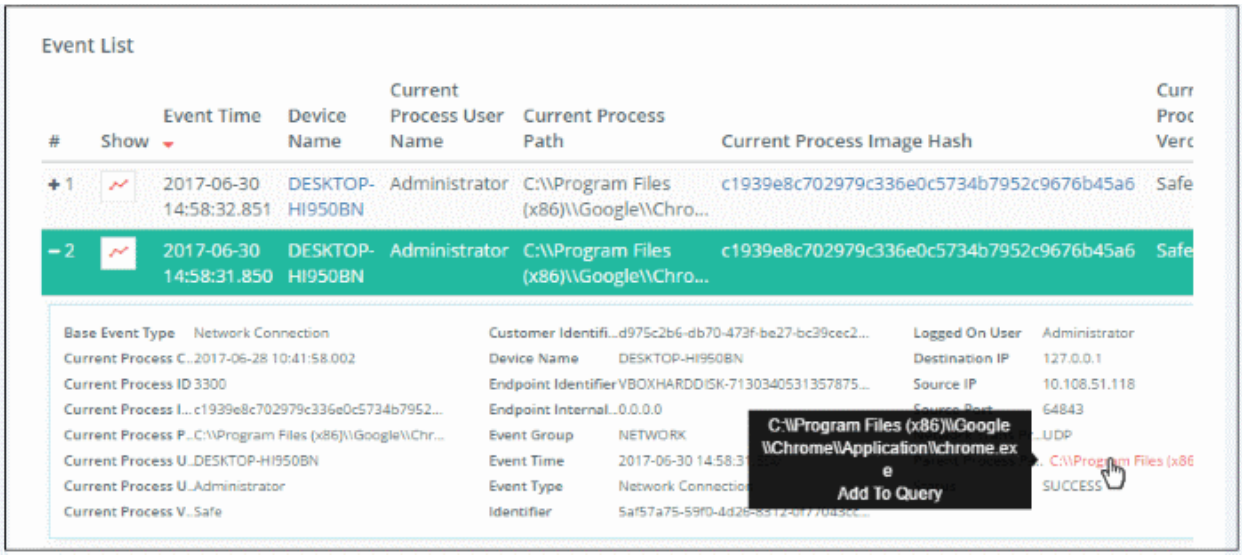
Summary Search Results



- The number beside each event detail indicates the total number of events recorded for that item.
- Clicking an event detail under an event field will display only the results pertaining to those items. This is similar to creating a **custom query**.

Event List

The lower section below the tiles displays the results for each event.



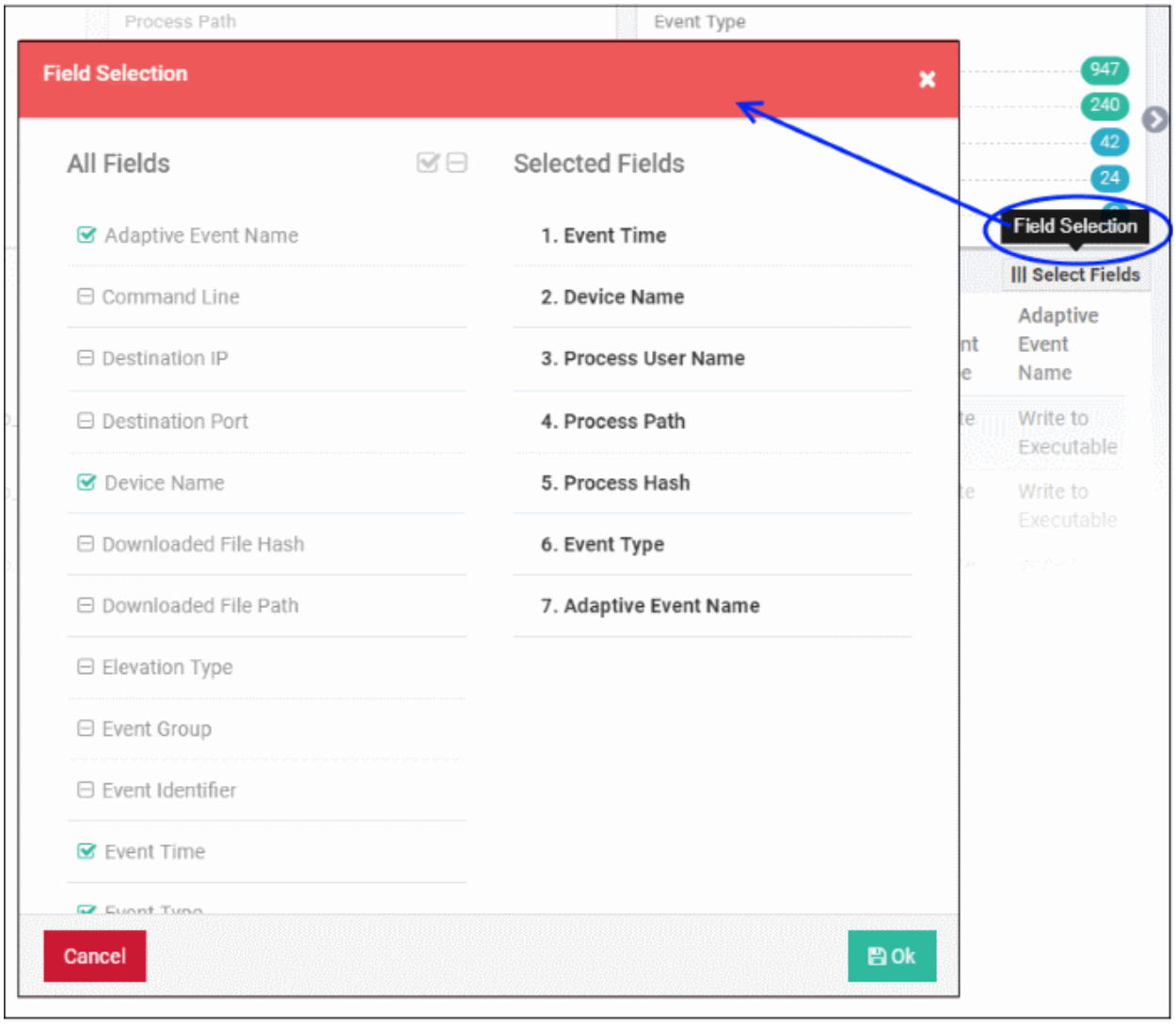
- Clicking an event row will display all the event fields for that event type. The number of event fields displayed depends on the event type.

- Clicking an event detail beside an event field will display only the results pertaining to those items. This is similar to creating a **custom query**.
- Clicking the icon in the 'Show' column for an event will display its timeline. See '**Process Timeline**' for more details.

Configure results table column headers for a query

You can configure the results table to show columns which are important to your custom query. You can also view all the event fields pertaining to your search by clicking the '+' sign beside a query result.

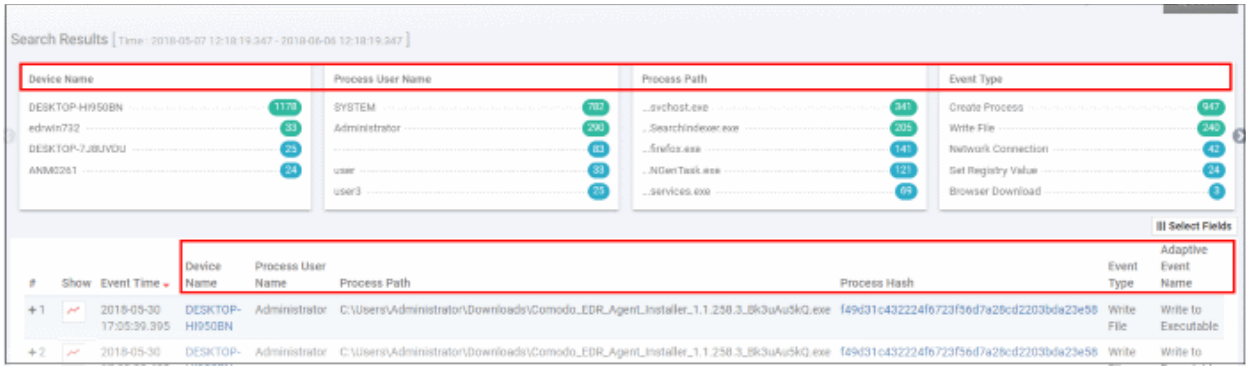
- Click 'Select Fields' on the right to configure the result table columns:



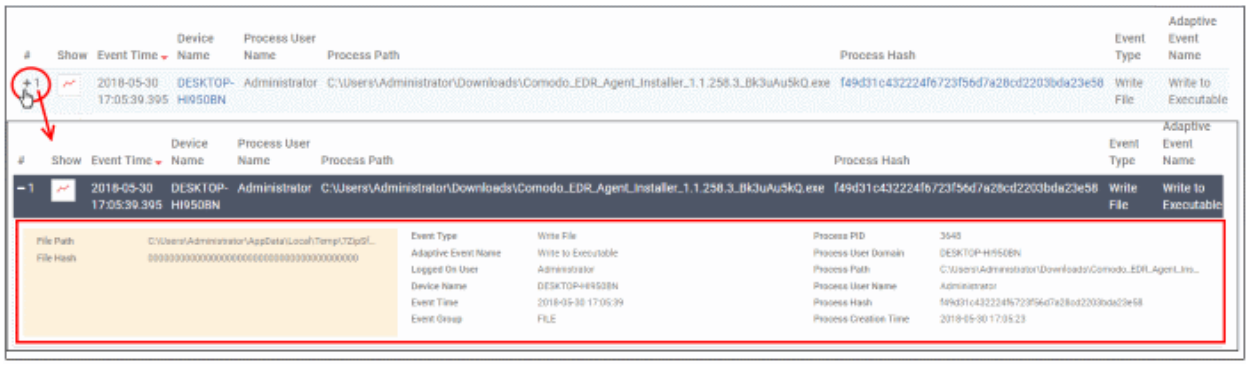
A check-mark is shown next to currently enabled fields. A 'field' in this sense is a column in the results table.

- Click the checkbox beside an individual field to enable or disable it.
- To display all fields, click at the top
- To hide all fields, click at the top.
- All enabled fields are shown on the right, with field # 1 being the first column on the left. Click and drag a particular field to re-position it in the table.
- Click 'Ok' when done.

Your selected fields will be shown as columns in the query search results. The same fields will also be shown for the results summary tiles above the 'Event List' results table. The results summary will not display the 'Event Time' field since this available beside 'Search Results' by default.



Tip. You can still view all event fields for a result by clicking the number beside a event result row:

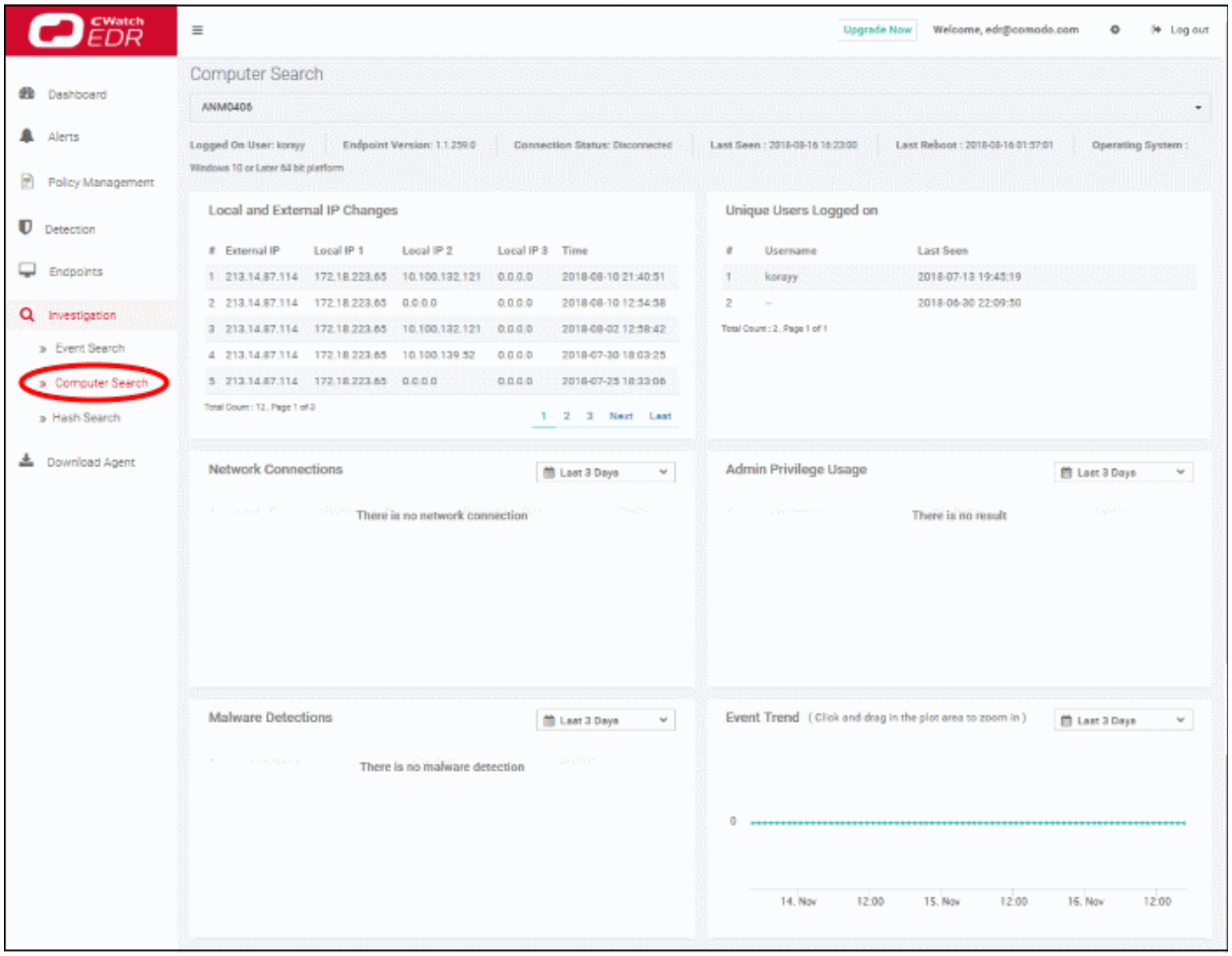


The number of event fields displayed in the detailed results depends on the event type.

10.2 Computer Search

The 'Computer Search' screen shows events recorded on all endpoints added to EDR. Details include event trends, network connection events, malware detection events and so on.

- Click 'Investigation' on the left then 'Computer Search' to open the interface



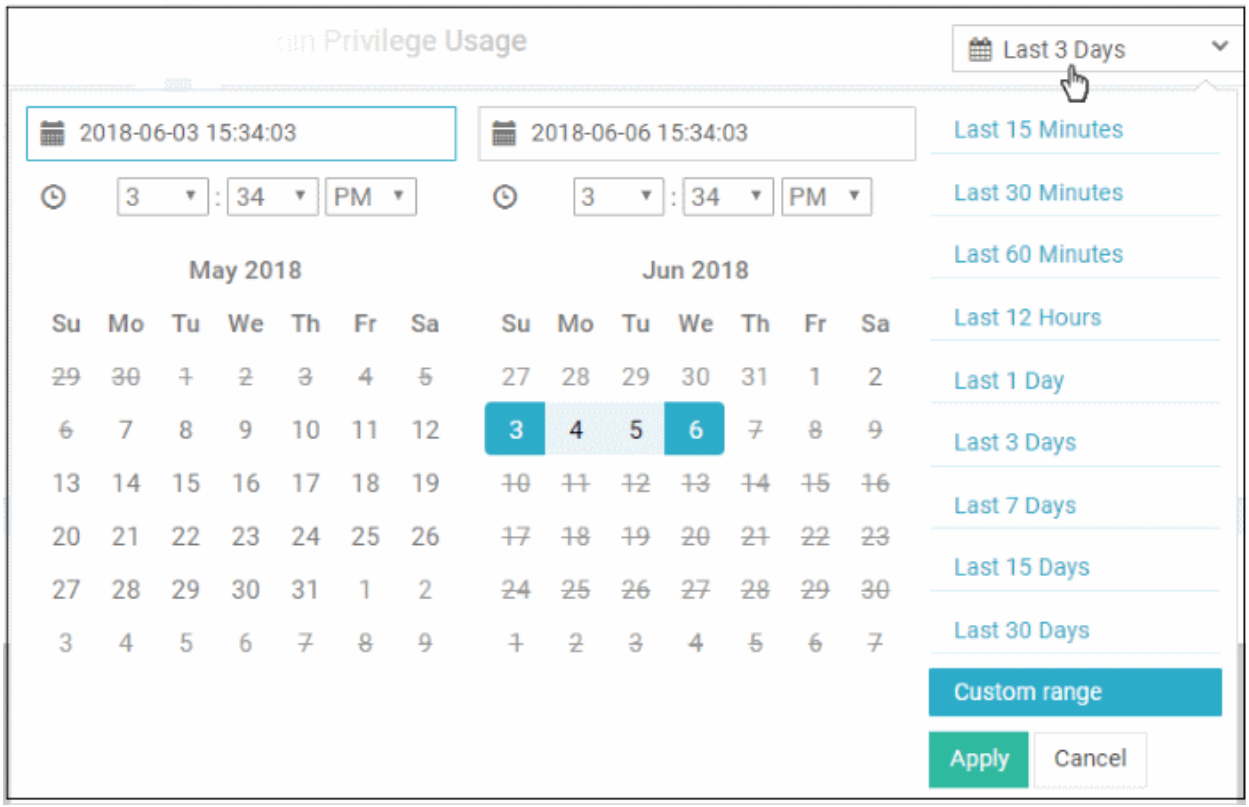
- By default, the screen will be blank with search time range pre-selected for the last 3 days.
- Please note the search field will be auto-populated and results displayed for the endpoint that is clicked from the dashboard.

Search and Sorting options

- **Search option** - The 'Search' box above the table allows you to filter the list.
  - Click anywhere on the row and select from the device list

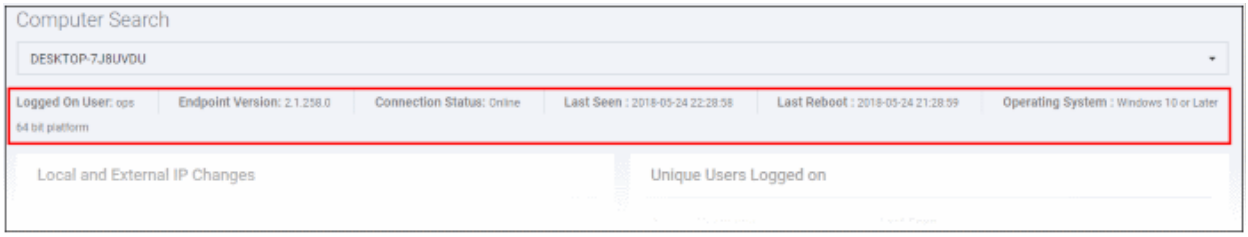
  OR
  - Click anywhere on the row and enter full or partial endpoint name in the search box and select from the suggestion

Use the time-range drop-down to show event information for a specific date or date range (applies to Network Connections, Admin Privilege Usage, Malware Detections and Event Trend tiles).



- Click 'Custom range' to choose specific dates.
- Click 'Apply'. The results for the selected period will be displayed.

Information about the selected endpoint is shown below the search box:



- Logged On User - Endpoint username at the time of event logging
- Endpoint Version - Software version of the EDR agent
- Connection Status - Indicates whether the endpoint is connected to EDR. The statuses are:
  - Online - Indicates the endpoint is normally sending message to the EDR server
  - Offline - Indicates that the agent sent last message to the server along with the information that it would of offline
  - Disconnected - Indicates the agent was not able to send the message that it would go offline.
- Last Seen - Indicates the latest date and time the EDR agent on the endpoint updated EDR
- Last Reboot - Date and time the endpoint was rebooted last
- Operating System - The details of endpoint's OS.

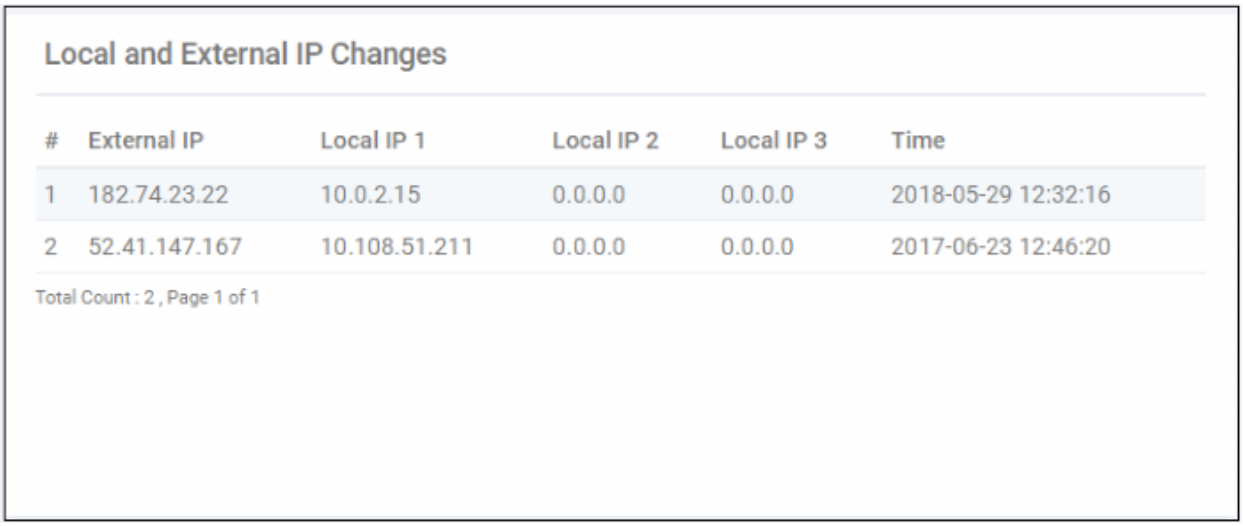
The six tiles below the endpoint info provide the details of events recorded for the selected endpoint.

- **Local and External IP Changes**
- **Event Trend**
- **Unique Users Logged on**
- **Admin Privilege Usage**

- **Network Connections**
- **Malware Detections**

Local and External IP Changes

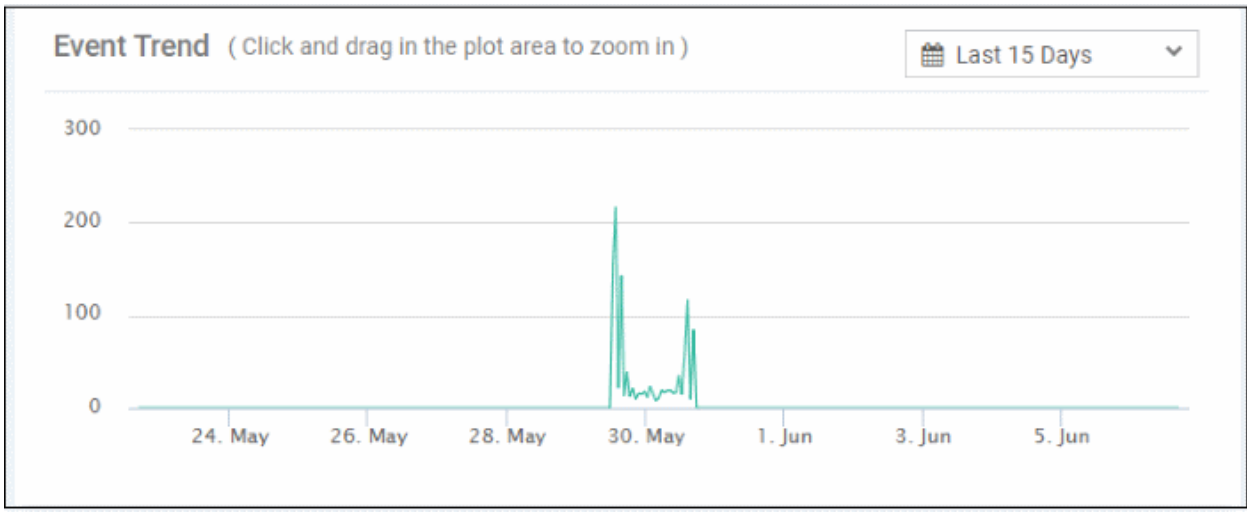
This tile lists any changes in the endpoint's local IP and external IP.



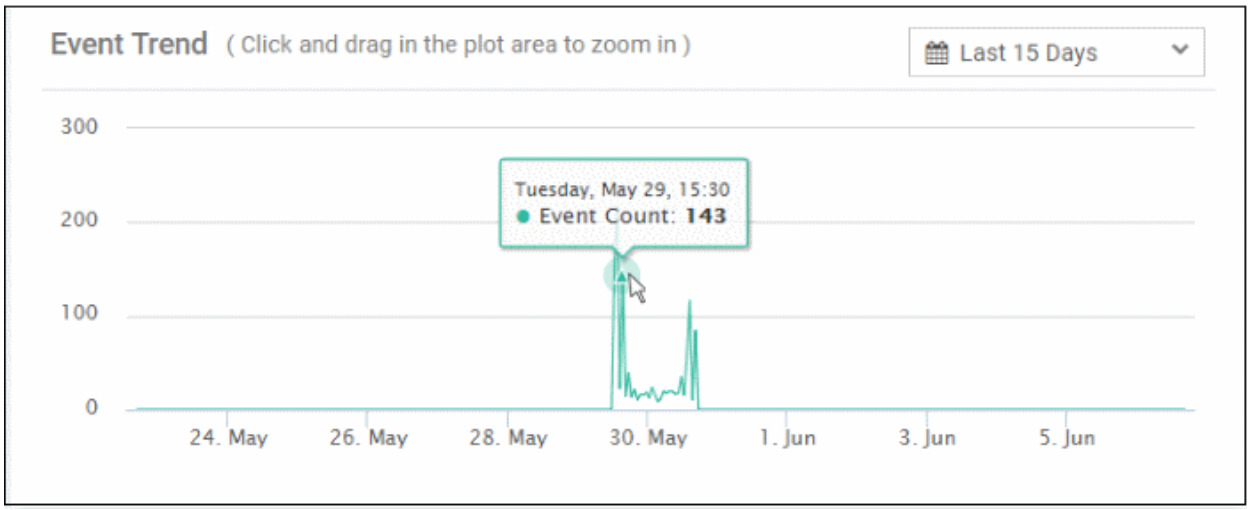
- External IP - The current external IP through which the endpoint connects to other external networks.
- Local IP 1 - The current local IP of the endpoint.
- Local IP 2 and 3 - Details of the previous local IPs (for example, the endpoint is moved from one network to another and allotted different IPs)
- Time - The date and time of last recorded change.

Event Trend

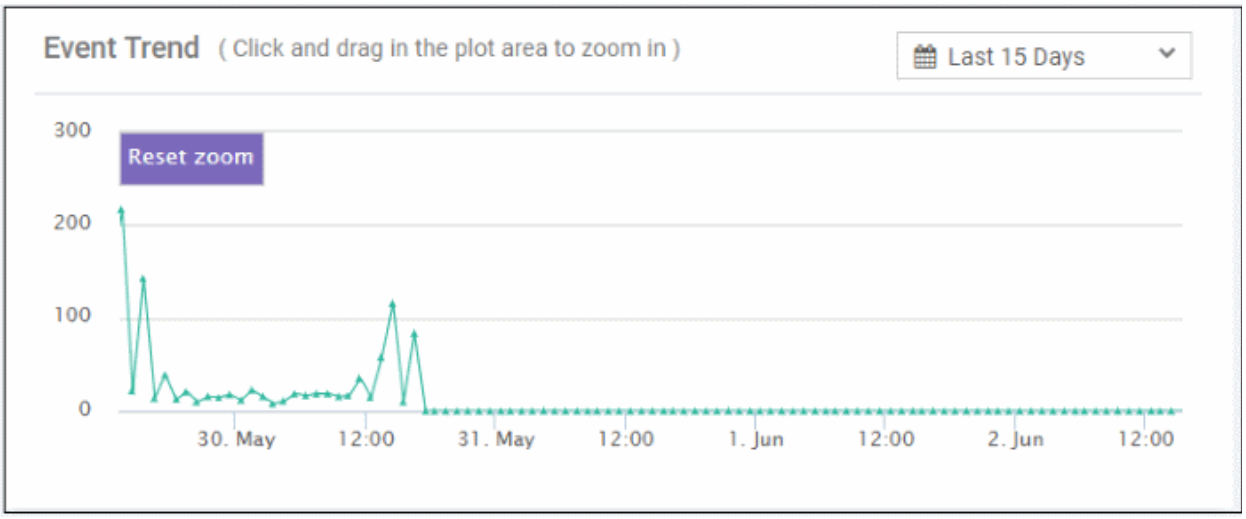
This tile displays the number of events that were recorded from the endpoint for the selected time-period.



- Select the time-period for which the event trend should be shown. The period ranges from last 15 minutes to 30 days.
- The X-axis displays the selected date range and Y-axis provides the number of events.
- Placing the mouse cursor on a particular point on the graph displays the number of events.



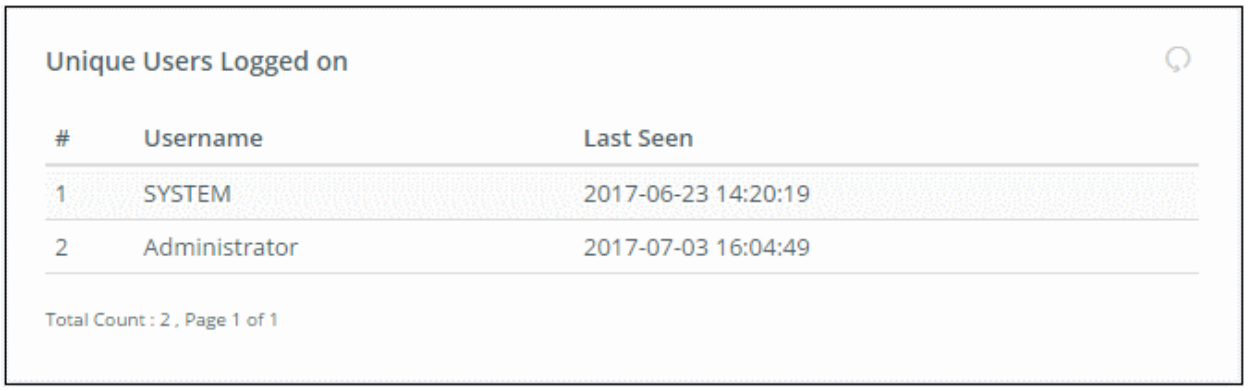
- To view the number of events for a particular of time, click on the graph and drag to zoom. You can view the number of recorded events by hourly basis. Zoom in again if required.



- Place your mouse cursor on a point in the line to see events for a specific day.
- Click 'Reset Zoom' to view the original graph.

Unique Users Logged on

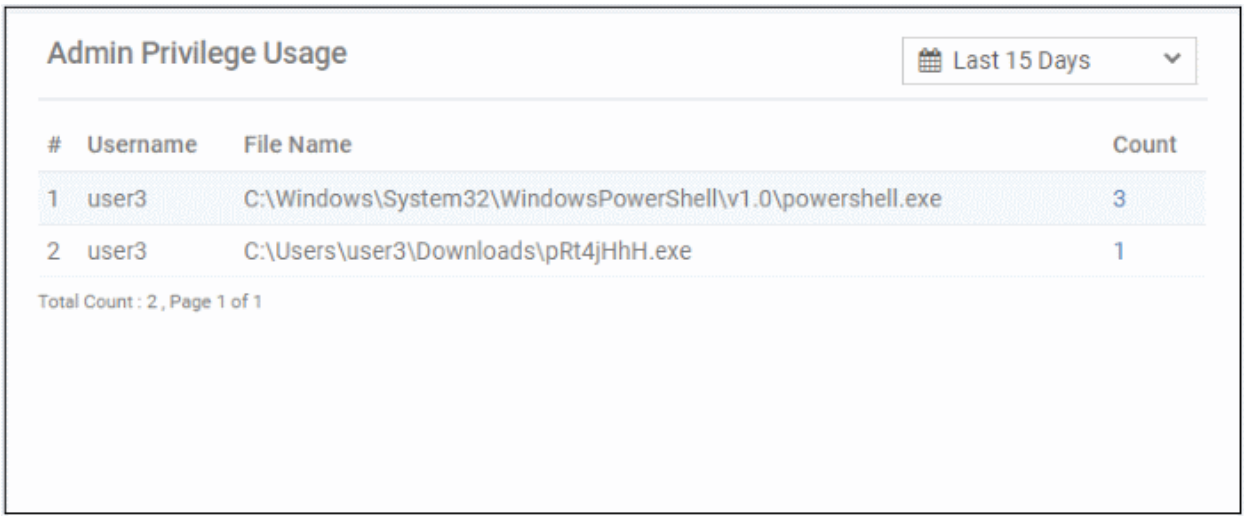
Displays the most recent login times of every user that has logged onto the endpoint.



- Username - The name of the user that is currently logged in and last communicated time to EDR. SYSTEM indicates the date and time the endpoint was first connected to EDR.
- Last Seen - Date and time the endpoint communicated to EDR.

Admin Privilege Usage

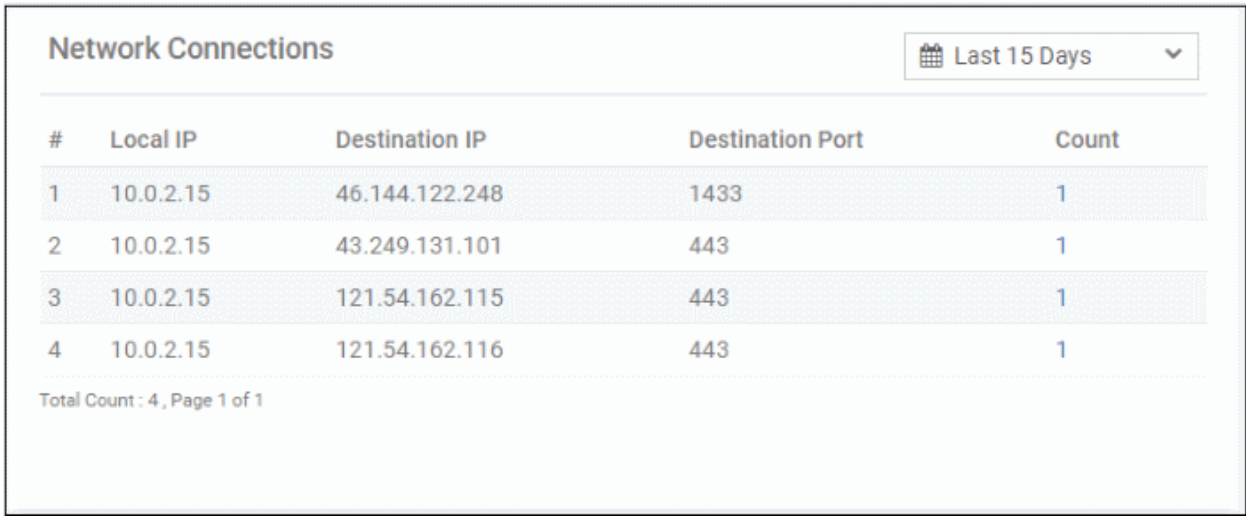
Displays details of events that required admin privileges.



- Select the time-period for which the data should be shown. The period ranges from last 15 minutes to 30 days. You can configure custom range also.
- Username - The name of the user that used the admin level privileges on the endpoint.
- File Name - The name of the application that was used.
- Count - The number of times the event was recorded. Clicking the number will display the event details in the '**Event Search**' interface.

Network Connections

Displays the details of network connection events for the selected time-period.



- Select the time-period for which the data should be shown. The period ranges from last 15 minutes to 30 days. You can configure custom range also.
- Local IP - The internal IP address of the endpoint.
- Destination IP - The destination IP details to which the connection was established.
- Destination Port - The destination port to which the connection was established.
- Count - The number of time the connection to the destination IP and port was established from the endpoint. Clicking the number will provide the event details in the '**Event Search**' interface.
- View more records by clicking 'Next', 'Last', 'First', 'Previous' or any number.

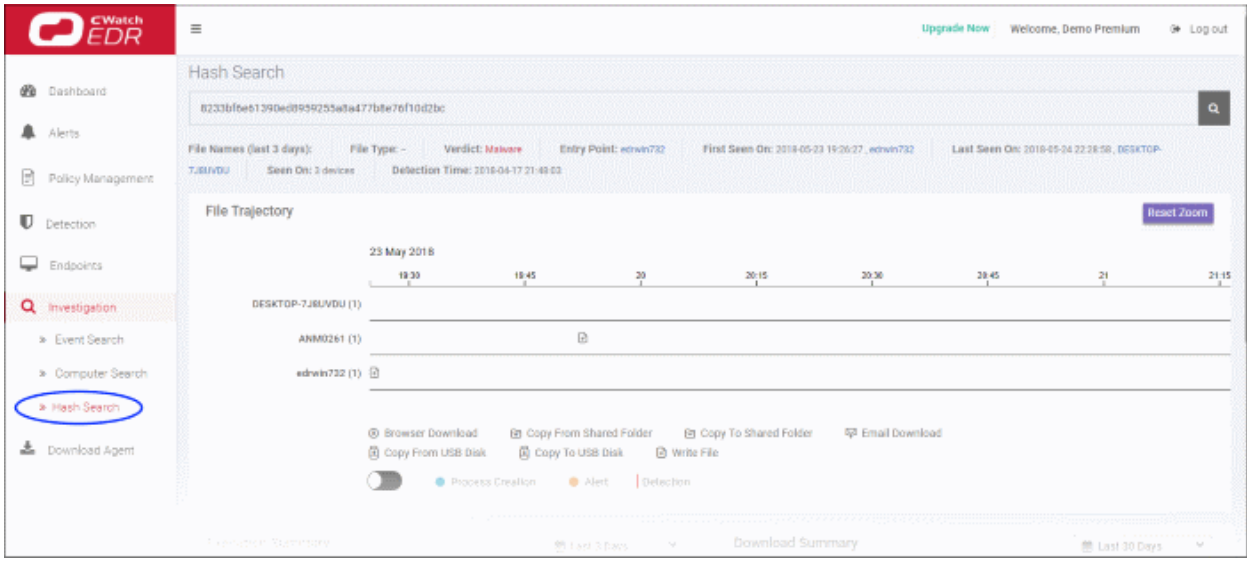
Malware Detections

Displays the malware detected events on the endpoint for the selected period.

- Select the time-period for which the data should be shown. The period ranges from last 15 minutes to 30 days. You can configure custom range also.
- File Name - The name of the file that was detected as malware by EDR.
- File Path - The location of the malware file.
- Sha256 - The hash signature of the malware file. Clicking a hash signature will provide the full details in the '**Hash Search**' interface.
- View more records by clicking 'Next', 'Last', 'First', 'Previous' or any number.

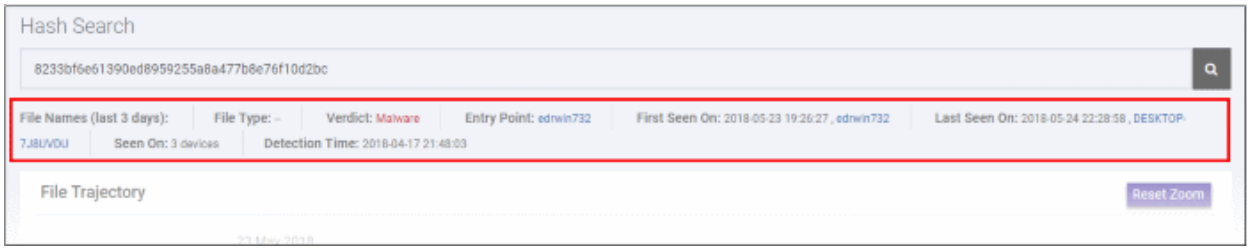
10.3 Hash Search

- A hash search allows you to locate files by their MD5 or SHA-1 hash value. Visibility, execution trend, file history and execution summary are listed for each file.
- Unlike the 'Event' and 'Computer' interfaces, you cannot simply search for a hash. You must either (i) copy and paste a hash value from the dashboard, detection or event search interfaces (ii) click a hash-value link in various screens such as the dashboard or 'Computer Search' screens. The latter will auto-populate the search interface.
- Click 'Investigation' on the left then 'Hash Search' to open the interface.



- By default, the screen will be blank
- Enter the hash value of the file you wish to analyze. Hash values of malware and safe files can be copied from various interfaces such as:
  - 'Dashboard' > 'Malware & Suspicious Activity' tile > under 'Most Found Malware' and 'Last Found Malware'
  - 'Detection' > in the 'Sha1' column
  - 'Investigation' > 'Event Search' > in the 'Process Hash' column
- Click a hash value on any of the screens above to automatically populate the search box here.
- Use the time-range drop-down to show event information for a specific date or date-range (applies to 'Execution Summary', 'Download Summary', 'Creation Summary' and 'Execution Trend' tiles)

Results are shown below the search box:



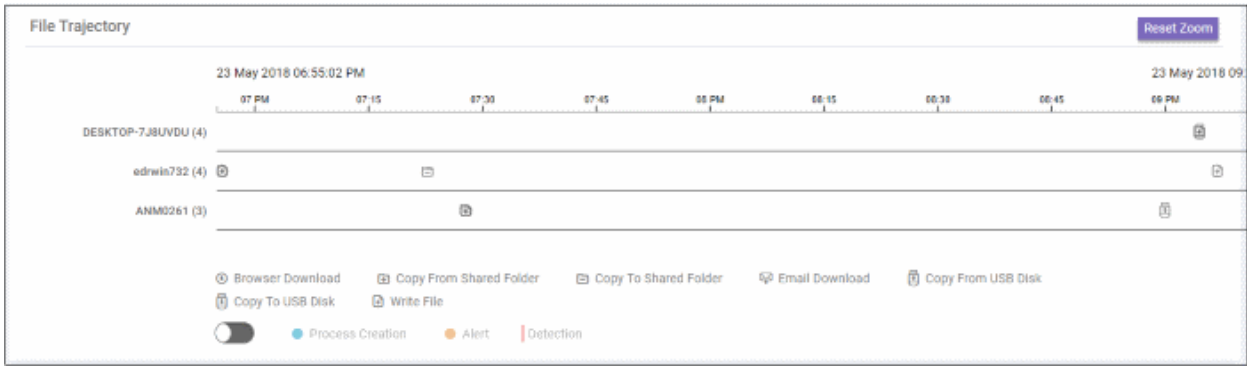
- File Name - Hash value's file name
- File Type - The nature of file. For example, an executable.
- Verdict - Displays the file's trust rating after EDR analysis.
- Entry Point - The name of the device on which the file was first detected. Click the device name to open the '**Computer Search**' screen with the device name auto-populated in the search box.
- First Seen On - The date and time of the event was first logged and the name of the device on which it was detected. Click the device name to open the '**Computer Search**' screen with the device name auto-populated in the search box.
- Last Seen On - The date and time of the last event logged for the same file and the name of the device on which it was detected. Click the device name to open the '**Computer Search**' screen with the device name auto-populated in the search box.
- Seen On - The number of devices on which the file was found.
- Detection Time - The date and time the trust verdict was awarded to the file. This may be some time in the past if Valkyrie has already encountered the file and has a database entry for it.

The results screen provides the following details about the file:

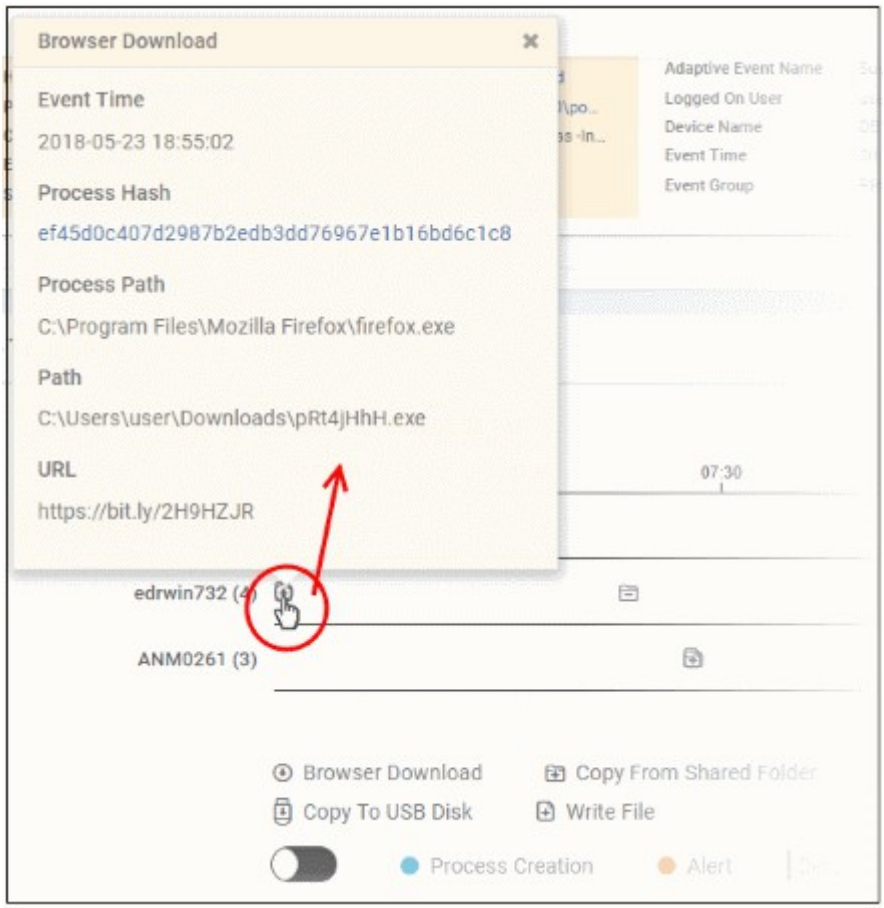
- File Trajectory
- Execution Summary
- Download Summary
- Creation Summary
- Execution Trend

File Trajectory

The first tile below the hash file info screen displays the movement of the file, that is from where it was downloaded, copied to which endpoint and so on.

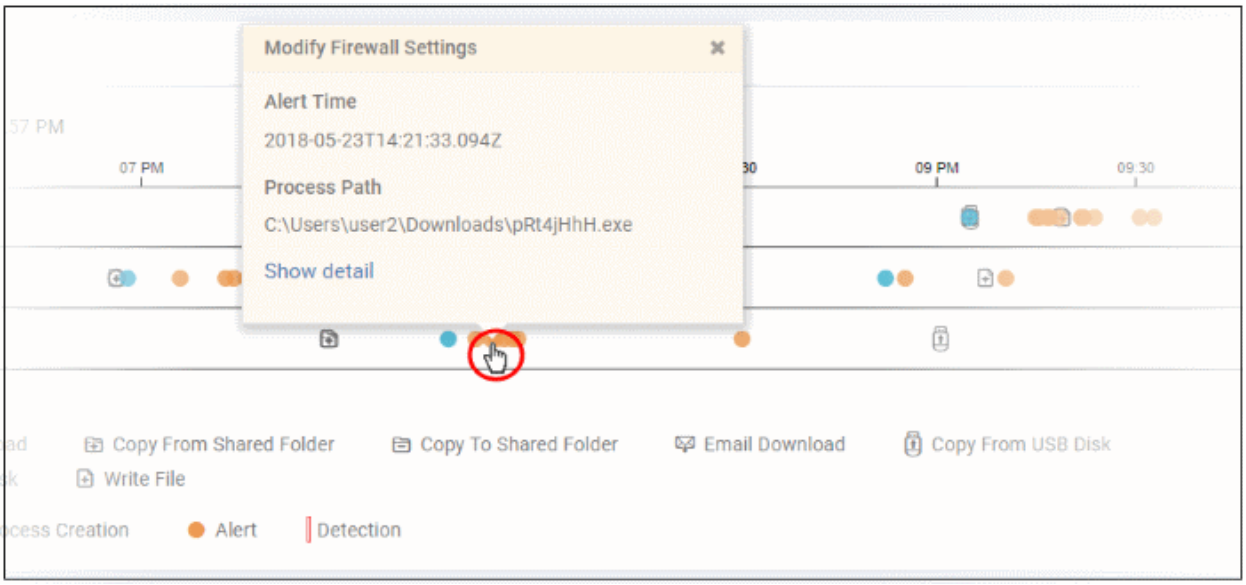


- Zoom in or out using your mouse. Right-click and move the chart left or right. Click 'Reset Zoom' to return to default view.
- Details of the icons is shown below the graph.
- Click an icon to view the trajectory details.



- Click 'X' to close the dialog.
- Click 'Process Creation' button to view time of process creation, event detected and alert generated.

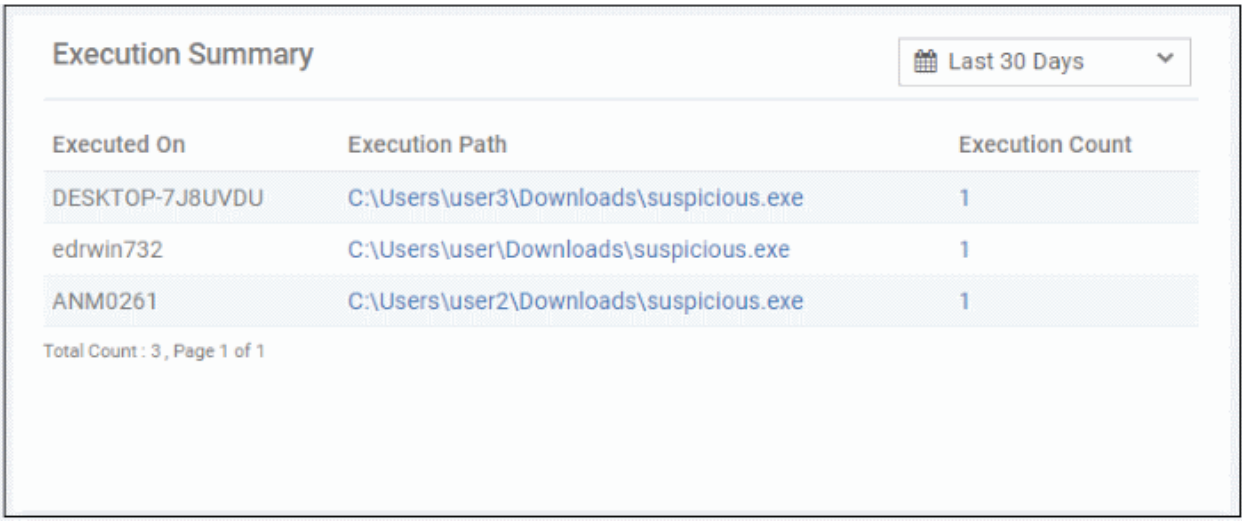
- Click an icon color code to view trajectory details.



- 'Show detail' link will be available for Alert dialog. Clicking the link will open the event details screen for which the alert was generated.
- Click 'X' to close the dialog.

Execution Summary

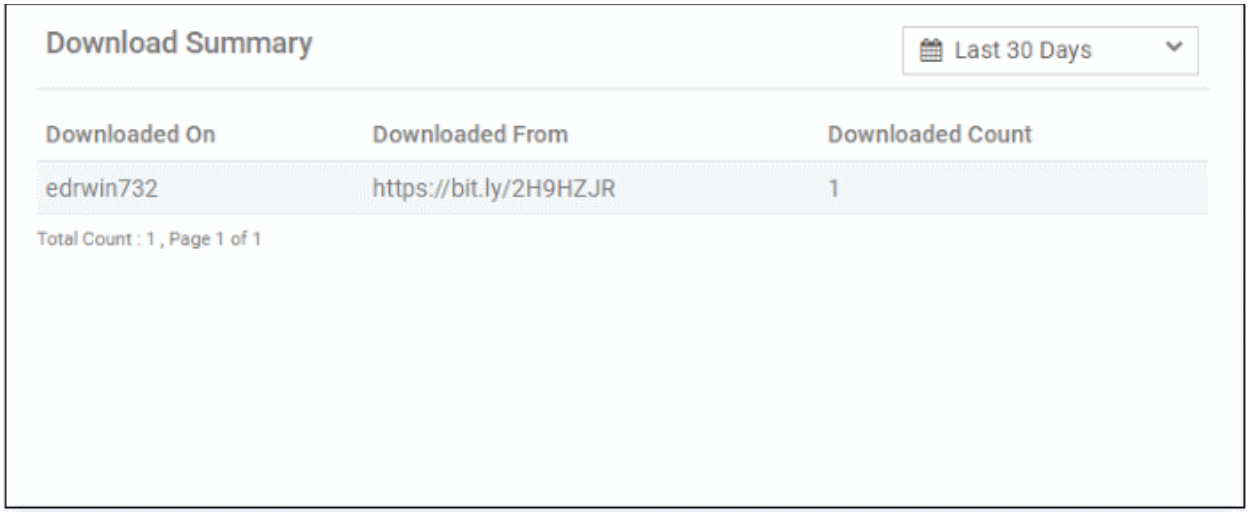
A summary of the devices on which the file was executed. Details include the file path and the number of times it was executed.



- Select the time-period for which the event trend should be shown. The period ranges from last 15 minutes to 30 days.
- View more records by clicking 'Next', 'Last', 'First', 'Previous' or any number.
- Executed On - The device on which the file was run.
- Execution Path - The location of the file on the device. Clicking the path link will open the '**Event Search**' screen with the query pre-populated.
- Execution Count - The number of times the event has occurred.

Download Summary

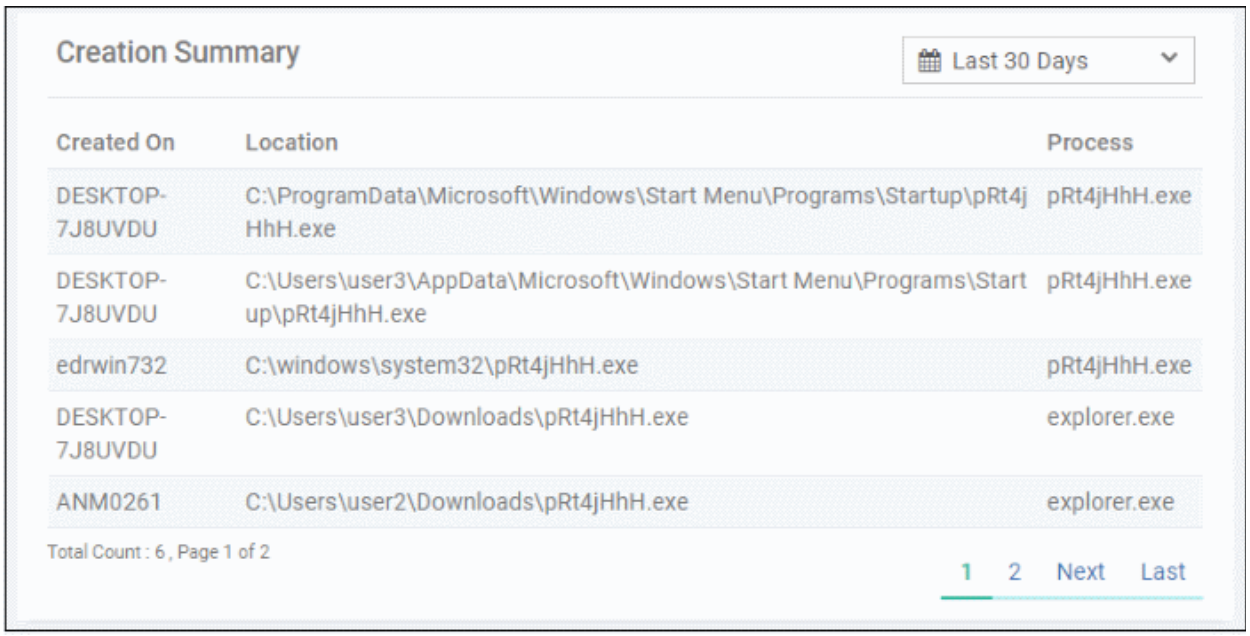
Shows the details on which endpoint the file was downloaded (aka 'Entry Point'), the URL from where it was downloaded and the number of times it was downloaded.



- Select the time-period for which the download summary should be shown. The period ranges from last 15 minutes to 30 days.
- View more records by clicking 'Next', 'Last', 'First', 'Previous' or any number.
- Downloaded On - The device on which the file was first downloaded
- Downloaded From - The location from which the file was downloaded
- Downloaded Count - The number of times the file was downloaded

Creation Summary

Details of endpoints on which the file has created processes and the location of file from where it was run.

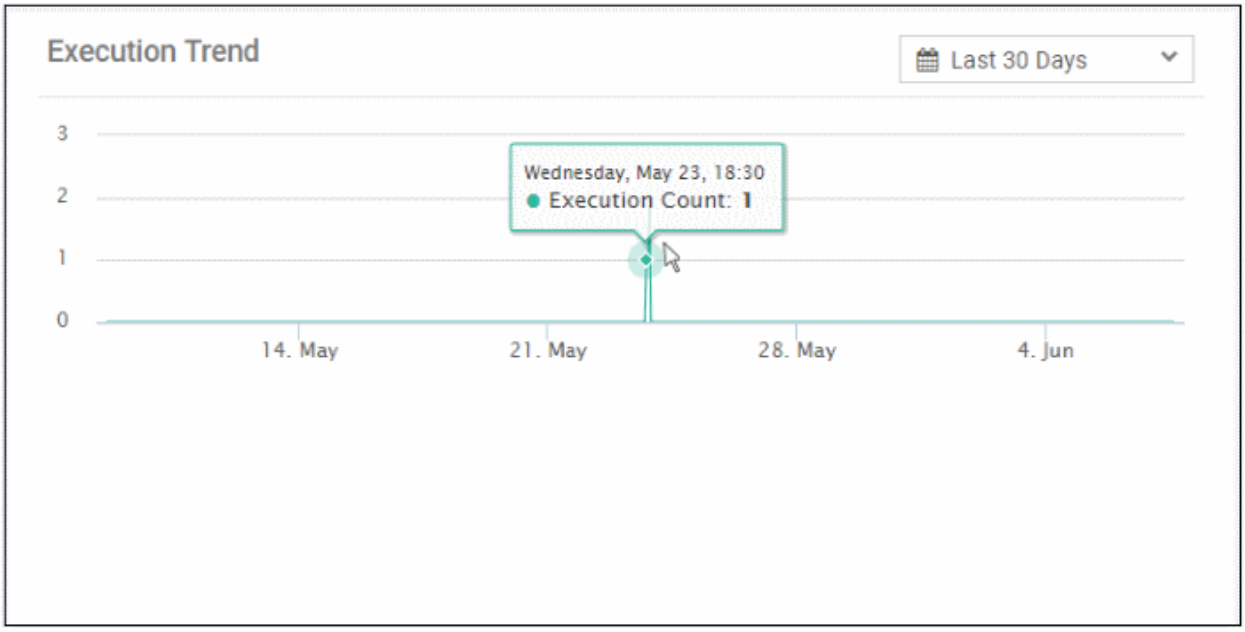


- Select the time-period for which the creation summary should be shown. The period ranges from last 15 minutes to 30 days.
- View more records by clicking 'Next', 'Last', 'First', 'Previous' or any number.
- Created On - The device on which the file was run
- Location - The path of the file from where it was run
- Process - The name of the application that was run

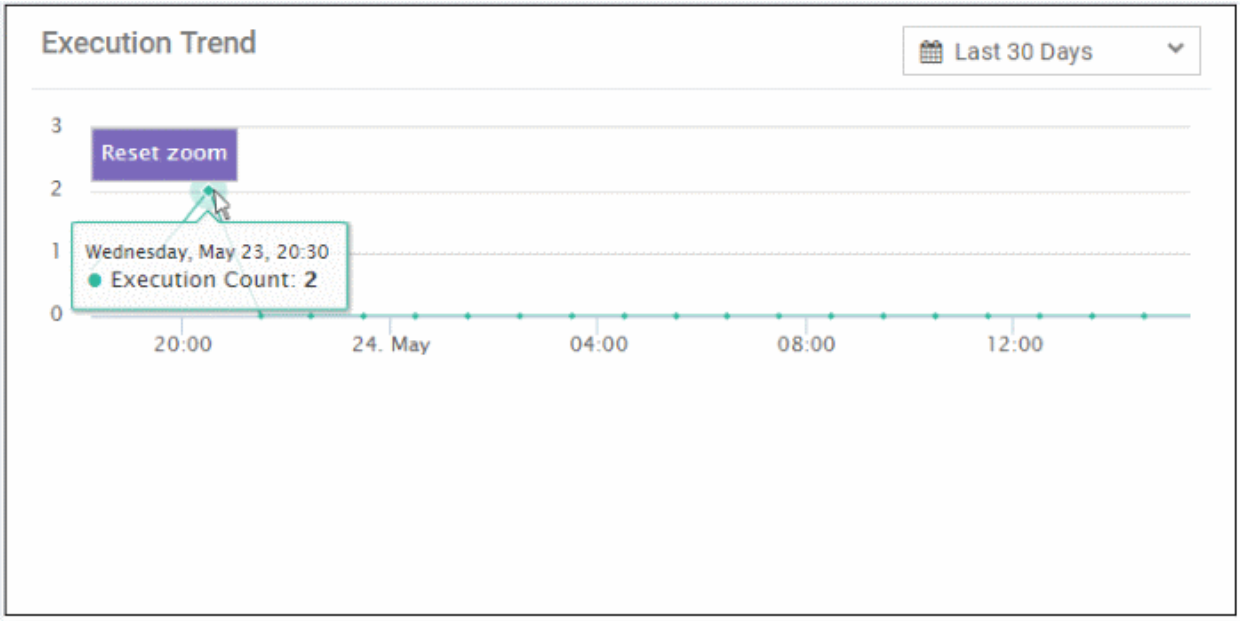
Execution Trend

The number of times the file ran during the selected time-period.

- Select the time-period for which the creation summary should be shown. The period ranges from last 15 minutes to 30 days.
- X-axis displays the selected date range and Y-axis provides the number of file execution counts.
- Place you mouse cursor on a particular point on the graph to see the number of executions.



- You can zoom in by dragging any point on the graph. This lets you, for example, more clearly see the hours of the day when the file ran.



- Place your mouse cursor on a point in the line to see the number of counts.
- Click 'Reset Zoom' to view the original graph.

10.4 Process Timeline

The 'Process Timeline' shows all processes spawned by an event.

You can view the timeline in two ways:

Event Search

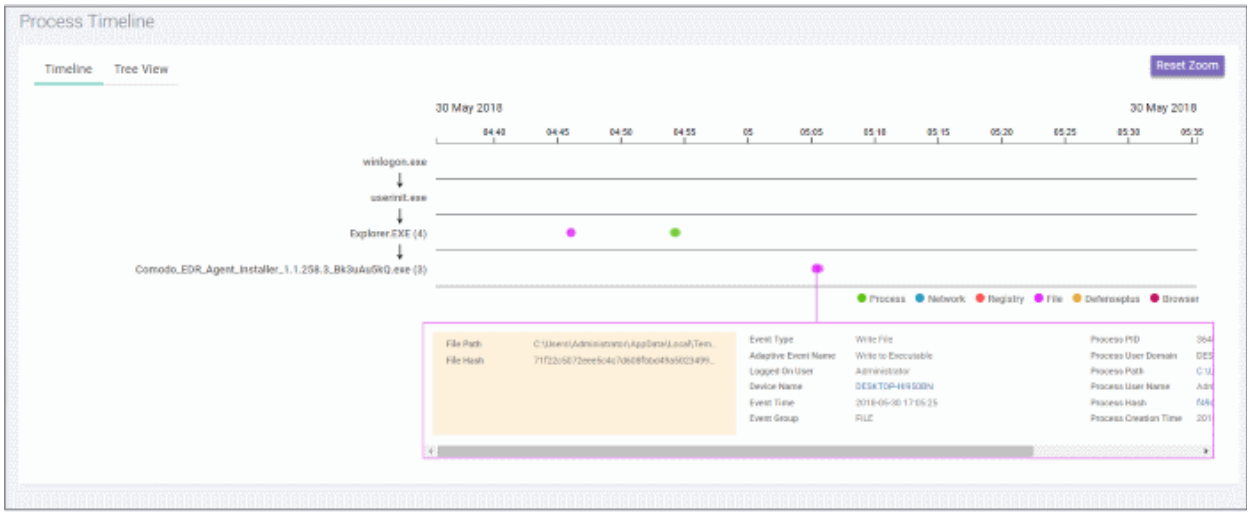
- Auto-populate the event ID from the '**Event Search**' results interface. Go to 'Investigation' > 'Event Search', select the time-period and click 'Search'. Under the 'Event List' section, click the process timeline icon beside an event in the 'Show column.

- Alternatively, you can provide the event ID manually in the field to view its timeline.

Alerts

- Go to 'Alerts' then click 'Show Alerts' in an Alert row. Under 'Events' section, click the process timeline icon beside an event in the 'Show column.

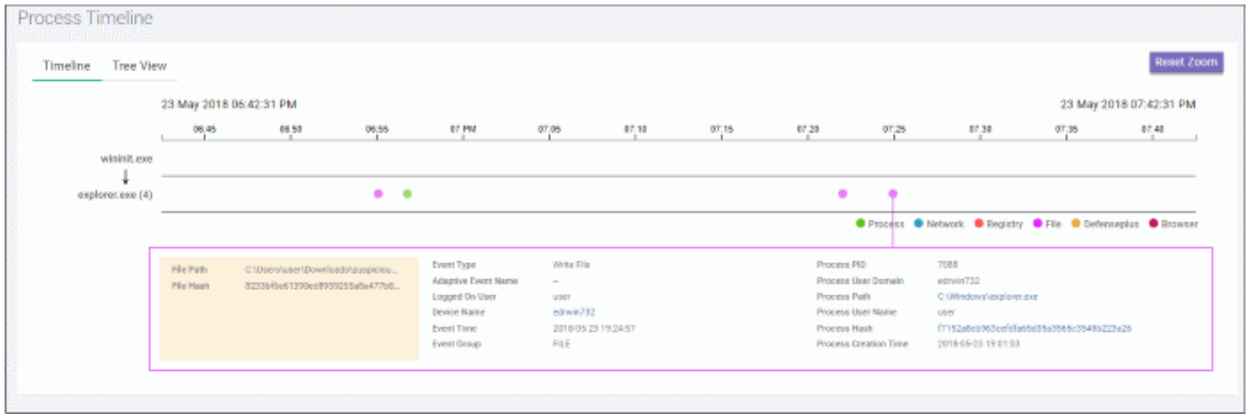
The timeline of the selected event will be displayed.



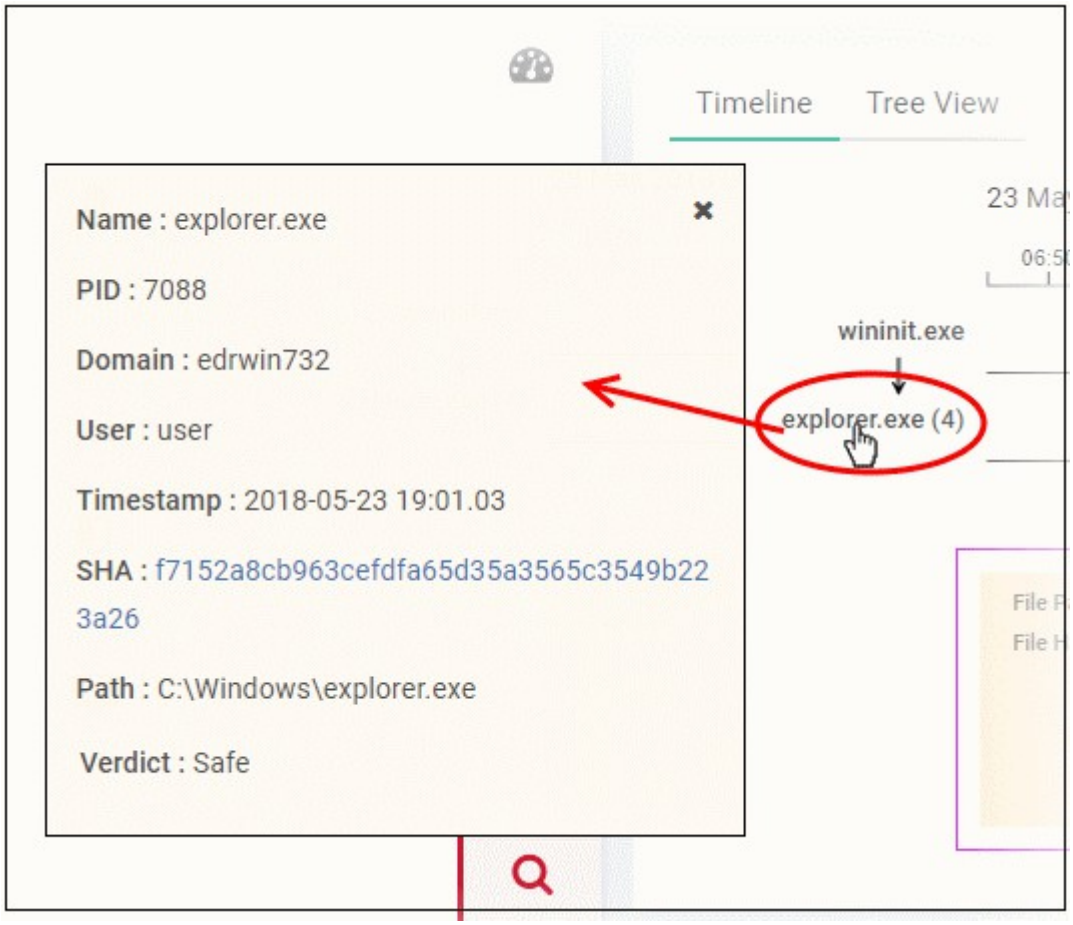
You can view the details in timeline or tree view.

Timeline View

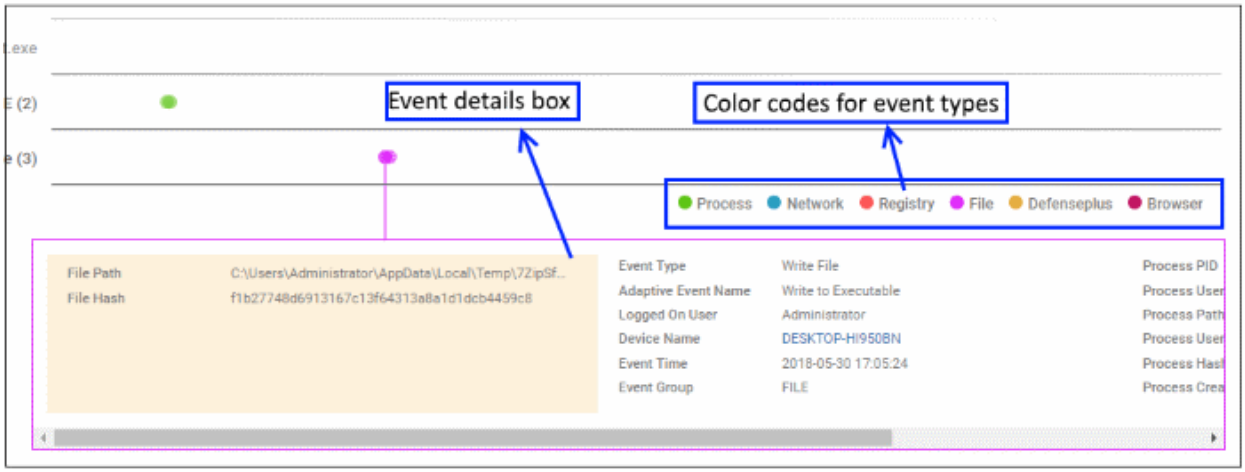
By default, the timeline view of the event will be displayed:



- The search time here indicates the processes that the event generated. The results are displayed for processes generated 30 minutes preceding and after the event. For example, for an event that started at 11.00.00, the results will displayed for processes generated by the event from 10.30.00 to 11.30.00.
- The timeline of the event is shown at the top with date and time preselected.
- The processes path initiated by the event is indicated by the down arrow.
- The number beside a process name indicates the number of events generated by the process.
- Click on a process to view process name, time-stamp, hash, path and verdict.



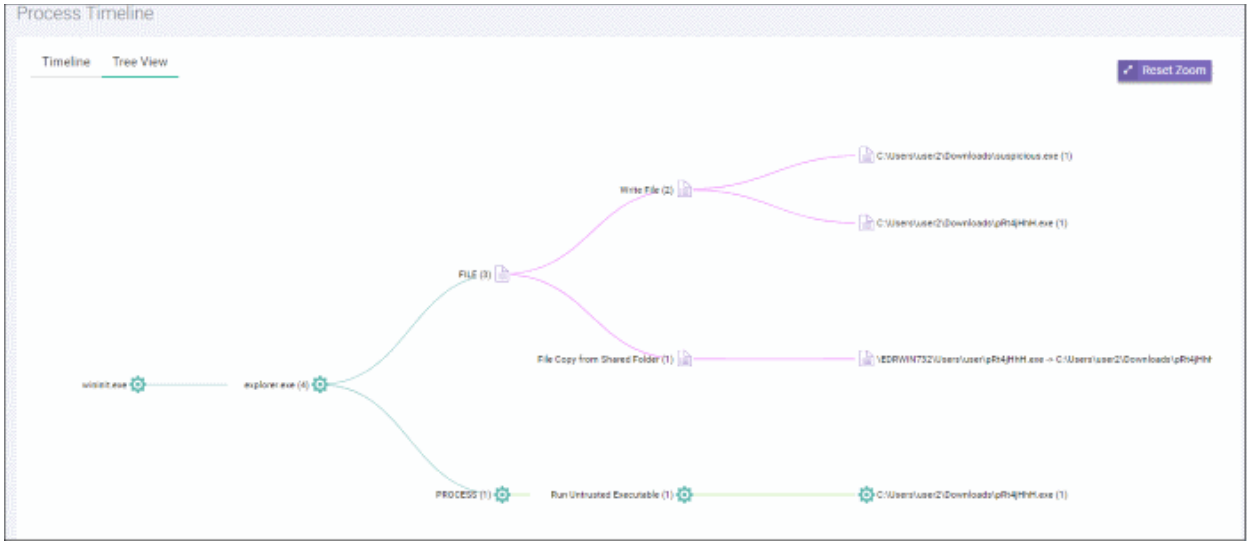
- The event (created by the process) details are shown in the box below the process path.
- The event types are color coded and displayed above the event details box.



- Event details displays all event fields for that event type. The number of event fields displayed depends on the event type.

Tree View

You can view the process hierarchy in tree view. In the 'Process Timeline' screen, click 'Tree View' tab.



- You can view the processes and event types with respective colors.
- Use mouse to zoom in and zoom out. Click 'Reset Zoom' to default view
- The number beside a process name indicates the number of events generated by the process.
- Clicking on a process name will open the '**Event Search**' screen with the event search box populated with the selected process parameters.

Appendix 1 - Default Comodo Security Policy Details

An EDR policy determines which events will generate an alert for you. Comodo EDR ships with a default security policy containing seven event categories. The table below contains details of the default rules in each event category.

The built-in event categories are:

- **Process Events** - Rules to generate alerts if an application causes an event
- **Registry Events** - Rules to alert you about changes to the Windows registry on your endpoints.
- **File Events** - Rules that detect modifications to any system files and folders
- **Download Events** - Rules to create alerts when applications are downloaded via browsers.
- **Upload Events** - Rules to alert you about file uploads to shared folders or external drives.
- **Defense+ Events** - No default rules are set for this event category.
- **Network Events** - No default rules are set for this event category.

Process Events

Event Category - Process Events		
Event Type - Create Process		
Event Name	**Score**	**Description**
Suspicious System Process Creation	6	Process verdict is not safe AND file path matches %systemroot%*
Remote Powershell Execution	5	File path matches *\wsmprovhost.exe
Suspicious Powershell Flag	5	Command line matches any of the following: *powershell*-NoP* *powershell*-Win* *powershell*-w* *powershell*-Exec* *powershell*-ex* *powershell*-ep* *powershell*-command* *powershell*-NoL* *powershell*-InputFormat* *powershell*-Enc* *powershell*-NonInteractive* *powershell*-nonI* *powershell*-file*
Stop Service	5	Command line matches %systemroot%\system32\net*stop*
Run Untrusted	4	Verdict is not safe

Executable		
Suspicious Process Hierarchy	3	Process path does not match *\explorer.exe AND path matches *\powershell.exe OR patch matches *\cmd.exe
Start Service	2	Command line matches %systemroot%\system32\net*start*

Registry Events

Event Category - Registry Events		
Event Type - Set Registyry Value		
Event Name	**Score**	**Description**
Disable User Account Control	9	Registry key path is equal to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System AND registry value name is equal to EnableLUA0 AND registry value data is equal to 0.
Disable Task Manager	9	Registry key path is equal to HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System AND registry value name is equal to DisableTaskMgr AND registry value data is equal to 1
Installation of Drivers	8	Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services* AND registry value name is equal to Type AND Registry value data is equal to 1 OR registry value data is equal to 2
Add Service to svchost	7	Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services* AND registry value name is equal to ImagePath AND registry value data matches *svchost.exe* OR Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*\Parameters AND registry value name is equal to ServiceDll AND registry matches *.dll
Add Active Setup Value In Registry	7	Registry key path matches HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components*
Modify Powershell Execution Policy	7	Registry key path is equal to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell AND registry value name is equal to ExecutionPolicy
Modify Firewall Settings	6	Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile*
Disable Registry Editing Tool	6	Registry key path is equal to HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System AND registry value name is equal to DisableRegistryTools AND registry value data is equal to 1.

Modify AppInit_DLLs in Registry	6	Registry key path is equal to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows AND registry value name is equal to AppInit_DLLs
Add Service	6	Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services* AND registry value name is equal to ImagePath AND registry value data matches *.exe* AND registry value data doesn't match *svchost.exe*
Layered Service Provider installation	6	Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries*
Add Autorun In Registry	5	Registry key path matches any of the following: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System\Scripts\Startup* HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\Scripts\Logon* HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce* HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows* HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows\Run* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run* HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run* HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\Scripts\Logoff* HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System\Scripts\Shutdown* OR Registry key path equals any of the following: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
Booting Time Execution	5	Registry key path is equal to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager AND registry value name is equal to BootExecute
Disable Auto Update	5	Registry key path is equal to HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU AND registry value name is equal to NoAutoUpdate AND registry value data is equal to 1 OR Registry key path is equal to

		HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate AND registry value name is equal to DisableWindowsUpdateAccess AND registry value data is equal to 1 OR Registry key path is equal to HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WindowsUpdate AND registry value name is equal to DisableWindowsUpdateAccess AND registry value data is equal to 1
Disable Service	5	Registry key path matches HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services* AND registry value name is equal to Start AND registry value data is equal to 4
Create Explorer Entry	5	Registry key path matches any of the following: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PROTOCOLS\Filter* HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PROTOCOLS\Handler* HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Desktop\Components* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components* HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad* HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad* HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks* HKEY_CURRENT_USER\Software\Classes*\ShellEx\ContextMenuHandlers* HKEY_LOCAL_MACHINE\Software\Classes*\ShellEx\ContextMenuHandlers* HKEY_CURRENT_USER\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers* HKEY_LOCAL_MACHINE\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers* HKEY_CURRENT_USER\Software\Classes\Directory\ShellEx\ContextMenuHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\ShellEx\ContextMenuHandlers* HKEY_CURRENT_USER\Software\Classes\Directory\Shellex\DragDropHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\DragDropHandlers* HKEY_CURRENT_USER\Software\Classes\Directory\Shellex\PropertySheetHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\PropertySheetHandlers* HKEY_CURRENT_USER\Software\Classes\Directory\Shellex\CopyHookHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\CopyHookHandlers* HKEY_CURRENT_USER\Software\Classes\Folder\Shellex\ColumnHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Folder\Shellex\ColumnHandlers* HKEY_CURRENT_USER\Software\Classes\Folder\ShellEx\ContextMenuHandlers*

		HKEY_LOCAL_MACHINE\Software\Classes\Folder\ShellEx\ContextMenuHandlers* HKEY_CURRENT_USER\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers* HKEY_LOCAL_MACHINE\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers* HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers* HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers* HKEY_CURRENT_USER\Software\Microsoft\Ctf\LangBarAddin* HKEY_LOCAL_MACHINE\Software\Microsoft\Ctf\LangBarAddin* HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved* HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved* OR Registry key path is equal to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler
Disable Windows Application	5	Registry key path is equal to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun
Disable Command Prompt	5	Registry key path is equal to HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System AND registry value name is equal to DisableCMD AND registry value data is equal to 2
Disable Show Hidden Files	4	Registry key path is equal to HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced AND registry value data is equal to 2 AND Registry value name is equal to Hidden OR registry value name is equal to ShowSuperHidden
Share Folder	4	Registry key path is equal to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\Shares
Addition of DNS Server	3	Registry key path matches HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces* AND registry value name is equal to NameServer
Modify Hosts File Registry	3	Registry key path is equal HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters AND registry value name equal to DataBasePath

File Events

Event Category - File Events		
Event Type - Write File		
Event Name	**Score**	**Description**
Add Scheduled Task	6	File path matches %systemroot%\System32\Tasks* OR %systemroot%\Tasks*
Write Fake System File	6	File path matches *svch0st.exe OR *svhost.exe
Write to System Directory	5	File path matches %systemroot%*
Add Startup File or Folder	5	File path matches any of the following: %appdata%\Microsoft\Windows\Start Menu\Programs\Startup* %programdata%\Microsoft\Windows\Start Menu\Programs\Startup* %systemroot%\system\iosubsys* %systemroot%\system\vmm32* %systemroot%\Tasks* OR File path equals any of the following: %systemdrive%\autoexec.bat %systemdrive%\config.sys %systemroot%\wininit.ini %systemroot%\winstart.bat %systemroot%\win.ini %systemroot%\system.ini %systemroot%\dosstart.bat
Modify Host File	4	File path is equal to %systemroot%\system32\drivers\etc\hosts
Write to Executable	4	File type is equal to PORTABLE_EXECUTABLE AND Process path doesn't match *\explorer.exe
Write to Infectible File	4	Process path doesn't match *\explorer.exe AND File path matches any of the following: *.lnk *.wsf *.hta *.mhtml *.html *.doc *.docm *.xls

		*.xlsm *.ppt *.pptm *.chm *.vbs *.js *.bat *.pif *.pdf *.jar *.sys
Modify Group Policy Settings	1	File path matches %systemroot%\system32\grouppolicy* OR %systemroot %\Sysvol\sysvol*\Policies*
Write to Program Files Directory	1	File path matches %programfiles%*

Download Events

Event Category - Download Events		
Event Type - Browser Download		
Event Name	**Score**	**Description**
Download Infectible File	3	File path matches any of the following: *.lnk *.wsf *.hta *.mhtml *.html *.doc *.docm *.xls *.xlsm *.ppt *.pptm *.chm *.vbs *.js *.bat *.pif *.pdf *.jar *.sys

Download Executable	2	File type is equal to PORTABLE_EXECUTABLE

Upload Events

Event Category - Upload Events		
Event Type - File Copy to Shared Folder		
Event Name	**Score**	**Description**
Write Executable to Shared Folder	5	File type is equal to PORTABLE_EXECUTABLE
Write Infectible to Shared Folder	5	File path matches any of the following: *.lnk *.wsf *.hta *.mhtml *.html *.doc *.docm *.xls *.xlsm *.ppt *.pptm *.chm *.vbs *.js *.bat *.pif *.pdf *.jar *.sys

Defense+ Events

No default rules for this event category.

Network Events

No default rules for this event category.

Appendix 2 - Agent Firewall Ports, IPs and Domains

We can capture DNS queries from network packets with Wireshark, and extract domain information.

Domain	IPs and Ports	Purpose	Miscellaneous
Valkyrie.comodo.com	52.60.56.170:443, 52.60.198.77:443	Valkyrie query and upload	Valkyrie server domain hardcoded
p10.fls.security.comodo.com	199.66.201.16:4448	FLS query	FLS server domain hardcoded
licensing.security.comodo.com	178.255.87.18:443	Register and security logs.	Hardcoded in the code, Wireshark capture traces during installation phase.
cmc.comodo.com	178.255.85.135:443	Acquire Valkyrie encrypted key from server	Hardcoded in the code, Wireshark capture traces during installation phase.
oscp.comodoca.com ocsp.comodoca.com.edgesuite.net	184.50.87.41:443 184.50.87.75:443	Encrypted communications (optional)	Wireshark capture traces during installation phase. Not defined in the solution code.
wtfibam2s5.execute-api.us-west-2.amazonaws.com	13.33.231.28:443, 13.33.231.89:443, 13.33.231.27:443, 13.33.231.45:443 (variable)	Policy, settings and heartbeat	EDR production server domain hardcoded in solution
6ynhsugqeg.execute-api.us-west-2.amazonaws.com	13.33.231.65:443, 13.33.231.105:443, 13.33.231.109:443, 13.33.231.39:443 (variable)	Policy, settings and heartbeat	EDR development server domain from edragentsettings.conf
h7tsgu3aej.execute-api.us-west-2.amazonaws.com	13.33.231.80:443, 13.33.231.90:443, 13.33.231.52:443, 13.33.231.25:443 (variable)	Policy, settings and heartbeat	EDR staging server domain from edragentsettings.conf
firehose.us-west-2.amazonaws.com	52.119.165.138:443 52.119.162.196:443 52.119.162.43:443	Upload event logs to AWS	SDK encapsulate the domain information. Extract the domain information from Wireshark monitor.

	52.119.169.95:443 52.119.168.237:443 (variable)		

The EDR agent uses port 443 to communicate over HTTPS with all servers *except*the Comodo FLS server, which uses port 4448.

There are only three server communications during installation - licensing.security.comodo.com, cmc.comodo.com, oscp.comodoca.com (ocsp.comodoca.com.edgesuite.net). The oscp.comodoca.com server domain is optional.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**