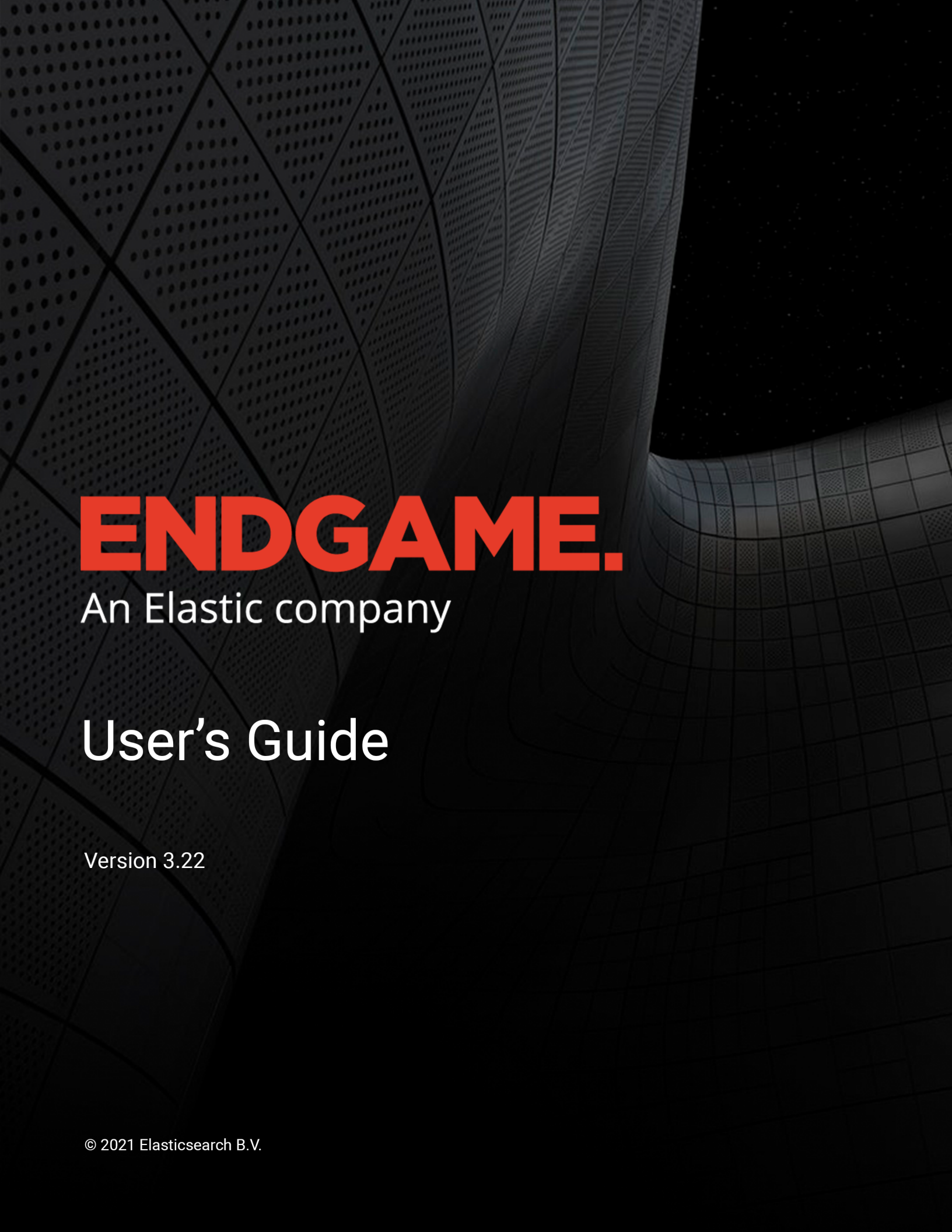


User's Guide

Version 3.22

COPYRIGHT NOTICE

Elasticsearch B.V.

3101 Wilson Blvd

Suite 500

Arlington, VA 22201

703-653-0361

https://www.elastic.co

Table of Contents

CHAPTER 1

GETTING STARTED

User's Guide Overview

This **User's Guide** is a comprehensive manual, designed to explain all features, tools and components of Endgame, version 3.22, so you can use them for maximum efficiency.

The following table lists the various icons you will see throughout the guide:

Name	Icon	Description
Info		Relevant, supplemental information about the aforementioned text.
Note		An important comment about the aforementioned text.
Refer to		A cross-reference to another topic or chapter in the manual.
Remember		A friendly reminder of information that appeared earlier in the manual.
Tip		A helpful, nice-to-know pointer.
Warning		A critical note that should be observed.

Introduction to Endgame

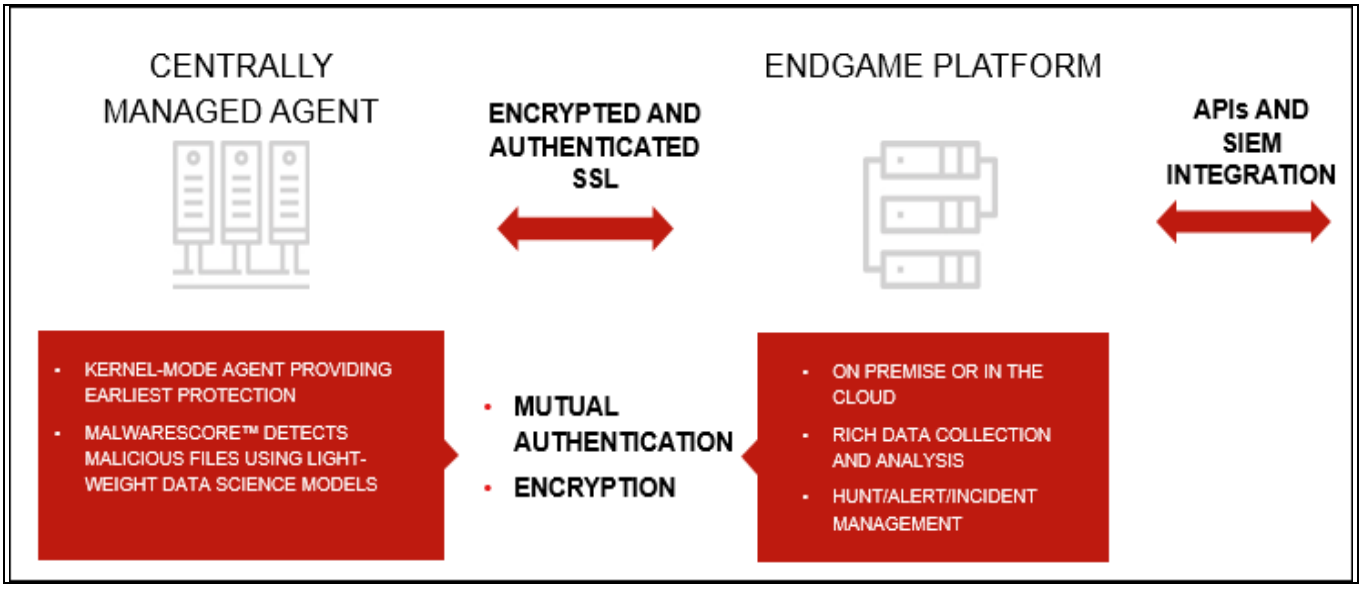
Endgame is a centrally managed endpoint detection and response platform that operates at the earliest and all stages of the attack life cycle. Through a single agent, Endgame instantly detects and stops privilege escalation, defense evasion, malicious persistence, credential access, and propagation.

Endgame automates the hunt for next generation attacks by automating data collection and analysis across all endpoints in seconds, instantly surfacing suspicious artifacts and malicious activity with tailored Tradecraft Analytics that highlight anomalous data. This enables analysts to act with precision to stop the adversary without business disruption.

Endgame provides the following capabilities:

- Accelerated endpoint detection and response
- In-band and out-of-band sensor deployment
- Advanced endpoint protection
- Automated hunting
- Multi-Client Management within an independent server

Endgame's advanced sensor technology allows the analyst choose to install a persistent sensor for long-term protection or a dissolvable sensor for minimal endpoint footprint.

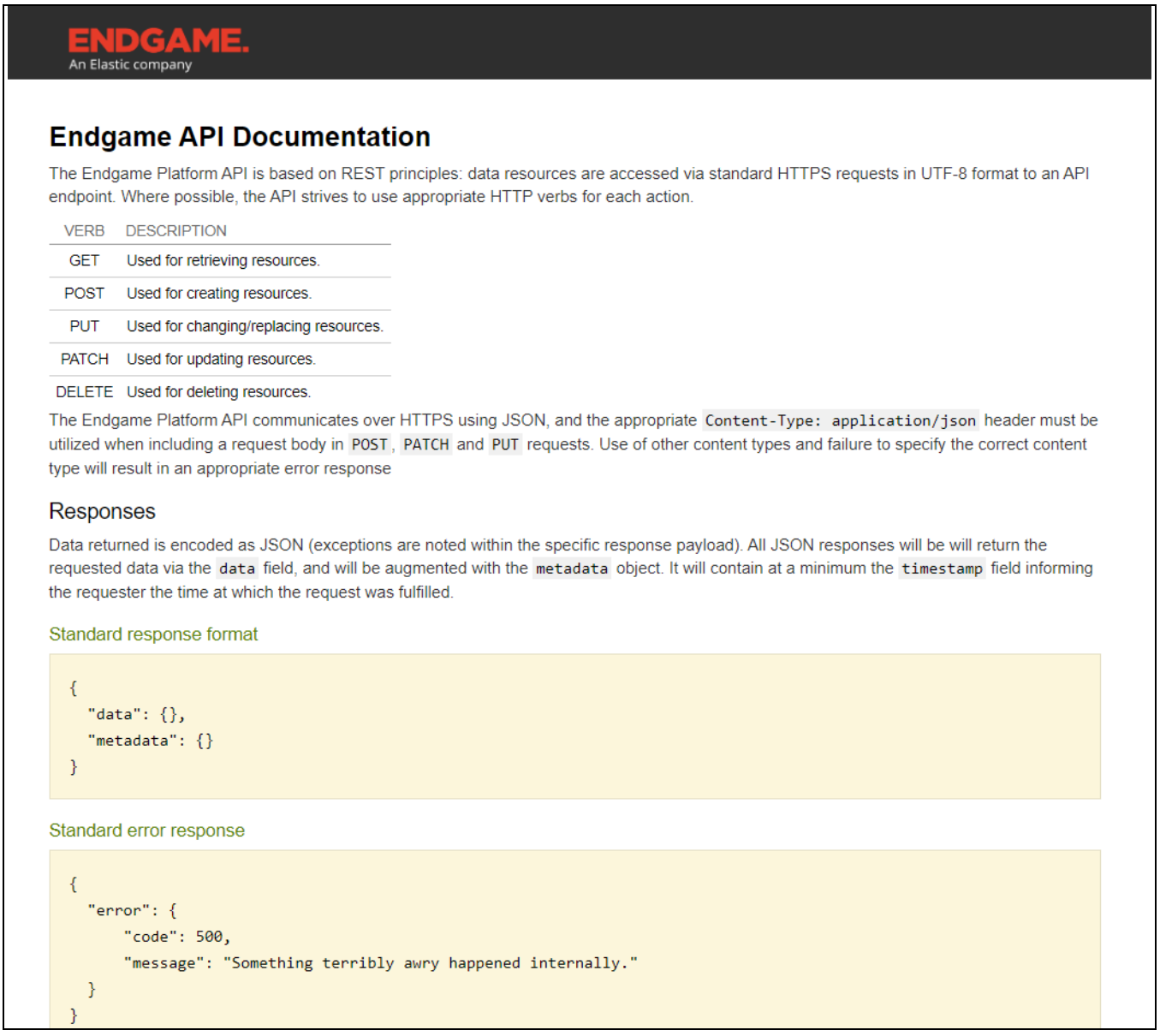


Endgame architecture

Application Programming Interface (API) Documentation

To view Endgame's API Documentation:

- Open a web browser and type the URL or hostname that hosts the Endgame platform followed by **/api/docs** (e.g., https://10.0.0.0/api/docs).



Endgame API Documentation

Glossary Terms

Before using Endgame, familiarize yourself with the following terms that are referenced in the User's Guide.

A

Activity Timeline

A chronological list of activities that occurred on an endpoint.

Adversary Behaviors

Adversary behavior alerts reflect the various behaviors attackers exhibit when executing an attack. These alerts are directly mapped to MITRE's ATT&CK™ and are useful in understanding the tactics and techniques an attacker may use when carrying out an attack.

Alert

A system-generated notification that indicates malicious activity on an endpoint.

Artemis

Endgame's artificial intelligence-powered security mentor that provides guided alert triage and event search.

B

Blocklist

A list of applications and files that an end user is forbidden to run within a network. The blocklist is maintained by an administrator.

C

Custom Rule

A statement, written in EQL, that instructs Endgame's sensor to monitor suspicious or malicious activity specific to your environment. If such activity is detected, the sensor generates an alert in the Endgame platform.

E

Endgame Resolver™ Attack Visualization

A visual depiction of chronological events that led up to the sensor generating an alert.

Endpoint

Any system or host that is connected to a network and functions as a client or server in any capacity. Desktop computers, laptops, and servers are all examples of endpoints.

Endpoint Policy

A policy that allows administrators to configure endpoint protections and event data collection. Policy reporting ensures compliance across all managed enterprise endpoints.

Endpoint Protections

Malicious activities and behaviors that are protected by Endgame's full autonomous sensor. Endpoint protections are enabled or disabled via Endpoint Policy configuration.

Event Query Language (EQL)

A syntax that enables you to structure more advanced queries that may be unavailable using natural language.

Exceptionlist

A list of items that specifies the attributes for which the sensor should not trigger an alert. The exceptionlist is maintained by an administrator.

F

File Quarantine

A process that isolates infected files on a computer's hard disk. Files put in quarantine are no longer capable of infecting their hosting system.

Fileless Attacks

An analytic and enhancement to the "Process" hunt that inspects the memory of running processes to discover potentially malicious code not backed on disk.

G

Group

The name given to a set of endpoints with similar attributes for easy endpoint management.

H

Histogram

A chart in Investigation Details that shows the number of occurrences — according to selected variables — on a defined percentage of endpoints. The Histogram also easily identifies outliers.

Host Isolation

A process that disconnects the host from the network so that adversaries are unable to move laterally and infect other systems. Isolated Hosts are only able to communicate with the Endgame platform or specific IPs that have been whitelisted.

Hunt

A task with specific parameters, executed by the sensor, that collects a current snapshot of events occurring on specified endpoints.

I

Investigation

A selection of one or more hunts used to identify malicious, suspicious, or anomalous behavior across endpoints.

IOC Search

A targeted search on one or more endpoints for a specific indicator of compromise, such as a file hash, process name, or network connection.

K

Key Performance Indicator (KPI)

A numerical measurement that represents the total number of items (e.g., endpoints, alerts, etc.) that fall into a specific category. KPIs also act as list filters.

M

MalwareScore™

A machine learning-powered malware prevention engine that prevents the execution of both known and unknown malware. Malware is scored on a scale from 0 (benign) to 100 (malicious).

Multi-Client Management

An independent server that allows an administrator to view and manage endpoint data from multiple Endgame platforms. It also serves as an entry point into those platforms.

P

Persistence

Any access, action, or configuration change to a system that allows a persistent presence on that system. Administrators define a sensor's persistence (i.e., persistent or dissolvable) when a sensor profile is created.

Q

Query

A structured syntax that specifies what endpoint data Artemis, Endgame's intelligent assistant, should search.

R

Reputation Score

An objective scoring based on third-party threat intelligence.

Response

A remediation action taken on an endpoint.

S

Sensor

Monitoring software deployed to an endpoint that continuously monitors it for malicious behavior and executes hunts, as tasked by a user. A sensor is also known as an agent.

Sensor Profile

A profile that contains the configuration settings required to deploy a sensor. After a profile is created, an installer executable becomes available to download for use in out-of-band deployment and sensor removal.

T

Threats

Threat alerts capture specific malicious activity that occurs on an endpoint. The alerts that are considered threats are Credential Dumping, Credential Manipulation, Exploit, Malicious File, Permission Theft, Process Injection, and Ransomware.

Tradecraft Analytics

Unique analytics for Process, Persistence, Network, and Users hunts that show uncommon or anomalous data in the Investigation Details view.

V

Visual Selector

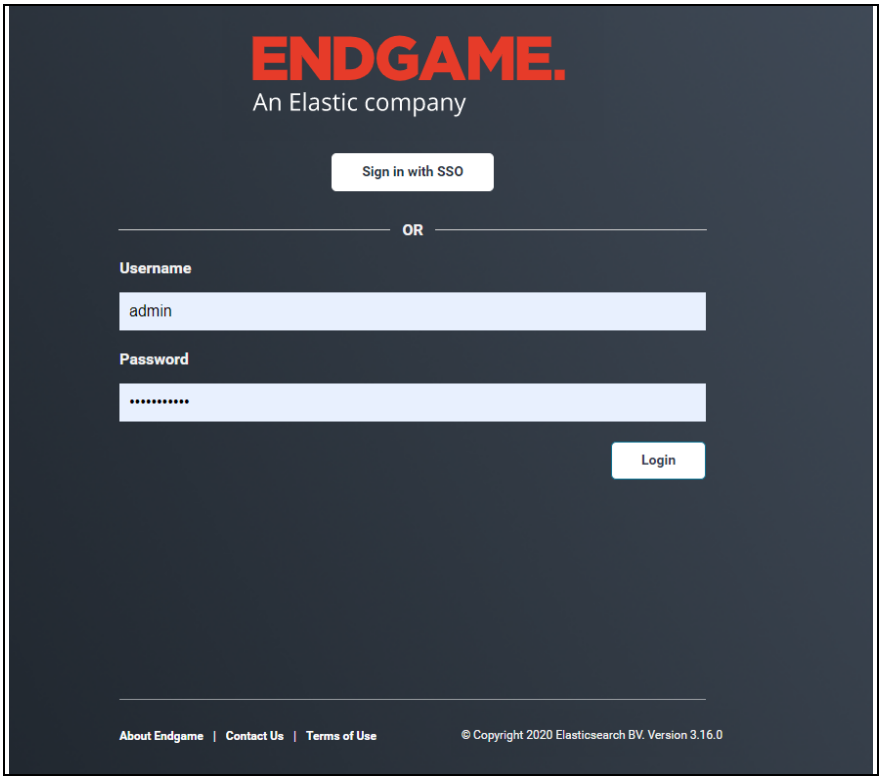
An interactive tool that enables the user to view the results of an investigation by selecting various data components.

Log in to Endgame

After the Endgame platform is successfully installed, you are ready to log in.

To log in:

1. Open a web browser and navigate to the IP or that hosts the platform.
2. In the **Username** and **Password** fields, type your username and password.
3. Click **Login**.

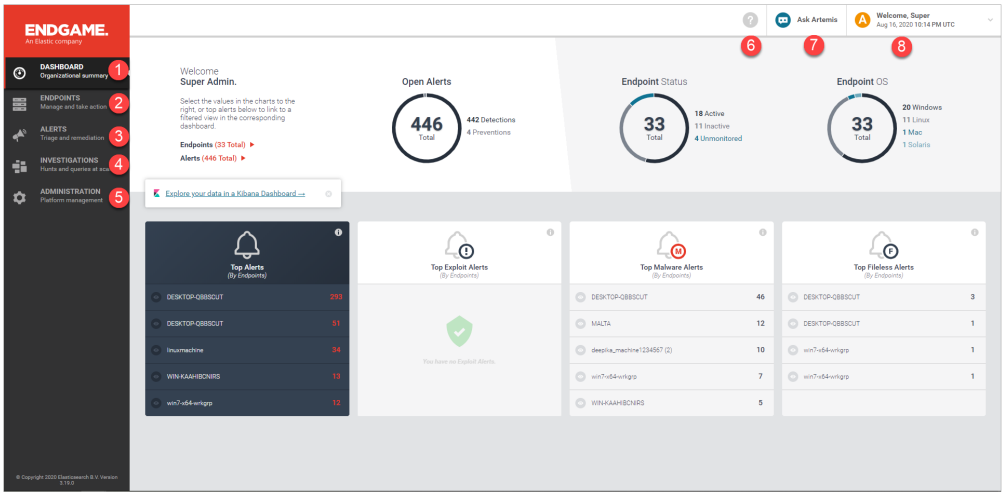


Endgame login screen

> **NOTE:** If your administrator has configured Single sign-on, click **Sign in with SSO** and enter your login credentials in the identity provider.

User Interface Overview

Endgame's user-friendly interface has two stationary toolbars which provide access to all of the platform's tools, features, and components.



ENDGAME USER INTERFACE

Side Navigation Toolbar

1. **Platform Dashboard.** Displays the current number of endpoints, organized by status and operating system, as well as the current number of alerts, organized by alert type.

2. **Endpoints.** View and manage endpoints on the Endpoint Dashboard.

3. **Alerts.** View a real-time summary of alert status on the Alert Dashboard.

4. **Investigations.** View and manage investigations on the Investigation Dashboard.

5. **Administration.** Manage all administrative functions from a single console.

Top Navigation Toolbar

6. **Online Help.** View Endgame's knowledge base to access documentation and print PDF guides.

7. **Ask Artemis.** Launch Artemis, Endgame's intelligent assistant, which enables you to search for specific endpoint data via an interactive chat interface.

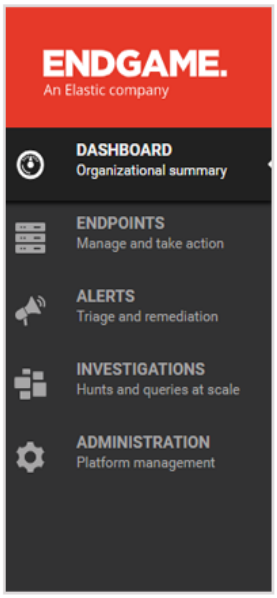
8. **User Settings.** View and manage user settings, go to the Administration page, or log out of the Endgame platform.

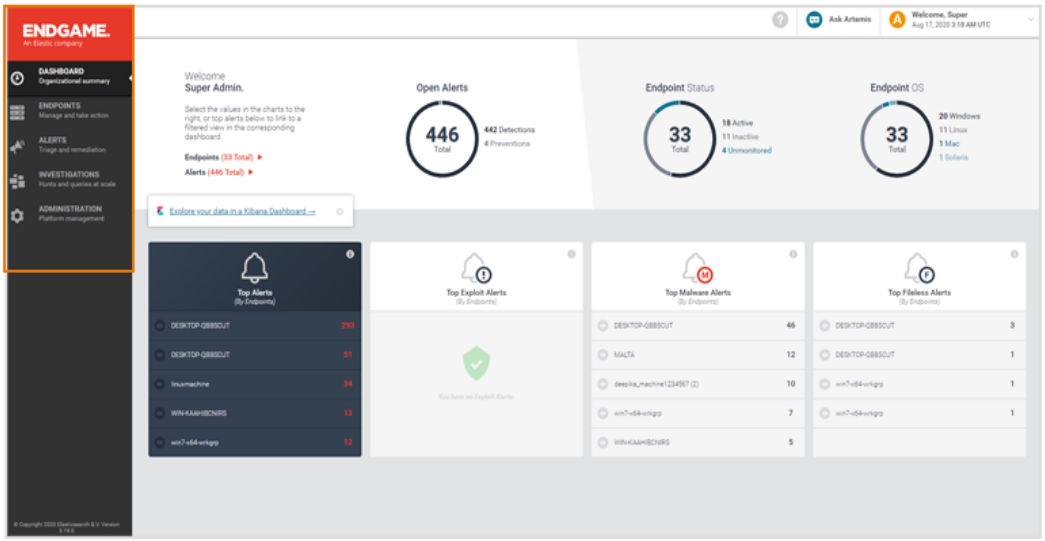
Endgame user interface

NOTE: Depending on your user role, you may have limited access and visibility to various content pages, tools, and features.

Left Navigation Toolbar

The Left Navigation toolbar is the main menu on the leftmost side of the screen.





Left Navigation toolbar

It has five buttons that each display a corresponding content page when selected:

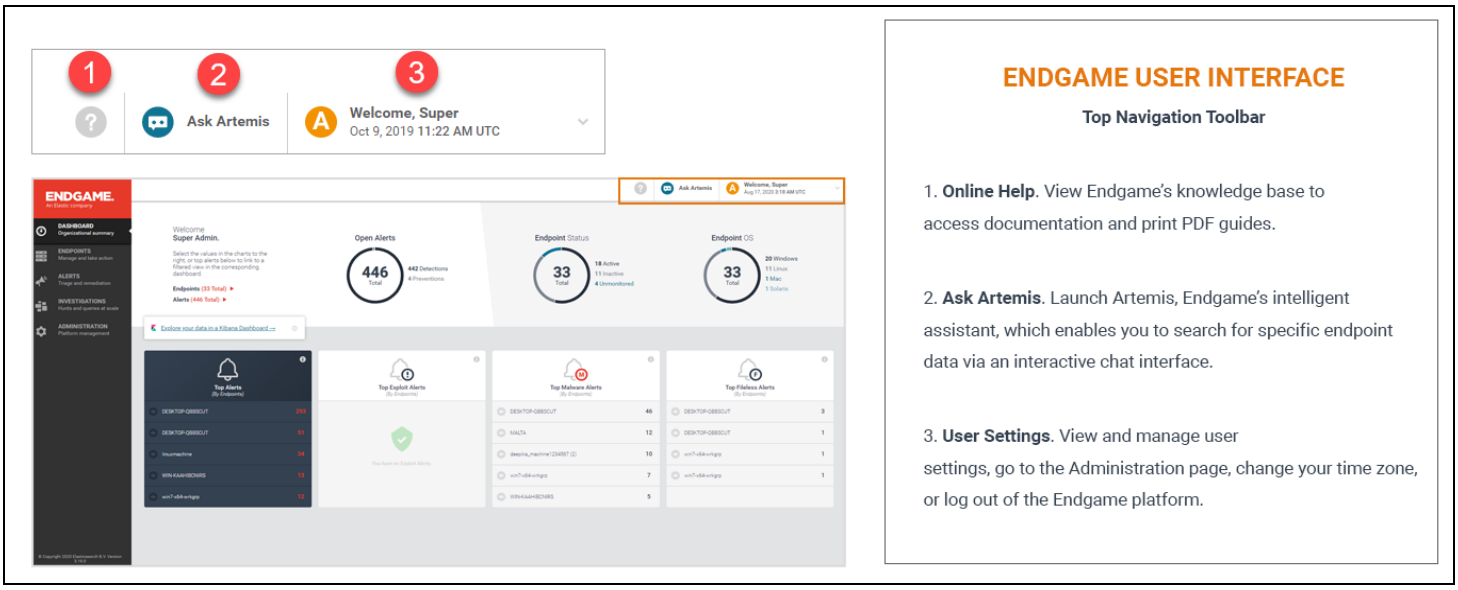
Button	Page	Description
	Platform Dashboard	View an overall status of endpoint and sensor health.
	Endpoint Dashboard	View and manage endpoints.
	Alert Dashboard	View an overall summary of current alerts in your environment.
	Investigation Dashboard	View and manage investigations.

Button	Page	Description
	Administration	View and manage all administrative functions.

NOTE: On all content pages besides the Platform Dashboard, the Left Navigation toolbar is a condensed version that does not display the name of each page, however, you can hover your cursor over a button to view the corresponding page name.

Top Navigation Toolbar

The Top Navigation toolbar contains three menu items that provide quick access to various tools and user interface elements.



Top Navigation toolbar

Online Help

Access Endgame's knowledge base to view all user documentation and print full-text print guides.

Artemis Chat

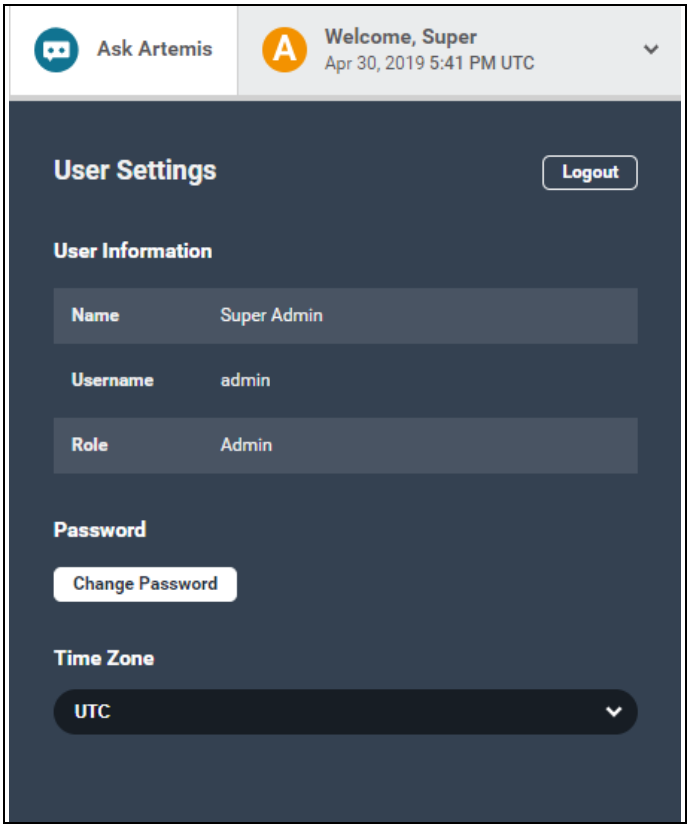
The **Ask Artemis** button launches Endgame's intelligent assistant, which enables you to search for specific endpoint data via an interactive chat interface.

For more information about Artemis, see "Artemis Search Overview."

User Settings

The **User Settings** tab displays your name, the number or letter that corresponds to your user role status (e.g., "A" if you are an administrator, "1" if you are a Level 1 user, etc.) and the current date and time. Select the tab to display the User Settings panel, which displays your user information and allows you to change your password, change your time zone, and log out of the platform.

> **NOTE:** The option to change the current password only appears if you logged in with a local user account.



User Settings panel

Change Your Password

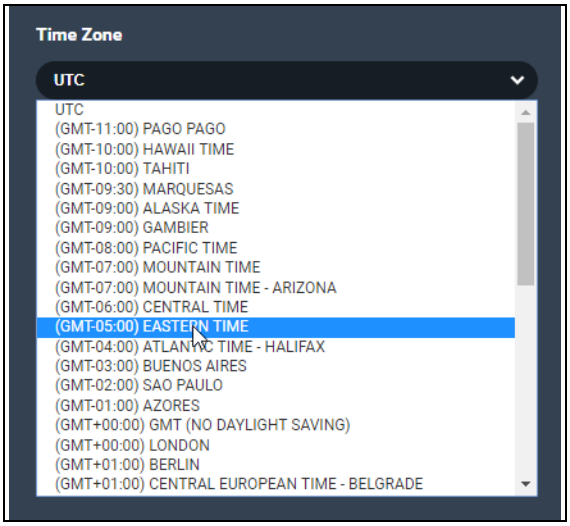
> **NOTE:** You can only change your password if you logged in with a local account. If you need to change your username or if you forgot your password, contact your administrator.

To change your password:

1. Select the **User Settings** tab.
2. On the User Settings panel, click **Change Current Password**.
3. Complete the requirements in the Change Password section:
   a. In the **Current Password** text box, type your current password.
   b. In the **New Password** text box, type a new password that meets the following minimum requirements:
      - Minimum 8 characters
      - 1 uppercase character
      - 1 lowercase character
      - 1 number
      - 1 special character (e.g., ~!@#$%, etc.)
   c. In the **Confirm New Password** text box, type the new password again.
4. Click **Save** to save your changes. If the password change was successful, a "Password Changed Successfully" confirmation appears.

Change Your Time Zone

By default, Endgame sets the time zone to Coordinated Universal Time (UTC). You can change your time zone from the default by selecting the appropriate time zone from the **Time Zone** drop-down list.



NOTE: If you are running Internet Explorer 11, UTC is the only time zone option. However, please note that UTC time zones are not displayed in the platform.

Log Out of Endgame

- Click **Logout** in the upper-right corner of the User Settings panel.

Supported Endgame Platform Functions by Operating System

Each of Endgame's supported operating systems provides various sensor deployment, endpoint protection, and search functionality within the platform. Refer to the following table for guidance on which functions are supported. Especially keep this information in mind when creating a new sensor profile or applying an Endpoint Policy to a group of endpoints.

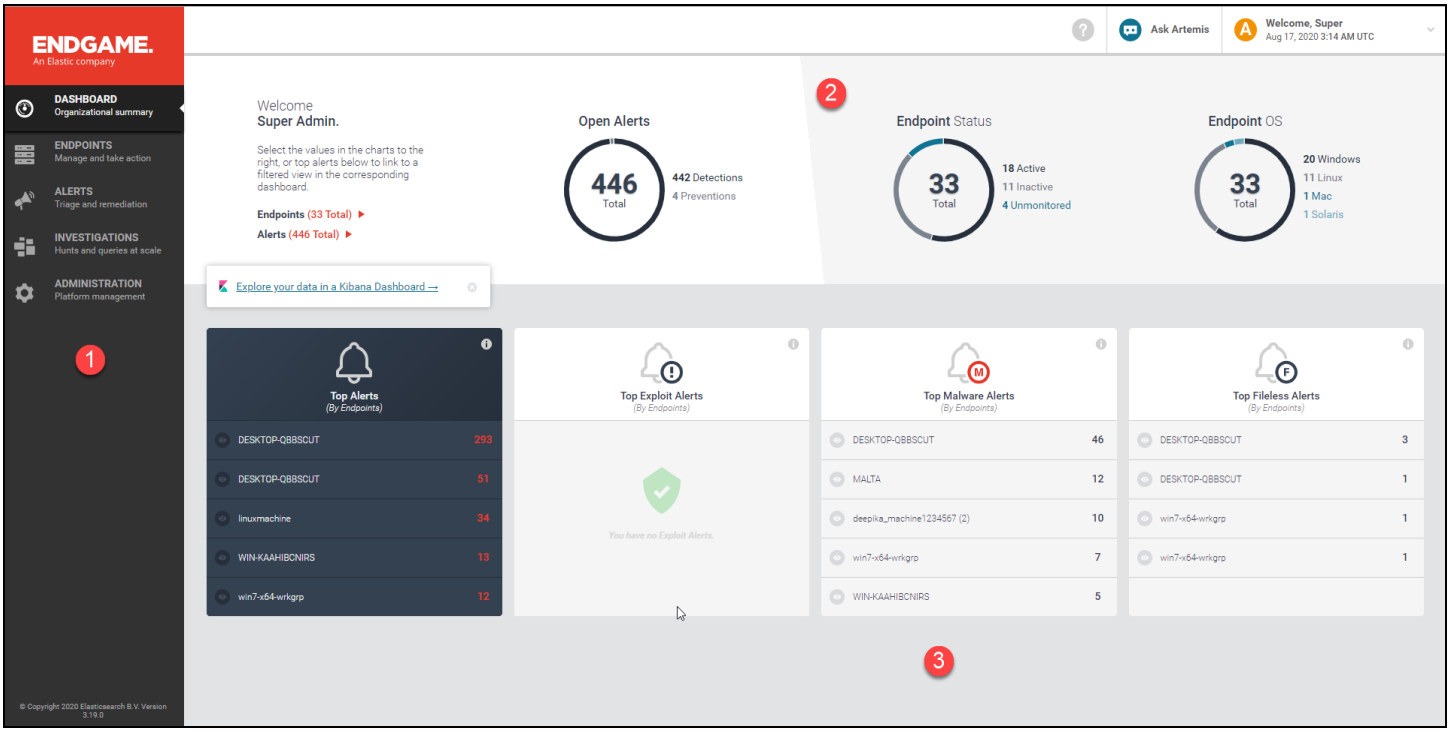
	Windows	Linux	macOS	Solaris
Persistent sensor	✓	✓	✓	✓
Dissolvable sensor	✓	✓	X	✓
Modifiable signatures	✓	X	X	X
In-band deployment	✓	X	X	X
Out-of-band deployment	✓	✓	✓	✓
Enable endpoint protection	✓	✓	✓	X
Add items to the exceptionlist	✓	✓	✓	X
Add items to the blocklist	✓	X	X	X
Artemis eventing	✓	✓	✓	X
Create investigations	✓	✓	X	✓
Add a trusted application	✓	X	✓	X

Platform Dashboard Overview

The Platform Dashboard is the default view when you log in to the Endgame platform. It is a summary screen that displays overall system health and sensor status.

The dashboard contains three sections:

1. Expanded navigation
2. Alert and Endpoint Key Performance Indicator (KPI) charts
3. Alert KPI cards

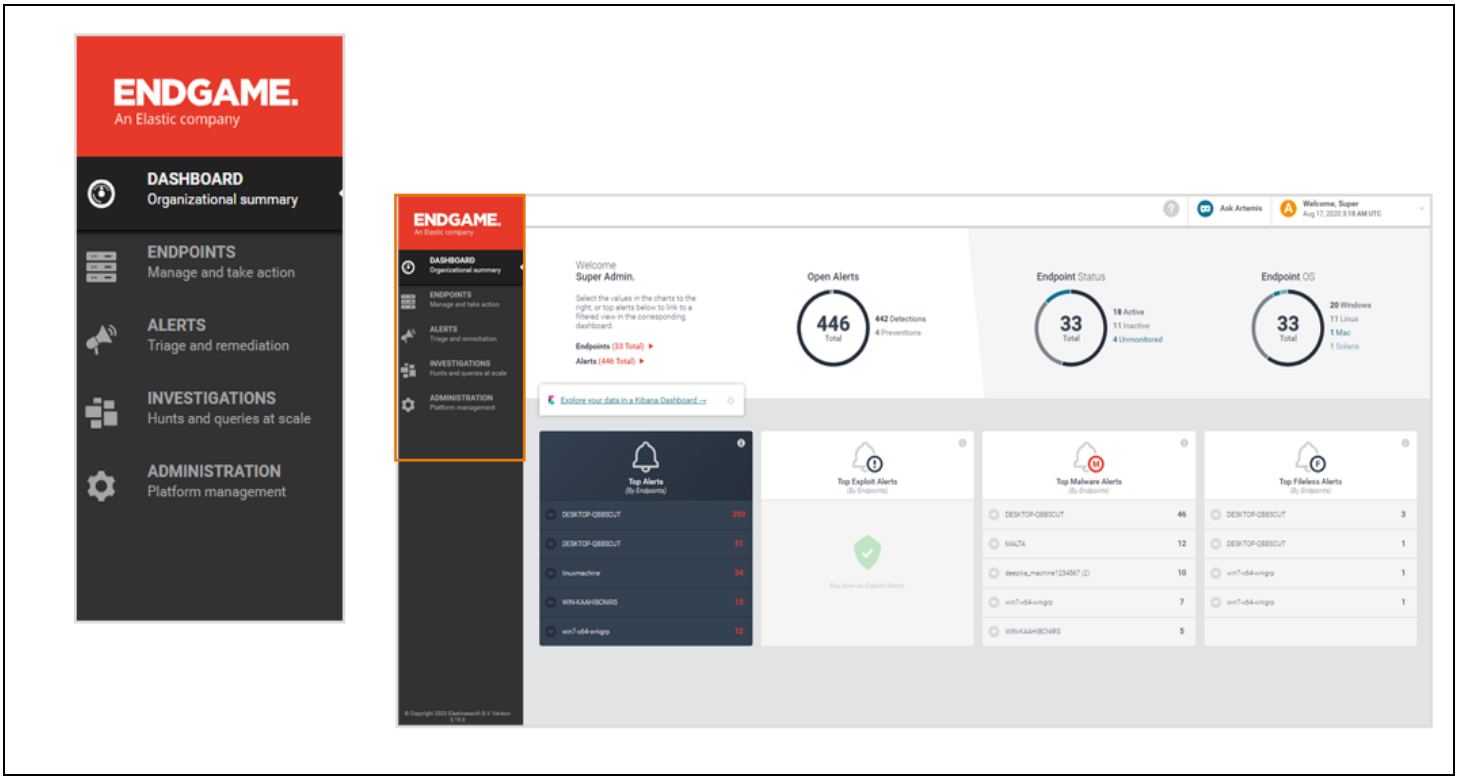


Platform Dashboard

Expanded Navigation

The Platform Dashboard provides an expanded navigation view that displays the name of each content page that corresponds to the six buttons on the Left Navigation toolbar. All other content pages in the Endgame platform display a condensed view of the toolbar that only displays the page buttons.

> **TIP:** If you are in another section of the platform, hover your cursor over a button on the Left Navigation toolbar to view the page name.



Expanded navigation view

Alert and Endpoint Charts

The top of the page displays three key performance indicator (KPI) charts that summarize the overall status of alerts and endpoints within your network:

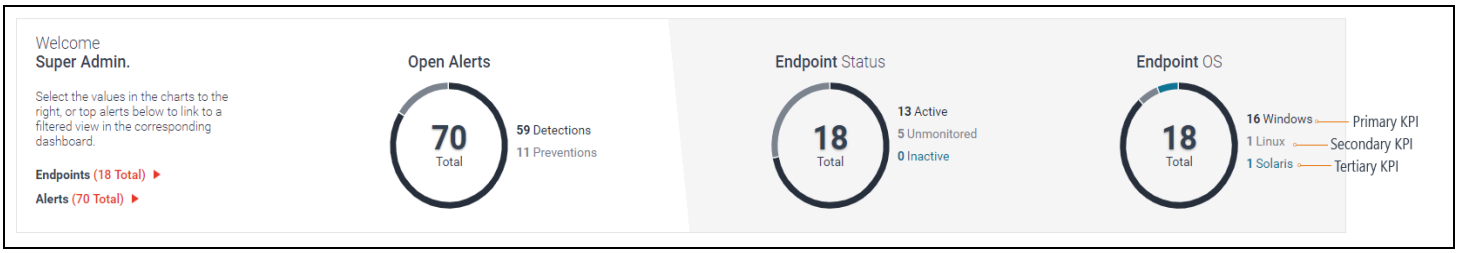
KPI Chart	Description
Open Alerts	The number of active detections, preventions, and alert notifications.
Endpoint Status	The number of endpoints that fall into one of the following categories: • **Active:** An endpoint with an installed sensor that currently is communicating with the

KPI Chart	Description

	Endgame platform.
	• **Inactive:** An endpoint with an installed sensor that currently is not communicating with the Endgame platform.
	• **Unmonitored:** An endpoint that has one of the following attributes:
	  • It does not have an installed sensor.
	  • It has not communicated with the platform in two weeks or more.
	NOTE: If there was a sensor previously installed but has since been installed, that endpoint also falls in the "unmonitored" status.
	For more information about how to run an endpoint scan to discover endpoints within your network, see "Discover New Endpoints" in Chapter 2, *Endpoints*.

Endpoint OS	The number of endpoints running on each of Endgame's supported operating systems.

Each numerical value in the KPI charts, called a KPI slice, represents the number of endpoints or alerts that fall into a specific category. The total count displays in the center of the chart, whereas primary (highest count), secondary, and tertiary (if applicable) KPIs display outside the chart. KPIs update in real time as new data becomes available.



Alert and Endpoint charts. Select a KPI to filter by the selected category.

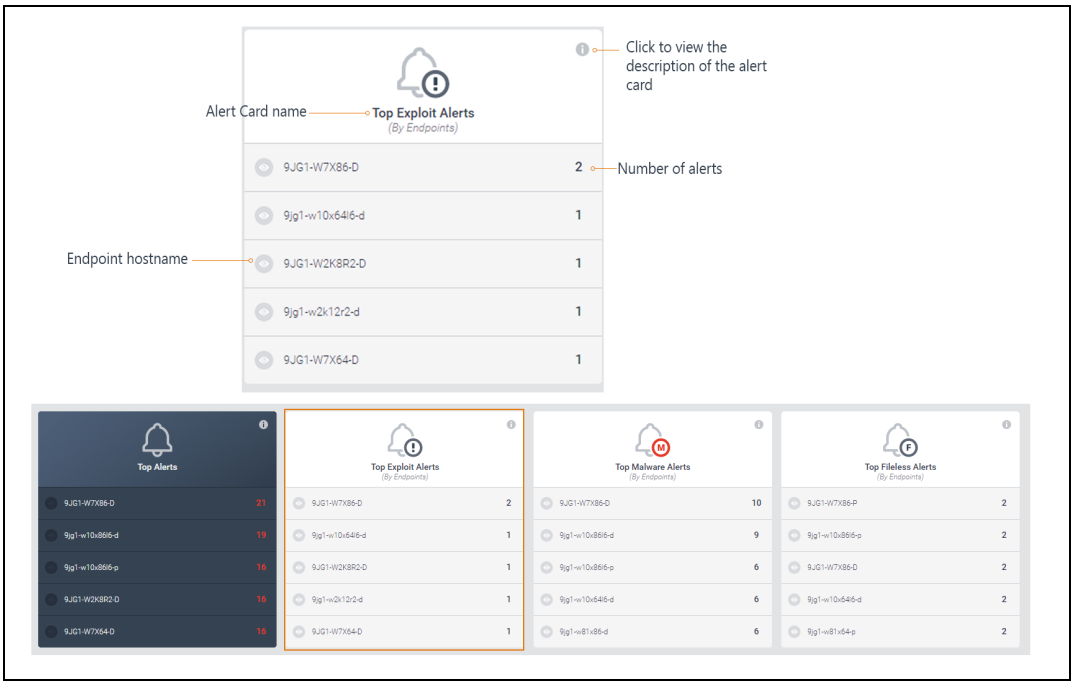
Each KPI is also an active link, that when clicked, filters the Endpoints list or Alerts list by the selected attribute. For example, to view all currently active endpoints in the Endpoints list, select the **Active** link on the Endpoint Status chart.

Alert KPI Cards

Beneath the Endpoint and Alert charts are four Alert KPI cards — individual snapshots that highlight the top five endpoints with the most alerts in the following categories:

Alert Card Name	Alert Type	Description
Top Alerts	• All	All alert types.
Top Exploit Alerts	• Exploit Detection • Exploit Prevention	Detected or blocked exploits.
Top Malware Alerts	• Malicious File Detection • Malicious File Prevention	Detected or blocked potentially malicious files present on disk.
Top Fileless Alerts	• Process Injection Detection • Process Injection Prevention	Detected or blocked malware running in memory.

NOTE: The Endgame platform generates alerts based on Endpoint Policy configuration. For more information, see "Endpoint Policy Overview" in the *Administrator's Guide*.



Alert KPI cards. Select an endpoint hostname to view a filtered Alerts list.

Each row displays the hostname of the affected endpoint and its alert count. Like the KPIs in the Endpoint and Alert charts, when a row is selected, those attributes are applied as filters to the Alerts list. For example, to view the top Malicious File alerts that were generated for a single endpoint, select the first row on the "Top Malware Alerts" card. The Alerts list displays the filtered data in reverse chronological order with newest alerts at the top.

A high alert count may indicate a potential data compromise; therefore, it is recommended you view alerts with the highest count first.

(missing or bad snippet) Click the Info button in the upper-right corner of an Alert KPI card for a description of the alert data.

CHAPTER 2

ENDPOINTS

Endpoints Overview

An endpoint is any network-connected system, piece of equipment, or host that functions as a client or server in any capacity, such as desktops, laptops, or servers. Endgame provides customized sensor configuration that enables endpoint protection against unauthorized access, changes to the environment, and other adversaries.

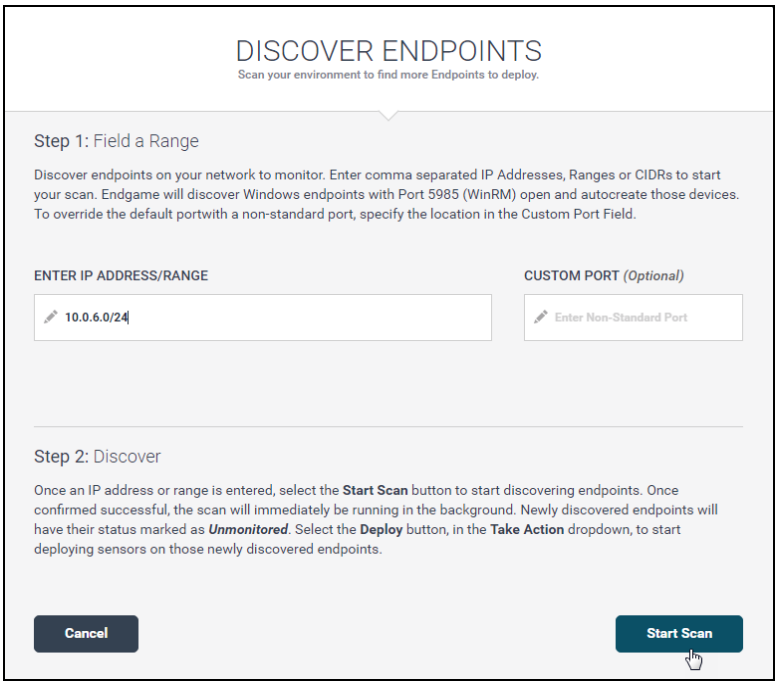
Discover Endpoints

The first step in deploying a sensor is to run a scan to discover network-connected endpoints.

> **NOTE:** This tool is only compatible with Windows. If you are deploying a sensor via out-of-band management you can skip this step. Although only administrators can deploy sensors, any user can run an endpoint scan.
>
> For more information about in-band and out-of-band sensor deployment, see "Sensor Deployment Overview" in the *Administrator's Guide.*

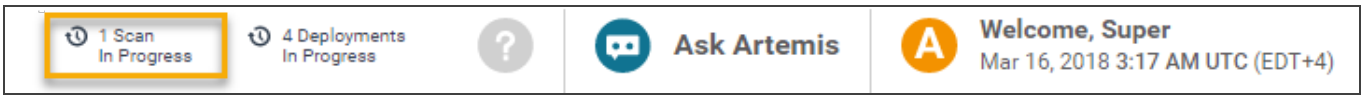
To scan for new endpoints:

1. On the Left Navigation toolbar, click the **ENDPOINTS** button  to display the Endpoint Dashboard.
2. On the Action toolbar, click **Discover Endpoints**.
3. Complete the requirements in the **DISCOVER ENDPOINTS** dialog window:
   - **ENTER IP ADDRESS/RANGE:** In the text box, type the IP address or IP range to scan. To specify a range of IP addresses, enter a Classless Inter-Domain Routing (CIDR) prefix (e.g., 10.0.6.0/24) or use a hyphen between the first and last addresses (e.g., 192.68.1.4 - 192.68.1.56).
   - **CUSTOM PORT (Optional):** By default, Endgame discovers Windows endpoints with port 5985 (WinRM). If you want to override the default port with a non-standard one, enter the location in the text box.
4. Click **Start Scan**. A "Scan successfully initialized" message appears to confirm the scan has begun.



Discover New Endpoints dialog window

5. Click **Finish**. After the scan begins, the total number of endpoints steadily increases as they are identified, and the **Scan in Progress** indicator appears in the upper-right corner of the Endpoint Dashboard.

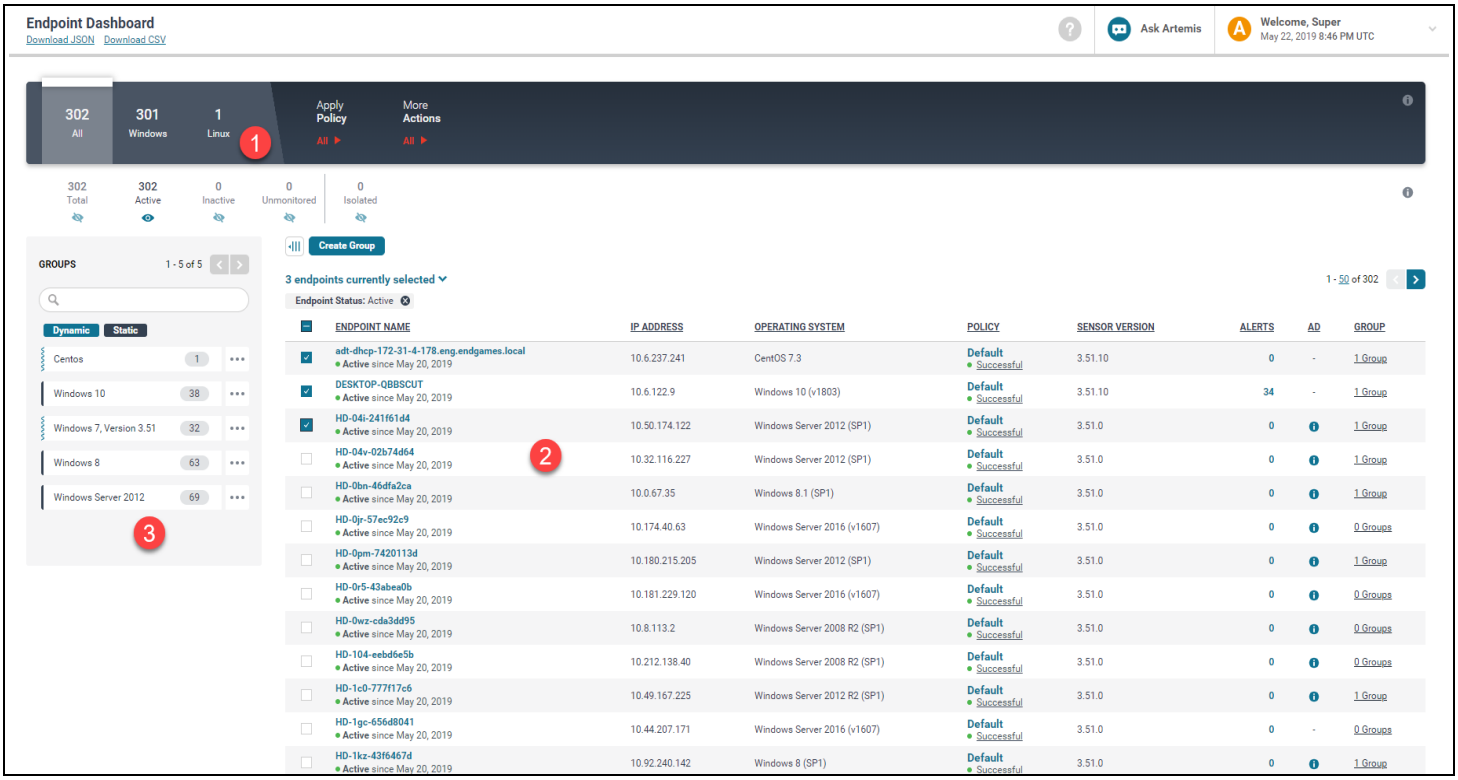


6. When the scan is finished, a "Scan Completed" confirmation appears with two options to either download the log file or dismiss the message. To download the scan log, click **Download Log File**.

Endpoint Dashboard Overview

The Endpoint Dashboard provides an overview of all endpoints in the Endgame platform, gives an overall status of sensor health, and provides options to view, execute specific actions, filter, and manage endpoints.

To view the Endpoint Dashboard, click the **ENDPOINTS** button  on the Left Navigation toolbar.



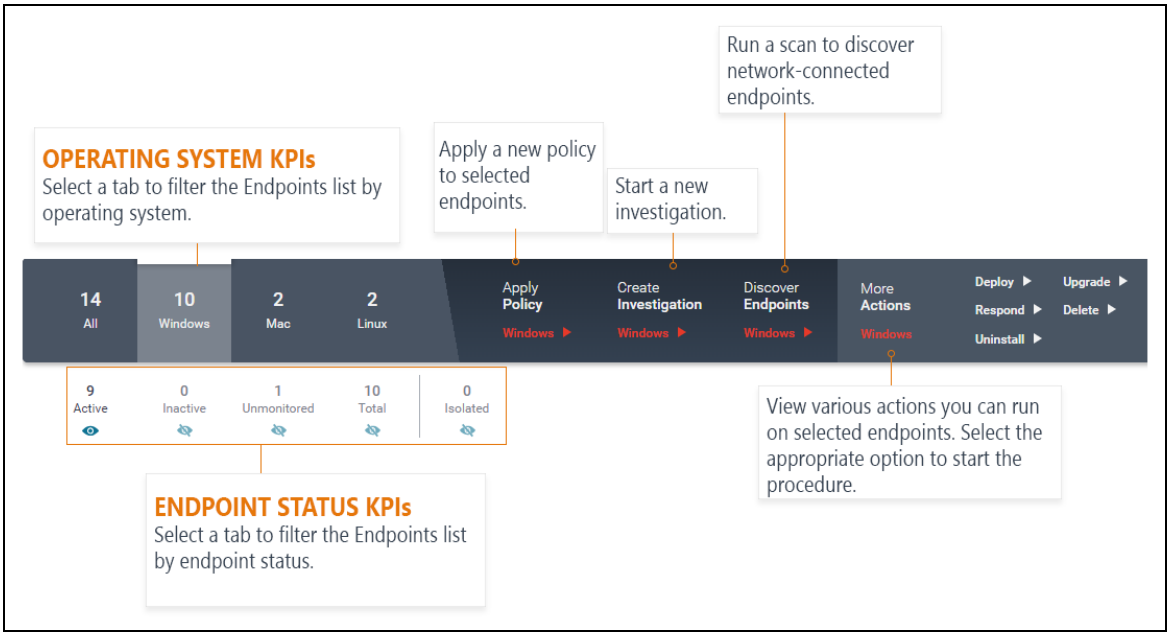
Endpoint Dashboard

The dashboard contains three major sections:

1. Action toolbar
2. Endpoints list
3. Groups panel

Action Toolbar

The Action toolbar enables you to execute various endpoint actions, such as start an investigation, scan, assign a group, and deploy endpoints. It also contains key performance indicators (KPIs) to narrow endpoints by specific parameters.



Action Toolbar on the Endpoint Dashboard

Operating System and Endpoint Key Performance Indicators

The toolbar contains operating system KPIs that display the total number of platform-connected endpoints and the unique number of endpoints running on Windows, Linux, macOS, and Solaris.

Beneath the toolbar, a secondary set of KPIs displays the number of endpoints that fall within a specific category:

KPI	Description
Active	Endpoints with an installed sensor that currently is communicating with the platform.
Inactive	Endpoints with an installed sensor that currently is not communicating with the platform.
Unmonitored	Endpoints with no installed sensor.
Total	The total number of endpoints that are running on the selected operating system, or the total number of endpoints across all operating systems if the **All** KPI is selected.
Isolated	The number of endpoints that are in an isolated state and, therefore, cannot communicate with other network-connected endpoints. For more information about host isolation, see "Host Isolation Overview."

The default Endpoint Dashboard view displays all active endpoints. KPIs update in real time when new data is available.

Each KPI in the Endpoint Dashboard is an interactive link that filters the Endpoints list by the selected category. For example, to view all endpoints that are running on Windows with an active sensor, select **Windows**, then select **Active**. Filters are useful to narrow a large number of endpoints by specific criteria to execute a task on those similar endpoints simultaneously.

You can also sort and filter columns within the Endpoints list. For more information, see "Sort and Filter Columns in the Endpoints List" in this topic.

Endpoint Actions

The Action toolbar also contains additional menu items that start specific endpoint procedures when selected.

NOTE: The set of available options depends on the selected operating system KPI.

Tab	Description
Create an Investigation	Starts a new investigation. **NOTE:** You must select at least one endpoint to enable this task. This option is not available if the **All** KPI is selected.
Apply Policy	Applies a new Endpoint Policy to selected endpoints.
Discover Endpoints	Runs a Windows endpoint scan to discover network-connected endpoints.
More Actions	Displays a list of specific actions you can take on selected endpoints:

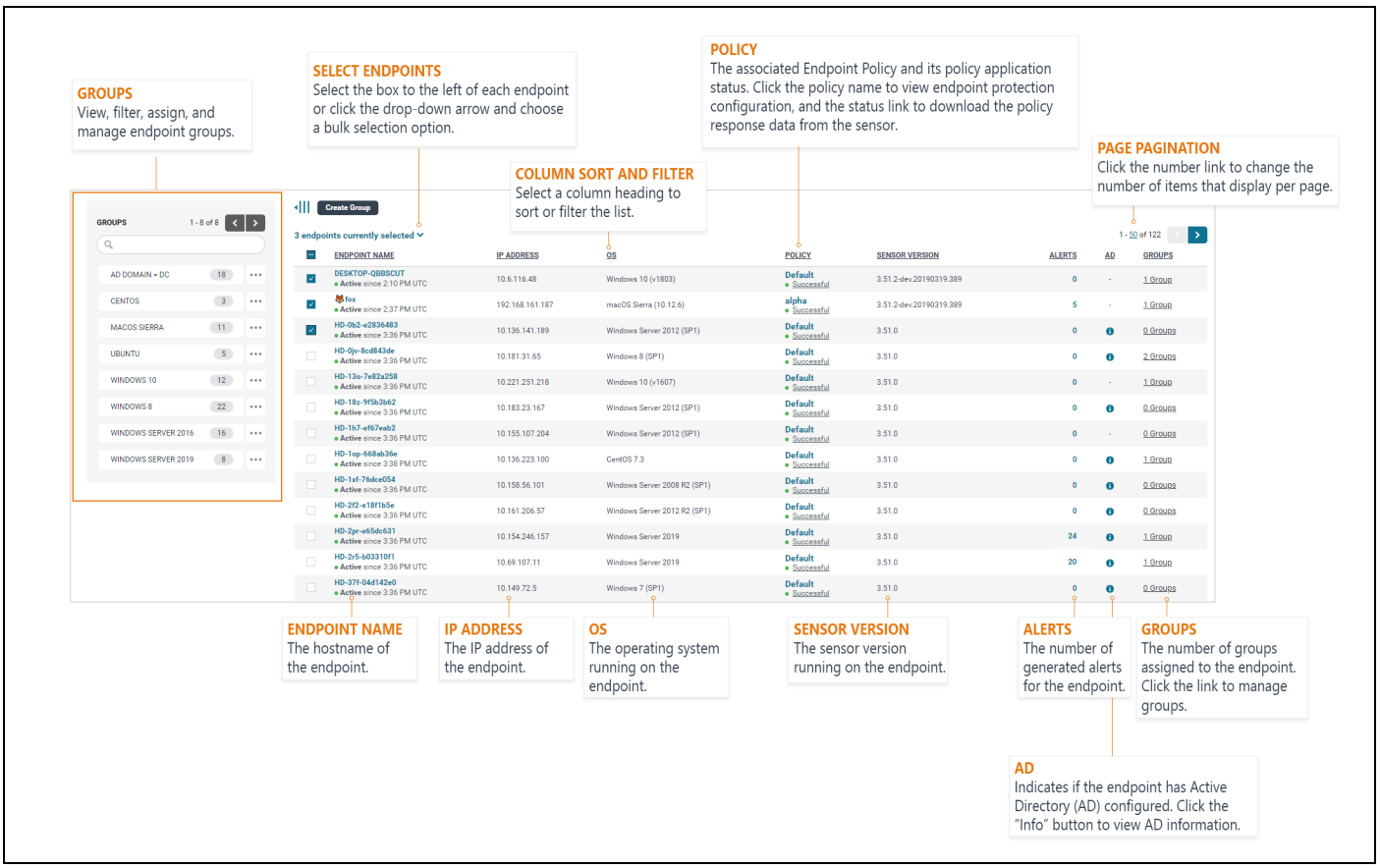
Action	Description
Deploy	Deploys a sensor to one or more endpoints.
Respond	Executes a specific task on the endpoint, such as deleting or uploading a file.
Uninstall	Uninstalls the sensor from the endpoint.
Upgrade	Upgrades selected endpoints to a newer sensor version.
Delete	Removes the endpoint from the Endgame platform.

If a sensor deployment or endpoint scan is in progress, a status indicator appears in the upper-right corner of the page. The number indicates how many procedures currently are running.

Endpoints List

The Endpoints list is an enumeration of all endpoints in the Endgame platform. The list organizes all relevant endpoint details in a table and is useful to view network statistics, find targeted data, and identify abnormal patterns in sensor status. For example, if the list indicates several sensors became inactive around the same time, this could signify an attempted data breach that requires immediate investigation.

Endpoints display in alphabetical order according to their hostname.



Endpoints list

The columns in the Endpoints list display the following endpoint and sensor data:

Column Name	Description
ENDPOINT NAME	The hostname of the endpoint. A secondary line displays the sensor status and the amount of time it has been in that state. The sensor status falls into one of the following categories: • **Active:** The sensor has established a connection to Endgame. • **Inactive:** The sensor was previously connected to Endgame but is now disconnected. • **Unmonitored:** No sensor is installed on the endpoint. • **Deployment Failure:** The sensor failed to deploy to the endpoint. Click the link to view the deployment error message in a pop-up window. **NOTE:** It is possible for two endpoints to have the same hostname. You can distinguish the difference by the IP address, or consider assigning it to a group. For more information about endpoint groups, see "Manage Groups" in this chapter.
IP ADDRESS	The current IP from which the endpoint is communicating to the platform.
OS	The current operating system running on the endpoint.
POLICY	The associated Endpoint Policy and its policy application status. Click the policy name to view the configuration, and the status link (e.g., Successful, Failed, etc.) to download the response from the sensor.
SENSOR VERSION	The sensor version running on the endpoint. If applicable, it also displays the status of the sensor upgrade.
ALERTS	The number of current alerts for the endpoint.
AD	Indicates if Active Directory (AD) is configured on the endpoint. Click the **Info** button to view Active Directory information. **NOTE:** If there are updates made to your AD structure, those updates are reflected in the platform within 24 hours.
GROUPS	Displays the number of groups assigned to the endpoint. Click the link to view the group names.

The Endpoints list automatically updates when new data is available; however, if you have selected endpoints to begin a procedure (e.g., sensor deployment) and the Endpoint Dashboard is inactive for several minutes, a dialog box that says, "Your endpoint list is out of date. You must refresh to continue" appears. Click the **Refresh** button to display the new data.

Sort and Filter Columns in the Endpoints List

You can sort columns in the Endpoints list to change the order the contents in a column appear, or search them to filter content by a particular value. Sorting and filtering columns are useful to quickly find specific information without browsing through a large amount of data.

NOTE: You cannot sort the **AD** or **GROUPS** columns, however, you can search for specific group names.

To sort or filter a column, select the appropriate column heading and choose from the following options:

To sort by increasing or decreasing value:

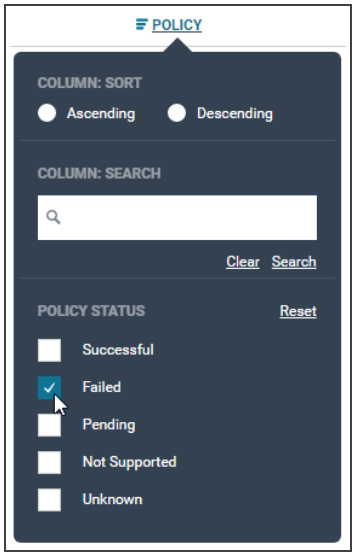
- Select the **Ascending** or **Descending** option. The currently sorted column is denoted by an up arrow or down arrow .

To search the column for a particular value:

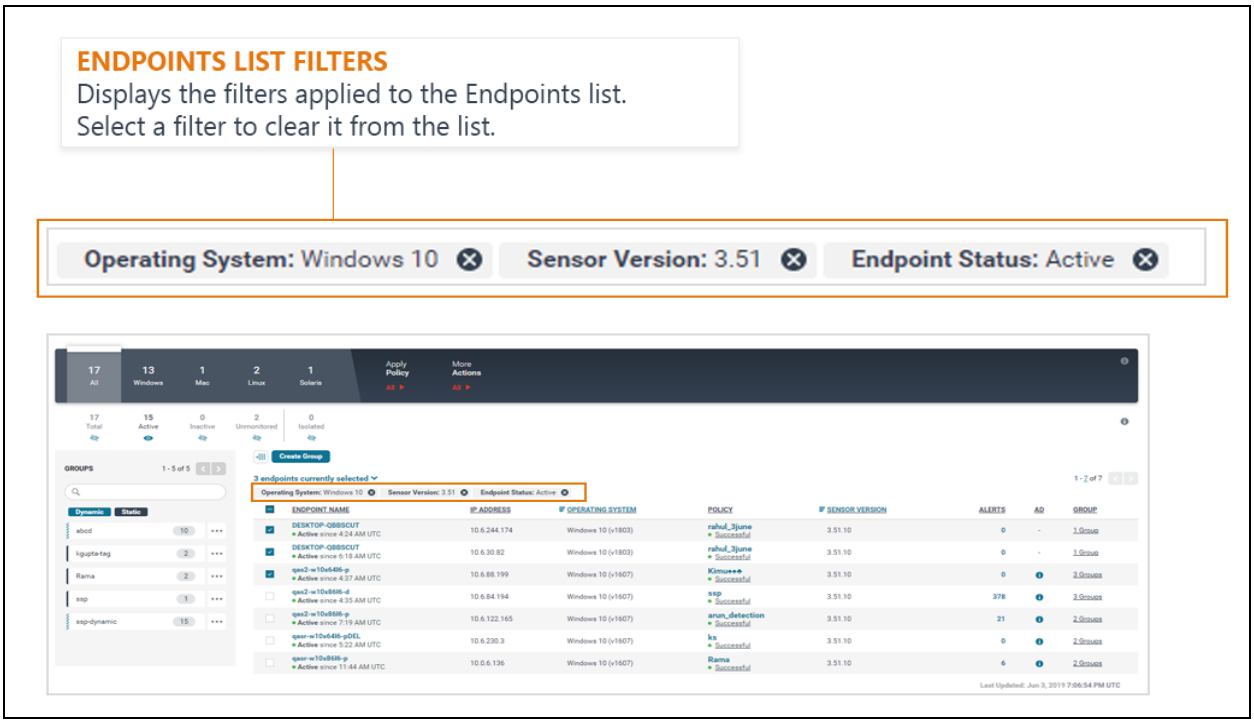
- In the text box, type the text you want to find, then click **Search**. The list filters to display results that match the entry. The currently filtered column is denoted by a symbol.

Column sort and filter

TIP: Sorting or filtering Endpoint Policies are useful to view the status of policy application. For example, to view failed policy applications, select the **POLICY** column heading, then select the **Failed** option in the **POLICY STATUS** section.



If you have applied a filter to the Endpoints list, those values appear directly above the list, providing a comprehensive view of all filter criteria. To clear a filter from the list, click the **x** on the appropriate value.



Filtered columns display the criteria in the Endpoints list

Filter Endpoint Groups

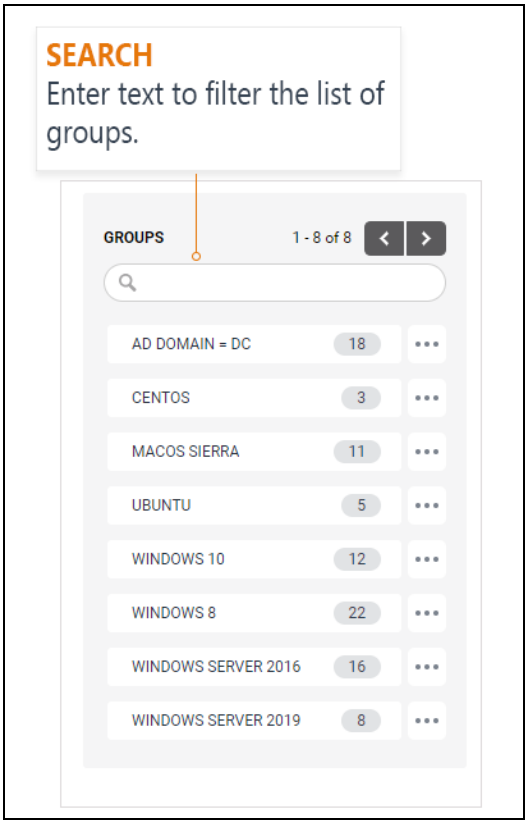
Filter endpoint groups via the Groups panel. For more information about endpoint groups, see "Endpoint Groups Overview."

To filter the Endpoints list by a specific group:

- Select the appropriate group name in the Groups panel.

To search for a specific group name:

- Begin typing text in the search bar. The list of groups filters to display results that match the typed text.



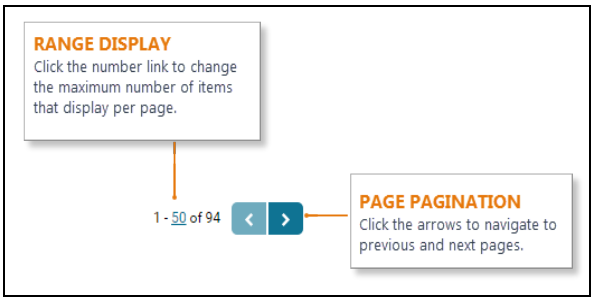
Filter groups via the Groups panel

Page Pagination

In the upper-right corner above the list is a range display, which displays the current number range of endpoints out of the total (e.g., 1-50 of 400). Click the left and right arrows to navigate to previous and next pages.

By default, a maximum of 50 endpoints display per page; however, you can change the number to a preferred choice:

1. On the range display, click the number link. For example, if the range display is 1-50, click **50**.
2. In the **Max count of** text box, enter a new number between 1 and 500.
3. Click ✓ to save your changes.

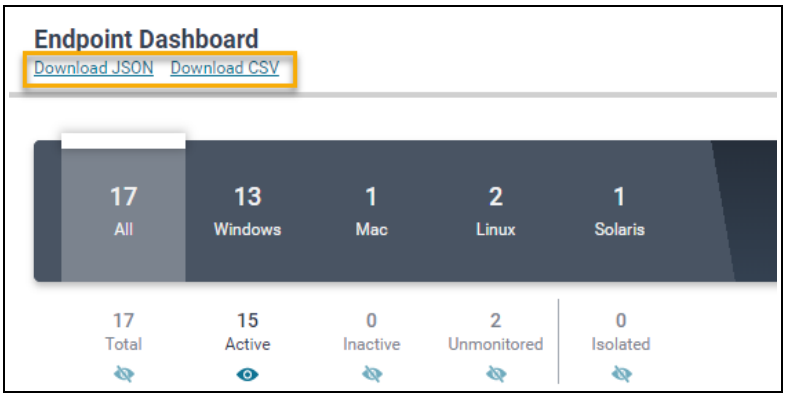


Download the Endpoints List

You can download the current Endpoints list to a comma-separated values (CSV) file or you can download the raw JSON to an external file. Any sort and filter preferences applied to the list are retained in the downloaded file.

To download the Endpoints list:

1. In the upper-left corner of the Endpoint Dashboard, click **Download JSON** or **Download CSV.**



2. When the download is complete, open or save the file from your browser.

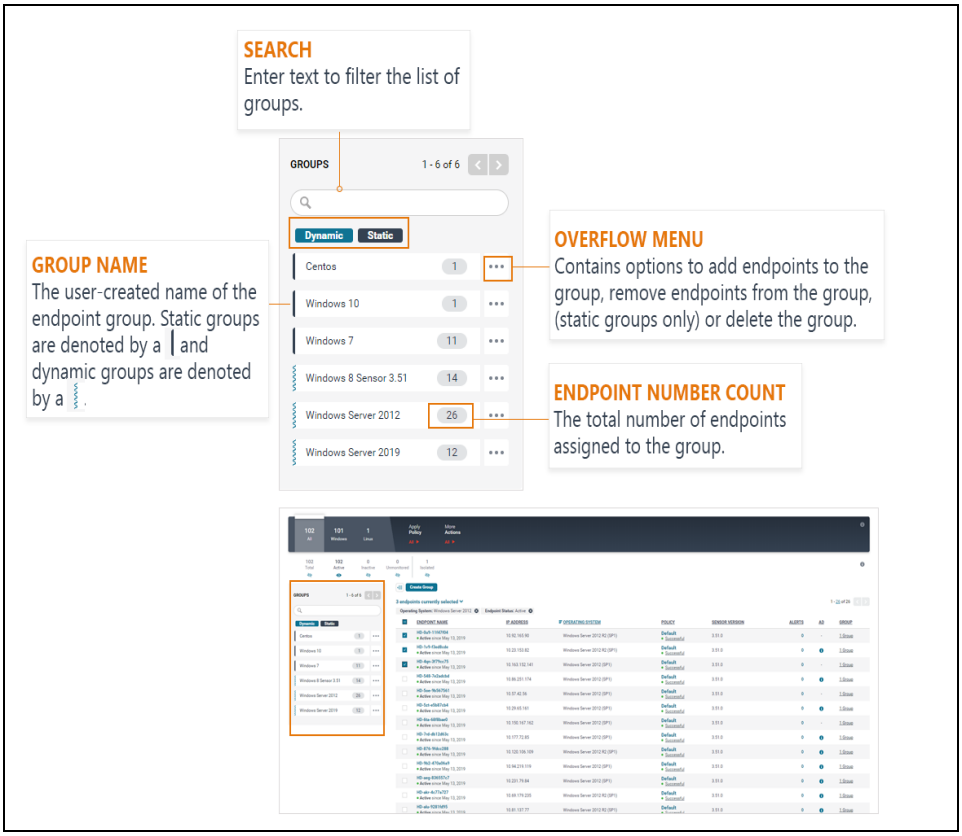
Endpoint Groups Overview

An endpoint group is a label assigned to selected endpoints and enables users to categorize endpoints with similar attributes. Groups assist with endpoint management — especially if there is a large amount of endpoints in your organization — and are useful to execute a task on multiple endpoints simultaneously, or quickly find endpoints with the same criteria. Take the following scenario as an example:

> You are an administrator and have 5,000 endpoints in the Endgame platform. You need to organize endpoints into groups by department (e.g., Sales, Marketing, etc.) and operating system so that you can install security patches on the appropriate machines when needed.

Groups are divided into two categories: static and dynamic. Static groups are based on manual endpoint selection, whereas dynamic groups are based on selected filters that determine which endpoints are included in the group. Any future endpoints added to the Endgame platform that match the filtered criteria — whether they are active or inactive — are automatically added to that dynamic group.

The list of groups appears in the "Groups" panel, located to the left of the Endpoints list. You can create a maximum of 500 groups and can manage them at any time.



Groups panel

Create an Endpoint Group

Create a new static endpoint group when you want to manually select specific endpoints to add to a new group. Create a new dynamic group when you want to select filters to control which endpoints are added to the group. Any new endpoints that match the filtered criteria are automatically added to the dynamic group.

> **NOTE:** Level 2 users and up can create groups. Level 1 users can view groups.

Create a Static Endpoint Group

1. In the Endpoints list, select the box to the left of each endpoint to add to the new group.

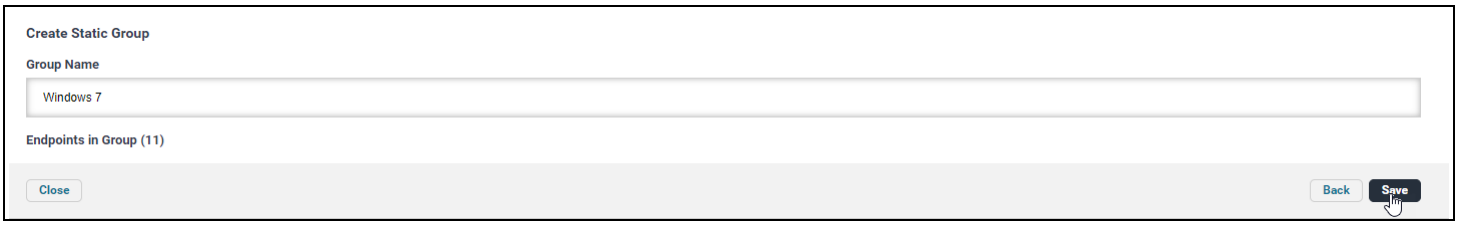
   > **NOTE:** If desired, you can create an empty group and add endpoints to it later. If so, proceed to Step 3 and see "Manage Endpoint Groups" for information about how to add endpoints to a group.

   > **TIP:** If you are selecting endpoints now, it is highly recommended to sort or filter the Endpoints list so that all endpoints you want to group are displayed. For more information, see "Endpoint Dashboard Overview." Also, keep in mind that you can increase the number of endpoints that display per page by selecting the number link in the upper-right corner and entering the desired number, up to 500.
   >
   

2. Select all the appropriate endpoints in the list to add to the group.

   > **TIP:** To select all endpoints on the current page, click the box to the left of the "ENDPOINT NAME" column heading.

3. Click **Create Group** to display the Create Group dialog window.
4. In the "Create Static Group" section, click **Select**.
5. In the "Group Name" text box, enter a unique name for the group.
6. In the "Endpoints in Group" section, ensure the number of selected endpoints is correct.
7. Click **Save**. A "*Group Name* has been created" confirmation appears.



> **NOTE:** If you enter a group name that already exists, an "A group with this name already exists" message appears.

8. Click **Close**. The new group appears in the Groups panel.

Create a Dynamic Endpoint Group

1. Filter the Endpoints list with all the appropriate criteria for the group you are creating.
2. Click **Create Group** to display the Create Group dialog window.
3. In the "Create Dynamic Group" section, click **Select**.
4. In the **Group Name** text box, enter a unique name for the group.
5. In the "Select filters" section, ensure the filters you applied are correct. Once the dynamic group is created, you cannot edit the filters unless you delete and recreate the group.

> **NOTE:** If you have applied any unsupported filters (i.e., policy status, endpoint status, alerts) those appear in the "Unsupported Filters" section and are not applied to the dynamic group. However, keep in mind that unsupported filters are still applied to the current Endpoints list view; therefore, it is possible that the dynamic group will include more endpoints than what is displayed on the page.

6. Click **Save**. A "*Group Name* has been created" confirmation appears.

7. Click **Close**. The new group appears in the Groups panel.

Manage Endpoint Groups

The Group panel provides options to add, delete, and filter groups for easy endpoint management.

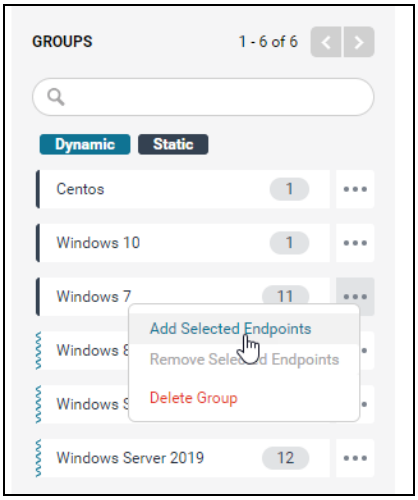
> **NOTE:** You cannot add or delete endpoints from dynamic groups since they are based on previously applied filters.

Add Selected Endpoints to a Static Group

1. In the Endpoints list, select the box to the left of each appropriate endpoint for which to add a group.
2. In the Groups panel, locate the group for which to add selected endpoints.

> **TIP:** If you have a large number of groups, type some text in the search bar to filter the list.

3. Click the **Overflow** menu ••• , then select **Add Selected Endpoints**. The new total number of endpoints in the group is reflected in the number count.



Groups panel in the Endpoints list

Remove Selected Endpoints from a Static Group

Removing endpoints from a group does not delete the group in its entirety; it solely disassociates the endpoint from that group.

To remove one or more endpoints from a static group:

1. Locate the group from which to remove the endpoint, then click the group name to filter the Endpoints list by that group.

> **TIP:** If you have a large number of groups, use the search bar to filter the list.

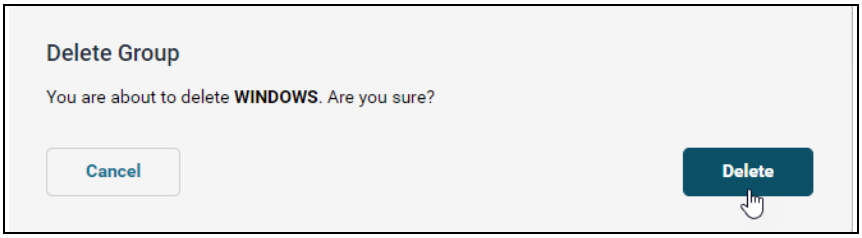
2. In the Endpoints list, select the box to the left of each appropriate endpoint to remove from the group.
3. On the Groups panel, click the **Overflow** menu ⋯, then select **Remove Selected Endpoints**. The new total number of endpoints in the group is reflected in the number count.

Delete an Endpoint Group

Deleting an endpoint group removes it from the Endgame platform, and, therefore, and removes the group relation of any assigned endpoints. If you want to remove an endpoint from a group but retain the group in the platform, see "Remove Selected Endpoints from a Static Group" in this topic.

To delete a group:

1. On the row that contains the group to delete, click the **Overflow** menu ⋯, then select **Delete Group**.
2. In the dialog box that says, "You are about to delete *group name*. Are you sure?" click **Delete**. A "Successfully deleted Group" confirmation appears.



3. Click **Finish**.

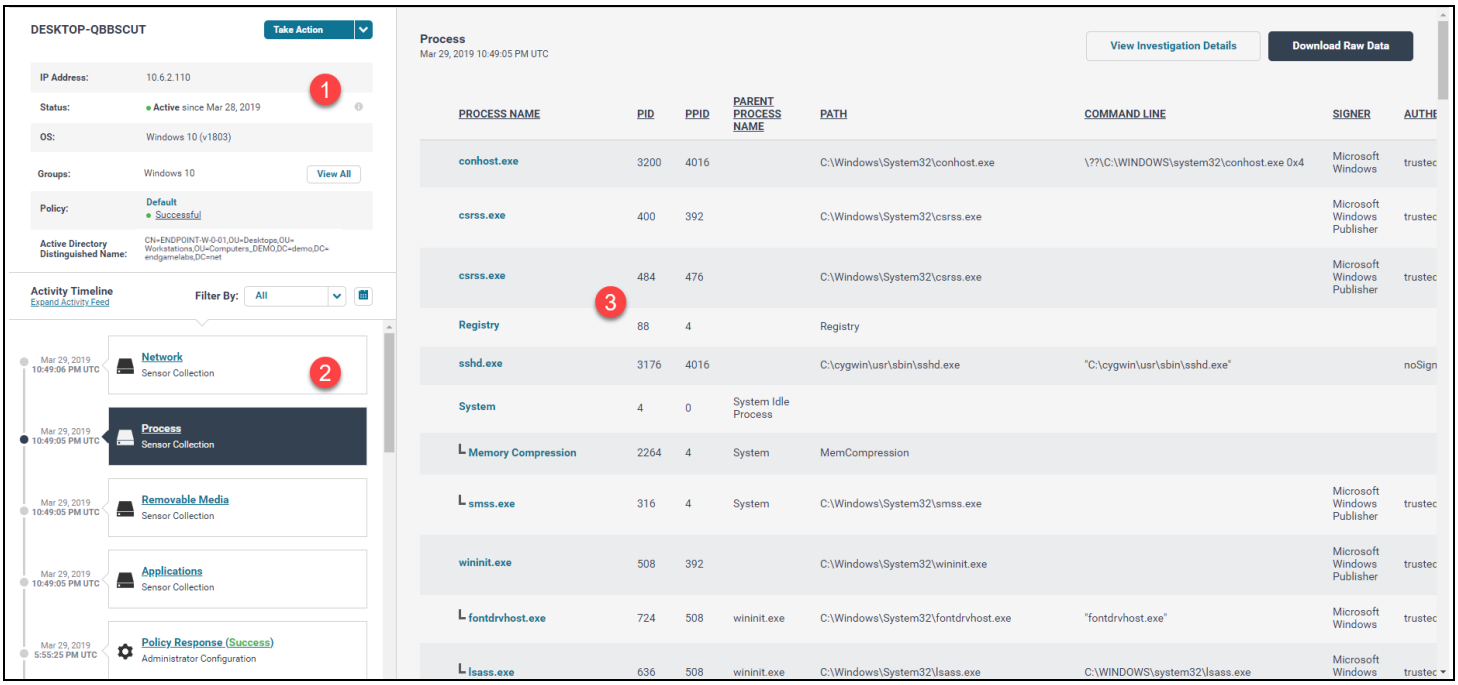
Endpoint Details Page Overview

The Endpoint Details page provides comprehensive details of the selected endpoint that enable you to analyze overall sensor health, view activity that occurred on the endpoint, and find specific data. The page is composed of two panes; the left pane contains the Endpoint Overview and Activity Timeline, and the right pane displays event details.

To view an Endpoint Details page, click an endpoint in the Endpoints list.

The page has three sections:

1. Endpoint Overview
2. Activity Timeline
3. Activity Details pane



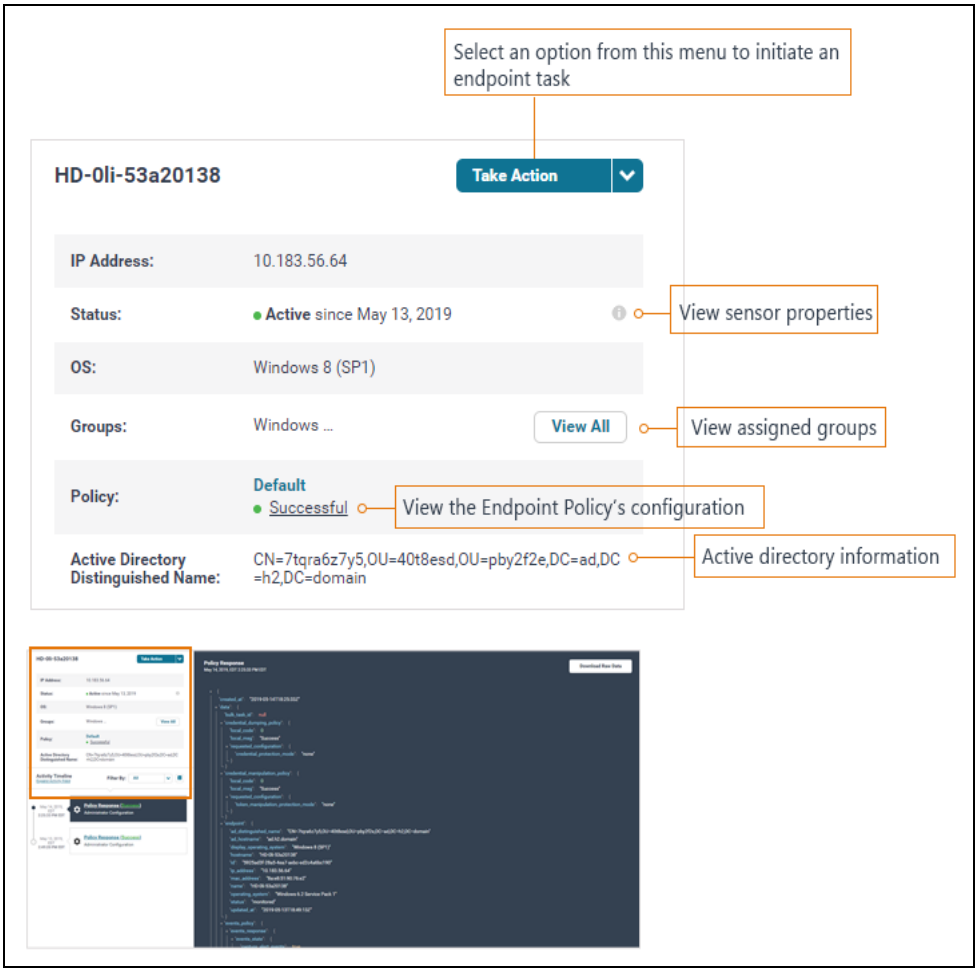
Endpoint Details page

Endpoint Overview

The Endpoint Overview section displays general information about the endpoint, including the name, IP address, status, operating system, associated Endpoint Policy, and if applicable, Active Directory information and assigned groups.

The **Take Action** menu contains a list of options that enable you to execute one of the following endpoint tasks:

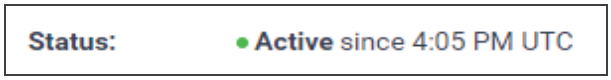
Menu Option	Description
Start Investigation	Starts a new investigation.
Respond	Executes an endpoint response.
Apply Policy	Applies a different Endpoint Policy to the current endpoint.
Uninstall	Uninstalls the sensor and the endpoint from the platform.
Delete Endpoint	Deletes the endpoint from the platform, but retains the sensor.



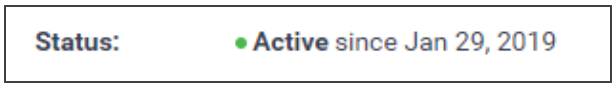
Endpoint Overview section

About Sensor Activity Status

If a sensor's status changes within 24 hours from the time the page is viewed, the user interface displays the time the status took effect:



After 24 hours have passed, the date the status took effect displays in MM DD, YYYY format:



NOTE: If you want to see the exact time the status took effect after the 24-hour time period has passed, hover your cursor towards the right of the date stamp.

Activity Timeline

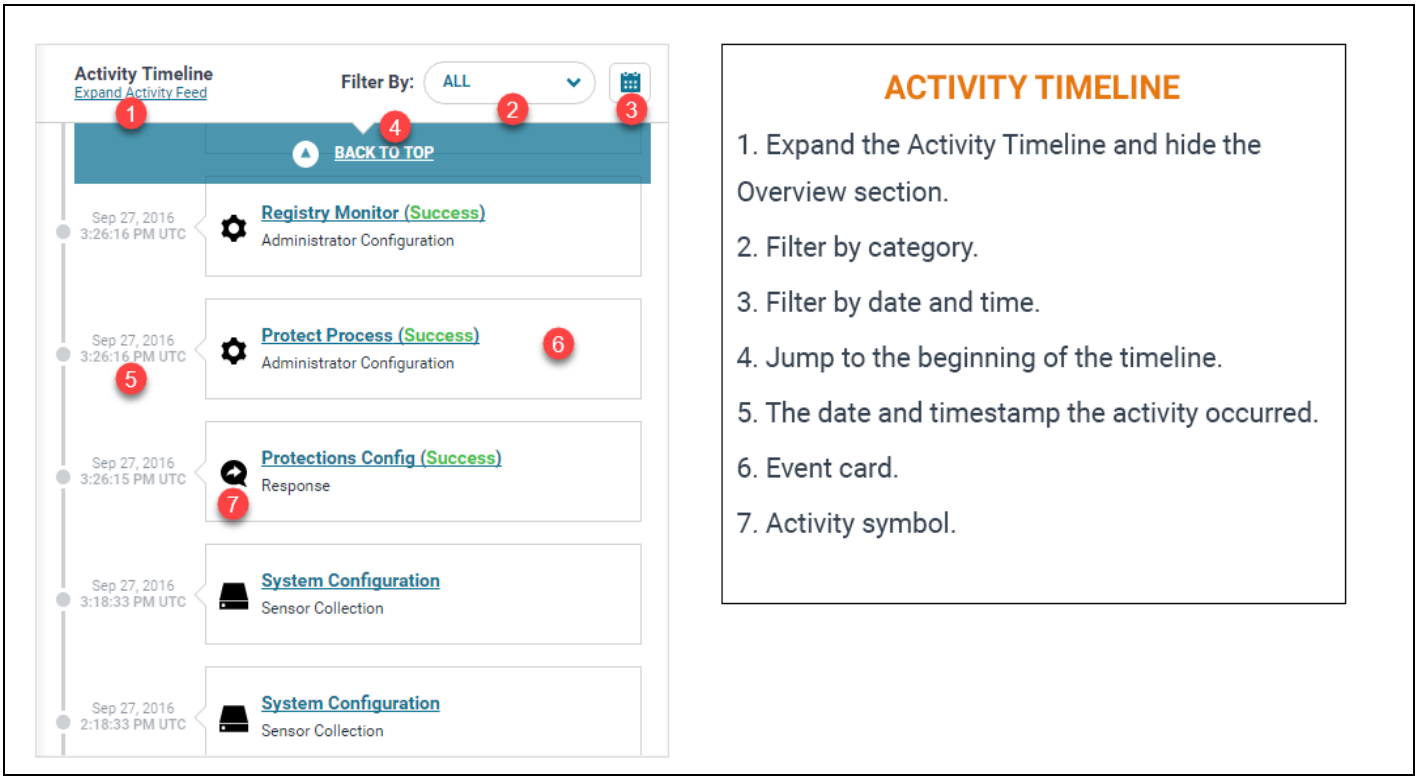
The Activity Timeline chronologically lists every activity that occurred on the endpoint, with the most recent activity at the top. Some endpoint activities in the timeline may include:

- Completed hunts for an investigation
- Sensor installs and uninstalls
- Alert detections and preventions
- Executed response actions (e.g., Get File, Download File, etc.)
- Administrative actions (e.g., Endpoint Policy changes)

NOTE: By default, the System Configuration hunt runs once an hour on all monitored endpoints.

Each timeline entry is called an **event card**. Each event card displays the activity type (e.g., collection, alert, response, etc.), a symbol that identifies the activity type, and the date and time the activity occurred.

Depending on the activity type, an event card may also display supplemental information in red or green type. For example, an event card for a detection indicates the severity level, or an event card for an executed endpoint response (e.g., kill process) indicates if it was a success or failure.



Activity Timeline

Scroll the timeline to view the history of all endpoint activity. It is recommended you pay close attention to any anomalies that may require further investigation. If any new activity is recorded while you scroll the timeline, a notification displays the number of new items. Click **BACK TO TOP** to go to the beginning of the timeline.

TIP: Click **Expand Activity Feed** to hide the Endpoint Overview section.

Filter the Activity Timeline

Although the timeline displays all endpoint activity, you can filter the timeline to specific criteria.

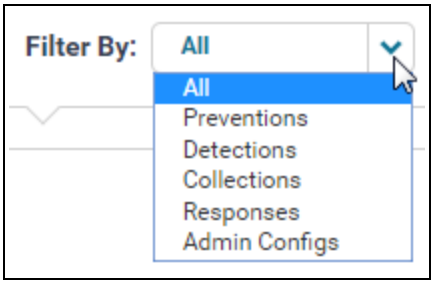
Filter by Category

In the timeline, endpoint activities are separated into six categories, each denoted by a distinct symbol:

Category	Symbol	Description
ALL	N/A	All activity types.
Preventions		Malicious activities that were detected and blocked.

Category	Symbol	Description
Detections		Potential malicious activities that were detected and require resolution.
Collections		Data returned from a hunt (e.g., process survey, network survey, etc.).
Responses		Response actions executed on an endpoint (e.g., delete file, execute file, etc.).
Admin Configs		Sensor configuration set by an administrator.

To filter the timeline by a specific category, click the **Filter By:** drop-down arrow and select the appropriate category from the list.

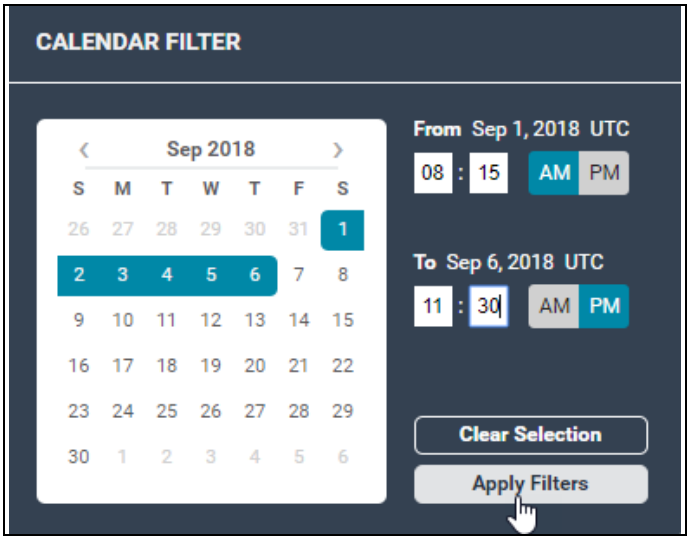


Activity Timeline filter

Filter by Date and Time

To filter the timeline by a date and time range:

1. In the **Filter By:** field, click the **Calendar** button  .
2. Select a start date from the calendar widget that appears. Use the **<** and **>** arrows to navigate to previous and following months.
3. To specify a starting time other than the default 12:00 AM UTC, place your cursor in each text box and enter the appropriate time in HH:MM format. Select **AM** or **PM**.
4. Specify an end date and time using the same procedure in steps 2 and 3.
5. Click **Apply Filters** to update the timeline.

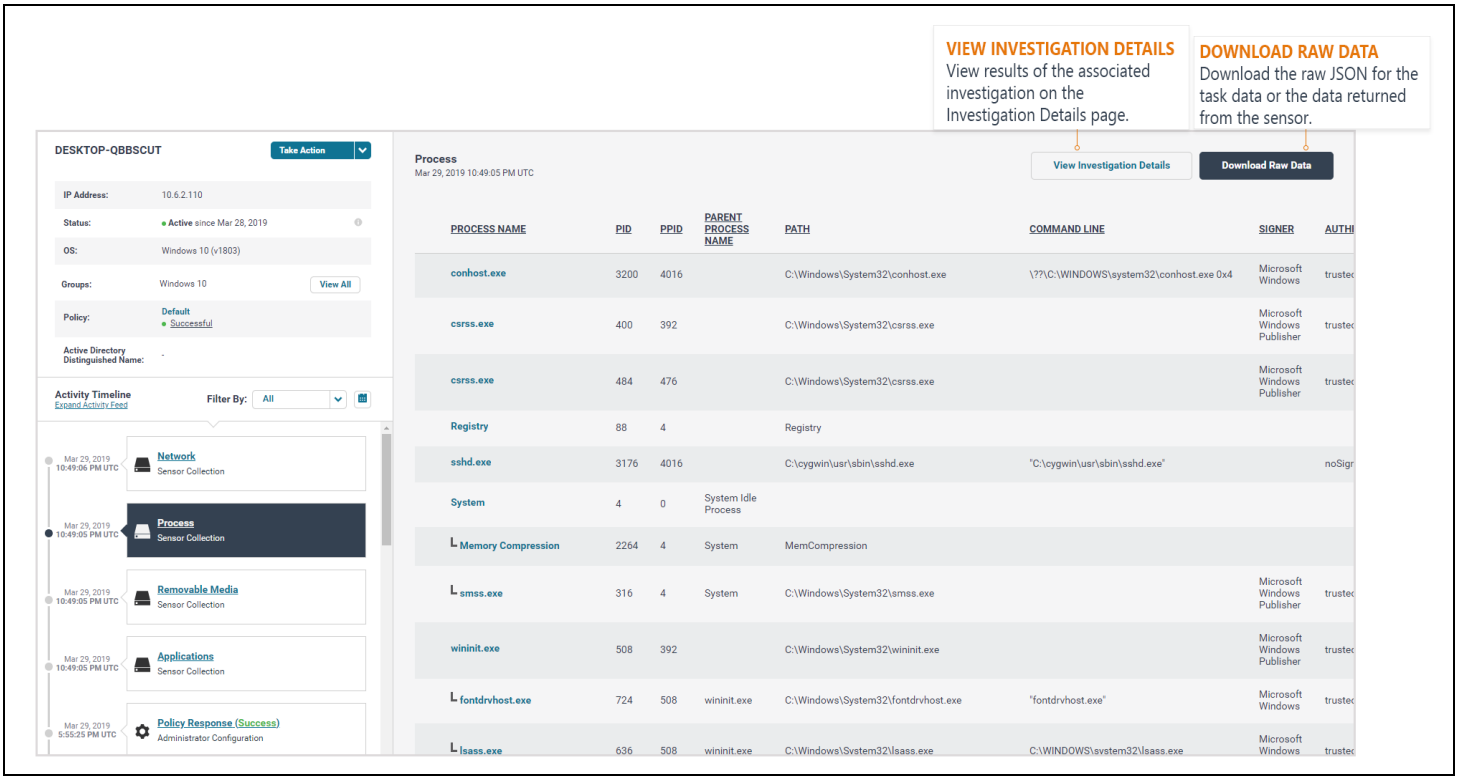


Activity Timeline date and time filter

Activity Details Pane

The Activity Details pane displays all-inclusive details about the selected activity in the timeline. The pane also provides options to view investigation details, download the raw JSON, and, for specific hunts, execute an endpoint response.

> **NOTE:** Some activities — such as IOC Search and administration configurations — display the raw JSON in the details pane. You can download this raw JSON by clicking **Download Raw Data** > **RAW TASK DATA**.



Activity Details pane

View Investigation Details

The **View Investigation Details** button in the upper-right corner navigates to the Investigation Details page to display results of the associated investigation. This button is only available when you select a hunt in the timeline.

> **NOTE:** IOC Search and System Configuration hunts do not have an Investigation Details view. Although the **View Investigation Details** button is available for IOC Search collections (it is not available for System Configuration hunts), if you click it, IOC Search does not appear in the hunt type selection list. However, if IOC Search is the sole hunt in the investigation and you click **View Investigation Details**, a message that says, "View results for this Hunt in search" appears. Click this link to view IOC Search results on the general search page.
> For more information, see "IOC Search Overview."

Download Raw Data

The **Download Raw Data** button enables you to either download the raw task data, which is the data for the task initiated by the sensor, or the raw response data, which is the data returned from the sensor.

To download the raw JSON:

1. Click **Download Raw Data** in the upper-right corner, then select **RAW TASK DATA** or **RAW RESPONSE DATA** from the menu.
2. Open the file in an external application or save it to a directory.

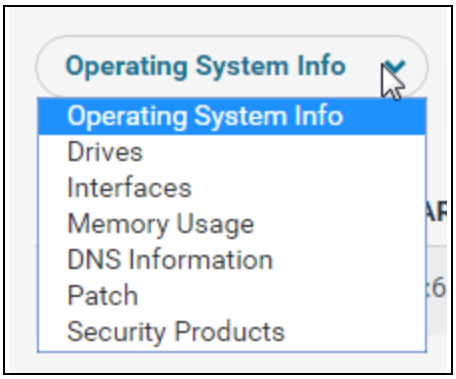
> **TIP:** To see the advanced configuration for a specific hunt, filter the timeline by "Collections," select the appropriate activity, then download the raw task data.

View Corresponding Collections

Some hunts, which appear as collections in the timeline, have one or more corresponding collections — distinct snapshots of specific data. For example, **System Configuration** has collections that display the drives, interfaces, memory usage, DNS and patch information.

To view a corresponding collection:

- In the details pane, click the Hunt arrow (e.g., Operating System Info, Network, etc.) and select the appropriate collection from the list.

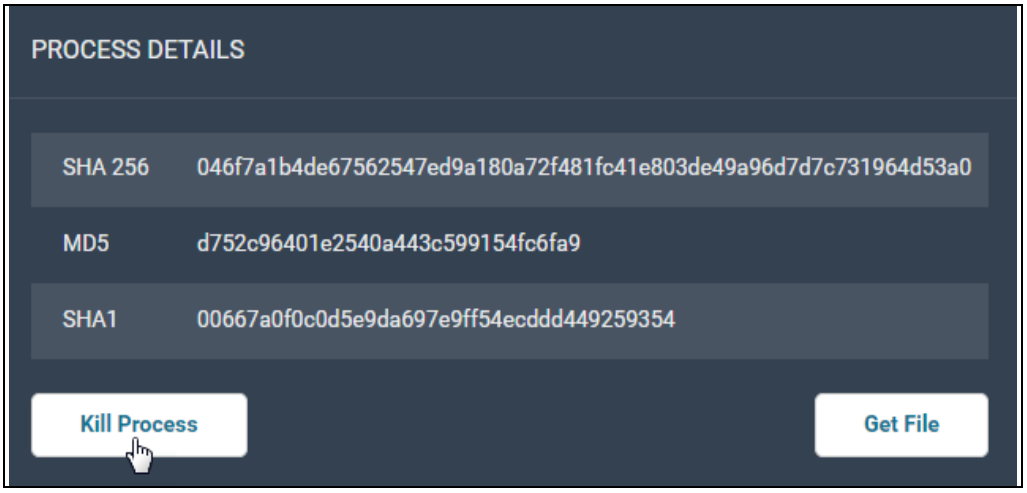


System Configuration collections view

Execute an Endpoint Response

For Process and Network hunts, which identify running processes, you can terminate a process or download a file directly from the details pane:

1. In the "PROCESS NAME" column, select the appropriate process for which to kill or download a file.
2. In the "PROCESS DETAILS" window, select **Kill Process** or **Get File**.
3. In the dialog box that asks if you are sure you would like to kill the process or download the file, click **Yes**. If you chose **Get File**, a "Get File submitted" message appears to confirm the file was downloaded. If you chose **Kill Process**, a "Kill Process submitted" message appears to confirm the process was terminated.
4. Click **Finish**.



Kill Process response from the details pane

Endpoint Responses Overview

Endpoint responses enable you to execute individual tasks for multiple endpoints simultaneously. For example, if you found a suspicious file running on a group of endpoints, you could initiate a Delete File response to remove the file from the

appropriate endpoints. Or, if you received an alert notification for a detected process injection, you could initiate a Kill Process response to terminate the malicious process.

To execute an endpoint response:

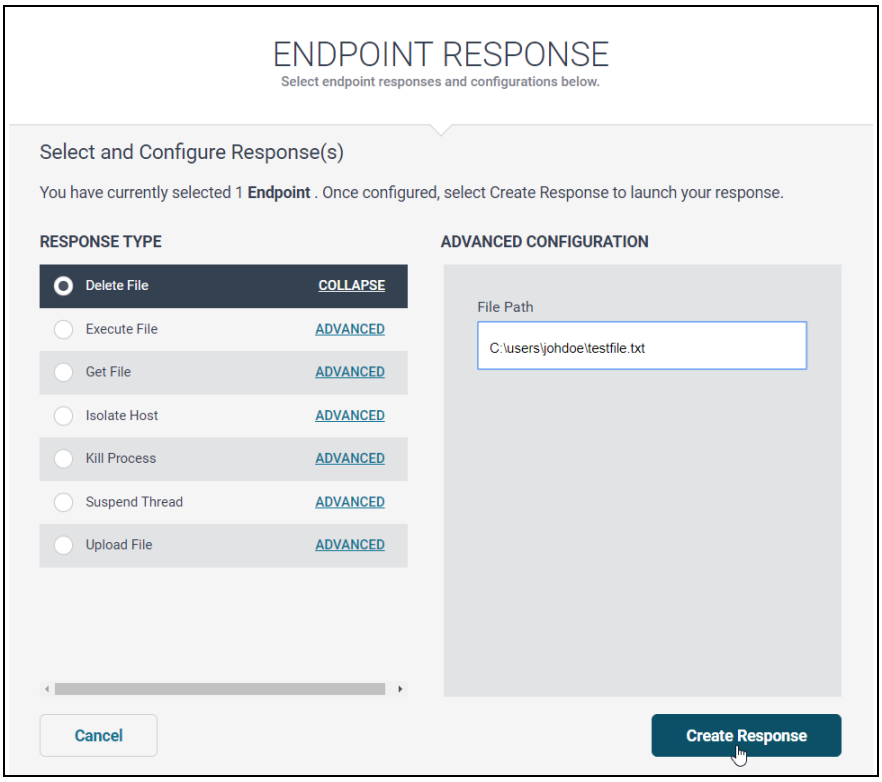
In the Endpoints list, select the box to the left of each appropriate endpoint.

1. On the **Action toolbar**, point to **More Actions**, then click **Respond**. An alphabetical list of response types appears.

   For complete descriptions of response types, see "Endpoint Response Types and Advanced Configuration Options."

2. In the left column, click the option button to the left of the response to execute.
3. In the right column, enter advanced configuration for the selected response. Advanced configuration options vary according to the response type, therefore, to ensure accuracy, review all options and enter property values accordingly.
4. Click **Create Response**.

   NOTE: If any required property values are missing, you cannot execute the response until those values are entered.

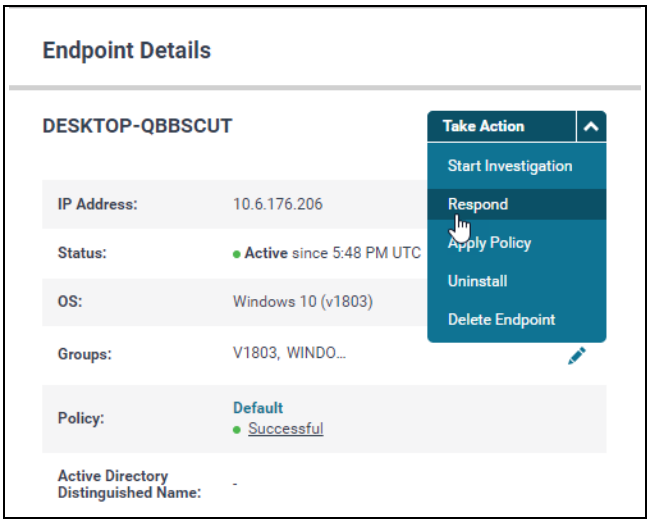


Delete File endpoint response

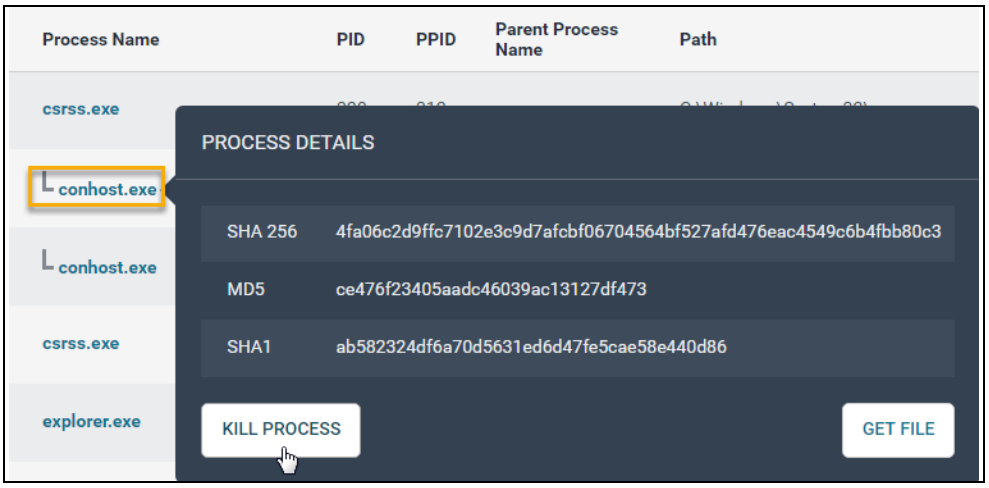
Additional Ways to Execute an Endpoint Response

You can also initiate an endpoint response by choosing from the following options:

- On the Endpoint Details page, click **Take Action** in the upper-left corner, then select **Respond**.



- If you are viewing the Endgame Resolver™ Attack Visualization for an alert, you can initiate the **Retrieve File** (equivalent to Get File) or **Kill Process** response. Some alerts also contain the Retrieve File, Download File, and Kill Process responses on the **Take Action** menu on the Alert Metadata panel.
- Display results of a Process or Network hunt in the Activity Details pane, select a process name, and then choose a response action in the **PROCESS DETAILS** dialog box.



Host Isolation Overview

Isolating a host temporarily prevents it from communicating with all systems besides the Endgame platform until the host is released. Isolating a host is useful to prevent malicious activity from spreading, as it blocks adversaries from making lateral movement across other endpoints. However, if necessary, you can allow isolated hosts to connect to specified IP addresses. For more information, see "Allow Isolated Hosts to Connect to Other IP Addresses" in this topic.

Host isolation is only compatible with Windows and macOS endpoints and the following sensor versions:
1) Windows: 3.0 and above
2) macOS: 3.51.6 and above

Isolate a Host

NOTE: To protect unwanted isolation, only Level 3 and Admin users can isolate a host. In addition, you can only isolate one host at a time.

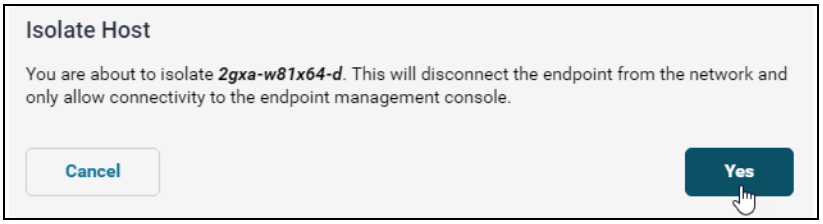
Depending on where you are in the platform, choose one of the following options:

If you are viewing an alert on the Alert Details page:

1. On the Alert Metadata panel, click **Take Action**, then select **Isolate Host** from the list.

   NOTE: Ensure the alert's affected endpoint is the one you want to isolate.

2. On the dialog box that says, "You are about to isolate *endpoint hostname*. This will disconnect the endpoint from the network and only allow connectivity to the endpoint management console" click **Yes**. A "Request successful" message appears.

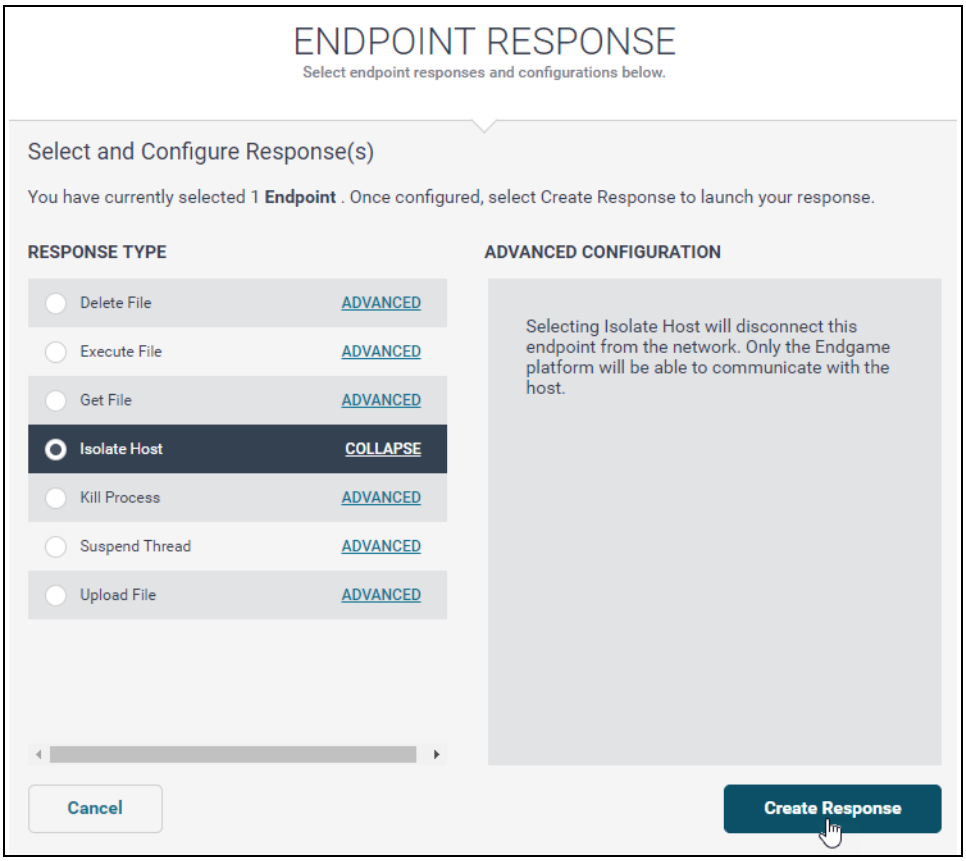


3. Click **Finish** to close the dialog box. To view the sensor response in the endpoint's Activity Timeline, click **Go to Endpoint**.

> **NOTE:** When the sensor initially receives the isolation request, the endpoint status — which is displayed on the Alert Metadata panel and in the Endpoints list — briefly changes to "Isolation Requested" until the isolation is successful, at which point the status changes to "Isolated." For more information, see "View Host Isolation Statuses" in this topic.

If you are viewing the Endpoint Details page:

1. In the Overview section located in the left pane, click **Take Action**, then click **Respond**. An alphabetical list of response types appears.
2. In the left column, click **Isolate Host**, then click **Create Response** in the lower-right corner. A "Responses successfully launched" confirmation appears.
3. Click **Close**.



Isolate host endpoint response

If you are viewing the Endpoint Dashboard:

1. On the Action toolbar, select the **Windows** or **Mac** tab to filter the Endpoints list by those running on the selected operating system.
2. In the Endpoints list, select the box to the left of the endpoint to isolate. Ensure you select only one.
3. On the Action toolbar, point to **More Actions**, then click **Respond**. An alphabetical list of response types appears.

> **NOTE:** If an operating system tab is not selected, the "Respond" option does not appear in the **More Actions** menu.

4. In the left column, click **Isolate Host**, then click **Create Response** in the lower-right corner. A "Responses successfully launched" confirmation appears.
5. Click **Close**.

> To filter the Endpoints list by isolated hosts, select the **Isolated** tab on the Action toolbar.

Release a Host

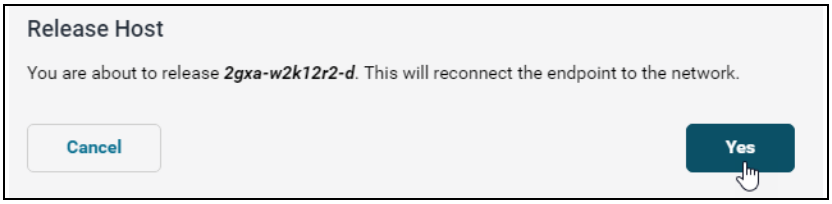
Releasing a host reestablishes communication between the host and other network-connected endpoints.

To release a host:

Depending on where you are in the platform, choose the appropriate option below:

If you are viewing an alert on the Alert Details page:

1. On the Alert Metadata panel, click **Take Action**, then click **Release Host**.
2. On the dialog box that says, "You are about to release *endpoint hostname*. This will reconnect the endpoint to the network." click **Yes**. A "Request successful" message appears.

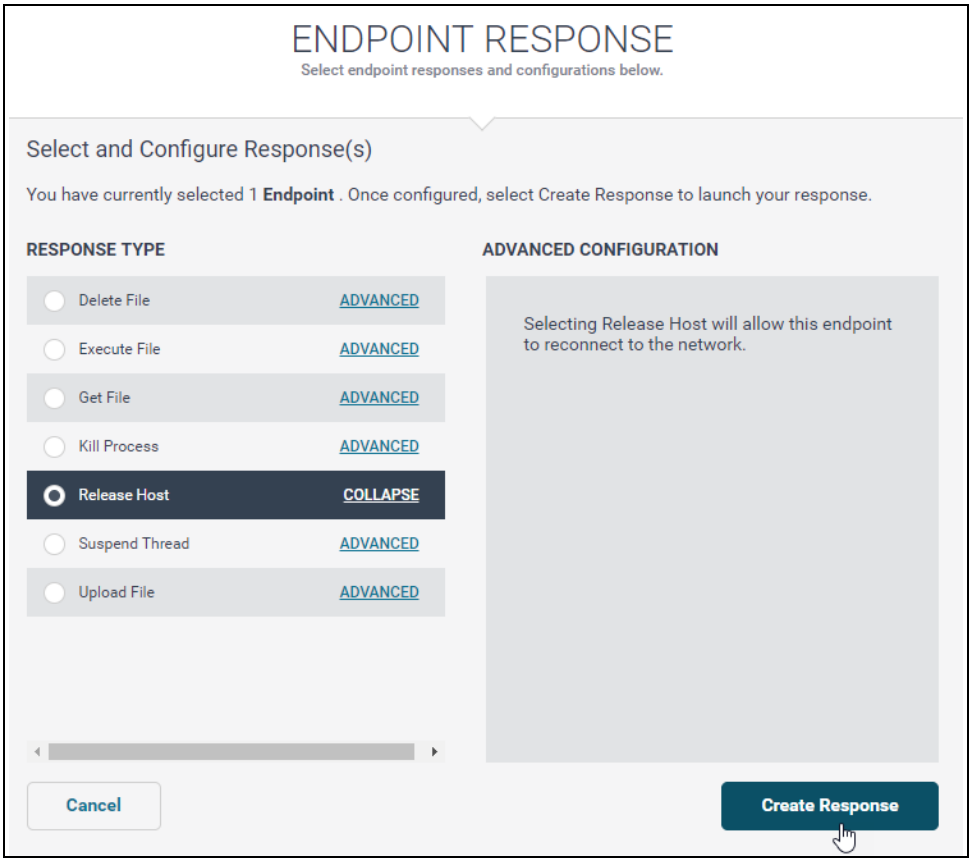


3. Click **Finish** to close the dialog box. To view the sensor response in the endpoint's Activity Timeline, click **Go to Endpoint**.

If you are viewing the Endpoint Details page:

1. In the Overview section, located in the left pane, click **Take Action**, then select **Respond** from the list. An alphabetical list of response types appears.

2. In the left column, click **Release Host**, then click **Create Response** in the lower-right corner. A "Responses successfully launched" confirmation appears.
3. Click **Close**.



Release host endpoint response

If you are viewing the Endpoint Dashboard:

1. On the Action toolbar, select the **Windows** or **Mac** tab to filter the Endpoints list by those running on the selected operating system.
2. In the Endpoints list, select the box to the left of the endpoint to release from isolation. Ensure you select only one.
3. On the Action toolbar, point to **More Actions**, then click **Respond**. An alphabetical list of response types appears.

> **NOTE:** If an operating system tab is not selected, the **Respond** option does not appear in the **More Actions** menu.

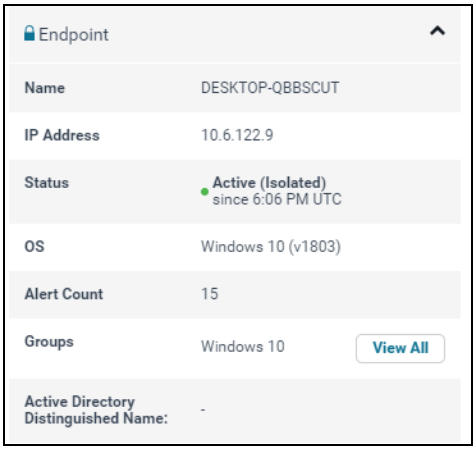
4. In the left column, click **Release Host**, then click **Create Response** in the lower-right corner. A "Responses successfully launched" confirmation appears.
5. Click **Close**.

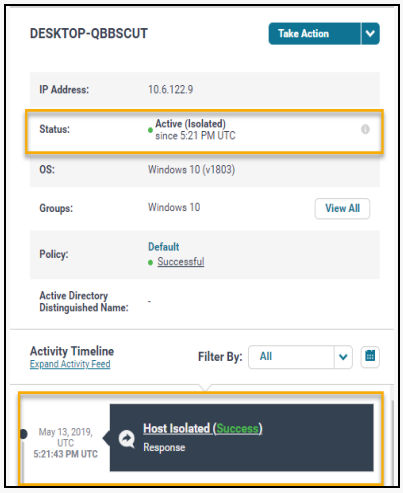
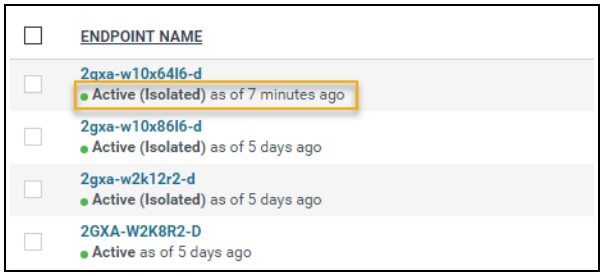
View Host Isolation Statuses

When the sensor receives a host isolation or release request, Endgame displays one of the following endpoint statuses throughout various places in the Endgame platform to indicate the progress:

Host Status	Description
Isolation Requested	The Endgame platform sent an 'isolate host' task to the sensor.
Isolated	The host is isolated and, therefore, can only communicate with Endgame.
Release Requested	The Endgame platform sent a 'release host' task to the sensor.
Released	The host has been released from isolation and, therefore, can communicate with network-connected endpoints.
Isolation Failed	The sensor was unable to isolate the host.
Release Failed	The sensor was unable to release the host.

The following table lists the locations in the platform where the "Released" and "Isolated" statuses are displayed:

Platform Location	Example
Alert Metadata panel	 An "Isolated" status is also denoted by a lock button next to the Endpoint section header. 

Platform Location	Example
Endpoint Details page (visible in the "Overview" section and Activity Timeline)	
Endpoints list	

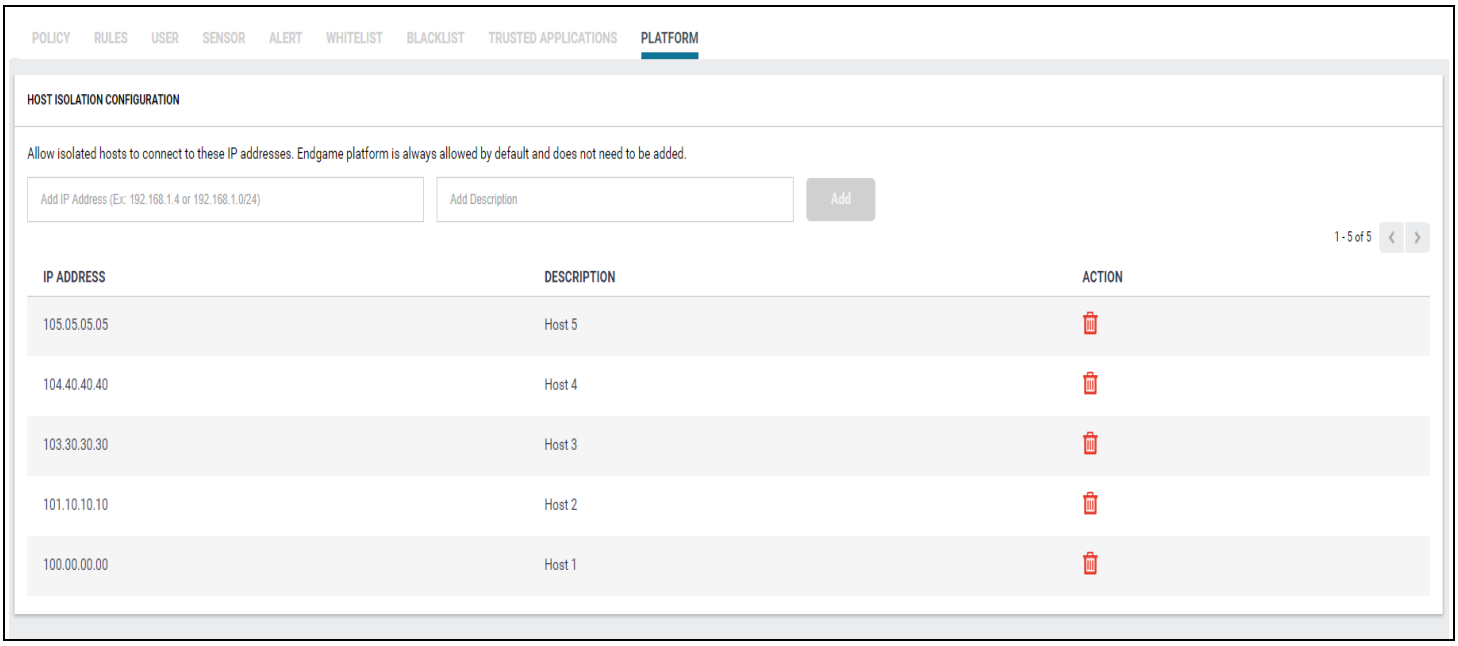
Allow Isolated Hosts to Connect to Other IP Addresses

When hosts are in an isolated state, communication to the Endgame platform remains enabled. However, if those isolated hosts need to establish an outbound connection to other hosts within their network, administrators can specify which ones are allowed network communication by adding that IP or IP range to a host isolation exceptionlist. This enables analysts to continue to use Endgame to manage endpoints.

To allow an isolated host to connect to an IP address:

1. On the Left Navigation toolbar, click the **ADMINISTRATION** button  .
2. On the Administration page, select the **PLATFORM** tab.
3. In the "Add IP Address" text box located in the **HOST ISOLATION CONFIGURATION** section, type the permissible IP address that can allow communication from an isolated host.
4. In the "Add Description" text box, type a description or note to identify the IP. Ensure the description is no more than 64 characters.
5. Click **Add**.

6. Repeat steps 1-5 to add additional IP addresses. The updated host isolation exceptionlist is immediately applied to all active sensors.

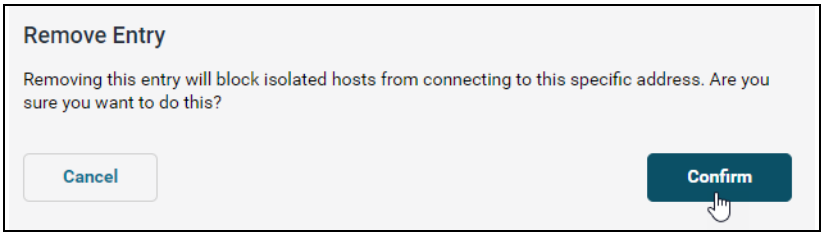


Host isolation exceptionlist

Manage the Host Isolation Exceptionlist

If you entered an incorrect IP address or if a current IP address in the host isolation exceptionlist should no longer allow communication from an isolated host, remove it from the exceptionlist by doing the following:

1. In the host isolation exceptionlist, locate the appropriate IP address to delete. In the corresponding **ACTION** column, click the **Delete** button .
2. In the dialog box that says, "Removing this entry will block isolated hosts from connecting to this specific address. Are you sure you want to do this?" click **Confirm**. An "Entry successfully deleted" confirmation appears and the updated host isolation exceptionlist is immediately applied to all active sensors.



Remove an entry from host isolation exceptionlist

3. Click **Finish**.

Endpoint Response Types and Advanced Configuration Options

The following table lists all endpoint response types and their advanced configuration options.

Response Name	Description	Advanced Configuration Options
Delete File	Deletes a file.	**File Path:** Type the path of the file to delete. **NOTE:** Ensure the path is correct. The file will not delete if the path does not match the file location.
Execute File	Executes a file.	**File Path:** Type the path of the file to execute. **Max Time:** (Seconds) Enter the maximum number of seconds the file execution process should run before collecting the output. • **Collect Output:** Select this option to capture the command line output. • **Delete After Execution:** Select this option to permanently delete the file after execution. **Arguments:** To enter command-line arguments to run with the executed file, type them in the text box.
Isolate Host	Isolates the endpoint to prevent it from communicating with all systems.	N/A
Get File	Retrieves a file from the endpoint to the platform.	**File Name:** Type the path of the file to download. **NOTE:** After this task is executed, you must download the file from the Endpoint Details page, which is in a password-protected zip file. The password is set to "dangerous."
Kill Process	Terminates a process by process ID, name, or file path.	Enter at least one of the following: **Process ID: (Single Endpoint Only):** Enter the process ID to terminate. **Process Name:** Type the name of the executable to terminate. **File Path:** Type the full file path of the process to terminate.

Response Name	Description	Advanced Configuration Options
Release Host[1]	Releases the endpoint from isolation, allowing it to communicate with all systems.	N/A
Suspend Thread[2]	Suspends a malicious process thread by thread ID.	**Thread ID:** Enter the thread ID to suspend. **NOTE:** Thread IDs are unique to individual endpoints, therefore, you can only suspend one thread at a time.
Upload File	Uploads a file.	**Select File:** Click **Upload File** and select the file to upload from the appropriate directory. **File Path:** Type the file path, including the file name, to specify where the uploaded file should reside on the endpoint. **NOTE:** There is a maximum file size of 16 MB. Only one file can be uploaded and only one file path can be entered at a time. It is critical that the path includes the filename so that you can upload the file to a different name than what is on the local machine. For example, **c:\documents\uploadedfiles** is an invalid path name because it is missing the filename, however, **c:\documents\uploadedfiles\newfile** is a valid path name. If you do not upload a file or if a directory path is incorrect, an error message appears. **Overwrite:** Select this option to overwrite an existing file that contains the same filename.

[1]Release Host appears in the list only if the endpoint has been isolated.

[2]Suspend Thread is only compatible with Windows.

Delete an Endpoint

Deleting an endpoint first uninstalls the sensor from the endpoint, then removes the endpoint from the Endgame platform.

> You can uninstall the sensor but retain the endpoint in the Endgame platform. For more information, see "Uninstall a Sensor" in the *Administrator's Guide*.

To delete an endpoint(s):

1. In the Endpoints list, select the box to the left of each appropriate endpoint.
2. On the **Action toolbar**, point to **More Actions**, then click **Delete**.
3. In the **Delete Endpoint(s)** dialog box that says, "Are you sure you would like to delete number endpoint(s)? Deleting an endpoint will first uninstall the sensor and then delete all endpoint records from the system (including alerts)." click **Yes**. An "Endpoints successfully deleted" message appears.
4. Click **Finish.**

To delete a single endpoint from the Endpoint Details page, click **Take Action**, then select **Delete Endpoint**.

CHAPTER 3

INVESTIGATIONS

Investigations Overview

An investigation is a custom search that collects and analyzes targeted data across multiple endpoints. It is created by assigning one or more hunts to selected endpoints. The main goals of an investigation are to identify suspicious activity and take remedial action before damage and loss occurs.

Results of the investigation are displayed on the Investigation Details page. It contains an interactive tool, similar to a pivot table, that shows all data collected across selected endpoints. It also discovers unknown IOCs (indicators of compromise) by identifying anomalies and enabling the user to filter data by tailored analytics.

> If you received an alert notification, it is recommended you start an investigation to determine if there was an attempted compromise and to identify additional areas in the current environment that also may have been compromised. You can only start an investigation for endpoints running on the same operating system.

Start an Investigation

The procedure for starting an investigation consists of three steps:

1. Select endpoints to include in the investigation.
2. Select and configure hunts.
3. Launch the investigation.

> **NOTE:** You can only create a single investigation for endpoints that run on the same operating system. For example, you cannot create an investigation that contains both Windows and Linux endpoints.

To start an investigation:

1. On the Left Navigation toolbar, click the **ENDPOINTS** button  .
2. On the Action toolbar, select an operating system tab (i.e., Windows, Linux, or Solaris) to filter the Endpoints list.
3. Select the box to the left of each endpoint to include in the investigation.

> **TIP:** Apply KPI filters as necessary to narrow the Endpoints list, or click the **Currently Selected** drop-down arrow and choose a bulk selection option. It is also recommended you create hunts for endpoints with active sensors; select the **Active** KPI to filter these endpoints.

4. On the Action toolbar, click **Create Investigation**.

> You can also start an investigation from the Endpoint Details page by clicking **Take Action**, then selecting **Start Investigation**. However, if you do, please note you can only create hunts for the current endpoint.

5. Complete the requirements in the **START INVESTIGATION** dialog window:

Step 1: Create an Investigation Profile

This section specifies the name, assignee, and hunts for the investigation.

> **NOTE:** If you have already created and saved an investigation profile, see "Apply an Existing Profile to an Investigation" in this topic.

- **INVESTIGATION NAME** (Optional)**:** In the text box, type a unique name to identify the investigation. If you do not specify a name, Endgame automatically assigns one in the following format: Username + YYYY-MM-DDtime_*time zone*, where YYYY-MM-DD represents the four-digit year, two-digit month, and two-digit day it was created (e.g., Super Admin + 2016-08-31T19:30:57.661614_utc).

> It is recommended to assign the investigation a name to distinguish the current investigation from others. You can use letters, spaces, numbers, and special characters in the text box.

- **ASSIGN TO:** By default, the investigation is assigned to yourself. To assign the investigation to another user:

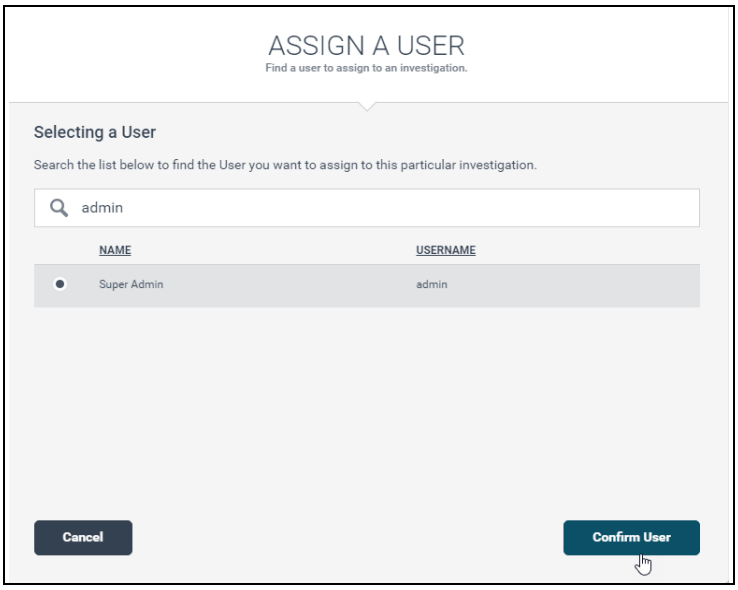
a. Click the **Find User** option button or link. The **ASSIGN A USER** dialog window displays an alphabetical list of all registered users and their designated usernames.

b. Choose one of the following options to locate the appropriate user:

   - In the **Search User Name** text box, begin typing the user's first or last name. The list filters to name(s) that match the entry. If no matching users are found, an "Invalid User" error message appears.
   - Scroll the list and locate the user's name.

c. Click the option button to the left of the appropriate user's name.

d. Click **Confirm User.**



Assign a User dialog window

- **SELECTED HUNTS:** To add and configure hunts:

a. Click **Manage Hunt(s)**. An alphabetical list of available hunt types appears.

b. In the left column, select each hunt to include in the investigation.

c. In the right column, enter advanced configuration for the selected hunt(s). Advanced configuration options vary according to the hunt type; therefore, to ensure accuracy, select all appropriate options and enter property values accordingly.

> **NOTE:** Not all hunts have an advanced configuration. For those that do, some options are selected by default; however, you can clear the selection if desired.
>
> If a required property value is missing, an error message displays the missing property value at the top of the **ADVANCED CONFIGURATION** column. You cannot confirm your hunts until all required values are specified. For a complete list of hunt types and advanced configuration options, see "Hunt Types and Advanced Configuration Options" in this chapter.

> **TIP:** Click ***What's this?*** next to an advanced configuration option to view the description.

d. Click **Confirm Hunts**.

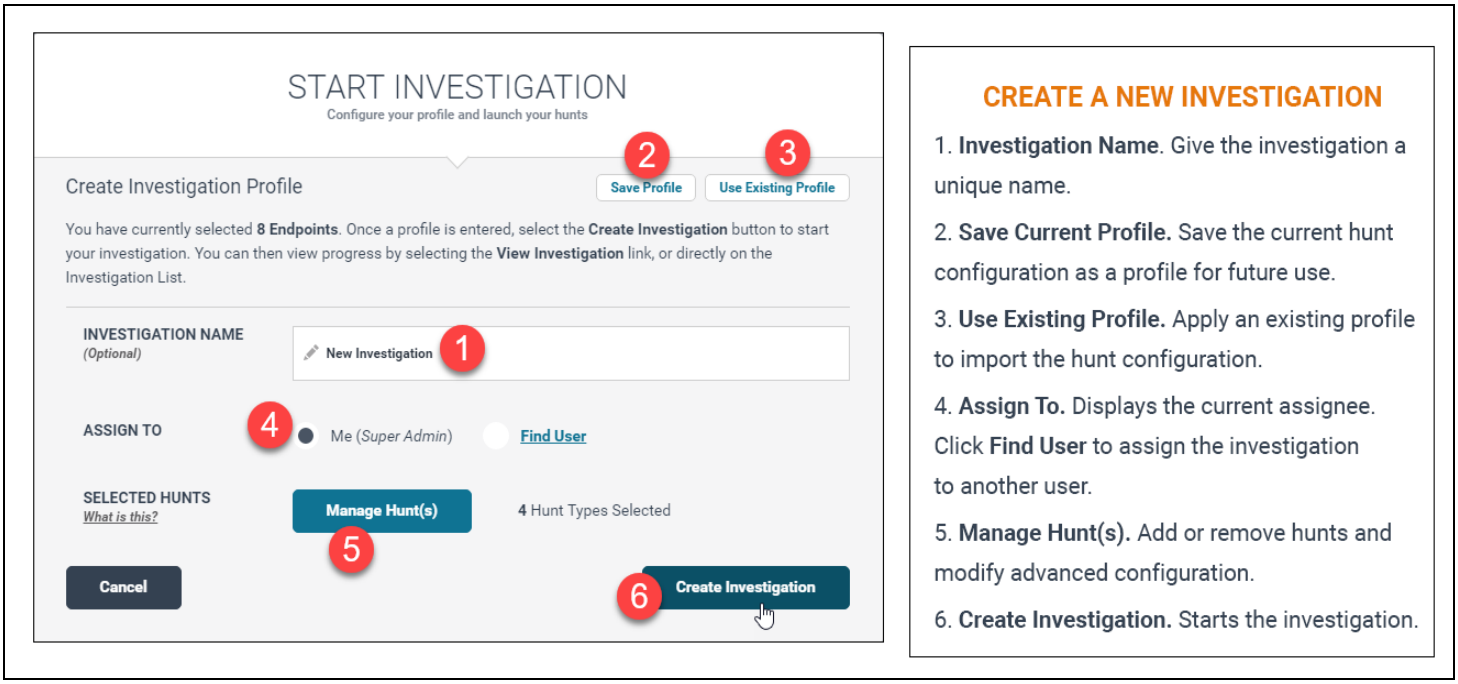
To save the current investigation name and hunt configuration as a profile for future use:

1. Click **Save Profile**. A "Profile created" message appears.
2. Click **Confirm**.

Step 2: Launch Your Hunts

When hunt configuration is complete:

1. Click **Create Investigation**. A "Hunts successfully launched" message appears to confirm the investigation has begun.
2. Click **View Investigation** to go to the Investigation Details page, or click **Close** to close the dialog window.



Start Investigation dialog window

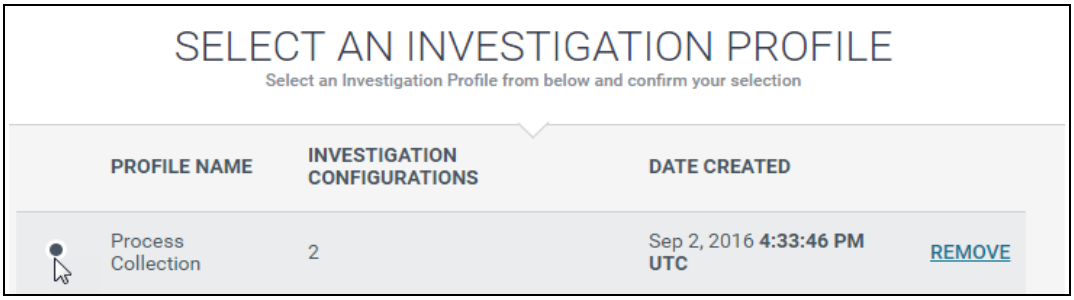
Remember: After you create an investigation, each hunt you selected appears as a separate event in the Activity Timeline.

Apply an Existing Profile to an Investigation

After you have selected which endpoints to include in the investigation, you can import the hunt configuration from a previously saved profile.

To apply a saved investigation profile:

1. Click **Use Existing Profile**.
2. In the Investigation Profiles list, click the option button to the left of the appropriate profile name.
3. Click **Confirm Profile**. The profile imports the investigation name, hunt configuration, and assignee.



Apply an existing profile

> **TIP:** To overwrite the existing investigation name, select the current name and replace it with new text. This is recommended if you do not want to confuse the current investigation with an existing one.

Manage Hunt Selection and Configuration

If necessary, you can modify or reconfigure selected hunts before you start the investigation.

To remove or reconfigure a hunt(s) from the investigation:

1. Click **Manage Hunts**. In the Hunt Types list that appears, previously configured hunts are selected.
2. Select or clear hunt types and edit advanced configuration as necessary.
3. Click **Confirm Hunts** to update the configuration.

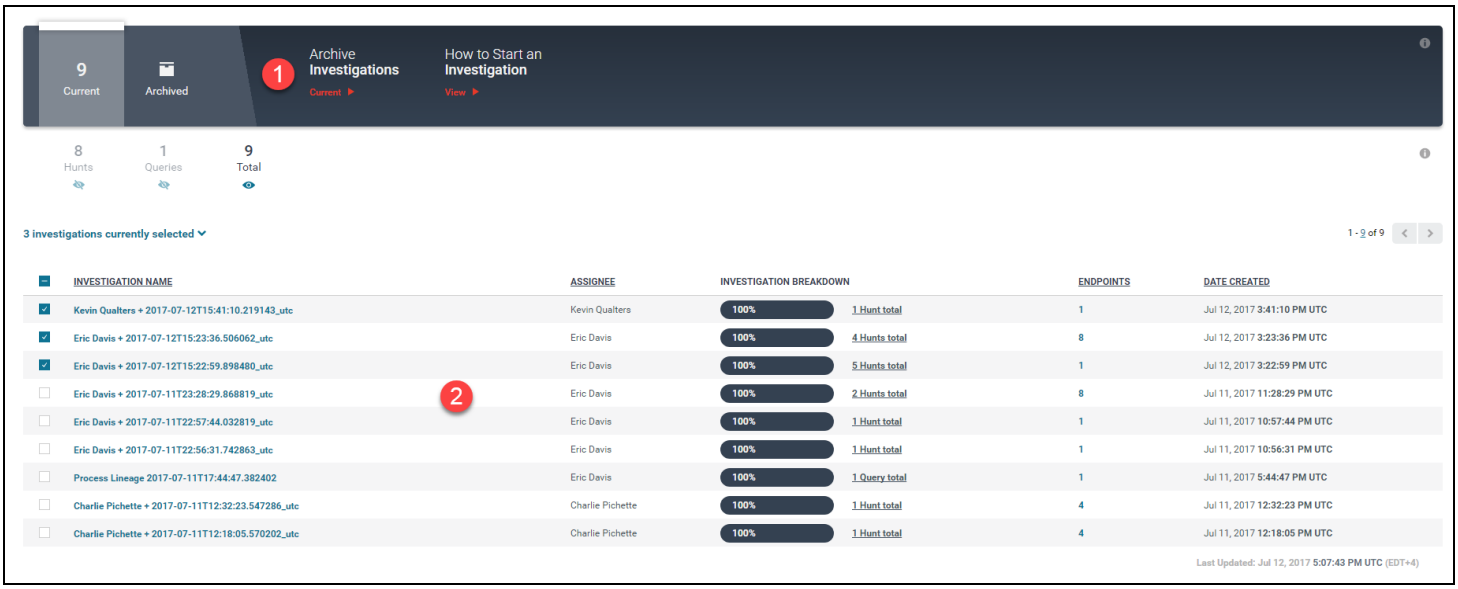
Investigation Dashboard Overview

The Investigation Dashboard displays essential details about all created investigations, gives an overall progress status of each one, and provides options to view, filter, and manage them.

To view the Investigation Dashboard, click the **INVESTIGATIONS** button on the Left Navigation toolbar.

The dashboard contains two sections:

1. Action toolbar
2. Investigations list

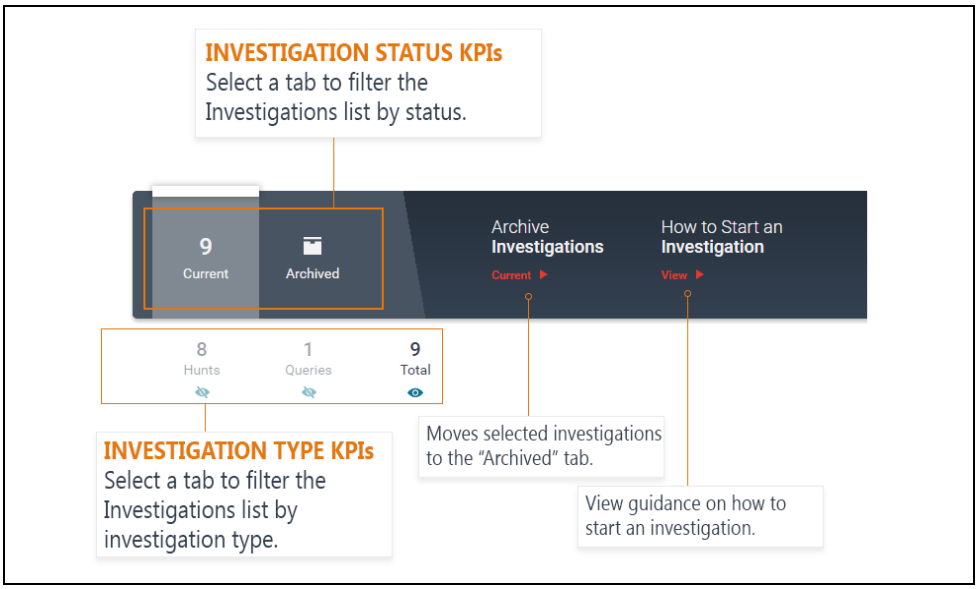


Investigation Dashboard

Action Toolbar

The Action toolbar contains two KPIs that filter the Investigation Dashboard by two views: **Current**, which displays by default, and **Archived**. By default, all investigations are current until they are archived. The Action toolbar also enables you to archive selected investigations and provides guidance on how to start an investigation.

> For more information about archiving investigations, see "Archive an Investigation" in this chapter.



Action toolbar on the Investigation Dashboard

Beneath the toolbar, a secondary set of KPIs displays the number of investigations that fall within a specific category:

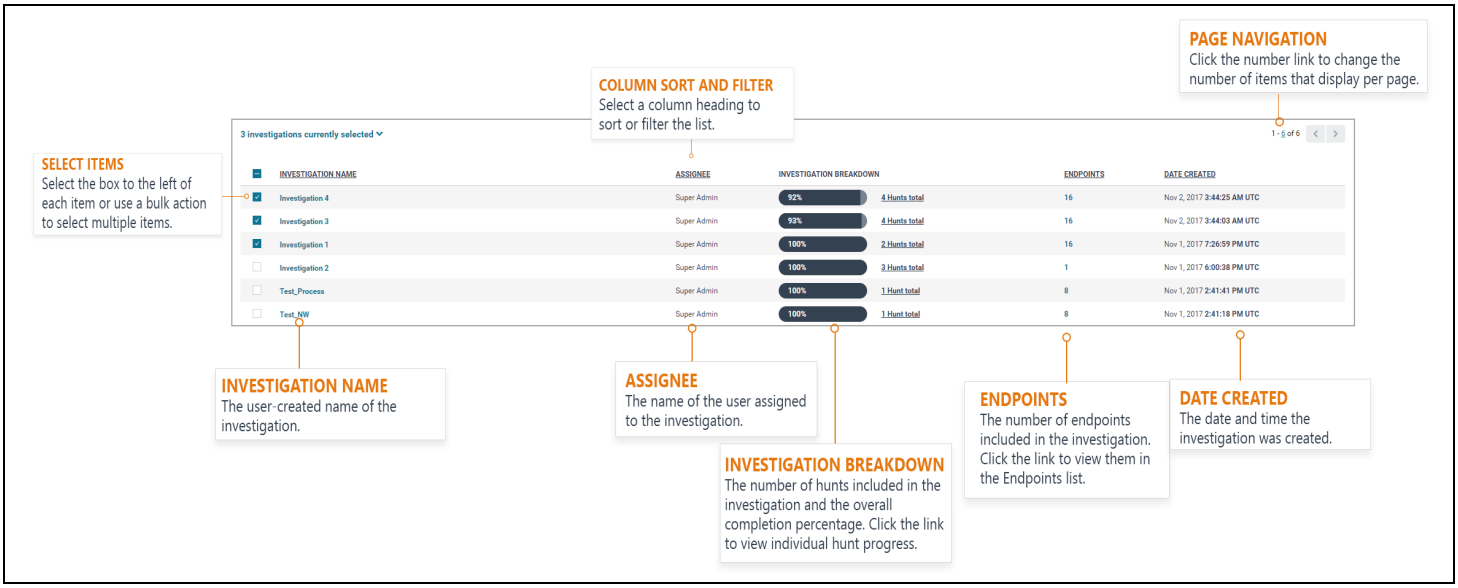
KPI	Description
Hunts	An investigation that includes tasks executed by the sensor to collect data across endpoints.
Queries	Search inquiries executed using Endgame's intelligent assistant, Artemis, to find process-related events on active endpoints. For more information about Artemis, see "Artemis Search Overview" in Chapter 5, *Artemis*.
Total	The total number of hunts and queries.

Each KPI in the Investigation Dashboard is an interactive link that filters the Investigations list by the selected category. Filters are useful to narrow investigations by a specific parameter. For example, to view all current hunt investigations, select **Current**, then select **Hunts**.

Investigations List

The Investigations list is an enumeration of all investigations and their relevant details, organized in a table. The list is useful to view investigation progress, and, more specifically, how many endpoints have returned data. Investigations display in reverse chronological order with the most recently created investigations at the top.

> By default, both hunts and queries appear in the Investigations list. Select the appropriate KPI on the Action toolbar if you need to view either separately.



Investigations list

The columns in the list provide general details about each investigation:

Column Name	Description
INVESTIGATION NAME	The user-created name of the investigation. To view results of an investigation on the Investigation Details page, click the name link.
ASSIGNEE	The name of the user assigned to the investigation.
INVESTIGATION BREAKDOWN	Displays a progress bar that indicates the investigation's or Artemis query's percentage completion across all tasked endpoints. Click the **Hunts total** or Query total link to view a breakdown of each hunt in a pop-up window.
ENDPOINTS	The number of endpoints included in the investigation. Click the number link to view those endpoints in the Endpoints list.
DATE CREATED	The date and time the investigation was created, according to Coordinated Universal Time (UTC) or your selected time zone.

TIP: To help manage the Investigations list, consider archiving investigations you are finished analyzing. For more information, see "Archive an Investigation" in this chapter.

Sort and Filter Columns in the Investigations List

You can sort columns in the list to change the order the contents appear, or search them to filter content by a particular value. Sorting and filtering columns are useful to quickly find specific information without browsing through a large amount of data.

To sort or filter a column, select the appropriate column heading and choose from the following options:

To sort by increasing or decreasing value:

- Select the **Ascending** or **Descending** option. The currently sorted column is denoted by an up arrow or down arrow .

To search the column for a particular value:

- In the text box, type the text you want to find, then click **Search**. The list filters to display results that match the entry. The currently filtered column is denoted by a symbol.

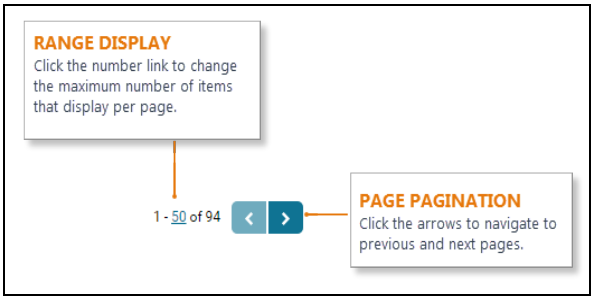
Column sort and filter

Page Pagination

In the upper-right corner above the list is a range display, which displays the current number range of investigations out of the total (e.g., 1-50 of 400). Click the left and right arrows to navigate to previous and next pages.

By default, a maximum of 50 investigations display per page; however, you can change the number to a preferred choice:

1. On the range display, click the number link. For example, if the range display is 1-50, click **50**.
2. In the **Max count of** text box, enter a new number between 1 and 500.
3. Click ✓ to save your changes.



View Investigation Results

After an investigation is created, it continuously runs in the background until complete. You can view an investigation while it is still in progress or when all endpoints have returned data.

To view results of an investigation, click the investigation you want to view from the Investigations list.

> **NOTE:** IOC search results do not have an Investigation Details view but display on the Search Results page instead. For more information, see "IOC Search" in this chapter.

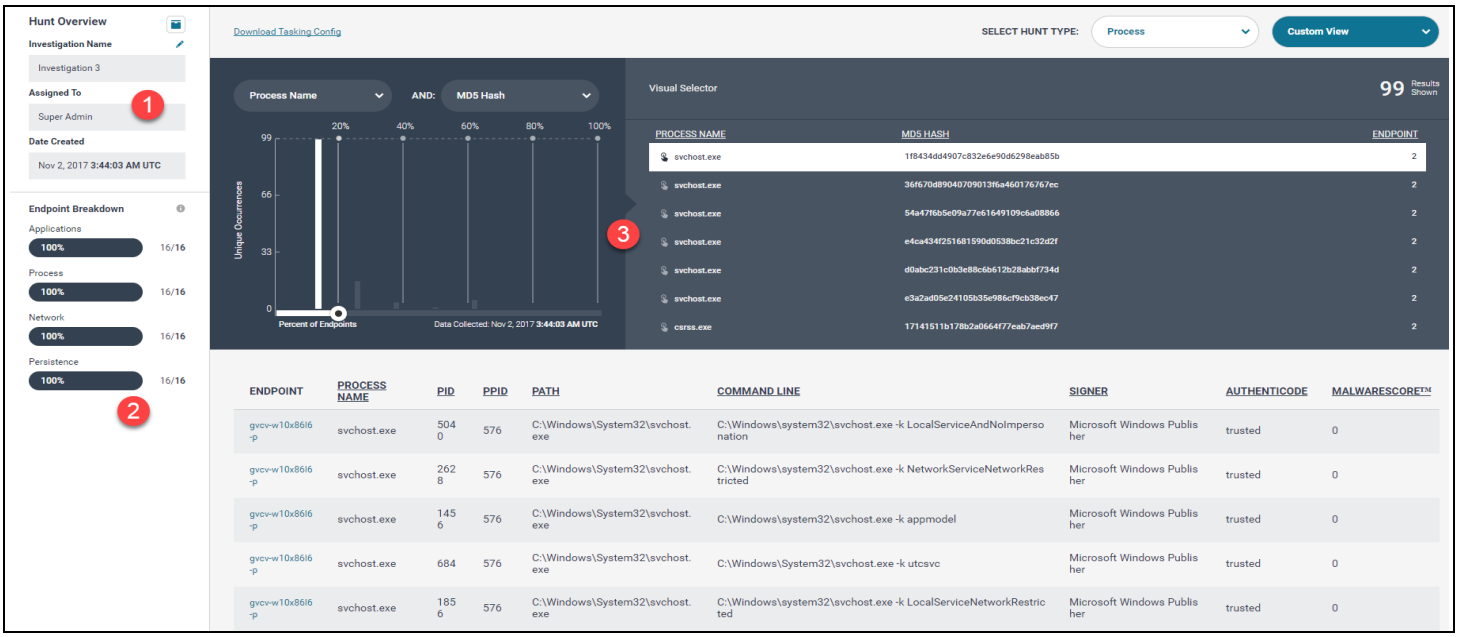
Investigation Details Page Overview

The Investigation Details page displays results of the selected investigation, and enables you to compare, filter, and analyze endpoint data across multiple parameters.

> **NOTE:** Artemis queries have a different view than investigations with hunts. For more information, see "View Artemis Search Results" in Chapter 5, *Artemis*.

The details page has three sections:

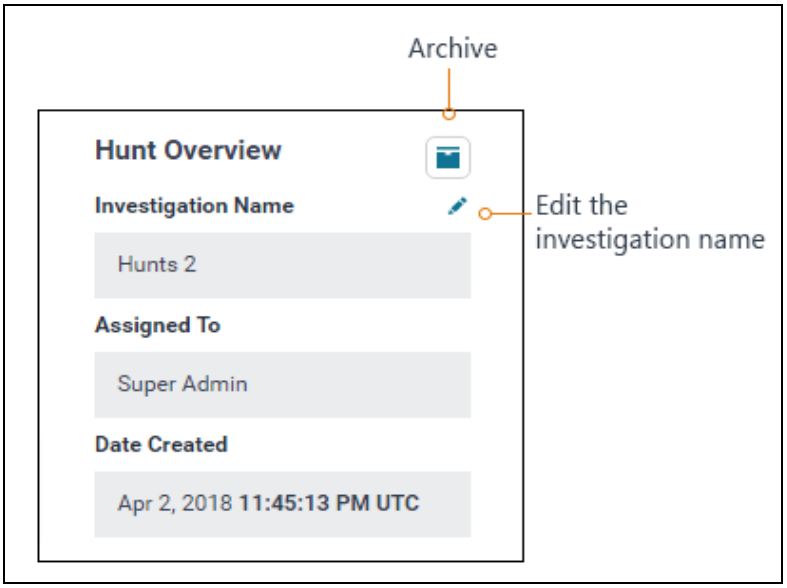
1. Investigation Overview
2. Endpoint Breakdown
3. Investigation Details



Investigation Details page

Hunt Overview

The Hunt Overview section displays general information about the investigation, including the name, assignee, and the date created. It also provides options to edit the name and archive the investigation.

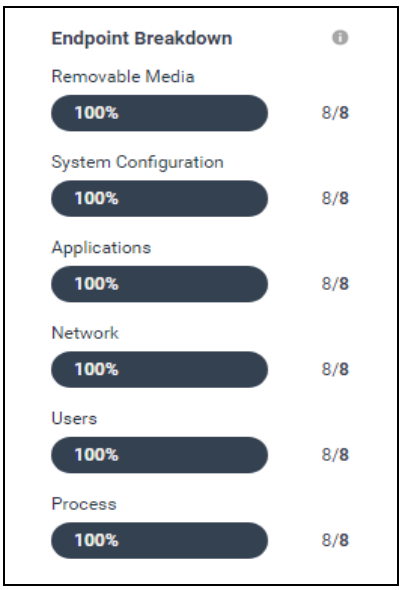


Investigation Overview section

Endpoint Breakdown

The Endpoint Breakdown displays the status of each hunt in the investigation, which includes the following information:

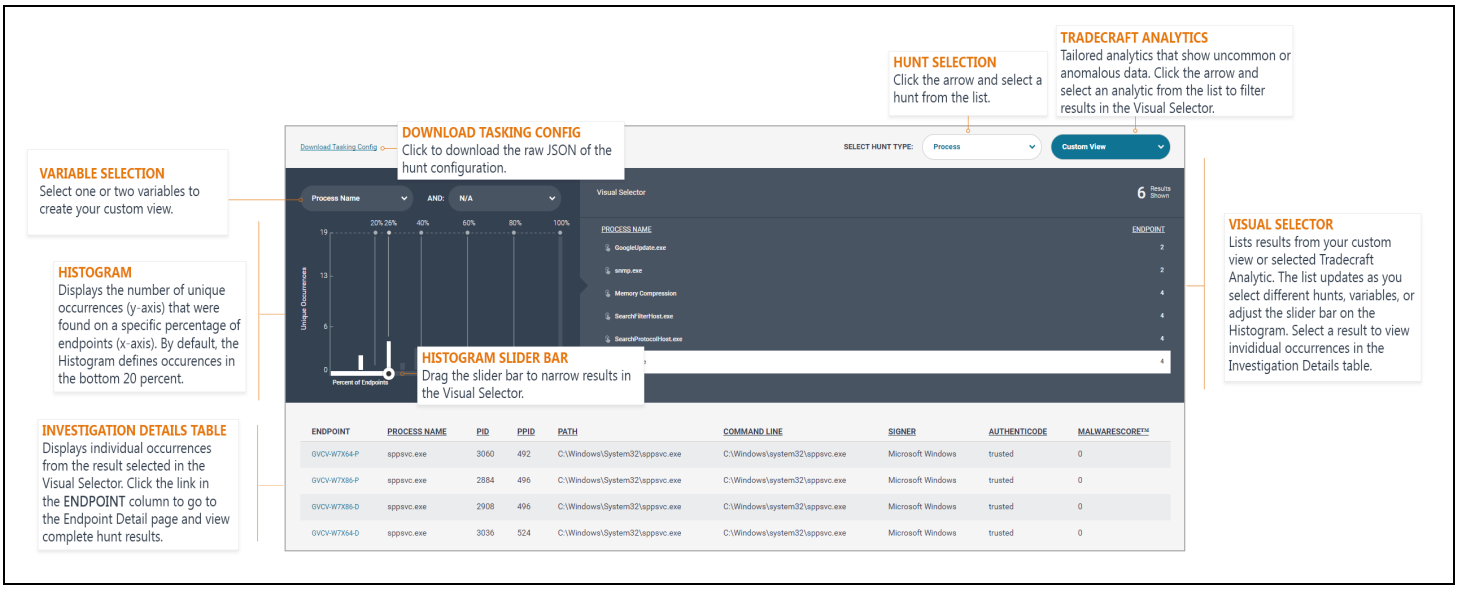
- Each hunt type listed in alphabetical order
- A progress bar that displays the percentage completion
- The number of endpoints out of the total selected that have returned data



Endpoint Breakdown

Investigation Details

Investigation results are displayed within the Investigation Details area. It contains an interactive, customized tool that enables you to filter returned endpoint data by choosing a specific hunt and one or two variables. With this method, you can focus on analyzing smaller components gradually, rather than inclusive results all at once.



Investigation Details

For maximum efficiency, filter investigation results by following these steps:

1. Create your custom view.
2. Find unique occurrences in the Histogram.
3. View results in the Visual Selector.
4. Analyze endpoint data in the Investigation Details table.
5. View hunt results on the Endpoint Details page and, if necessary, execute a response action.

> **NOTE:** In the Investigation Details area, you can view current results for hunts that are in progress, and if needed, respond accordingly without waiting for all data to return; however, the results may not be entirely accurate until all hunts are complete.

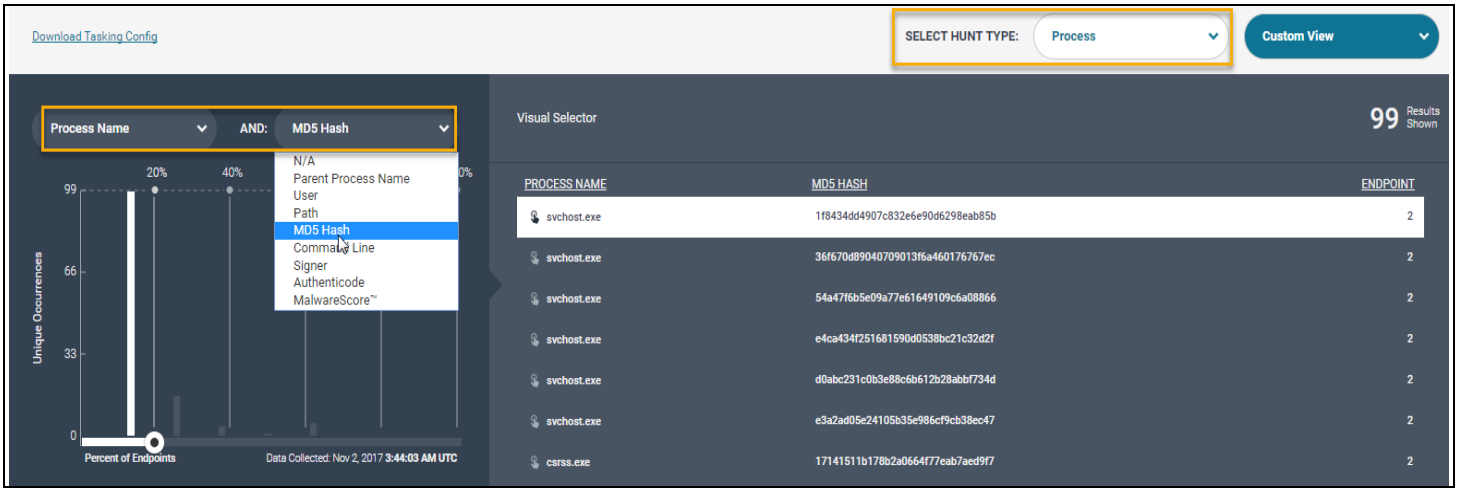
Create Your Custom View

On the upper-right side of the Investigation Details page are two drop-down lists that enable you to either create a custom view or select one of the Tradecraft Analytics — tailored, unique views that show uncommon or anomalous data.

> **NOTE:** Tradecraft Analytics are not available for investigations that contain Linux endpoints.

To create your custom view:

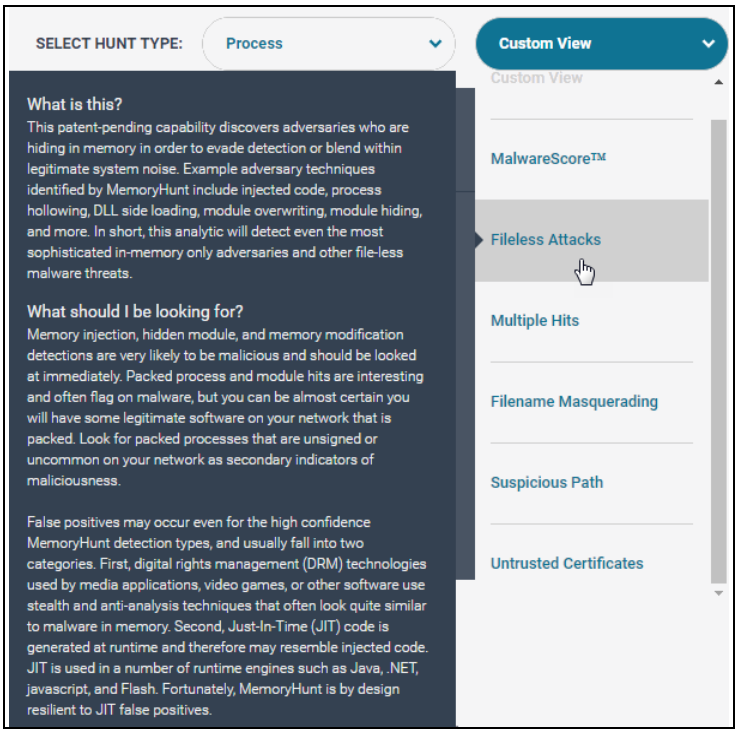
1. Click the **SELECT HUNT TYPE** drop-down arrow, then select a hunt from the list.
2. On the Histogram, click the leftmost drop-down arrow and select a variable from the list. To add a second variable, click the second drop-down arrow and select it from the list. Variables vary by hunt type.



Custom view: select a hunt and one or two variables to analyze data

To view results from one of the Tradecraft Analytics:

1. Click the **SELECT HUNT TYPE** drop-down arrow, then select a hunt from the list.
2. Click the **Custom View** drop-down arrow, then select an analytic from the list.



The list of Tradecraft Analytics for the Process hunt.

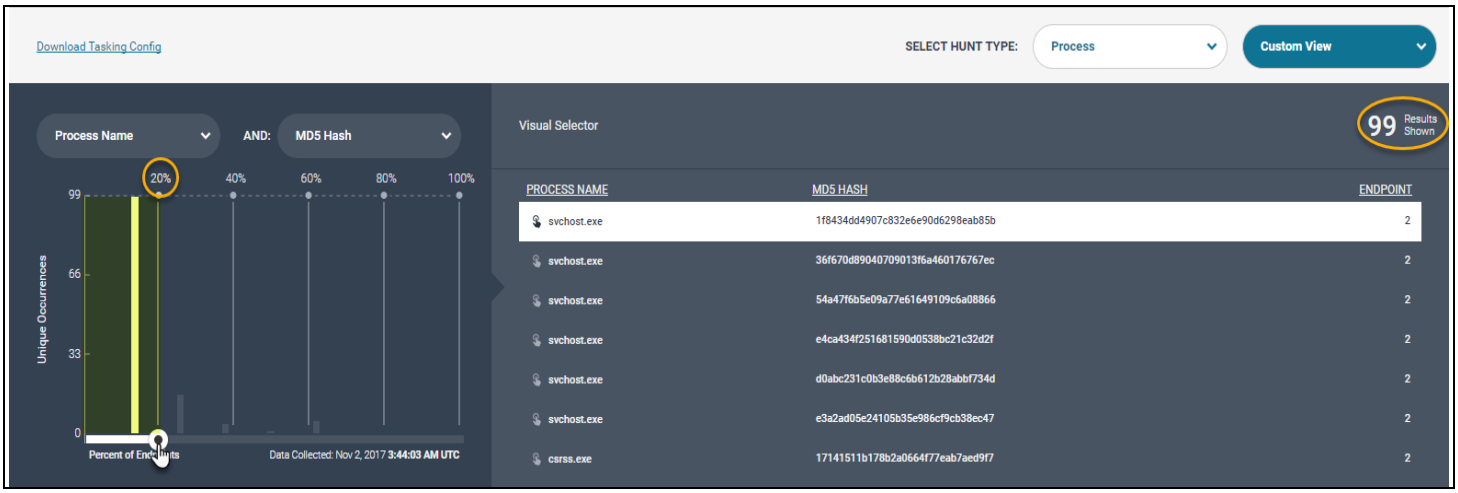
> Tradecraft Analytics are only available for Network, Persistence, Network, and Users hunts vary and by the selected hunt. For a brief description of each analytic, see "Tradecraft Analytics" in this chapter or hover your cursor over an analytic to display the pop-up window.

Find Unique Occurrences in the Histogram

The Histogram is a bar graph that displays the number of unique occurrences (y-axis) —based on the selected variables — that were found on a specific percentage of endpoints (x-axis). The number scale on the y-axis is unique for each investigation; however, the x-axis always displays a number scale of 0 to 100 percent, with percentage markers at intervals of 20 (i.e., 20, 40, 60, 80, and 100).

The Histogram highlights anomalies, if any, at first glance. For example, unique occurrences on the majority of endpoints may not indicate suspicious behavior. On the other hand, occurrences on only a few endpoints may indicate a potential compromise to endpoint data.

While viewing investigation results, the recommended goal is to identify outliers by finding occurrences on a lower percentage of endpoints. As such, after you create your custom view or select one of the Tradecraft Analytics, the Histogram automatically defines unique occurrences in the bottom 20 percent.



The Histogram automatically defines occurrences in the bottom 20 percent. Drag the slider bar to update the Visual Selector.

To narrow results, drag the slider bar on the Histogram left or right to the desired percentage marker. Alternatively, you can select a column bar on the Histogram to view the exact percentage of unique occurrences.

> **NOTE:** Although the Histogram defaults to display occurrences in the bottom 20 percent, it is possible to not see any results if there were no occurrences within that range.

Visual Selector

On the rightmost side of the page is the Visual Selector, a summarized list that displays results according to the current view in the Investigation Details area. The list displays the following data in separate columns:

- The value of each endpoint variable
- The number of endpoints that have one or both variable values

> If you select one of the Tradecraft Analytics, the corresponding endpoint variables are pre-defined, whereas with the custom view, you choose the variables.

Visual Selector

By default, the list sorts according to the least number of endpoints; however, you can change the sort order of any column by doing the following:

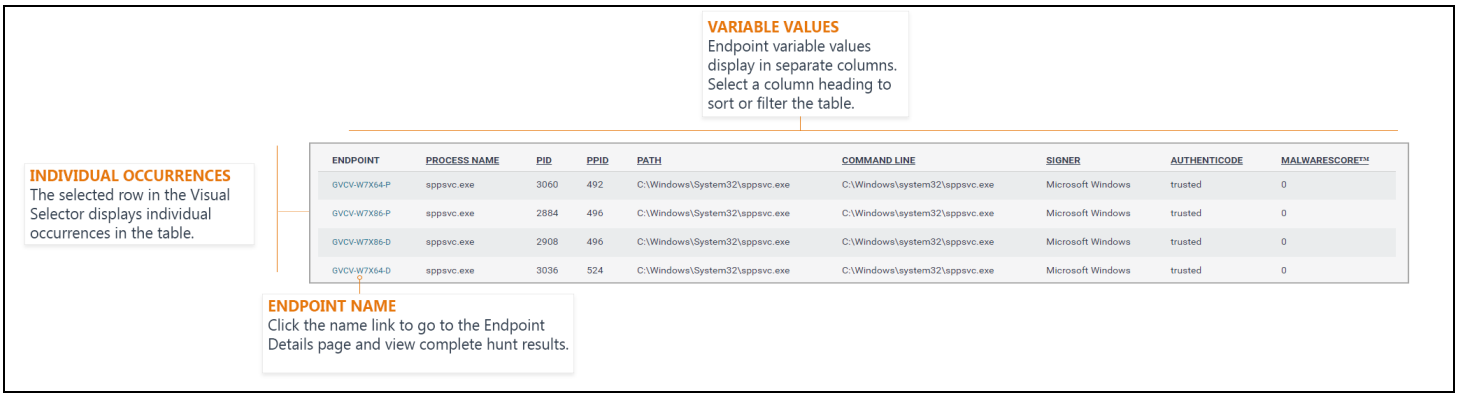
1. Select the column heading you want to sort.
2. To sort by increasing value, click **Ascending**. To sort by decreasing value, click **Descending**.

As you select different hunts, variables, Tradecraft Analytics, or adjust the slider bar on the Histogram, the Visual Selector updates to reflect the most recent data. Analyze results to find possible anomalies; for example, if you are comparing the process name and path variables for a Process hunt and you find a suspicious process, it is recommended you view results of the Process hunt, in its entirety, on the Endpoint Details page to further investigate.

TIP: To help identify suspicious processes, select the **Suspicious Path** analytic from the **Custom View** drop-down list.

View Endpoint Data

To view endpoint data for individual occurrences, select a row in the Visual Selector. The Investigation Details table displays each occurrence on a separate row and each variable value in a separate column.



Investigation Details table

> **NOTE:** Initially, the table displays boilerplate text until you select a row in the Visual Selector.

Like most lists in the Endgame platform, you can sort the columns in the table to change the order the contents appear, or search them to filter content by a particular value. Sorting and filtering the table are also useful to find outliers.

To sort or filter a column, select the appropriate column heading and choose from the following options:

To sort by increasing or decreasing value:

- Select the **Ascending** or **Descending** option. The currently sorted column is denoted by an up arrow or down arrow .

To search the column for a particular value:

- In the text box, type the text you want to find, then click **Search**. The list filters to display results that match the entry. The currently filtered column is denoted by a symbol.

Column sort and filter

View Hunt Results

In the **ENDPOINT** column, click the endpoint name to go to the Endpoint Details page, where you can view all-inclusive results of the completed hunt.

Process
Nov 2, 2017 3:43:59 AM UTC

View Investigation Details | Download Raw Data

PROCESS NAME	PID	PPID	PARENT PROCESS NAME	PATH	COMMAND LINE	SIGNER	AUTHE
conhost.exe	3024	2992		C:\Windows\System32\conhost.exe	\??\C:\Windows\system32\conhost.exe 0x4	Microsoft Windows	trusted
csrss.exe	384	376		C:\Windows\System32\csrss.exe		Microsoft Windows Publisher	trusted
csrss.exe	472	452		C:\Windows\System32\csrss.exe		Microsoft Windows Publisher	trusted
sshd.exe	3072	2992		C:\cygwin\usr\sbin\sshd.exe	"C:\cygwin\usr\sbin\sshd.exe"		noSign
System	4	0	System Idle Process				
L Memory Compression	1756	4	System				
L smss.exe	288	4	System	C:\Windows\System32\smss.exe		Microsoft Windows Publisher	trusted
wininit.exe	460	376		C:\Windows\System32\wininit.exe		Microsoft Windows Publisher	trusted
L lsass.exe	588	460	wininit.exe	C:\Windows\System32\lsass.exe	C:\Windows\system32\lsass.exe	Microsoft Windows Publisher	trusted
L services.exe	576	460	wininit.exe	C:\Windows\System32\services.exe		Microsoft Windows Publisher	trusted

Process hunt results on the Endpoint Details page

If necessary, execute a response action from the Endpoint Details page. For example, if results from a process hunt show a suspicious process name or path, you can terminate that process by doing the following:

1. In the **PROCESS NAME** column, select a process to kill.
2. In the **PROCESS DETAILS** window, click **Kill Process**.
3. In the dialog box that says, "Are you sure you would like to kill the process (PID: *process ID*) on *endpoint hostname*"? click **Yes**. A "Kill Process submitted" message appears to confirm the termination.
4. Click **Finish**.

> You can also initiate a kill process response by doing the following:
> Click **Take Action** on the Endpoint Details page, select **Respond** from the list, then select the **Kill Process** option button. Please note that you will have to enter the process ID.

Archive an Investigation

Archiving an investigation moves it from the **Current** tab on the Investigation Dashboard to the **Archived** tab. To help manage the Investigations list, consider archiving an investigation after you have analyzed all returned endpoint data to distinguish it from investigations that are either still in progress or have not yet been analyzed.

To archive multiple investigations:

1. In the Investigations list, select the box to the left of each appropriate investigation.

   TIP: To select all investigations on the current page, select the box to the left of the **INVESTIGATION NAME** column heading.

2. On the Action toolbar, click **Archive Investigations**.
3. In the **Archive Investigations** dialog box that says, "You are about to archive number Investigations. The investigations will be immediately sent to the Archive Tab and be set as Archived..." click **Archive**. A "Successfully archived investigation(s)" message appears.
4. Click **Finish**.

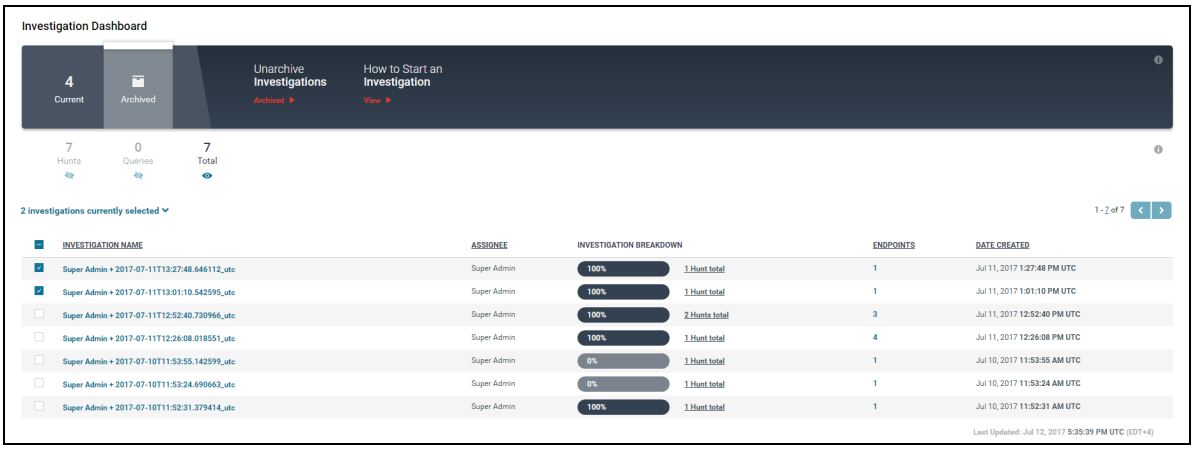
Archive an Investigation dialog window

You can also archive a single investigation from the Investigation Details page by clicking the **Archive** button in the Investigation Overview section.

Investigation Dashboard - Archived View

The Archived view is a separate view within the Investigation Dashboard that displays all investigations that have been archived. To display the Archived view, select the **Archived** tab on the Action toolbar.

The Archived view is identical to the Current view in the Investigation Dashboard, except the Action toolbar contains an option to unarchive selected investigations.



Archived view in the Investigation Dashboard

Unarchive an Investigation

If you mistakenly archived an investigation, you can unarchive it, which moves it back to the Current view in the Investigation Dashboard.

To unarchive an investigation(s):

1. In the Investigations list, select the box to the left of each appropriate investigation to unarchive.
2. On the Action toolbar, click **Unarchive Investigations**.
3. In the dialog box that says, "You are about to unarchive ***number Investigation(s)***. The investigation(s) will be immediately sent back to the Current Tab..." click **Unarchive**. A "Successfully unarchived investigation(s)" message appears.
4. Click **Finish**.

Hunt Types and Advanced Configuration Options

A hunt is a specific task executed by the sensor to collect various endpoint data, and an investigation is a mission to analyze that data.

Before you start a new investigation, keep the following in mind:

- Not all hunt types have advanced configuration. For those that do, required fields are noted as such. The rest are optional.
- Click **EXPAND** or **COLLAPSE** on a hunt type to show or hide its advanced configuration. You can also click the same option on an advanced configuration section heading.
- As a recommendation, some advanced configuration options are selected by default, however, you can clear the selection, if desired.
- IOC Search and System Configuration hunts do not have an Investigation Details view. As such, it is recommended you create separate investigations with each of these as the sole hunt.
- To ensure accuracy, carefully review advanced configuration for each hunt type. Select all appropriate options and enter values accordingly.

The following table describes each hunt type and its advanced configuration options.

Hunt Type	Data Returned	Compatible OS	Advanced Configuration Options
Applications	A list of all installed applications.	• Windows	N/A
File System[1]	A list of all directories and file names within the specified path.	• Windows	**Directory (Required):** Type the path of the starting directory. ▪ **Directories Only:** Returns a list of directories, but no file names. **NOTE:** The following fields and options are unavailable if you select the **Directories Only** option.

[1] You can only create this hunt for a single endpoint.

Hunt Type	Data Returned	Compatible OS	Advanced Configuration Options
			Search Depth: Enter a number between 1 and 3 to specify the number of levels beneath the path the survey should return a list of directories and file names for. For example, if **C:\Program Files** is the directory path and you enter **1** in the **Search Depth** field, the survey will return a list of all subdirectories and file names one level beneath C:\ProgramFiles. **Metadata** Select an option(s) to return additional data: ■ **Collect Hashes:** Returns the MD5, SHA1 and SHA256 hash values. ■ **Collect Timestamps:** Returns dates and times of when the directory was last created, accessed, and modified.
Firewall Rules	A list of all Windows firewall rules that also indicates if they are enabled or disabled.	• Windows	N/A
IOC Search	Executes an IOC (indicators of compromise) search on selected endpoints.	• Windows • Linux • Solaris	See "IOC Search Types and Advanced Configuration Options" in Chapter 3, *Investigations*.
Loaded Drivers	A list of all installed drivers on the system.	• Windows	N/A
Network	A list of all current network connections.	• Windows • Linux • Solaris	**ARP, DNS Cache, NetBIOS, & Routes:** Returns Domain Name System (DNS) records, NetBios neighborhood, Address Resolution Protocol (ARP) entries, and route entries.
Persistence	A list of applications configured to launch when a	• Windows	Click **EXPAND** on each section to view the following advanced configuration options:

Hunt Type	Data Returned	Compatible OS	Advanced Configuration Options
	system reboots.		**Filter By** (Optional) Select an option to filter returned results: ■ **No Filter:** Returns all applications. ■ **Only Return Unsigned:** Returns applications that do not have an SSL certificate. ■ **Only Return not Signed by Microsoft:** Returns applications that do not have a signed Microsoft certificate. **Select Categories** (Required) Deselect any applications that should not be checked for persistence. By default, all applications in the list are selected. **Include Metadata** (Optional) Select an option(s) to return additional data: ■ **MD5 Hash** ■ **SHA1 Hash** ■ **SHA256 Hash** ■ **MalwareScore™:** Returns a score on a scale of 0-100 to indicate the level of malware. ■ **Signer Information:** Returns the certificate owner's information.
Process	A list of running parent and child processes.	• Windows • Linux • Solaris	Select an option to indicate which processes to return: ■ **All Processes:** Returns all running processes. ■ **Suspicious Processes:** Returns

Hunt Type	Data Returned	Compatible OS	Advanced Configuration Options
			unbacked executable processes. **Detect** ■ **Malware with MalwareScore™:** Detects potential malware files that are present on disk. If found, it returns a score on a scale of 0 (benign) to 100 (malicious) to indicate the level of maliciousness. ■ **Fileless Attacks:** Detects potential malware running in memory. If found, it displays those processes in the Fileless Attacks analytic. [1] **Collect** Select an option(s) to return additional data: ■ **Hashes**: Returns the MD5 hash value of each found process. ■ **Modules:** Returns all loaded modules in a process. ■ **Handles:** Returns information about open handles owned by a given process, including the type of handle. ■ **Threads:** Returns information about threads owned by the process, including the thread ID and the starting address.
Registry	Windows information from the specified registry hives.	• Windows	**Registry Path:** Type the full registry path, including the base hive, to filter survey results (e.g., HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft).

[1] For more information about the Fileless Attacks analytic, see "Fileless Attacks."

Hunt Type	Data Returned	Compatible OS	Advanced Configuration Options
			Depth: Enter a number between 1 and 3 to specify the number of subkeys beneath the registry path to return.
Removable Media	A list of devices plugged into a USB port (e.g., flash drives, portable hard drives, etc.)	• Windows	N/A
System Configuration[1]	Operating system and configuration information, such as hostnames, system architecture, and memory usage.	• Windows • Linux • Solaris	N/A
Users	A list of all users who are currently logged in.	• Windows • Linux • Solaris	N/A

[1]System Configuration does not have an Investigation Details view.

Tradecraft Analytics Overview

Tradecraft Analytics are unique views that show uncommon or anomalous data on the Investigation Details page. This differs from the custom view, which allows you to choose which endpoint variables you want to analyze. When you select a hunt and an analytic, the Visual Selector and Histogram update with the corresponding data.

The following table describes the available Tradecraft Analytics for Network, Persistence, Process, and Users hunts, and the data each returns.

NOTE: Tradecraft Analytics are not available for investigations with Linux endpoints, however, you can choose endpoint variables to create a custom view.

Analytic Type	Description (Data Returned)
Network	
Uncommon Connections	The least occurring remote network connections within the environment.
Listening Ports	Listeners that are actively listening for an inbound remote connection on a port that is an outlier in the environment.
Suspicious Connections	Remote connections to web ports (e.g., 80, 443, etc.) that are not linked to a web browser.
Persistence	
MalwareScore	Persistent files that exceed the set malware threshold.
COM Hijacking	Persistent files that contain COM (Component Object Model) hijacks —a technique where the adversary writes a current user COM entry in the registry corresponding to a legitimate entry in the local machine hive.
Search Order Hijacking	Persistent files that contain DLL search order hijacks — a technique where the adversary places a malicious DLL with the same name as a legitimate DLL in a location that is loaded before the legitimate DLL.
Phantom DLL Hijacking	Persistent files that contain phantom DLLs hijacks —a technique where an adversary names their library to match a phantom DLL — a program that attempts to load but is not present on the system. The adversary then sets an application to load the phantom DLLs to persist.
Multiple Hits	Persistent files that triggered multiple suspicious behaviors as a result of existing high and medium analytics (e.g., Fileless Attacks, Filename Masquerading, Untrusted Certificates, etc.)
Filename Masquerading	Persistent files with the same name as a well-known system or application, or running processes that do not match the correct path.

Analytic Type	Description (Data Returned)
Filename Mismatch	Persistent files that are empty or do not match the filename on disk.
Suspicious Path	Persistent files that are persisting out of abnormal paths.
Untrusted Certificates	Persistent files that are unsigned or do not properly verify on the system.
Modified Persistence	Previously observed persistent files whose hash or signer information has changed.
New Persistence	Persistent files that are newly discovered in the environment which are not signed by trusted sources.
Persistence Not Found	Persistent files with an execution target that does not exist on disk.
Process	
MalwareScore	Processes that exceed the set malware threshold.
Fileless Attacks	Processes that are hiding in memory to evade detection.
Multiple Hits	Processes that triggered multiple suspicious behaviors as a result of existing high and medium analytics (e.g., Fileless Attacks, Filename Masquerading, Untrusted Certificates, etc.)
Filename Masquerading	Processes with the same name as a well-known system or application, or running processes that do not match the correct path.
Suspicious Path	Processes that are running out of non-traditional applications or system folders.
Untrusted Certificates	Processes that are unsigned or do not verify on the system.
Users	
Multiple Logons	Users who are accessing multiple endpoints.

Fileless Attacks Overview

Fileless Attacks is an analytic and enhancement to the Process hunt that inspects the memory of running processes to discover adversaries hiding in memory to evade detection. Fileless Attacks identifies evasion techniques such as injected code, process hollowing, DLL side loading, module overwriting, and module hiding. If such techniques or other fileless threats are detected in your environment, it is a strong indicator of a potential compromise that requires immediate investigation. Details of each flagged process and its modified memory are displayed on the Investigation Details page.

> The difference between Fileless Attacks and MalwareScore™ detection is that the former detects malware running in memory; the latter detects potential malware files that are present on disk. Fileless Attacks and Malware with MalwareScore™ are two detection options selected by default in the Process hunt's advanced configuration.

What to Look Out For

Fileless Attacks categorizes hidden memory techniques into four attack types: Memory Modification, Memory Injection, Hidden Module, and Software Packing. Memory Modification, Memory Injection, and Hidden Module detections are likely malicious and each process should be investigated immediately. Although packed processes often indicate malware, it is common to have some legitimate software on your network that is packed.

Depending on the packer used, legitimately packed applications may show hits for Memory Injection. As a secondary indicator of present malware, look for packed processes that are unsigned or uncommon within your network.

> **TIP:** When viewing investigation details of a Process hunt, in addition to Fileless Attacks, select other Tradecraft Analytics — such as Untrusted Certificates and Suspicious Path — to display anomalous data.

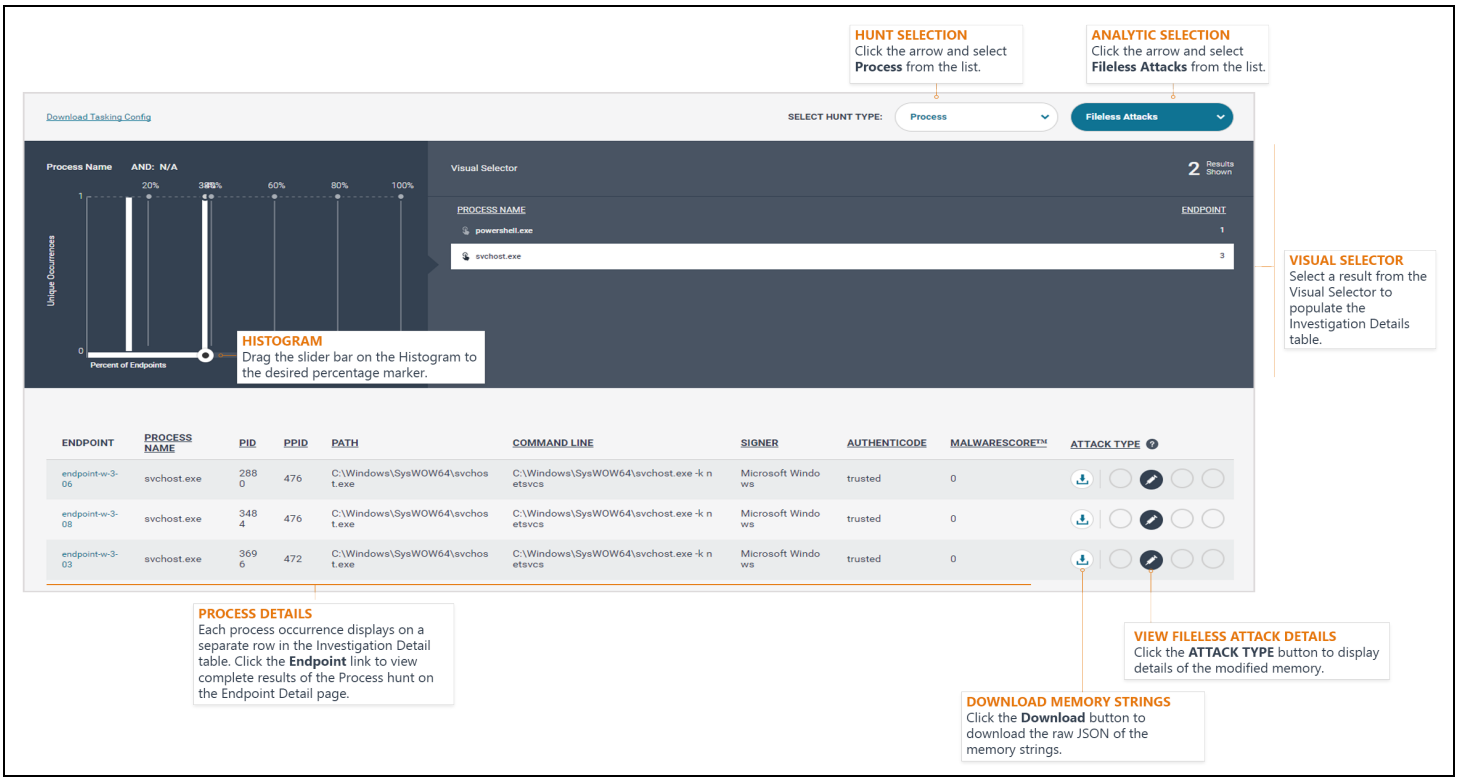
The following table describes the four attack types and the type of malware Fileless Attacks identifies. On the Investigation Details page, each attack type is identified by a distinct symbol.

Attack Type	Description	Symbol
Memory Modification	Identifies malware that modifies or overwrites the process memory of legitimate modules to hide its presence on the system.	
Memory Injection	Analyzes running threads and memory segments to find injected code and dynamic link libraries (DLLs) in memory. **NOTE:** Memory Injection hits typically require immediate attention.	
Hidden Module	Identifies malware that removes traces of itself from the Process Environment Block (PEB) and exists on disk as a DLL.	
Software Packing	Identifies packed processes. Packing an executable changes the file signature in an attempt to avoid signature-based detection. **NOTE:** Consider investigating packed processes for other unusual behavior, such as anomalous network connections.	

Discover Fileless Attacks

To discover hidden adversaries using the Fileless Attacks analytic:

1. In the Investigations list, click the appropriate investigation to view it on the Investigation Details page. Ensure you included the Process hunt in your investigation.
2. In the upper-right corner of the page, select the **Custom View** drop-down arrow, and then select **Fileless Attacks** from the list. The Histogram automatically defaults to display results in the bottom 20 percent and lists each process name in the Visual Selector. If there are no results, drag the slider bar to a different percentage marker or click a column bar.
3. Select a result from the Visual Selector, which populates the Investigation Details table. The table displays each process occurrence in a separate row and each variable value — such as the process name, process ID and parent process ID — in a separate column.
4. In the **Attack Type** column, click the button that represents the attack type you want details of. A pop-up window displays details of where the memory was modified.



Fileless Attacks view in the Investigation Details area

TIP: Click ? to view a description of each attack type. To filter occurrences in the Investigation Details table by attack type, click the Attack Type column heading and select the box to the left of each appropriate type. To clear the filters, click Reset.

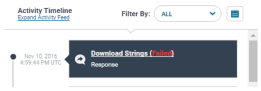
Analyze Fileless Attacks

The initial step in analyzing Fileless Attacks is to confirm whether the memory process is malicious. Each process that detected hidden memory has memory strings available to download. It is recommended you analyze those strings for artifacts such as call back URLs and harvested system information for indicators that the process is malicious.

To download the memory strings:

1. In the Investigation Details table, click the **Download** button in the appropriate **ATTACK TYPE** column.
2. In the dialog box that says, "Are you sure you would like to download strings from process name?" Click **Yes**. A "Request successful" message appears.
3. Click **Go to Endpoint** to go to the Endpoint Details page. The initiated task is selected in the Activity Timeline.

NOTE: If the process is no longer active, a "Download Strings" failure appears in the timeline:



4. In the upper-right corner of the Details pane on the right, click **Download Raw Data**, then select **RAW RESPONSE DATA**.
5. Save the file or open it in an external application.

Execute an Endpoint Response

After you have confirmed the process is malicious, as a remedial action, you can execute an endpoint response to suspend or kill the associated threads or processes.

NOTE: Only administrators and Level 3 users can execute an endpoint response.

To execute an endpoint response:

1. In the Investigation Details table, click the link in the Endpoint column to go to the Endpoint detail page. The all-inclusive data returned from the Process hunt appears.
2. In the **PROCESS NAME** column, select the appropriate process to terminate.

TIP: Processes that were flagged for hidden memory have a red exclamation point to the left of the process name. Click it to view the attack type.

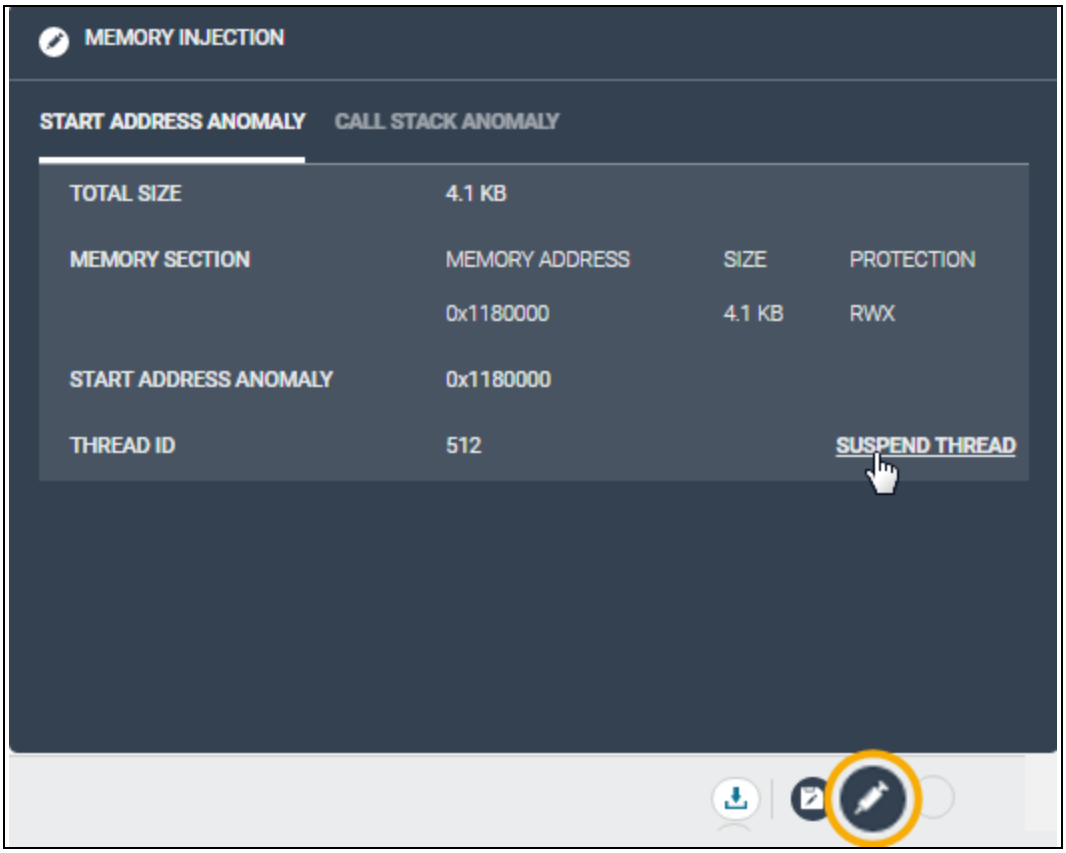
3. In the **PROCESS DETAILS** window, click **Kill Process**.
4. In the dialog box that says,"Are you sure you would like to kill the process process name (process ID) on endpoint hostname? click **Yes**. A "Kill Process submitted" appears to confirm the process was terminated.
5. Click **Finish.**

WARNING: There is also a **GET FILE** option; however, please use caution and ensure you are analyzing the file in an isolated environment as the file is likely malicious.

Suspend a Thread for Memory Injection Hits

For Memory Injection attack types, you can suspend the thread directly from the Memory Details window:

1. On the THREAD ID row, click **SUSPEND THREAD**.



Memory Injection details

2. In the dialog box that says, "Are you sure you would like to suspend thread thread ID from endpoint hostname?" click **Yes**. A "Request successful" message appears.
3. Click **Finish**.

IOC Search Overview

IOC (indicators of compromise) Search is a type of hunt that enables you to search across selected, monitored endpoints for specific attributes that would indicate the endpoint data was compromised. There are five IOC search types: File, Network, Process, Registry, and User, each which has a set of advanced configuration options. Although each of these can be added as individual hunts within an investigation, creating an IOC search compiles them into a single hunt, and after data is returned, displays results on the Search Results page.

> **NOTE:** The difference between IOC Search and Artemis — Endgame's intelligent assistant —is the former searches for current endpoint data for both Windows and Linux endpoints, and the latter searches for historical process-related events that occurred on Windows endpoints.
>
> For more information about Artemis, see "Artemis Overview" in Chapter 5, *Artemis*.

Execute an IOC Search

> **NOTE:** IOC Search results do not appear on the Investigation Details page, but on the Search Results page. As such, it is recommended you create an investigation with IOC Search as the sole hunt.

To create and execute an IOC search:

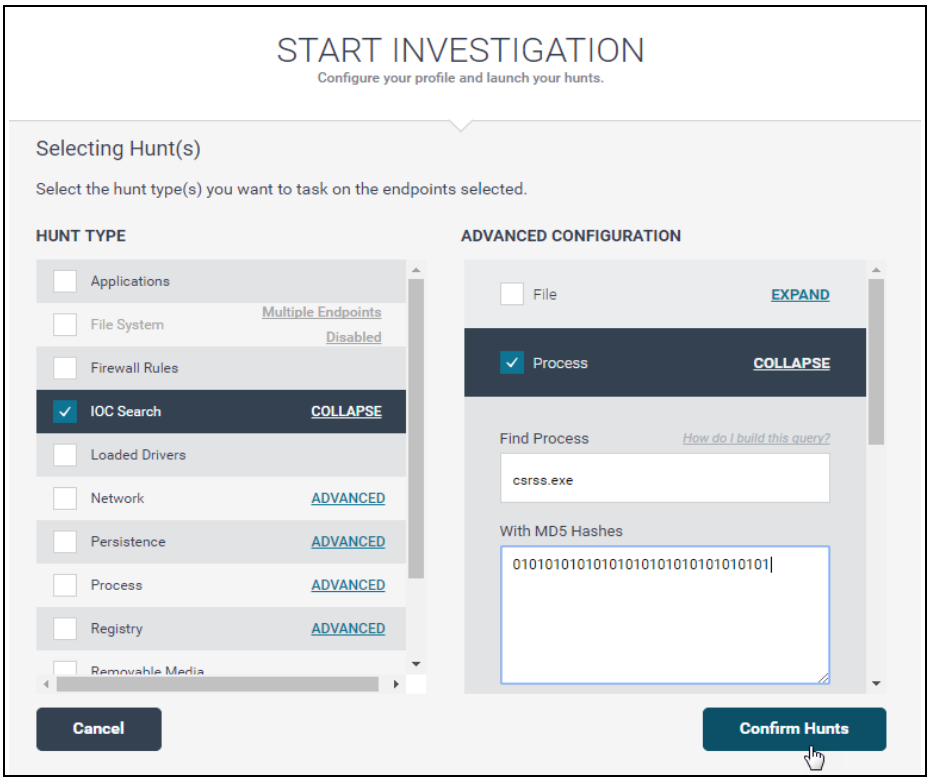
1. In the Endpoints list, select the box to the left of each appropriate endpoint.
2. On the Action toolbar, select an operating system tab (i.e., Windows, Linux, or Mac) to filter the Endpoints list.
3. Select the box to the left of each endpoint to include in the search.
4. On the Action toolbar, click **Create Investigation**.
5. In the **START INVESTIGATION** dialog window, type a unique name to identify the search and assign it to a different user, if necessary.
6. Click **Add Hunt(s)**. An alphabetical list of all hunt types appears.
7. In the left column, select **IOC Search**.
8. In the right column, click **EXPAND** on each category to include in the search and enter advanced configuration as necessary. After you enter a value in one of the fields, the corresponding IOC search type is automatically selected.

> **NOTE:** Registry search is not available for Linux endpoints.

> **NOTE:** If you are searching for a specific filename on Windows endpoints, do not use uppercase letters.

9. Proceed with creating the investigation.

> **Remember:** IOC Search appears as an event in the Activity Timeline of each endpoint that was included.



Sample Process IOC search

> For a complete list of advanced configuration options, see "IOC Search Types and Advanced Configuration Options" in this chapter.

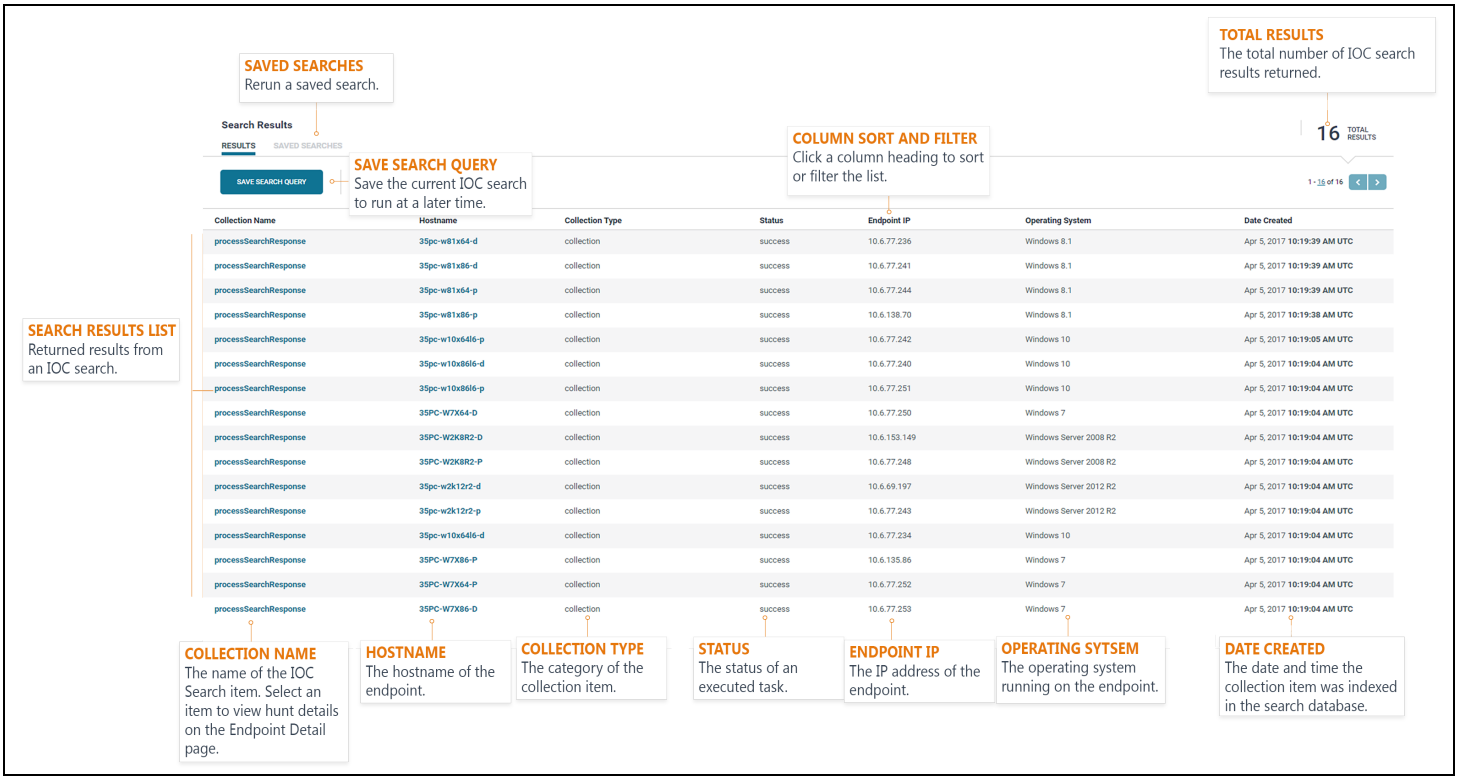
View IOC Search Results

Unlike other hunts, IOC search results do not have an Investigation Details view, but display on the Search Results page instead.

To view IOC search results:

- After you launch the investigation, click the "View Investigation" link on the **START AN INVESTIGATION** dialog window.

IOC search results are formatted as a tabular list. The total number of results displays in the upper-right corner.



IOC Search Results list

NOTE: If the IOC search does not return any results, the page says, "There are no results."

IOC Search Results Overview

The columns in the IOC Search Results list provide the following endpoint data:

Column Name	Description
COLLECTION NAME	The name of the IOC Search item, e.g., processSearchResponse. (Note: This is one text string with no spaces).
HOSTNAME	The hostname of the endpoint.
COLLECTION TYPE	The category of the collected endpoint data (e.g., detection, prevention, response, etc.). All IOC searches are collections.

Column Name	Description
STATUS	Indicates whether the collected endpoint data was a success or failure.
ENDPOINT IP	The IP address of the endpoint.
OPERATING SYSTEM	The operating system running on the endpoint.
DATE CREATED	The date and time the endpoint data was indexed in the search database.

View Results for a Single Endpoint

To view complete hunt details for a specific endpoint:

1. In the IOC Search Results list, locate the appropriate endpoint hostname or IP address.
2. Click the search item in the corresponding **COLLECTION NAME** column.
3. View results in the Activity Details pane on the Endpoint Details page.

Process hunt details for a single endpoint

NOTE: If you included other hunts in the investigation, you can click **VIEW INVESTIGATION DETAILS** to view those results on the Investigation Details page. However, if IOC Search is the sole hunt in the investigation as recommended, if you click **VIEW INVESTIGATION DETAILS**, a message that says, "View results for this Hunt in search" appears. When selected, it redirects to the Search Results page.

Sort Columns in the IOC Search Results List

You can sort columns in the IOC Search Results list to change the order the contents appear.

To change the sort order within a column:

1. Select the appropriate column heading to sort or filter.
2. To sort by increasing value, click **Ascending**. To sort by decreasing value, click **Descending**. The currently sorted column is denoted by an arrow.

TIP: If there is a large number of results, consider changing the range display to a higher number to avoid searching the same criteria on multiple pages.

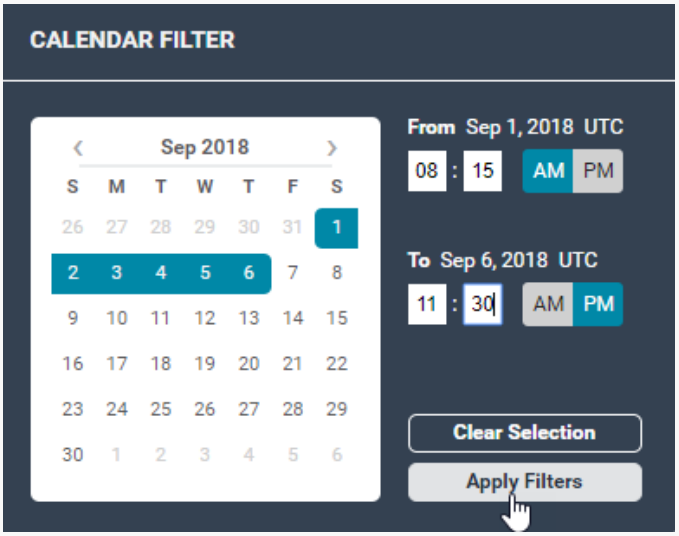
IOC Search Types and Advanced Configuration Options

The following table describes each IOC search type and its advanced configuration options. When you configure an IOC search, keep the following in mind:

- In the **ADVANCED CONFIGURATION** column, click **EXPAND** or **COLLAPSE** on an IOC Search type to show or hide the configuration settings.
- You must enter a value in at least one field of the selected IOC search type.
- To ensure accuracy, carefully review advanced configuration for each search type. Select all appropriate options and enter values accordingly.
- Click ***How do I build this query?*** for guidance on how to structure a query.
- For text box entries, follow the same format as the parenthetical examples, if given.

IOC Search Type	Description	Advanced Configuration
File	Searches for running files.	**Directory:** Type the starting directory path (e.g., C:\windows\system32). **Find File:** Type the filename(s) to search. **TIP:** Type a regex (regular expression) to narrow search results. For example, to find a file that ends with test.txt, use the following regex: **.*test\.txt'** ■ **With MD5 Hashes:** Type the MD5 hash(es). Separate multiple entries with a semicolon. ■ **Or SHA1 Hashes:** Type the SHA1 hash(es). Separate multiple entries with a semicolon. ■ **Or SHA256 Hashes:** Type the SHA256 hash(es). Separate multiple entries with a semicolon.
Process	Searches for running processes.	**Find Process:** Type the process name or file path you are looking for. Separate multiple entries with a semicolon. ■ **With MD5 Hashes:** Type the MD5 hash(es). Separate multiple entries with a semicolon. ■ **Or SHA1 Hashes:** Type the SHA1 hash(es). Separate multiple entries with a semicolon. ■ **Or SHA256 Hashes:** Type the SHA256 hash(es). Separate

IOC Search Type	Description	Advanced Configuration
		multiple entries with a semicolon.
Network	Searches for network connections.	**Find Remote IP Address:** Type the remote IP address or range. **Find Local IP Address:** Type the local IP address or range. **Communicating on Port** Select one of the following options and enter the port in the text box: ■ **Remote Port** ■ **Local Port** ■ **With State:** Click the arrow and select which port state(s) to return. ■ **Over Protocol:** Click the arrow and select which connection type(s) to return.
Registry	Searches for a registry key or value name.	**Base Hive (Required):** Click the arrow and select all or one of the six root keys. **NOTE:** You must enter a value in at least one of the following options: **Enter Registry Key or Value Name Containing:** Type a registry key or value name. Separate multiple entries with a semicolon. **By Size** ■ **Max Byte Size:** Enter the maximum file size of the registry key, in bytes. ■ **Min Byte Size:** Enter the minimum file size of the registry key, in bytes. **Registry Date Modified:** Specify a date and time range of when the registry was modified: 1. Select a start date from the calendar widget. Use the **<** and **>** arrows to navigate to previous and following months. 2. To specify a starting time other than the default 12:00 AM UTC, place your cursor in each text box and enter the appropriate time in HH:MM format. Select **AM** or **PM**. 3. Specify an end date and time using the same procedure in steps 1 and 2.

IOC Search Type	Description	Advanced Configuration
		
User	Searches the network for logged in users.	**Find User:** Type a username(s). Separate multiple entries with a semicolon. **On Domain:** Type the domain name.

CHAPTER 4

ALERTS

Alerts Overview

Alerts are Endgame sensor-generated notifications that detect potentially malicious activity on monitored endpoints, such as a process injection or permission theft. Alerts are a vital feature of Endgame because they identify abnormal behavioral patterns that may require an investigation.

A previously configured Endpoint Policy, which is enabled upon deployment, specifies which endpoint activities the sensor monitors and the action the sensor should take if it detects potentially malicious activity. If the sensor detects such malicious activity, it generates an alert in the Endgame platform.

Alerts are divided into two sensor action types: **preventions** and **detections**. A prevention alert is generated when the sensor blocks malicious activity on an endpoint by executing an automated response. A detection alert is generated when the sensor detects potentially malicious activity on an endpoint but does not execute a response. You can view the inclusive list of generated alerts in the Alerts list.

> **NOTE:** If the sensor is offline, it locally stores recent alerts and resends them to the Endgame platform once it has reestablished a connection.

When an alert is generated, the sensor collects related endpoint metadata, stores it in the Endgame platform, and displays it in the Alert Metadata panel, located on the Alert Details page. The Alert Details page also displays the Endgame Resolver™ Attack Visualization, a visual timeline that chronologically depicts the events that led up to the alert.

> For more information about the Alert Details page, see "View Alert Details" in this chapter.

Alerts are also divided into two categories: **threats** and **adversary behaviors**. Threat alerts capture specific malicious activity that occurs on an endpoint. If a threat is detected, in addition to a generating an alert, the sensor displays a notification in the Endgame platform, which appears as a flashing red "Alerts" button (megaphone icon) on the Left Navigation toolbar. The button continues to flash until you select it to view the Alert Dashboard.

New threat alert notification

The following alerts are considered threats:

- Malware
- Exploit
- Process Injection
- Ransomware
- Credential Manipulation
- Credential Dumping

- Permission Theft
- Blocklist alerts

Adversary behavior alerts are directly mapped to MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) and are useful to understand the tactics and techniques an attacker may use when executing an attack.

Alert Dashboard Overview

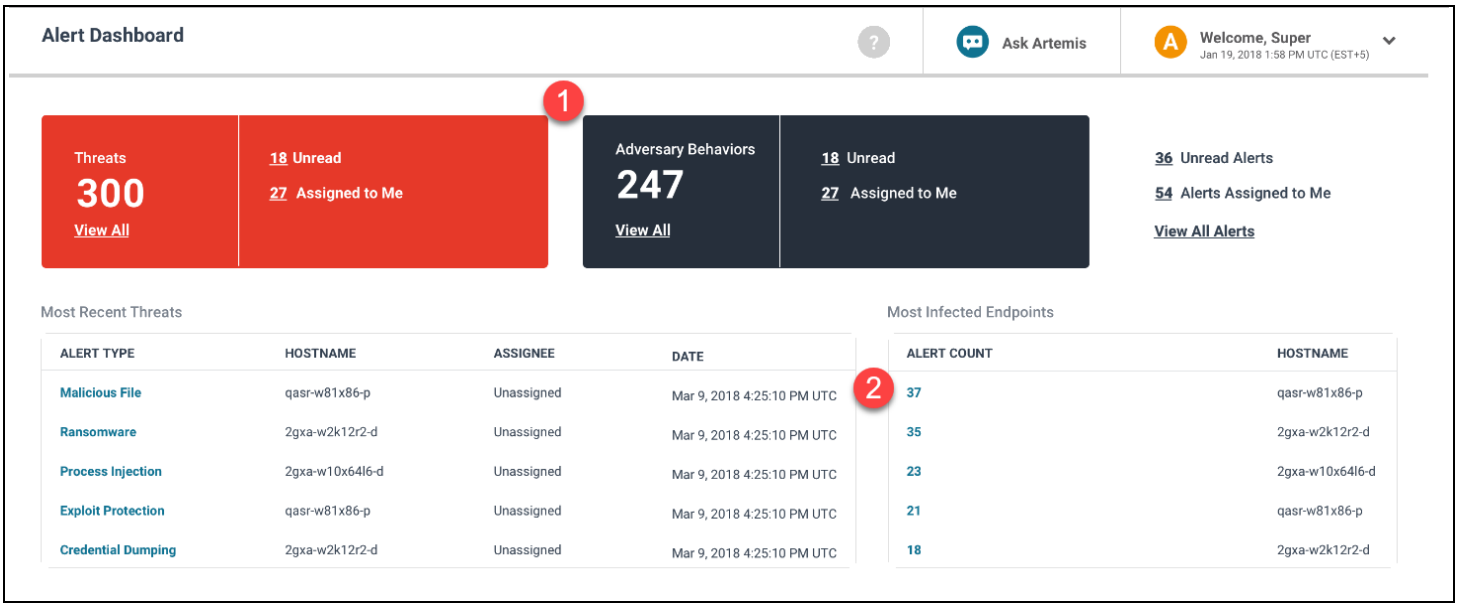
The Alert Dashboard provides a statistical summary of alert status within your environment. It consolidates qualitative alert data into a concise visualization that enables you to do the following:

- Monitor incoming alerts in real time
- Identify which alerts are unread and assigned to you
- Identify behavioral patterns across your endpoints
- Triage alerts so you can prioritize items that may require immediate attention

To view the Alert Dashboard, click the **ALERTS** button  on the Left Navigation toolbar.

The dashboard contains two major components:

1. Threats and Adversary Behaviors Key Performance Indicator (KPI) charts
2. Most Recent Threats and Infected Endpoints



Alert Dashboard

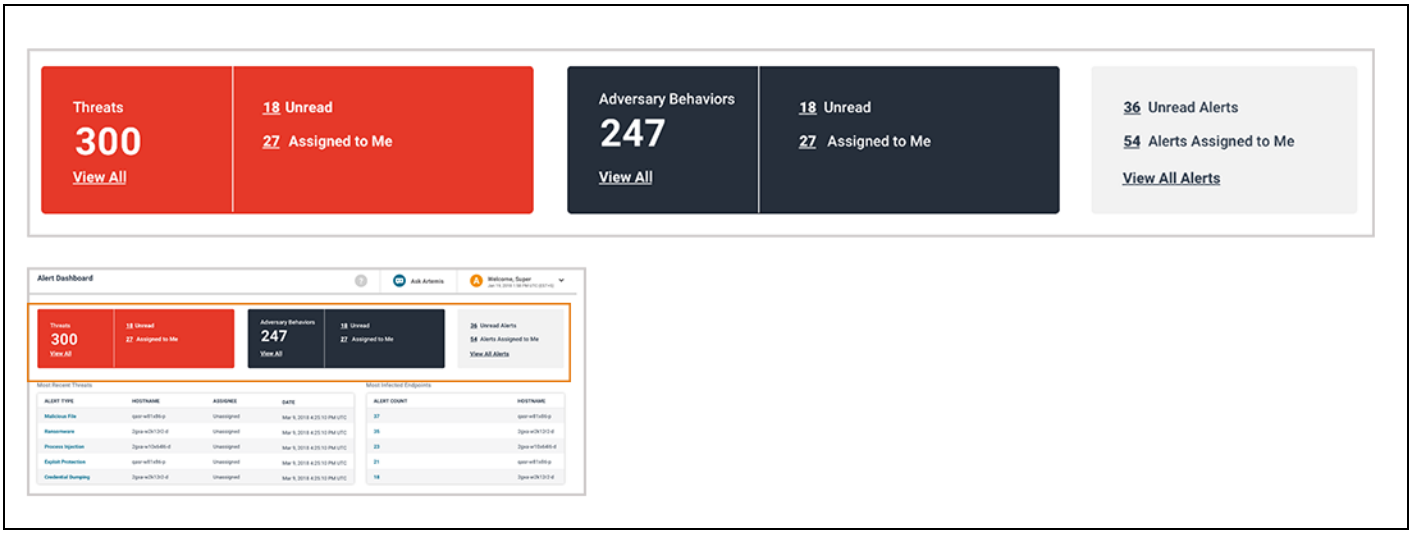
Threats and Adversary Behaviors KPI Charts

Threats and Adversary Behaviors charts display the total number of alerts that fall into each of these categories. Threats capture specific malicious activity that occurs on an endpoint. Adversary behaviors alerts are directly mapped to MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™).

Each chart also displays the number of unread alerts and the number of alerts assigned to you. These numerical values are user-specific, and, therefore, may vary for each user. Each numerical value is also an active link that when selected, filters

the Alerts list by that attribute. For example, to view all unread threat alerts, click the "Unread" number link on the Threats KPI chart.

The Totals chart on the far right provides numerical values for the total number of unread and assigned alerts. To view a comprehensive list of Alerts, click **View All Alerts**.



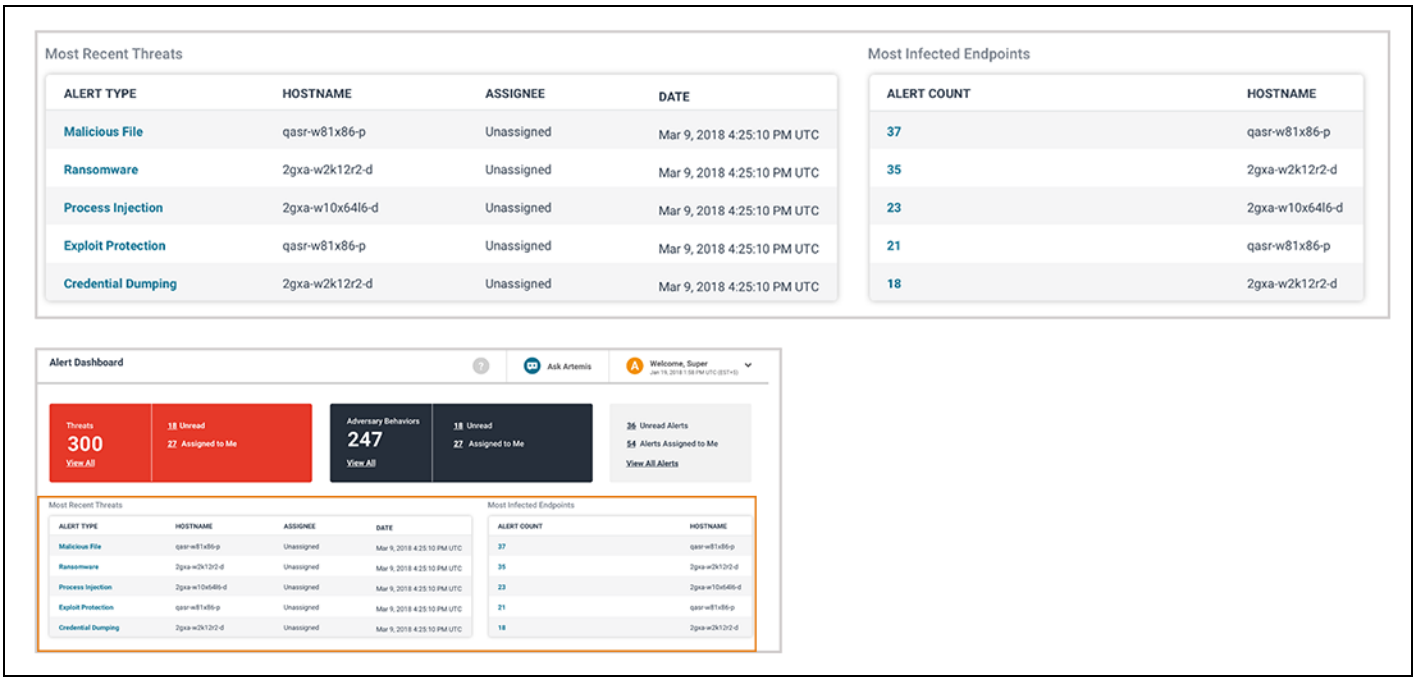
Threats and Adversary Behaviors charts

Most Recent Threats and Infected Endpoints Cards

The Most Recent Threats card lists the most recent threat alerts generated in the Endgame platform. It also lists general details about the alert, including the hostname, assignee, and date it was generated. Select an alert from this list to view inclusive details on the Alert Details page.

The Most Infected Endpoints card lists the top five endpoints with the highest alert count. Each row displays the affected hostname and alert count. The alert count value is an active link that when selected, filters the Alerts list by the alerts associated with that endpoint.

> **NOTE:** The number included in the total alert count includes threats and adversary behaviors that have not been resolved (i.e., not dismissed or marked as "Resolved").



Most Recent Threats and Infected Endpoints Cards

Alerts Page Overview

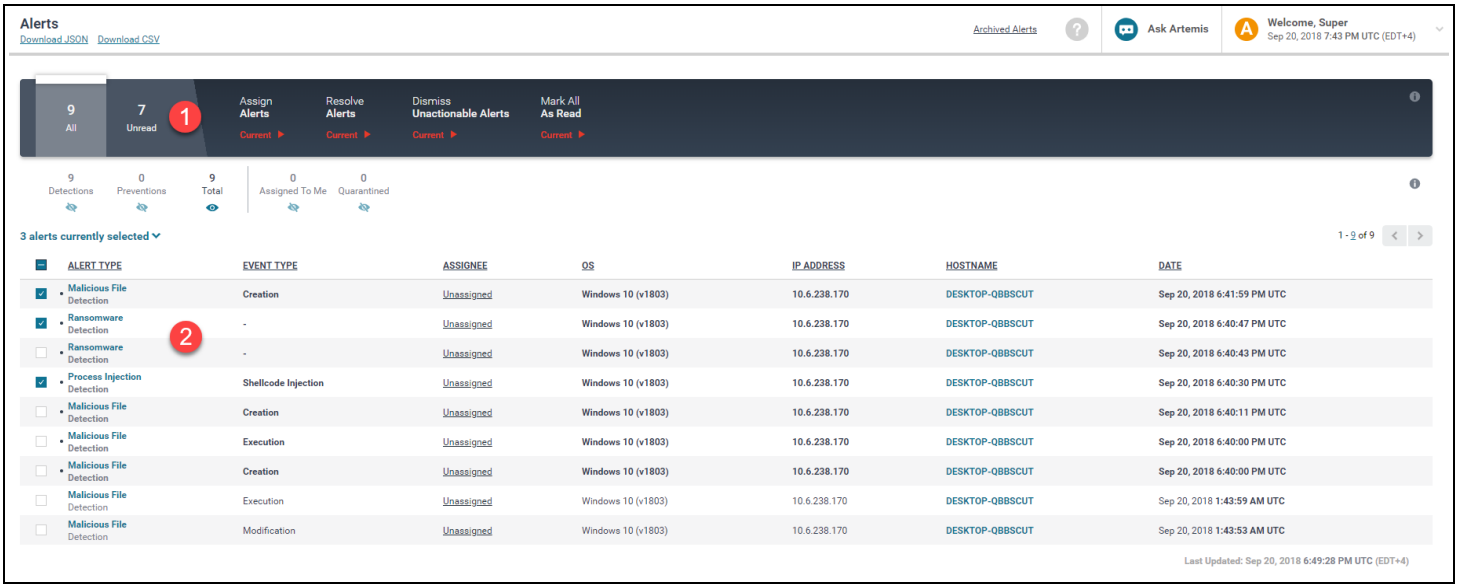
The Alerts page displays essential details about all alerts generated in the Endgame platform and provides options to filter, respond to, and manage them.

The Alerts page contains two major sections:

1. Action toolbar
2. Alerts list

To view the Alerts page, click the **ALERTS** button  on the Left Navigation toolbar to view the Alert Dashboard, then choose one of the following options:

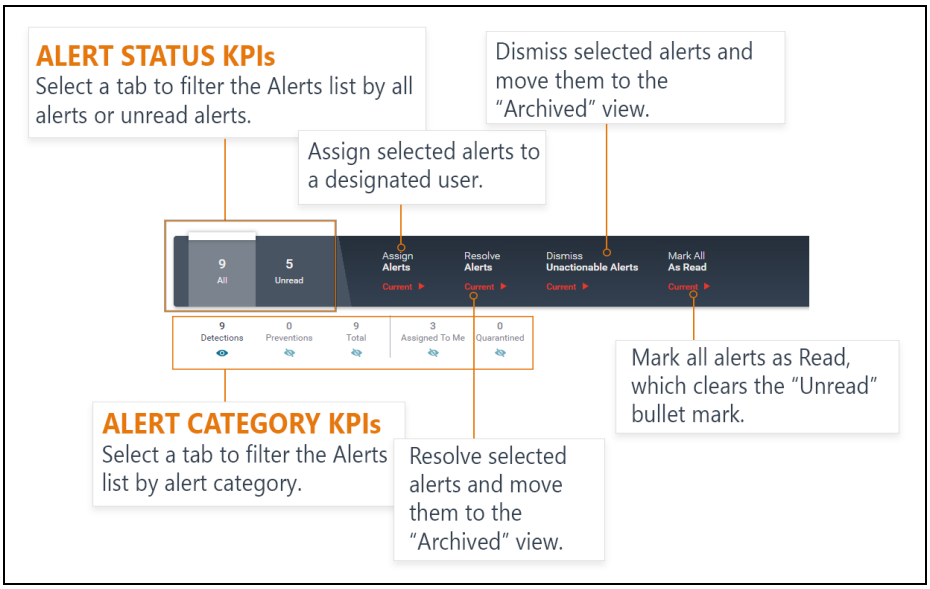
- Select a value on the Threats or Adversary Behaviors chart, which shows a filtered view of alerts that fall within the selected category
- Click **View All Alerts** on the Totals chart on the far right to view all generated alerts



Alerts page

Action Toolbar

The Action toolbar is located at the top of the Alerts page and enables you to execute various tasks for selected alerts. It also contains various key performance indicators (KPIs) to narrow alerts by specific parameters.



Action toolbar on the Alerts page

Alert Key Performance Indicators

The Action toolbar contains two main KPIs, **All** and **Unread**, that display the total number of alerts and the total number of unread alerts, respectively.

A secondary set of KPIs beneath the toolbar displays the number of alerts that fall within a specific category:

KPI	Description
Detections	Potentially malicious activities on monitored endpoints that were detected but require remediation.
Preventions	Malicious activities on monitored endpoints that were detected and blocked.
Quarantined Files	Malicious File alerts that contain quarantined files.
Assigned To Me	Alerts that are assigned to you.
Total	The total number of generated alerts.

Each KPI is an active link, that when selected, filters the Alerts list by the selected category. Filters are useful to narrow alerts by specific criteria to find targeted data. For example, to view all unread detections, select **Unread**, and then select **Detections**.

Alert Actions

The Action toolbar also contains three menu options that execute specific tasks for selected alerts simultaneously:

Menu Option	Function
Assign Alerts	Assigns alerts to a specific user.
Resolve Alerts	Resolves alerts and moves them to the Archived view.
Dismiss Unactionable Alerts	Dismisses alerts and moves them to the Archived view.
Mark All As Read	Marks all alerts as read and clears the "Unread" bullet mark.

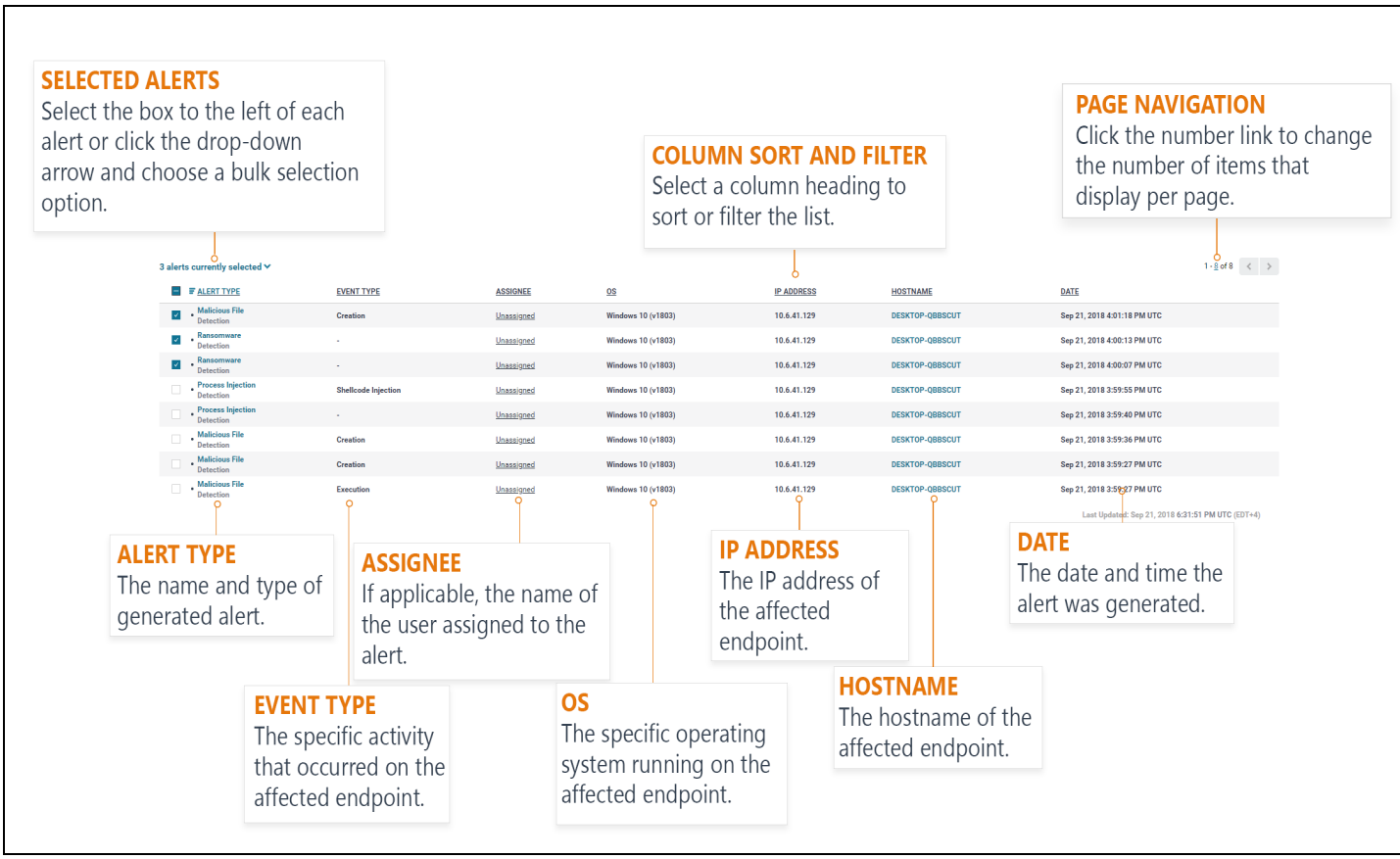
Dismissing or resolving an alert moves it to the Archived view. For more information about alert responses, see "Respond to an Alert" in this chapter.

Alerts List

The Alerts list is an enumeration of all generated alerts and their relevant details, organized in a table. The list is useful to view the history of accumulated alerts to identify outliers or abnormal endpoint activity. For example, if the list shows several alerts for a process injection that each occurred one minute apart, this could signify an attempted data breach that requires an immediate response.

Alerts display in reverse chronological order with the most recently generated alerts at the top. Unread alerts are distinguished with a bullet mark • that disappears after the current user views the alert.

NOTE: The bullet mark • appears on each user's screen until they view it. Therefore, if another user is logged in to the platform and views the alert, it still appears as new to the current user.



Columns in the Alerts list

The columns in the list provide the following information about each alert:

Column Name	Description
ALERT TYPE	The name of the alert and whether it is a detection or prevention.
EVENT TYPE	Specifies the type of activity that occurred on the affected endpoint (e.g., "Shellcode Injection" for a Process Injection alert). **NOTE:** If an alert was triggered by a Custom Rule, the event type is listed as the user-created rule name.
ASSIGNEE	If applicable, the name of the user assigned to the alert. If no user is assigned, the column says, "Unassigned." **TIP:** You can click the "Unassigned" link to assign a user to the current alert.
OS	The operating system running on the affected endpoint.
IP ADDRESS	The IP address of the affected endpoint.

Column Name	Description
HOSTNAME	The hostname of the affected endpoint.
DATE	The date and time the alert was generated according to Coordinated Universal Time (UTC).

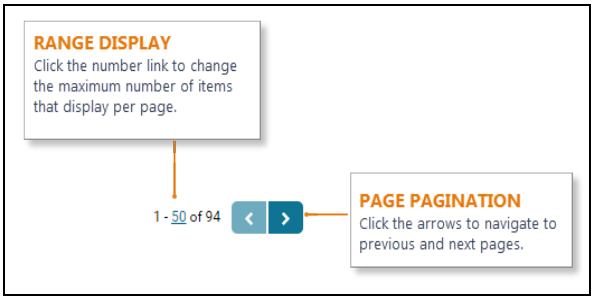
> **NOTE:** If you filter the list by alert type, the columns change to display data relevant to the alert type. For more information, see "Sort and Filter Alerts."

Page Pagination

In the upper-right corner above the list is a range display, which displays the current number range of alerts out of the total (e.g., 1-50 of 400). Click the left and right arrows to navigate to previous and next pages.

By default, a maximum of 50 alerts display per page; however, you can change the number to a preferred choice:

1. On the range display, click the number link. For example, if the range display is 1-50, click **50**.
2. In the **Max count of** text box, enter a new number between 1 and 500.
3. Click ✓ to save your changes.

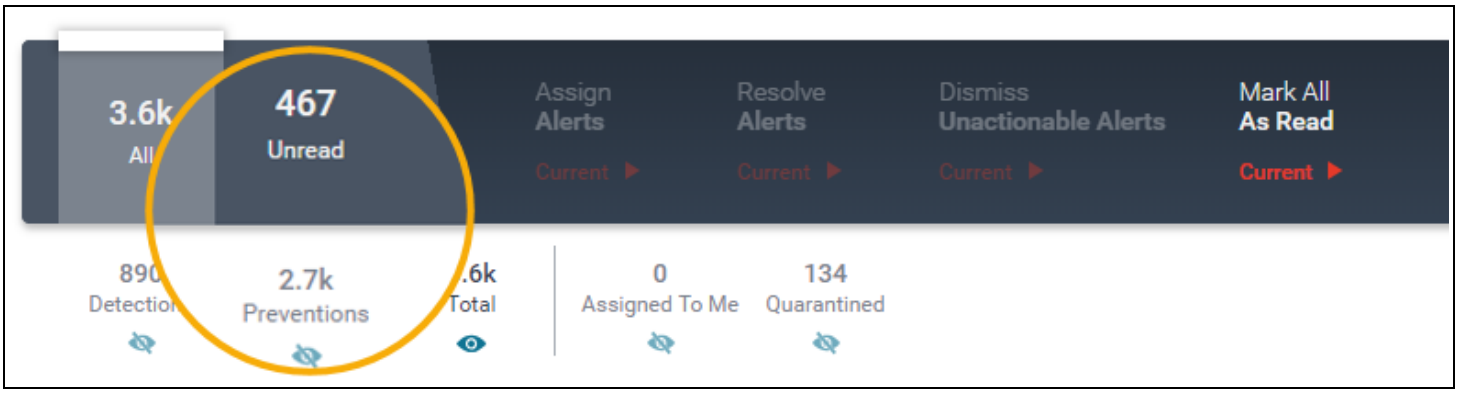


Sort and Filter Alerts

Aside from the filters on the Alert Dashboard, the Endgame platform provides other options to sort and filter alerts. Sorting and filtering are time-efficient methods to find specific information without browsing through a large amount of data. In addition, it helps prioritize which alerts require an immediate investigation or remedial action.

Filter by Key Performance Indicator

Each key performance indicator (KPI) on the Alerts page is an interactive link that filters the Alerts list by the selected category. For example, to view all unread preventions, select **Unread**, then select **Preventions**.

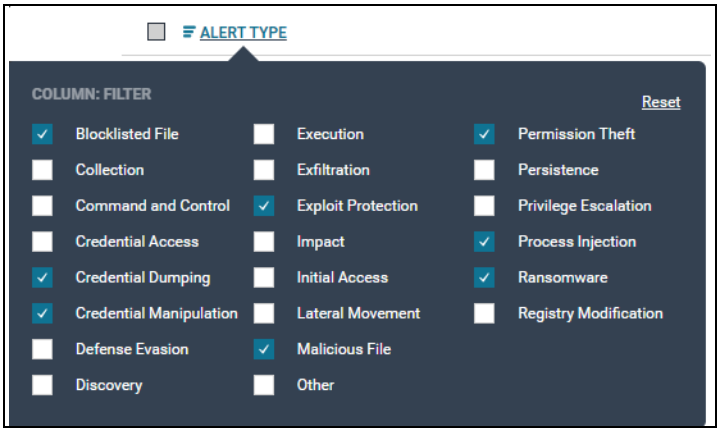


KPIs on the Alerts page are also selectable filters

Filter by Alert Type

Filtering by alert type narrows alerts by selected threats or adversary behaviors, which can identify false positives or behavioral trends. To filter by alert type, select the **ALERT TYPE** column heading, then select the box to the left of each appropriate alert type. If you select a single alert type, the columns in the Alerts list change to display data relevant to the selected type. However, if you select more than one alert type to filter by, the standard set of columns appears in the list.

> **NOTE:** If you select the Threats or Adversary Behaviors numerical value on the Alert Dashboard, the alerts that fall within the selected category are automatically selected in the "ALERT TYPE" column.



Filter by alert type

Sort by Order

To sort by ascending or descending order:

1. Select the appropriate column heading. The Column Sort and Filter panel appears.
2. In the **COLUMN: SORT** section, select the **Ascending** option to sort by increasing value or the **Descending** option to sort by decreasing value. The currently sorted column is denoted by an arrow ↑.

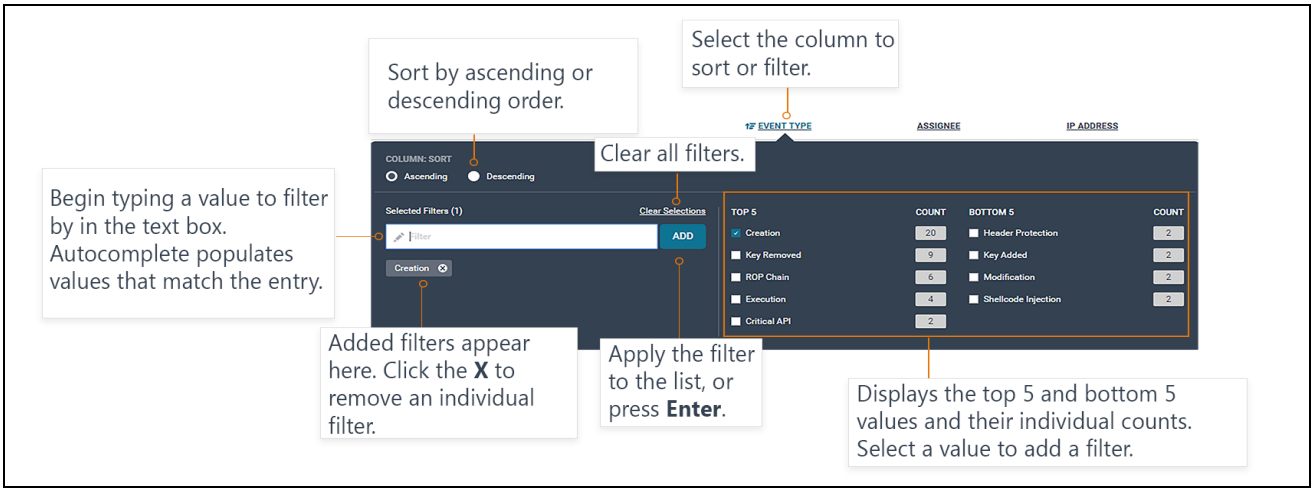
Filter by Value

You can filter columns in the Alerts list by one or more specific values by doing the following:

1. Select the appropriate column heading. The Column Sort and Filter panel appears.
2. Choose one of the following options to add filters:
   - In the **Selected Filters** section, begin typing a value in the text box. Autocomplete displays the value(s) that matches the entry. Select the appropriate value, and then click **ADD** or press **Enter**.

> **TIP:** If you do not know the exact name, type a wildcard character (*) anywhere in the text to help find desired values.

   - Select the appropriate values from the **TOP 5** and/or **BOTTOM 5** columns. These are auto-populated values that display the five highest and five lowest values from the selected column, which is useful to view possible values of interest. The numerical count of each value is also displayed in a separate column. Each added value appears as a selectable filter.



Column sort and filter panel

> Values in the bottom 5 are less common, therefore, it is recommended you analyze alerts within this category to determine if there are any outliers.

After you sort a column by order or apply filters, the Alerts list updates with the new data. The currently filtered column is denoted by an symbol, and columns that are sorted and filtered are denoted by an symbol.

> **NOTE:** If you select values from the top or bottom 5, you do not have to click **ADD** — they automatically appear as filters.

Remove Filters

To remove a filter from a column:

1. Select the appropriate column heading. The Column Sort and Filter panel appears.
2. Choose one of the following options:
   - In the **Selected Filters** section, click the **X** on the appropriate filter.
   - Deselect the appropriate values from the TOP 5 or BOTTOM 5.
   - To remove all filters, click **Clear Selections**.

TIP: To clear all column filters and the sort order, select the **All** tab on the Action toolbar.

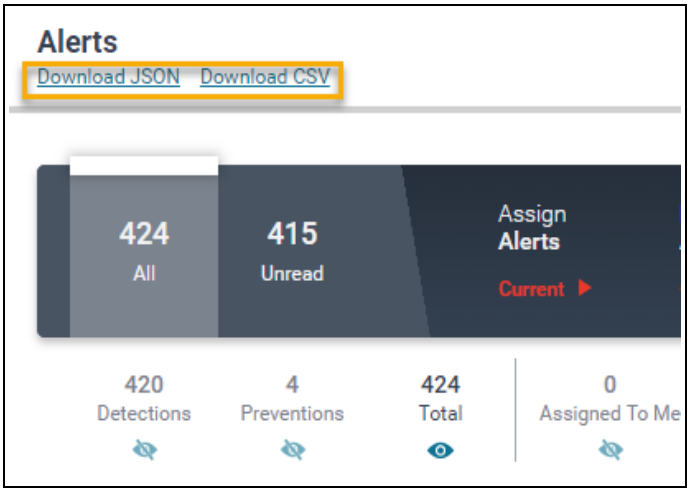
Download the Alerts List

You can download the current Alerts list to a comma-separated values (CSV) file or JSON file. Any sort and filter preferences applied to the list are retained in the downloaded file.

> **NOTE:** Downloading the Alerts list to an external file is different from exporting the list to a third-party tool.

To download the Alerts list:

1. In the upper-left corner of the Alerts page, click **Download JSON** or **Download CSV.**



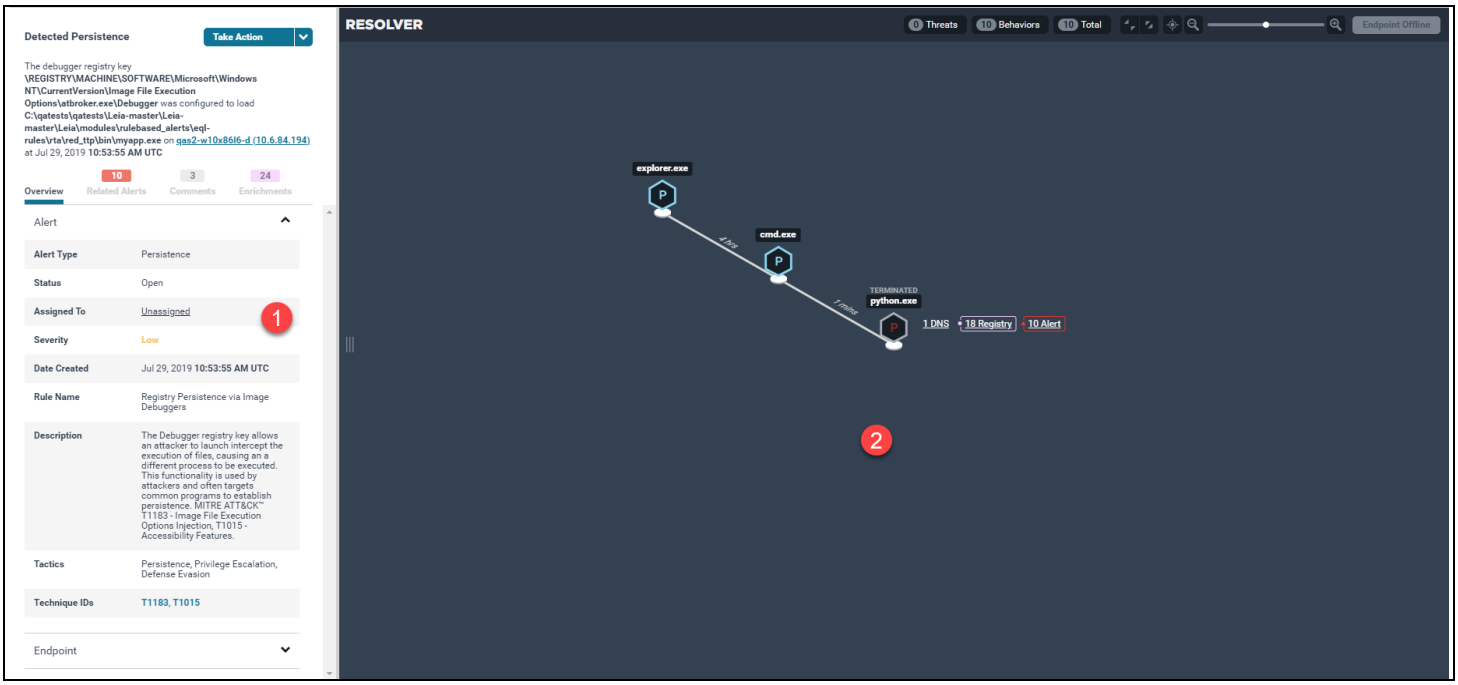
2. When the download is complete, open or save the file from your browser.

Alert Details Page Overview

The Alert Details page provides comprehensive details about the selected alert, various user actions to respond to the alert, and it displays the Endgame Resolver™ Attack Visualization, which shows the series of events that led to the alert.

The Alert Details page contains two sections:

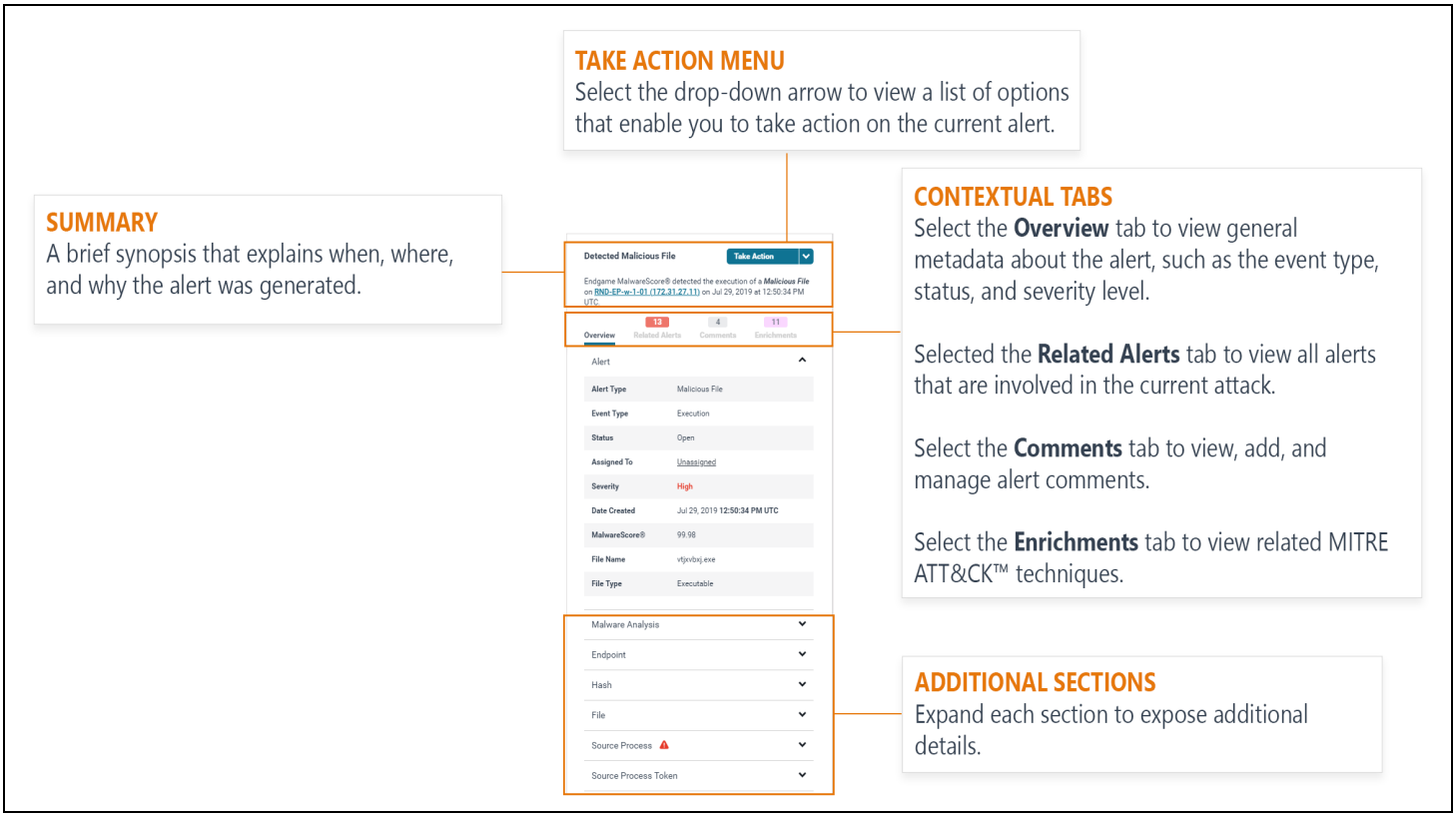
1. Alert Metadata panel
2. Endgame Resolver™ Attack Visualization



Alert Details page

Alert Metadata Panel Overview

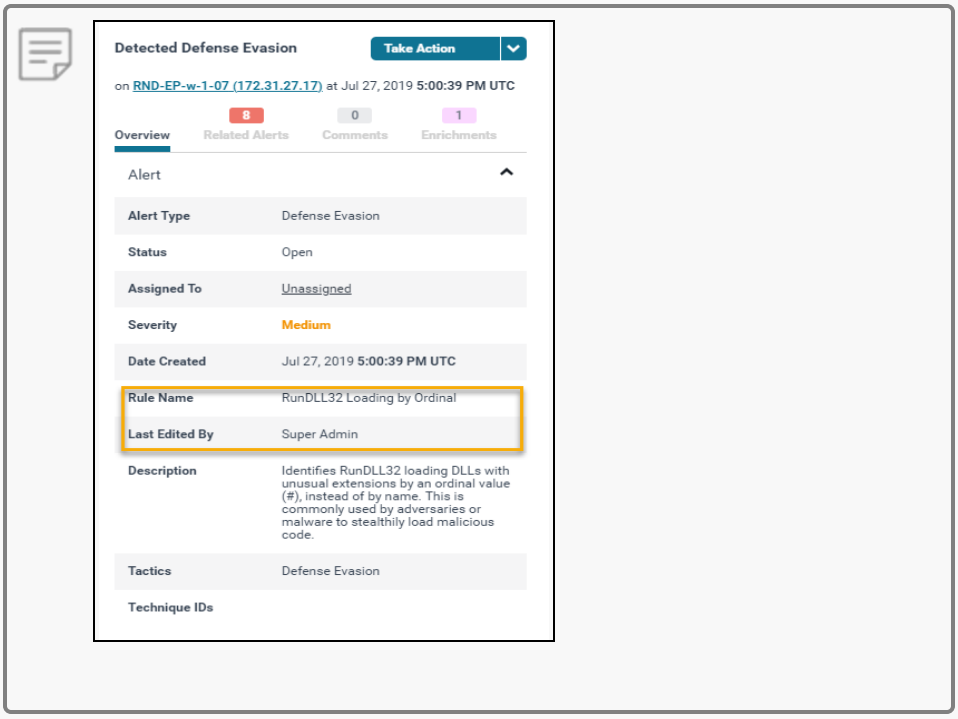
The leftmost side of the Alert Details page displays the Alert Metadata panel. The panel is an accumulation of alert details, comprised of multiple sections that provide details about a specific data component. When selected, each section expands or collapses to either expose or hide details.



Alert Metadata panel

Although the information displayed in these sections varies according to the alert type, each alert contains the following sections in the metadata panel:

Section	Description
Summary	A brief synopsis that explains what malicious activity occurred to generate the alert, the hostname of the affected endpoint, and the date and time it occurred, according to Coordinated Universal Time (UTC) or your selected time zone.
Overview	General metadata about the alert, including the type, event type, status, assignee, severity level, and the date created. This section displays in an expanded state by default. **NOTE:** If an alert is triggered from a Custom Rule, two additional fields appear In the Overview section: "Rule Name" and "Last Edited By."

Section	Description
	
Related Alerts	A list of threat and behavior alerts related to the current attack. Select an alert to view general details and a list of spawned processes in the Endgame Resolver™. For more information, see "Alert Details Page Overview" in this topic.
Comments	View and add comments about an alert, which are shared among team members who have access to Endgame. For more information, see "Alert Commenting Overview."
Enrichments	A list of unique, related MITRE ATT&CK™ techniques that provide additional contextual information about an alert.
Endpoint	Information about the affected endpoint, including the hostname, IP address, endpoint status, operating system, the total number of generated alerts, and any assigned groups.

The endpoint hostname appears in the "Summary" and "Endpoint" sections and is an active hyperlink that goes to the relative Endpoint Details page.

In the upper-right corner of the Alert Metadata panel is the **Take Action** menu, which contains a list of options that enable you to execute one of the following alert tasks:

Take Action Menu Option	Description
Download Alert	Downloads the raw JSON of the alert details.

Take Action Menu Option	Description
Download Timeline	Downloads the raw JSON of the events that occurred in the Endgame Resolver™ Attack Visualization.
Resolve	Marks the alert as resolved and moves it to the Archived view.
Dismiss	Marks the alert as dismissed and moves it to the Archived view.
Start Investigation	Starts a new investigation.
Kill Process (Exploit alerts only)	Terminates the source process.  **NOTE:** This option is a pivot action on the Endgame Resolver™ Attack Visualization.
Suspend Thread (Process Injection alerts only)	Suspends the malicious process thread by thread ID.
Download File (Malicious File alerts only)	Downloads the malicious file.  **NOTE:** The file must be retrieved from the endpoint before you can download it.
Retrieve File (Malicious File alerts only)	Retrieves the malicious file from the endpoint and sends it to the Endgame platform.  **NOTE:** If the file was previously retrieved, the "Download File" option appears instead. However, the "Retrieve File" option is a pivot action on the Endgame Resolver™ Attack Visualization.
Delete File (Malicious File alerts only)	Deletes the file from the affected endpoint.
Delete from Blocklist (Blocklist alerts only)	Deletes the hash from the blocklist, and, if the option is selected, restores the quarantined file to its original location.
Unarchive Alert	Moves the alert from the Archived view to the Current view.  **NOTE:** This option is available only if the alert was resolved or dismissed.
Add to Exceptionlist	Adds selected alert attributes to the exceptionlist to prevent future alerts from generating.
Isolate Host	Isolates the endpoint to prevent it from communicating with all systems.
Release Host	Releases the endpoint from isolation.

NOTE: Options in the **Take Action** menu only execute a task for the current alert. You can execute a task for multiple alerts from the Alerts page.

Endgame Resolver™ Attack Visualization Overview

The Endgame Resolver™ Attack Visualization is a visual timeline of events that led up to the alert and the events that occurred immediately after the alert. Viewing the Endgame Resolver™ Attack Visualization is useful to determine the origin of the malicious activity and other areas in your environment that may be compromised once that activity is detected. The Endgame Resolver™ provides process, DNS, file, network, image load, and registry data for both parent and child events, and provides one-click response actions to resolve the alert.

> **NOTE:** API, CLR (Common Language Runtime),WMI ((Windows Management Instrumentation), and PowerShell currently are beta events.

How it Works

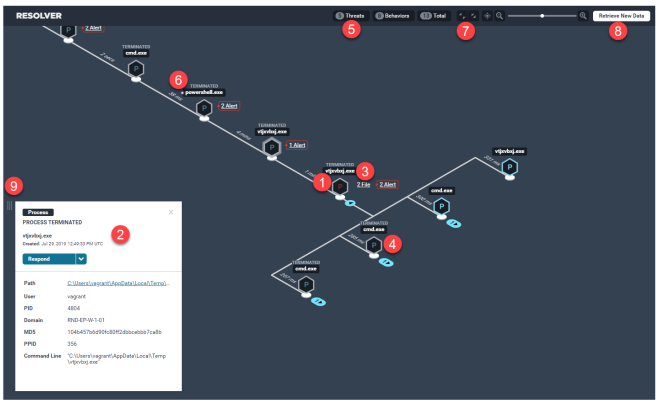
Once an alert is generated, the sensor collects event data and stores it in the Endgame platform. Once you select an alert to view, the Endgame Resolver™ Attack Visualization, which appears on the right-hand side of the Alert Details page, presents the collected event data as a visual timeline to display the series of events that occurred before and following the malicious activity. By default, the Endgame Resolver™ centers on the malicious process that generated the alert. Related events are grouped in a hierarchical structure so you can view events in sequential order.

> **NOTE:** Registry Monitor alerts do not have an Endgame Resolver™ Attack Visualization and display a generic error message in its place.

Endgame Resolver™ Attack Visualization User Interface

The Endgame Resolver™ Attack Visualization contains the following user interface components:

1. Event nodes
2. Event Metadata card
3. Child events
4. Child process event nodes
5. Related Alerts
6. Alert Enrichments
7. Endgame Resolver™ controls
8. Endgame Resolver™ timeline status
9. Expand/Collapse



ENDGAME RESOLVER ATTACK VISUALIZATION™

1. **Event nodes**. Represents each process event that occurred before and after the alert was generated.
2. **Event Metadata card**. Displays process details when an event node is selected.
3. **Child events**. DNS, network, file, or registry child events that spawned from the parent process. Select a link to view those events on the Event Metadata card.
4. **Child process events**. Process events that spawned from the parent process.
5. **Related Alert Key Performance Indicators (KPIs)**. Displays the number of related alerts that are categorized as threats and behaviors. The total number is the summation of these categories. Select a KPI to view those alerts in the Alert Metadata panel.
6. **Alert Enrichments.** Related MITRE ATT&CK™ techniques that provide additional information about an alert. Select an enrichment (denoted by a purple circle next to the process name) to view details in the Alert Metadata panel.
7. **Endgame Resolver™ controls**. Control the Resolver view: Reset, Expand All, Center, and Zoom.
8. **Endgame Resolver™ status**. Indicates the current status of data displayed in the Resolver.
9. **Expand/Collapse button**. Expand the Resolver to a full page and hide the Alert Metadata panel. Click the button again to collapse it.

Endgame Resolver™ Attack Visualization on the Alert Details page

Event Nodes

Each process event that occurred before and after the alert was generated is called an "event node" and is denoted by a hexagonal icon with the letter "P." A time value is displayed between each event node to indicate how much time passed between the previous and next event.

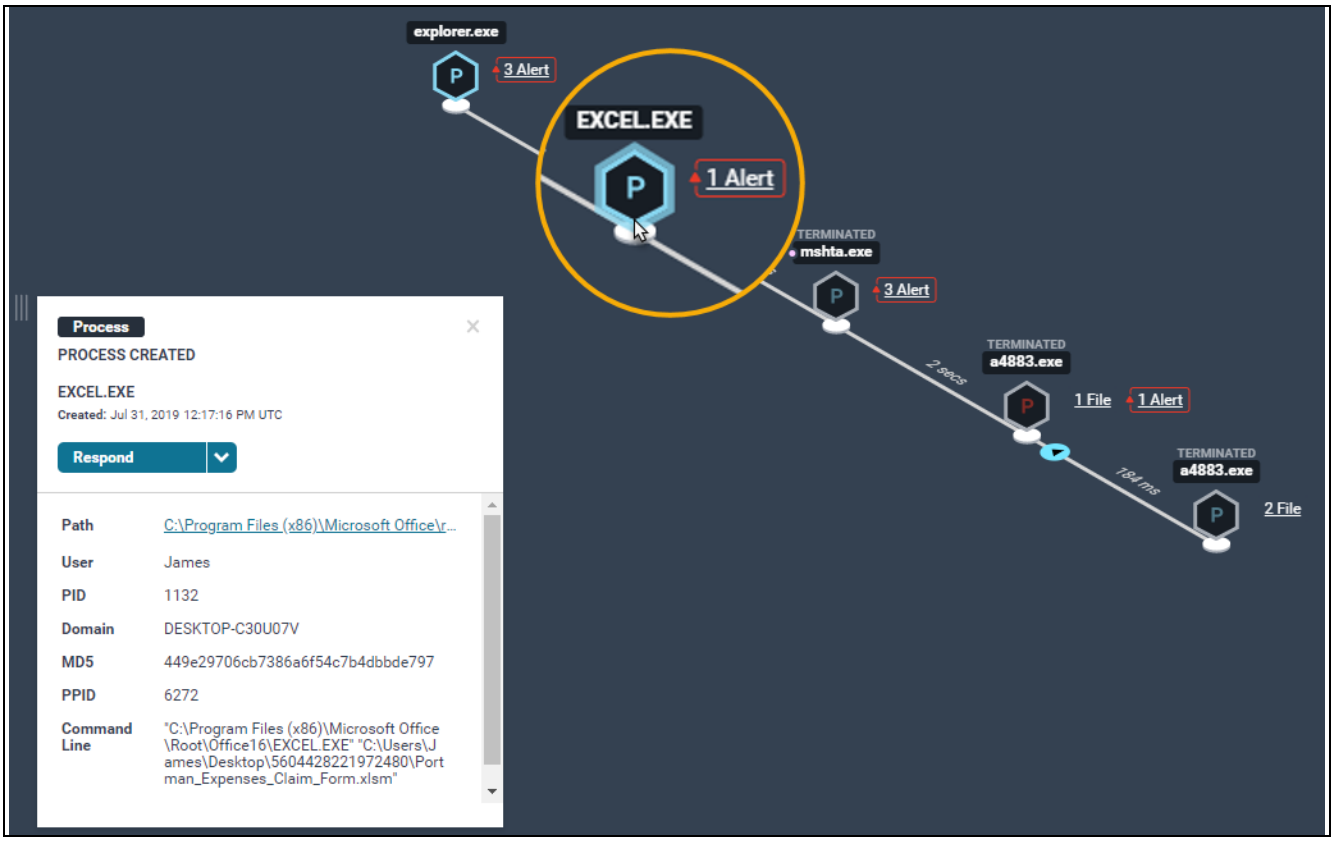
> The time values are listed as milliseconds (ms), seconds (secs), minutes, (mins), hours (hrs), and weeks.

Event nodes are color-coded to indicate the status of the process:

Color	Status	Description
Blue	Benign	The sensor did not determine the file is malicious.
Red	Malicious	The sensor determined the file is malicious.
Gray	Terminated	The process was terminated via a "kill process" task.

Process Details

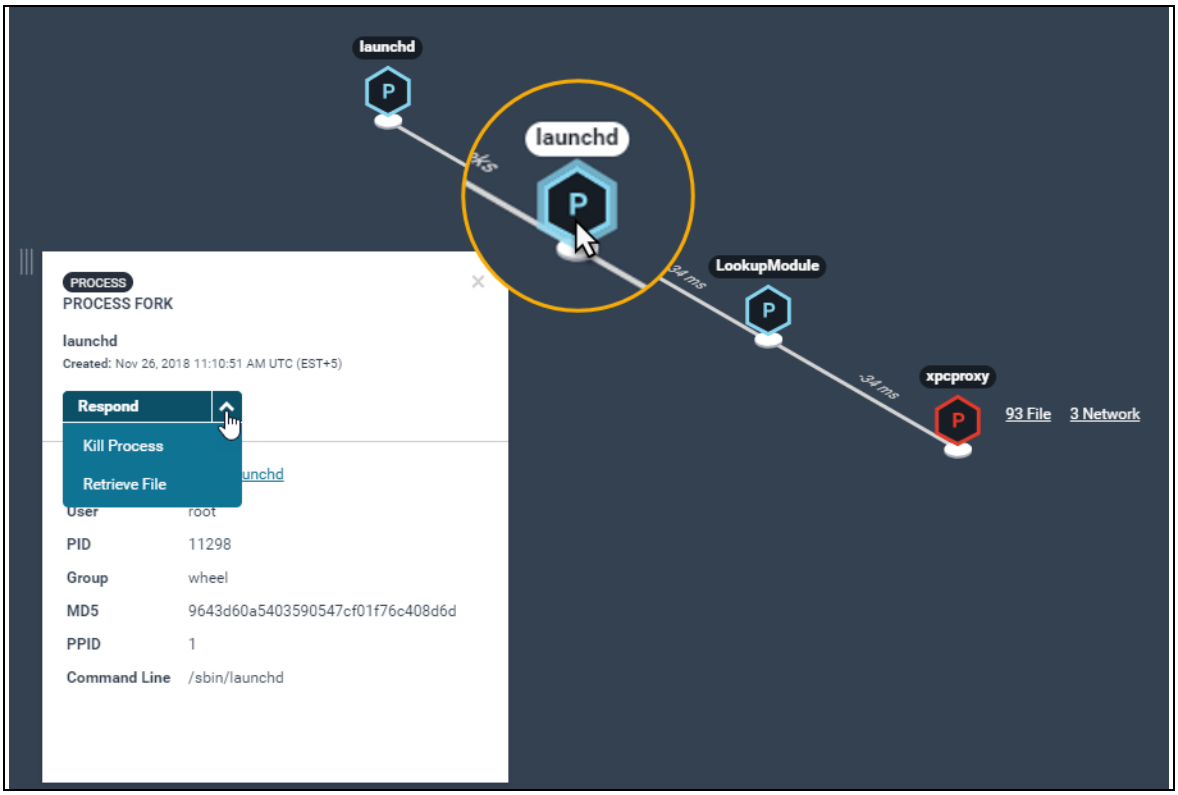
To view details of a specific process, select the appropriate event node, which displays an Event Metadata card. The card provides the event type (e.g., process running, process created, process terminated, etc.), the date and time the process event occurred, and additional data such as the path, user, PID, domain, and MD5 hash value. The **Respond** drop-down menu contains two options to either retrieve the file or kill the process, which is a method of responding to the alert if it requires you to take action.



*Select an event node to view details in the Event Metadata card. Click the **Respond** drop-down arrow to kill the process or retrieve the file.*

> **NOTE:** The "Process Terminated" event type appears on the Event Metadata card only if the **Kill Process** response was executed successfully. The "Retrieve File" response sends a "Get File" task to transfer the file from the endpoint to the platform. After this task is executed, you must download the file — which is in a password-protected zip file — from the Endpoint Details page. For more information, see ""Endpoint Response Types and Advanced Configuration Options.""

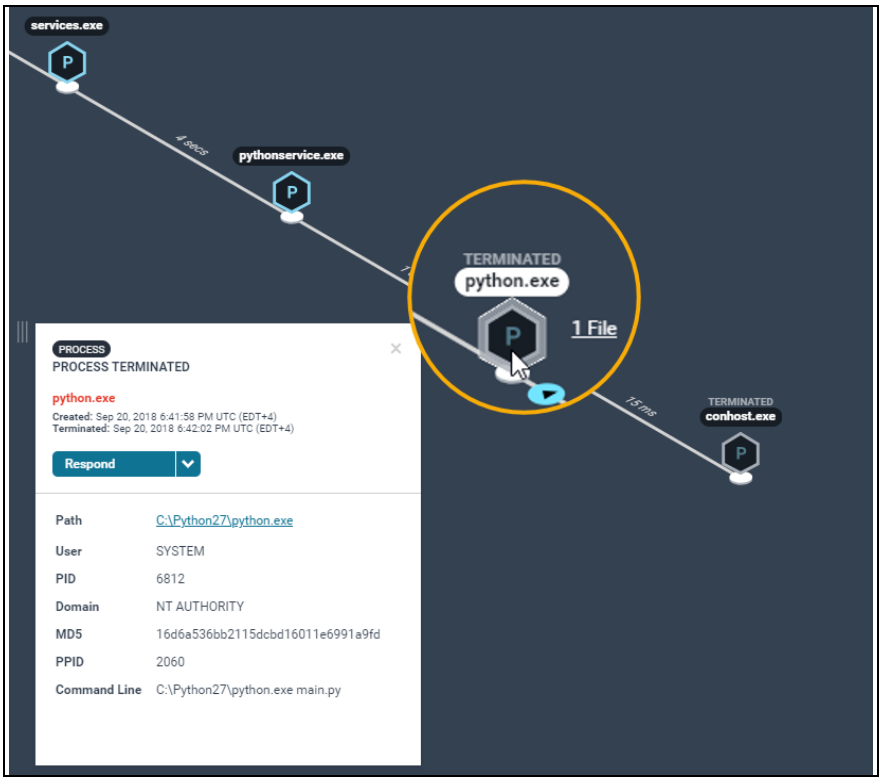
macOS events contain fork and exec processes:



Process fork running on a Mac endpoint

About Terminated Processes in the Endgame Resolver™

If a process was terminated, the hexagonal borders of the event node appear gray to indicate the process was killed. If you terminate a process via the inline "Respond" option in the Endgame Resolver™, you must first retrieve the latest data before you can see it in the timeline. For more information, see "Retrieve New Timeline Data in the Endgame Resolver™."

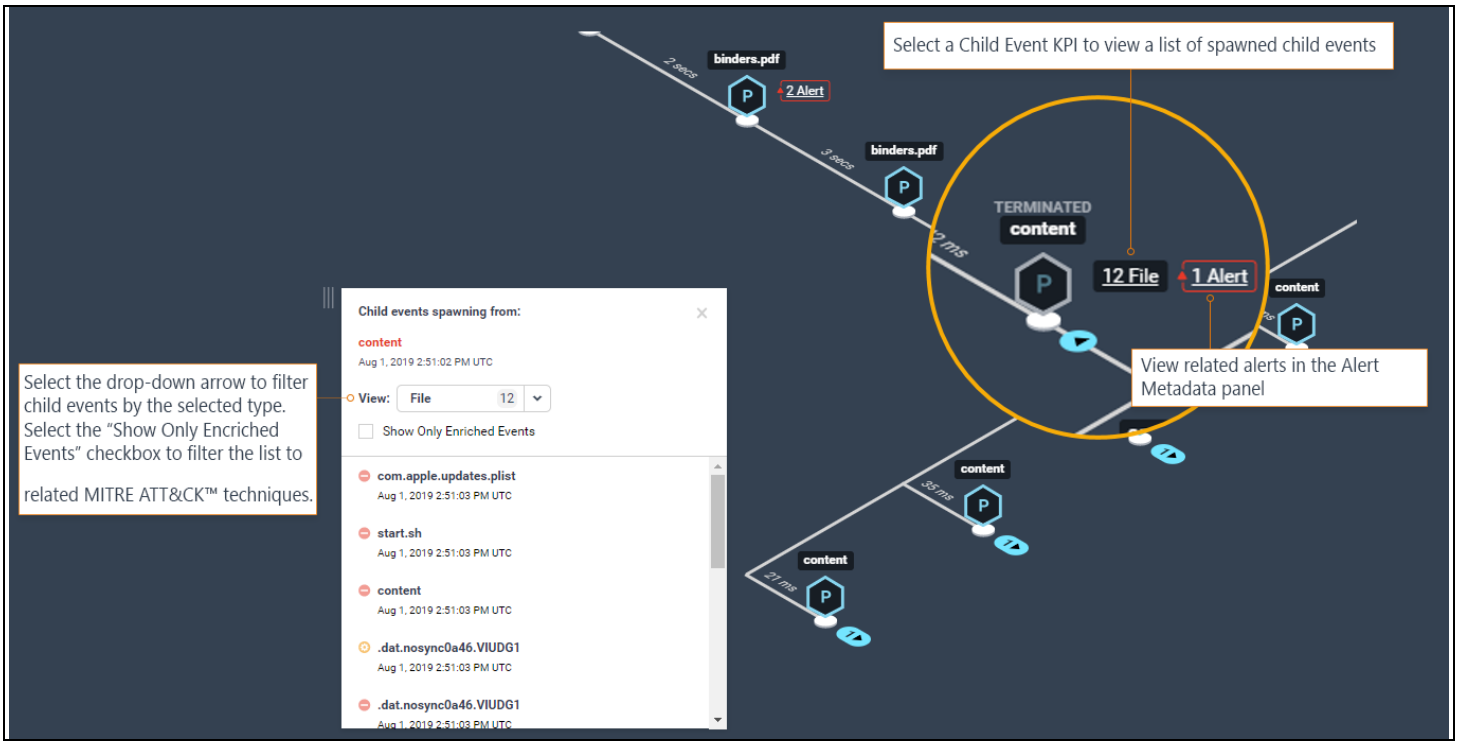


A terminated process in the Endgame Resolver™

Child Events

If there are process, DNS, network, file, or registry child events that spawned from the parent process, a group of numerical values that represent the number of child events, called Child Event KPIs (Key Performance Indicators), displays to the right of the event node. The DNS, network, file, and registry values are active hyperlinks that display an inclusive list of child events in a secondary window when selected. To view inclusive details about one of these child events, select an event from the list and view details in the secondary window that appears. To switch to a different event type, click the **View** drop-down arrow and select the appropriate option from the list.

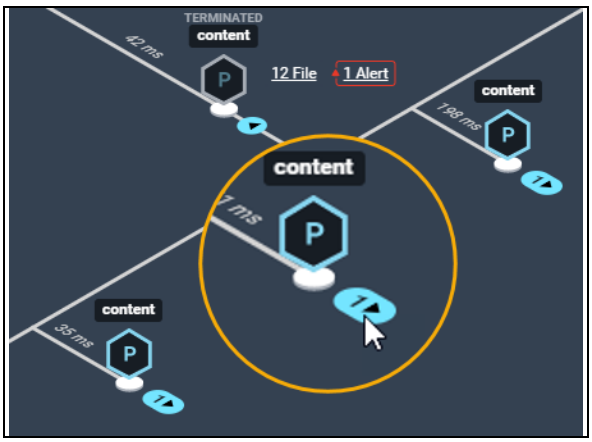
> Endpoints running on macOS do not contain DNS or registry child events.



Select one of the Child Event KPIs to view a list of child events that spawned from the parent process. Select one of the child events in the Event Metadata card to view inclusive details.

Child Process Events

If there are child process that spawned from the parent process, they are denoted by a blue cylindrical button with a number, as seen in the following image:

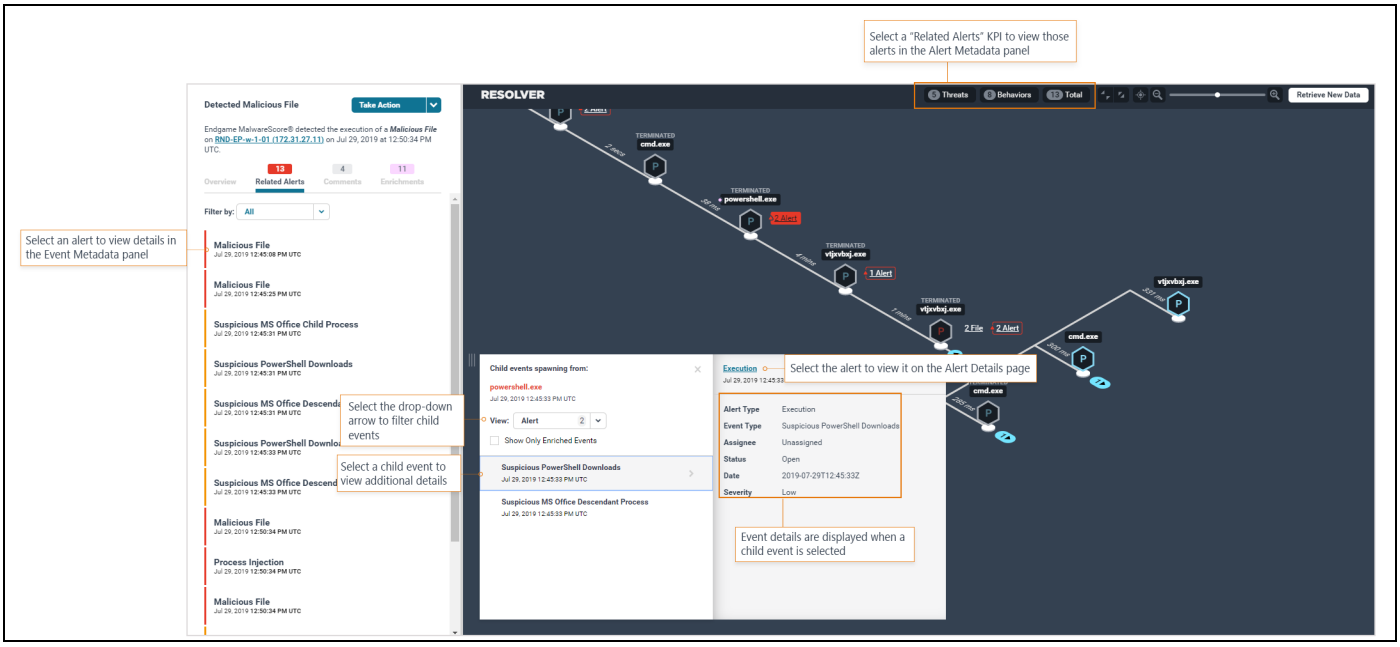


This number indicates the total number of child processes, which you can view in the timeline by selecting the button. Viewing child process events is useful to see what activity occurred on the endpoint after the alert was generated — which is especially recommended for threat alerts. Multiple child processes display at a perpendicular angle and can be collapsed by clicking the blue button again, which, in its expanded state, appears as a small triangle inside a circle.

NOTE: By default, the Endgame Resolver™ displays the first level of child process events. You can continue expanding child process events as necessary.

Related Alerts

At the top of the Endgame Resolver™ are Related Alert Key Performance Indicators, which display the number of threats and behaviors that are related to the same process tree on a single endpoint. Select a KPI to view a list of those alerts in "Related Alerts" tab of the Alert Metadata panel. From here, you can select an alert to view general alert details and spawned child events in the Event Metadata card.



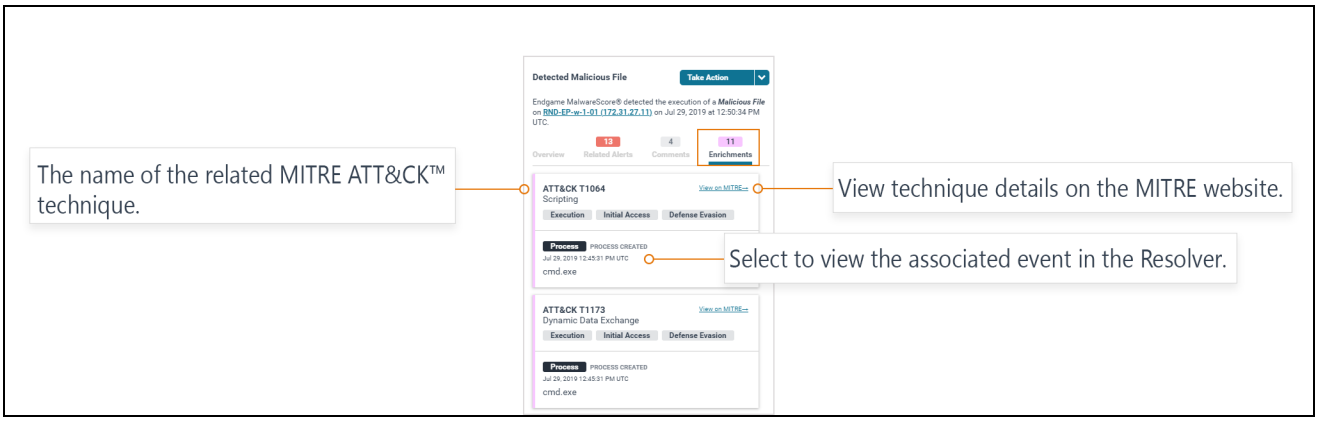
Related Alerts view in the Endgame Resolver™

Viewing related alerts is useful to see all related activity from a single location, identify attack artifacts, and respond to elements of an attack quickly and easily.

TIP: You can filter the list of alerts in the "Related Alerts" tab by selecting the **Filter By** drop-down arrow.

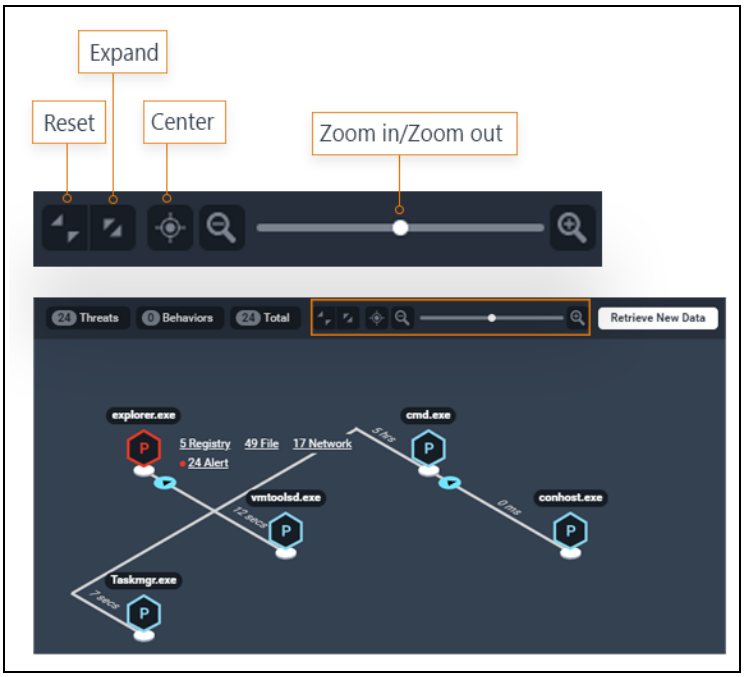
Alert Enrichments

Alert Enrichments are a list of unique, related MITRE ATT&CK™ techniques that provide additional contextual information about an alert. While these actions are not necessarily malicious on their own, enrichments help paint a bigger picture and facilitate the process of scoping a problem and building a response plan. Techniques appear in reverse chronological order, with the most recent events at the bottom. Each technique also contains a link to the associated MITRE page. Select a technique from the list to view the associated event in the Endgame Resolver™.



Endgame Resolver™ Controls

In the upper-right corner of the Endgame Resolver™ are four buttons that enable you to control the current view:



Their functions are as follows:

Name	Button	Description
Reset View		Resets the Endgame Resolver™ to its original view.
Expand All		Displays all available data in the Endgame Resolver™, including child process events beyond the default first level that is displayed.

Name	Button	Description
Center		Re-centers the Endgame Resolver™ on the process at the end of the timeline.
Zoom		Zooms in and out of the Endgame Resolver™. **NOTE:** Zooming out shows a condensed view of the timeline that does not display the Child Event KPIs or the time elapsed between events.

Other Options to Control the Endgame Resolver™ View:

- **Pan:** If data in the Endgame Resolver™ is hidden from view, select any area in the background and drag your cursor to pan up, down, left, or right until the desired data is visible.
- **Expand/Collapse:** To expand the width of the Endgame Resolver™ to a full page and hide the Alert Metadata panel, click the **Expand/Collapse** button  .

Retrieve New Timeline Data in the Endgame Resolver™

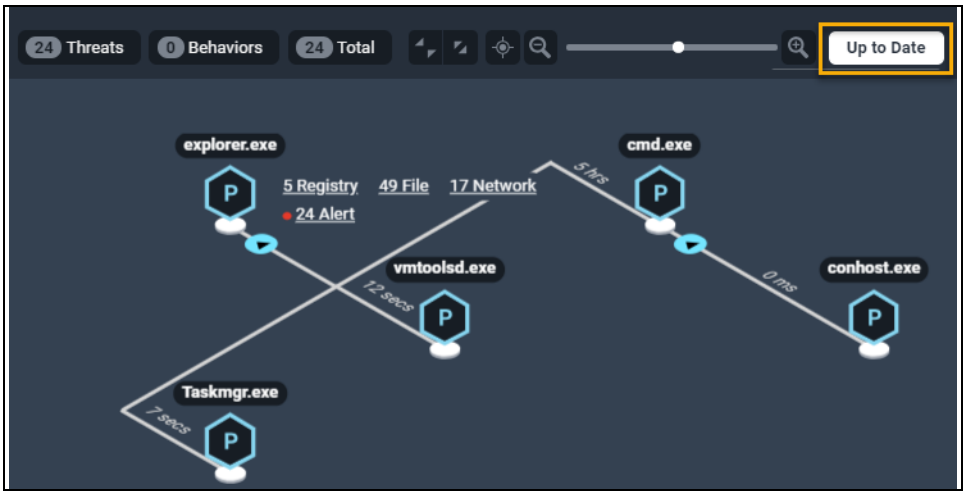
In the upper-right corner of the Endgame Resolver™ is a button that displays the current timeline status. If the status button says "Retrieve New Data," you can initiate a task for the sensor to check for updates of new data.

To update the Endgame Resolver™ with the latest data:

1. Click **Retrieve New Data** in the upper-right corner.

   > **NOTE:** As the sensor is checking for updates, the status changes to "Retrieving."

2. If the sensor has retrieved new data, click **View New Data** to refresh the Endgame Resolver™. If the data in the timeline is up to date, the status button changes to "Up to Date."

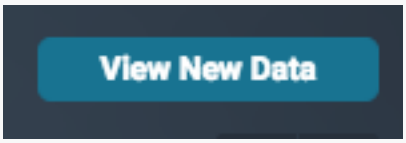
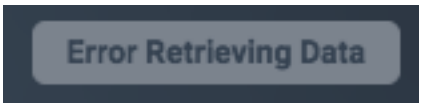
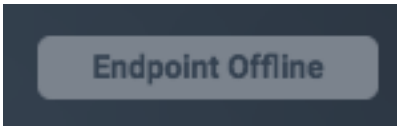


An "Up to Date" status in the Endgame Resolver™ indicates the timeline is displaying the most recent data

Endgame Resolver™ Attack Visualization Statuses

The following table describes the statuses you may see in the upper-right corner of the Endgame Resolver™:

Status	Definition
Loading	The user interface is loading data collected from the sensor. This occurs when the Endgame Resolver™ Attack Visualization is loading for the first time.
Retrieve New Data	Initiates a request to retrieve the latest data from the sensor.
Retrieving	The sensor is currently retrieving the latest Endgame Resolver™ Attack Visualization data.

Status	Definition
	The sensor has returned the latest data. Click this option to refresh the Endgame Resolver™ Attack Visualization.
	The Endgame Resolver™ Attack Visualization user interface encountered an error while communicating with the platform. This can be the result of failing services or sensors. You cannot interact with the resolver in this state.
	Due to a hard-coded limit, the Endgame Resolver™ Attack Visualization is unable to display any more event nodes.
	The endpoint is offline.

Alert Commenting Overview

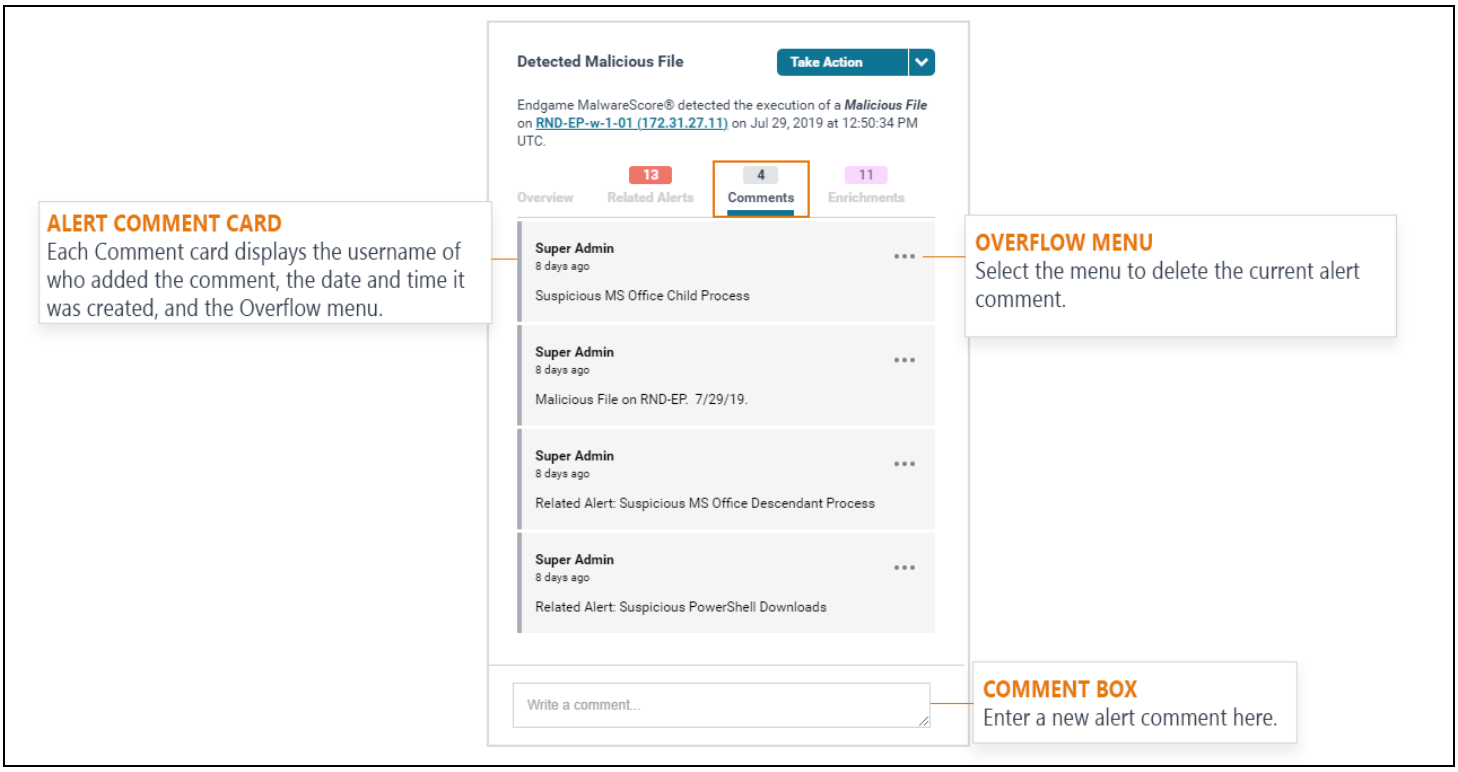
The Alert Details page contains an option to add free-form comments to the current alert. Alert comments are useful to share notes or findings with your team to expedite the alert triage process. All users who have access to the Endgame platform can add alert comments.

Add an Alert Comment

To add an alert comment:

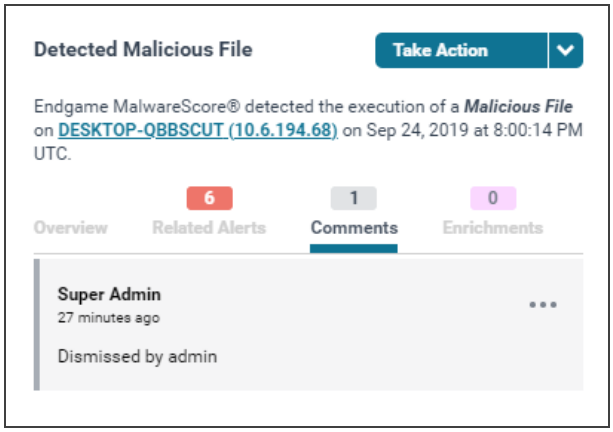
1. Select the **Comments** tab on the Alert Metadata panel.
2. In the **Comment** box, type an alert comment. Ensure it is no more than 1,024 characters. Unicode characters are supported.
3. Click **Add Comment**. The new comment appears in the Comments list.

> **NOTE:** There is a maximum of 100 comments allowed per alert.



Alert Comments list

NOTE: Alerts that have been resolved or dismissed automatically get a comment added. The comment displays the name of the user who executed the alert action, the type of alert action that was executed (i.e., whether it was dismissed or resolved), and the date.



Delete an Alert Comment

NOTE: Level 1, Level 2, and Level 3 users can only delete comments they originally added. Admins can delete all comments. If the alert is dismissed or resolved, the comments are retained in the Archived view.

To delete an alert comment:

1. In the Comments list, locate the appropriate alert comment to delete.
2. Click the **Overflow** menu ••• , then select **Delete Comment**.
3. In the dialog box that says, "Are you sure you want to delete this comment by *user*?" verify that the comment that appears is the correct one to delete, then click **Delete Comment**. A "Comment successfully deleted" confirmation appears.

4. Click **Finish**.

Respond to an Alert

If you receive an alert notification, it is recommended you respond accordingly as soon as possible to prevent malicious activity from going unnoticed, thus preventing a possible data breach. Responding to an alert also helps manage the number of alerts that can accumulate. After you have responded to an alert, it is recommended you mark it as resolved. For more information, see "Resolve an Alert" in this chapter.

In general, once you receive an alert notification and analyze the details, you conclude that it:

a. Requires no response and can be ignored

b. Is a false positive that should be suppressed in the future

c. Requires a response

You can respond to an alert from the following places in the Endgame platform:

- The Take Action menu on the Alert Metadata panel
- A pivot action on the Endgame Resolver™ Attack Visualization
- The Action toolbar on the Alerts page (recommended for multiple alerts)

> **NOTE:** Alert response options in the Take Action menu and Endgame Resolver™ Attack Visualization apply to the current alert only.

The following is a list of Take Action menu items on the Alert Metadata panel that enable you to respond to or execute a specific task for the current alert. Please note the list of options varies by alert type.

Menu Option	Description
Download Alert	Downloads the raw JSON of the alert details.
Download Timeline	Downloads the raw JSON of events that occurred in the Endgame Resolver™ Attack Visualization.
Resolve	Marks the alert as resolved and moves it to the Archived view. For more information, see "Resolve an Alert." **NOTE:** Resolved alerts automatically get a comment added to the "Comments" tab on the Alert Details page. The comment displays the name of the user who executed the alert action and the date.
Dismiss	Marks the alert as dismissed and moves it to the Archived view. For more information, see "Dismiss an Alert." **NOTE:** Dismissed alerts also automatically get a comment added to the "Comments" tab on the Alert Details page. The comment displays

Menu Option	Description
	the name of the user who executed the alert action and the date.
Start Investigation	Starts a new investigation.
Kill Process (Exploit alerts only)	Terminates the source process. **NOTE:** This option is an available pivot action on the Endgame Resolver™ Attack Visualization.
Suspend Thread (Process Injection alerts only)	Suspends the malicious process thread by thread ID.
Download File (Malicious File alerts only)	Downloads the malicious file. **NOTE:** The file must be retrieved from the endpoint before you can download it.
Retrieve File (Malicious File alerts only)	Retrieves the malicious file from the endpoint and sends it to the Endgame platform. **NOTE:** If the file was previously retrieved, the **Download File** option appears instead. However, the **Retrieve File** option is an available pivot action in the Endgame Resolver™ Attack Visualization.
Delete File (Malicious File alerts only)	Removes the file from the affected endpoint.
Add to Exceptionlist	Displays available attributes to add to the exceptionlist.

NOTE: Options in the **Take Action** menu only execute a task for the current alert. However, you can resolve and dismiss multiple alerts from the Alerts page.

Refer to the following scenarios for general guidance on how to respond to an alert:

- As a precautionary measure, it is recommended to always start an investigation when you receive an alert notification.
- If an alert requires no response, select **Dismiss**. This moves the current alert to the Archived view. To dismiss multiple alerts, select each appropriate alert in the Alerts list and click **Dismiss Unactionable Alerts** on the Action toolbar.
- If an alert is a false positive and you want to suppress future alerts from generating, select **Add to Exceptionlist** to add selected attributes to the exceptionlist. For more information, see "Add Threat Alerts to the Exceptionlist."

> **NOTE:** When you add an item to the exceptionlist, there is a default selected option on the dialog box to dismiss all alerts that match the exception rule. It is recommended you leave this option selected.

- If an alert requires an immediate action, select the appropriate response from the **Take Action** menu. For example, if you suspect a process is malicious, you can select the **Delete File** option to remove the file from the endpoint, or to respond to an exploit detection, you can select **Kill Process** option to kill the source process.

Additional Endpoint Responses

The Endgame Resolver™ Attack Visualization also contains two pivot actions that enable you to either retrieve a file or kill a process when you select a process event node. For more information, see "Endgame Resolver™ Attack Visualization Overview."

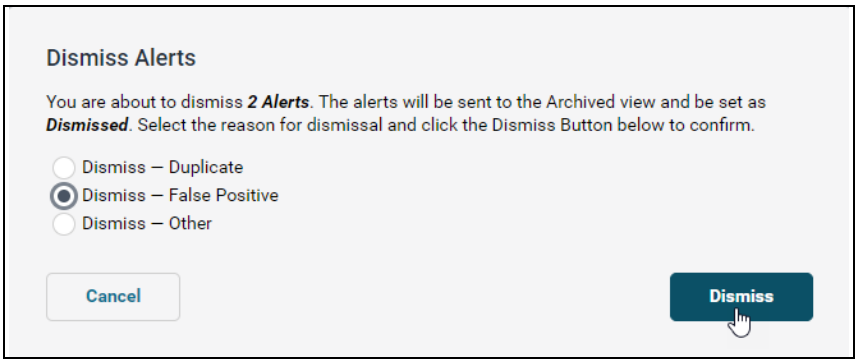
Dismiss an Alert

Dismissing an alert indicates that after analyzing the alert details, the alert does not require further action — for example, if an alert is a false positive or a duplicate. You can dismiss a single alert via the **Take Action** menu on the Alert Metadata panel, or you can dismiss multiple alerts via the Action toolbar on the Alerts page. Once an alert is dismissed, the following automated actions occur:

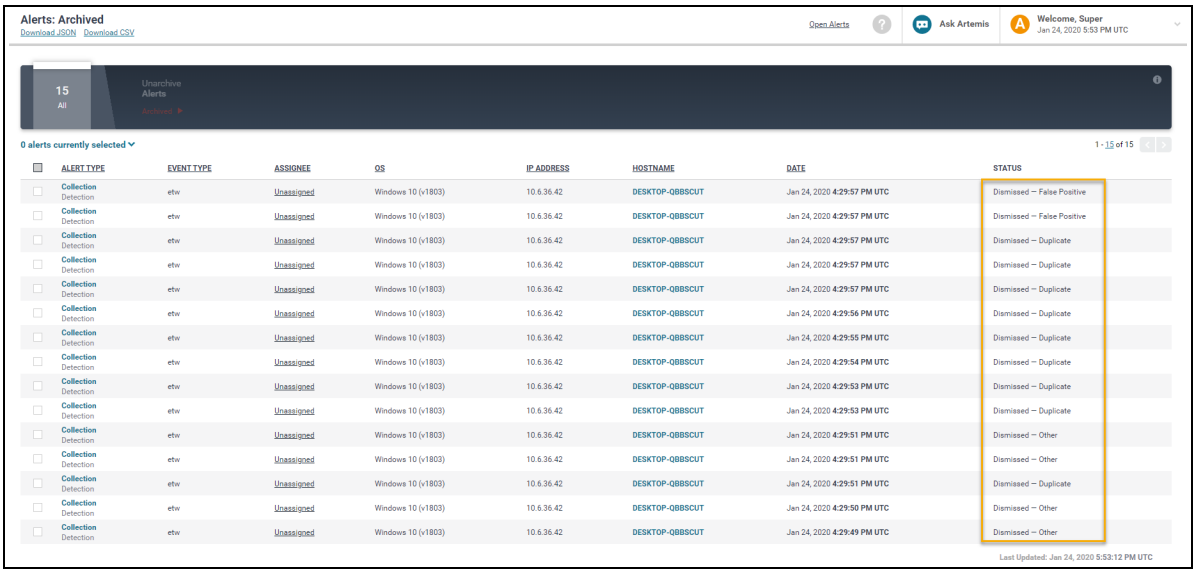
- Alerts are moved to the Archived view
- A comment is added to the "Comments" tab on the Alert Details page. The comment displays the name of the user who executed the alert action and the date

To dismiss multiple alerts simultaneously:

1. In the Alerts list, select the box to the left of each alert to dismiss.
2. On the Action toolbar, click **Dismiss Unactionable Alerts**.
3. In the **Dismiss Alerts** dialog box that appears, select one of the following reasons for the dismissal, then click **Dismiss**.
   - Dismiss — Duplicate
   - Dismiss — False Positive
   - Dismiss — Other
4. A "Successfully dismissed alert(s)" confirmation appears.
5. Click **Finish**.



To view all dismissed alerts, on the Alerts page, click the "Archived Alerts" link in the upper-right corner. The dismissal reason you selected appears in the "STATUS" column of the Alerts list.



Archived Alerts view

Resolve an Alert

After you have responded to an alert, it is recommended you mark it as resolved, which moves it to the "Archived Alerts" page. Resolving an alert keeps the Alerts list updated and distinguishes which alerts were handled from those that require a response. The difference between a resolved alert and a dismissed alert is the former indicates a response action (e.g., download file, suspend thread, etc.) was run; the latter indicates a response action was unneeded.

> **NOTE:** Although prevention alerts block malicious activity, they still need to be marked as resolved.

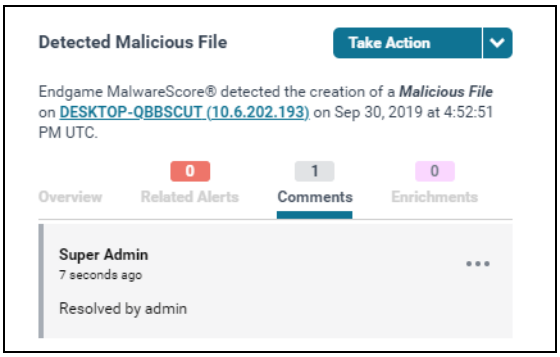
To resolve an alert(s):

1. In the Alerts list, select the box to the left of each appropriate alert.
2. On the Action toolbar, click **Resolve Alerts**.

3. In the **Resolve Alerts** dialog box that says, "You are about to resolve *number* Alerts. The alerts will be immediately sent to the Archived view and be set as Resolved..." click **Resolve**. A "Successfully resolved alert(s)" message appears.
4. Click **Finish**.

> To resolve a current alert displayed on the Alert Details page, click **Take Action**, then select **Resolve** from the list.

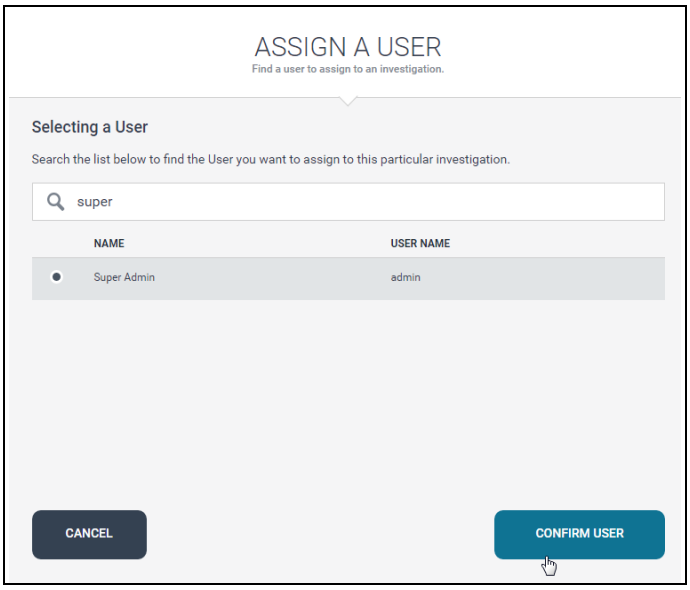
Resolved alerts automatically get a comment added in the "Comments" tab on the Alert Details page. The comment displays the name of the user who executed the alert action and the date.



Assign an Alert

To assign an alert(s) to a specific user to investigate:

1. In the Alerts list, select the box to the left of each appropriate alert.
2. On the Action toolbar, click **Assign Alerts**. The **ASSIGN A USER** dialog window displays a list of all registered users and their designated usernames.
3. Choose one of the following options to locate the appropriate user:
   - In the **Search User Name** text box, begin typing their first or last name. The list filters to name(s) that match the entry. If no matching users are found, an **INVALID USER** error message appears.
   - Scroll the list and locate the user's name.
4. Select the option button to the left of the appropriate user's name.
5. Click **CONFIRM USER**. In the Alerts List, the assignee's name appears in the **ASSIGNEE** column.



Assign an alert to a user

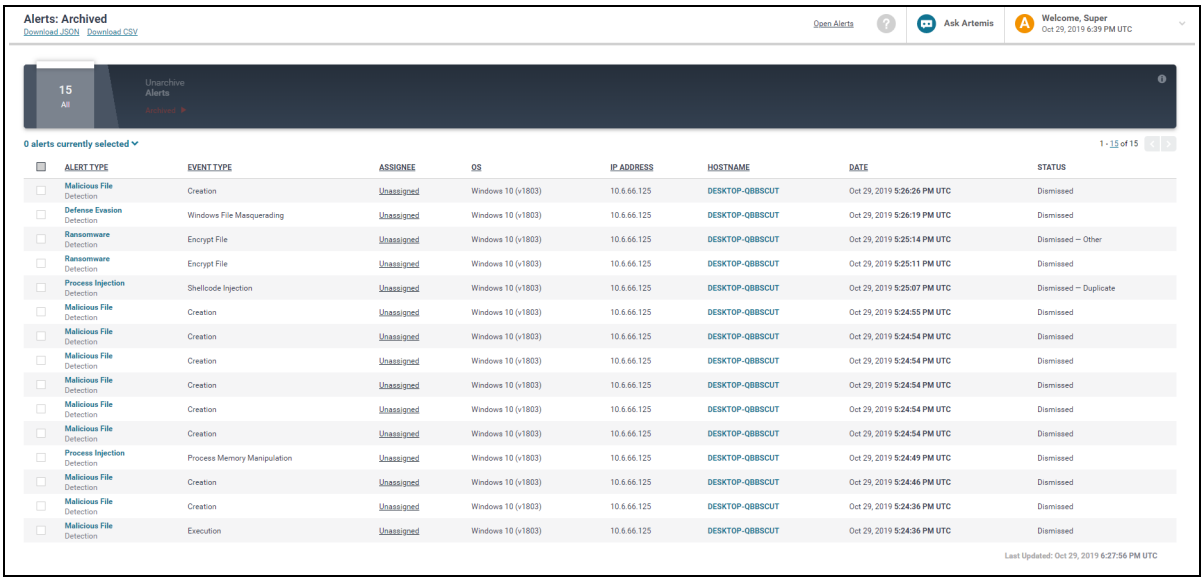
> **TIP:** To assign a single alert to a user or to change the current assignee, either click the link in the **Assignee** column, or on the Alert Metadata panel, click the link in the **Assigned To** field.

Archived Alerts Page Overview

The Archived Alerts page is an enumeration of all alerts that have been resolved or dismissed, and their relevant details, organized in a table. It also contains an option on the Action toolbar to unarchive selected alerts.

> **NOTE:** If you selected a reason for an alert's dismissal, it appears in the "Status" column.

To display the Archived Alerts page, click the "Archived Alerts" link in the upper-right corner of the Alerts page.



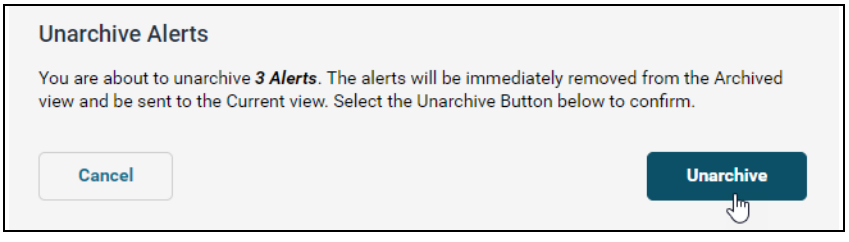
Archived Alerts page

Unarchive an Alert

If you mistakenly dismissed or resolved an alert, you can unarchive it, which moves it back to the default view on the Alerts page.

To unarchive an alert(s):

1. In the Alerts list, select the box to the left of each appropriate alert to unarchive.
2. On the Action toolbar, click **Unarchive Alerts**.
3. In the dialog box that says, "You are about to unarchive *number* Alerts. The alerts will be immediately removed from the Archived view and be sent to the Current view..." click **Unarchive.** A "Successfully unarchived alert(s)" message appears.



4. Click **Finish.**

CHAPTER 5

ARTEMIS

Artemis Search Overview

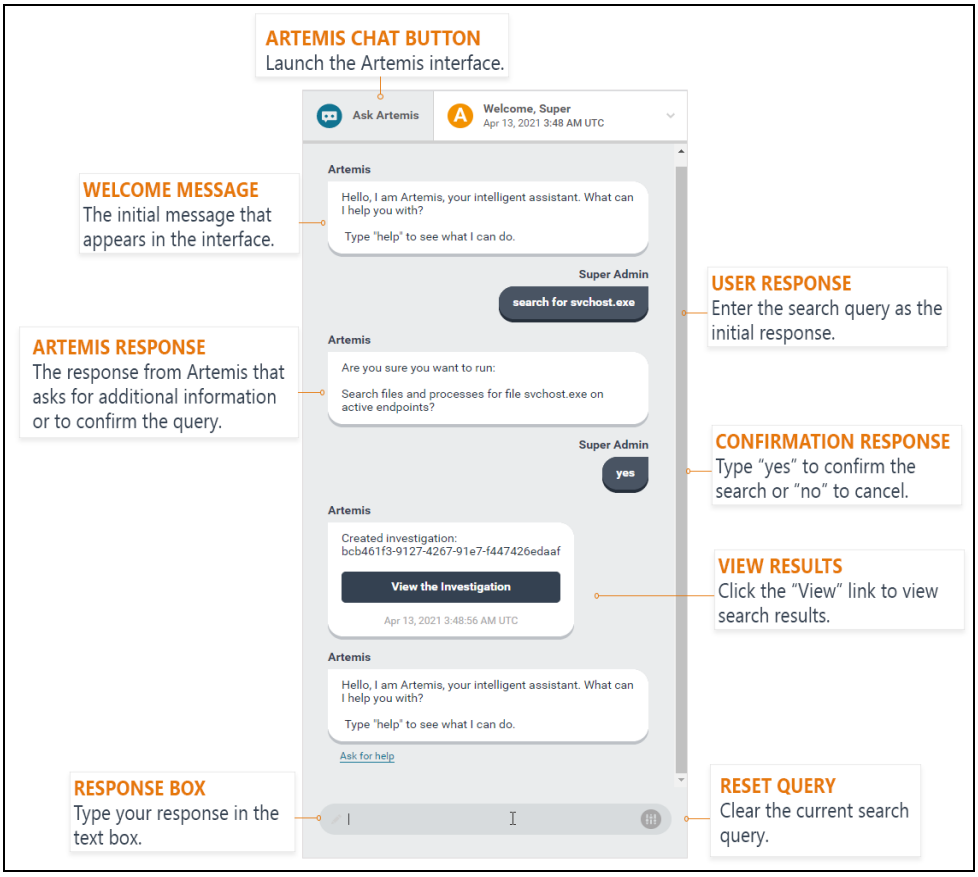
After a sensor is deployed to a Windows, Linux, or macOS endpoint, it enables collection of various events as they occur and stores the data on the endpoint. You can then search for this historical data using Artemis, Endgame's intelligent assistant that executes a precision query based on your input. You can also use Artemis to search for current endpoint data.

Endgame's sensor stores a maximum of 500 MB of event data. The time frame of how far back you can search for event data depends on how much activity occurs on the endpoint. Once the sensor has reached the maximum amount of data, the oldest data is deleted.

> **NOTE:** In order for Windows to store user logon events, the "Audit account logon events" setting in Windows Local Security Policy must be configured. For more information, see "Verify that Logon Events are Enabled in Windows."

Artemis User Interface

Artemis' interface is a narrow chat window that enables you to have an interactive conversation. Once you type the search criteria in the text box, it either asks for more details so it can formulate a precise query, or it asks you to confirm the search. The natural, conversational language enables you to find targeted event data without having to construct a query language-based search.



Artemis user interface

About Artemis Queries

An Artemis query is a formulated search that enables you to search for event data. The following table describes the specific event data you can search once a sensor has been deployed and event collection is enabled.

> **NOTE:** Ensure the specific events you want to collect are enabled on each operating system. Event collection is configured in an Endpoint Policy. For more information, see "Create and Configure an Endpoint Policy" in the *Administrator's Guide*.

Event Type	Data You Can Search	Supported OS
Process	A process name, hash, or process ID.	• Windows • Linux • Mac
Process lineage	A historical timeline of when and how a process was created.	• Windows • Linux • Mac
Network	IP, port, and the amount of data transmitted or received in a network connection.	• Windows • Linux • Mac
File	A specific filename.	• Windows • Linux • Mac
Domain Name System (DNS) information	The domain name of the corresponding endpoint.	• Windows
Security	Dates and times of when a user logged on or off an endpoint.	• Windows

A query requires a specified search intent and value to execute successfully. Unless specified, with the exception of process lineage search — which requires an IP address — Artemis searches all active endpoints by default. Keep this in mind if you need to search endpoints running on a specific operating system.

The following example is a valid query because it specifies the process name:

```
search for process calc.exe on all Windows endpoints
```

To search more than one value for a given entity — which is supported only for active endpoint searches— separate each value with a semi-colon:

```
search for processes calc.exe; lsass.exe
```

Sample Artemis Queries

The following table lists examples of full-text queries that meet the requirements to execute a successful search in Artemis. Refer to this table for guidance when constructing a query. Also keep the following in mind:

- When searching for a file or process with no extension, include “process” or “file” before the process name.
- When searching for port, include “port” in front of the port number.
- When searching for anything by user, include “user” before the username.

For a complete list of sample queries, visit Endgame's Knowledge Base, which you can access by clicking on the Top Navigation toolbar.

> **NOTE:** Do not include the surrounding quotation marks in your query. They are solely meant to indicate the start and end of the phrase.

Search Intent	Sample Query Text
Process	
A specific process by name or hash	"Show me process.exe on all Windows endpoints" "Show me process.exe on all Linux endpoints" "Find process.exe on inactive endpoints" "Search process for file process.exe on active endpoints" "Search for process hash ABC1234567890 on IP 10.1.2.34"
The lineage of a specific process	**NOTE:** Ensure you specify an IP address in the query and precede it with "endpoint." "Show me the process lineage for badguy.exe on endpoint 10.1.2.34" "Search the process lineage for notepad.exe on endpoint 10.1.2.34" "Give me the process lineage for badguy.exe on endpoint 10.1.2.34" "Give me the process lineage for PID 123 on endpoint 10.1.2.34" "Show me resolver for process winword.exe and PID 2956 on hostname endpoint-1-2-03"
Network	

Search Intent	Sample Query Text
Endpoints that communicated to a specific IP	"Search for any endpoint that communicated to IP 10.1.2.34" "Show me any endpoint that communicated to IP 10.1.2.34"
Endpoints running on a specific operating system that communicated to a specific IP	"Did any Windows 10 endpoints communicate to IP 10.1.2.34" "Have Windows 7 endpoints communicated with 10.1.2.34"
Endpoints sending more than a specific amount of data	"Search network data for endpoints sending more than 100MB" "Search network communications for endpoints sending more than 100MB" **NOTE:** Ensure there is no space between the data size and unit.
Endpoints running a specific process sending more than a specific amount of data	"Search network data for process.exe sending more than 100MB" "Search network communications for process.exe sending more than 100MB"
Endpoints sending less than a specific amount of data	"Search network data for endpoints sending less than 100MB" "Search network communications for endpoints sending less than 100MB"
Endpoints that communicated on a specific port	"Search for any endpoints that communicated on port 123"
User	
Any endpoints a specific user	"Search for user johndoe" "Search logins for user johndoe"

Search Intent	Sample Query Text
logged on to	
If a user logged on to an endpoint running on a specific operating system	"Has johndoe logged on to any Windows 7 endpoints"
All processes launched by a specific user	"Search processes created by user johndoe"
DNS	
All endpoints that communicated with a specific domain	"Search for any endpoint that communicated with www.domain.com" "Search for www.domain.com" "Search DNS data for www.domain.com"
If a server running on a specific operating system communicated with a specific domain	"Did any Windows 10 endpoints communicate with www.domain.com"

Search by Hostname or Endpoint Group

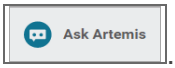
Including a hostname or group in an Artemis query is useful to narrow search results by a specific endpoint value. Refer to the examples below for guidance on how to format these queries.

To Search by	Include in the Artemis Query	Sample Query Text
Hostname	The hostname.	"Search for process.exe on hostname endpoint-hostname"
Group	The name of the assigned group(s). If the groups include spaces or semicolons, surround them with quotation marks. Separate multiple values with a semicolon.	**NOTE:** If a group contains a space or semi-colon, separate it with quotation marks. "Search for process.exe on endpoints with groups ABC; XYZ" "Search for process hi.exe on group ABC"

Execute a Search in Artemis

The following example describes how to execute a search in Artemis.

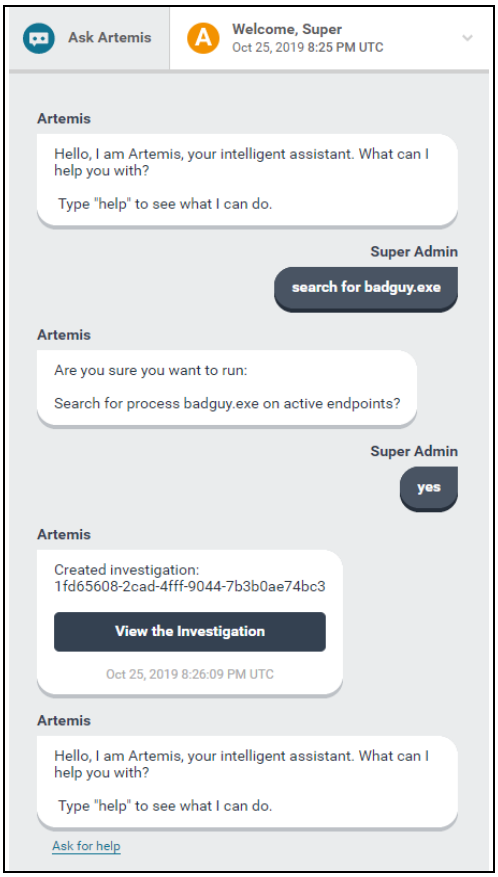
> **Scenario:** You want a historical account of every time process "badguy.exe" was run on all endpoints within your network — even on the endpoints that are inactive or were deleted.

1. On the Top Navigation toolbar, click 

.
2. In the Response box at the bottom of the chat window, type `search for badguy.exe` and press **Enter**.

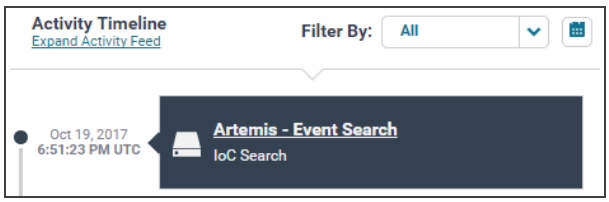
> **TIP:** When you launch Artemis, the interface automatically displays the last 10 executed search queries. Place your cursor in the Response box and press the up arrow to populate the most recent response in Artemis. Press the up arrow again to see previous recent responses.

3. Artemis asks you to confirm the query. If it is correct, type `yes` and press **Enter**. If it is incorrect, type `no` or `cancel` and type a new query.



Sample process data search in Artemis

4. Artemis confirms the search has begun. To view results, click "View Search Results."

> Each executed active endpoint query appears in the Activity Timeline as an "Artemis - Event Search" entry.
>
> 
>

Artemis Search Optimization Tips

When constructing a search query, keep the following tips in mind:

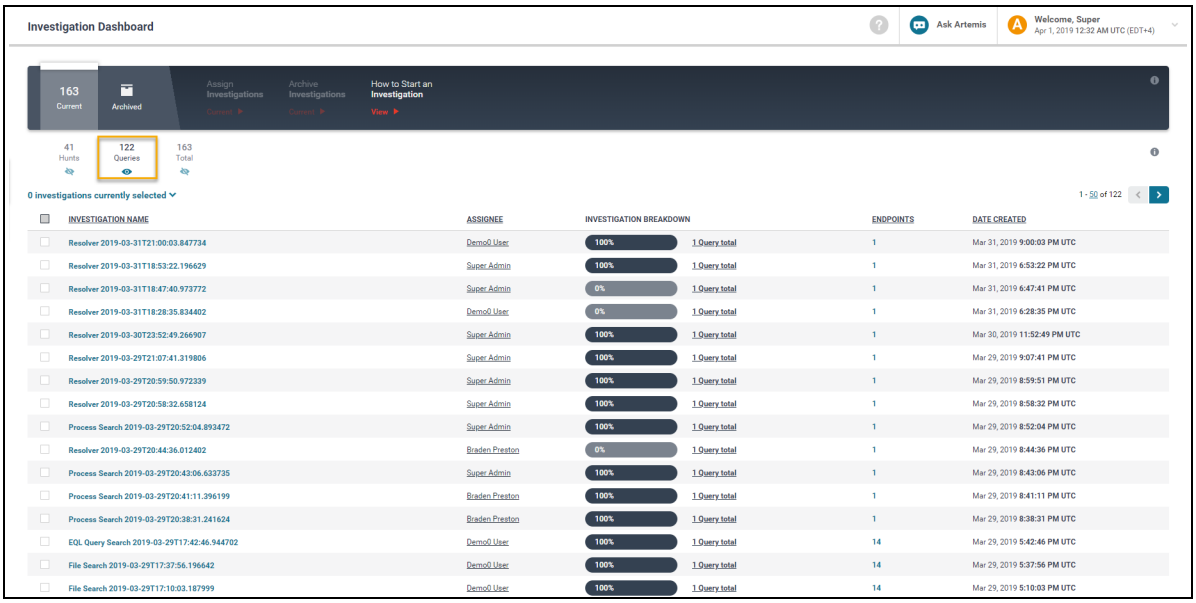
1. For guidance on how to construct a query, see "About Artemis Queries."
2. Use correct spelling. While Artemis tries to recognize misspellings, it can return an error.
3. Ensure the query specifies what you are searching for and the value (e.g., process lineage must have a process name or process ID). Omitting information can return an error.
4. When specifying the search intent and entity value, ensure you type the correct IP address, process name, etc.
5. If you are stuck at any time and want to start over, type `cancel` in the chat window, or click the **Reset** button, then click **RESET QUERY**.

View Artemis Search Results

After you execute a search in Artemis, it extracts the requested event data from the endpoint log file and displays the results on the Investigation Details page.

To view search results, choose one of the following options:

- After you type "yes" in the Artemis chat window to launch the search, click the link that says "Click here to view the Investigation."
- On the Investigation Dashboard, select the **Queries** tab on the Action toolbar, then click the appropriate query in the Investigations list.



Artemis Queries list on the Investigation Dashboard

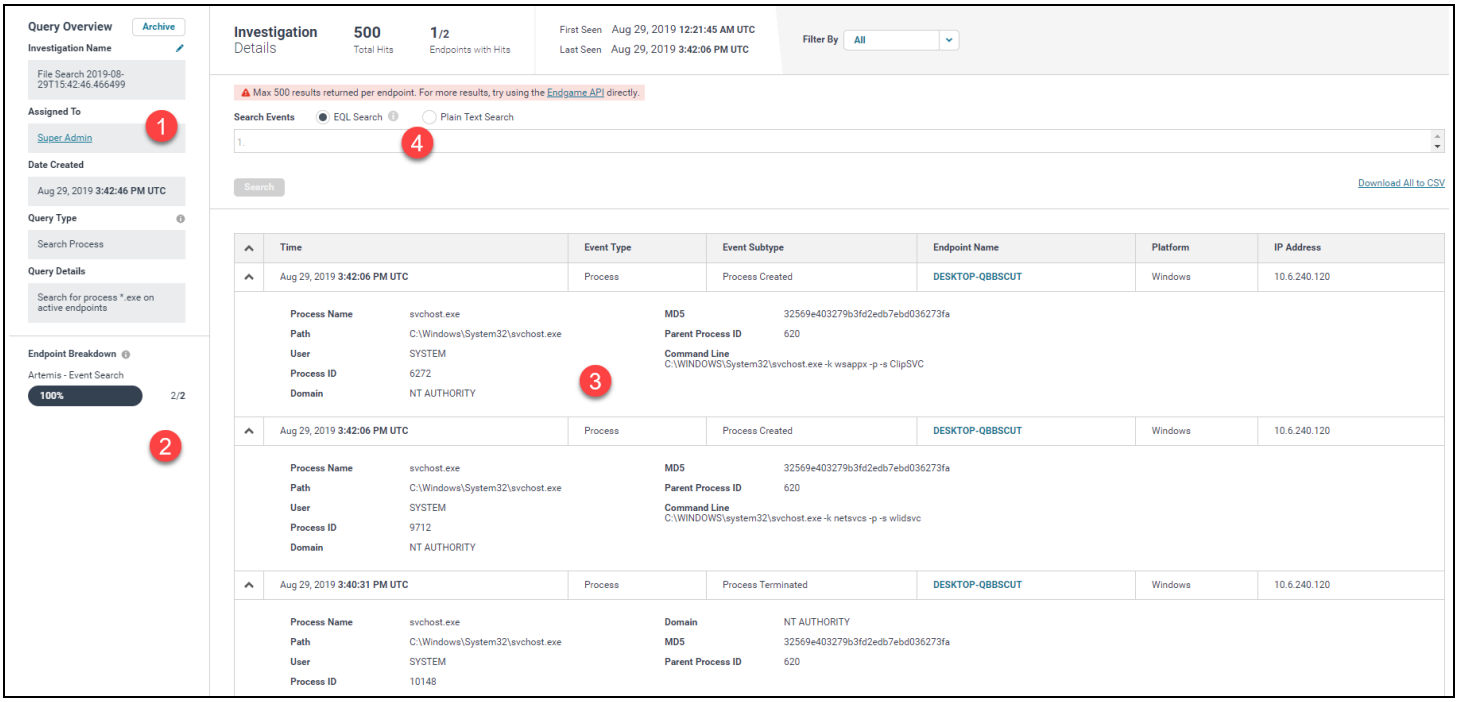
> **TIP:** You can also go directly to the search results page from the Artemis chat window. After you type "`yes`" in the Artemis chat window to launch the search, click the response link that says "View the Investigation."

Artemis Search Results Overview

Search results for active endpoint searches appear on the Investigation Details page, which displays details of the selected Artemis query and provides options to edit the name and archive the query. Search results are listed in a tabular format and appear in chronological order with the first endpoint occurrence at the top.

The results page contains four sections:

1. Artemis Query Overview
2. Endpoint Breakdown
3. Individual search results
4. Filter events



Artemis query search results

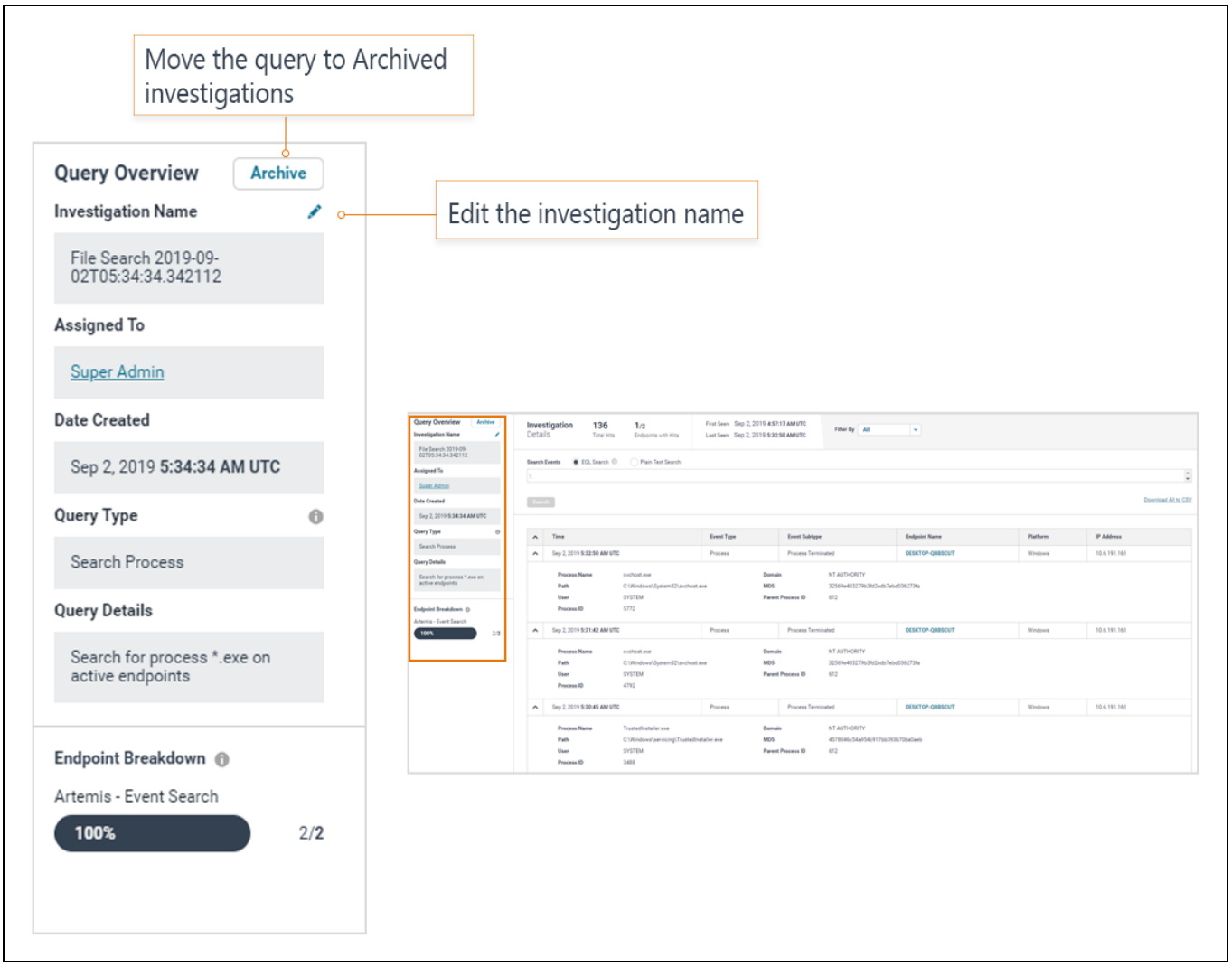
The top of the Artemis Investigation Details page displays the following data about the query:

Data	Description
Total Hits	The total number of search results.
Endpoints with Hits	The total number of events that occurred on unique endpoints. **NOTE:** It is possible to see a different number of "Total Hits" and "Endpoints with Hits." The former displays the total number of occurrences, even if it occurred on the same endpoint.
First Seen	The date and time the event occurred first on the endpoint within the specified time frame.
Last Seen	The date and time the event occurred last on the endpoint within the specified time frame.

NOTE: The search results page shows a maximum of 500 results per endpoint and a maximum of 1,000 results overall. If the maximum is reached, a warning that says, "Max *number* returned overall. For more results, try using the Endgame API directly or download from the CSV link below."

Artemis Query Overview

The Artemis Query Overview section displays general information about the query, including the name, assignee (the user who ran the search), query type, and date it was created. In addition, you can view the details of the query, which is useful if you want to rerun the search at a later time or see if the query syntax is accurate. The Overview section also provides options to edit the name or archive the query.

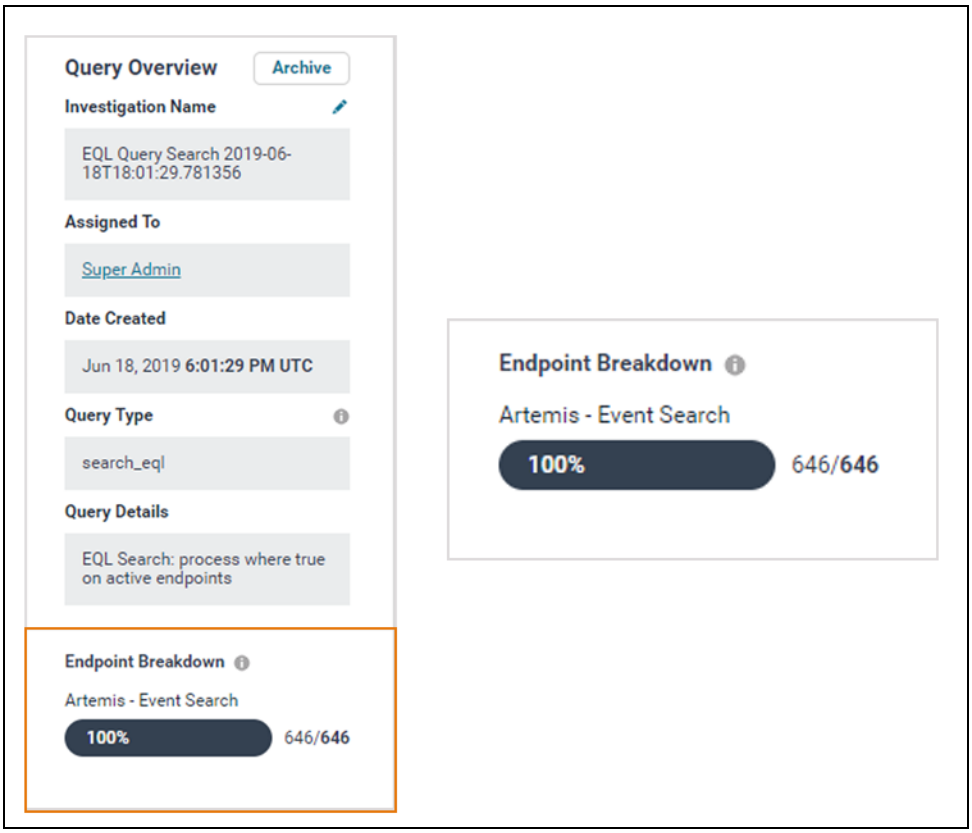


Artemis Query Overview section

> **NOTE:** The default name of each query is formatted as **Query Type YYYY-MM-DD:HH:MM:SS:MMSS** (e.g., File Search 2019-01-10T18:40:28.251406). You can edit this name to something unique by clicking the pencil button.

Endpoint Breakdown

The Endpoint Breakdown summarizes the status of the Artemis query and includes a progress bar that displays the percentage completion and the number of endpoints out of the total included that have returned data.



Endpoint Breakdown

Individual Search Results

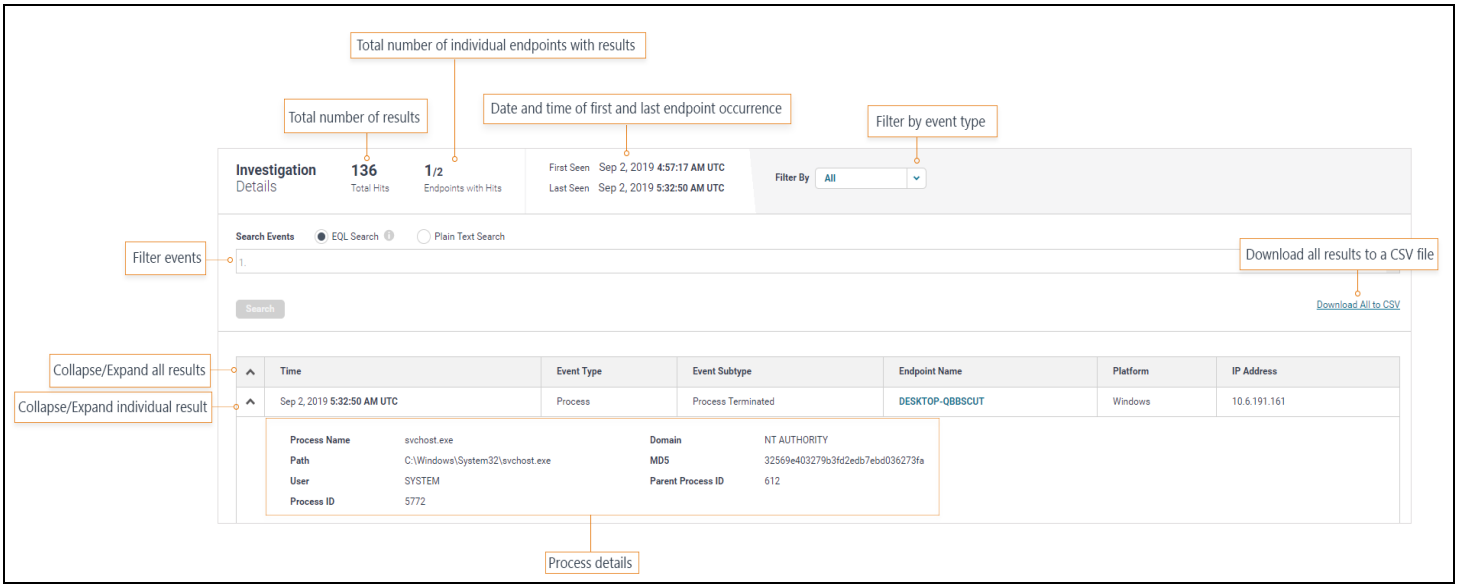
Search results are displayed in a tabular format and appear in chronological order. A search result card displays comprehensive event details about each endpoint occurrence that was found, based on the requested data in Artemis. For example, if you asked Artemis to find each time an lsass.exe process was run on a group of 16 endpoints and that process was found on all 16, the Investigation Details page displays 16 results.

NOTE: The page displays a maximum of 1,000 results.

In addition to all-inclusive details, each result card contains the following columns that provide the following data:

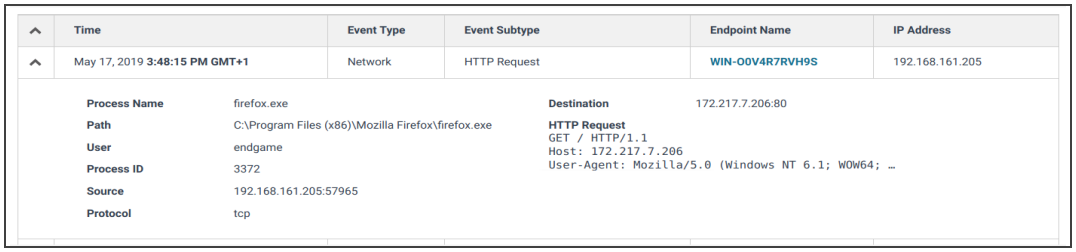
Column Name	Description
Time	The date and time the event occurred.
Event Type	The type of event that occurred (e.g., process, network, DNS, etc.)
Event Subtype	A description of the specific event action (e.g., process created, process terminated, etc.)
Endpoint Name	The hostname on which the event occurred.

Column Name	Description
	TIP: The endpoint hostname is an active link that goes to the Endpoint Details page.
IP Address	The IP address on which the event occurred.

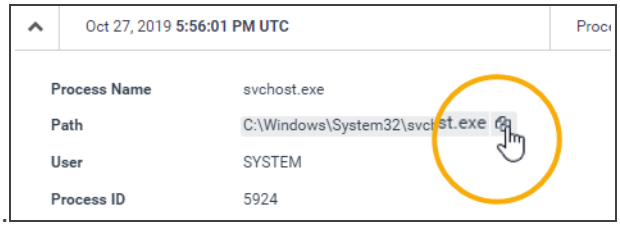


A search result from a Windows process query

TIP: For applicable network data queries, you can view HTTP request data in the search results, which is useful to detect and remediate incidents.

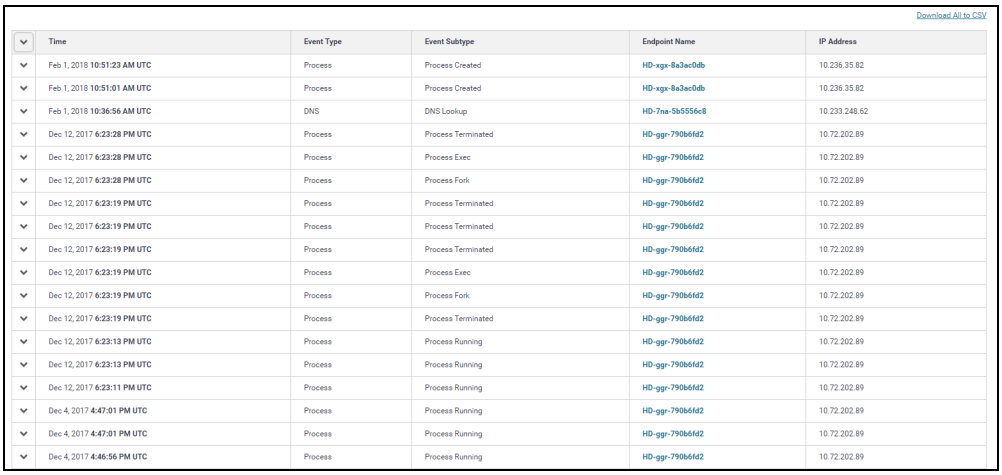


TIP: Copy the path or process name by clicking inside the field. It copies the text to the clipboard, which you can then paste into a new Artemis search or other application.



Expand and Collapse Results

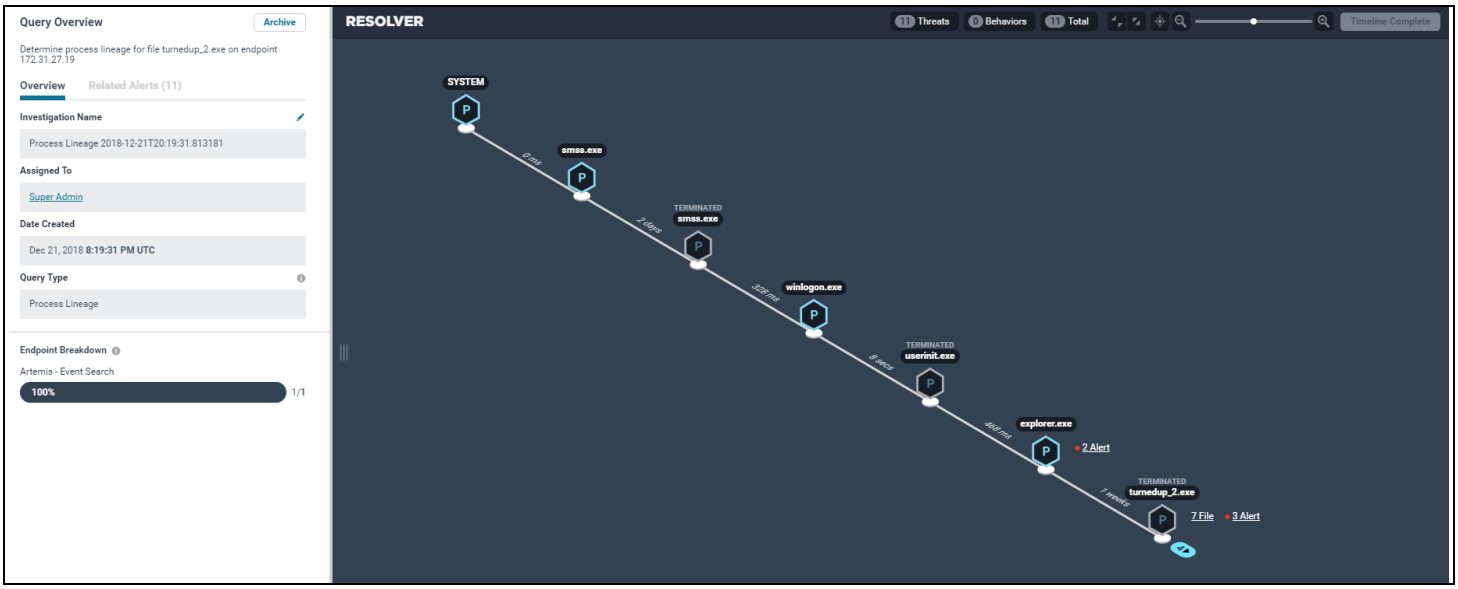
By default, each result is expanded to display event details. However, you can collapse the comprehensive list of results to a consolidated list that only includes each event type, event subtype, endpoint name, and IP address by clicking the **Collapse** arrow to the left of the "Time" column heading. Click the **Expand** arrow to return to the expanded state. You can also collapse and expand individual results.



Collapsed view of Artemis results

Process Lineage Search Results Overview

Search results for a process lineage appear as a visual timeline of events, known as the Endgame Resolver™ Attack Visualization. This view provides a more concise and efficient method to analyze which process events occurred and in what order, as opposed to the standard "result card" view. The Endgame Resolver™ also displays child processes and other events (e.g., DNS, registry, network, etc.) that spawned from the parent process, related alerts, and provides options to take action on a selected process. For complete details about the Endgame Resolver™, see "Alert Details Page Overview."

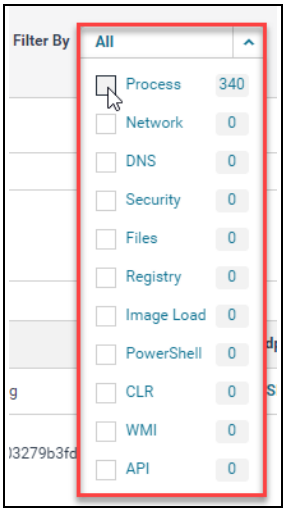


Process lineage search results appear in the Endgame Resolver™ view

When viewing Artemis results, you can filter the data by event type, search string, or EQL Search. Filtering data is useful to find targeted data, especially if there are several results.

Filter By Event Type

By default, the search results display all endpoint occurrences; however, you can filter by one or more event types by selecting the **Filter By** drop-down and selecting the appropriate event type(s). Once you apply a filter, the number of total hits and endpoints with hits updates to display the filtered data. Each event type is color-coded for distinction.



Filter by event type

Filter by EQL (Endgame Query Language) Search

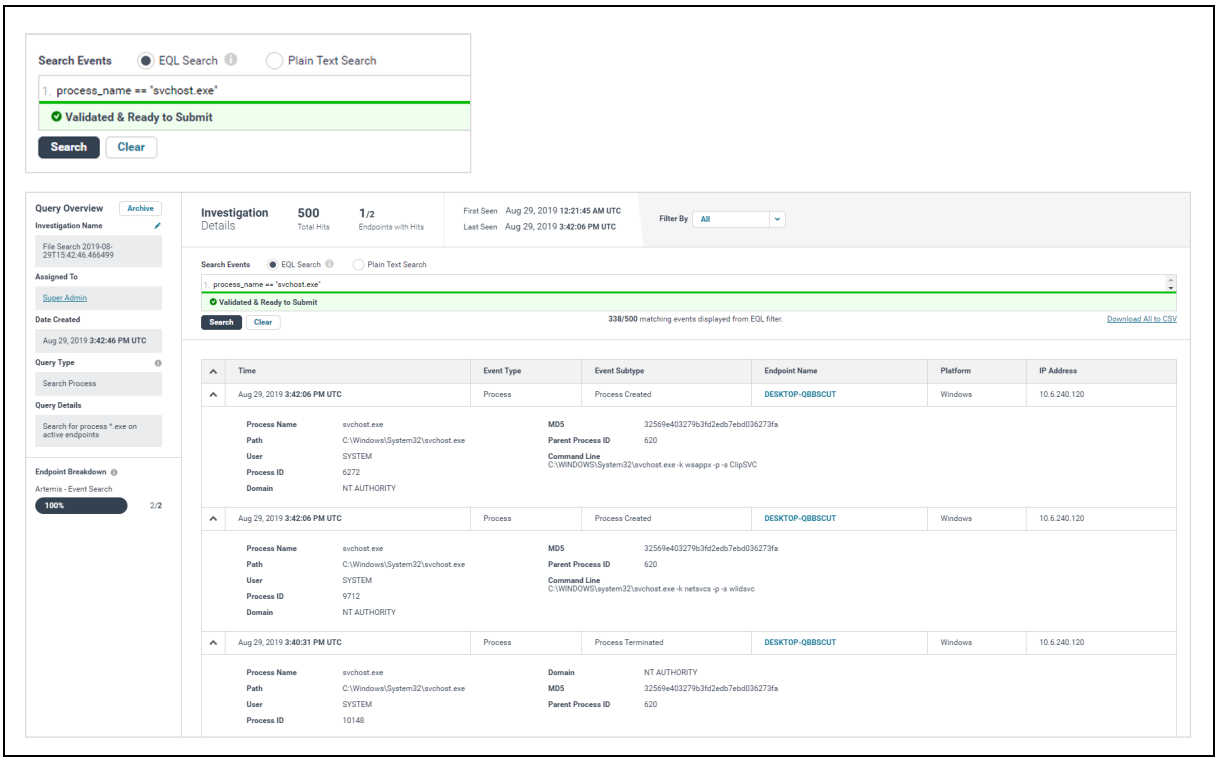
As an alternative to filtering results by event type, you can also filter Artemis results by specific EQL. Using this method of filtering leverages the full capabilities of EQL, which provides the ability to do such as the following:

- Use Boolean operators, such as **and**, **or**, **not** (**NOTE:** Boolean operators are case sensitive and must be lowercase in EQL searches)
- Use a wildcard (*) in the search for field values
- Search for a partial match

> For examples of EQL queries, view the EQL Quick Help Guide or visit: https://eql-lib.readthedocs.io/en/latest/analytics.html.

To filter results by EQL:

1. In the Search Events section, select the **EQL Search** option.
2. In the search bar, enter an EQL query. The EQL validator validates the query as you type. If the EQL is incorrect, a validation error with a suggested fix appears beneath the query.
3. When the "Validated & Ready to Submit" confirmation appears, the EQL query is correct. Click **Search** or press **Enter** on your keyboard. The number of matching events out of the total displays beneath the search bar.



Filter results by EQL

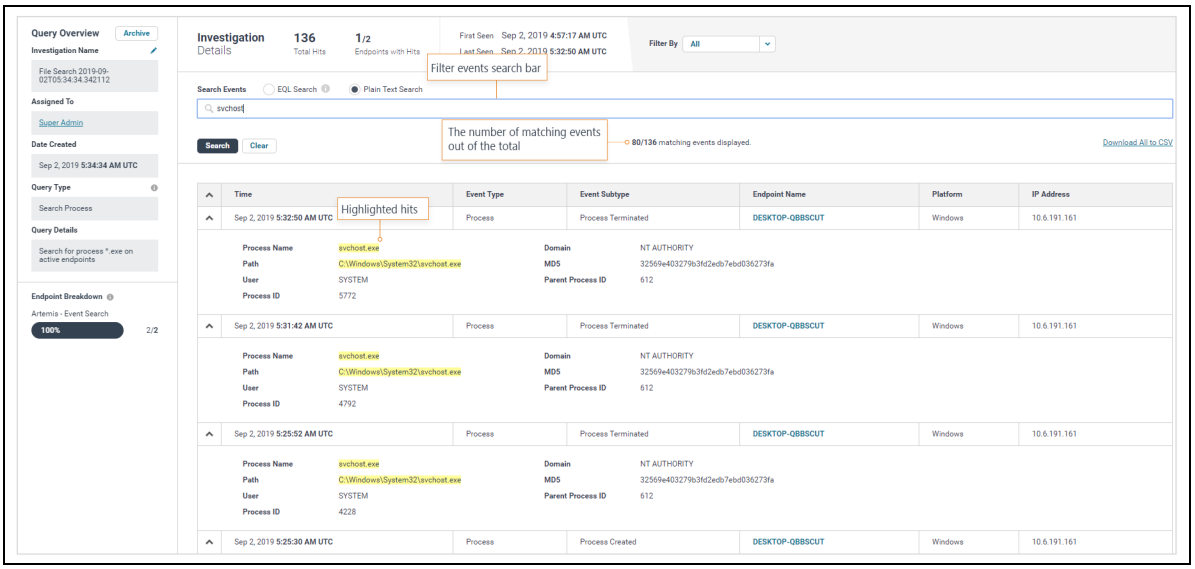
Filter by Search String

Filtering by a search string is useful if you want to look for basic, simple words within the list of search results.Before you filter events by a text string, keep the following tips in mind:

- Results are returned from prefix search strings only — or the beginning of a word. For example, if you are searching for `process.exe` and you type `pro` in the search bar, any events that contain "process.exe" appear as matches. However, if you type a suffix, such as `cess`, "process.exe" events do not appear as matches.
- A string is defined as phrases that are split on the following characters: **/ \ - _** and **.** If the results do not show events you expect to be listed, try removing the aforementioned characters from your search string.

To filter results by a search string:

1. In the Search Events section, select the **Plain Text** search option.
2. In the search bar, enter the search string by which to filter. Click **Search** or press **Enter** on your keyboard. The list of results filters to display matching events, which are highlighted. The number of matching events out of the total is displayed beneath the search bar.

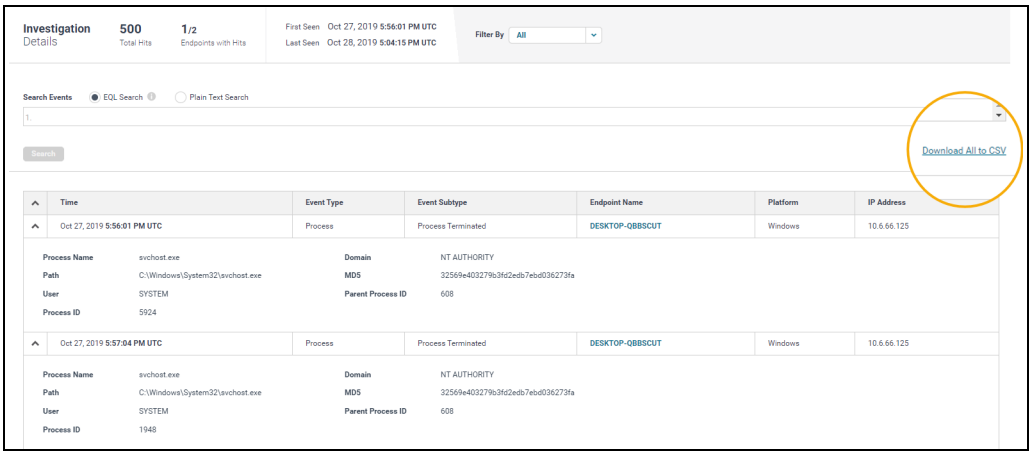


Filter Artemis events by search string

Download Artemis Results

You can download the current search results from Artemis to a comma-separated values (CSV) file by doing the following:

1. In the upper-right corner of the search results page, directly beneath the search bar, click **Download All to CSV**.



2. When the download is complete, open or save the file from your browser.

> **NOTE:** The downloaded CSV file does not include any applied search filters.

Find Additional Endpoint Occurrences Using Artemis Shortcuts

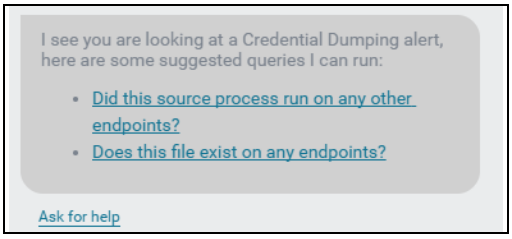
When you view an alert's details, the Alert Metadata panel displays correlated endpoint data, such as a the process name, SHA1 hash, MD5 hash, or path. Artemis contains pivot actions and shortcuts that enable you to quickly search for those same values that may exist on other endpoints. These features are useful to determine if similar malicious activity has occurred elsewhere within your environment without needing to manually enter specific search criteria. As such, this can also expedite alert remediation.

Execute a Recommended Artemis Query

If you are viewing details of a specific alert, you can launch Artemis to view recommended queries for guidance on what other data to search. A preceding message appears to inform you it recognizes which alert you are viewing.

Recommended queries appear in Artemis when the following alerts are displayed:

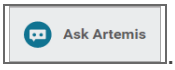
- Credential Dumping
- Credential Manipulation
- Malicious File
- Permission Theft
- Process Injection
- Ransomware



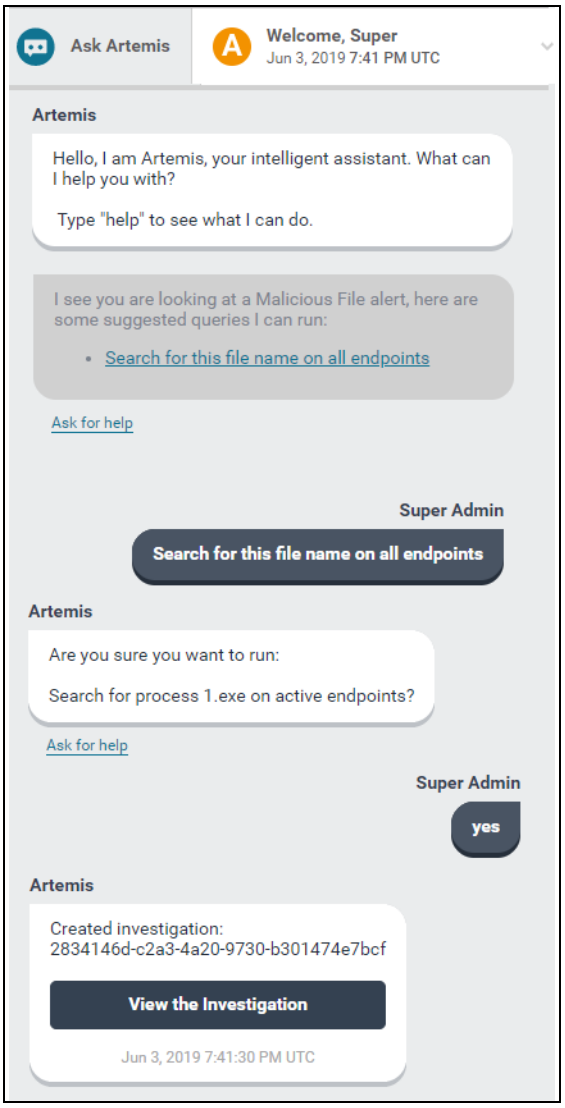
Recommended queries for a Credential Dumping alert

When you execute a recommended query — which is contextual according to the alert type — Artemis extracts the endpoint data from the current alert.

To execute a recommended Artemis query:

1. View an alert that provides recommended queries (see list above).
2. On the Top Navigation toolbar, click 

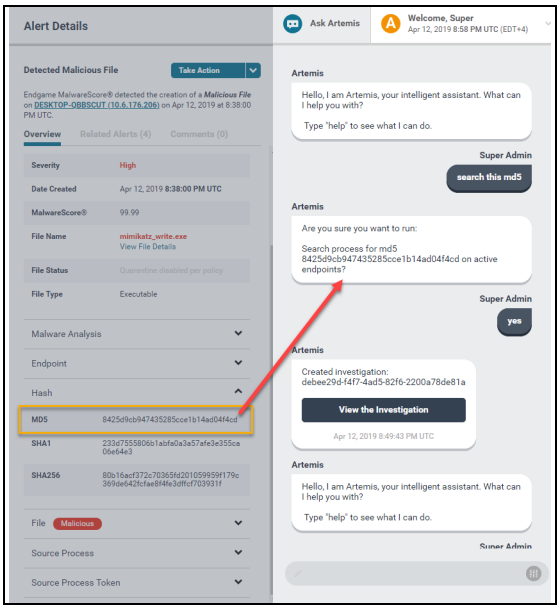
. The recommended queries appear in the chat window.
3. Click the appropriate query, which then populates in the response text box.
4. If the query is correct, press **Enter**. If it is not, you can modify the query as appropriate.
5. When Artemis asks you to confirm the search query, type `yes` in the text box and press **Enter**.
6. Click **View the Investigation** to view results on the Investigation Details page.



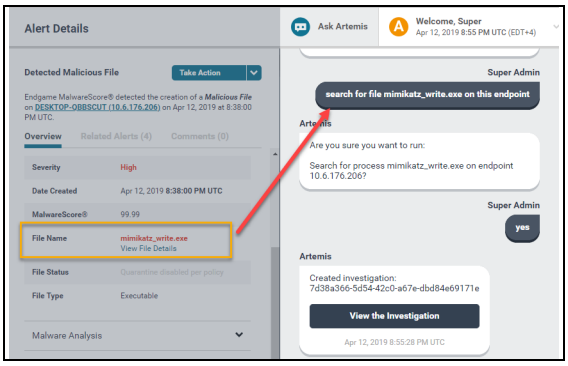
An executed recommended query for a Malicious File alert

Search Current Alert Metadata on Other Endpoints

When an alert's details are displayed, you can also use Artemis to search for specific values in the current metadata that may exist on other endpoints by typing **`"this"`** in the query followed by the search intent. For example, if you are viewing a Malicious File alert, you can type **`"search this md5"`** to determine if the current MD5 hash exists on other endpoints. This eliminates the need to manually type or copy or paste this metadata in the response text box.



This feature also enables you to search for event data that occurred solely on the current endpoint by specifying the search intent followed by **`"this endpoint"`** in the query (e.g., **`"search process lsass.exe on this endpoint"`**).



A sample file search on the current endpoint using the "this" parameter

The specific metadata you can search on other endpoints using the "this" parameter varies by alert type, as illustrated in the following table:

	Credential Dumping	Credential Manipulation	Exploit	Permission Theft	Ransomware	Process Injection	Malicious File
Endpoint	✓	✓	✓	✓	✓	✓	✓
PID	X	✓	✓	X	✓	X	X
Source PID	✓	X	X	✓	X	✓	X
Target PID	✓	X	X	✓	X	✓	X
Process	X	✓	✓	X	✓	X	✓
Source Process	✓	X	X	✓	X	✓	X
Target Process	✓	X	✓	✓	X	✓	X
Path	X	✓	✓	X	✓	X	✓
Source Path	✓	X	X	✓	X	✓	X
Target Path	✓	X	✓	✓	X	✓	X
SHA256	X	X	X	X	✓	X	✓
MD5	X	X	X	X	✓	X	✓
SHA1	X	X	X	X	✓	X	✓

Sample Queries Using the "this" Parameter

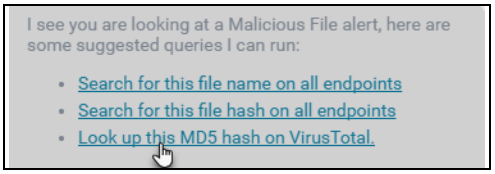
The following table lists examples of metadata can you search on other endpoints using the "this" parameter in Artemis. Refer to the preceding table to ensure you display the appropriate alert and search for applicable data.

Search Intent	Sample Query Text
The file or process	"Find this file on all endpoints" "Does this file exist" "Search for this file on all endpoints" "Find this process"
The file path	"Find this file path" "Does this file path exist on other endpoints" "Search for this file path on active endpoints"
The MD5 hash	"Find this MD5 hash" "Does this MD5 hash exist" "Does this MD5 hash exist on Windows endpoints" "Search for this MD5 hash"
The SHA1 hash	"Find this SHA1 hash" "Does this SHA1 hash exist" "Search for this SHA1 hash"
The SHA256 hash	"Find this SHA256 hash" "Does this SHA256 hash exist" "Search for this SHA256 hash"
The process lineage of a file	**NOTE:** Be sure you specify an endpoint. "Determine the process lineage for this file on endpoint 10.1.2.34" "Find the process lineage for this file on endpoint-hostname" "Show me the process lineage for this file on endpoint 10.1.2.34"

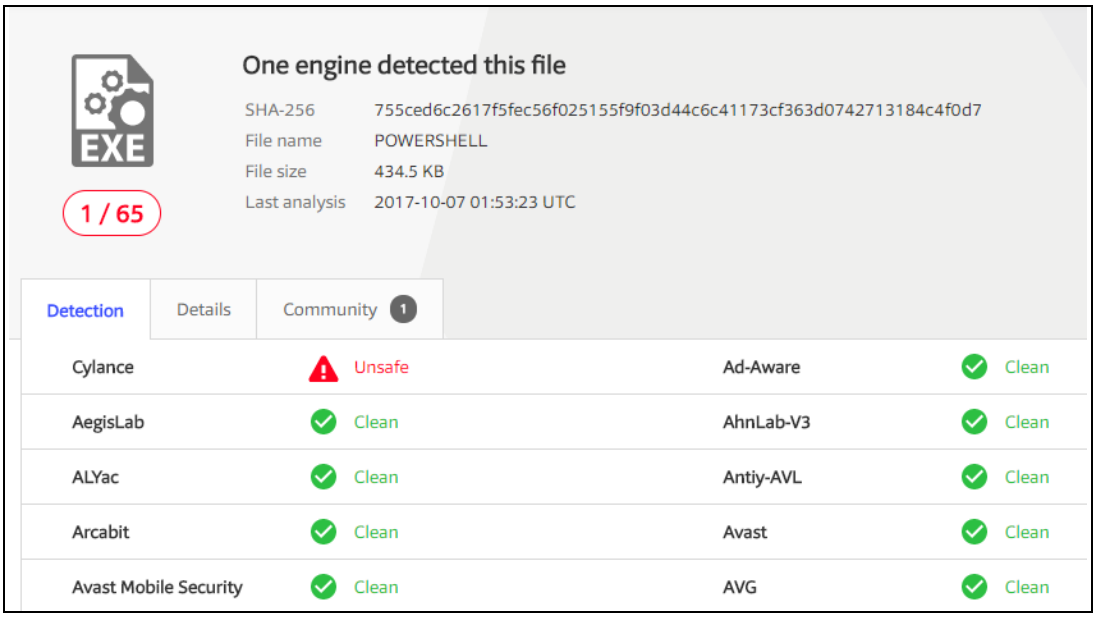
Configure Third-Party Applications to Connect to Endgame

If a third-party application is configured to connect to Endgame, you can use Artemis to pivot to that application to search for external files that contain the same metadata. This feature leverages Endgame's detection and prevention capabilities with services that can provide additional context.

For example, if you view a Malicious File alert and VirusTotal integration is configured, when you launch Artemis, a recommended query that allows you to pivot to a hash search in VirusTotal appears in the chat window:



If you execute this search, the results from VirusTotal display in a new tab:

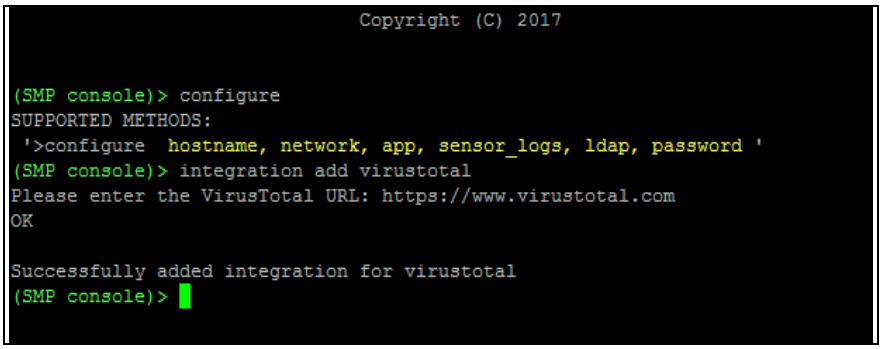


To configure a third-party application to connect to Endgame:

1. Open a secure shell to the Endgame platform.
2. At the command prompt, run the following command:

```
configure integration add <name of application>
```

3. At the command prompt, type the URL of the application, including the https://, and press **Enter**. If the integration was successful, a "Successfully added integration for <company>" confirmation appears.



Sample third-party configuration for VirusTotal

Event Query Language (EQL) Overview

Event Query Language (EQL) enables you to execute advanced queries via Artemis that may be unavailable using natural language. EQL is also the syntax administrators use to create **Custom Rules**[1].

EQL supports equality matching and wildcard characters, basic "`and`", "`or`", "`not`", and "`in`" Boolean search operators, and process lineage relationships. It can also join multiple events for a single process and compare values of fields to strings, integers, decimal values, and against other fields.

> **NOTE:** Boolean search operators are case sensitive and must be lowercase in EQL searches. To view the complete guide on EQL documentation, go to: http://eql.readthe-docs.io/.

EQL Query Examples

The following lists supported EQL query types and search examples.

> **TIP:** You can find more examples of sample EQL queries by going to: https://eql-lib.readthedocs.io/en/latest/analytics.html.

Boolean

Basic Query Structure: `<event_type> where <schema_value> [==, !=, <=, <, >, >=] <value>`

Query Example:

[1] A statement, written in EQL, that instructs Endgame's sensor to monitor suspicious or malicious activity specific to your environment. If such activity is detected, the sensor generates an alert in the Endgame platform.

```
process where process_name == "svchost.exe" and command_line != "* -k *"
```

Description: Finds all processes named `"svchost"` but without the string `"-k"` in the command line.

OS: Windows, macOS, Linux.

Event Relationships

Basic Query Structure:

```
<event_type> where child of [<event_type> where <clause>]
```

Query Example:

```
process where child of [process where parent_process_name == "wmiprvse.exe"]
```

Description: Finds grandchildren of the Windows Management Instrumentation Provider service.

OS: Windows.

Join

Basic Query Structure:

```
join by <schema_value>
[<event_type> where <clause>]
[<event_type> where <clause>]
```

Query Example:

```
join by pid
[process where true]
[network where true][registry where true]
[file where true]
until [process where event_subtype_full == "termination_event"]
```

Description: Finds events that are joined until an expiration event is met.

OS: Windows, macOS, Linux.

Sequence

Basic Query Structure:

```
sequence with maxspan=<time>
[<event_type> where <clause>]
[<event_type> where <clause>]
```

Query Example:

```
sequence with maxspan=30s
[network where destination_port==3389 and event_subtype_full="*_accept_event*"]
[security where event_id in (4624, 4625) and logon_type == 10
```

Description: Network logon over Remote Desktop - With a maxspan of 30 seconds, looks for an incoming network connection from a host, followed by a separate event for the remote authentication success or failure.

OS: Windows, macOS, Linux.

Data Pipes

Basic Query Structure:

```
| unique <expression> [, <expression>] ...
| count
| count <expression> [, <expression>] ...
| filter <expression>
| unique_count <expression> [, <expression>] ...
| tail <int>
| head <int>
```

Query Example:

```
process where true | count parent_process_name, process_name
// results look like
// {"count": 100, "key": ["explorer.exe", "cmd.exe", "percent": .4}
// {"count": 100, "key": ["cmd.exe", "cmd.exe", "percent": .4}
```

Description: Counts the number of times a set of values occurs.

Query Example:

```
security where event_id == 4624| tail 10
```

Description: Retrieves the 10 most recent logon events.

OS: Windows, macOS, Linux.

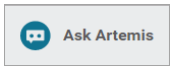
Supported Event Types

The following table lists the supported EQL event types by operating system:

Name	EQL Event Type	Supported OS
CLR (Common Language Runtime) (Beta)	clr	• Windows
DNS	dns	• Windows
File	file	• Windows • Linux • macOS
Image Load	image_load	• Windows
Network	network	• Windows • Linux • macOS
PowerShell (Beta)	powershell	• Windows
Process	process	• Windows • Linux • macOS
Registry	registry	• Windows
Windows API (Beta)	api	• Windows
Windows Security Logs	security	• Windows
WMI (Windows Management Instrumentation) (Beta)	etw	• Windows

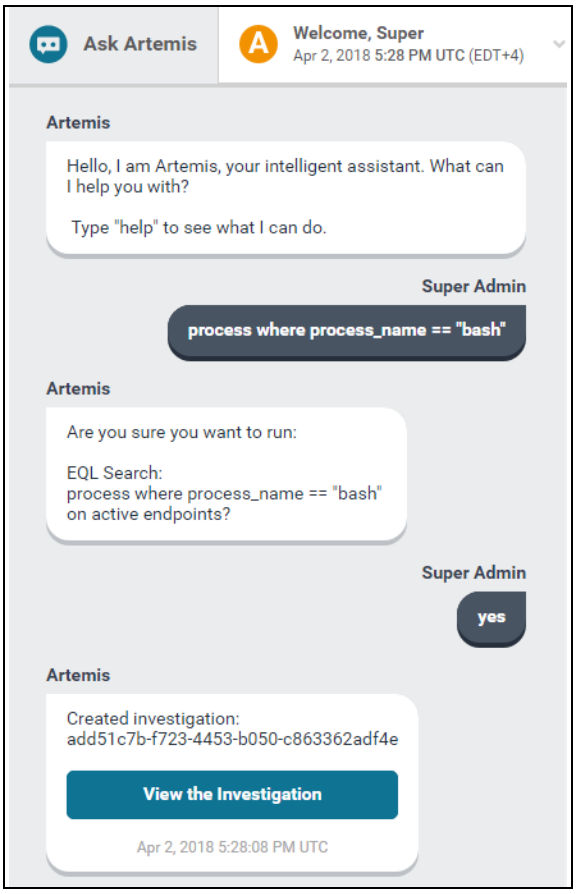
Execute EQL Queries via Artemis

To execute an EQL search via Artemis:

1. On the Top Navigation toolbar, click 

.
2. In the response text box, type the EQL query. If the EQL syntax is correct, Artemis asks you to confirm the search.
3. Type **`yes`**, then press **Enter** to create a query investigation.

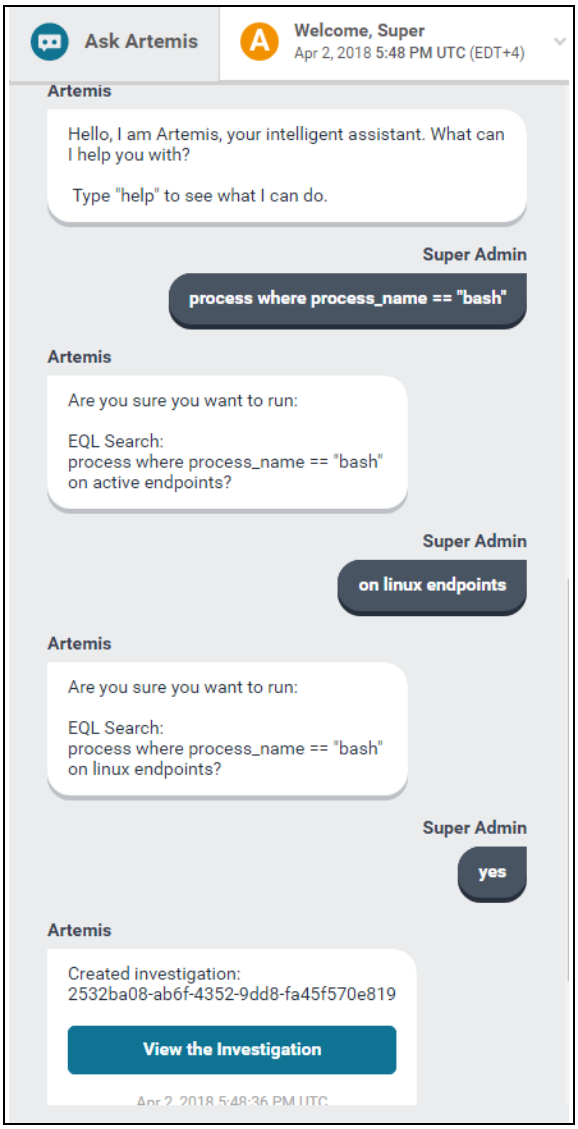
Example:



Sample EQL search using Artemis

> **NOTE:** If Artemis does not recognize the syntax and does not reply with "EQL Search: [query]", type **`Cancel`** and try a new query.

To run an EQL search across a specific operating system, first type the query and press **Enter**, then when Artemis responds, specify which endpoints to search, as seen in the following example:



Sample EQL search across multiple endpoints using Artemis

Eventing Schema

The following table lists the fields that are indexed in the Endgame platform when the sensor collects event data. You can use these fields to construct advanced searches in Artemis using Event Query Language (EQL). The ECS column shows the most recently mapped field names in Elastic Common Schema, which you can use to create searches in the Elastic Discover application.

EQL	ECS (Elastic Common Schema)	Operating System
API		
Subtypes api_event		
access_timestamp	N/A	Windows (All)
acting_process_creation_time	N/A	
acting_process_id	N/A	
acting_process_name	N/A	
acting_process_path	N/A	
acting_process_unique_pid	N/A	
acting_thread_authentication_id	N/A	
acting_thread_creation_time	N/A	
acting_thread_elevation_type	N/A	
acting_thread_id	N/A	
acting_thread_impersonation_level	N/A	
acting_thread_integrity_level	N/A	
acting_thread_start_module	N/A	
acting_thread_start_time	N/A	
acting_thread_user_domain	N/A	
acting_thread_user_name	N/A	
acting_thread_user_sid	N/A	
apc_routine	N/A	
apc_routine_bytes	N/A	
apc_routine_context	N/A	

EQL	ECS (Elastic Common Schema)	Operating System
apc_routine_context_bytes	N/A	
api_name	N/A	
callstack_hash	N/A	
change_timestamp	N/A	
creation_timestamp	N/A	
delete_file	N/A	
event_message	message	
event_subtype_full	event.action	
event_type_full	N/A	
file_attributes_int	N/A	
file_attributes_string	N/A	
file_disposition	N/A	
file_name	N/A	
file_path	N/A	
getclipboard_format	N/A	
hidden_flag_set	N/A	
key_path	N/A	
opcode	N/A	
pid	N/A	
process_name	N/A	
process_path	N/A	
query_file_path	N/A	
rename_count	N/A	
return_value	N/A	
serial_event_id	event.sequence	
service_access	N/A	
service_bin_path	N/A	
service_display_name	N/A	

EQL	ECS (Elastic Common Schema)	Operating System
service_start_name	N/A	
service_start_type	N/A	
service_type	N/A	
system_flag_set	N/A	
target_domain_name	N/A	
target_process_creation_time	N/A	
target_process_id	N/A	
target_process_name	N/A	
target_process_path	N/A	
target_process_unique_pid	N/A	
target_thread_creation_time	N/A	
target_thread_id	N/A	
target_thread_start_module	N/A	
target_thread_start_time	N/A	
target_token_authentication_id	N/A	
target_token_elevation_type	N/A	
target_token_impersonation_level	N/A	
target_token_integrity_level	N/A	
target_token_user_domain	N/A	
target_token_user_name	N/A	
target_token_user_sid	N/A	
target_user_name	N/A	
tid	N/A	
time_stomped	N/A	
timestamp	@timestamp	
timestamp_utc	N/A	
unique_pid	N/A	
user_domain	user.domain	

EQL	ECS (Elastic Common Schema)	Operating System
user_name	user.full_name	
user_sid	user.id	
write_timestamp	N/A	
callers	N/A	
CLR		
Subtypes load_image load_module		
bytes	N/A	Windows (All)
event_subtype_full	event.action	
module_name	N/A	
namespace_hash	N/A	
opcode	N/A	
pid	N/A	
process_name	N/A	
process_path	N/A	
serial_event_id	event.sequence	
timestamp	@timestamp	
typedef_hash	N/A	
typeref_hash	N/A	
unique_pid	N/A	
user_domain	user.domain	
user_name	user.full_name	
user_sid	user.id	
event_message	message	
event_type_full	N/A	
tid	N/A	
timestamp_utc	N/A	

EQL	ECS (Elastic Common Schema)	Operating System
typedefs	N/A	
typerefs	N/A	
DNS		
Subtypes lookup_failure request_event		
event_id	N/A	Windows (All)
event_subtype_full	event.action	
event_type_full	N/A	
opcode	N/A	
pid	process.pid	
process_name	process.name	
process_path	process.executable	
query_name	dns.question.name	
query_options	N/A	
query_results	N/A	
query_status	N/A	
query_type	N/A	
serial_event_id	N/A	
timestamp	@timestamp	
timestamp_utc	N/A	
unique_pid	N/A	
File		
Subtypes file_create_event file_modify_event file_delete_event		

EQL	ECS (Elastic Common Schema)	Operating System
file_rename_event		
file_overwrite_event		
event_subtype_full	event.action	Windows, Linux, macOS
event_type_full	N/A	Windows, Linux, macOS
file_attributes	file.attributes	Windows, Linux, macOS
file_name	file.name	Windows, Linux, macOS
file_path	file.path	Windows, Linux, macOS
old_file_name	N/A	Windows, Linux, macOS
old_file_path	N/A	Windows, Linux, macOS
opcode	N/A	Windows, Linux, macOS
pid	process.pid	Windows, Linux, macOS
process_name	process.name, process.title	Windows, Linux, macOS
process_path	process.executable	Windows, Linux, macOS
serial_event_id	event.sequence	Windows, Linux, macOS
share_mode	N/A	Windows, Linux, macOS
timestamp	@timestamp	Windows, Linux, macOS
timestamp_utc	N/A	Windows, Linux, macOS
unique_pid	N/A	Windows, Linux, macOS
zone_id	N/A	Windows, Linux, macOS
create_disposition	N/A	Windows
desired_access	N/A	Windows
create_options	N/A	Windows
user_domain	user.domain	Windows
user_name	user.full_name	Windows
user_sid	user.id	Windows
effective_gid	file.gid	Linux, macOS
effective_group_name	file.group	Linux, macOS
effective_uid	file.uid	Linux, macOS

EQL	ECS (Elastic Common Schema)	Operating System
effective_user_name	N/A	Linux, macOS
real_gid	N/A	Linux, macOS
real_group_name	N/A	Linux, macOS
real_user_name	N/A	Linux, macOS
real_uid	N/A	Linux, macOS
Image Load		
Endgame collects the following image names: • System.Management.Automation.dll • System.Management.Automation.ni.dll • jscript.dll • jscript9.dll • chakra.dll • vbscript.dll • scrobj.dll • scrrun.dll • wlbsctrl.dll • wbemcomn.dll • WptsExtensions.dll • Tsmsisrv.dll • TSVIPSrv.dll • Msfte.dll • wow64log.dll • WindowsCoreDeviceInfo.dll • Ualapi.dll • wlanhlp.dll • phoneinfo.dll • EdgeGdi.dll • cdpsgshims.dll		

EQL	ECS (Elastic Common Schema)	Operating System
• windowsperformancerecordercontrol.dll • diagtrack_win.dll • Taskschd.dll • wmiutils.dll • vaultcli.dll • bcrypt.dll • psapi.dl • msxml3.dll • 7z.dll • pgpcrypt.dll • pgpencrypt.dll • wbemdisp.dll • wbemprox.dll • wbemsvc.dll • fastprox.dll • ntdll.dll		
Subtypes driver_load_event image_load_event		
event_subtype_full	event.action	Windows (All)
event_type_full	N/A	
image_name	dll.name	
image_path	dll.path	
md5	dll.hash.md5	
opcode	N/A	
pid	process.pid	
process_name	process.name, process.title	
process_path	process.executable	

EQL	ECS (Elastic Common Schema)	Operating System
serial_event_id	event.sequence	
sha1	dll.hash.sha1	
sha256	dll.hash.sha256	
timestamp	@timestamp	
timestamp_utc	N/A	
unique_pid	N/A	
Network		
Subtypes		
ipv4_connection_attempt_event	N/A	Windows, Linux, macOS
ipv4_connection_accept_event		Windows, Linux, macOS
ipv4_disconnect_received_event		Windows, Linux, macOS
ipv4_reconnect_attempt_event		Windows, Linux, macOS
ipv6_disconnect_received_event		Windows, Linux, macOS
ipv6_connection_accept_event		Windows, Linux, macOS
ipv6_reconnect_attempt_event		Windows, Linux, macOS
ipv4_http_request_event		Windows
ipv6_http_request_event		Windows
connection_id	N/A	Windows, Linux, macOS
destination_address	destination.address, server.address, server.ip	Windows, Linux, macOS
destination_port	destination.port, server.port	Windows, Linux, macOS
event_id	N/A	Windows, Linux, macOS
event_subtype_full	event.action	Windows, Linux, macOS
event_type_full	N/A	Windows, Linux, macOS
in_packet_count	network.packets	Windows, Linux, macOS
opcode	N/A	Windows, Linux, macOS
out_packet_count	network.packets	Windows, Linux, macOS
partial_flow	N/A	Windows, Linux, macOS
pid	process.pid	Windows, Linux, macOS

EQL	ECS (Elastic Common Schema)	Operating System
process_name	process.name, process.title	Windows, Linux, macOS
process_path	process.executable	Windows, Linux, macOS
protocol	network.iana_number	Windows, Linux, macOS
serial_event_id	event.sequence	Windows, Linux, macOS
source_address	source.address, source.ip	Windows, Linux, macOS
source_port	source.port	Windows, Linux, macOS
task	N/A	Windows, Linux, macOS
timestamp	@timestamp	Windows, Linux, macOS
timestamp_utc	N/A	Windows, Linux, macOS
total_in_bytes	destination.bytes, server.bytes	Windows, Linux, macOS
total_out_bytes	client.bytes, source.bytes	Windows, Linux, macOS
unique_pid	N/A	Windows, Linux, macOS
user_domain	user.domain	Windows
user_name	user.full_name	Windows
user_sid	user.id	Windows
effective_gid	destination/client/server/source.user.group.id	Linux, macOS
effective_group_name	destination/client/server/source.user.group.name	Linux, macOS
effective_uid	destination/client/server/source.user.id	Linux, macOS
effective_user_name	destination/client/server/source.user.name	Linux, macOS
real_gid	user.group.id	Linux, macOS
real_group_name	user.group.name	Linux, macOS
real_user_name	user.name	Linux, macOS
real_uid	user.id	Linux, macOS
PowerShell		
Subtypes ps_cmdlet_etw_event ps_scriptblock_etw_event		
event_subtype_full	event.action	Windows (All)

EQL	ECS (Elastic Common Schema)	Operating System
header	N/A	
message	N/A	
opcode	N/A	
pid	N/A	
process_name	N/A	
process_path	N/A	
serial_event_id	event.sequence	
timestamp	@timestamp	
unique_pid	N/A	
user_domain	user.domain	
user_name	user.full_name	
user_sid	user.id	
is_obfuscated	N/A	
event_message	message	
event_type_full	N/A	
tid	N/A	
timestamp_utc	N/A	
Process		
Subtypes		
already_running	N/A	Windows, Linux, macOS
creation_event	N/A	Windows
still_running	N/A	Windows, Linux, macOS
termination_event	N/A	Windows, Linux, macOS
exec_event	N/A	Linux, macOS
fork_event	N/A	Linux, macOS
gid_change	N/A	Linux, macOS
session_id_change	N/A	Linux, macOS
still_running	N/A	Linux, macOS

EQL	ECS (Elastic Common Schema)	Operating System
uid_change	N/A	Linux, macOS
authentication_id	N/A	Windows, Linux, macOS
command_line	process.args, process.args_count, process.-command_line	Windows, Linux, macOS
event_type_full	N/A	Windows, Linux, macOS
exit_code	process.exit_code	Windows, Linux, macOS
md5	process.hash.md5	Windows, Linux, macOS
original_file_name	process.pe.original_file_name	Windows, Linux, macOS
parent_process_name	process.parent.name, process.parent.title	Windows, Linux, macOS
parent_process_path	process.parent.executable	Windows, Linux, macOS
pid	process.pid	Windows, Linux, macOS
ppid	process.parent.pid	Windows, Linux, macOS
process_name	process.name, process.title	Windows, Linux, macOS
process_path	process.executable	Windows, Linux, macOS
serial_event_id	event.sequence	Windows, Linux, macOS
sha1	process.hash.sha1	Windows, Linux, macOS
sha256	process.hash.sha256	Windows, Linux, macOS
timestamp	@timestamp	Windows, Linux, macOS
timestamp_utc	N/A	Windows, Linux, macOS
unique_pid	N/A	Windows, Linux, macOS
unique_ppid	N/A	Windows, Linux, macOS
event_subtype_full	event.action	Windows, Linux, macOS
opcode	N/A	Windows
package_name	N/A	Windows
signature_signer	process.code_signature.subject_name	Windows
signature_status	process.code_signature.status	Windows
user_domain	user.domain	Windows
user_name	user.full_name	Windows
	user.id	

EQL	ECS (Elastic Common Schema)	Operating System
user_sid	N/A	Windows
effective_gid	N/A	Linux, macOS
effective_group_name	N/A	Linux, macOS
effective_uid	N/A	Linux, macOS
effective_user_name	user.group.id	Linux, macOS
real_gid	user.group.name	Linux, macOS
real_group_name	user.name	Linux, macOS
real_user_name	user.id	Linux, macOS
real_uid	N/A	Linux, macOS
session_id	process.thread.id	Linux, macOS
tid		Linux, macOS

Security

Subtypes

admin_logon

explicit_user_logon

user_logoff

user_logon

user_logon_failed

workstation_unlocked

workstation_locked

Subtype Full	Windows Event ID
admin_logon	4672
explicit_user_logon	4648
user_logoff	4634
user_logon	4624
user_logon_failed	4625
workstation_unlocked	4801
workstation_locked	4800

EQL	ECS (Elastic Common Schema)	Operating System
channel_name	N/A	Windows (All)
computer_name	N/A	
event_id	N/A	
event_message	message	
event_subtype_full	event.action	
event_type_full	N/A	
ip_address	N/A	
logon_type	N/A	
opcode	N/A	
pid	process.pid	
privilege_list	N/A	
process_name	process.name, process.title	
process_path	process.executable	
provider_guid	N/A	
provider_name	N/A	
serial_event_id	event.sequence	
subject_domain_name	user.domain	
subject_logon_id	N/A	
subject_user_name	user.full_name, user.name	
subject_user_sid	user.id	
system_pid	N/A	
system_process_name	N/A	
system_thread_id	N/A	
target_domain_name	user.target.domain	
target_logon_id	N/A	
target_user_name	user.target.name	
task	N/A	
timestamp	@timestamp	

EQL	ECS (Elastic Common Schema)	Operating System
timestamp_utc	N/A	
unique_pid	N/A	
Registry		
Subtypes registry_modify_event		
bytes_written	registry.data.bytes	Windows (All)
bytes_written_count	N/A	
bytes_written_string	registry.data.strings	
bytes_written_string_list	registry.data.strings	
bytes_written_u32	registry.data.strings	
bytes_written_u64	registry.data.strings	
event_subtype_full	event.action	
event_type_full	N/A	
key_path	registry.data.key, registry.data.path, registry.data.value	
key_type	registry.data.type	
opcode	N/A	
pid	process.pid	
process_name	process.name, process.title	
process_path	process.executable	
serial_event_id	event.sequence	
timestamp	@timestamp	
timestamp_utc	N/A	
unique_pid	N/A	
WMI		
Subtypes file_create_event file_delete_event		

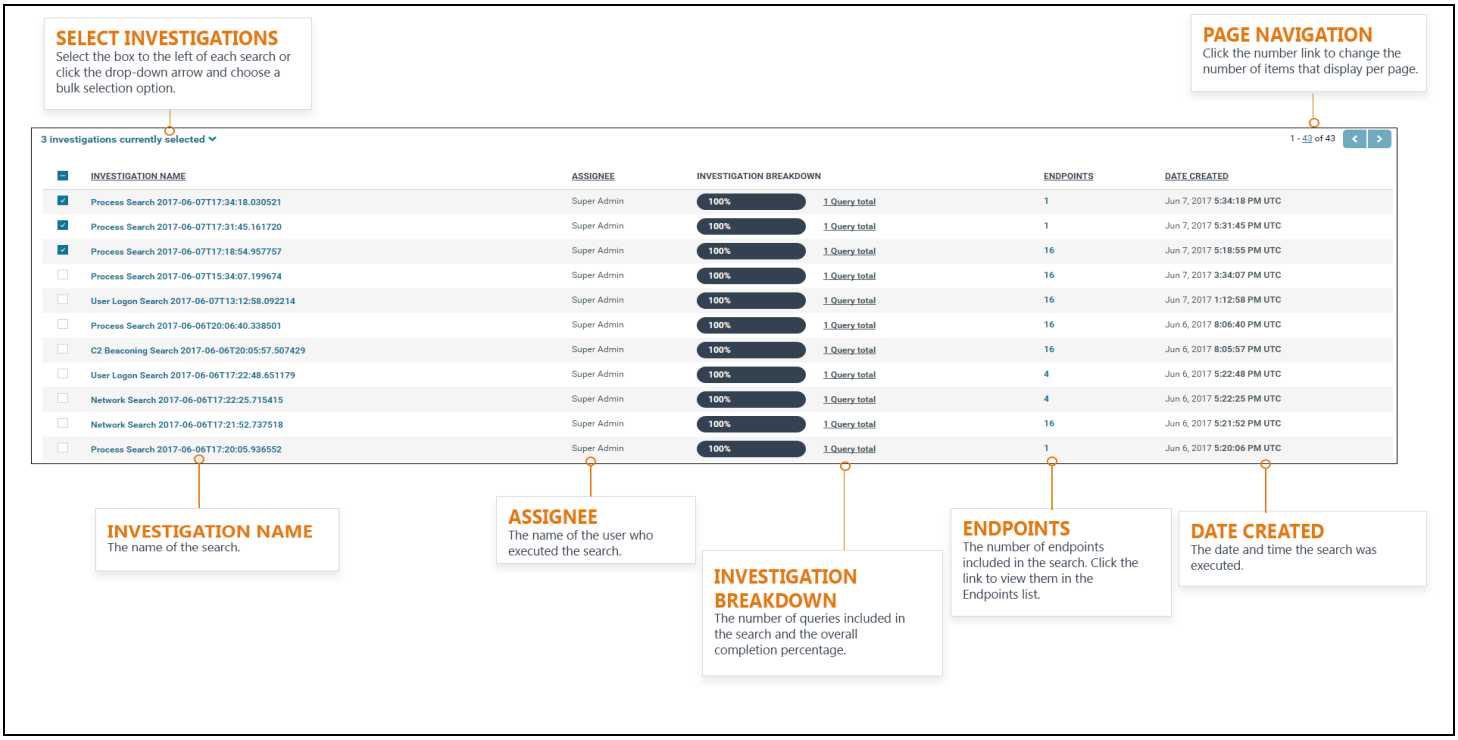
EQL	ECS (Elastic Common Schema)	Operating System
file_exchange_event		
file_modify_event		
file_overwrite_event		
file_rename_event		
event_id	N/A	Windows (All)
event_subtype_full	event.action	
opcode	N/A	
pid	N/A	
process_name	N/A	
process_path	N/A	
provider_guid	N/A	
serial_event_id	event.sequence	
tid	N/A	
timestamp	@timestamp	
timestamp_utc	N/A	
unique_pid	N/A	
user_domain	user.domain	
user_name	user.full_name	
user_sid	user.id	
properties.CONSUMER	N/A	
properties.ClassName	N/A	
properties.ClientMachine	N/A	
properties.ClientMachineFQDN	N/A	
properties.ClientProcessCreationTime	N/A	
properties.ClientProcessId	N/A	
properties.Commandline	N/A	
properties.ComponentName	N/A	
properties.CorrelationId	N/A	

EQL	ECS (Elastic Common Schema)	Operating System
properties.CreatedProcessId	N/A	
properties.ESS	N/A	
properties.ErrorId	N/A	
properties.FileName	N/A	
properties.Flags	N/A	
properties.GroupOperationId	N/A	
properties.HostProcess	N/A	
properties.Id	N/A	
properties.ImplementationClass	N/A	
properties.IsLocal	N/A	
properties.MachineName	N/A	
properties.Message	N/A	
properties.MessageDetail	N/A	
properties.MethodName	N/A	
properties.Namespace	N/A	
properties.NamespaceName	N/A	
properties.Operation	N/A	
properties.OperationId	N/A	
properties.Path	N/A	
properties.PossibleCause	N/A	
properties.Protocol	N/A	
properties.ProviderGuid	N/A	
properties.ProviderName	N/A	
properties.ProviderPath	N/A	
properties.Query	N/A	
properties.QueryId	N/A	
properties.ResultCode	N/A	
properties.User	N/A	

EQL	ECS (Elastic Common Schema)	Operating System
properties.unique_ClientProcessId	N/A	
properties.unique_CreatedProcessId	N/A	

Artemis Queries List Overview

The Artemis Queries list is an enumeration of all Artemis queries and their relevant details, organized in a table. It is displayed on the Investigation Dashboard within the **Queries** tab. The list is useful to view general search details, investigation progress, and to view results of a specific search. Queries display in reverse chronological order with the most recently executed queries at the top.



Artemis Queries list

The columns in the list provide the following general details about each Artemis query:

Column Name	Description
INVESTIGATION NAME	The name of the Artemis query, which initially is auto-generated. You can change the name on the Investigation Details page.
ASSIGNEE	The name of the user who executed the search.
INVESTIGATION BREAKDOWN	Displays a progress bar that indicates the query's percentage completion across all endpoints in the investigation. The **Query total** link displays the number of queries in the search, which is always **1**.
ENDPOINTS	The number of endpoints included in the search. Click the number link to view those

Column Name	Description
	endpoints in the Endpoints list.
DATE CREATED	The date and time the search was executed according to Coordinated Universal Time (UTC) or your selected time zone.

Sort and Filter Columns in the Queries List

You can sort columns in the list to change the order the contents appear, or search them to filter content by a particular value. Sorting and filtering columns are useful to quickly find specific information without browsing through a large amount of data.

> **NOTE:** You cannot sort or filter the **INVESTIGATION BREAKDOWN** column.

To sort or filter a column, select the appropriate column heading and choose from the following options:

To sort by increasing or decreasing value:

- Select the **Ascending** or **Descending** option. The currently sorted column is denoted by an up arrow or down arrow .

To search the column for a particular value:

- In the text box, type the text you want to find, then click **Search**. The list filters to display results that match the entry. The currently filtered column is denoted by a symbol.

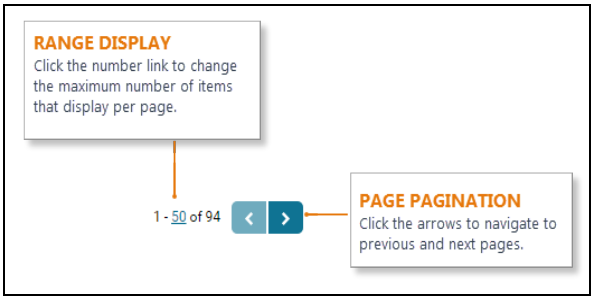
Column sort and filter

Page Pagination

In the upper-right corner above the list is a range display, which displays the current number range of investigations out of the total (e.g., 1-50 of 400). Click the left and right arrows to navigate to previous and next pages.

By default, a maximum of 50 investigations display per page; however, you can change the number to a preferred choice:

1. On the range display, click the number link. For example, if the range display is 1-50, click **50**.
2. In the **Max count of** text box, enter a new number between 1 and 500.
3. Click ✓ to save your changes.



Archive an Artemis Query

Archiving an Artemis query moves it from the **Current** tab on the Investigation Dashboard to the **Archived** tab. Consider archiving a query after you have reviewed the search results to distinguish it from queries that have not yet been reviewed.

To archive multiple Artemis queries:

1. On the Investigation Dashboard, select the **Queries** tab to filter the list to Artemis queries.
2. In the Investigations list, select the box to the left of each query to archive.

   TIP: To select all queries on the current page, select the box to the left of the **INVESTIGATION NAME** column heading.

3. On the Action toolbar, click **Archive Investigations**.
4. In the **Archive Investigations** dialog box that says, "You are about to archive *number* Investigations. The investigations will be immediately sent to the Archive Tab and be set as Archived..." click **Archive**. A "Successfully archived investigation(s)" message appears.
5. Click **Finish**.

Archive Investigations dialog box

You can also archive a single query from the Investigation Details page by clicking the **Archive** button in the Artemis Query Overview section.

Verify that Logon Events are Enabled in Windows (Optional)

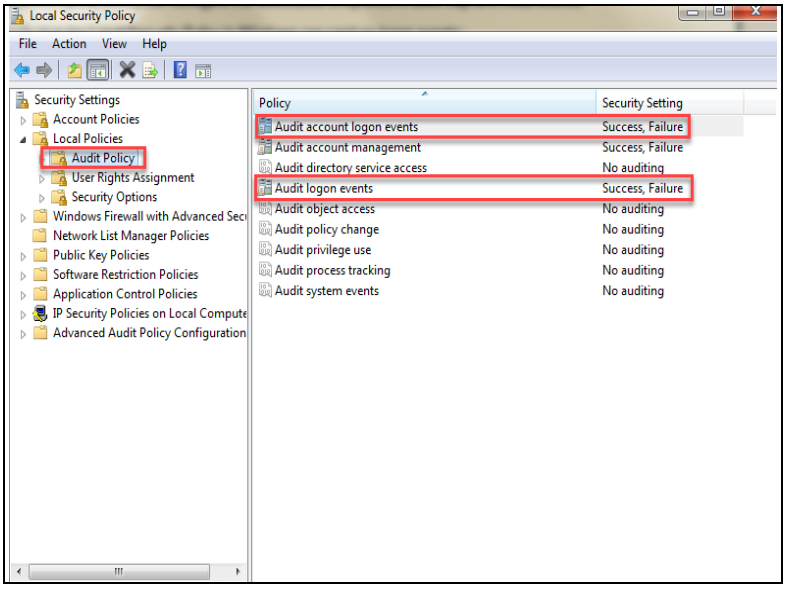
The "Audit account logon events" setting in Windows Local Security Policy determines whether to audit each time a user logs on or off a computer. If this setting is not configured, Endgame's sensor is unable to store those events in the platform. Consequently, any user activity searches executed via Artemis will return with no results.

To verify that the Local Security Policy in Windows can capture logon events:

1. Navigate to the Audit Policy setting within the Windows Local Security Policy:
   a. Open the Control Panel, and then go to **Administrative Tools > Local Security Policy**.
   b. Expand the **Local Policies** folder, and then select the **Audit Policy** folder.

   > **TIP:** As an alternative, you can type `secpol.msc` in the Windows search bar to go directly to the Local Security Policy panel, and then click **Local Policies** > **Audit Policy**.

2. In the right pane, verify that the security settings for **Audit account logon events** and **Audit logon events** both say, "Success, Failure." This ensures Windows captures logon events and also ensures the sensor in the Endgame platform can store these events. If the security settings do not say "Success, Failure," an administrator can modify the local security policy to change them, or the organization group policy can configure the associated endpoints to audit capture these events.



Audit Policy in Windows

Customer Support

For any questions or issues using the Endgame platform, please contact Customer Success by submitting a request at https://support.endgame.com or emailing support@endgame.com.

Customer Success is available Monday through Friday from 9:00 a.m. – 9:00 p.m. ET.