



The Splunk logo consists of the word "splunk" in a large, white, lowercase, sans-serif font. A grey right-pointing arrow is positioned at the end of the "k". A small "TM" symbol is located in the top right corner of the "k".

# Course-Ware



- > Introduction
- > Splunk Inc
- > Licensing
- > Installation
- > Login
- > Splunk Home
- > Getting Data
- > Search Dashboard
- > Data Summary
- > Search Actions and Modes
- > Search Language
- > Using Sub search
- > Field Lookups
- > Saving and Sharing Reports
- > More Searches and Reports
- > Creating Dashboards

# INTRODUCTION



- Splunk Enterprise is the leading platform for real-time operational intelligence. It's the easy, fast and secure way to search, analyze and visualize the massive streams of machine data generated by your IT systems and technology infrastructure—physical, virtual and in the cloud.
- Troubleshoot application problems and investigate security incidents in minutes instead of hours or days, avoid service degradation or outages, deliver compliance at lower cost and gain new business insights

# INTRODUCTION



Feature	Description
Indexing	Splunk indexes machine data. This includes data streaming from packaged and custom applications, application servers, web servers, databases, networks, virtual machines, telecoms equipment, operating systems, sensors, and so on, that make up your IT infrastructure. The maximum indexing volume depends on the Splunk Enterprise license.
Data model	A data model is a hierarchically-structured search-time mapping of semantic knowledge about one or more datasets. It encodes the domain knowledge necessary to build a variety of specialized searches of those datasets. These specialized searches are used by Splunk Enterprise to generate reports for Pivot users. Data model objects represent different datasets within the larger set of data indexed by Splunk Enterprise.
Pivot	Pivot refers to the table, chart, or data visualization you create using the Pivot Editor. The Pivot Editor lets users map attributes defined by data model objects to a table or chart data visualization without having to write the searches to generate them. Pivots can be saved as reports and added to dashboards.

# INTRODUCTION



Search	an index, use statistical commands to calculate metrics and generate reports, search for specific conditions within a rolling time window, identify patterns in your data, predict future trends, and so on. Searches can be saved as reports and used to power dashboard panels.
Alerts	Alerts are triggered when conditions are met by search results for both historical and real-time searches. Alerts can be configured to trigger actions such as sending alert information to designated email addresses, post alert information to an RSS feed, and run a custom script, such as one that posts an alert event to syslog.
Reports	Reports are saved searches and pivots. You can run reports on an ad hoc basis, schedule them to run on a regular interval, set a scheduled report to generate alerts when the results of their runs meet particular conditions. Reports can be added to dashboards as dashboard panels.
Dashboards	Dashboards are made up of panels that contain modules such as search boxes, fields, charts, tables, forms, and so on. Dashboard panels are usually hooked up to saved searches or pivots. They can display the results of completed searches as well as data from backgrounded real-time searches.

# SPLUNK INC.



- Founded in 2003 and headquartered in San Francisco, California
- **Specialties** – “Machine Data To Operational Intelligence” –  
The machine data that facilitates operational intelligence comes in many different from many different sources. Splunk is able to collect and index data from many different sources, including logfiles written by web servers or business applications, syslog data streaming in from network devices, or the output of custom developed scripts.
- Searching, monitoring, and analyzing machine-generated big data, via a web-style interface
- According to tech target, Splunk is designated as the SIEM of the year.
- The name "Splunk" is a reference to exploring caves, as in spelunking.

# SPLUNK – LICENSING

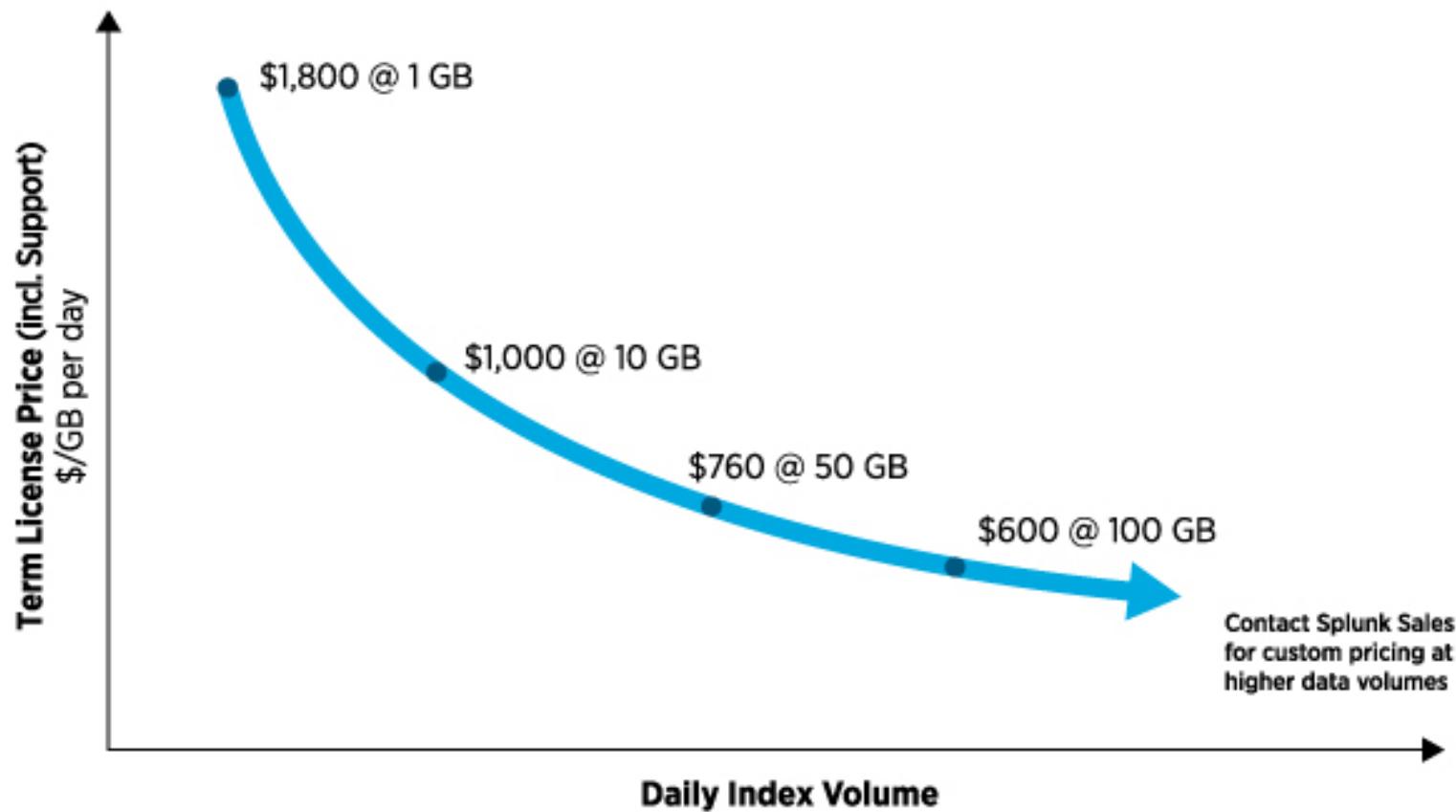


- You'll get a Splunk Enterprise **FREE** license for 60 days and you can index up to 500 megabytes of data per day.
- **Perpetual and Term Licensing**

There are two options for licensing Splunk Enterprise:  
Perpetual license: this includes the full functionality of Splunk Enterprise and starts as low as \$4,500 for 1 GB/day\*, plus annual support fees.

Term license: this provides the option of paying a yearly fee instead of the one-time perpetual license fee. Term licenses start at \$1,800 per year\*, which includes annual support fees.

# SPLUNK – LICENSING



# INSTALLATION



- **Linux** installation instructions

```
tar xvzf splunk_package_name.tgz -C /opt
```

- **Windows** installation instructions

1. To start the installer, double-click the `splunk.msi` file.
2. In the Welcome panel, click Next.
3. In Customer Information, enter the requested details and click Next.
4. Splunk Enterprise is installed by default into the `\Program Files\Splunk` directory.

# INSTALLATION



- **Mac OS X installation instructions**

1. Navigate to the folder or directory where the installer is located.
2. Double-click on the DMG file.
3. Double-click on splunk.pkg.
4. Choose a location to install Splunk.
5. Click Install.

The installer places a shortcut on the Desktop.

# Users



## • About Splunk Enterprise users

Persona	Industry Role	Activities
Administrator	network engineer, system administrator	<ul style="list-style-type: none"><li>Configures, administers, optimizes, and secures the Splunk Enterprise deployment.</li><li>Sets up user accounts and permissions.</li><li>Gets data into Splunk Enterprise.</li></ul>
Knowledge Manager	data analyst, system administrator	<ul style="list-style-type: none"><li>Oversees knowledge object creation, normalization, and usage across teams, departments, and deployments.</li><li>Gets the data into Splunk, or works with the administrator to do so.</li><li>Creates and shares data models.</li></ul>
Search User	data analyst, IT professional, network engineer, security analyst, system administrator	<ul style="list-style-type: none"><li>Uses Search to investigate server problems, understand configurations, monitor user activities, and troubleshoot escalated problems.</li><li>Builds reports and dashboards to monitor the health, performance, activity, and capacity of their IT Infrastructure.</li><li>Identifies patterns and trends that are indicators of routine problems.</li></ul>

# Users



## • About Splunk Enterprise users

Pivot User	business professional, data analyst, executive, IT professional, manager, system administrator	<ul style="list-style-type: none"><li>• Uses Pivot to build reports based on data models created by the Knowledge Manager.</li><li>• Creates reports and dashboards to monitor their businesses.</li><li>• Identifies trends in the health and performance of their businesses.</li></ul>
Developer	system Integrator, professional developer	<ul style="list-style-type: none"><li>• Integrates data and functionality of applications with Splunk Enterprise.</li><li>• Builds Splunk Apps and add-ons with custom dashboards and data visualizations.</li></ul>

# First time Login



- The Splunk interface is web-based, which means that no client needs to be installed.

`http://localhost:8000`

- First time signing credentials

Username – admin

Password - changeme

It is a good idea to change this password to prevent unwanted changes to your deployment.

# Splunk Home



- **Apps**

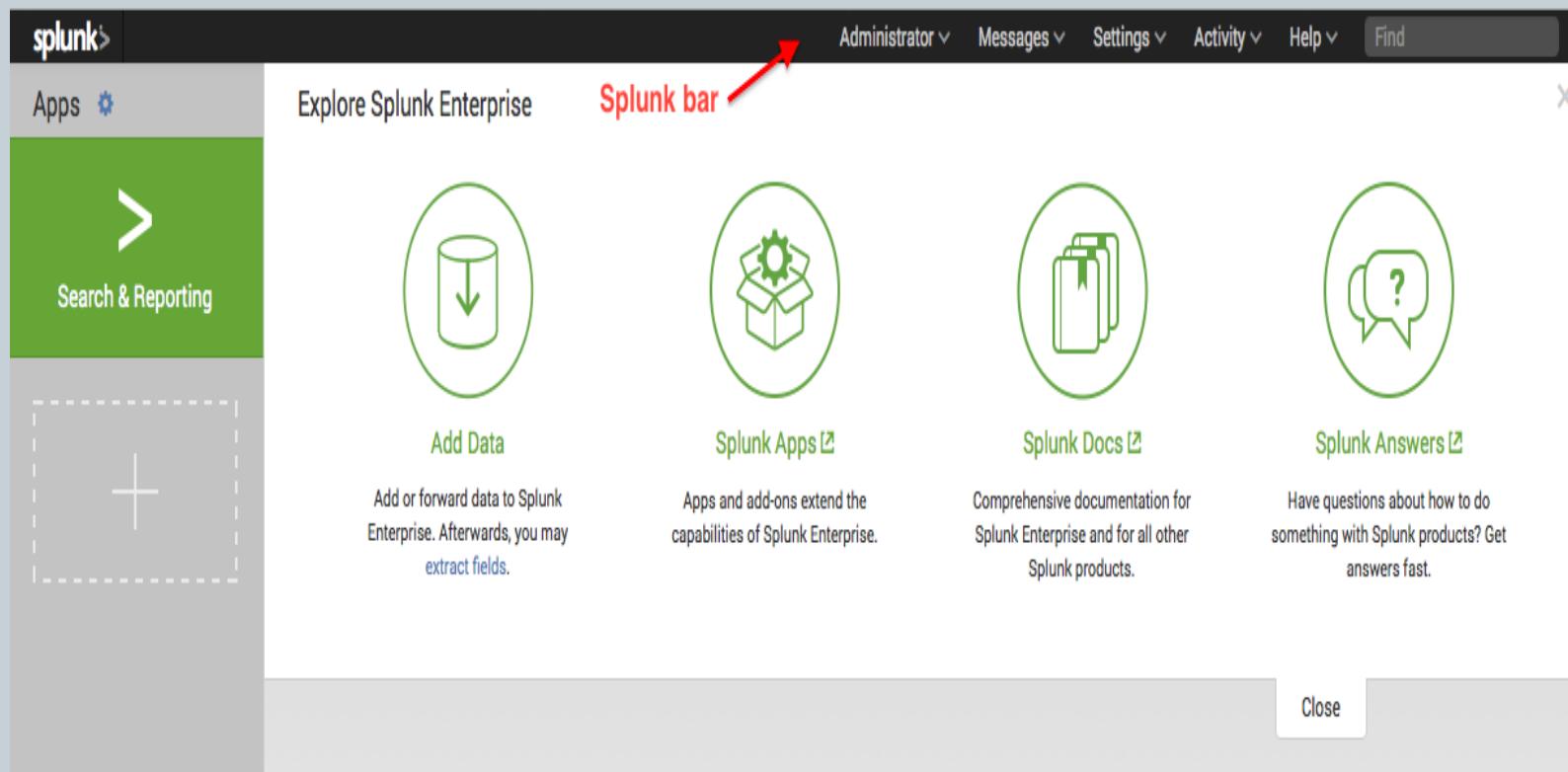
The Apps panel lists the apps that are installed on your Splunk instance that you have permission to view. Select the app from the list to open it.

For an out-of-the-box Splunk Enterprise installation, you see one App in the workspace: Search & Reporting. When you have more than one app, you can drag and drop the apps within the workspace to rearrange them.

- You can do two actions on this panel:
  - Click the gear icon to view and manage the apps that are installed in your Splunk instance.
  - Click the plus icon to browse for more apps to install.

# Splunk Home

- Splunk Bar



# Splunk Home



- **Settings menu**

The Settings menu lists the configuration pages for Knowledge objects, Distributed environment settings, System and licensing, Data, and Authentication settings. If you do not see some of these options, you do not have the permissions to view or edit them.

- **User menu**

The User menu here is called "Administrator" because that is the default user name for a new installation. You can change this display name by selecting Edit account and changing the Full name. You can also edit the time zone settings, select a default app for this account, and change the account's password. The User menu is also where you Logout of this Splunk installation.

# Splunk Home



- **Messages menu**

All system-level error messages are listed here. When there is a new message to review, a notification displays as a count next to the Messages menu.

- **Activity menu**

-Click Jobs to open the search jobs manager window, where you can view and manage currently running searches.

-Click Triggered Alerts to view scheduled alerts that are triggered. This tutorial does not discuss saving and scheduling alerts.

-Click System Activity to see Dashboards about user activity and status of the system.

# GETTING DATA



- A Splunk data repository is called an index. During indexing (or event processing), Splunk processes the incoming data stream to enable fast search and analysis, storing the results in the index as events.
- Events are stored in the index as a group of files that fall into two categories:
  - Rawdata, which is the raw data in a compressed form.
  - Index files and some metadata files that point to the raw data.
- These files reside in sets of directories, called buckets, organized by age.

# GETTING DATA

The screenshot shows the Splunk web interface for adding data. The top navigation bar includes 'splunk> Apps >', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. A progress bar at the top indicates the 'Add Data' process is at the 'Select Source' step. Below the progress bar, the main area is titled 'Select Source' with the sub-instruction 'Choose a file to upload to Splunk, either by browsing your computer or by dropping a file into the target box below.' A 'Learn More' link is also present. A 'Selected File: No file selected' message is shown, along with a 'Select File' button and a large dashed green box for file uploads. Inside this box is a green icon of a document with an upward arrow. Below the box, the text 'Drop your data file here' is displayed, followed by a note that 'The maximum file upload size is 500 Mb'. To the right of the main content area is a sidebar with several categories:

- KNOWLEDGE**: Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Advanced search; All configurations.
- SYSTEM**: Server settings; Server controls; Licensing.
- DATA**: Data inputs; Forwarding and receiving; Indexes; Report acceleration summaries.
- DISTRIBUTED ENVIRONMENT**: Indexer clustering; Forwarder management; Distributed search.
- USERS AND AUTHENTICATION**: Access controls.

**FAQ**

- > What kinds of files can Splunk index?
- > What is a source?
- > How do I get remote data onto my Splunk instance?

localhost:8000/en-US/manager/search/adddata

# SEARCH DASHBOARD



splunk > App: Search & Reporting ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Pivot Reports Alerts Dashboards **App bar** Search & Reporting

Search **Search bar** Time range picker  All time ▾ 

enter search here...

## How to Search

If you aren't familiar with searching in Splunk, or want to learn more, checkout one of the following resources.

[Documentation](#) ↗

[Tutorial](#) ↗

## What to Search

109,864 Events  
INDEXED

9 days ago  
EARLIEST EVENT

21 hours ago  
LATEST EVENT

[Data Summary](#)

# DATA SUMMARY



- The Data Summary dialogue displays three tabs: Hosts, Sources, Sourcetypes.
- The host of an event is the host name, IP address, or fully qualified domain name of the network machine from which the event originated.
- The source of an event is the file or directory path, network port, or script from which the event originated.
- The source type of an event tells you what kind of data it is, usually based on how it is formatted. This classification lets you search for the same type of data across multiple sources and hosts.

# DATA SUMMARY

**App bar**

**Save as menu** → Save As ▾ Close

**Search bar**

**Time range picker** → All time ▾

**Search results tabs**

**Events (36,819)** Patterns Statistics **Visualization**

**Search action buttons**

**Job** ▾ II ■ ↻ ↻ ↓ ↪ Smart Mode ▾

**Timeline**

**Events list**

i	Time	Event
>	10/5/14 6:22:16.000 PM	91.205.189.15 - - [05/Oct/2014:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP/1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159  host = www2   source = tutorialdata.zip:/www2/access.log   sourcetype = access_combined_wcookie
>	10/5/14 6:20:56.000 PM	182.236.164.11 - - [05/Oct/2014:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP/1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506  host = www1   source = tutorialdata.zip:/www1/access.log   sourcetype = access_combined_wcookie

**Fields sidebar**

Selected Fields  
 a host 3  
 a source 3  
 a sourcetype 1

Interesting Fields  
 a action 5  
 # bytes 100+  
 a categoryId 8

# Time Range Picker

[Search](#)   [Pivot](#)   [Reports](#)   [Alerts](#)   [Dashboards](#)

Search &amp; Reporting

[New Search](#)**Time range picker**[Save As](#) [Close](#)[All time](#)

buttercupgames

✓ 36,819 events (before 10/7/14 2:48:15.000 PM)

[Job](#) [||](#) [\[ \]](#) [↶](#) [↷](#) [Download](#) [Print](#)[Smart Mode](#)

- By default, the time range for a search is set to All time. When you search large volumes of data, results return faster when you run the search over a smaller time period.
- If one of the Presets is not what you want, you can define a custom time range, such as a Relative time range or a Date & Time Range.  
To run a search over the last two hours, use the Relative time range option.

# Time Range Picker



- > Presets
- > Relative
- > Real-time
- > Date Range
- > Date & Time Range**

Earliest:

09/30/2014

08:40:00.000

HH:MM:SS.SSS

Latest:

09/30/2014

08:45:00.000

HH:MM:SS.SSS

Apply

- > Advanced

- For example, to troubleshoot an issue that took place September 30th at 8:42 PM, you can specify the earliest time to be 09/30/2014 08:40:00.000 and the latest time to be 09/30/2014 08:45:00.000.

# Search Actions and Modes

The screenshot shows the Splunk search interface. At the top, there's a navigation bar with tabs: Search, Pivot, Reports, Alerts, Dashboards, and a dropdown for Search & Reporting. Below the navigation bar is a search bar with the placeholder "New Search". A dropdown menu is open, showing a search term "buttercupgames", a count of "36,819 events (before 4/30/14 2:19:02.000 PM)", and a "Save as menu" section with "Save As" and "Close" options. To the right of the search bar is a "Search mode selector" with "All time" and a search icon. Below the search bar are "Search action buttons" including "Job", "Pause", "Stop", "Next", "Previous", and "Smart Mode". A red box highlights the "Search action buttons" area, and a red arrow points to it from the text below. Another red arrow points to the "Search mode selector" from the same text.

- Control search job progress

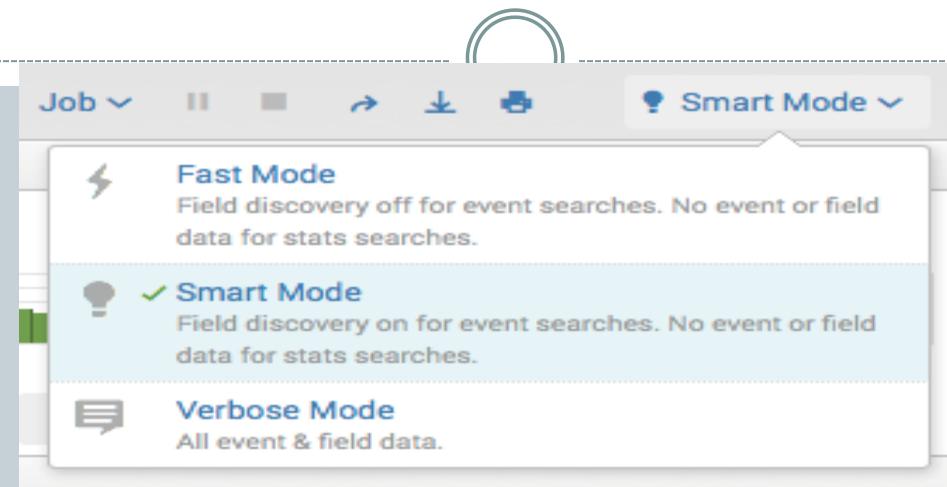
After you launch a search, you can pause it and stop it using the buttons under the search bar. Also, you can access and manage information about the search's job without leaving the Search page.

# Search Actions and Modes



- Click Job and choose from the available options there.
- **Edit job settings.** Select this option to open the Job Settings dialog box, where you can change the job's read permissions, extend the job's lifespan, and get a URL for the job that you can use to share the job with others or put a link to the job in your browser's bookmark bar.
- **Send job to the background.** Select this option if the search job is slow and you want to run the job in the background while you work on other Splunk Enterprise activities (including running a new search job).
- **Inspect job.** Opens a separate window and displays information and metrics for the search job using the Search Job Inspector.
- **Delete job.** Use this option to delete a job that is running, is paused, or which has finalized. After you delete the job, you can save the search as a report.

# Search Actions and Modes

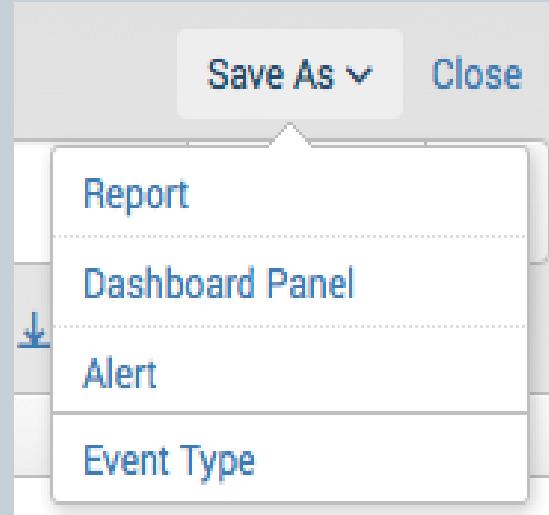


- The Search mode controls the search experience. You can set it to speed up searches by cutting down on the event data it returns (Fast mode), or you can set it to return as much event information as possible (Verbose mode). In Smart mode (the default setting) it toggles search behavior based on the type of search you're running.

# Search Actions and Modes



- Save the results
- The Save as menu lists options for saving the results of a search as a Report, Dashboard Panel, Alert, and Event type.



# Search Actions and Modes



- Other search actions
  - The **Share** option shares the search job. This option extends the job's lifetime to seven days and set the read permissions to Everyone.
  - The **Export** option exports the results. Select this option to output to CSV, raw events, XML, or JSON and specify the number of results to export.
  - The **Print** option sends the results to a printer that has been configured.

# Search Actions and Modes



- **Search Results Tabs**

The screenshot shows the Splunk search interface. At the top, there's a green navigation bar with tabs: Search, Pivot, Reports, Alerts, Dashboards, and a right-aligned "Search & Reporting" section. Below this is a search bar with the query "buttercupgames". To the right of the search bar are "Save As" and "Close" buttons. Underneath the search bar, a message indicates "36,819 events (before 10/8/14 2:14:27.000 PM)". The main area features a "Search results bar" with tabs: Events (36,819) (highlighted with a red box), Patterns, Statistics, and Visualization. A red arrow points from the text "Search results bar" to the right edge of the highlighted tab. Below the search results bar, there are controls for "Format Timeline" (with options: Zoom Out, Zoom to Selection, Deselect), a timeline visualization showing event density over time, and pagination controls at the bottom.

- If your search retrieves events, you can view the results in the Events tab and the Patterns tab, but not in the other tabs. If your search includes transforming commands, you can view the results in the Statistics and Visualization tabs.

# Search Actions and Modes

- Events - The keyword search used in this screenshot retrieves events and populates the Events results tab.

Screenshot of Splunk interface showing search results for "buttercupgames".

**Search terms:** buttercupgames

**Events view options:** List, Format, 20 Per Page

**Timeline of events:** 1 day per column

**Search term matches:**

Time	Event
10/5/14 6:22:16.000 PM	91.205.189.15 - - [05/Oct/2014:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP/1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159 host = www2   source = tutorialdata.zip://www2/access.log   sourcetype = access_combined_wcookie
10/5/14 6:20:56.000 PM	182.236.164.11 - - [05/Oct/2014:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=B9-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP/1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506 host = www1   source = tutorialdata.zip://www1/access.log   sourcetype = access_combined_wcookie

**Fields sidebar:**

- Selected Fields:
  - host 3
  - source 3
  - sourcetype 1
- Interesting Fields:
  - action 5
  - # bytes 100+
  - categoryid 8

# Search Actions and Modes



- The Events tab displays the timeline of events, the fields sidebar, and the events viewer. To change the event view, use the List and Format options. By default, the events appear as a list that is ordered starting with the most recent event. In each event, the matching search terms are highlighted.

# Search Actions and Modes



- **Timeline of events:** A visual representation of the number of events that occur at each point in time. As the timeline updates with your search results, you might notice clusters or patterns of bars. The height of each bar indicates the count of events. Peaks or valleys in the timeline can indicate spikes in activity or server downtime. Thus, the timeline highlights patterns of events or investigates peaks and lows in event activity. The timeline options are located above the timeline. You can zoom in, zoom out, and change the scale of the chart.

# Search Actions and Modes



- **Timeline of events:** A visual representation of the number of events that occur at each point in time. As the timeline updates with your search results, you might notice clusters or patterns of bars. The height of each bar indicates the count of events. Peaks or valleys in the timeline can indicate spikes in activity or server downtime. Thus, the timeline highlights patterns of events or investigates peaks and lows in event activity. The timeline options are located above the timeline. You can zoom in, zoom out, and change the scale of the chart.

# Search Actions and Modes



- **Fields sidebar:** When you index data, Splunk by default extracts information from your data that is formatted as name and value pairs, which we call fields. When you run a search, Splunk lists all of the fields it discovers in the fields sidebar next to your search results. You can select other fields to show in your events. Also, you can hide this sidebar and maximize the results area.
- Selected fields are set to be visible in your search results. By default, host, source, and sourcetype appear.
- Interesting fields are other fields that Splunk has extracted from your search results.

# Search Actions and Modes



## ○ Patterns

The Patterns tab simplifies event pattern detection. It displays a list of the most common patterns among the set of events returned by your search. Each of these patterns represents a number of events that all share a similar structure.

## ○ You can click on a pattern to:

- View the approximate number of events in your results that fit the pattern.
- See the search that returns events with this pattern.
- Save the pattern search as an event type, if it qualifies.
- Create an alert based on the pattern.

# Search Actions and Modes



- **Statistics**
- The Statistics tab populates when you run a search with transforming commands such as stats, top, chart, and so on. The previous keyword search for "buttercupgames" does not display any results in this tab because it does not have any transforming commands.
- With a transforming search, such as one to find the popular categories of items sold on the Buttercup Games online store, the Statistics tab displays a table of results.

# Search Actions and Modes

[Search](#)   [Pivot](#)   [Reports](#)   [Alerts](#)   [Dashboards](#)

Search &amp; Reporting

[New Search](#)[Save As](#) [Close](#)

buttercupgames | top categoryId

All time



✓ 36,819 events (before 10/8/14 9:09:50.000 PM)

[Job](#) [II](#) [III](#) [IV](#) [V](#) [VI](#) [VII](#) [VIII](#)[Smart Mode](#)[Events](#)   [Patterns](#)   [Statistics \(8\)](#)   [Visualization](#)[20 Per Page](#) [Format](#) [Preview](#)**Statistics view options**

categoryId	count	percent
STRATEGY	4399	26.654144
ARCADE	2631	15.941590
NULL	2041	12.366699
ACCESSORIES	2035	12.330344
TEE	1937	11.736549
SIMULATION	1375	8.331314
SHOOTER	1323	8.016238
SPORTS	763	4.623122

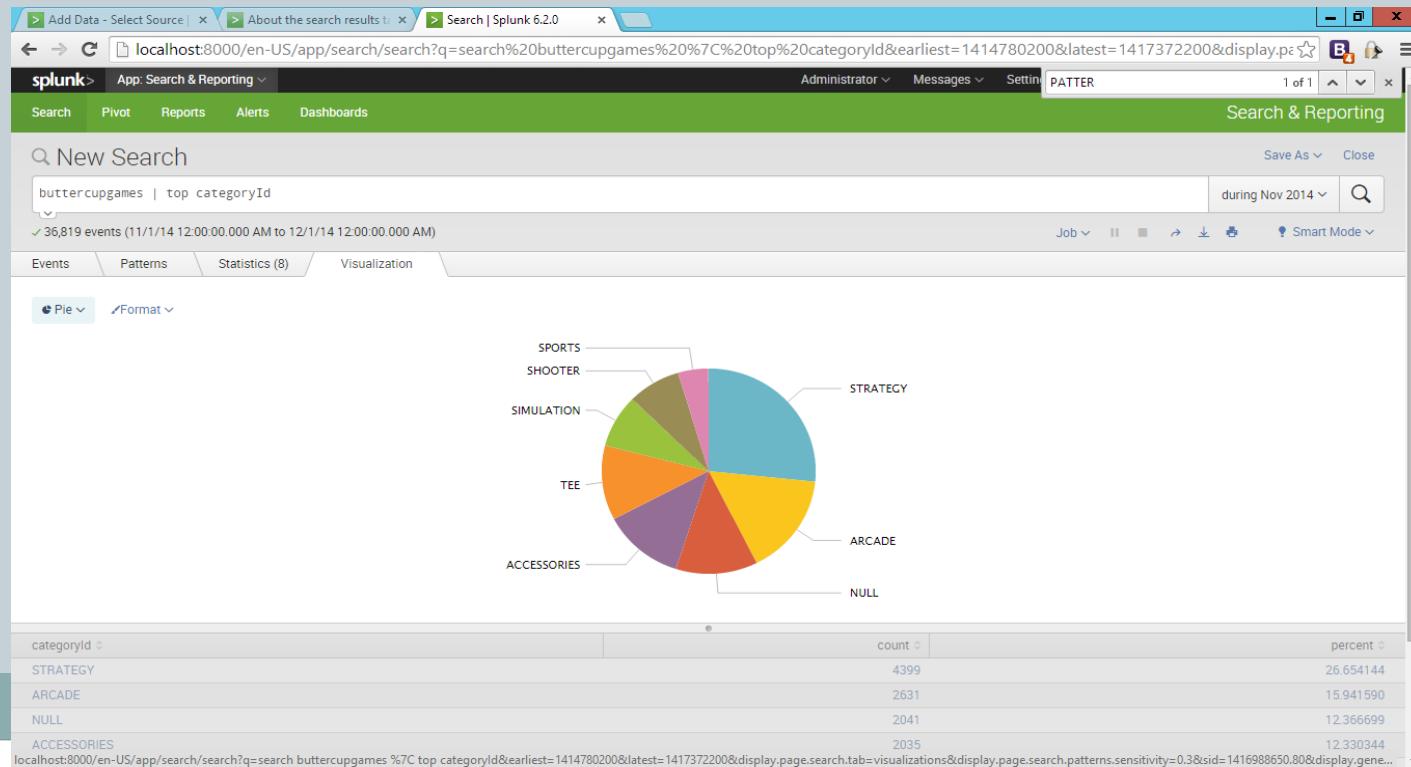
**Statistics table**

# Search Actions and Modes



## • Visualizations

Transforming searches also populate the Visualization tab. The results area of the Visualizations tab includes a chart and the statistics table used to generate the chart. By default, the visualization type is the Columnchart.



# Start Searching



- **Retrieve events from the index**
- 1. Type in keywords to find errors or failures and use Boolean operators: AND, OR, NOT.
- EXAMPLE: buttercupgames (error OR fail\* OR severe)
- Boolean operators need to be capitalized. The AND directive is implied between terms, so you do not need to write it. You can use parentheses to group terms. When evaluating boolean expressions, precedence is given to terms inside parentheses. AND or NOT clauses are evaluated before OR clauses. The asterisk wildcard is used to match terms that start with "fail". These terms can include: failure, failed, and so on.

# Start Searching



- **Use fields to search**
- Fields exist in machine data in many forms. Often, a field is a value (with a fixed, delimited position on the line) or a name and value pair, where there is a single value to each field name. A field can be multivalued, that is, it can appear more than once in an event and has a different value for each appearance.
- Some examples of fields are clientip for IP addresses accessing your Web server, \_time for the timestamp of an event, and host for domain name of a server. One of the more common examples of multivalue fields is email address fields. While the From field will contain only a single email address, the To and Cc fields have one or more email addresses associated with them.
- In Splunk Enterprise, fields are searchable name and value pairings that distinguish one event from another because not all events will have the same fields and field values. Fields let you write more tailored searches to retrieve the specific events that you want.

# Start Searching



- **Find and select fields**
- SEARCH BAR: sourcetype="access\_\*"

Search for fields use the syntax: fieldname="fieldvalue" . Field names are case sensitive, but field values are not. You can use wildcards in field values. Quotes are required when the field values include spaces.

This search indicates that you want to retrieve only events from your web access logs and nothing else.

This search uses the wildcard access\_\* to match any Apache web access sourcetype, which can be access\_common, access\_combined, or access\_combined\_wcookie.

- **In the Events tab, scroll through the list of events.**
  - If you are familiar with the access\_combined format of Apache logs, you recognize some of the information in each event, such as:
    - IP addresses for the users accessing the website.
    - URIs and URLs for the pages requested and referring pages.
    - HTTP status codes for each page request.
    - GET or POST page request methods.

# Start Searching



List ▾ Format ▾ 20 Per Page ▾

< Prev 1 2 3 4 5 6 7 8 9 ... Next >

Hide Fields		All Fields	t	Time	Event
			>	4/30/14 6:22:16.000 PM	91.205.189.15 - - [30/Apr/2014:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159 host = www2   source = tutorialdata.zip.:./www2/access.log   sourcetype = access_combined_wcookie
Selected Fields			>	4/30/14 6:22:15.000 PM	91.205.189.15 - - [30/Apr/2014:18:22:15] "GET /category.screen?categoryId=SHOOTER&JSESSID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1369 "http://www.google.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 779 host = www2   source = tutorialdata.zip.:./www2/access.log   sourcetype = access_combined_wcookie
Interesting Fields			>	4/30/14 6:20:56.000 PM	182.236.164.11 - - [30/Apr/2014:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506 host = www1   source = tutorialdata.zip.:./www1/access.log   sourcetype = access_combined_wcookie
			>	4/30/14 6:20:55.000 PM	182.236.164.11 - - [30/Apr/2014:18:20:55] "POST /oldlink?itemId=EST-18&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 408 893 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 134 host = www1   source = tutorialdata.zip.:./www1/access.log   sourcetype = access_combined_wcookie

# Start Searching

Select action, categoryId, and productId and close the Select Fields window. The three fields appear under Selected Fields in the sidebar. The selected fields appear under the events in your search results if they exist in that particular event. Every event might not have the same fields.

# Start Searching



- Under Selected Fields, click the action field.  
This opens the field summary for the action field.

The screenshot shows a search interface with a sidebar and a main summary panel.

**Left Sidebar:**

- < Hide Fields
- All Fields
- Selected Fields
  - a action 5
  - a categoryId 8
  - a host 3
  - a productId 16
  - a source 3
  - a sourcetype 1
- Interesting Fields
  - # bytes 100+

**Main Summary Panel:**

**Panel Title:** action

**Summary Statistics:** 5 Values, 49.878% of events

**Filter Buttons:** Selected Yes No

**Report Options:** Top values, Top values by time, Rare values

**Events with this field:**

Values	Count	%
addtocart	5,743	29.126%
purchase	5,737	29.095%
view	5,391	27.34%
remove	1,445	7.328%
changequantity	1,402	7.11%

# Start Searching



- **Run more targeted searches**
- **Example1:** Search for successful purchases from the Buttercup Games store.

sourcetype=access\_\* status=200 action=purchase

You can search for failed purchases in a similar manner using status!=200, which looks for all events where the HTTP status code is not equal to 200.

sourcetype=access\_\* status!=200 action=purchase

**Example 2:** Search for general errors.

(error OR fail\* OR severe) OR (status=404 OR status=500 OR status=503)

**Example 3:** Search for how many simulation games were bought yesterday.

Select the Preset time range, Yesterday, from the time range picker and run:

sourcetype=access\_\* status=200 action=purchase categoryId=simulation

# Use The Search Language



- The searches you have run to this point have retrieved events from your Splunk index. You were limited to asking questions that could only be answered by the number of events returned.
- For example, we can run this search to see how many simulation games were purchased:
- `sourcetype=access_* status=200 action=purchase categoryId=simulation`
- To find this number for the days of the previous week, you have to run it against the data for each day of that week. To see which products are more popular than the other, you have to run the search for each of the eight `categoryId` values and compare the results.

# Use The Search Language



## Learn with search assistant

Here we are going to talk about the search assistant to learn about the Splunk search processing language and construct searches.

Return to the search dashboard and restrict your search to Yesterday:

```
sourcetype=access_* status=200 action=purchase
```

As you type in the search bar, search assistant opens with syntax and usage information for the search command (on the right side). If search assistant doesn't open, click the down arrow under the left side of the search bar. You've seen before that search assistant displays typeahead for keywords that you type into the search bar. It also explains briefly how to search.

# Use The Search Language



Search Pivot Reports Alerts Dashboards

Search &amp; Reporting

## New Search

Save As ▾ Close

sourcetype=access\_\* status=200 action=purchase

All time ▾



### How to Search

✓ Auto Open

Smart Mode ▾

1 day per column

8 9 ... Next &gt;

#### Step 1: Retrieve Events

The simplest searches return events that match terms you type into the search bar:

terms: error login

quoted phrases: "database error"

boolean operators: login NOT (error OR fail)

wildcards: fail\*

field values: status=404, status!=404, or status>200

#### Step 2: Use Search Commands

More advanced searches use commands to transform, filter, and report on the events you retrieved. Use the vertical bar " | ", or pipe character, to apply a command to the retrieved events.

a host 3

a source 3

-MG-G10" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 178

# Use The Search Language



**Type a pipe character, " | ", into the search bar.**

The pipe indicates to Splunk that you're about to use a command, and that you want to use the results of the search to the left of the pipe as the input to this command. You can pass the results of one command into another command in a series, or pipeline, of search commands.

# Use The Search Language

Search Pivot Reports Alerts Dashboards **Search & Reporting**

## New Search

sourcetype=access\_\* status=200 action=purchase |

Save As ▾ Close All time ▾

Common next commands

- timechart
- chart
- top
- dedup
- stats
- fields
- multikv
- collect
- regex
- rex

**How to Search** ✓ Auto Open

**Using Search Commands**

More advanced searches use commands to transform, filter, and report on the events you retrieved.

- Use the vertical bar, or pipe character, to apply a command to the retrieved events:  
`sourcetype=access_* error | top 20 uri`
- Further refine or transform your search results with additional commands:  
`sourcetype=access_* error | top 20 uri | search count>5`

Search assistant will suggest commands for you to use next and show you examples to help you build your search.

**Other commands**

a host 3

urchase&itemId=ES  
www.buttercupgame  
TION&productId=SC  
-MG-G10" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Ge

# Use The Search Language

You want Splunk to give you the most popular items bought at the online store.

Search Pivot Reports Alerts Dashboards **Search & Reporting**

## New Search

Save As ▾ Close

```
sourcetype=access_* status=200 action=purchase | top
```

All time ▾

Command history

- ... | top ESXHost
- ... | top user
- ... | top limit=100 signature
- ... | top src\_ip
- ... | top dest\_ip

top Help More » Smart Mode ▾

Displays the most common values of a field.

Examples

Return the 20 most common values of the "url" field.  
... | top limit=20 url

Return top URL values.  
... | top url

Return top "user" values for each "host".  
... | top user by host

1 day per column

8 9 ... Next >

urchase&itemId=ES  
www.buttercupgame  
TION&productId=SC  
-MG-G10" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Ge

a host 3

# Use The Search Language



- Type the categoryId field into the search bar to complete your search.  
`sourcetype=access_* status=200 action=purchase | top categoryId`
- **View reports in the Statistics tab**

The results of a search are reports. The top command is a transforming command and returns a tabulated report for the most common values of categoryId. You can view the results of transforming searches in the Statistics tab.

# Use The Search Language



Search   Pivot   Reports   Alerts   Dashboards   **Search & Reporting**

## New Search

sourcetype=access\_\* status=200 action=purchase | top categoryId

All time

✓ 5,224 events (before 10/13/14 10:15:20.000 AM)

Job Smart Mode

Events   Patterns   Statistics (7)   **Visualization**

20 Per Page Format Preview

categoryId	count	percent
STRATEGY	806	30.495649
ARCADE	493	18.653046
TEE	367	13.885736
ACCESSORIES	348	13.166856
SIMULATION	246	9.307605
SHOOTER	245	9.269769
SPORTS	138	5.221339

# Use The Search Language



- View and format reports in the Visualization tab

You can also view the results of transforming searches in the Visualizations tab

Search Pivot Reports Alerts Dashboards **Search & Reporting**

**New Search** Save As ▾ Close

```
sourcetype=access_* status=200 action=purchase | top categoryId
```

All time ▾ Job ▾ Smart Mode ▾

Events Patterns Statistics (7) **Visualization**

Column Format

Line  
Area  
**Column** Recommended  
Bar Recommended  
Pie Recommended  
Scatter  
Bubble  
Single Value  
Radial Gauge  
Filler Gauge  
Marker Gauge  
Map

The chart displays the count of events for various category IDs. The x-axis is labeled 'categoryId' and shows categories: TEE, ACCESSORIES, SIMULATION, SHOOTER, and SPORTS. The y-axis is labeled 'count'. The bars are colored teal.

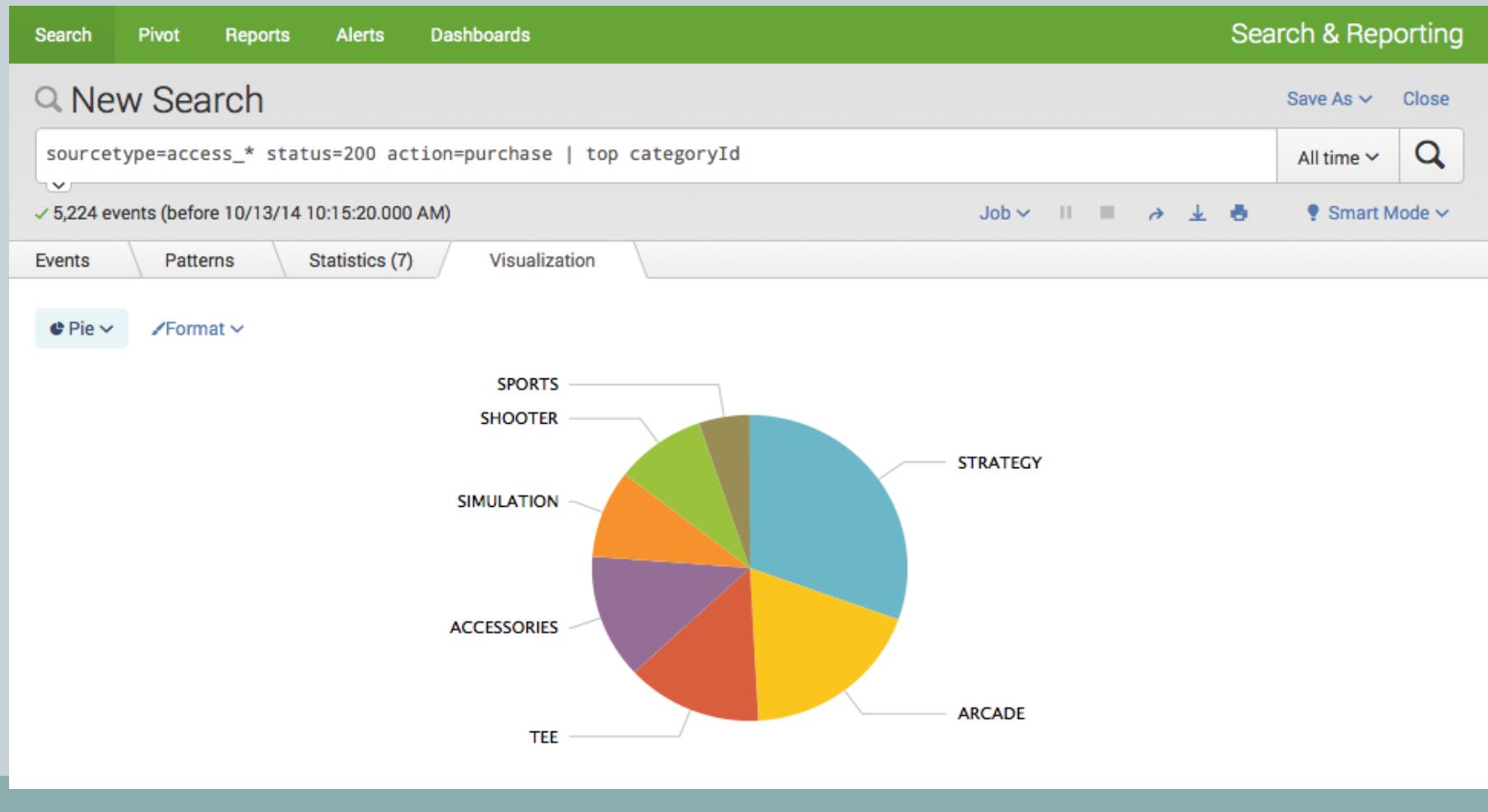
categoryId	count
TEE	806
ACCESSORIES	806
SIMULATION	806
SHOOTER	806
SPORTS	806

percent ▾ 30.495649

# Use The Search Language



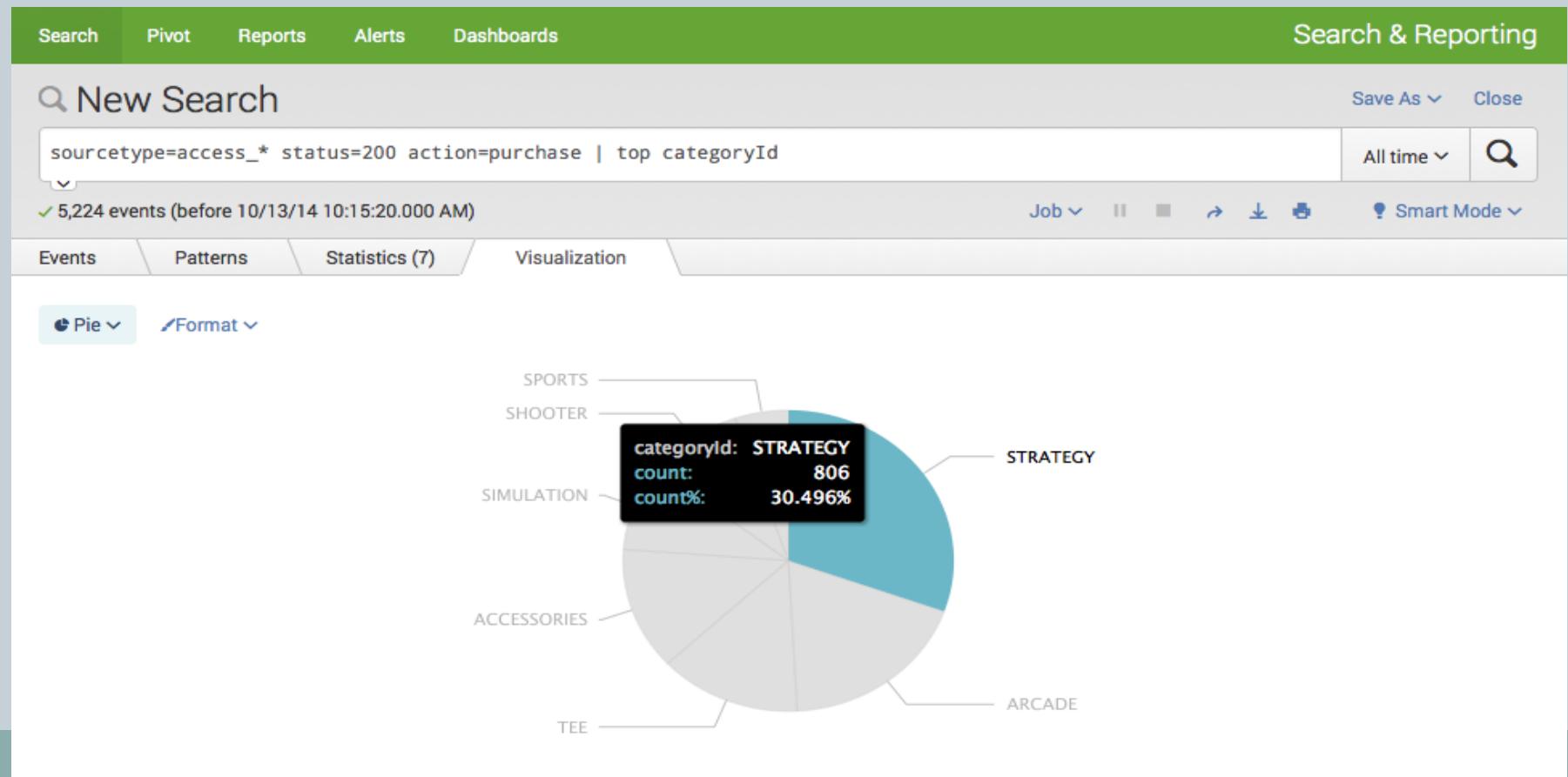
## SELECT PIE



# Use The Search Language



Mouse over each slice of the pie to see the count and percentage values for each categoryId.



# Use The Search Language



Search   Pivot   Reports   Alerts   Dashboards   **Search & Reporting**

## New Search

**sourcetype=access\_\* status=200 action=purchase categoryId=STRATEGY**   All time

✓ 806 events (before 10/13/14 11:07:47.000 AM)

Job Smart Mode

Events (806)   Patterns   Statistics   Visualization

Format Timeline         1 hour per column

List   Format   20 Per Page   < Prev   1   2   3   4   5   6   7   8   9   ...   Next >

All Fields			
< Hide Fields	t	Time	Event
Selected Fields	>	10/11/14 6:02:54.000 PM	74.53.23.135 - - [11/Oct/2014:18:02:54] "POST /cart.do?action=purchase&itemId=EST-12&jSESSIONID=SD8SL10FF5ADFF53017 HTTP 1.1" 200 3848 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-12&categoryId=STRATEGY&productId=DB-SG-G01" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 119 host = www1   source = tutorialdata.zip:/www1/access.log   sourcetype = access_combined_wcookie
Interesting Fields	>	10/11/14 5:42:06.000 PM	125.89.78.6 - - [11/Oct/2014:17:42:06] "POST /cart.do?action=purchase&itemId=EST-13&jSESSIONID=SD10SL8FF3ADFF52952 HTTP 1.1" 200 3957 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-13&categoryId=STRATEGY&productId=DB-SG-G01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 183 host = www2   source = tutorialdata.zip:/www2/access.log   sourcetype = access_combined_wcookie
	>	10/11/14 5:26:38.000 PM	76.169.7.252 - - [11/Oct/2014:17:26:38] "POST /cart.do?action=purchase&itemId=EST-12&jSESSIONID=SD6SL9FF9ADFF52880 HTTP 1.1" 200 1548 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-12&categoryId=STRATEGY&productId=DB-SG-G01" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 473 host = www1   source = tutorialdata.zip:/www1/access.log   sourcetype = access_combined_wcookie

# Use a Subsearch



- This topic walks you through examples of correlating events with subsearches.

A subsearch is a search with a search pipeline as an argument. Subsearches are contained in square brackets and evaluated first. The result of the subsearch is then used as an argument to the primary, or outer, search.

## Example 1: Without a subsearch

Let's try to find the single most frequent shopper on the Buttercup Games online store and what this customer has purchased.

To do this, search for the customer who accessed the online shop the most.

### 1. Use the top command:

```
sourcetype=access_* status=200 action=purchase | top limit=1 clientip
```

Limit the top command to return only one result for the clientip. To see more than one "top purchasing customer", change this limit value.

# Use a Subsearch



Search   Pivot   Reports   Alerts   Dashboards

Search & Reporting

New Search

Save As ▾   Close

```
sourcetype=access_* status=200 action=purchase | top limit=1 clientip
```

All time ▾



✓ 5,224 events (before 10/13/14 11:56:58.000 AM)

Job ▾   II   ■   →   ↓   ↕   Smart Mode ▾

Events

Patterns

Statistics (1)

Visualization

20 Per Page ▾

Format ▾

Preview ▾

clientip	count	percent
87.194.216.51	134	2.565084

This search returns one clientip value, which we'll use to identify our VIP customer.

# Use a Subsearch



Use the stats command to count this VIP customer's purchases:

```
sourcetype=access_* status=200 action=purchase clientip=87.194.216.51 | stats count, dc(productId) by clientip
```

Searched in **Search & Reporting**

New Search Save As ▾ Close

`sourcetype=access_* status=200 action=purchase clientip=87.194.216.51 | stats count, dc(productId) by clientip` All time 🔍

✓ 134 events (before 10/13/14 12:29:33.000 PM) Job ▾ || ☰ ↶ ↓ ↶ Smart Mode ▾

Events Patterns Statistics (1) **Visualization**

20 Per Page Format ▾ Preview ▾

clientip	count	dc(productId)
87.194.216.51	134	14

This search used the `count()` function which only returns the total count of purchases for the customer. The `dc()` function is used to count how many different products he buys.

# Use a Subsearch



The drawback to this approach is that you have to run two searches each time you want to build this table. The top purchaser is not likely to be the same person at any given time range.

Hence we induce the concept of SUBSEARCH !!

# Use a Subsearch



## Example 2: With a subsearch

```
sourcetype=access_* status=200 action=purchase [search  
sourcetype=access_* status=200 action=purchase | top limit=1 clientip | table  
clientip] | stats count, dc(productId), values(productId) by clientip
```

- Here, the subsearch is the segment that is enclosed in square brackets, []. This search, search sourcetype=access\_\* status=200 action=purchase | top limit=1 clientip | table clientip is the same as Example 1 Step 1, except for the last piped command, | table clientip
- Because the top command returns count and percent fields as well, the table command is used to keep only the clientip value.

# Use a Subsearch



Search Pivot Reports Alerts Dashboards

Search &amp; Reporting

New Search

Save As ▾ Close

```
sourcetype=access_* status=200 action=purchase [search sourcetype=access_* status=200 action=purchase | top  
limit=1 clientip | table clientip] | stats count, dc(productId), values(productId) by clientip
```

All time ▾



✓ 134 events (before 10/13/14 12:01:32.000 PM)

Job ▾ || ⏪ ⏴ ⏵ ⏶ ⏷ ⏸

Smart Mode ▾

Events

Patterns

Statistics (1)

Visualization

20 Per Page ▾

Format ▾

Preview ▾

clientip	count	dc(productId)	values(productId)
87.194.216.51	134	14	BS-AG-G09 CU-PG-G06 DB-SG-G01 DC-SG-G02 FI-AG-G08 FS-SG-G03 MB-AG-G07 MB-AG-T01 PZ-SG-G05 SC-MG-G10 WC-SH-A01 WC-SH-A02 WC-SH-G04 WC-SH-T02

# Use a Subsearch



Rename the columns to make the information more understandable.

```
sourcetype=access_* status=200 action=purchase [search
sourcetype=access_* status=200 action=purchase | top limit=1 clientip | table
clientip] | stats count AS "Total Purchased", dc(productId) AS "Total Products",
values(productId) AS "Products ID" by clientip | rename clientip AS "VIP
Customer"
```

# Use a Subsearch



Search Pivot Reports Alerts Dashboards **Search & Reporting**

## New Search

Save As ▾ Close

```
sourcetype=access_* status=200 action=purchase [search sourcetype=access_* status=200 action=purchase | top limit=1 clientip | table clientip] | stats count AS "Total Purchased", dc(productId) AS "Total Products", values(productId) AS "Products ID" by clientip | rename clientip AS "VIP Customer"
```

All time ▾ 

✓ 134 events (before 10/13/14 12:02:05.000 PM)

Job ▾  Smart Mode ▾

Events Patterns Statistics (1) **Visualization**

20 Per Page ▾ Format ▾ Preview ▾

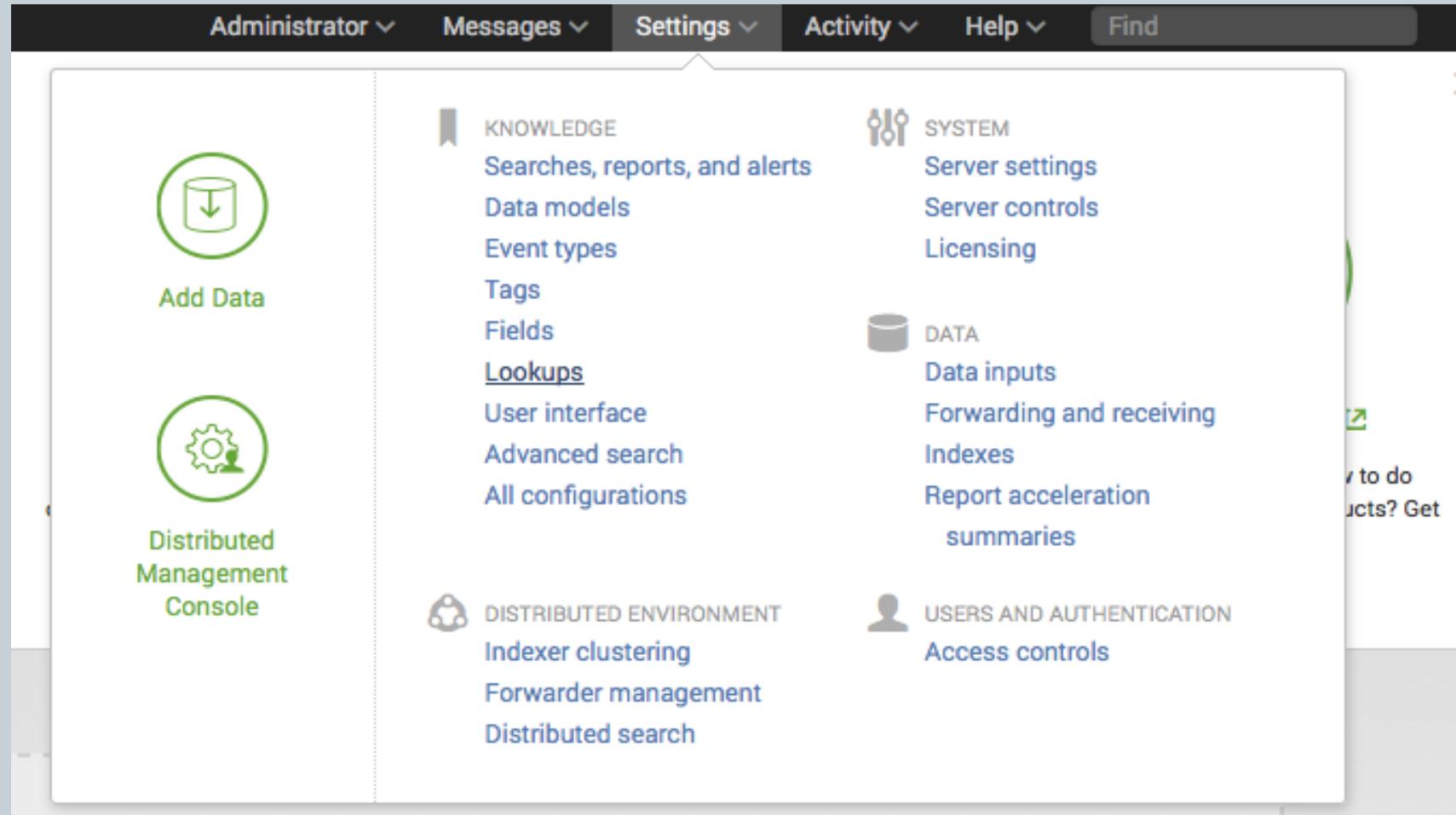
VIP Customer ▾	Total Purchased ▾	Total Products ▾	Products ID ▾
87.194.216.51	134	14	BS-AG-G09 CU-PG-G06 DB-SG-G01 DC-SG-G02 FI-AG-G08 FS-SG-G03 MB-AG-G07 MB-AG-T01 PZ-SG-G05 SC-MG-G10 WC-SH-A01 WC-SH-A02 WC-SH-G04 WC-SH-T02

# Use Field Lookups



This topic takes you through using field lookups to add new fields to your events. Field lookups let you reference fields in an external CSV file that match fields in your event data. Using this match, you can enrich your event data by adding more meaningful information and searchable fields to each event.

# Use Field Lookups



The screenshot shows a software application interface with a navigation bar at the top and a main content area below.

**Navigation Bar:**

- Administrator ▾
- Messages ▾
- Settings ▾
- Activity ▾
- Help ▾
- Find

**Main Content Area:**

- Add Data** (Icon: Circular arrow)
- Distributed Management Console** (Icon: Gear and monitor)
- KNOWLEDGE** (Icon: Book)
- [Searches, reports, and alerts](#)
- [Data models](#)
- [Event types](#)
- [Tags](#)
- [Fields](#)
- [Lookups](#)
- [User interface](#)
- [Advanced search](#)
- [All configurations](#)
- SYSTEM** (Icon: Tools)
- [Server settings](#)
- [Server controls](#)
- [Licensing](#)
- DATA** (Icon: Database)
- [Data inputs](#)
- [Forwarding and receiving](#)
- [Indexes](#)
- [Report acceleration summaries](#)
- DISTRIBUTED ENVIRONMENT** (Icon: Cluster)
- [Indexer clustering](#)
- [Forwarder management](#)
- [Distributed search](#)
- USERS AND AUTHENTICATION** (Icon: User)
- [Access controls](#)

# Use Field Lookups



## Lookups

Create and configure lookups.

---

**Actions****Lookup table files**[Add new](#)

*List existing lookup tables or upload a new file.*

**Lookup definitions**[Add new](#)

*Edit existing lookup definitions or define a new file-based or external lookup.*

**Automatic lookups**[Add new](#)

*Edit existing automatic lookups or configure a new lookup to run automatically.*

# Use Field Lookups



- Upload the lookup table file
  1. In the Lookups manager under "Actions" for Lookup table files, click Add new. This takes you to the 'Add new' lookup table files view where you upload CSV files to use in your definitions for field lookups.

## Add new

[Lookups](#) » [Lookup table files](#) » Add new

Destination app \*

Upload a lookup file

prices.csv

Select either a plaintext CSV file or a gzipped CSV file.

The maximum file size that can be uploaded through the browser is 500MB.

Destination filename \*

Enter the name this lookup table file will have on the Splunk server. If you are uploading a gzipped CSV file, enter a filename ending in ".gz". If you are uploading a plaintext CSV file, we recommend a filename ending in ".csv".

# Use Field Lookups

2. To save your lookup table file in the Search app, leave the Destination app as search.
3. Under Upload a lookup file, browse for the CSV file (prices.csv) to upload.
4. Save

**Lookup table files**  
[Lookups](#) » [Lookup table files](#)

Successfully saved "prices.csv" in search.

App context  Owner

Show only objects created in this app context [Learn more](#)

**New**

Showing 1-1 of 1 item Results per page

Path	Owner	App	Sharing	Status	Actions
/Applications/splunk/etc/users/admin/search/lookups/prices.csv	admin	search	<a href="#">Private   Permissions</a>	Enabled	<a href="#">Move   Delete</a>

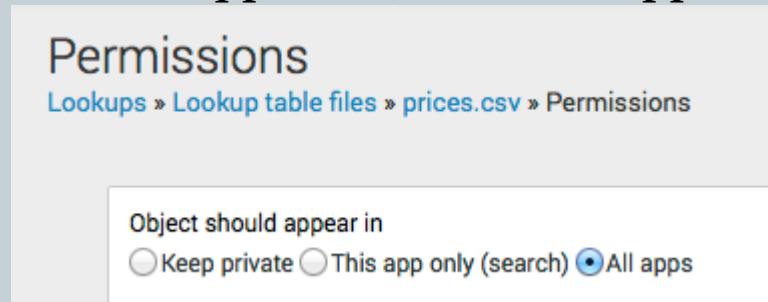
# Use Field Lookups



- **Share the lookup table file globally**

If the lookup file is not shared, you can not select it when you define the lookup.

1. Go to the Lookup table files list.
2. Under Sharing for the prices.csv lookup table's Path, click Permissions. This opens the Permission dialog box for the prices.csv lookup file.
3. Under Object should appear in, select All apps.



4. Click Save.

Path	Owner	App	Sharing	Status	Actions
/Applications/splunk/etc/apps/search/lookups/prices.csv	admin	search	Global   Permissions	Enabled	Move   Delete

# Use Field Lookups



- **Add the field lookup definition**

1. Return to the Lookups manager.
2. Under Actions for Lookup definitions, click Add New.

This takes you to the Add new lookups definitions view where you define your field lookup.

## Add new

Lookups » [Lookup definitions](#) » Add new

Destination app \*

Name \*

Type \*

Lookup file \*

Create and manage [lookup table files](#).

Configure time-based lookup

Advanced options

[Cancel](#) **Save**

# Use Field Lookups

3. Leave the Destination app as search.
4. Name your lookup prices\_lookup.
5. Under Type, select File-based.
  - File-based lookups add fields from a static table, usually a CSV file.
6. Under Lookup file, select prices.csv (the name of your lookup table).
7. Leave Configure time-based lookup and Advanced options unselected.
8. Click Save.

This defines prices\_lookup as a file-based lookup.

## Lookup definitions

[Lookups](#) > [Lookup definitions](#)

Successfully saved "prices\_lookup" in search.

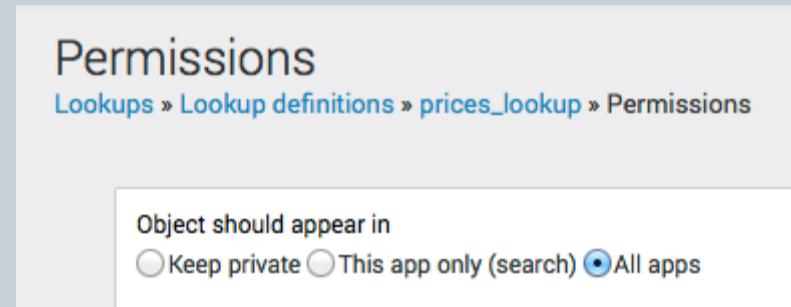
App context	Search & Reporting (search)	Owner	Any				
<input type="checkbox"/> Show only objects created in this app context	<a href="#">Learn more</a>						
<b>New</b>							
Showing 1-4 of 4 items						Results per page <input type="button" value="25"/>	
Name	Type	Supported fields	Owner	App	Sharing	Status	Actions
dnslookup	external	clienthost,clientip	No owner	system	Global   Permissions	Enabled   Disable	<a href="#">Clone</a>
guid_lookup	file	None	No owner	system	Global   Permissions	Enabled   Disable	<a href="#">Clone</a>
prices_lookup	file	productId,product_name,price,sale_price,Code	admin	search	Private   Permissions	Enabled   Disable	<a href="#">Clone</a>   <a href="#">Move</a>   <a href="#">Delete</a>
sid_lookup	file	None	No owner	system	Global   Permissions	Enabled   Disable	<a href="#">Clone</a>

# Use Field Lookups



- Share the lookup definition with all apps
  1. Return to the Lookup definitions list.
  2. Under Sharing for prices\_lookup, click Permissions.  
The Permission dialog box for the prices.lookup opens.
  3. Under Object should appear in, select All apps.
  4. Click Save.

Now, prices\_lookup should be shared with Global permissions.



# Use Field Lookups



- **Make the lookup automatic**

1. In the Lookups manager, under Actions for Automatic lookups, click Add New. This takes you to the Add New automatic lookups view where you configure the lookup to run automatically.

Add new

Lookups » Automatic lookups » Add new

Destination app \*

search

Name \*

Lookup table \*

prices\_lookup

Apply to \*

sourcetype named \*

Lookup input fields

= Delete

Add another field

Lookup output fields

= Delete

Add another field

Overwrite field values

Cancel Save

# Use Field Lookups

2. Leave the Destination app as search.
3. Name your automatic lookup price\_lookup.
4. Under Lookup table, select prices\_lookup.

The screenshot shows two input fields. The first field is labeled 'Name \*' and contains the value 'price\_lookup'. The second field is labeled 'Lookup table \*' and contains the value 'prices\_lookup', which is highlighted in blue, indicating it is selected or being typed.

5. Under Apply to and named, select sourcetype and type in access\_combined\_wcookie.

The screenshot shows two dropdown menus. The left menu is labeled 'Apply to' and has 'sourcetype' selected. The right menu is labeled 'named \*' and has 'access\_combined\_wcookie' selected.

6. Under Lookup input fields type in productId in both text areas under Lookup input fields .

The screenshot shows a single entry in the 'Lookup input fields' section. It consists of two adjacent text boxes separated by an equals sign (=). Both text boxes contain the value 'productId'. To the right of the second text box is a 'Delete' button. Below this entry is a blue 'Add another field' link.

Splunk Enterprise matches the field in the lookup table (which is the one specified on the left) with the field on the right (which is the field in your events). In this case the field names match.

# Use Field Lookups



7. Under Lookup output fields, type in the name of the fields that you want to add to your event data based on the input field matching and rename the fields.

Lookup output fields

product_name	=	productName	<a href="#">Delete</a>
price	=	price	<a href="#">Delete</a>

[Add another field](#)

- 7.1 In the first text area, type product\_name, which contains the descriptive name for each productId.
- 7.2. In the second text area, after the equal sign, type productName. This renames the field to productName.
- 7.3. Click Add another field to add more fields after the first one.
- 7.4. Add the field price, which contains the price for each productId. Do not rename this field.
8. Leave Overwrite field values unchecked.
9. Click Save.

# Use Field Lookups

This returns you to the list of automatic lookups and you should see your configured lookup.

Automatic lookups

Lookups » Automatic lookups

Successfully saved "price\_lookup" in search.

App context: Search & Reporting (search) ▾ Owner: Any ▾

Show only objects created in this app context [Learn more](#)

New

Showing 1-1 of 1 item Results per page: 25 ▾

Name ▾	Lookup ▾	Owner ▾	App ▾	Sharing ▾	Status ▾	Actions
access_combined_wcookie : LOOKUP-price_lookup	prices_lookup productId AS productId OUTPUTNEW price AS price productName AS productName	admin	search	Private   Permissions	Enabled	Clone   Move   Delete

# Use Field Lookups

- Show the new fields in your search results
  1. Return to Search.
  2. Run the search for web access activity.  
sourcetype=access\_\*
  3. Scroll through the list of Interesting Fields in the fields sidebar, and find the price field.
  4. Click price to open its field summary dialog box.



# Use Field Lookups

5. Next to Selected, click Yes.

6. Close the dialog box.

The price field appears under Selected Fields in the fields sidebar.

7. Repeat Steps 3 to 5 for the productName field.

<a href="#">List</a> <a href="#">Format</a> <a href="#">20 Per Page</a> <span style="float: right;">◀ Prev 1 2 3 4 5 6 7 8 9 ... Next ▶</span>			
<a href="#">Hide Fields</a> <a href="#">All Fields</a>			
<b>Selected Fields</b> <a href="#">action</a> 5 <a href="#">categoryId</a> 8 <a href="#">host</a> 3 <a href="#"># price</a> 6 <a href="#">productId</a> 16 <a href="#">productName</a> 12 <a href="#">source</a> 3 <a href="#">sourcetype</a> 1			<i>t</i> Time Event
<a href="#">▶</a> 5/2/14 6:22:16.000 PM 91.205.189.15 - - [02/May/2014:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159 host = www2   source = tutorialdata.zip.:./www2/access.log   sourcetype = access_combined_wcookie			
<a href="#">▶</a> 5/2/14 6:22:15.000 PM 91.205.189.15 - - [02/May/2014:18:22:15] "GET /category.screen?categoryId=SHOOTER&JSESSID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1369 "http://www.google.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 779 categoryId = SHOOTER   host = www2   source = tutorialdata.zip.:./www2/access.log   sourcetype = access_combined_wcookie			
<a href="#">▶</a> 5/2/14 6:20:56.000 PM 182.236.164.11 - - [02/May/2014:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506 action = addtocart   host = www1   price = 24.99   productId = BS-AG-G09   productName = Benign Space Debris   source = tutorialdata.zip.:./www1/access.log   sourcetype = access_combined_wcookie			
<a href="#">▶</a> 5/2/14 6:20:55.000 PM 182.236.164.11 - - [02/May/2014:18:20:55] "POST /oldlink?itemId=EST-18&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 408 893 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 134 host = www1   productId = SF-BVS-G01   source = tutorialdata.zip.:./www1/access.log   sourcetype = access_combined_wcookie			

# Use Field Lookups



## Search with the new lookup fields

- 1. Copy and paste or type in the previous subsearch example to see what the VIP customer bought. This time, replace the productId field with productName.

```
sourcetype=access_* status=200 action=purchase [search sourcetype=access_*
status=200 action=purchase | top limit=1 clientip | table clientip] | stats count AS "Total
Purchased", dc(productId) AS "Total Products", values(productName) AS "Product
Names" by clientip | rename clientip AS "VIP Customer"
```

The result is the same as in the previous subsearch example, except that the VIP customer's purchases are more meaningful with the added descriptive product names.

# Use Field Lookups



Search   Pivot   Reports   Alerts   Dashboards

Search & Reporting

New Search

Save As ▾   Close

```
sourcetype=access_* status=200 action=purchase [search sourcetype=access_* status=200 action=purchase | top  
limit=1 clientip | table clientip] | stats count AS "Total Purchased", dc(productId) AS "Total Products",  
values(productName) AS "Product Names" by clientip | rename clientip AS "VIP Customer"
```

All time ▾



✓ 134 events (before 10/13/14 1:20:51.000 PM)

Job ▾   II   ■   ↗   ↘   ⌂   Smart Mode ▾

Events   Patterns   Statistics (1)

Visualization

20 Per Page ▾

Format ▾

Preview ▾

VIP Customer ▾	Total Purchased ▾	Total Products ▾	Product Names ▾
87.194.216.51	134	14	Benign Space Debris Curling 2014 Dream Crusher Final Sequel Fire Resistance Suit of Provolone Holy Blade of Gouda Manganiello Bros. Mediocre Kingdoms Orvil the Wolverine Puppies vs. Zombies SIM Cubicle World of Cheese

# Saving and Sharing Reports

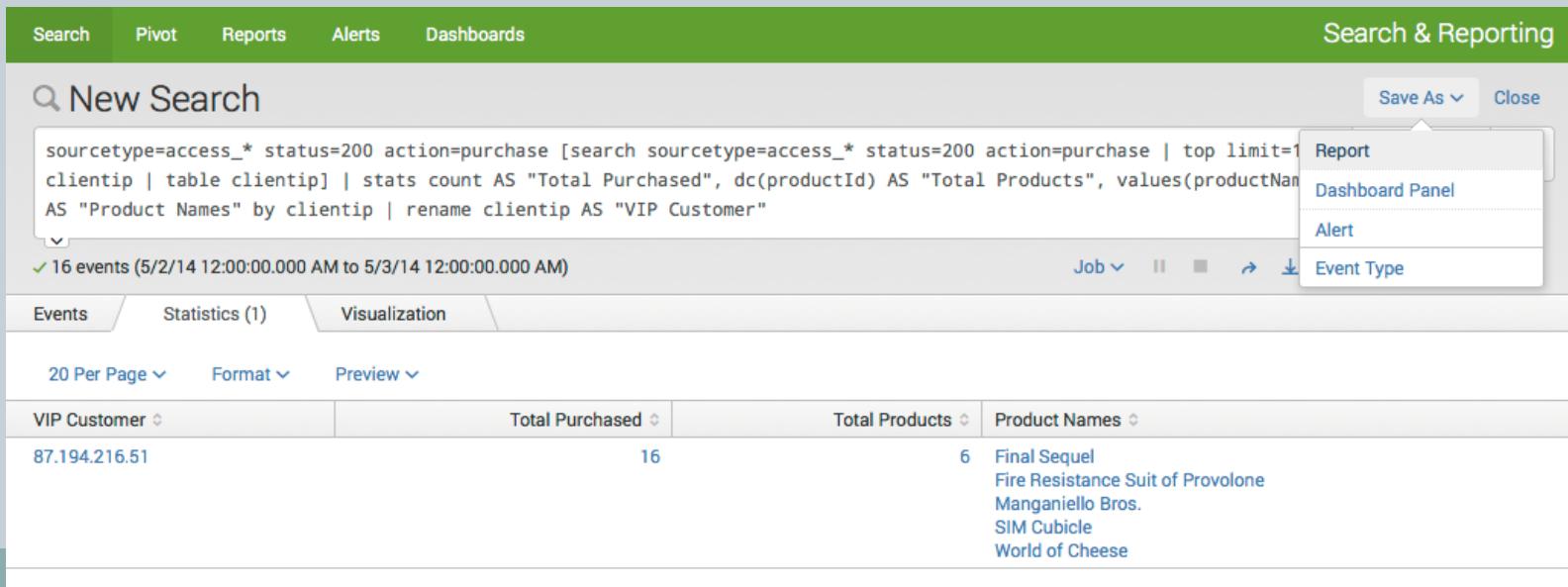


- Save as a report

1. Select the time range Yesterday and run the subsearch

```
sourcetype=access_* status=200 action=purchase [search sourcetype=access_*
status=200 action=purchase | top limit=1 clientip | table clientip] | stats count AS "Total
Purchased", dc(productId) AS "Total Products", values(productName) AS "Product
Names" by clientip | rename clientip AS "VIP Customer"
```

2. To save it as a report, click Save as above the search bar and select Report.



The screenshot shows the Splunk interface with a green header bar containing 'Search', 'Pivot', 'Reports', 'Alerts', and 'Dashboards'. The main area is titled 'New Search' and contains the following search command:

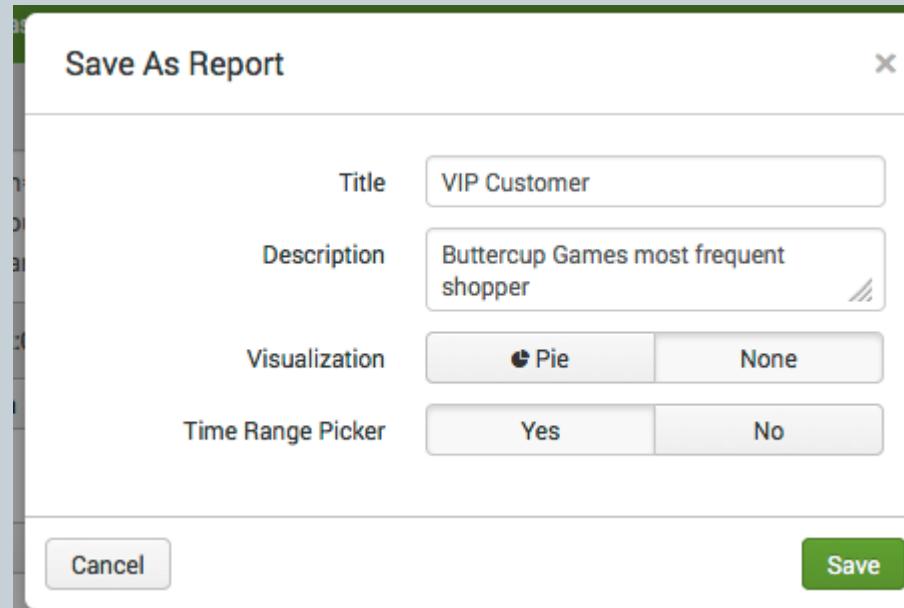
```
sourcetype=access_* status=200 action=purchase [search sourcetype=access_*
status=200 action=purchase | top limit=1 clientip | table clientip] | stats count AS "Total
Purchased", dc(productId) AS "Total Products", values(productName) AS "Product
Names" by clientip | rename clientip AS "VIP Customer"
```

Below the search bar, it says '16 events (5/2/14 12:00:00.000 AM to 5/3/14 12:00:00.000 AM)'. The interface includes tabs for 'Events', 'Statistics (1)', and 'Visualization'. At the bottom, there are filters for 'VIP Customer', 'Total Purchased', 'Total Products', and 'Product Names', along with pagination controls for '20 Per Page', 'Format', and 'Preview'.

A dropdown menu is open at the top right, under 'Save As', showing options: 'Report' (selected), 'Dashboard Panel', 'Alert', and 'Event Type'. A preview of the report results is shown below, listing items like 'Final Sequel', 'Fire Resistance Suit of Provolone', 'Manganiello Bros.', 'SIM Cubicle', and 'World of Cheese'.

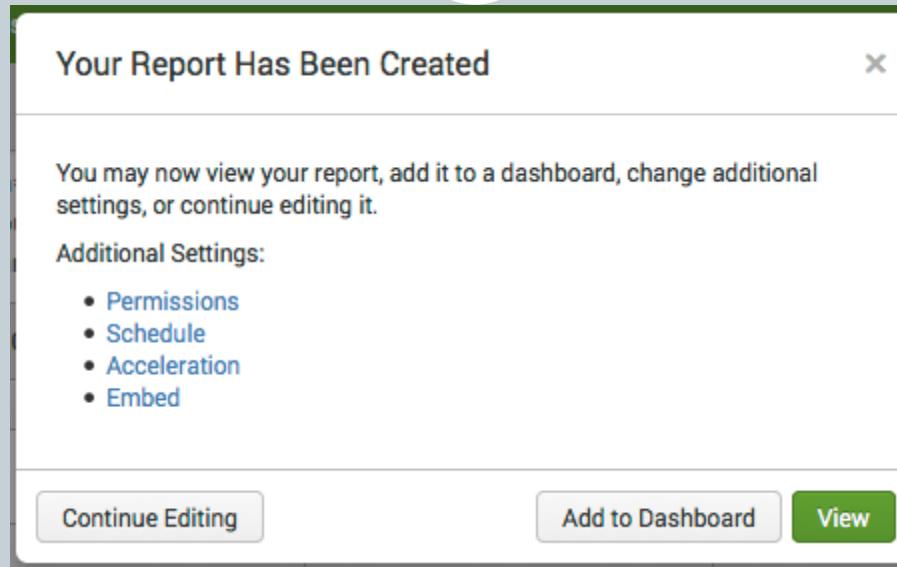
# Saving and Sharing Reports

3. Enter a Title VIP Customer.
4. (Optional) Enter a Description Buttercup Games most frequent shopper.



5. Because the report is a table, for Visualization, click None.
6. To include a Time Range Picker, click Yes.
7. Click Save.  
The Your report has been created dialog box opens.

# Saving and Sharing Reports



- There are other options in this window.  
Continue Editing lets you refine the search and report format.  
Add to dashboard lets you add the report to a new or existing dashboard.  
View lets you view the report.

# Saving and Sharing Reports

8. Click View.

Search Pivot Reports Alerts Dashboards **Search & Reporting**

## VIP Customer

Buttercup Games most frequent shopper

**Yesterday** ✓ 16 events (5/2/14 12:00:00.000 AM to 5/3/14 12:00:00.000 AM) Job ▾

1 result 20 per page ▾

VIP Customer	Total Purchased	Total Products	Product Names
87.194.216.51	16	6	Final Sequel Fire Resistance Suit of Provolone Manganiello Bros. SIM Cubicle World of Cheese

# Saving and Sharing Reports



- **View and edit saved reports**

You can view and edit the saved report from its report view.  
1. In the report view for "VIP Customer", click Edit.

The screenshot shows a report view for a user named "VIP Customer". The top navigation bar includes links for Search, Pivot, Reports, Alerts, and Dashboards, along with a "Search & Reporting" dropdown. The main content area displays the title "VIP Customer" and a subtitle "Buttercup Games most frequent shopper". A date filter shows "Yesterday". Below this, a summary states "16 events (5/2/14 12:00:00.000 AM to 5/3/14 12:00:00.000 AM)". The results table has columns for "VIP Customer", "Total Purchased", "Total Products", and "Product ID". One row is visible for the IP address "87.194.216.51" with values "16", "6", and "Final Sec...". To the right of the table is a context menu with the following items:

- Open in Search
- Edit Description
- Edit Permissions
- Edit Schedule
- Edit Acceleration
- Clone
- Embed
- Delete

VIP Customer	Total Purchased	Total Products	Product ID
87.194.216.51	16	6	Final Sec... Fire Resi... Mangan... SIM Cub... World of Cheese

You can open the report in the search view and edit the saved search's description, permissions, schedule, and acceleration. You can also clone, embed, and delete the report from this menu.

# Saving and Sharing Reports

## 2. Click More Info.

Search Pivot Reports Alerts Dashboards **Search & Reporting**

VIP Customer  
Buttercup Games most frequent shopper

Yesterday ▾

✓ 16 events (5/2/14 12:00:00.000 AM to 5/3/14 12:00:00.000 AM)

1 result 20 per page ▾

VIP Customer	Total Purchased	Total Product
87.194.216.51	16	

More Info ▾

Creator ..... Created by [Search](#).  
App ..... [search](#)  
Schedule ..... Not scheduled. [Edit](#)  
Acceleration ..... Disabled. [Edit](#)  
Permissions ..... Private. Owned by admin. [Edit](#)  
Embedding ..... Disabled. [Edit](#)

6 Final Sequel  
[Fire Resistance Suit of Provolone](#)  
[Manganiello Bros.](#)  
[SIM Cubicle](#)  
[World of Cheese](#)

You can view and edit different properties of the report, including its schedule, acceleration, permissions, and embedding.

# Saving and Sharing Reports



3. Look at the time range picker, located to the top left.

- You saved this report with a time range picker. The time range picker lets you change the time period to run this search. For example, you can use this time range picker to run this search for the VIP Customer Week to date, Last 60 minutes, Last 24 hours just by selecting the Preset time range or defining a custom time range.

The screenshot shows a reporting interface with a green header bar containing 'Search', 'Pivot', 'Reports', 'Alerts', 'Dashboards', and 'Search & Reporting' on the right. Below the header, a report titled 'VIP Customer' is displayed, showing 'Buttercup Games most frequent shopper'. A green button labeled 'Yesterday' is visible. To the right of the report are three buttons: 'Edit', 'More Info', and 'Add to Dashboard'. A large dropdown menu for 'Time Range' is open, divided into sections: 'Presets', 'Relative', and 'Other'. The 'Presets' section includes options like 'Real-time', '30 second window', and 'All time (real-time)'. The 'Relative' section includes 'Today', 'Week to date', and 'Last 15 minutes'. The 'Other' section includes 'All time'. At the bottom of the dropdown are links for 'Relative', 'Real-time', 'Date Range', 'Date & Time Range', and 'Advanced'. To the right of the dropdown, there's a preview area showing a list of product names: 'Famil Sequel', 'Cheese Resistance Suit of Provolone', 'Langaniello Bros.', 'IM Cubicle', and 'World of Cheese'. There are also icons for 'Job', 'Edit', 'More Info', 'Add to Dashboard', and file operations like 'Download' and 'Print'.

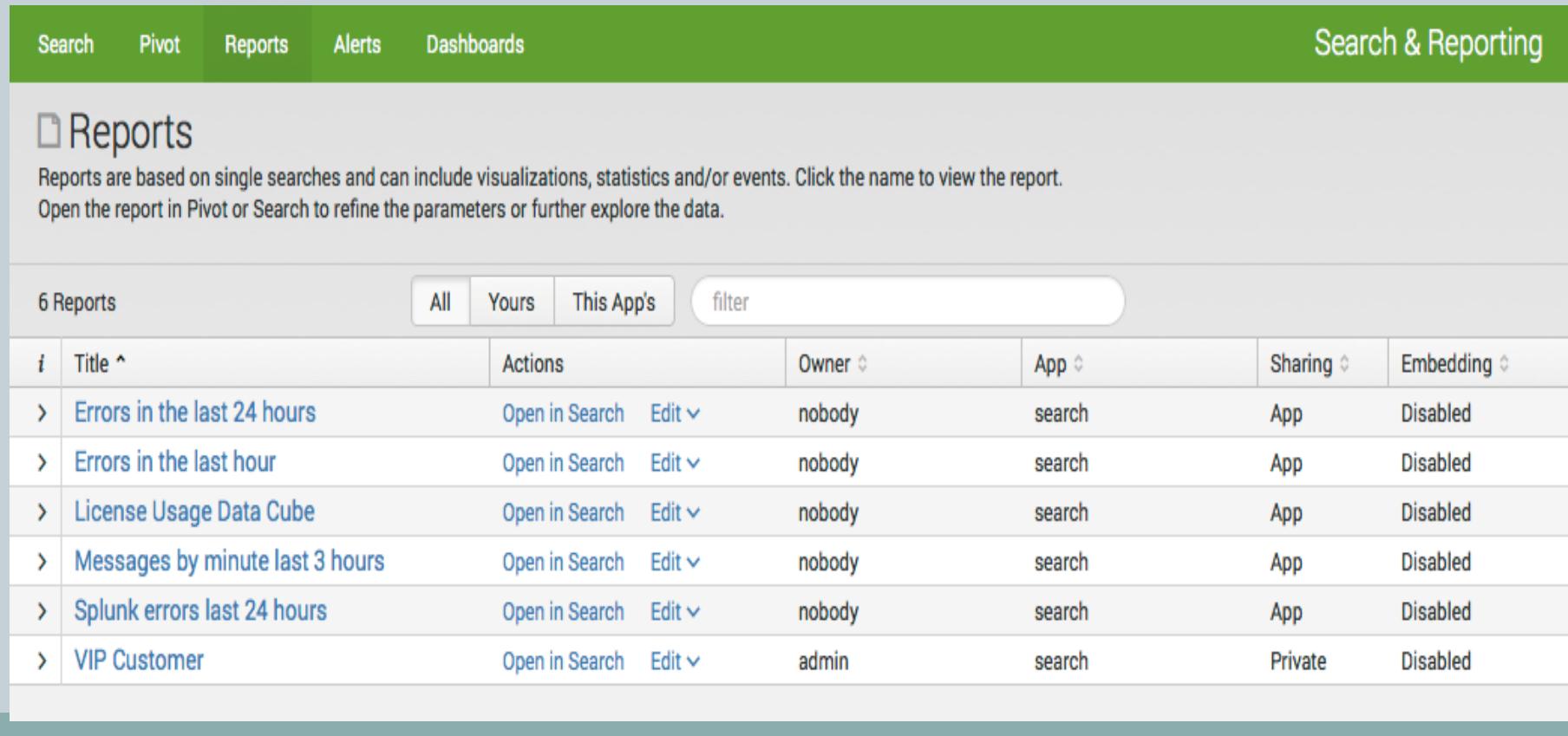
# Saving and Sharing Reports



- Find and share saved reports

You can access your saved reports using the app navigation bar.

1. Click Reports to open the Reports listing page.



The screenshot shows the "Reports" section of the Splunk mobile application. At the top, there is a green navigation bar with tabs for "Search", "Pivot", "Reports" (which is selected and highlighted in blue), "Alerts", and "Dashboards". To the right of the tabs, the text "Search & Reporting" is displayed. Below the navigation bar, the title "Reports" is shown with a report icon. A descriptive text block states: "Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data." A summary indicates "6 Reports". Below this, a table lists six saved reports with columns for Title, Actions, Owner, App, Sharing, and Embedding. Each report row includes a disclosure triangle icon and a link to "Open in Search".

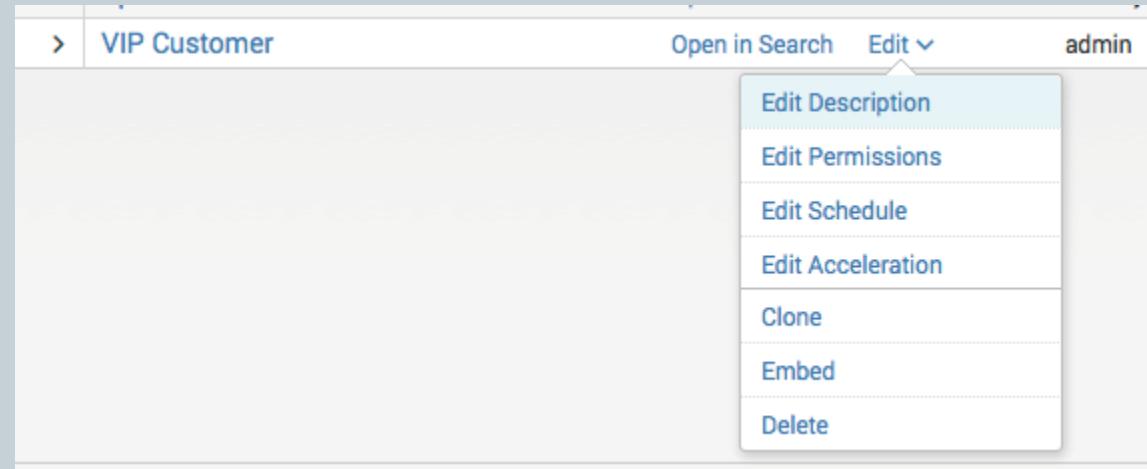
	Title ^	Actions	Owner	App	Sharing	Embedding
>	<a href="#">Errors in the last 24 hours</a>	<a href="#">Open in Search</a> <a href="#">Edit</a>	nobody	search	App	Disabled
>	<a href="#">Errors in the last hour</a>	<a href="#">Open in Search</a> <a href="#">Edit</a>	nobody	search	App	Disabled
>	<a href="#">License Usage Data Cube</a>	<a href="#">Open in Search</a> <a href="#">Edit</a>	nobody	search	App	Disabled
>	<a href="#">Messages by minute last 3 hours</a>	<a href="#">Open in Search</a> <a href="#">Edit</a>	nobody	search	App	Disabled
>	<a href="#">Splunk errors last 24 hours</a>	<a href="#">Open in Search</a> <a href="#">Edit</a>	nobody	search	App	Disabled
>	<a href="#">VIP Customer</a>	<a href="#">Open in Search</a> <a href="#">Edit</a>	admin	search	Private	Disabled

# Saving and Sharing Reports



When you save a new report, its Permissions are set to Private. This means that only you can view and edit the report. You can allow other apps to view, or edit, or view and edit the reports by changing its Permissions.

1. Under Actions for the VIP Customer report, click Edit and select Edit Permissions.



This opens the Edit Permissions dialog box.

# Saving and Sharing Reports



2. In the Edit Permissions dialog box, set Display For to App and check the box under Read for Everyone.

**Edit Permissions**

Report	VIP Customer	
Owner	admin	
App	search	
Display For	<input type="radio"/> Owner <input type="radio"/> App <input checked="" type="radio"/> All Apps	
	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
can_delete	<input checked="" type="checkbox"/>	<input type="checkbox"/>
power	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
splunk-system-role	<input checked="" type="checkbox"/>	<input type="checkbox"/>
user	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Cancel** **Save**

This action gives everyone who has access to this app the permission to view it.

3. Click Save.

# Saving and Sharing Reports



Back at the Reports listing page, you see that the Sharing for VIP Customer now reads App.

Search Pivot Reports Alerts Dashboards Search & Reporting

## Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

6 Reports		All	Yours	This App's	filter		
i	Title ^	Actions		Owner ▾	App ▾	Sharing ▾	Embedding ▾
>	<a href="#">Errors in the last 24 hours</a>	<a href="#">Open in Search</a>	<a href="#">Edit ▾</a>	nobody	search	App	Disabled
>	<a href="#">Errors in the last hour</a>	<a href="#">Open in Search</a>	<a href="#">Edit ▾</a>	nobody	search	App	Disabled
>	<a href="#">License Usage Data Cube</a>	<a href="#">Open in Search</a>	<a href="#">Edit ▾</a>	nobody	search	App	Disabled
>	<a href="#">Messages by minute last 3 hours</a>	<a href="#">Open in Search</a>	<a href="#">Edit ▾</a>	nobody	search	App	Disabled
>	<a href="#">Splunk errors last 24 hours</a>	<a href="#">Open in Search</a>	<a href="#">Edit ▾</a>	nobody	search	App	Disabled
>	<a href="#">VIP Customer</a>	<a href="#">Open in Search</a>	<a href="#">Edit ▾</a>	admin	search	App	Disabled

# More Searches and Reports



- **Example 1: Compare counts of user actions**

In this example, calculate the number of views, purchases, and adds to cart for each type of product. This report requires the productName field from the fields lookup example. If you did not add the lookup, refer to that example and follow the procedure.

1. Run this search:

```
sourcetype=access_* status=200 | chart count AS views count(eval(action="addtocart")) AS addtocart count(eval(action="purchase")) AS purchases by productName | rename productName AS "Product Name", views AS "Views", addtocart AS "Adds to Cart", purchases AS "Purchases"
```

# More Searches and Reports



Search Pivot Reports Alerts Dashboards Search & Reporting

Q New Search Save As ▾ Close

```
sourcetype=access_* status=200 | chart count AS views count(eval(action="addtocart")) AS addtocart
count(eval(action="purchase")) AS purchases by productName | rename productName AS "Product Name", views AS
"Views", addtocart AS "Adds to Cart", purchases AS "Purchases"
```

✓ 34,282 events (before 10/13/14 2:57:49.000 PM) Job ▾ II ■ → ↓ ↴ Smart Mode ▾

Events Patterns Statistics (12) Visualization

20 Per Page ▾ Format ▾ Preview ▾

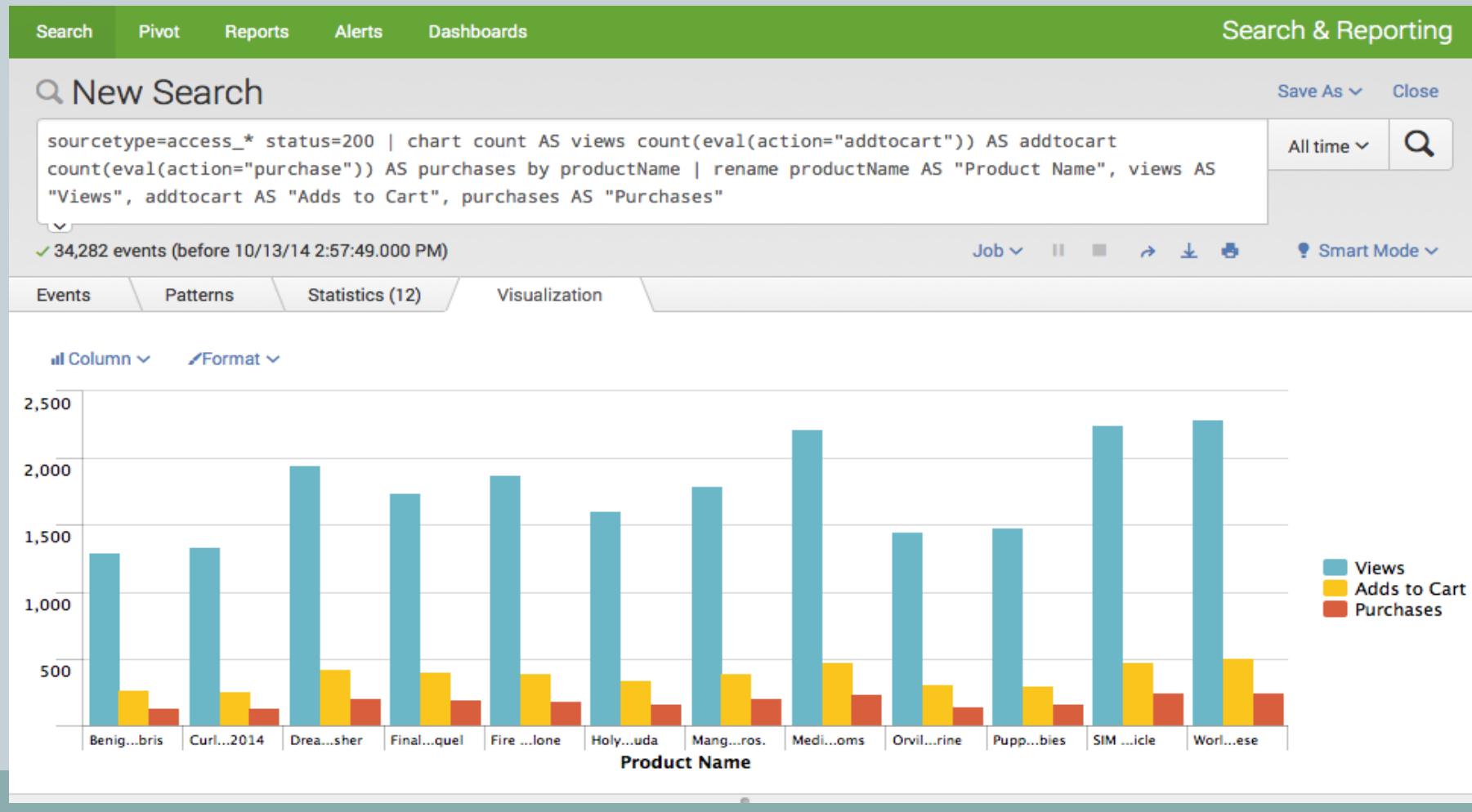
Product Name	Views	Adds to Cart	Purchases
Benign Space Debris	1292	270	134
Curling 2014	1336	263	138
Dream Crusher	1954	421	206
Final Sequel	1745	403	200
Fire Resistance Suit of Provolone	1879	396	187
Holy Blade of Gouda	1604	347	161
Manganiello Bros.	1799	397	209
Mediocre Kingdoms	2222	480	238
Orvil the Wolverine	1455	313	150
Puppies vs. Zombies	1481	296	162
SIM Cubicle	2251	479	246
World of Cheese	2295	509	245

This search uses the [chart command](#) to count the number of events that are action=purchase and action=addtocart.

# More Searches and Reports



2. Use the Visualization view options to format the results as a column chart.



# More Searches and Reports



Example 2: Overlay Actions and Conversion Rates on one chart

1. Run this search:

```
sourcetype=access_* status=200 | stats count AS views count(eval(action="addtocart")) AS addtocart count(eval(action="purchase")) AS purchases by productName | eval viewsToPurchase=(purchases/views)*100 | eval cartToPurchase=(purchases/addtocart)*100 | table productName views addtocart purchases viewsToPurchase cartToPurchase | rename productName AS "Product Name" views AS "Views", addtocart as "Adds To Cart", purchases AS "Purchases"
```

Instead of the chart command, this search uses the stats command to count the user actions. Then, it uses the eval command to define two new fields which calculate conversation rates for "Product Views to Purchases" and "Adds to cart to Purchases".

# More Searches and Reports

Search Pivot Reports Alerts Dashboards Search & Reporting

New Search

Save As ▾ Close

All time ▾ 

sourcetype=access\_\* status=200 | stats count AS views count(eval(action="addtocart")) AS addtocart count(eval(action="purchase")) AS purchases by productName | eval viewsToPurchase=(purchases/views)\*100 | eval cartToPurchase=(purchases/addtocart)\*100 | table productName views addtocart purchases viewsToPurchase cartToPurchase | rename productName AS "Product Name" views AS "Views", addtocart as "Adds To Cart", purchases AS "Purchases"

✓ 34,282 events (before 10/13/14 4:13:37.000 PM) Job ▾ Smart Mode ▾

Events Patterns Statistics (12) Visualization

20 Per Page ▾ Format ▾ Preview ▾

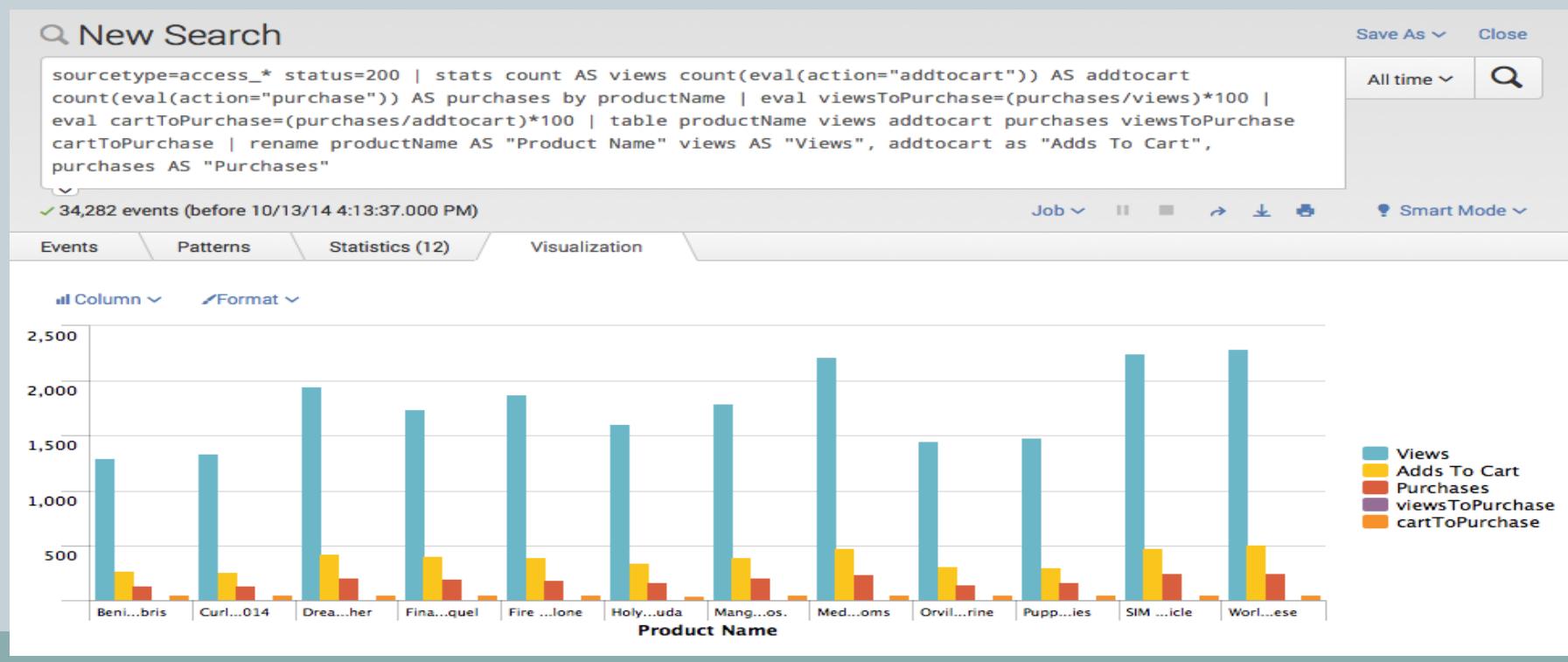
Product Name	Views	Adds To Cart	Purchases	viewsToPurchase	cartToPurchase
Benign Space Debris	1292	270	134	10.371517	49.629630
Curling 2014	1336	263	138	10.329341	52.471483
Dream Crusher	1954	421	206	10.542477	48.931116
Final Sequel	1745	403	200	11.461318	49.627792
Fire Resistance Suit of Provolone	1879	396	187	9.952102	47.222222
Holy Blade of Gouda	1604	347	161	10.037406	46.397695
Manganiello Bros.	1799	397	209	11.617565	52.644836
Mediocre Kingdoms	2222	480	238	10.711071	49.583333
Orvil the Wolverine	1455	313	150	10.309278	47.923323
Puppies vs. Zombies	1481	296	162	10.938555	54.729730
SIM Cubicle	2251	479	246	10.928476	51.356994
World of Cheese	2295	509	245	10.675381	48.133595

# More Searches and Reports

- Steps 2 to 6 reformat the visualization to overlay the Conversion series onto the Actions series.

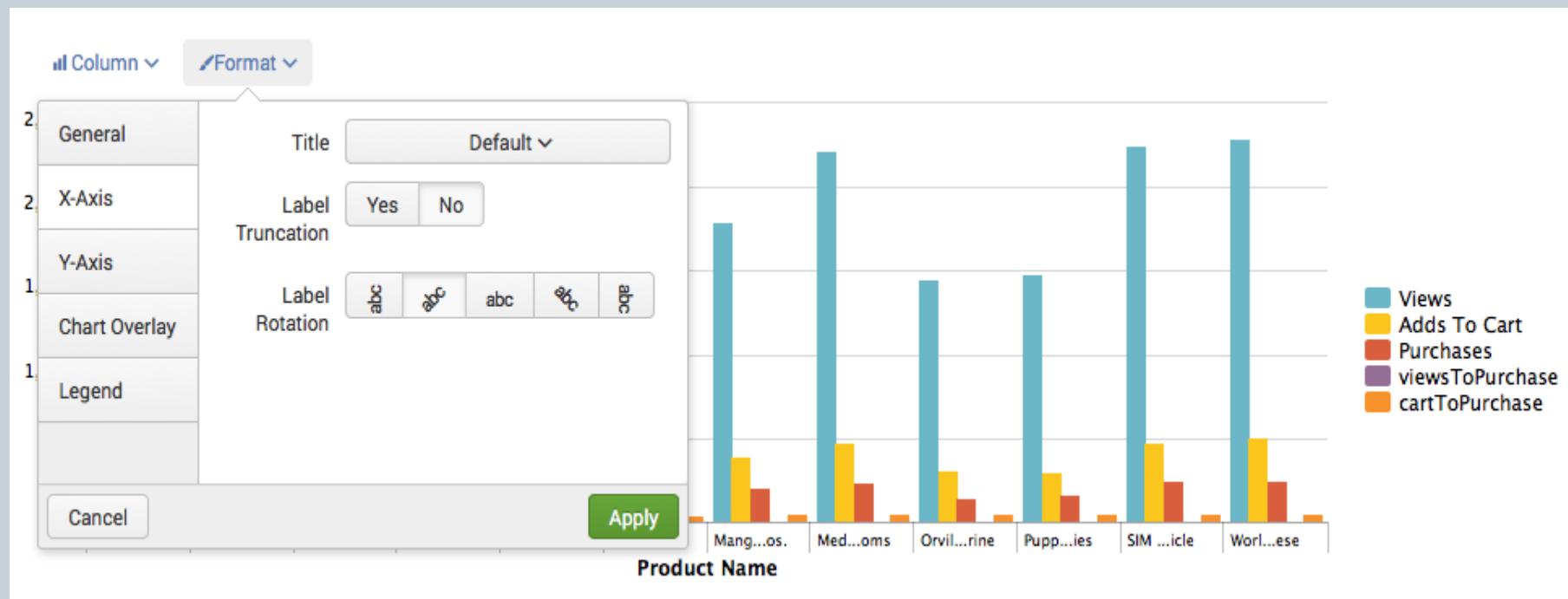
## 2. Click Visualization.

This is the same chart as in Example 1, with two additional series, "viewsToPurchase" and "cartToPurchase".



# More Searches and Reports

## 3. Click Format and X-Axis.

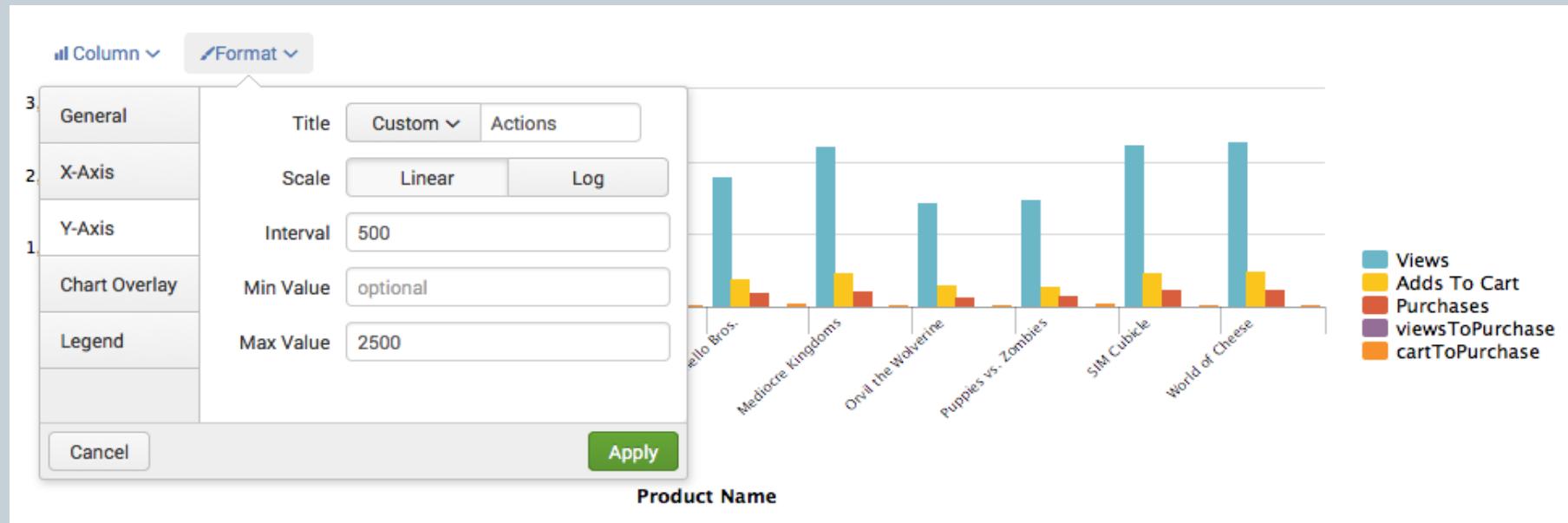


- 3.1 Rotate the label -45 degrees and do not truncate the label.
- 3.2 Click Apply.

# More Searches and Reports



## 4. Click Format and Y-Axis.

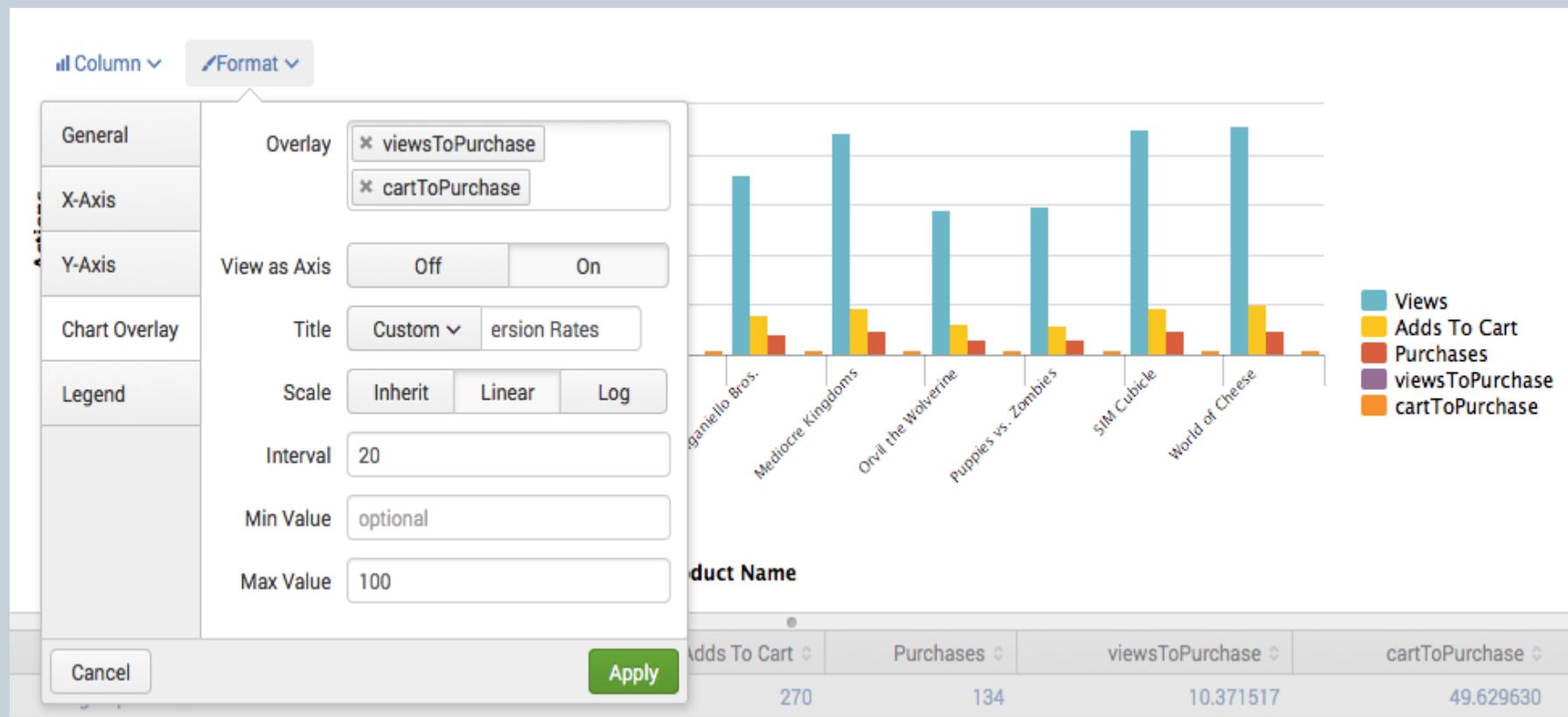


- 4.1 For Title, choose Custom and type in "Actions".
- 4.2 Set the Max Value to 2500 and the Interval to 500.
- 4.3 Click Apply.

# More Searches and Reports



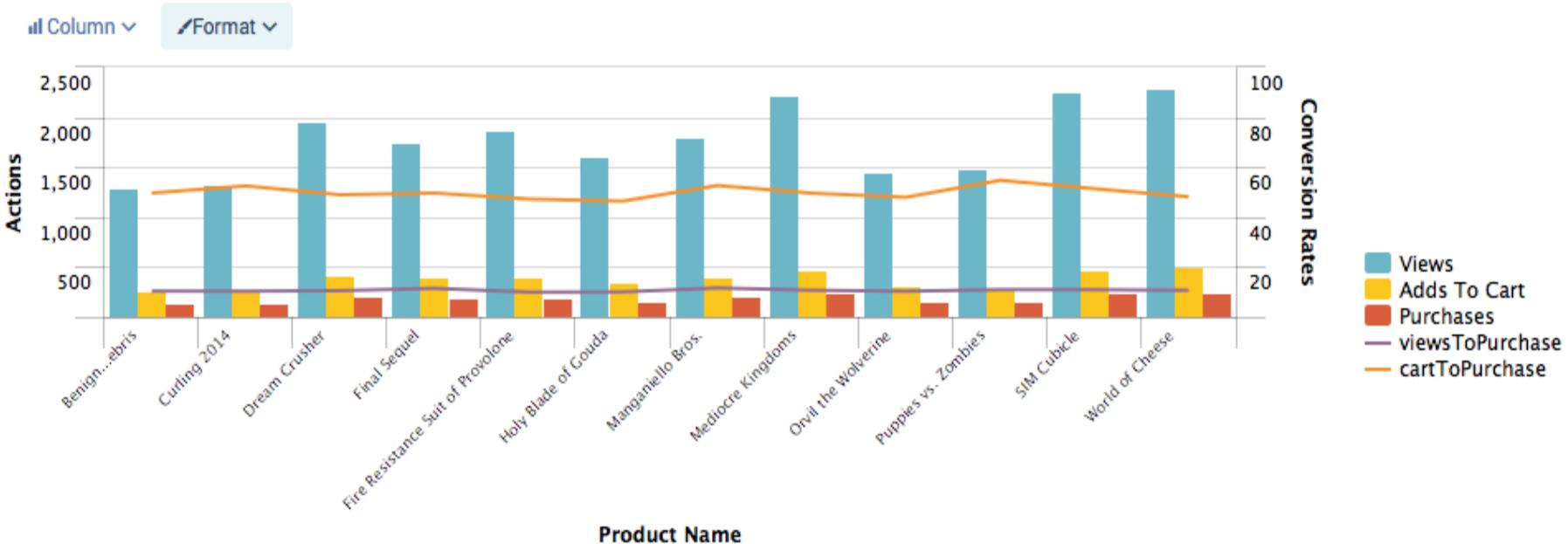
5. Click Format and Chart Overlay.



# More Searches and Reports



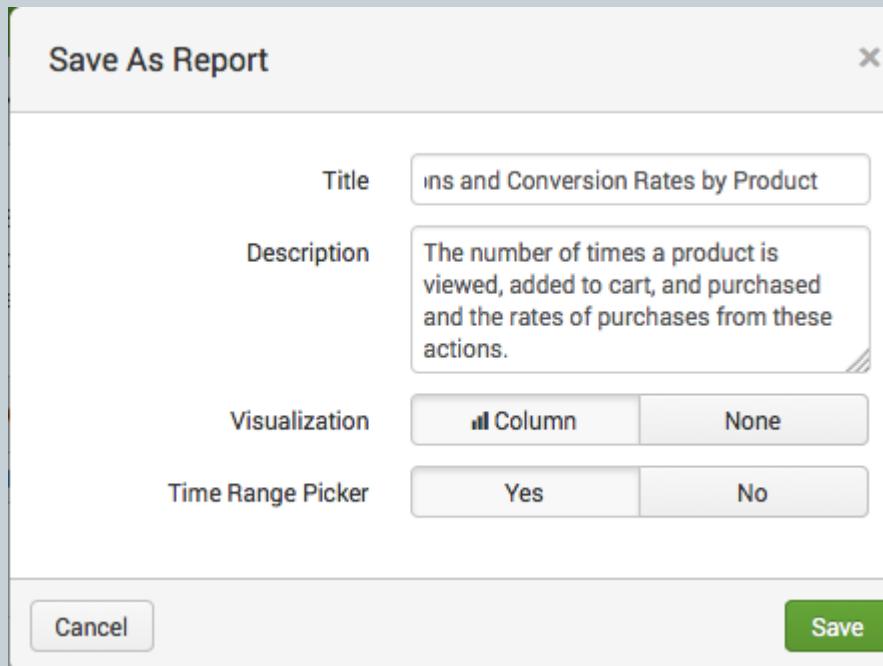
- 5.1 Type in or select the fields, "viewsToPurchase" and "cartToPurchase".
- 5.2 For View as Axis, click On.
- 5.3 For Title, choose Custom and type in Conversion Rates.
- 5.4 For Scale, choose Linear.
- 5.5 Set the Max Value to 100 and the Interval to 20.
- 5.6 Click Apply.



# More Searches and Reports



- 6. Click Save As and select Report.



- 6.1 In the Save Report As dialog box, enter a Title, "Comparison of Actions and Conversion Rates by Product".
- 6.2 (Optional) Enter a Description, "The number of times a product is viewed, added to cart, and purchased and the rates of purchases from these actions."

# More Searches and Reports



- 7. Click Save.

Search Pivot Reports Alerts Dashboards Search & Reporting

## Comparison of Actions and Conversion Rates by Product

The number of times a product is viewed, added to cart, and purchased and the rates of purchases from these actions.

All time ▾ Edit ▾ More Info ▾ Add to Dashboard

✓ 34,282 events (before 10/13/14 6:26:10.000 PM) Job ▾

Product Name	Views	Adds To Cart	Purchases	viewsToPurchase	cartToPurchase
Benign...bris	1450	450	350	10.371517	49.629630
Curling 2014	1450	450	350	10.329341	52.471483
Dream Crusher	2050	550	350	10.542477	48.931116
Final Sequel	1950	550	400	11.461318	49.627792
Fire Resistance Suit of Provokone	2050	550	400		
Holy Blade of Gouda	1750	500	400		
Manganiello Bros.	2000	550	350		
Mediocre Kingdoms	2350	550	450		
Oval the Wolverine	1650	450	350		
Puppies vs. Zombies	1650	450	350		
SIM Cubicle	2400	550	350		
World of Cheese	2400	550	400		

12 results 20 per page ▾

Product Name	Views	Adds To Cart	Purchases	viewsToPurchase	cartToPurchase
Benign Space Debris	1292	270	134	10.371517	49.629630
Curling 2014	1336	263	138	10.329341	52.471483
Dream Crusher	1954	421	206	10.542477	48.931116
Final Sequel	1745	403	200	11.461318	49.627792

# More Searches and Reports



## Example 3: Products purchased over time

For this report, chart the number of purchases that were completed for each item.

This report requires the productName field from the fields lookup example. If you didn't add the lookup, refer to that example and follow the procedure.

1. Search for:

```
sourcetype=access_* | timechart count(eval(action="purchase")) by productName  
usenull="f" useother="f"
```

Use the count() function to count the number of events that have the field action=purchase. Use the usenulland useother arguments to make sure the chart counts events that have a value for productName.

This produces the following statistics table.

# More Searches and Reports


[Search](#) [Pivot](#) [Reports](#) [Alerts](#) [Dashboards](#)
[Search & Reporting](#)

## New Search

[Save As](#) [Close](#)

```
sourcetype=access_* | timechart count(eval(action="purchase")) by productName usenull="f" useother="f"
```

[All time](#)


✓ 39,532 events (before 10/13/14 5:51:03.000 PM)

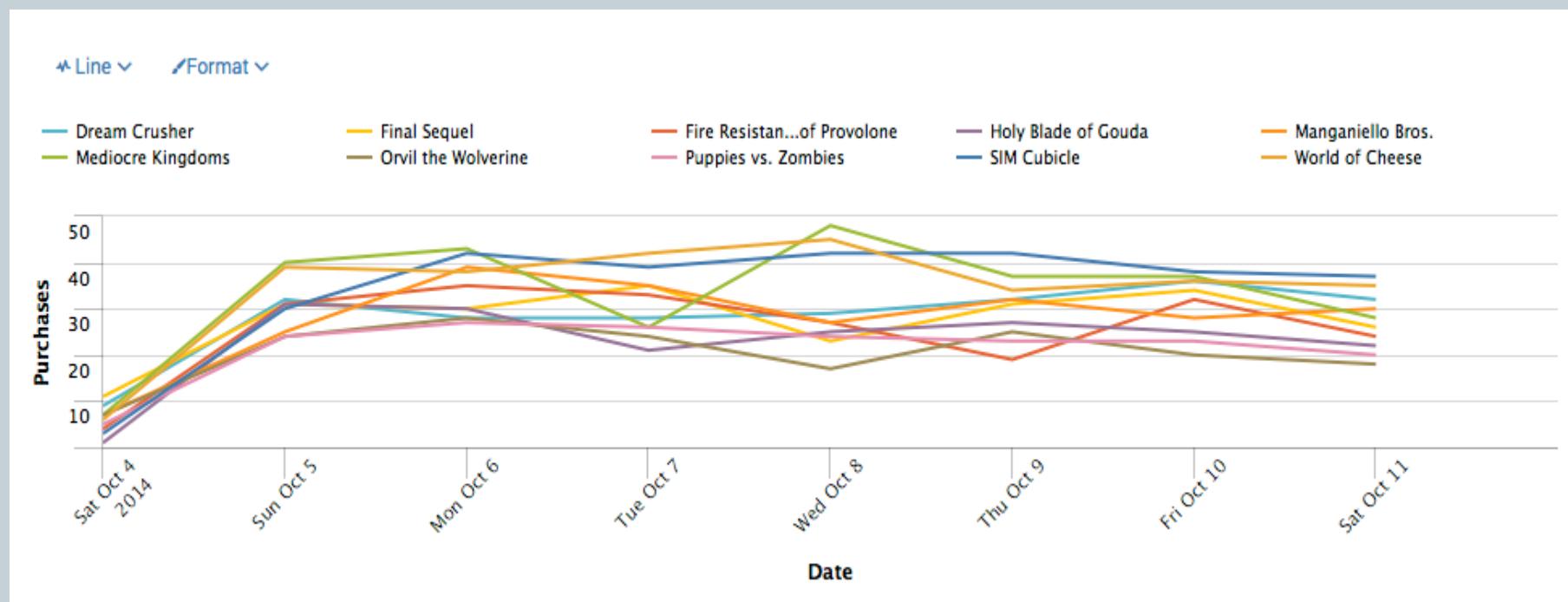
[Job](#)     
[Smart Mode](#)
[Events](#)
[Patterns](#)
[Statistics \(8\)](#)
[Visualization](#)
[20 Per Page](#)
[Format](#)
[Preview](#)

_time	Dream Crusher	Final Sequel	Fire Resistance Suit of Provolone	Holy Blade of Gouda	Manganiello Bros.	Mediocre Kingdoms	Orvil the Wolverine	Puppies vs. Zombies	SIM Cubicle	World of Cheese
2014-10-04	9	11	4	1	7	7	7	5	3	6
2014-10-05	32	31	31	31	25	40	24	24	30	39
2014-10-06	28	30	35	30	39	43	28	27	42	38
2014-10-07	28	35	33	21	35	26	24	26	39	42
2014-10-08	29	23	27	25	27	48	17	24	42	45
2014-10-09	32	31	19	27	32	37	25	23	42	34
2014-10-10	36	34	32	25	28	37	20	23	38	36
2014-10-11	32	26	24	22	30	28	18	20	37	35

# More Searches and Reports



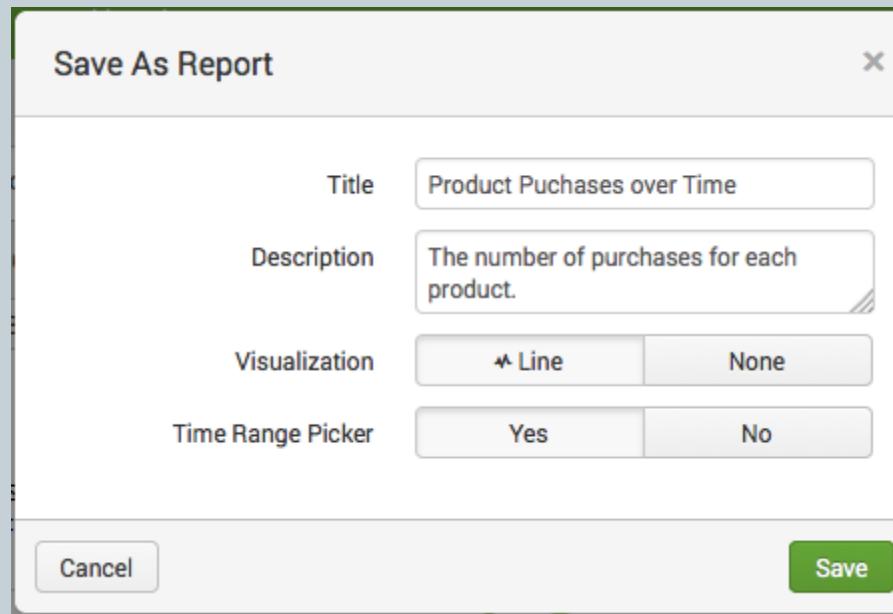
2. Click the Visualization tab and Format the X-Axis, Y-Axis, and Legend to produce the following line chart.



# More Searches and Reports



3. Click Save As and select Report

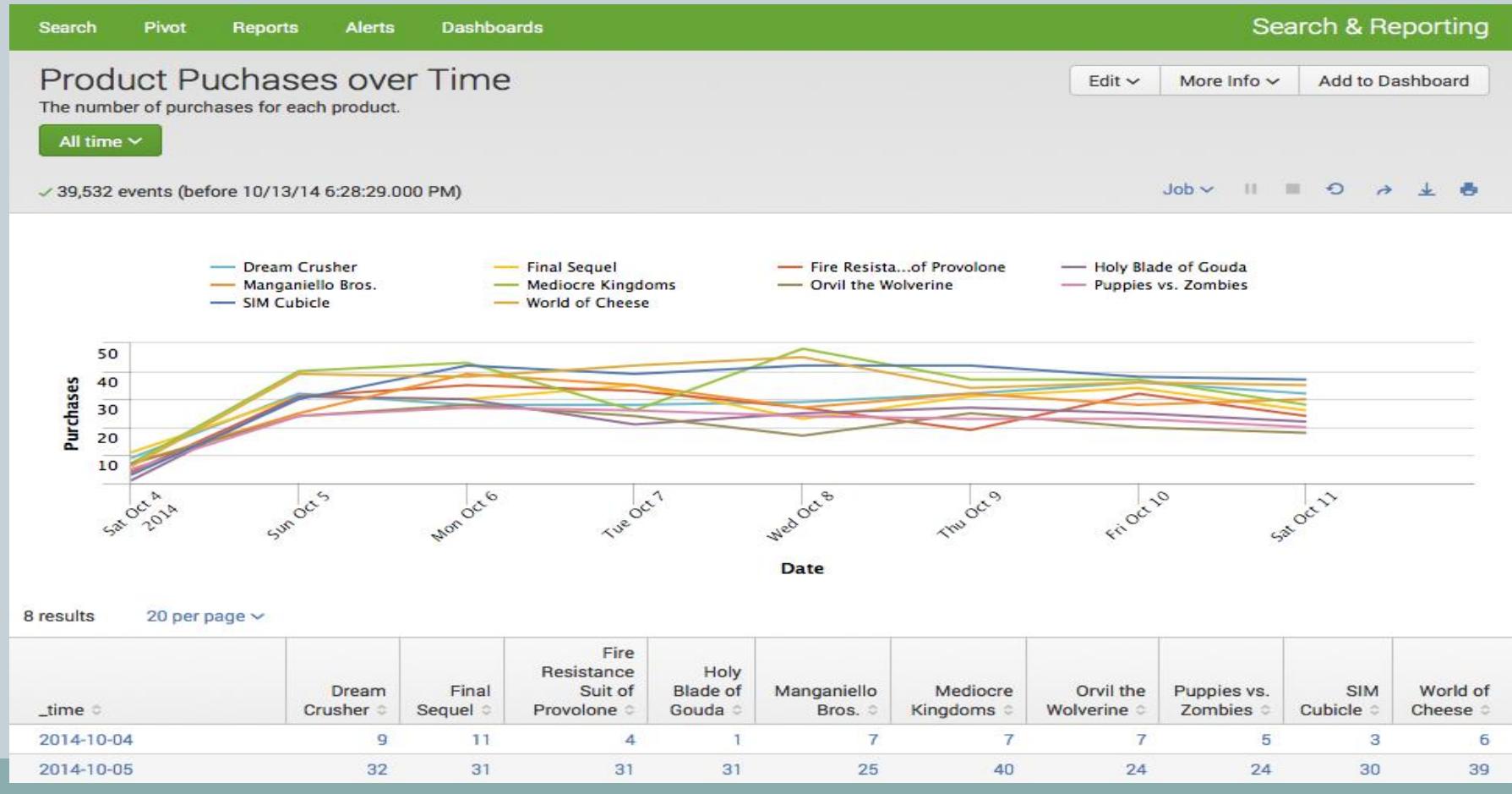


- 3.1 In the Save Report As dialog box, enter a Title, "Product Purchases over Time".
- 3.2 (Optional) Enter a Description, "The number of purchases for each product."

# More Searches and Reports



4. Click Save and View the report.



# More Searches and Reports



## Example 4: Purchasing trends

This example uses sparklines to trend the count of purchases made over time.

For stats and chart searches, you can add sparklines to their results tables. Sparklines are inline charts that appear within the search results table and are designed to display time-based trends associated with the primary key of each row.

This example requires the productName field from the fields lookup example. If you did not add the lookup, refer to that example and follow the procedure.

1. Run the following search:

```
sourcetype=access_* status=200 action=purchase| chart sparkline(count) AS "Purchases Trend" count AS Total by categoryId | rename categoryId AS "Category"
```

# More Searches and Reports



This search uses the chart command to count the number of purchases, action="purchase", made for each product, productName. The difference is that the count of purchases is now an argument of the sparkline()function.

Search Pivot Reports Alerts Dashboards Search & Reporting

Q New Search Save As ▾ Close

```
sourcetype=access_* status=200 action=purchase | chart sparkline(count) AS "Purchase Trend" count AS Total by categoryId | rename categoryId AS "Category"
```

All time 🔍

✓ 5,224 events (before 10/13/14 6:13:37.000 PM) Job ▾ II ⏸ ⏹ ⏷ ⏵ ⏴ Smart Mode ▾

Events Patterns Statistics (7) Visualization

20 Per Page ▾ Format ▾ Preview ▾

Category	Purchases Trend	Total
ACCESSORIES		348
ARCADE		493
SHOOTER		245
SIMULATION		246
SPORTS		138
STRATEGY		806
TEE		367

# More Searches and Reports



This search uses the chart command to count the number of purchases, action="purchase", made for each product, productName. The difference is that the count of purchases is now an argument of the sparkline()function.

Search
Pivot
Reports
Alerts
Dashboards
Search & Reporting

New Search
Save As ▾
Close

```
sourcetype=access_* status=200 action=purchase | chart sparkline(count) AS "Purchase Trend" count AS Total by categoryId | rename categoryId AS "Category"
```

All time ▾

✓ 5,224 events (before 10/13/14 6:13:37.000 PM)
Job ▾

Smart Mode ▾

Events
Patterns
Statistics (7)
Visualization

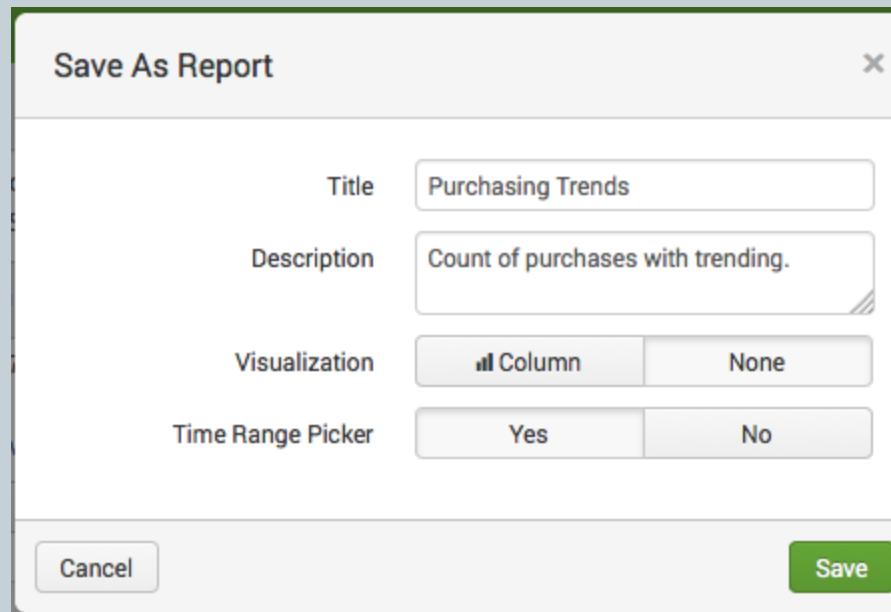
20 Per Page ▾
Format ▾
Preview ▾

Category ▾	Purchases Trend ▾	Total ▾
ACCESSORIES		348
ARCADE		493
SHOOTER		245
SIMULATION		246
SPORTS		138
STRATEGY		806
TEE		367

# More Searches and Reports



3. Click Save As and select Report.



4. In the Save Report As dialog box, enter a Title, "Purchasing trends".
5. (Optional) Enter a Description, "Count of purchases with trending."
6. Click Save and View the report.

# DASHBOARDS



- Dashboards are views that are made up of panels that can contain modules such as search boxes, fields, charts, tables, and lists. Dashboard panels are usually hooked up to saved searches.
- After you create a visualization or report, you can add it to a new or existing dashboard using the Save as report dialog box. You can also use the Dashboard Editor to create dashboards and edit existing dashboards. Using the Dashboard editor is useful when you have a set of saved reports that you want to quickly add to a dashboard.

# DASHBOARDS



- **Change dashboard permissions**
  - You can specify access to a dashboard from the Dashboard Editor. However, your user role (and capabilities defined for that role) might limit the type of access you can define.
  - If your Splunk user role is admin (with the default set of capabilities), then you can create dashboards that are private, visible in a specific app, or visible in all apps. You can also provide access to other Splunk user roles, such as user, admin, and other roles with specific capabilities.
  
- **Change dashboard panel visualizations**
  - After you create a panel with the Dashboard Editor, use the Visualization Editor to change the visualization type in the panel, and to determine how that visualization displays and behaves. The Visualization Editor lets you choose from visualization types that have their data structure requirements matched by the search that has been specified for the panel.

# DASHBOARDS



**Creating dashboards and dashboard panels**

# DASHBOARDS



- **Save a search as a dashboard panel**

1. Run the following search:

```
sourcetype=access_* status=200 action=purchase | top categoryId
```

Search Pivot Reports Alerts Dashboards Search & Reporting

### New Search

Save As ▾ Close

All time

✓ 5,224 events (before 10/15/14 12:35:22.000 PM) Job ▾ II ⌂ ⌄ ⌅ Smart Mode ▾

Events Patterns Statistics (7) Visualization

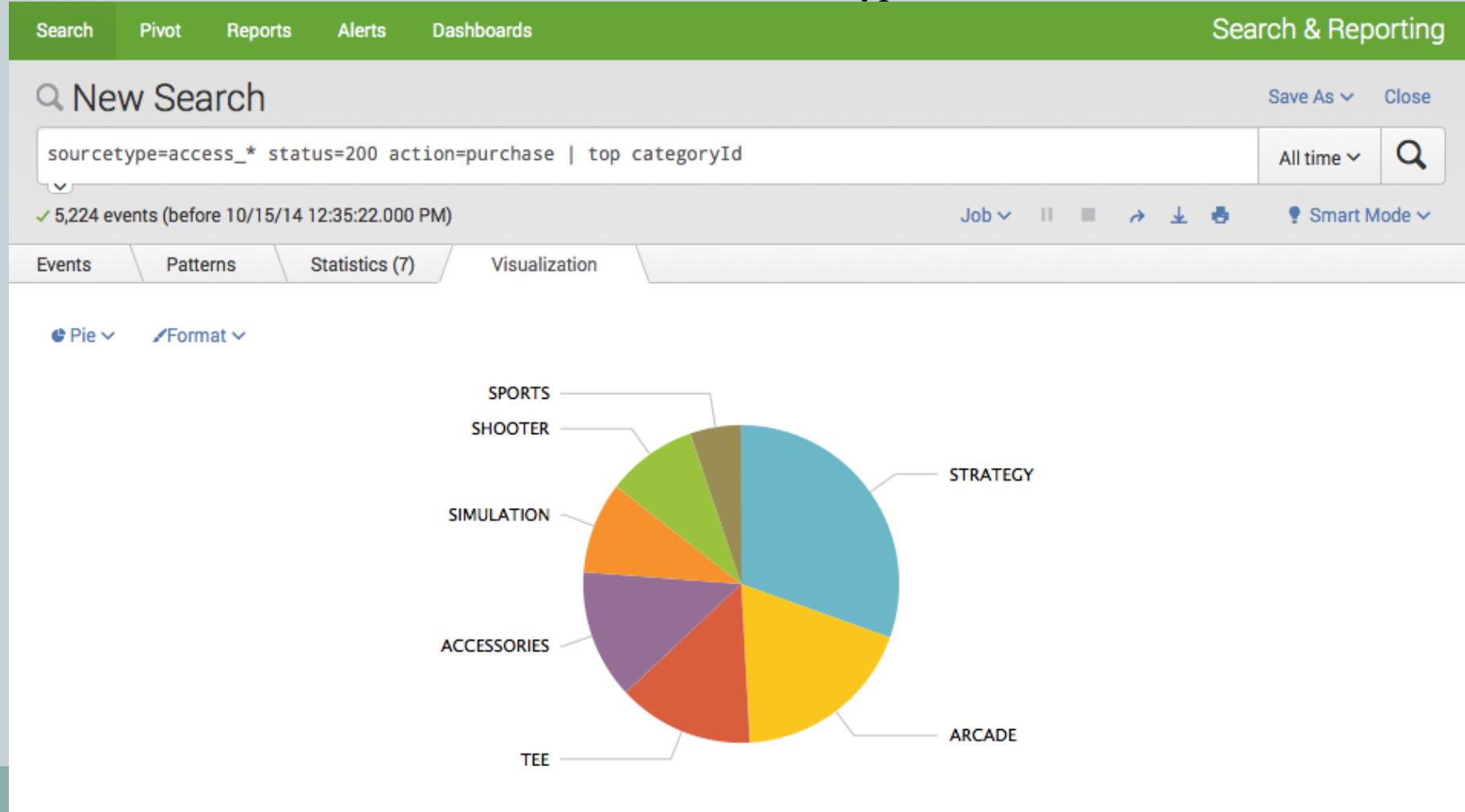
20 Per Page ▾ Format ▾ Preview ▾

categoryId	count	percent
STRATEGY	806	30.495649
ARCADE	493	18.653046
TEE	367	13.885736
ACCESSORIES	348	13.166856
SIMULATION	246	9.307605
SHOOTER	245	9.269769
SPORTS	138	5.221339

# DASHBOARDS



2. Click the Visualization tab and select the Pie chart type.



# DASHBOARDS



3. In the Search view, click Save as and select Dashboard Panel.

Searched: sourcetype=access\_\* status=200 action=purchase | top categoryId

5,224 events (before 10/15/14 12:35:22.000 PM)

Events Patterns Statistics (7) Visualization

Pie Format

Save As ▾ Close

- Report
- Dashboard Panel**
- Alert
- Event Type

# DASHBOARDS



3. In the Search view, click Save as and select Dashboard Panel.

Search & Reporting

New Search

sourcetype=access\_\* status=200 action=purchase | top categoryId

5,224 events (before 10/15/14 12:35:22.000 PM)

Events Patterns Statistics (7) Visualization

Pie Format

Save As ▾ Close

- Report
- Dashboard Panel**
- Alert
- Event Type

The Save as Dashboard Panel dialog box opens.

# DASHBOARDS



## 4. Define a new dashboard and dashboard panel.

Save As Dashboard Panel ×

Dashboard	<input checked="" type="button"/> New <input type="button"/> Existing
Dashboard Title	Buttercup Games Purchases
Dashboard ID ?	buttercup_games_purchases <small>Can only contain letters, numbers and underscores.</small>
Dashboard Description	Reports on Buttercup Games purchases data.
Dashboard Permissions	<input checked="" type="button"/> Private <input type="button"/> Shared in App
Panel Title	Top Purchases by Category
Panel Powered By	<input type="button"/> <a href="#">Inline Search</a>
Panel Content	<input checked="" type="radio"/> Statistics <input type="radio"/> Pie

Cancel  Save

# DASHBOARDS

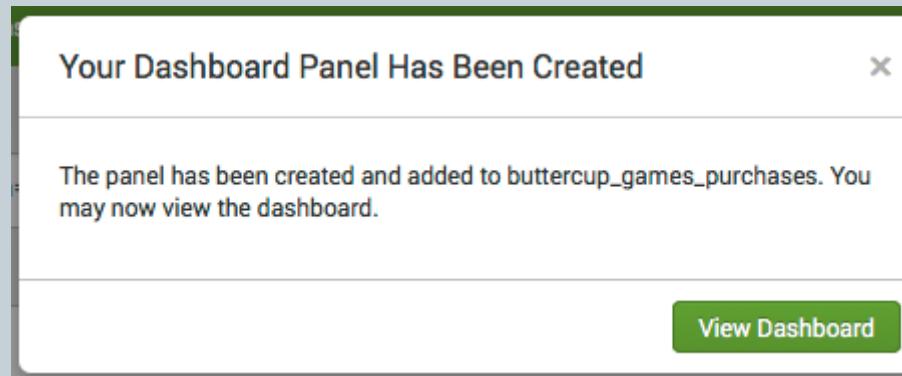


- 4.1. For Dashboard, click New.
- 4.2. Enter the Dashboard Title, "Buttercup Games Purchases", The Dashboard ID updates with "Buttercup\_games\_purchases".
- 4.3. (Optional) Add a Dashboard Description, "Reports on Buttercup Games purchases data".
- 4.4. Type in the Panel Title, "Top Purchases by Category"
- 4.5. Leave the Panel Powered By as Inline search.

# DASHBOARDS



5. Click Save.



# DASHBOARDS



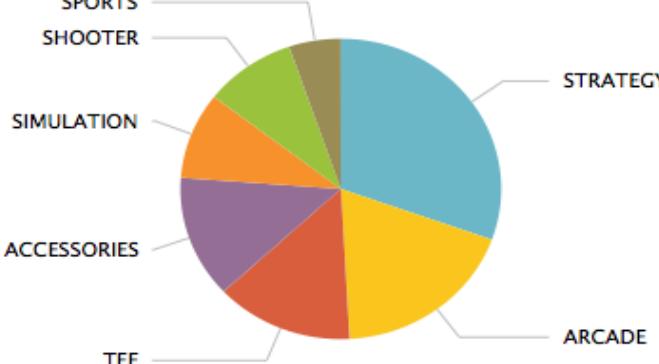
6. Click View Dashboard.

Search Pivot Reports Alerts Dashboards **Search & Reporting**

**Buttercup Games Purchases**  
Reports on Buttercup Games purchases data.

Edit More Info  

**Top Purchases by Category** <1m ago



Category	Percentage
STRATEGY	35%
ARCADE	15%
ACCESSORIES	10%
TEE	8%
SIMULATION	7%
SHOOTER	5%
SPORTS	3%

This creates a dashboard with one report panel. To add more report panels, you can run new searches and save them to this dashboard, or you can add saved reports.

# DASHBOARDS



- View and edit dashboard panels

# DASHBOARDS



1. Click Dashboards in the app navigation bar.  
This takes you to the Dashboards listing page.

Search Pivot Reports Alerts Dashboards Search & Reporting

## Dashboards

Dashboards are comprised of multiple reports or inline searches.

Create New Dashboard

1 Dashboards		All	Yours	This App's	filter
i	Title ^				
>	Buttercup Games Purchases			Edit ▾	admin
					search
					Private

You can Create a new dashboard and edit existing dashboards. You see the Buttercup Games Purchases dashboard that you created.

# DASHBOARDS



- Under the i column, click the arrow next to Buttercup Games Purchases to see more information about the dashboard: What app context it is in, whether or not it is scheduled, and its permissions.

Search   Pivot   Reports   Alerts   Dashboards   **Search & Reporting**

## Dashboard

Create New Dashboard

1 Dashboards

All   Yours   This App's   filter

i	Title ^	Actions	Owner ♦	App ♦	Sharing ♦
▼	Buttercup Games Purchases  Reports on Buttercup Games successful purchases data.  App ..... search Schedule ..... Not scheduled. <a href="#">Edit</a> Permissions ..... Private. Owned by admin. <a href="#">Edit</a>	Edit ▾	admin	search	Private

# DASHBOARDS



- Under the i column, click the arrow next to Buttercup Games Purchases to see more information about the dashboard: What app context it is in, whether or not it is scheduled, and its permissions.

Search   Pivot   Reports   Alerts   Dashboards   **Search & Reporting**

## Dashboards

Create New Dashboard

1 Dashboards

All   Yours   This App's   filter

i	Title ^	Actions	Owner ♦	App ♦	Sharing ♦
▼	Buttercup Games Purchases  Reports on Buttercup Games successful purchases data.  App ..... search Schedule ..... Not scheduled. <a href="#">Edit</a> Permissions ..... Private. Owned by admin. <a href="#">Edit</a>	Edit ▾	admin	search	Private

You can use the quick links that are inline with the information to edit the dashboard's Schedule and Permissions.

# DASHBOARDS



- **Add an input to the dashboard**

1. In the Dashboards list, click Buttercup Games Purchases to return to the saved dashboard.
2. Click Edit and select Edit Panels.

Search Pivot Reports Alerts Dashboards Search & Reporting

Buttercup Games Purchases Reports on Buttercup Games purchases data.

Top Purchases by Category

Category	Percentage
SPORTS	35%
ARCADE	15%
TEE	10%
ACCESSORIES	10%
SIMULATION	8%
SHOOTER	5%

Edit ▾ More Info ▾ Download Print <1m ago

Edit Panels

Edit Source XML

Convert to HTML

Edit Title or Description

Edit Permissions

Schedule PDF Delivery

Set as Home Dashboard

Clone

Delete

# DASHBOARDS



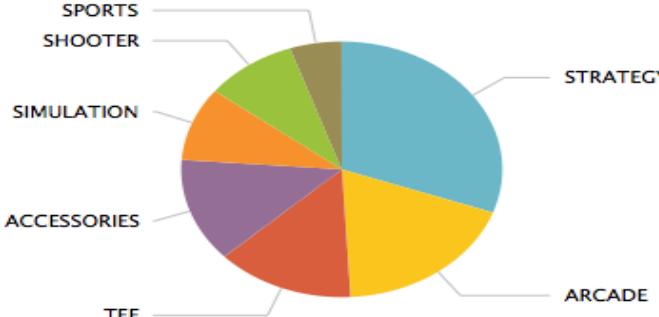
- This changes the view so that edit options appear in the panels and modules on the dashboard.

Search Pivot Reports Alerts Dashboards **Search & Reporting**

Edit: Buttercup Games Purchases + Add Panel + Add Input ↳ Edit Source Done

Untitled

Top Purchases by Category



Category	Percentage
STRATEGY	~35%
ARCADE	~15%
ACCESSORIES	~10%
TEE	~8%
SIMULATION	~6%
SHOOTER	~4%
SPORTS	~3%

🔍 ⚪️ 🖊️

# DASHBOARDS



- 3. Click Add Input and select Time.

Search Pivot Reports Alerts Dashboards **Search & Reporting**

Edit: Buttercup Games Purchases

+ Add Panel + Add Input ▾ ↗ Edit Source Done

Untitled

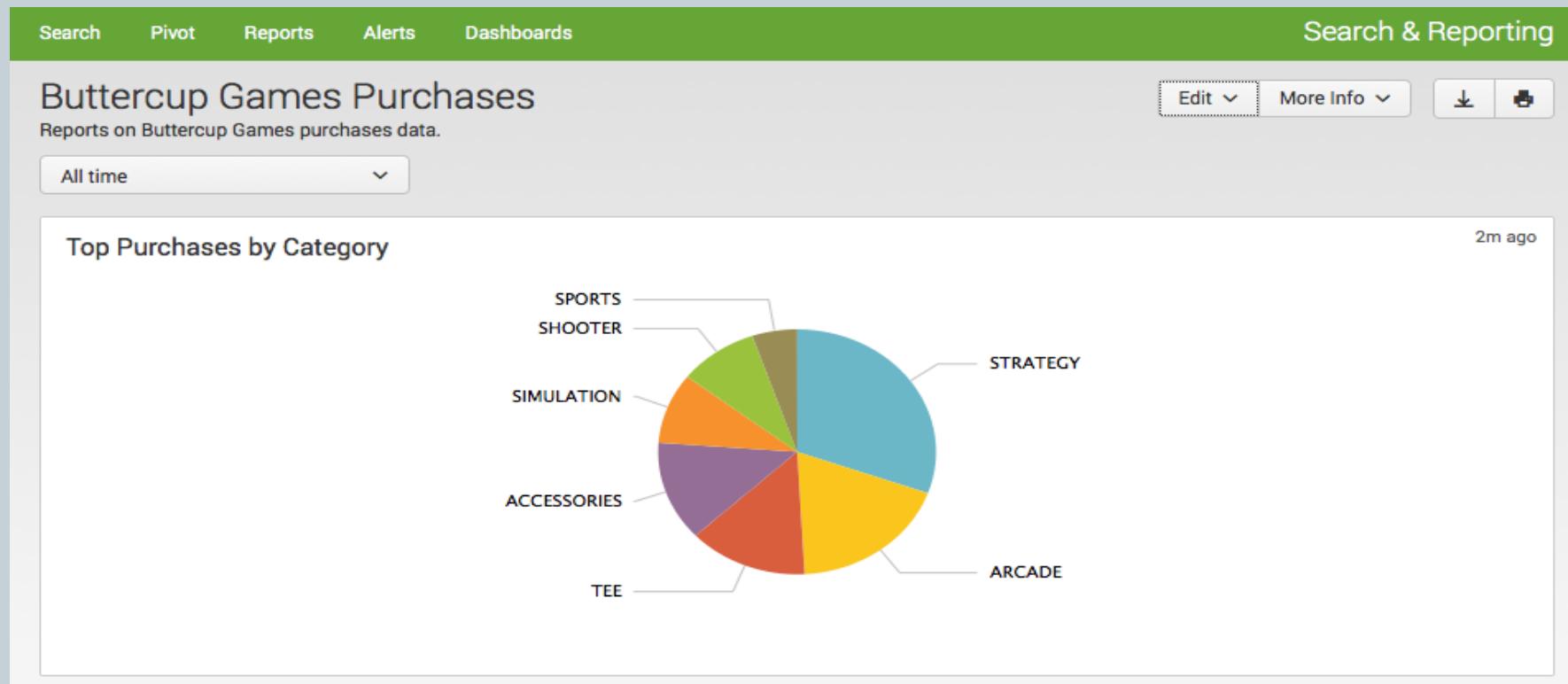
Top Purchases by Category

Category	Percentage
SPORTS	~25%
SHOOTER	~10%
SIMULATION	~10%
ACCESSORIES	~10%
TEE	~10%
ARCADE	~15%
STRATEGY	~20%

T Text  
🕒 Radio  
▼ Dropdown  
☑ Checkbox  
▼ Multiselect  
🕒 Time  
🔍 Submit



- 4. Click Done.



- Now you can use this time range picker to restrict all the inline searches that power the panels to the same time range.

# DASHBOARDS



**Add more panels to the dashboard**

# DASHBOARDS



- Add saved reports to the dashboard
- 1. Return to the Buttercup Games Purchases dashboard.

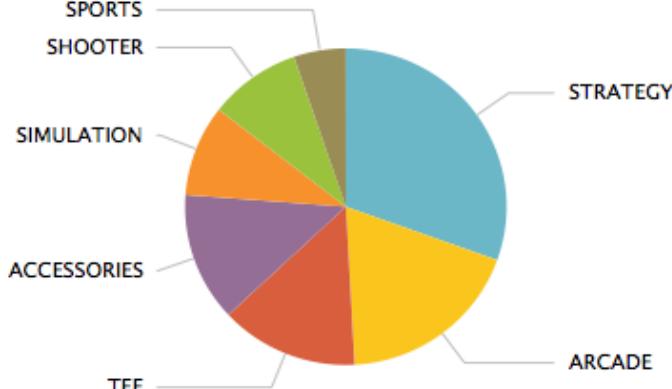
Search Pivot Reports Alerts Dashboards **Search & Reporting**

## Buttercup Games Purchases

Reports on Buttercup Games purchases data.

All time ▼

Top Purchases by Category 2m ago



Category	Percentage
STRATEGY	35%
ARCADE	20%
ACCESSORIES	15%
TEE	10%
SIMULATION	8%
SHOOTER	5%
SPORTS	3%

# DASHBOARDS



- 2. Click Edit and select Edit Panels.

Search Pivot Reports Alerts Dashboards Search & Reporting

## Buttercup Games Purchases

Reports on Buttercup Games purchases data.

Top Purchases by Category

Category	Percentage
SPORTS	35%
ARCADE	15%
TEE	10%
ACCESSORIES	10%
SIMULATION	8%
SHOOTER	7%

Edit ▾ More Info ▾ Download Edit <1m ago

[Edit Panels](#)

---

[Edit Source](#) XML

---

[Convert to HTML](#)

---

[Edit Title or Description](#)

---

[Edit Permissions](#)

---

[Schedule PDF Delivery](#)

---

[Set as Home Dashboard](#)

---

[Clone](#)

---

[Delete](#)

# DASHBOARDS



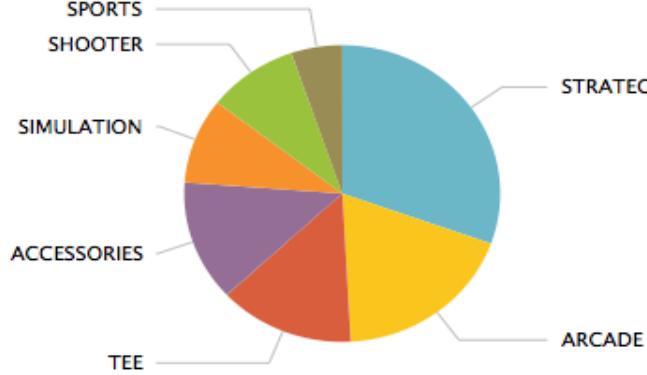
- 3. In the Buttercup Games Purchases dashboard editor, click Add Panel.

Search Pivot Reports Alerts Dashboards **Search & Reporting**

Edit: Buttercup Games Purchases + Add Panel + Add Input ↳ Edit Source Done

Untitled

Top Purchases by Category



Category	Percentage
SPORTS	~25%
STRATEGY	~20%
ARCADE	~15%
TEE	~10%
ACCESSORIES	~8%
SIMULATION	~5%
SHOOTER	~3%

🔍 ⚪️ 🖊️

# DASHBOARDS



- The Add Panel sidebar menu slides opens.

The screenshot shows the Splunk interface for editing a dashboard named "Buttercup Games Purchases". The top navigation bar includes the Splunk logo, the "App: Search & Reporting" dropdown, and user roles like "Administrator", "Messages", and "Settings". Below the navigation is a green header bar with tabs for "Search", "Pivot", "Reports", "Alerts", and "Dashboards", with "Dashboards" being the active tab. The main workspace displays the title "Edit: Buttercup Games Purchases" and a time range selector set to "All time". To the right, a sidebar menu titled "Add Panel" is open, containing a search bar and four options: "New (14)", "New from Report (9)", "Clone from Dashboard (1)", and "Add Prebuilt Panel (0)".

# DASHBOARDS



- 4. To add a new panel from a report, click New from Report.
- This opens the list of saved reports.

Splunk > App: Search & Reporting >

Administrator > Messages > Settings >

Search Pivot Reports Alerts Dashboards

Edit: Buttercup Games Purchases

All time

Untitled

Top Purchases by Category

Add Panel

find...

+ Add Panel

> New (14)

> New from Report (9)

- Comparison of Actions and Conversion Rates
- Errors in the last 24 hours
- Errors in the last hour
- License Usage Data Cube
- Messages by minute last 3 hours
- Product Purchases over Time
- Purchasing Trends
- Splunk errors last 24 hours
- VIP Customer

> Clone from Dashboard (1)

> Add Prebuilt Panel (0)

# DASHBOARDS



- 5. Select Purchasing Trends.
- This opens a preview of the saved Report.

**splunk > App: Search & Reporting**

Search Pivot Reports

Edit: Buttercup Games

All time

Untitled

Top Purchases by Category

Add Panel find... X

- > New (14)
- ▽ New from Report (9)
  - Comparison of Actions and Conversion Rates
  - Errors in the last 24 hours
  - Errors in the last hour
  - License Usage Data Cube
  - Messages by minute last 3 hours
  - Product Purchases over Time
  - Purchasing Trends
  - Splunk errors last 24 hours
  - VIP Customer
- > Clone from Dashboard (1)
- > Add Prebuilt Panel (0)

**Preview**

**Add to Dashboard** X

Creator ..... Created by Search.  
 App ..... search  
 Schedule ..... Not scheduled.  
 Acceleration ..... Disabled.  
 Permissions ..... Private. Owned by admin.  
 Embedding ..... Disabled.  
 Search String ..... sourcetype=access\_\* status=200 action=purchase| chart sparkline(count) AS "Purchases Trend" count AS Total by categoryId | rename categoryId AS "Category"

Category	Purchases Trend	Total
ACCESSORIES		348
ARCADE		493
SHOOTER		245
SIMULATION		246
SPORTS		138
STRATEGY		806
TEE		367

# DASHBOARDS



- 6. Click Add to Dashboard.
- The new panel is placed in the dashboard editor. You can click anywhere to close the Add Panel sidebar menu or choose another report to add to the dashboard.
- 7. Select the report Comparison of Actions and Conversion Rates by Product and add it to the dashboard.

Splunk > App: Search & Reporting

Search Pivot Reports Alerts

Edit: Buttercup Games

All time

Untitled

Top Purchases by Category

Untitled

Add Panel

find...

> New (14)

< New from Report (9)

Comparison of Actions and Conversion Rates by Product

Errors in the last 24 hours

Errors in the last hour

License Usage Data Cube

Messages by minute last 3 hours

Product Purchases over Time

Purchasing Trends

Splunk errors last 24 hours

VIP Customer

> Clone from Dashboard (1)

> Add Prebuilt Panel (0)

Preview

Add to Dashboard

Creator ..... Created by Search.  
App ..... search  
Schedule ..... Not scheduled.  
Acceleration ..... Disabled.  
Permissions ..... Private. Owned by admin.  
Embedding ..... Disabled.  
Search String ..... sourcetype=access\_\* status=200 | stats count AS views  
count(eval(action="addtocart")) AS addtocart  
count(eval(action="purchase")) AS purchases by  
productName | eval viewsToPurchases=  
(purchases/views)\*100 | eval cartToPurchase=  
(purchases/addtocart)\*100 | table productName views  
addtocart purchases viewsToPurchase cartToPurchase  
rename productName AS "Product Name" views AS  
"Views", addtocart as "Adds To Cart", purchases AS  
"Purchases"

Actions

Conversion Rates

Product Name

Views  
Ad...rt  
Pu...s  
vi...se  
ca...se

# DASHBOARDS



- 8. Close the Add Panel sidebar and rearrange the panels on the dashboard.
- While in the dashboard editor, you can drag and drop a panel to rearrange it on the dashboard.

**Edit: Buttercup Games Purchases**

+ Add Panel + Add Input ↗ Edit Source Done

Autorun dashboard

All time

**Untitled**

**Top Purchases by Category**

Category	Purchases
SPORTS	348
SHOOTER	493
SIMULATION	245
ACCESSORIES	246
TEE	138
ARCADE	806

**Untitled**

**Purchasing Trends**

Category	Purchases Trend	Total
ACCESSORIES	Wavy line	348
ARCADE	Wavy line	493
SHOOTER	Wavy line	245
SIMULATION	Wavy line	246
SPORTS	Wavy line	138
STRATEGY	Wavy line	806
TEE	Wavy line	367

**Untitled**

**Comparison of Actions and Conversion Rates by Product**

Product Name	Views	Adds To Cart	Purchases	ViewsToPurchase	CartToPurchase
Benign_ebris	2,584	646	1292	1.938	96
Cutting_2014	1,938	646	1292	1.938	72
Dream_Crusher	1,938	646	1292	1.938	48
Final_Sequel	1,938	646	1292	1.938	48
Fire_Resistance_Suit_of_Provocation	1,938	646	1292	1.938	48
Holy_Blae_of_Couda	1,938	646	1292	1.938	48
Manganillo_Bros.	1,938	646	1292	1.938	48
Mediocre_Kingdoms	1,938	646	1292	1.938	48
Oval_the_Wolverine	1,938	646	1292	1.938	48
Puppies_vs_Zombies	1,938	646	1292	1.938	48
Slim_Cubicle	1,938	646	1292	1.938	48
World_of_Cheese	1,938	646	1292	1.938	48

Actions

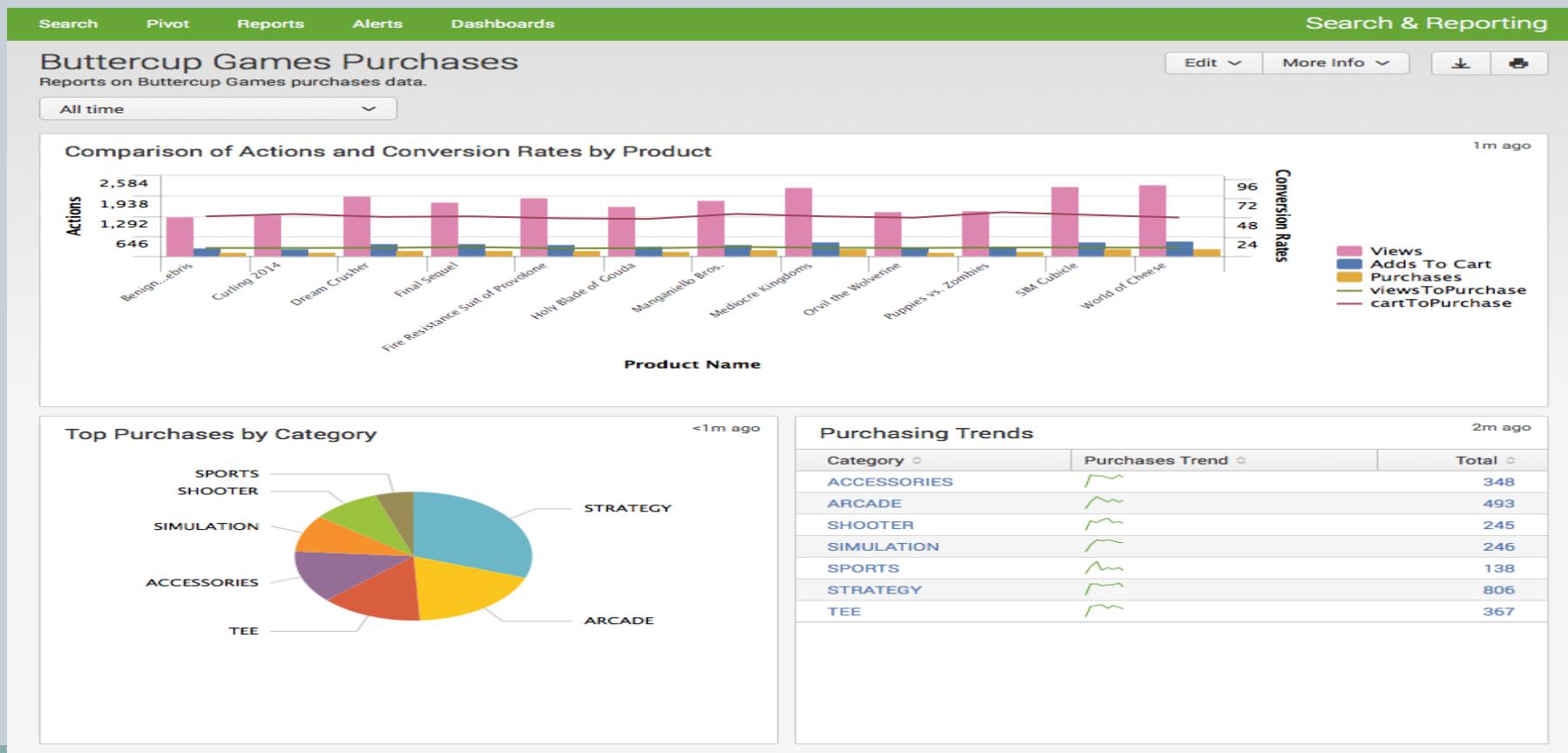
Conversion Rates

Views  
Adds To Cart  
Purchases  
ViewsToPurchase  
CartToPurchase

# DASHBOARDS



- 9. Click Done.
- Your finished dashboard should look like this:



# Deployment



- **Splunk Enterprise and your IT infrastructure**
- Splunk Enterprise indexes data from the servers, applications, databases, network devices, virtual machines, and so on, that make up your IT infrastructure. As long as the machine that generates the data is a part of your network, Splunk Enterprise can collect the data from machines located anywhere, whether it is local (on-the-premises in a server room), remote (off-the-premises in a datacenter), entirely in the cloud, or a hybrid (such as on-premise and in the cloud).
- Most users connect to Splunk Enterprise with a web browser and use Splunk Web to administer their deployment, manage and create knowledge objects, run searches, create pivots and reports, and so on. You can also use the command-line interface to administer your Splunk Enterprise deployment.

# Splunk Enterprise Components



Component	Description
Apps	Apps are a collection of configurations, knowledge objects, and customer designed views and dashboards that extend the Splunk Enterprise environment to fit the specific needs of organizational teams such as Unix or Windows system administrators, network security specialists, website managers, business analysts, and so on. A single Splunk Enterprise Installation can run multiple apps simultaneously.
Forwarder	A forwarder is a Splunk Enterprise Instance that forwards data to another Splunk Enterprise Instance (an Indexer or another forwarder) or to a third-party system.
Indexer	An Indexer is the Splunk Enterprise Instance that indexes data. The Indexer transforms the raw data into events and stores the events into an Index. The Indexer also searches the indexed data in response to search requests.
Receiver	A receiver is a Splunk Enterprise Instance configured to receive data from a forwarder. The receiver is either an Indexer or another forwarder.
Search head	In a distributed search environment, the search head is the Splunk Enterprise Instance that handles search management functions, directing search requests to a set of search peers and then merging the results back to the user. If this instance does only searching and not indexing, it is usually referred to as a dedicated search head.
Search peer	In a distributed search environment, the search peer is the Splunk Enterprise Instance that performs indexing and fulfills search requests originating from the search head.