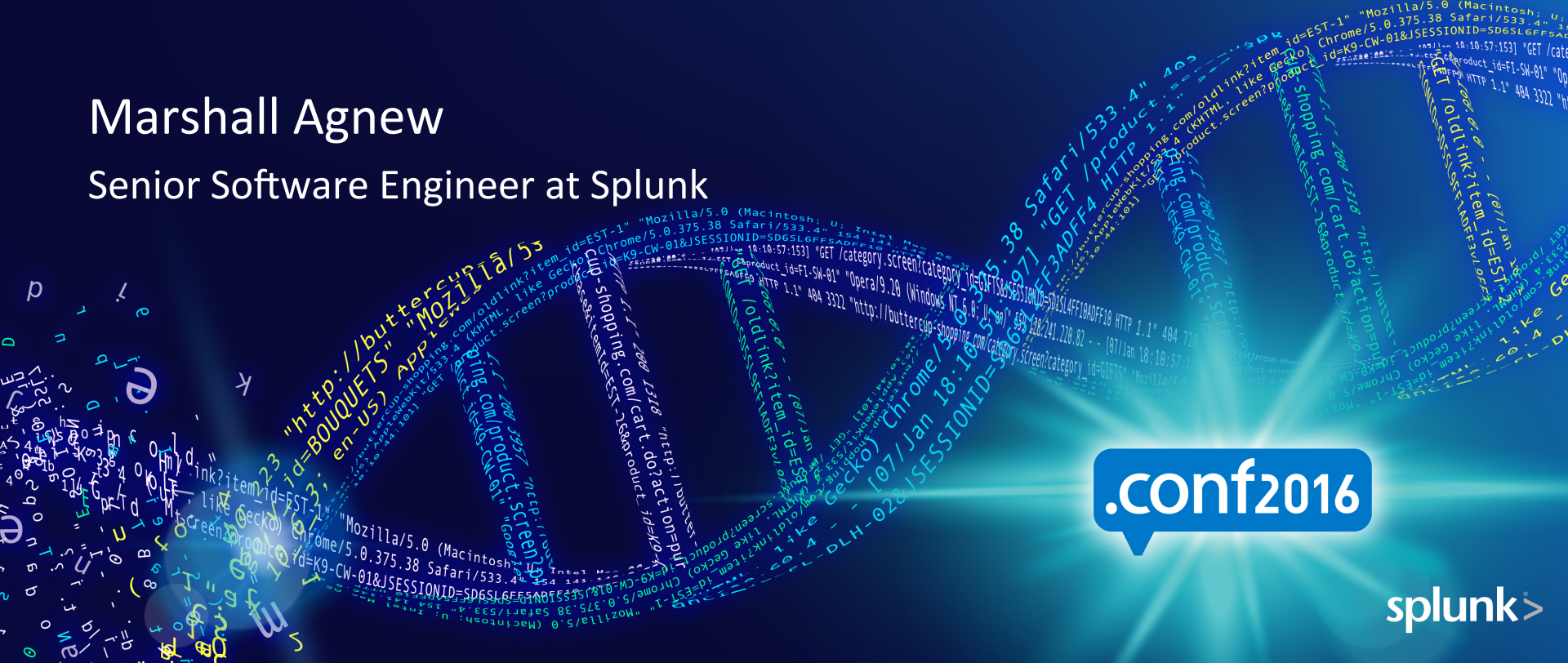
Building Splunk Visualizations with the New Custom Visualization API

Marshall Agnew

Senior Software Engineer at Splunk



Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Agenda

- Why Use Custom Visualizations
- Custom Visualizations in Splunk
- Overview of the API
- Coding Demo
- Learning More

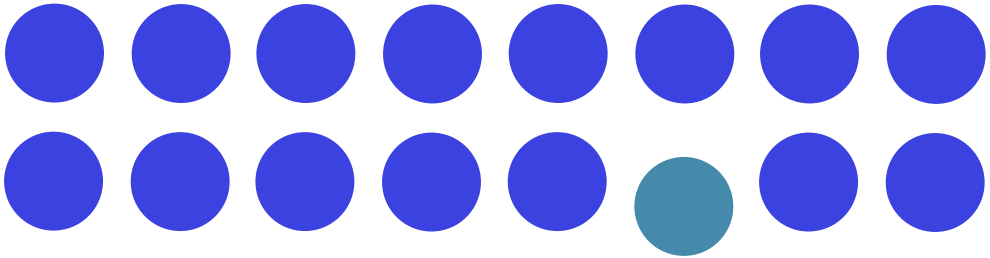
Why Visualization Matters

Splunk excels at understanding machine data

8/18/15 12:02:25.432 PM	127.0.0.1 - admin [18/Aug/2015:12:02:25.432 -0700] "GET /en-US/splunkd/__raw/servicesNS/nobody/search/search/jobs/rt_1439924493. p/search/search?q=search%20index%20%3D%20_internal%20%7C%20stats%20count%20by%20sourcetype%20status&display.page.search.mode=ver stics&display.visualizations.type=charting&display.visualizations.charting.chart=column&sid=rt_1439924493.48" "Mozilla/5.0 (Maci 3.155 Safari/537.36" - ee3dfac895be408cfce2028261452290 3ms bytes = 6758 | host = magnew-mbpr.sv.splunk.com | source = /Users/magnew/dev/build/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access
8/18/15 12:02:24.430 PM	127.0.0.1 - admin [18/Aug/2015:12:02:24.430 -0700] "GET /en-US/splunkd/__raw/servicesNS/nobody/search/search/jobs/rt_1439924493. p/search/search?q=search%20index%20%3D%20_internal%20%7C%20stats%20count%20by%20sourcetype%20status&display.page.search.mode=ver stics&display.visualizations.type=charting&display.visualizations.charting.chart=column&sid=rt_1439924493.48" "Mozilla/5.0 (Maci 3.155 Safari/537.36" - ee3dfac895be408cfce2028261452290 3ms bytes = 6758 | host = magnew-mbpr.sv.splunk.com | source = /Users/magnew/dev/build/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access
8/18/15 12:02:23.446 PM	127.0.0.1 - admin [18/Aug/2015:12:02:23.446 -0700] "GET /en-US/splunkd/__raw/services/search/jobs/rt_1439924493.48/timeline?offs ch/search?q=search%20index%20%3D%20_internal%20%7C%20stats%20count%20by%20sourcetype%20status&display.page.search.mode=verbose&e s&display.visualizations.type=charting&display.visualizations.charting.chart=column&sid=rt_1439924493.48" "Mozilla/5.0 (Macintos Safari/537.36" - ee3dfac895be408cfce2028261452290 3ms bytes = 841 | host = magnew-mbpr.sv.splunk.com | source = /Users/magnew/dev/build/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access | s
8/18/15 12:02:23.445 PM	127.0.0.1 - admin [18/Aug/2015:12:02:23.445 -0700] "GET /en-US/splunkd/__raw/servicesNS/nobody/search/search/jobs/rt_1439924493. t=host%2Csource%2Csourcetype%2Clog_level%2Cgroup%2Ctimeendpos%2Ctimestartpos%2Ccpu_seconds%2Cbytes%2Cstatus%2Cspent%2C_raw%2C_ti splunk_server&truncation_mode=abstract&_=1439923988797 HTTP/1.1" 200 185959 "http://localhost:8000/en-US/app/search/search?q=sea y.page.search.mode=verbose&earliest=rt-5m&latest=rt&display.page.search.tab=events&display.general.type=statistics&display.visua 3.48" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2403.155 Safari/537.36

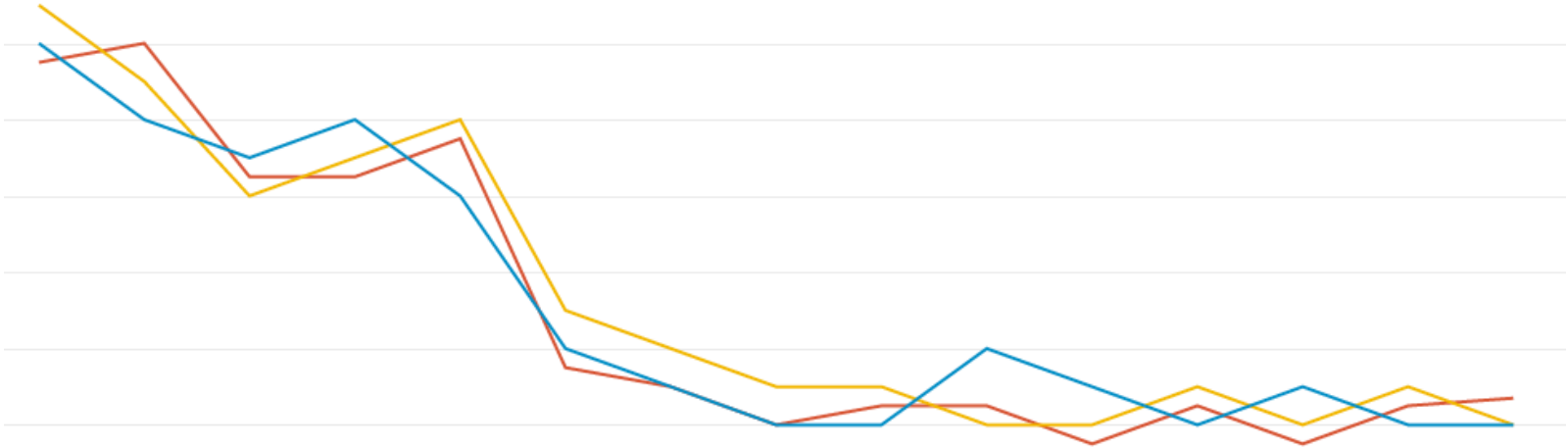
Why Visualization Matters

Humans are excellent at seeing visual patterns



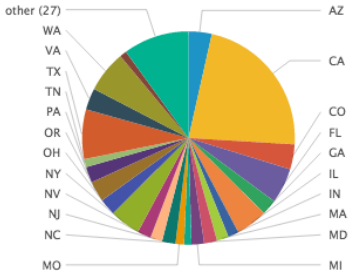
Why Visualization Matters

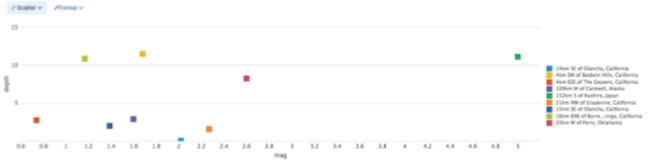
Visualization bridges the gap

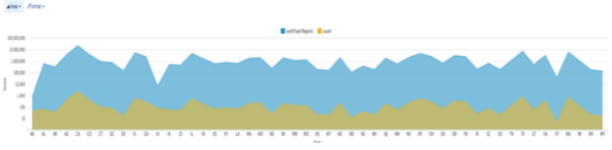


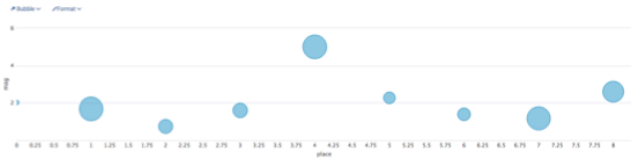
Built-In Visualizations

Splunk has built-in visualizations for many of the most common data types and tasks



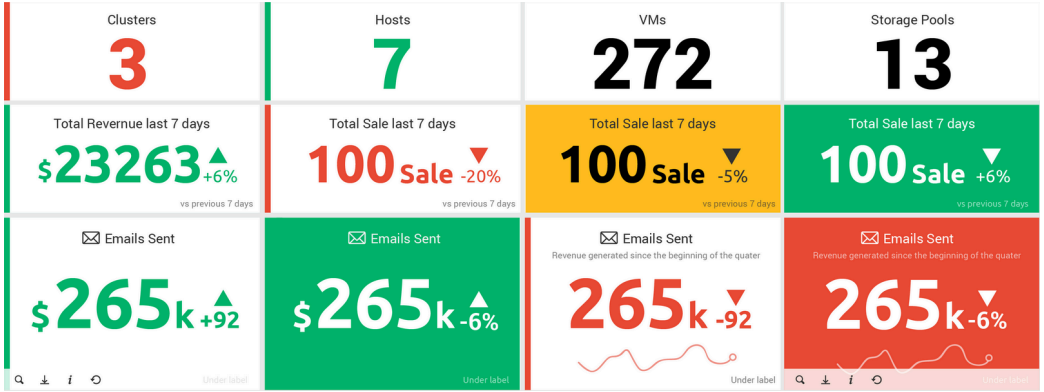


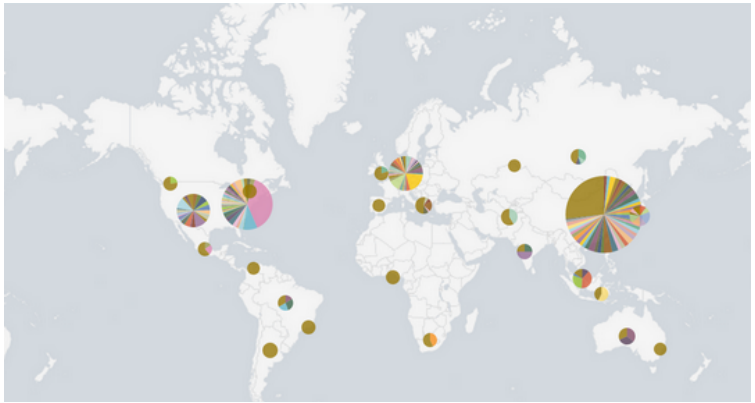


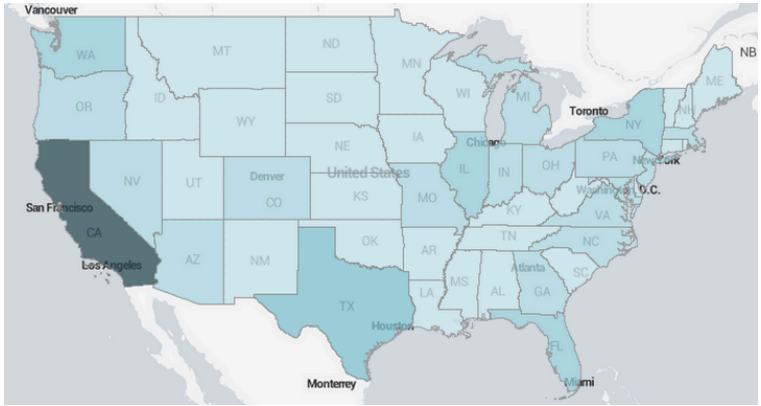


Built-In Visualizations

Splunk has built-in visualizations for many of the most common data types and tasks

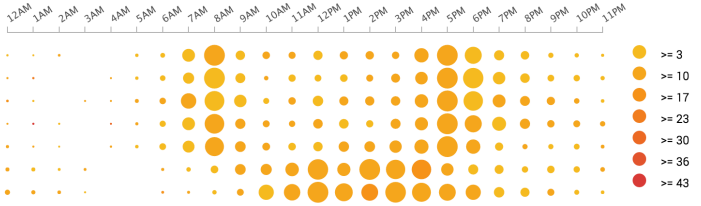


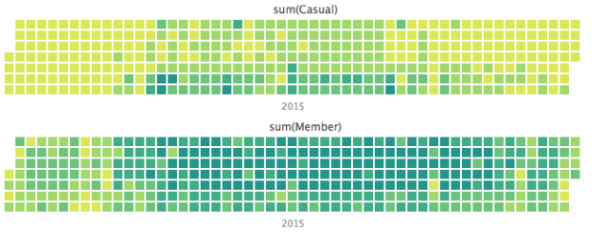


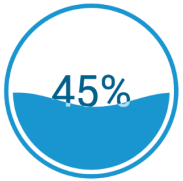


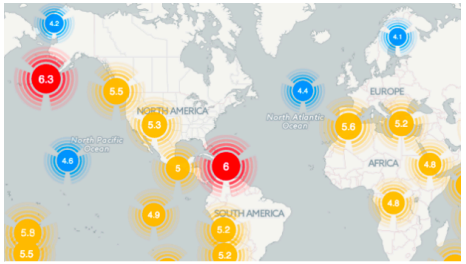
Custom Visualizations

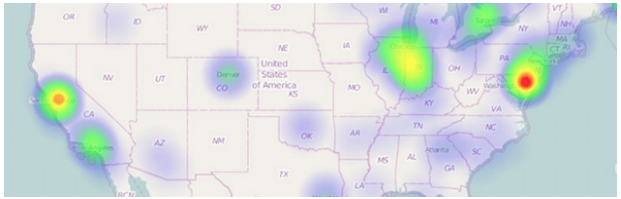
The visualization framework makes it possible for Splunk users to bring in any visualization they want

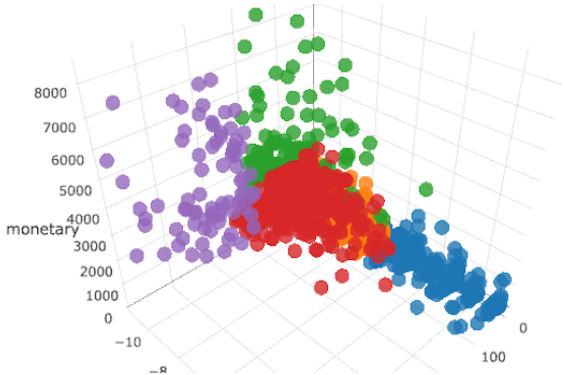


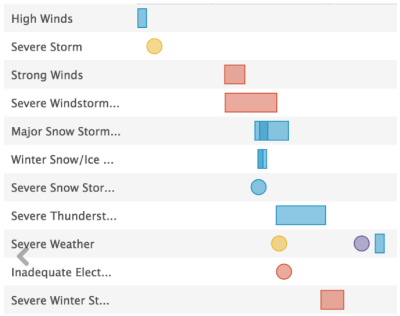












Quick Demo

Splunk Supported Visualizations

We built a set of supported visualizations to both address some of the top requests, and to serve as samples for developers

- Sankey Diagram
- Treemap
- Timeline
- Punchcard
- Calendar Heatmap
- Horseshoe Meter
- Status Indicator
- Horizon Chart
- Location tracker
- Parallel Coordinates
- Bullet Chart

But that is just the tip of the iceberg—the real power is the API

Custom Visualizations in Splunk

- Packaged in apps
- Available across Splunk (Search, dashboards, reports, other apps)
- Permissioned like all Splunk knowledge objects
- Can be found and installed from the Splunk UI
- Implemented in JavaScript using any framework a developer wants

A Custom Visualization App

appname
  appserver
    static
      visualizations
        <visualization_name>
          visualization.js
          visualization.css
          formatter.html
default
    visualizations.conf

JavaScript

- SplunkVisualizationBase
  - Main entrypoint for logic and rendering
  - Extend in visualization.js
  - Override data handling and rendering methods
- SplunkVisualizationUtils
  - Utilities for color schemes, timezone handling, boolean normalization, and security best-practices

formatter.html

- Contains html for the viz editor dialog
- Property values get picked up and passed to JavaScript
- Supports Splunk-style form elements as webcomponents
- Also supports html inputs

visualization.css

- Contains css rules for the visualization

visualizations.conf

- System-wide configuration for the visualizations
  - User-facing labels
  - User help strings
  - Default height
  - Selectability
- Can declare multiple vizes per app

Webpack

- We strongly suggest using webpack to build visualizations into a contained package

A Custom Visualization App with Webpack

```
appname
  appserver
    static
      visualizations
        <visualization_name>
          src
            visualization_source.js
          webpack.config.js
          visualization.js
          visualization.css
          formatter.html
          package.json
  default
    visualizations.conf
```

Coding Demo

Learning More

Related breakout sessions and activities…

- **What's New – Custom Visualizations:** Michael Porath
- **Dashboards, Alerting, Reporting and Visualization - What's New:** Michael Porath and Nicholas Filippi
- **STEP up your app development game:** Tedd Hellmann and David Poncelow
- **Dashboard Wizardry:** Siegfried Puchbauer and Nicholas Filippi
- **Faster Splunk App Certification with Splunk AppInspect:** Grigori Melnik and Andrew Nortrup
- **Best Practices for Developing Splunk Apps and Add-ons:** Jason Conger
- **Visualization and dashboard clinics and booths on the show floor**

Learning More

Online Resources

- Custom Visualization Overview
- Step-by-Step Tutorial
- API Reference
- Examples on SplunkBase
- Code From this Talk

THANK YOU

splunk>