End-to-End Monitoring Unified Performance Dashboard (UPD)

Calvin Smith
Project Solution Architect
Rich Galloway
Systems Integration Engineer
Michael Rodriguez
Splunk Analytics Engineer
Karen Wilson
Program Manager
Northrop Grumman Information Systems (NGIS)

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.

About Northrop Grumman

- Global provider of advanced solutions that deliver timely, enabling information to where it is needed most for our military, intelligence, civilian, state and local, and commercial customers.
- **NGIS Vision/Mission**: Trusted partner of mission-enabling information systems for the security and well-being of our nation and allies.
- 16,000+ Employees, 50 states, 21 countries
- Headquarters in McLean, VA

About Us

The End-to-End Monitoring team supports federal, state and local government programs, specializing in cyber and performance monitoring.

- Cal - 25 years in networking & monitoring, 5 years as cyber strategist and technologist; avid music collector, internet tech enthusiast and road warrior

- Rich – 27 years in fault-tolerant, high-volume computing; 3 years in continuous and end-to-end monitoring. 20-year Habitat for Humanity volunteer

- Michael – 8 years in .com engineering and advanced analytics; 4 years in continuous and end-to-end monitoring. Supporter of Central Texas Dachshund Rescue and member of Extra Life, an organization that raises money through gaming for Dell Children's Medical Center of Texas

IT Challenges

Complex IT Environment

- State-wide agency
- Large state-wide application, millions of transactions per day
- 11 Regions
- 1,100 Field sites
- Tens of thousands of users: case workers, CBOs and citizens
- Thousands of servers, network and infrastructure devices

Data Difficulties

- Many disparate data sources, highly complex network environment
- Siloed information
- Hard to aggregate and correlate information in real time

Availability Issues

- Impacts productivity within agency
- Disrupts delivery of public-facing citizen services

Concept of Operations

Design and Integrate into existing data management platform

- Splunk central event and log data aggregation point

Integrate and Interoperate

- Current legacy application, network, infrastructure monitoring and systems management tools

Implement real-time dashboards for 3 key stakeholder groups

- Executives – Business insight on citizen service delivery, customer activity
- Operations – Real-time KPI tracking with dynamic trending & prediction
- Technical – Device detail of endpoints, network, application & data center

3 Dashboards, each with 3 levels, 9 integrated dashboards total

UPD by the Numbers # 1

Texas State Application

- 5M Transactions per day
- 165M Transactions per month
- .95 sec Transaction rate (avg)
- 5K Concurrent Users
- 20K Total Users

Texas State Network

- 11 Regions
- 262 Cities
- 1,100 Field Sites
- 3 Dot Com Sites
- 815 Network Devices
- 1388 Network Device Interfaces
- 100 Servers
- 50+ Database Instances
- 15TB Data mart

UPD by the Numbers # 2

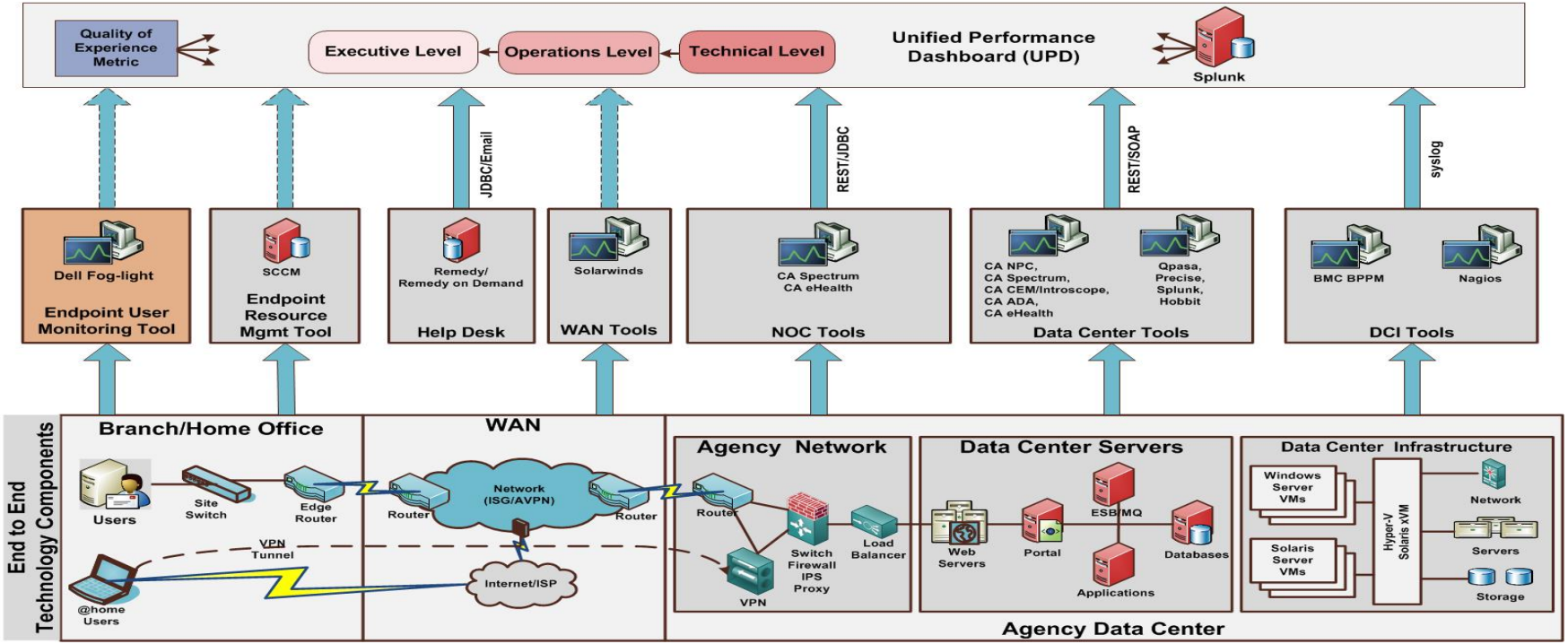
System Operation

- 43 Identified KPIs
- 110 UPD Metrics
- 12 Integrated Performance Monitoring Tools
- 4 Planned by end of year
- 24 Operating Scripts
- Data Integration APIs: SOAP: 4, REST: 1, DB Connect: 3, UF: 3, Email: 1
- 110 Splunk Searches
- 9 Integrated dashboards
- 5-17 Minute dashboard refresh rates
- 850M Data indexed daily

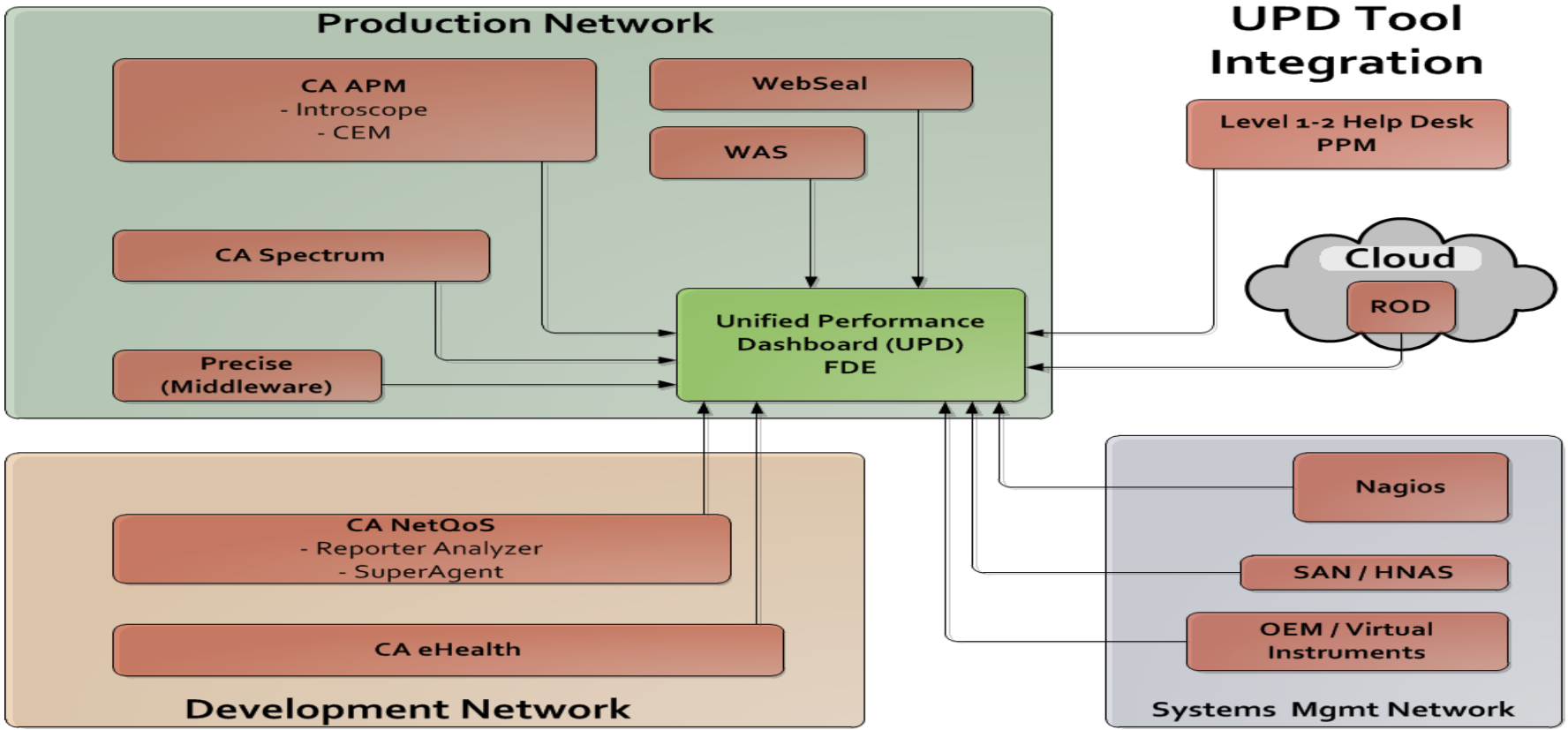
System Delivery

- Requirements Analysis: 90 Days
- System Design: 60 Days:
- Data Management: 30 Days
- System Development: 270 Days
- Total: 15 Months
- Agile development, weekly customer reviews

High Level Architecture



Tool Integration Architecture



UPD Ninja Weapons

Advanced Visual Analytics

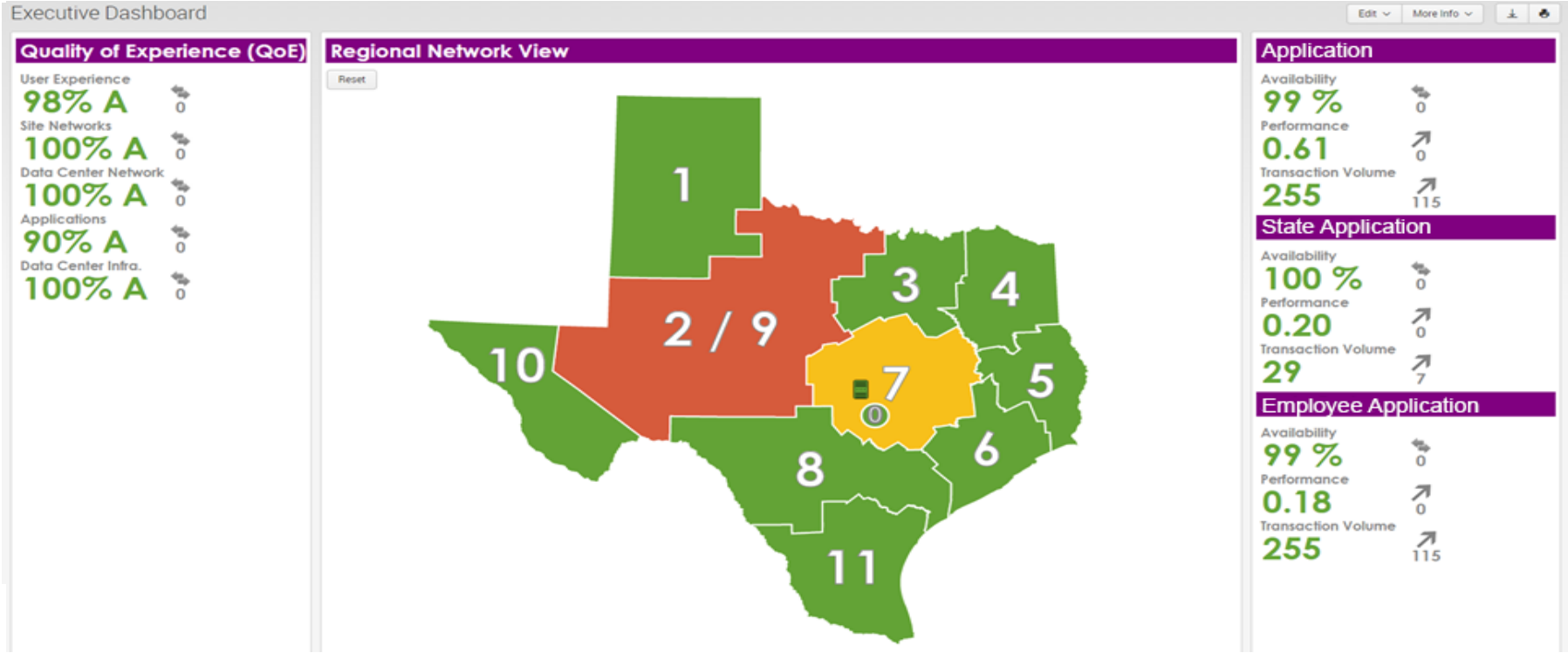
- **Acceptable Performance Range (APR)** – A chart based display of DCC based on our predictive analytics minute per minute
- **Enhanced Mapping** – Using real time data paired with predictive analytics we are able to display exact locations with unique critical metrics
- **Dynamic Color Coding (DCC)** – Display scheme of green, yellow and red based on predictive analytics
- **Interactive Calendar** – Clickable calendar with metric totals per day paired with critical daily metrics
- **Key Performance Indicator (KPI) with Trending** – A real time metric with DCC paired with a display comparing the current bucket of time to the previous per metric

Predictive Analytics

- Combination of a real time metrics, time, historical baselines, local and seasonal level values, and different confidence interval parameters minute per minute uniquely 24/7 builds our predictive models for each of our metrics continuously

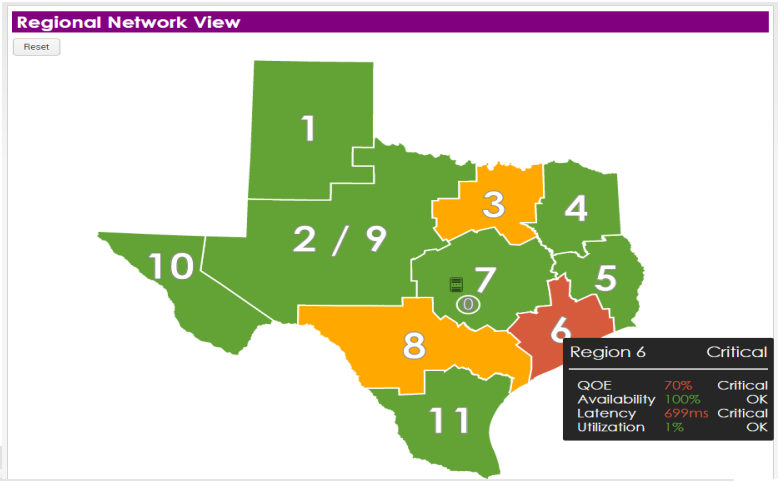
Executive Performance Dashboard

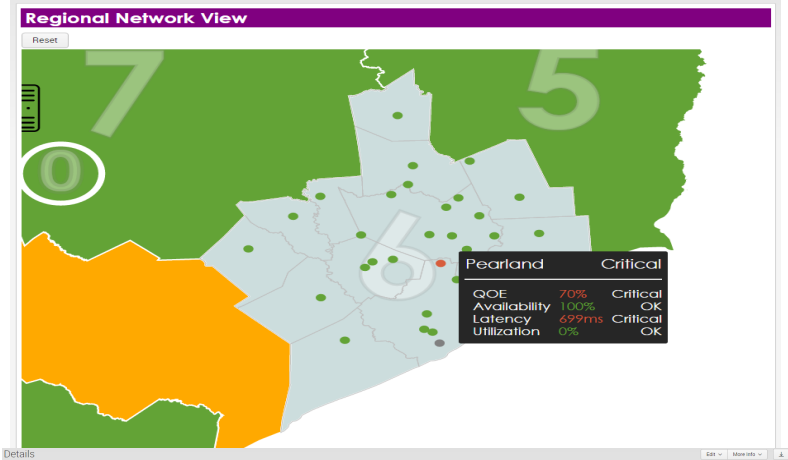
KPI w/ Trending, Enhanced Mapping, DCC

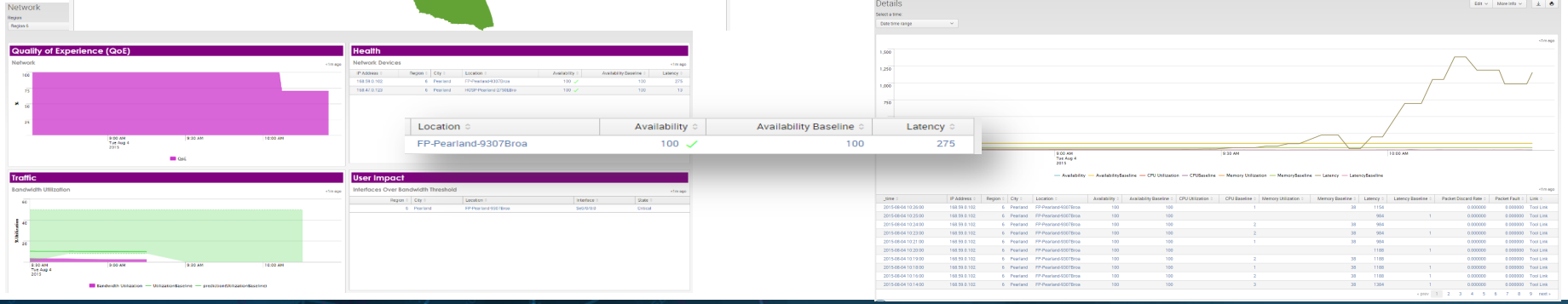


Enhanced Mapping

Region, City, Location, Device

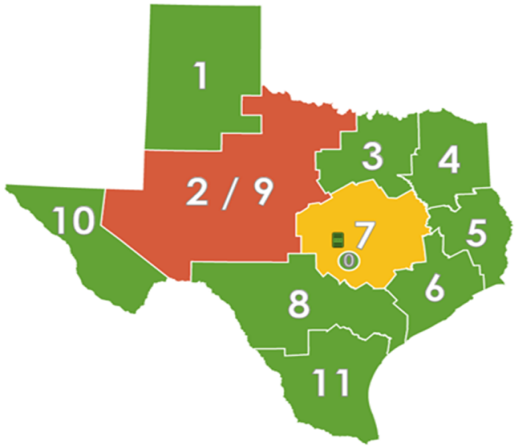






Enhanced Mapping

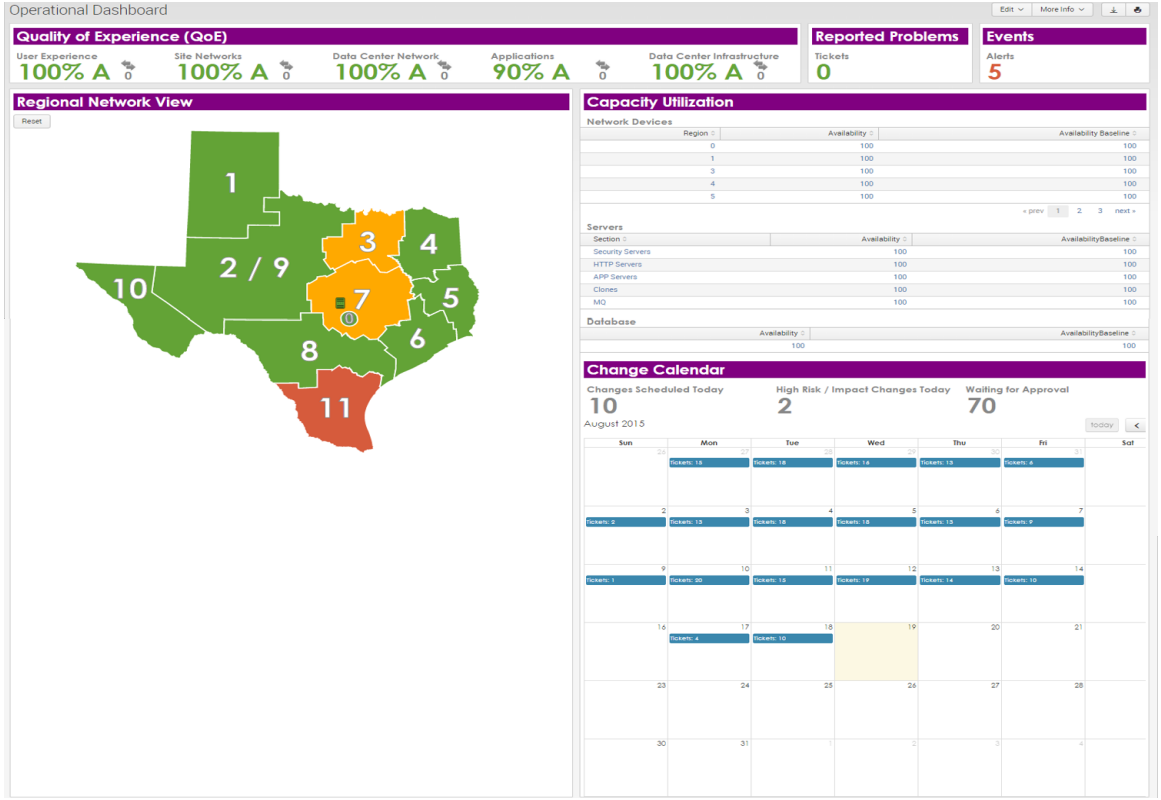
- Texas counties and agency regions called for a custom map
- Mashup of US Census, Texas agency data
- Implemented using D3, JavaScript, CSS, Simple XML



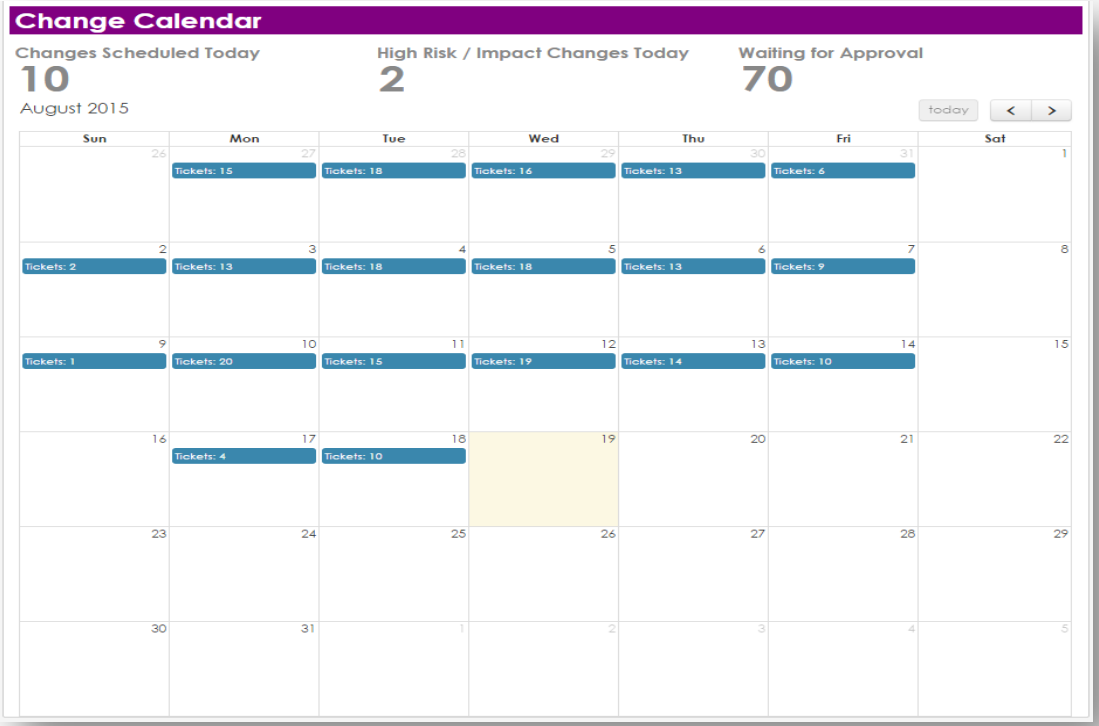

```
<panel>
  <html>
    <div style="background-color:Purple">
    <h1 style="font-size:24px; color:white; padding-left: 5px">Regional Network View
      </h1>
    </div>

        <div id="mapSearch"
             class="splunk-manager"
             data-require="splunkjs/mvc/savedsearchmanager"
             data-options='{
                 "searchname" : "Texas Map",
                 "cancelOnUnload" : true,
                 "preview" : true
             }'>
        </div>

         <div id="map"
             class="splunk-view"
             data-require="app/UPD/texas-map"
             data-options='{
                "managerid" : "mapSearch",
                "tooltip_table_fields" : [ "QOE", "Availability", "Latency", "Utilization" ],
                "tooltip_title_field" : "id",
                "city_drilldown" : "OpsNetwork?form.Region=$Region$&amp;form.City=$City$",
                "city_drilldown_target" : "_blank"

             }'>
        </div>
    </html>
```

Operations Performance Dashboard

KPI w/ Trending, Enhanced Mapping, DCC, Interactive Calendar



Interactive Calendar



FullCalendar

- Open source JavaScript
- Standard Splunk Search
- Simple XML Dashboard Code

Download code at fullcalendar.io

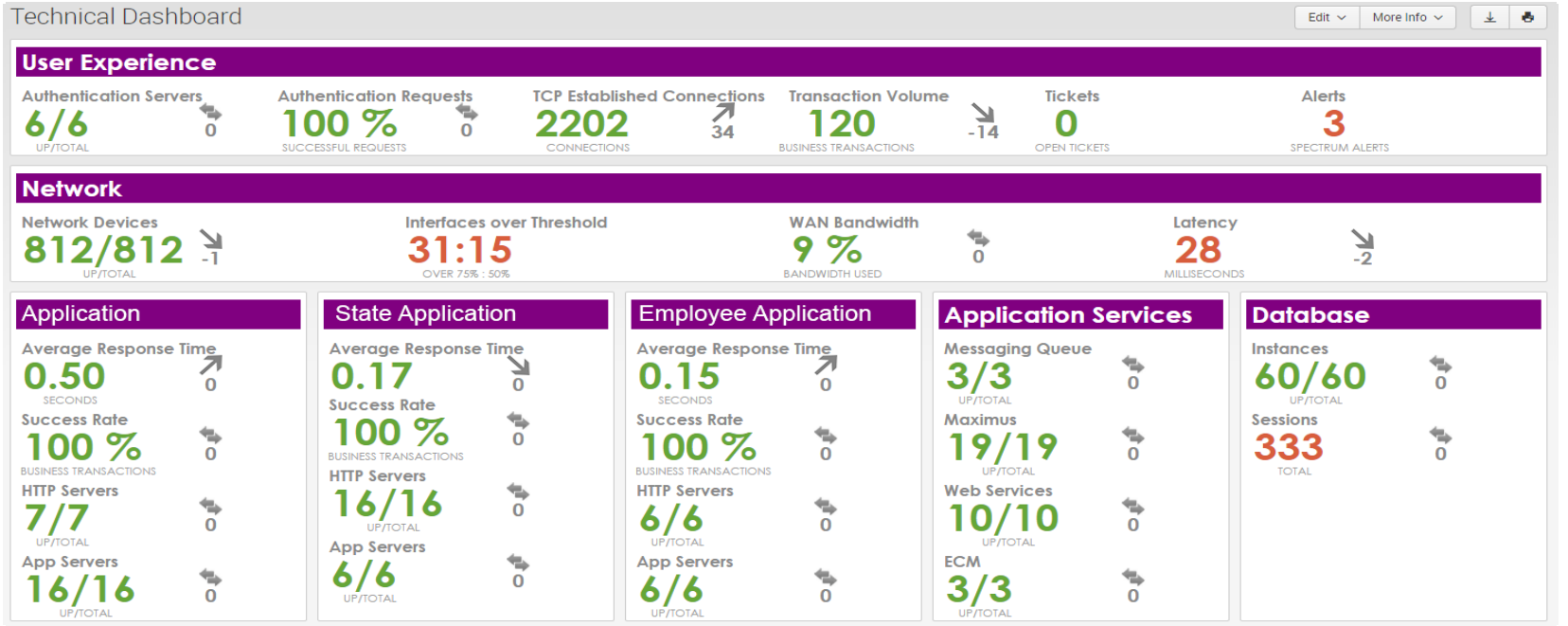
```
</single>
<html>
      <div id="calSearch"
      class="splunk-manager"
      data-require="splunkjs/mvc/searchmanager"
      data-options='{
            "search" :
"index=upd_summary source=\"Change Tickets Index\" earliest=-30d@d latest=+30d@d
| dedup \"Change ID\"
| search \"Approval Status\"=Approved Status!=Pending Status!=Cancelled
| bucket _time span=1d
| stats count AS Tickets by _time
| convert timeformat=\"%m/%d/%Y\" ctime(_time) AS date
| stats count by date Tickets",
                  "cancelOnUnload" : true,
                  "preview" : true
                }
      '>
      </div>

       <div
          id="eventCalendar"
          class="splunk-view"
          data-require="app/CalendarExample/components/eventcalendar/eventcalendar"
          data-options='{
          "managerid": "calSearch",
          "valueField": "Tickets",
          "dateField": "date",
          "linkUrl": "/app/UPD/OpsCalendar",
          "destFormField": "date"
```

Interactive Calendar

- Remedy On Demand (cloud) sends daily CSV as email attachment
- Scripted input uses Office365 REST API to read the attachment
- Splunk indexes scripted input into correct sourcetype/fields
- Sourcetype/fields are connected to automatic lookup tables
- JS and CSS files were updated to match our field names and “look and feel”
- A standard Splunk search is created and put into the simple xml
- Calendar click sends user to a Level 2 Change Calendar dashboard

Technical Performance Dashboard

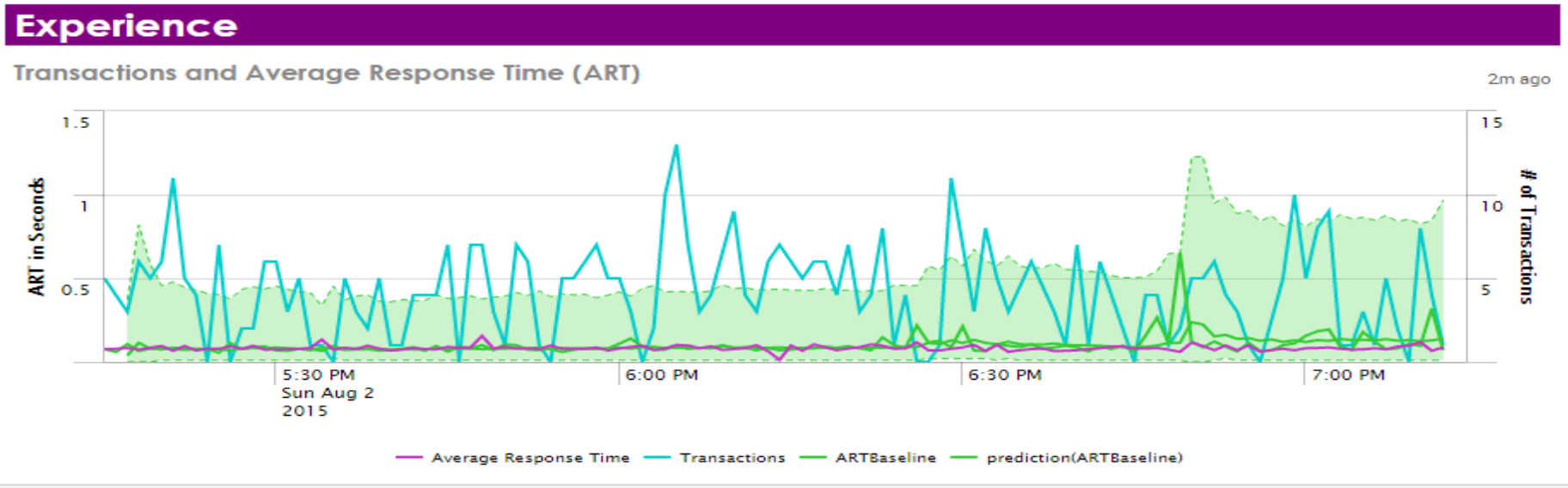
KPI w/ Trending, DCC



Ninja Skills for Tool Integration

- Mostly scripted inputs
  - SOAP and REST queries
  - XML responses parsed and fields extracted by the script
  - Reduces indexed data by 50% saving customer licensing costs
- Email input
  - Office 365 has a very comprehensive REST interface
  - Can read messages and attachments
  - Script decodes CSV attachment and passes to indexer

Acceptable Performance Range (APR)



- Based on our predictive analytics minute per minute.
- No static or predefined thresholds.
- A secondary metric can be added for context.

Primary Metric
Primary Metric Baseline
Primary Metric APR
Secondary Metric

Lessons Learned & Future Events

Use separate apps for UI / inputs

- Easier updates
- UI app only on search heads; input scripts only on indexers

Don't be afraid to DIY

- Sometimes there isn't an app for that
- Scripted inputs can filter and format data

UI Design Considerations

- Design for multiple platforms (Mobile, TV, Desktop)
- Simple, clean, and flat design will make you stand out in a crowd
- Get continuous customer input throughout design and development process

What's Next…

- Integrate additional network, infrastructure and system management tools
- Extend dashboard to monitor other development environments
- Build Cyber Dashboard for Data Center

Points of Contact

Karen Wilson
Program Manager
Email: karen.wilson@ngc.com

Calvin Smith
Solution Architect & Project Lead
Email: ch.smith@ngc.com

Rich Galloway
Systems Engineer, Splunk Integrator
Email: richard.galloway@ngc.com

Michael Rodriguez
Systems Engineer, Splunk Analytics and Design
Email: michael.rodriguez@ngc.com

Questions?

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

THANK YOU

splunk>