Cloud Supersession

Praveen Rangnath

Sr. Director of Cloud Product Mktg, Splunk

Gary Mikula

Sr. Director of Information Security, FINRA

Andrew Linn

SVP, CISO, Orrstown Bank

Joe Hardstaff

Business Systems Architect, Gatwick Airport

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

- Splunk Cloud Overview
- Customer Use Cases
  - **FINRA:** AWS Cost Management
  - **Orrstown Bank:** Debit Card Fraud
  - **Gatwick Airport:** Business Analytics and Aircraft Turnaround Time
- Splunk Cloud – What's Next
- Conclusion

Cloud Portfolio

SaaS

splunk>cloud

Software

splunk>enterprise

Hunk

Apps

- App for AWS
- App for ServiceNow
- App for Salesforce
- More SaaS apps…

GEICO · RoyalCaribbean INTERNATIONAL · Adobe · Coca-Cola · AUTODESK. · SolarCity

Splunk Cloud Value Drivers

Instant

Secure

Reliable

100% Uptime

Hybrid

Thought Experiment

If CPU utilization reaches x%, trigger an alert

Thought Experiment

Raise your hand if x is between 50% - 100%

Thought Experiment

Raise your hand if x is between 10% - 30%

FINRA

splunk>

Who We Are

- FINRA—the Financial Industry Regulatory Authority— is an independent, non-governmental regulator for all securities firms doing business with the public in the United States
- FINRA protects investors by regulating brokers and brokerage firms and by monitoring trading on U.S. stock markets
- FINRA monitor over 6 billion shares traded on the stock market each day
- FINRA handles more 'Big Data' on a daily basis than the Library of Congress or Visa®—to build a holistic picture of the trading market
- FINRA – Deter, Detect, Discipline

Investor Protection

Historical View

- **Cyclic Processes**
  - POC – Budget Approval – SDLC - Maintenance
- **Defined Roles**
  - Coders Code
  - Managers Manage
  - Administrators Administer
- **Agile Development/Cloud Computing**
  - Developers Make These Decisions:
    - Security
    - Financial
    - Architecture
  - And It's All Point and Click
- **Hacking Redefined Security**
  - Defensive Coding
  - Baked In, Not Painted On

"You guys start coding, I'll go find out what the users want."

Same Challenges/Different Environment

- **Security**
  - Engaged All Necessary AWS Security Features
  - Are we Firewalled Correctly
- **Compliance**
  - Followed All Published Standards
- **Networking**
  - Placed Servers on the Correct Network
- **Finance**
  - Stayed within Budget
- **Capacity Planning**
  - Used Resources Optimally
- **But, Now in a Decentralized Model**
  - It's déjà vu all over again…*Yogi Berra*

"With great power comes great responsibility."

Project Cost Management in AWS

Harnessing the Power of Splunk

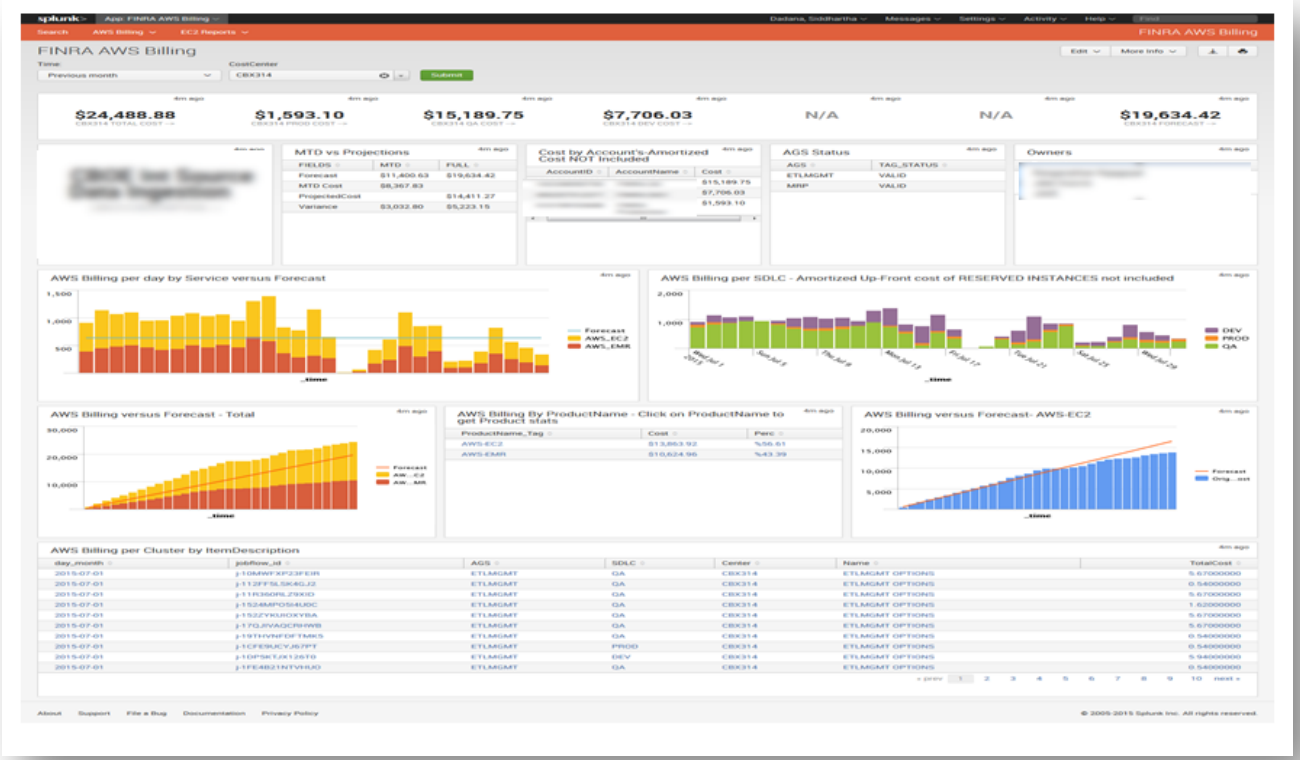
Where We Were

- **Traditional Financial Review Cycles Too Long**
  - Quarterly Reviews
- **AWS Detailed Billing Reports Are Daunting**
  - Over 10 Million Line Items
- **Project Managers Need Focus**
  - Am I Below My Budget?
  - Where Are My Costs Going?
  - Who's Spending Them?
- **Manual Compilation of Reports**
  - Integrate FINRA Data

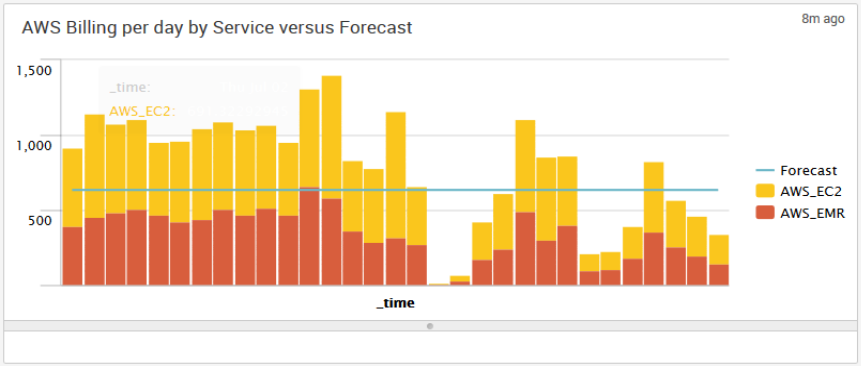
Approach Chosen

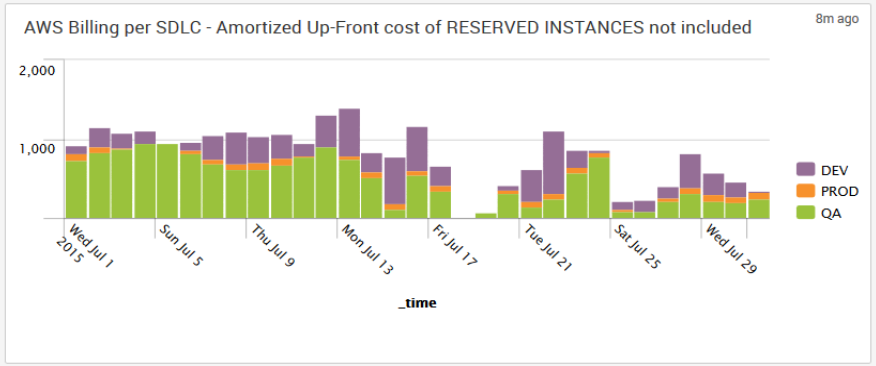
- **Use Splunk as Process/Delivery System**
  - Ability to Collect/Analyze/Visualize
- **Collect AWS Billing Data in Splunk**
  - Billing Data from S3 bucket (Daily Load)
  - Detailed Line Items w/Resources & Tags
- **Data Enrichment**
  - Project Code Lookups
  - Forecast Projections
  - Billing Adjustments
- **Build Interfaces**
  - FINRA AWS Billing App

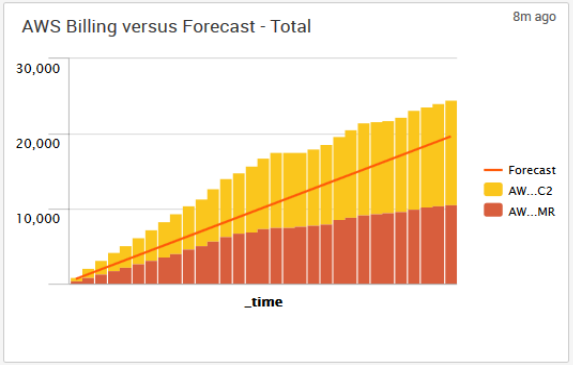
FINRA AWS Billing App



AWS Billing App



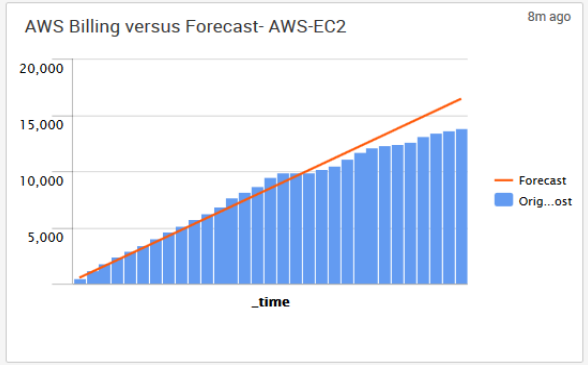




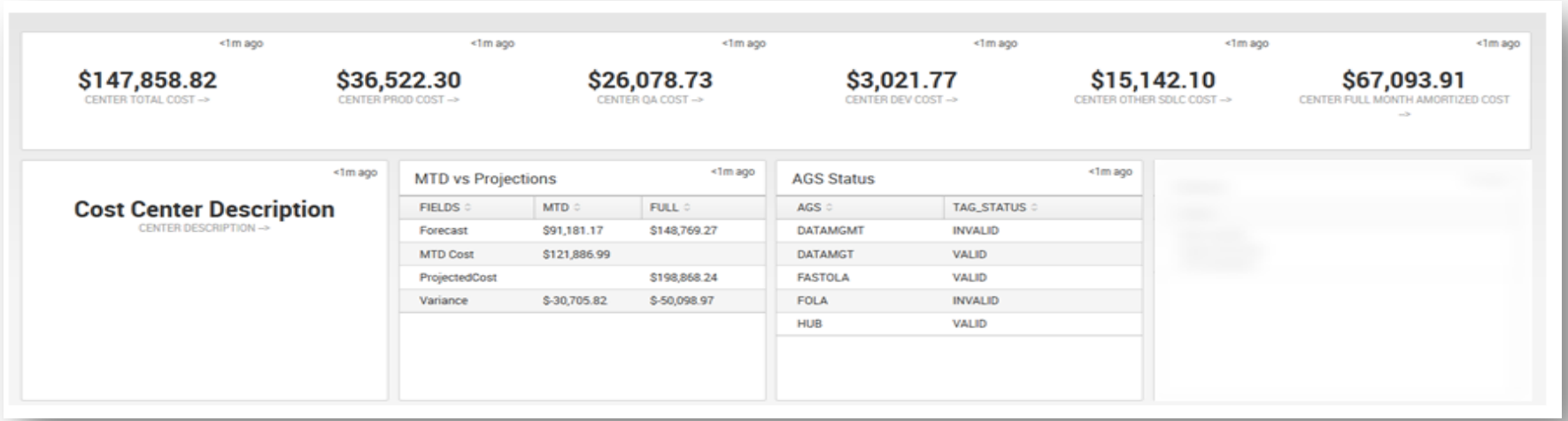
AWS Billing By ProductName - Click on ProductName to get Product stats

8m ago

ProductName_Tag	Cost	Perc
AWS-EC2	$13,863.92	%56.61
AWS-EMR	$10,624.96	%43.39



AWS Billing App



Impact – Reduced Costs

- **Focus on Low Hanging Fruit**
  - Shutting Down Services over Weekends/Evenings
  - Storage Sun Setting/Dormant EC2
  - Identify AWS Services with Highest Spending
  - Projects Over Budget
- **Results**
  - 13.5% Reduction in Billing Line Items in 1 Month
- **Better Forecast Projections**
  - Feedback and Control

THANK YOU

splunk>

Orrstown Bank

splunk>

About ORRSTOWN BANK

Orrstown Bank is a **community bank in PA and MD** with about $1.2 billion in assets

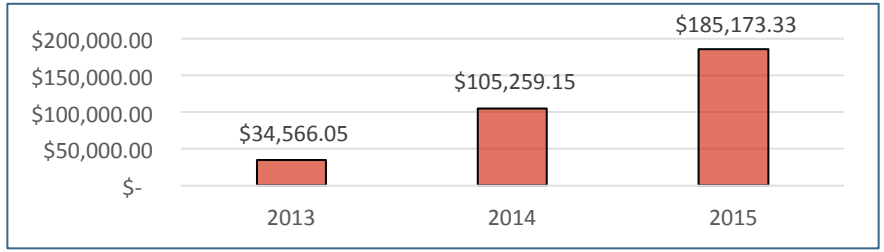
Orrstown has adopted a **cloud-first model for technology** solutions

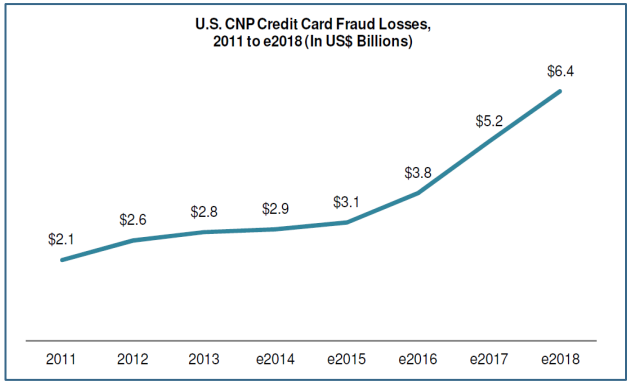
Orrstown has been running splunk>cloud for over 1 year to facilitate **operational and security data analytics**

Orrstown continues to explore opportunities to use splunk>cloud to solve **additional problems such as Fraud**

Overview of the Problem

Amount **charged off due to Card Fraud** has grown **435%** in the past 3 years





This pattern represents a **similar if not conservative experience as our peers**

Many **solutions** offered to smaller banks **cannot keep pace with the fraud** patterns

ORRSTOWN BANK

Fraudulent Behavior Patterns

Attacker steals card data from…

…and local merchants

Card data sold on the black market, cloned, and used….

Often the first fraudulent transaction is followed shortly by many other transactions

Smarter criminals are selling cards back into the local area from which the card was stolen to evade fraud detection

Fraudulent card present transactions usually occur at…

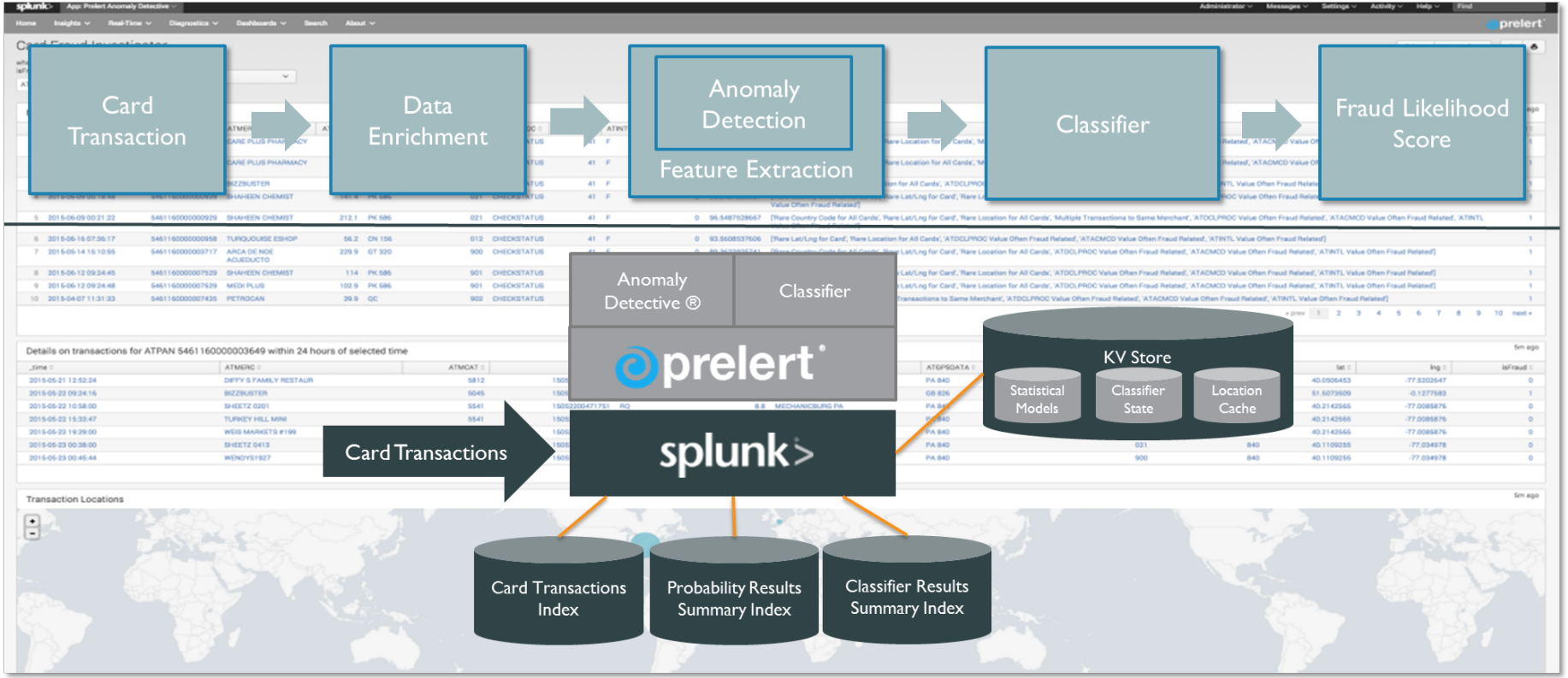
- Grocery stores
- Pharmacies
- Walmart
- GameStop
- Best Buy

Card not present transactions at…

- Apple
- On-line electronics retailers
- Travel

ORRSTOWN BANK

Card Fraud Prediction – App Architecture

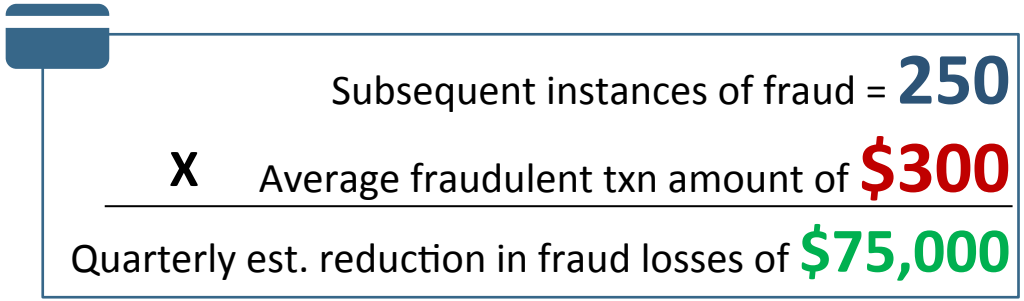


Results and the Business Case

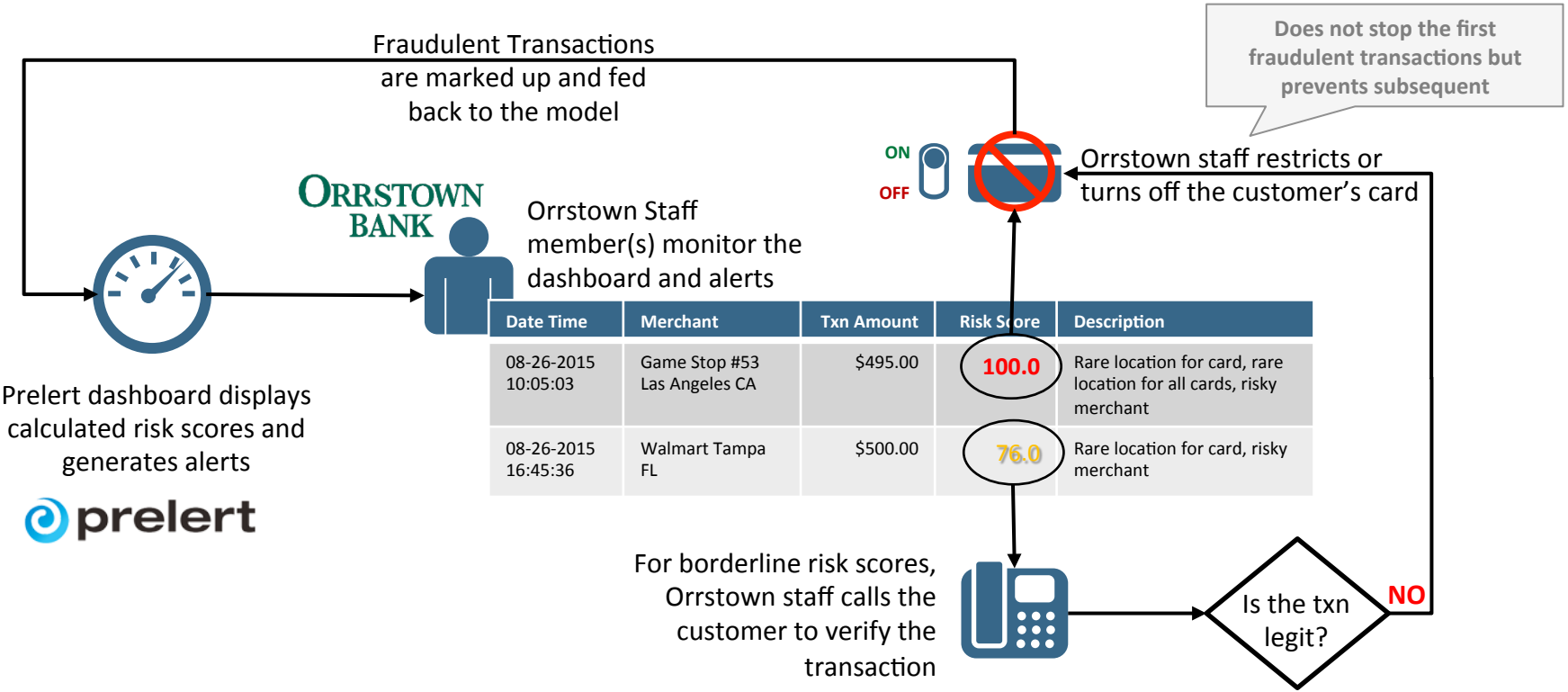
Initial experiment with **1 quarter's worth of transactions** identified…

- Approximately **50%** of the fraudulent *card present* transactions
- A small population of only **330** false positives
- Of the fraudulent transactions identified, there were **250 instances of subsequent fraudulent transactions** occurred using the same card

These are the fraudulent txns we can stop



Operationalizing the Model



Potential

Potential for ORRSTOWNBANK ...

- Continue to use Prelert as an **additional layer of fraud control** beyond what our process offers
- Explore feeding **additional information** (e.g. on-line transfers, etc) into prelert via splunk>cloud **to identity other customer behavior anomalies**

Potential for the Industry…

- A **centralized Fraud Investigator service** to which many banks can subscribe
- The **model improves by** learning from a larger volume of information
- Each bank can still maintain the ability to **influence the model based on their local experiences**

THANK YOU

splunk>

50%

Gatwick Airport

splunk>

YOUR LONDON AIRPORT Gatwick

Who are Gatwick Airport?

Busiest single runway airport in the world

- 925 Flights per day in August 2015
- 40 Million passengers by 2016
- 10 Years ahead of UK Government predictions on passenger numbers
- 52 Airlines flying to 200 locations in 90 countries
- We fly to more destinations than any other UK airport

YOUR LONDON AIRPORT Gatwick

Proof of Value

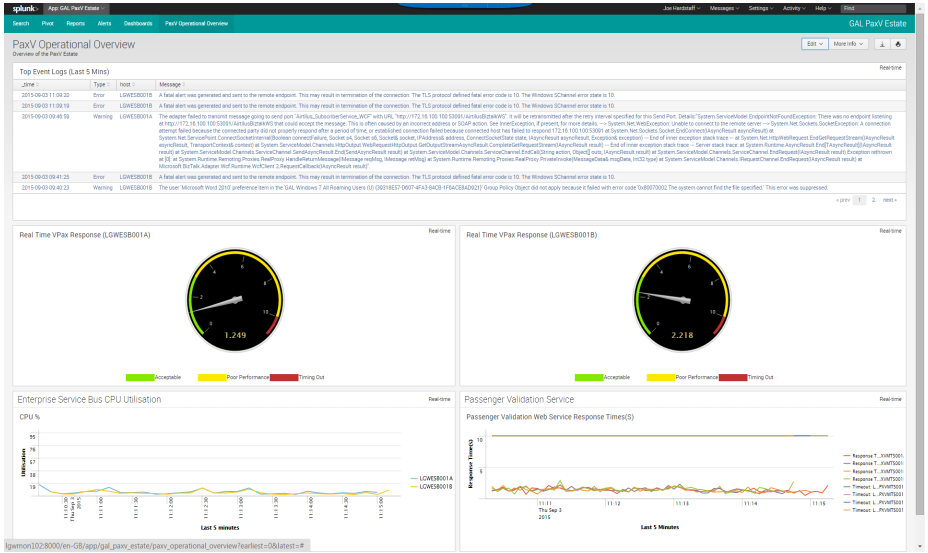
Performance & Availability

Used to scan boarding passes to ensure:

- Right airport, terminal, day, time
- Flight not cancelled or delayed

Splunk provided:

- Insight on performance gains
- Reduction in incidents
- At a glance root cause analysis



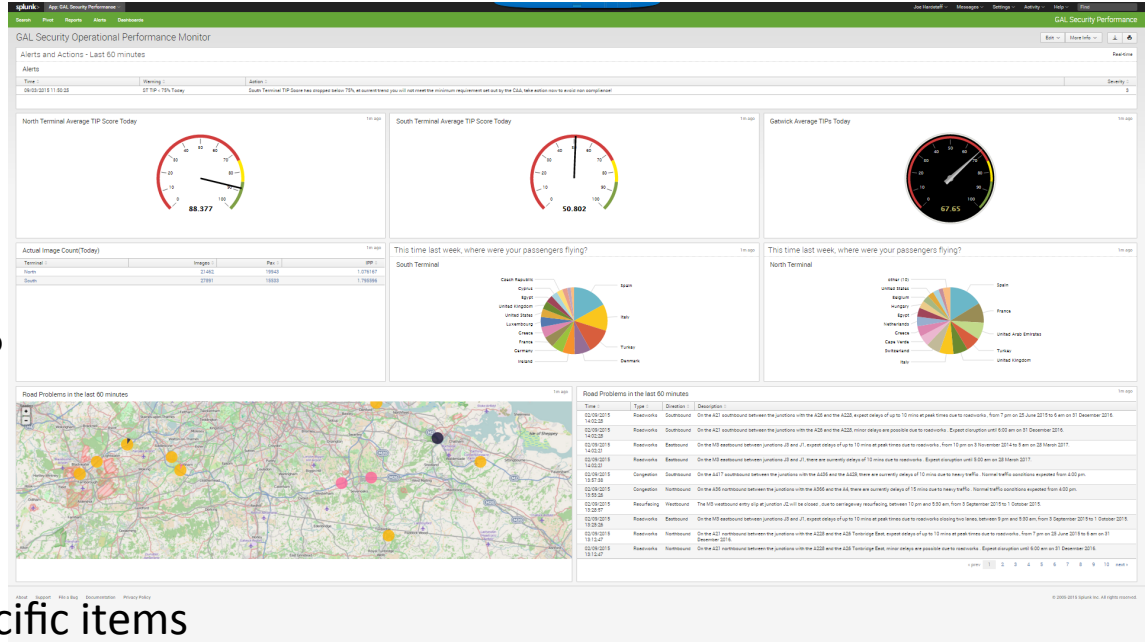
YOUR LONDON AIRPORT Gatwick

The Dawn of Realization

Compliance with SQR

First attempt with business data:

- How are we doing with TIP?
- Where are passengers going?
- Are there problems with travel?



Splunk provided:

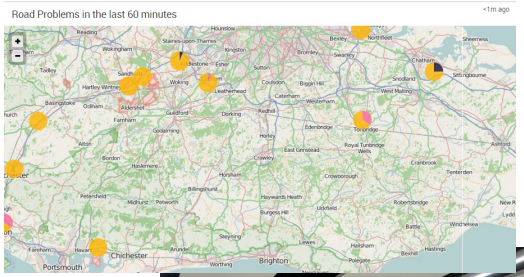
- Insight into security compliance
- Prepare security to look for specific items
- Understand road and rail incidents & their effect
- A combination of historical fact with current event

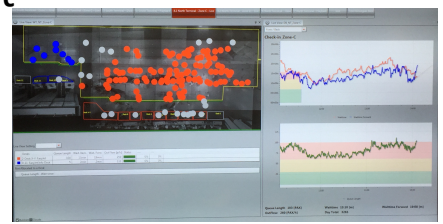
YOUR LONDON AIRPORT Gatwick

Terminal Performance

Monitor the moving parts

- Road, rail & bus services
- Building management system
- Passenger information displays
- Electronic way-finding
- Manned check-in desks in use
- Common use – self service kiosks
- Self service/automated bag drop
- Area occupancy & queue measurement
- Security gates
- X-Ray throughput
- Gate announcements/call to gate





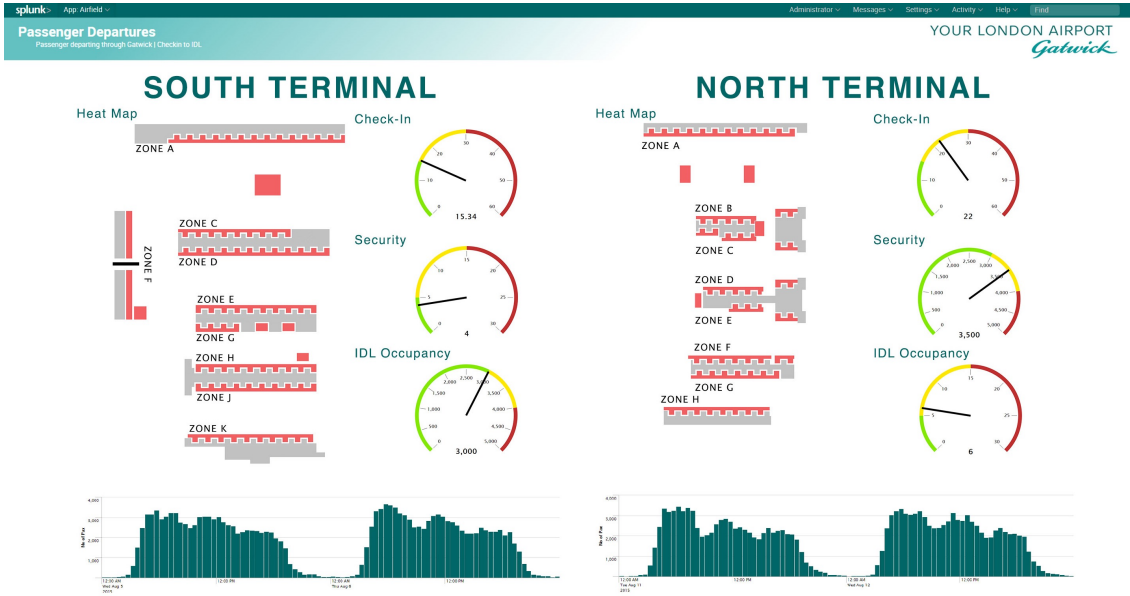
YOUR LONDON AIRPORT Gatwick

Terminal Dashboard

At-A-Glance Performance

Provides:

- Passenger flow monitoring
- Early view of opportunities
- Flag where we can do better
- Highlight potential issues
- Impact analysis
- Allows timely intervention



Historical Fact/Current Event

Disruption Cause & Effect – Where could Splunk>Cloud take us?

- Travel Disruption:
  - Capture road, rail, bus disruption & expected duration
  - Reduction in the expected passenger numbers
  - Check-in, security, airlines, ground handlers informed
- Passenger Flow:
  - Capture passenger flow from curb to gate & back
  - Reduce queues, congestion & pinch points
  - Improve on the passenger experience
- Social Media:
  - Capture feedback from Twitter, Facebook, Yammer
  - Provides real time information about Gatwick
  - When it's not perfect, we can make it great again

THANK YOU

splunk>

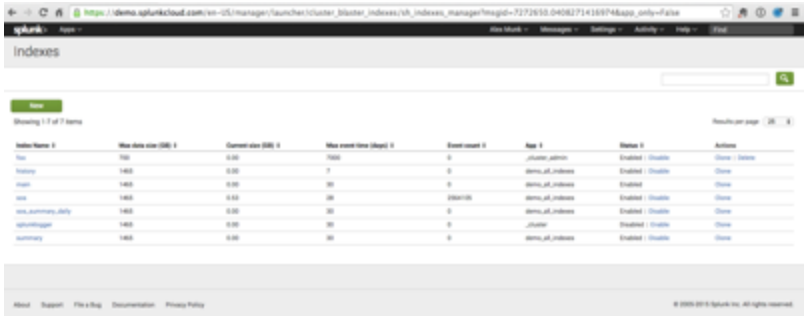
Splunk Cloud – What's Next

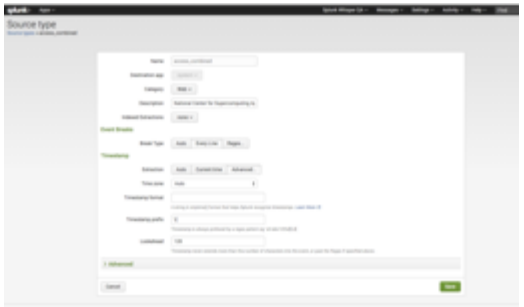
splunk>

Self-Service

Spend less time configuring, more time analyzing

- Index Management
- Sourcetype Management
- Seamless App Installation
- Forwarder Visibility & Management





Data Roll

- Move data to S3 buckets
- Store data for compliance reasons
- Keep data searchable

More Applications for Cloud Data Sources

- Gain SaaS / PaaS visibility
- Correlate across cloud data sources
- Feed into Splunk Enterprise Security and IT Service Intelligence

Security Attestations

Completed

In-process

Conclusion

What can you do with..

splunk> cloud™

Hear From Our Customers