



.conf2015

# 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 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

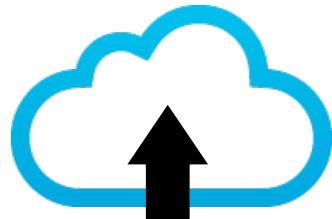
Coca-Cola

AUTODESK

SolarCity

# Splunk Cloud Value Drivers

Instant



Secure



Reliable



Hybrid



100% Uptime

# 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%



# .conf2015

# FINRA



splunk®

# Who We Are

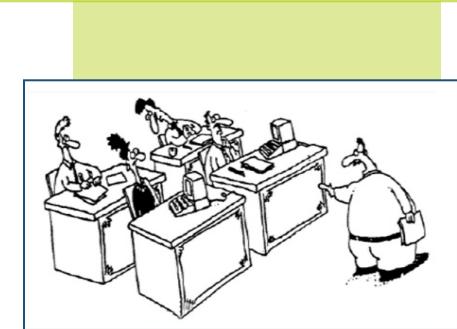
- FINRA—the Financial Industry Regulatory Authority—is an independent, non-governmental regulator for all securities firms doing business with the public in the United States
- FINRA protects investors by regulating brokers and brokerage firms and by monitoring trading on U.S. stock markets
- FINRA monitors 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

Splunk - App: FINRA AWS Billing

Alerting | Dashboards | EC2 Reports

## FINRA AWS Billing

Time: Previous month CostCenter: CBX314 Submit

**Summary Metrics**

- 4m ago: \$24,488.88 (CBX314 TOTAL COST)
- 4m ago: \$1,593.10 (CBX314 PREV COST)
- 4m ago: \$15,189.75 (CBX314 GA COST)
- 4m ago: \$7,706.03 (CBX314 DEV COST)
- 4m ago: N/A
- 4m ago: N/A
- 4m ago: \$19,634.42 (CBX314 FORECAST)

**MTD vs Projections**

FIELD	MTD	FULL
Forecast	\$11,400.63	\$19,634.42
MTD Total	\$8,687.83	
ProjectedCost	\$14,411.27	
Variance	\$3,032.80	\$3,223.15

**Cost by Account's Amortized Cost NOT Included**

AccountID	AccountName	Cost
		\$15,189.75
		\$7,706.03
		\$1,693.10

**AGS Status**

AGS	ETLMGMT	TAG_STATUS	MRP
		VALID	VALID

**Owners**

AWS Billing per day by Service versus Forecast

AWS Billing per SDLC - Amortized Up-Front cost of RESERVED INSTANCES not included

AWS Billing versus Forecast - Total

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

ProductName, Tag	Cost	Per%
AWS-EC2	\$1,386.92	%55.81
AWS-EMR	\$10,624.96	%43.39

AWS Billing versus Forecast- AWS-EC2

AWS Billing per Cluster by ItemDescription

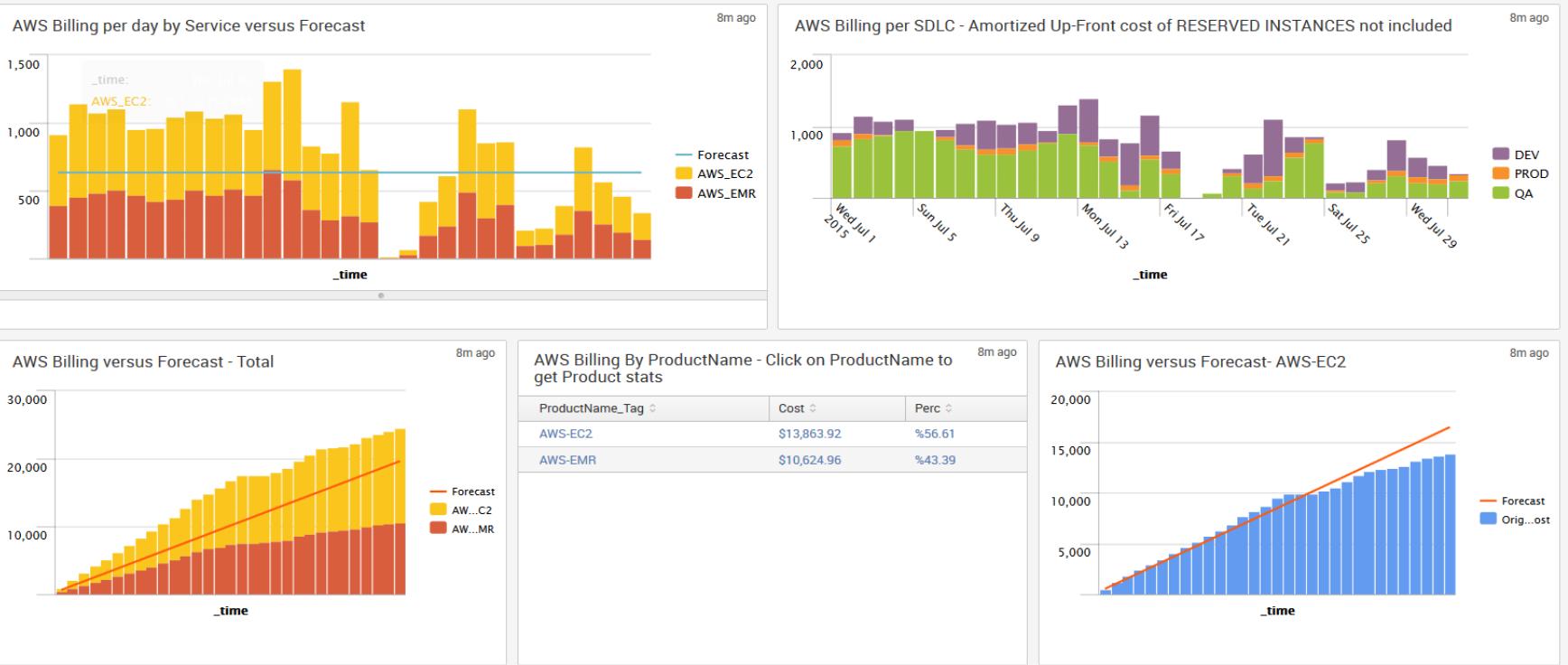
date	product_id	AGS	SDLC	Center	Name	Tags
2015-07-01	j-1113390129239039	ETLMGMT	GA	CBX314	ETLMGMT OPTIONS	0.67000000
2015-07-01	j-1113390129239039	ETLMGMT	GA	CBX314	ETLMGMT OPTIONS	0.64000000
2015-07-01	j-1113390129239039	ETLMGMT	GA	CBX314	ETLMGMT OPTIONS	0.67000000
2015-07-01	j-1524405050000	ETLMGMT	GA	CBX314	ETLMGMT OPTIONS	0.62000000
2015-07-01	j-1524405050000	ETLMGMT	GA	CBX314	ETLMGMT OPTIONS	0.67000000
2015-07-01	j-1702940000000	ETLMGMT	GA	CBX314	ETLMGMT OPTIONS	0.64000000
2015-07-01	j-1919410000000	ETLMGMT	GA	CBX314	ETLMGMT OPTIONS	0.54000000
2015-07-01	j-1CF030UJUJ7PT	ETLMGMT	PROD	CBX314	ETLMGMT OPTIONS	0.54000000
2015-07-01	j-1DP94T413979	ETLMGMT	DEV	CBX314	ETLMGMT OPTIONS	0.54000000
2015-07-01	j-1FP449213TVEH00	ETLMGMT	GA	CBX314	ETLMGMT OPTIONS	0.54000000

x PREV 1 2 3 4 5 6 7 8 9 10 next x

About | Support | File a Bug | Documentation | Privacy Policy

© 2009-2015 Splunk Inc. All rights reserved.

# AWS Billing App



# AWS Billing App

<small>&lt;1m ago</small> <b>\$147,858.82</b> CENTER TOTAL COST →	<small>&lt;1m ago</small> <b>\$36,522.30</b> CENTER PROD COST →	<small>&lt;1m ago</small> <b>\$26,078.73</b> CENTER QA COST →	<small>&lt;1m ago</small> <b>\$3,021.77</b> CENTER DEV COST →	<small>&lt;1m ago</small> <b>\$15,142.10</b> CENTER OTHER SDLC COST →	<small>&lt;1m ago</small> <b>\$67,093.91</b> CENTER FULL MONTH AMORTIZED COST →
---	---	---	---	---	---

<small>&lt;1m ago</small> <b>Cost Center Description</b> CENTER DESCRIPTION →	<small>&lt;1m ago</small> <b>MTD vs Projections</b>	<small>&lt;1m ago</small> <b>AGS Status</b>																											
	<table><thead><tr><th>FIELDS ◊</th><th>MTD ◊</th><th>FULL ◊</th></tr></thead><tbody><tr><td>Forecast</td><td>\$91,181.17</td><td>\$148,769.27</td></tr><tr><td>MTD Cost</td><td>\$121,886.99</td><td></td></tr><tr><td>ProjectedCost</td><td></td><td>\$198,868.24</td></tr><tr><td>Variance</td><td>\$-30,705.82</td><td>\$-50,098.97</td></tr></tbody></table>	FIELDS ◊	MTD ◊	FULL ◊	Forecast	\$91,181.17	\$148,769.27	MTD Cost	\$121,886.99		ProjectedCost		\$198,868.24	Variance	\$-30,705.82	\$-50,098.97	<table><thead><tr><th>AGS ◊</th><th>TAG_STATUS ◊</th></tr></thead><tbody><tr><td>DATAMGMT</td><td>INVALID</td></tr><tr><td>DATAMGT</td><td>VALID</td></tr><tr><td>FASTOLA</td><td>VALID</td></tr><tr><td>FOLA</td><td>INVALID</td></tr><tr><td>HUB</td><td>VALID</td></tr></tbody></table>	AGS ◊	TAG_STATUS ◊	DATAMGMT	INVALID	DATAMGT	VALID	FASTOLA	VALID	FOLA	INVALID	HUB	VALID
FIELDS ◊	MTD ◊	FULL ◊																											
Forecast	\$91,181.17	\$148,769.27																											
MTD Cost	\$121,886.99																												
ProjectedCost		\$198,868.24																											
Variance	\$-30,705.82	\$-50,098.97																											
AGS ◊	TAG_STATUS ◊																												
DATAMGMT	INVALID																												
DATAMGT	VALID																												
FASTOLA	VALID																												
FOLA	INVALID																												
HUB	VALID																												

# 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





.conf2015

2015

2011

2012

2013

2014

2015

THANK YOU

splunk®



.conf2015

# 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**

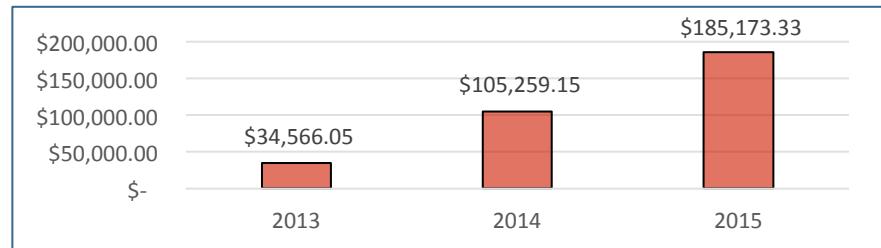
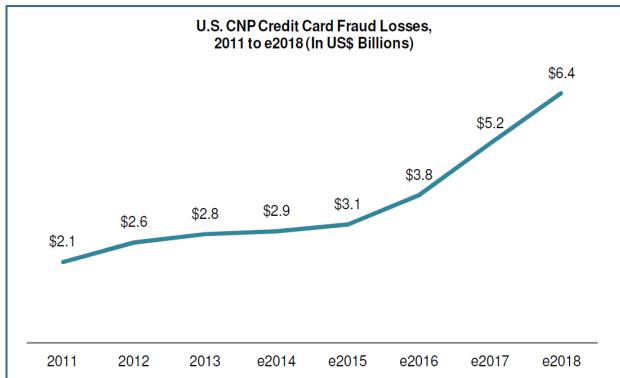


Orrstown continues to explore opportunities to use **splunk>cloud™** to solve **additional problems such as Fraud**

# 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...

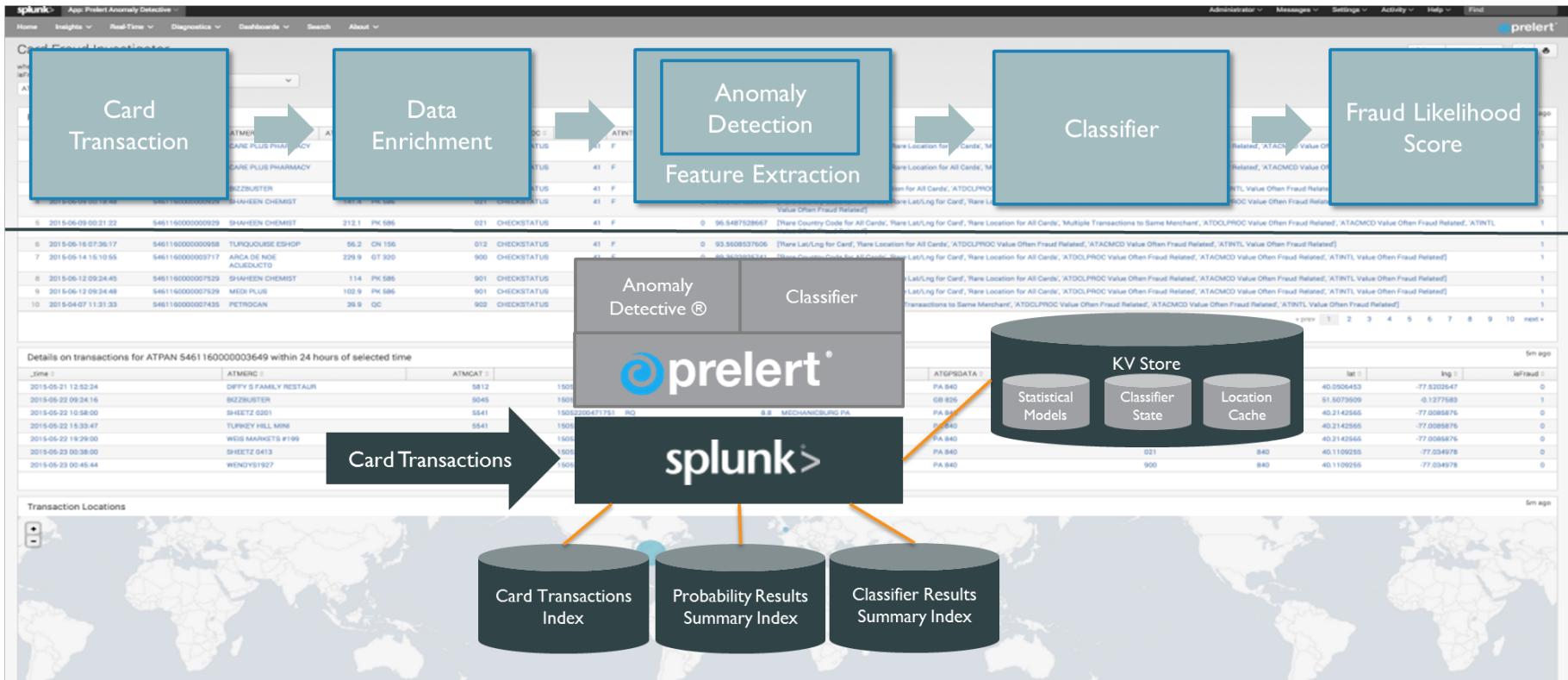
- Grocery stores
- Pharmacies
- Walmart
- GameStop
- Best Buy

Card not present transactions at...

- Apple
- On-line electronics retailers
- Travel

**ORRSTOWN  
BANK**

# Card Fraud Prediction – App Architecture

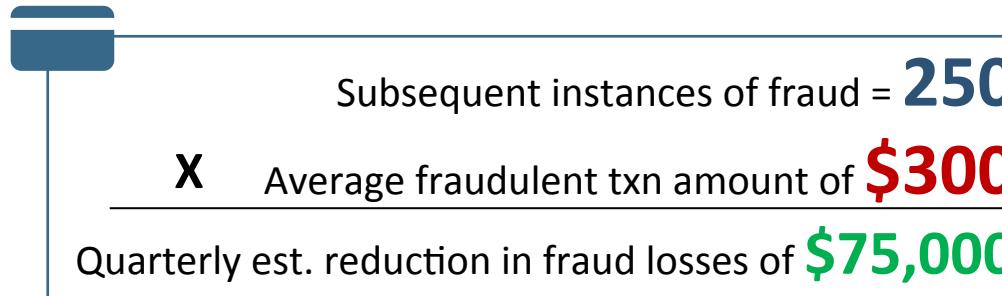


# Results and the Business Case

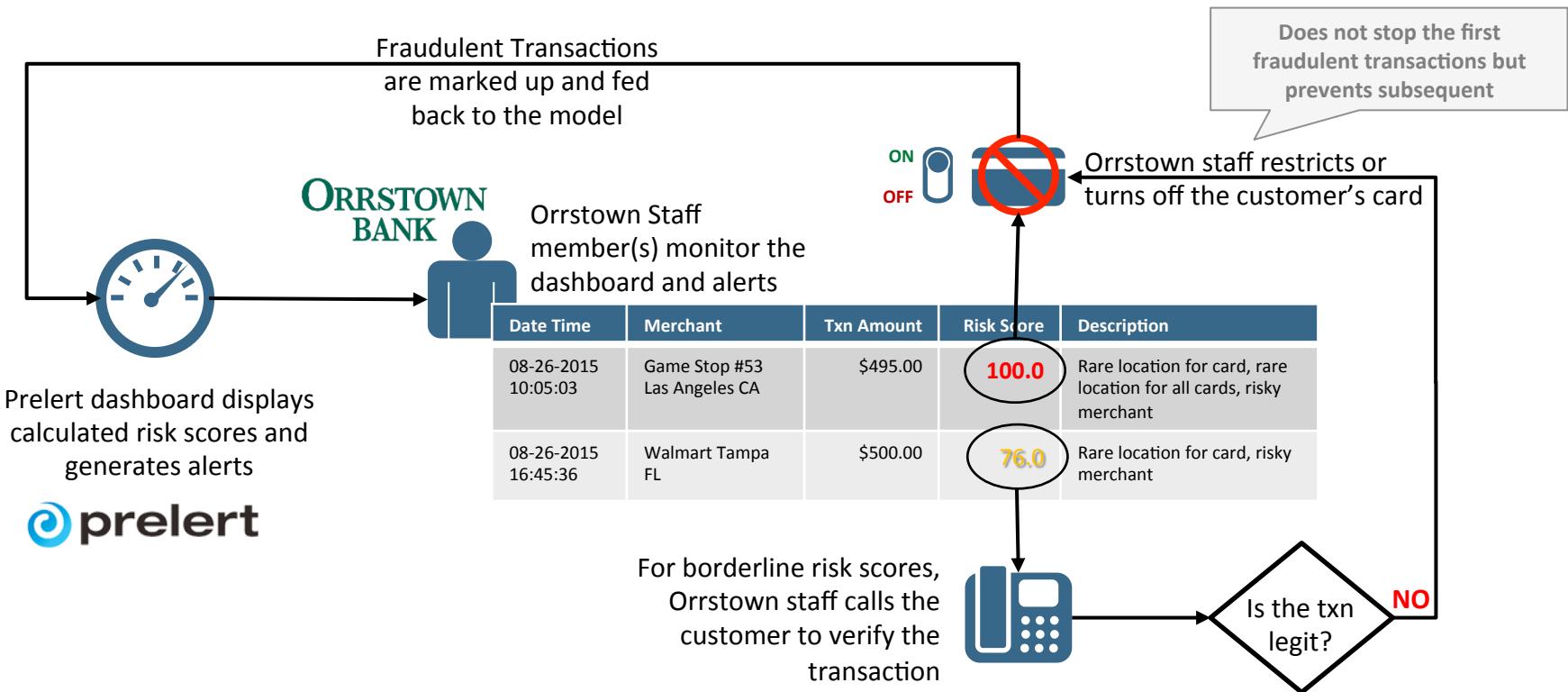
Initial experiment with **1 quarter's worth of transactions** identified...

- 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



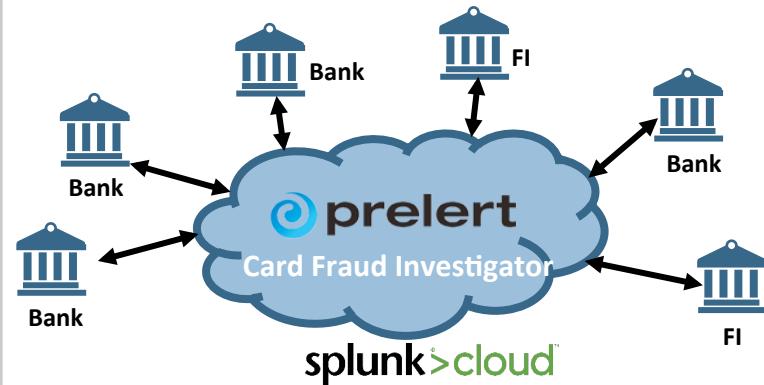
...



- 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 **prealert** via **splunk>cloud** to **identify 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



.conf2015

# THANK YOU

splunk®

# 50%



.conf2015

# Gatwick Airport

splunk®

# 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



# Proof of Value

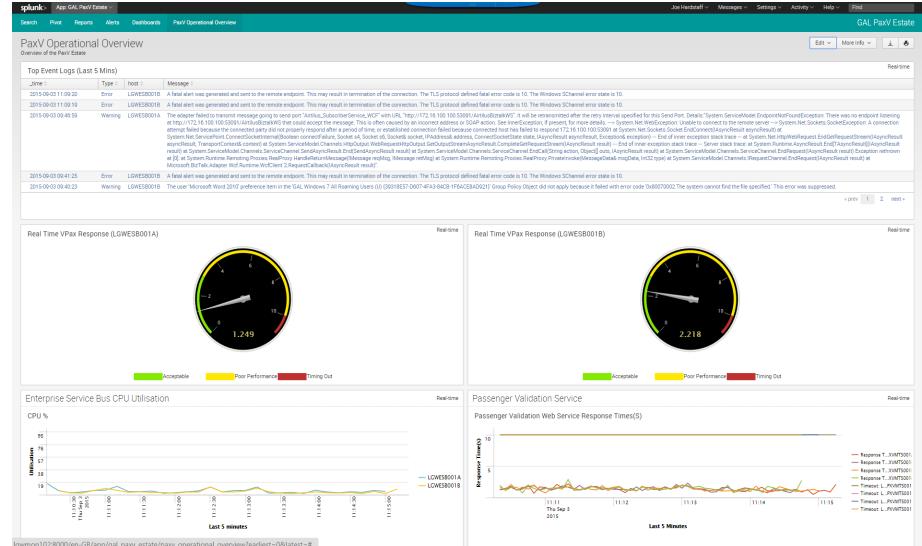
## Performance & Availability

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

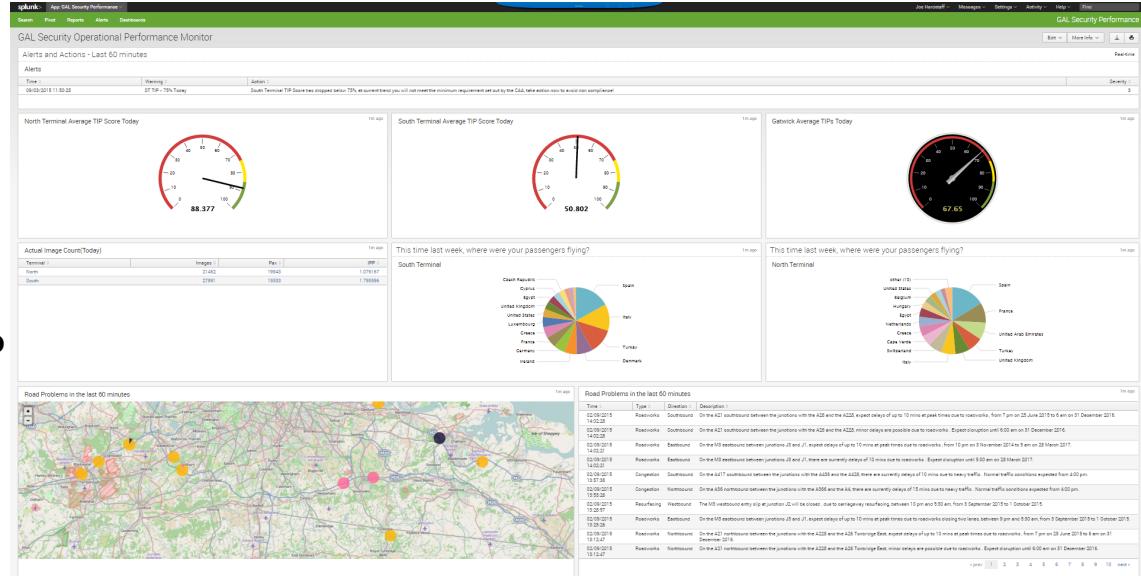


# The Dawn of Realization

## Compliance with SQR

First attempt with business data:

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



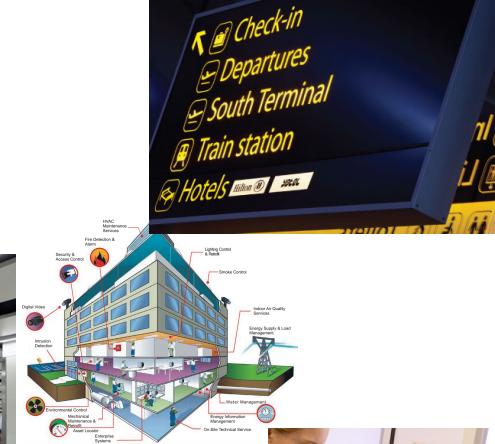
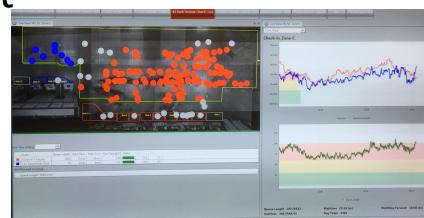
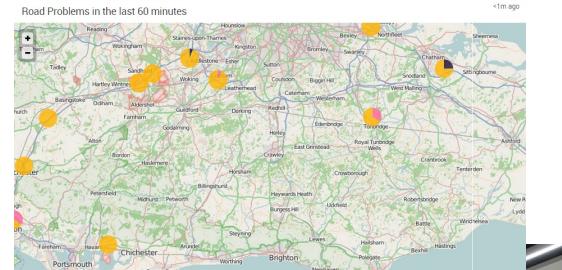
Splunk provided:

- 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

# 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

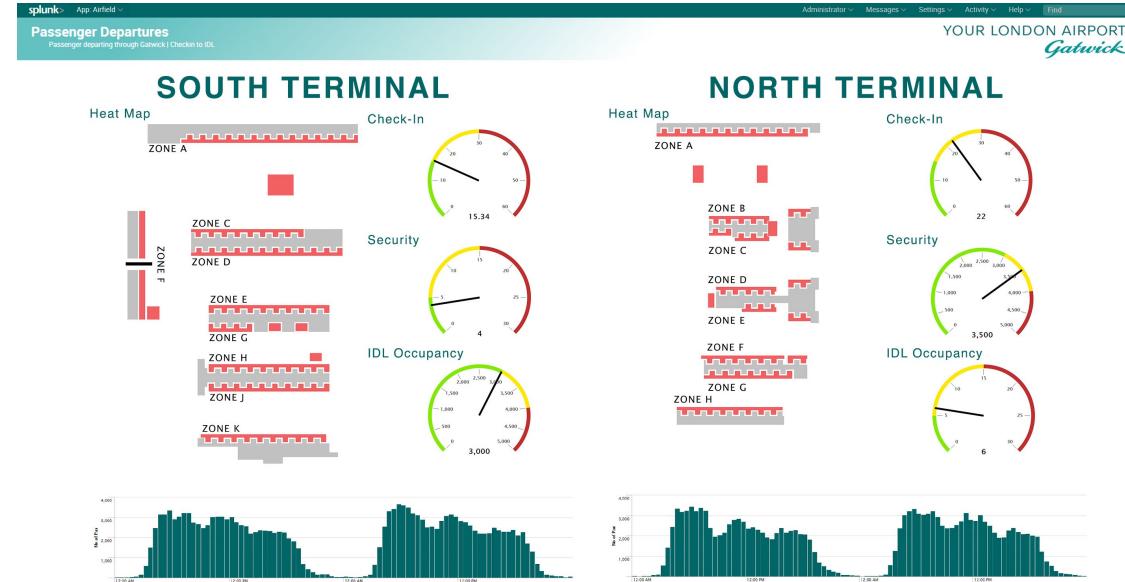


# Terminal Dashboard

## 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



James Morris @MorrisJFM · 20h  
@Gatwick\_Airport any reason you have failed to provide adequate parking for vehicles over 1.8m high this evening? #poorservice #pooreffort

Gatwick Airport LGW @Gatwick\_Airport · 18 hrs  
@MorrisJFM Sorry to hear you had trouble parking, James. Did you try the North Terminal long stay parking or before short stay in the South?

12:35 p.m. - 3 Sep 2015 · Details

[Hide conversation](#)

.conf2015

# THANK YOU

**splunk®**



.conf2015

# 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

The image contains two screenshots of the Splunk Cloud interface. The top screenshot shows the 'Indexes' page, which lists various indexes with columns for Name, Max data size (MB), Current size (MB), Max event size (bytes), Event count, Type, Status, and Actions. The bottom screenshot shows the 'Source type' configuration page, where users can define source types with fields for Name, Input type, Input spec, Output type, and various processing and buffering configurations.

# 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<sup>®</sup>>cloud<sup>™</sup>

# Hear From Our Customers



AURIZON  
YOUR LONDON AIRPORT  
*Gatwick*

