



# Manage AWS Services

Cost, Security, Best Practice and Troubleshooting

Elias Haddad | Principal Product Manager  
Peter Chen | Principal Software Engineer

September 2017 | Washington, DC





# Challenges

## in Managing Enterprise Level AWS Services



Cost Optimization



Security Strategy



- ▶ Access monitoring
- ▶ API call monitoring
- ▶ User management
- ▶ Anomaly detection
- ▶ Smart alerting

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CU-01"
ows NT 317 27.160.0.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3 HTTP/1.1"
do?action=purchase&itemId=EST-16&product_id=RP-LI-02" 468 125.17.14.111 [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3 HTTP/1.1"
opping.com/purchase&itemId=EST-16&product_id=RP-LI-02" 468 125.17.14.111 [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3 HTTP/1.1"
do?action=purchase&itemId=EST-16&product_id=RP-LI-02" 468 125.17.14.111 [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF2ADFF3 HTTP/1.1"

```



# Challenges

in Managing Enterprise Level AWS Services

 Cost Optimization

 Security Strategy

 Best Practice

 Troubleshooting

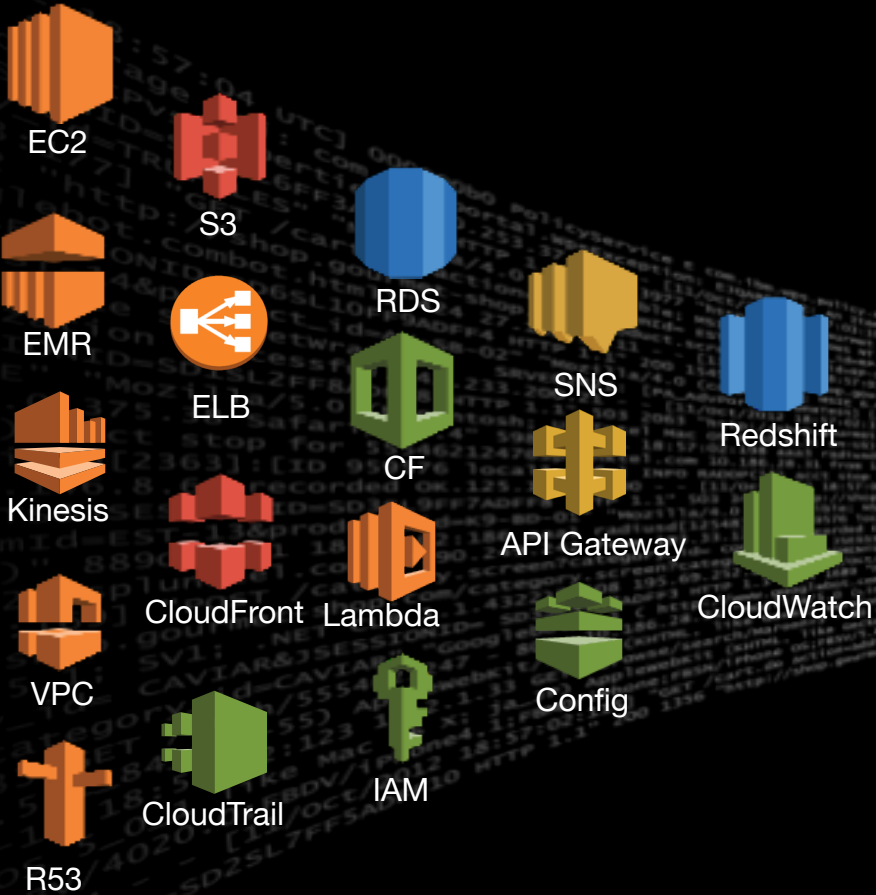
- ▶ Change management
- ▶ Network topology
- ▶ Association analysis



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MX-IL-WZ-01"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 468 125.17.14.118 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP/1.1"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MX-IL-WZ-01"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 468 125.17.14.118 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP/1.1"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MX-IL-WZ-01"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 468 125.17.14.118 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP/1.1"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MX-IL-WZ-01"
317.27.160.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 468 125.17.14.118 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP/1.1"
```

# Splunk Solution

## AWS App & Add-on



**Splunk App for AWS**

**Splunk Add-on for AWS**



# Get Data In

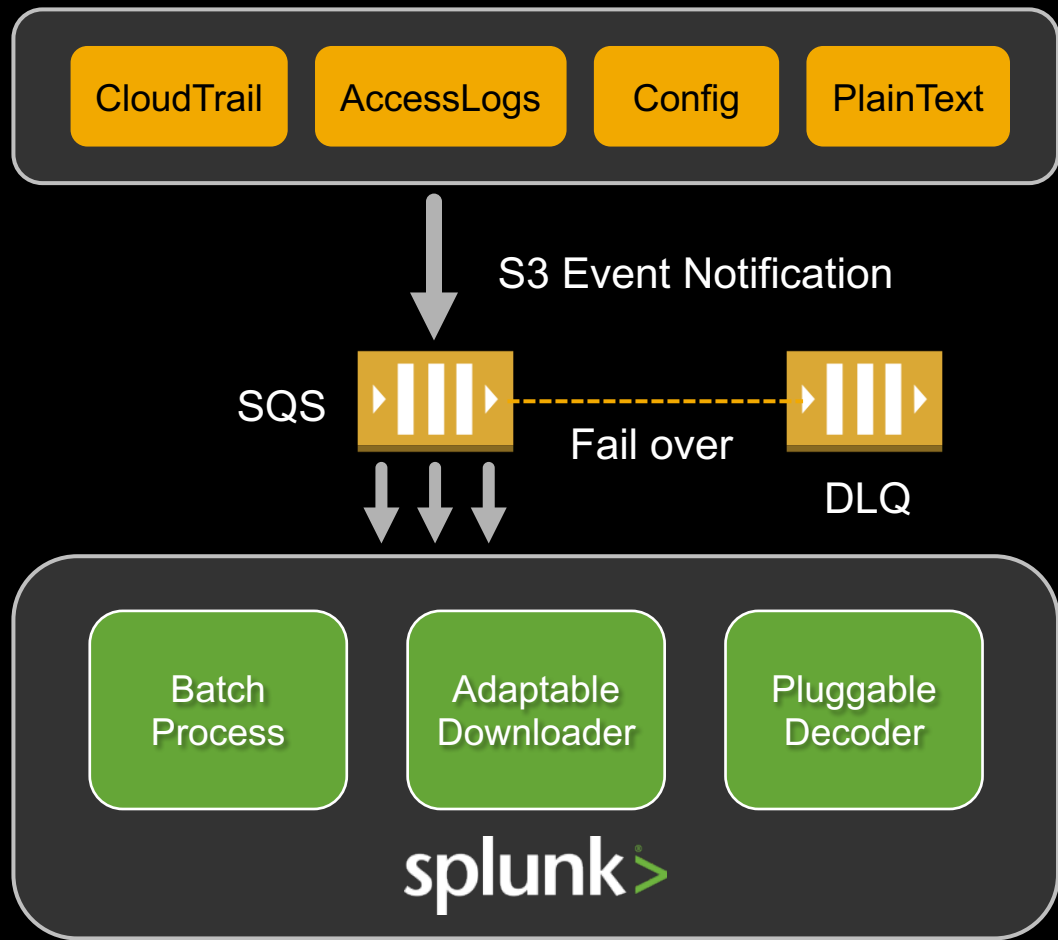
---





# Key New Features in AWS Add-on 4.3 and 4.4

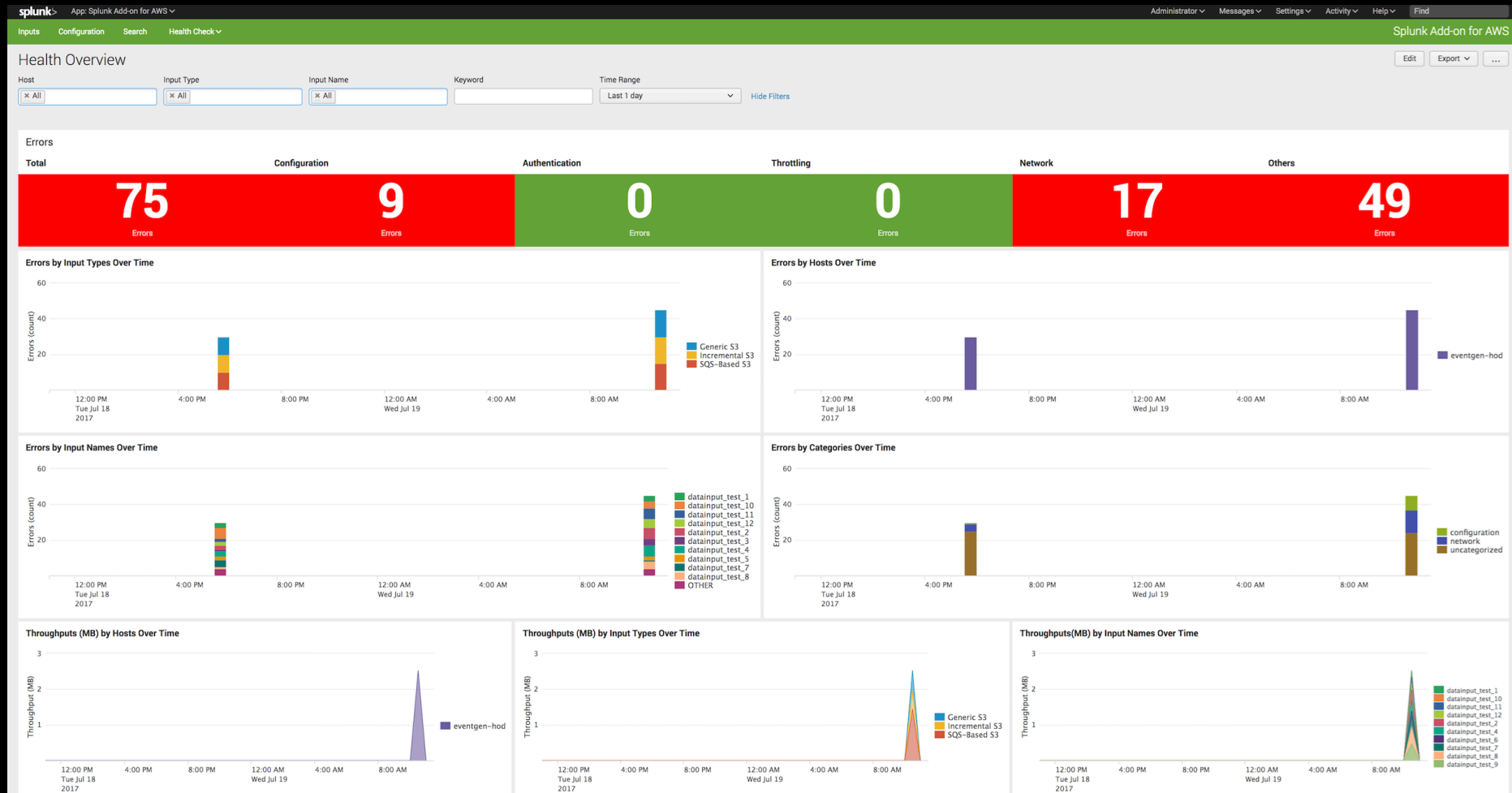
## New Input: SQS-Based S3



- ▶ Higher throughput
- ▶ Real-time ingestion
- ▶ Cost efficient
- ▶ High availability
- ▶ Scale out capability

# Key New Features in AWS Add-on 4.3 and 4.4

## Trouble Shooting: Health Dashboard



# Key New Features in AWS Add-on 4.3 and 4.4

## Easier Configuration: New Designed Configuration GUI

splunk App: Splunk Add-on for AWS

Power User 3 Messages Settings Activity Help Find

Inputs Configuration Search Health Check Splunk Add-on for AWS

### CloudWatch

Inputs > Create New Input

Namespace	Dimension?	Dimension Value?	Metrics?	Metric Statistics
AWS/ApiGateway	×	AutoScalingGroupName	["AutoScalingGroupName":*]	<input type="checkbox"/> All <input type="checkbox"/> Average <input type="checkbox"/> Sum <input type="checkbox"/> SampleCount <input type="checkbox"/> Maximum <input type="checkbox"/> Minimum
AWS/ApplicationELB	×			
AWS/AutoScaling	×			
AWS/Billing	×			
AWS/CloudFront	×	ImageId	["ImageId":*]	<input type="checkbox"/> All <input type="checkbox"/> Average <input type="checkbox"/> Sum <input type="checkbox"/> SampleCount <input type="checkbox"/> Maximum <input type="checkbox"/> Minimum
AWS/CloudSearch	×			
AWS/DX	×			
AWS/DynamoDB	×	InstanceId	["InstanceId":*]	<input type="checkbox"/> All <input type="checkbox"/> Average <input type="checkbox"/> Sum <input type="checkbox"/> SampleCount <input type="checkbox"/> Maximum <input type="checkbox"/> Minimum
AWS/EBS	×			
AWS/EC2	×			
AWS/EC2Spot	×	InstanceType	["InstanceType":*]	<input type="checkbox"/> All <input type="checkbox"/> Average <input type="checkbox"/> Sum <input type="checkbox"/> SampleCount <input type="checkbox"/> Maximum <input type="checkbox"/> Minimum
AWS/ECS	×			
AWS/ELB	×			
AWS/ES	×			
AWS/ElasticCache	×			
AWS/ElasticMapReduce	×			
AWS/Events	×			
AWS/Kinesis	×			
AWS/Lambda	×			
AWS/Logs	×			
AWS/ML	×			

+ Add Another

Cancel OK

Settings Activity Help Find

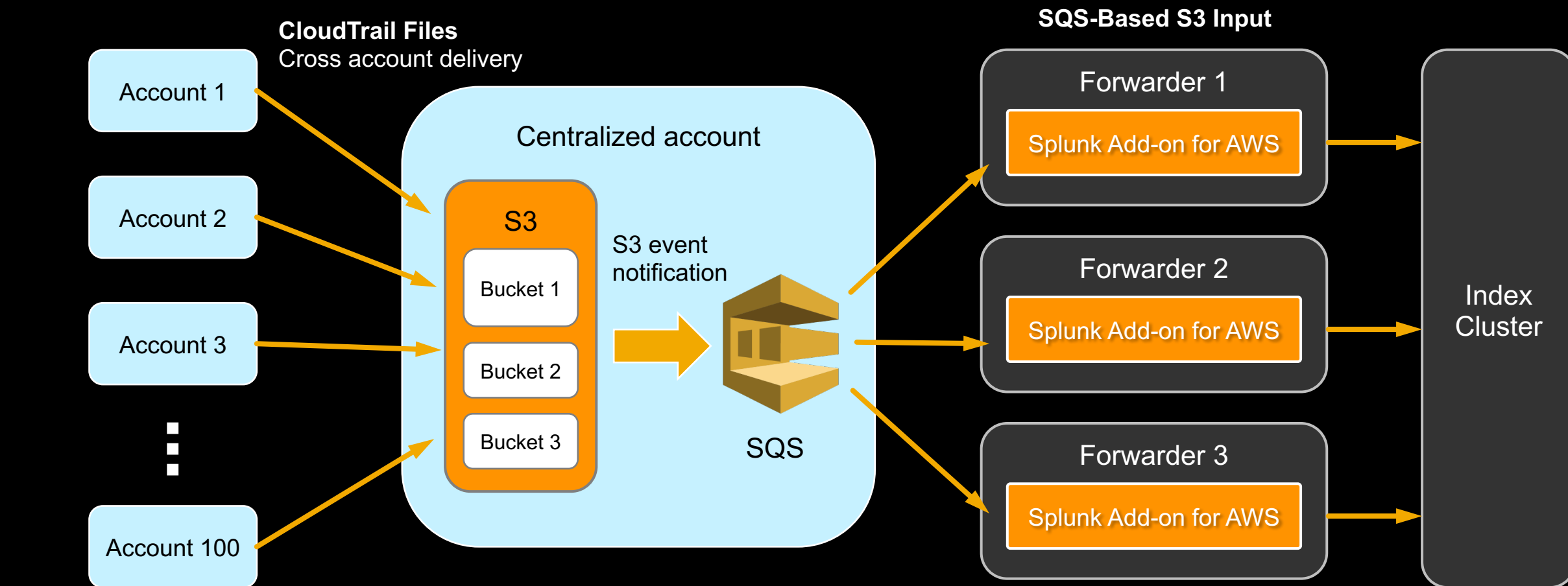
Splunk Add-on for AWS

Create New Input

Input	Source
SQLS-Based S3 (Recommended)	< CloudTrail
CloudTrail	CloudWatch
Generic S3	< Cloudfront Access Logs
Incremental S3	< Config
aws:cloudwatch	Config Rule
aws:cloudwatch	Description
aws:cloudwatch	< ELB Access Logs
aws:cloudwatch	Inspector
aws:cloudwatch	< S3 Access Logs
aws:cloudwatchlogs:vpctest	< VPC Flow Logs
aws:cloudwatchlogs:vpctest	< Others
aws:cloudtrail	Edit   Clone   Delete

# Best Practice of Get Data In

Example 1: Get CloudTrail Data of Hundreds Accounts in Real-time



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL9FF1ADFF3"
ows NT 27.160.0.0 - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17.14 [oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3]
itemId=EST-16&product_id=RP-LI-02" 468 125.17.14 [itemId=EST-16&product_id=RP-LI-02]
07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17.14 [oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3]
http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" 200 2423 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=RP-LI-02"
http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-188&product_id=AV-CB-01&SESSIONID=SD10SL9FF1ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-188&product_id=AV-CB-01&SESSIONID=SD10SL9FF1ADFF9"
http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-119&product_id=FL-SW-01" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-119&product_id=FL-SW-01"
http://buttercup-shopping.com/category.screen?category_id=FLOWERS&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&SESSIONID=SD5SL9FF1ADFF3"
http://buttercup-shopping.com/category.screen?category_id=EST-119&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/category.screen?category_id=EST-119&SESSIONID=SD5SL9FF1ADFF3"
  
```

# Best Practice of Get Data In

## Example 2: Get Data More Securely

EC2 with Instance Role



AssumeRole

Account 1

Account 2

Account 3



Config



CloudWatch



CloudTrail



Kinesis



SQS



Billing



S3



Config Rule



Inspector



# Data Analysis and Visualization

---

# AWS App

## Data Analysis and Visualization

Dashboard

Network Topology

Overlay Layers

Change Playback

Timeline

Real-time Status

Security Strategy

Forecast Analysis

RI Planning

Anomaly Detection

Smart Alerting

Best Practice



Saved Search



Report  
Acceleration



Lookup



Data Models



Summary

↑

Data Transformation  
Search Acceleration  
Machine Learning



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Windows NT 6.0; rv:38.0) Gecko/20100801 Firefox/38.0"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL1E2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Windows NT 6.0; rv:38.0) Gecko/20100801 Firefox/38.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Windows NT 6.0; rv:38.0) Gecko/20100801 Firefox/38.0"
130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Windows NT 6.0; rv:38.0) Gecko/20100801 Firefox/38.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/5.0 (Windows NT 6.0; rv:38.0) Gecko/20100801 Firefox/38.0"

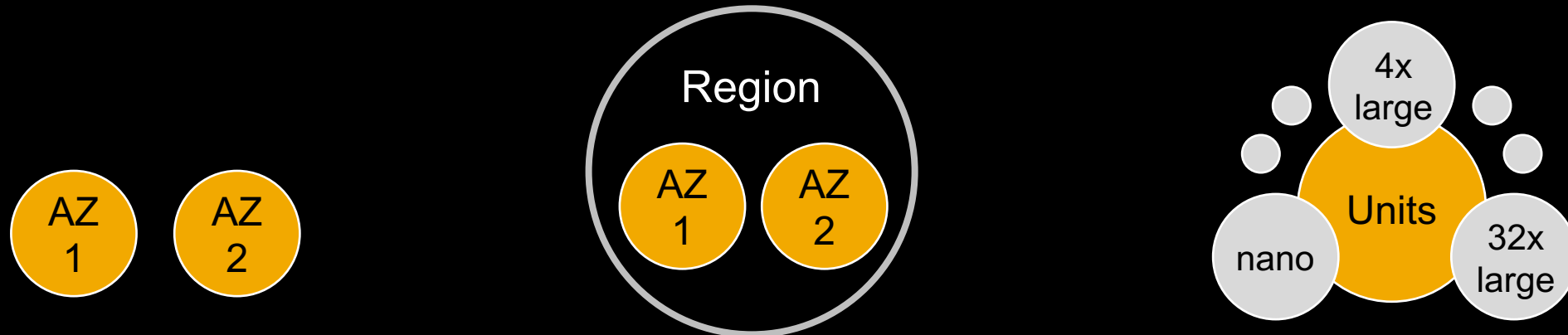
```



# Key New Features in AWS App 5.1

## Reserved Instance Inventory and Planner

- ▶ Add support of “Instance Size Flexibility”



**AZ Scope**

**Regional Benefit**

**Instance Size Flexibility**



# Key New Features in AWS App 5.1

## Reserved Instance Inventory and Planner

### ► Add support of “Instance Size Flexibility”

<i>i</i>	Account ID	Region	Platform	Tenancy	Instance type	Existing RIs	Optimal RIs
>	880758383673	EU (Ireland)	Linux/UNIX	default	c4	48 (unit)	4 (unit)
>	880758383673	Asia Pacific (Tokyo)	Linux/UNIX	default	t1	0 (unit)	0.5 (unit)
✓	880758383673	US West (N. California)	Linux/UNIX	default	t2	5 (unit)	1 (unit)

#### Existing RIs:

You already had 3 reserved instances in this category, converting to unit : 5 = 2 x 2 (medium) + 1 x 1 (small).

- 2 t2.medium with Region scope
- 1 t2.small with Region scope

#### Optimal RIs:

Optimal reserved instances are 1 in unit without considering existing ones.

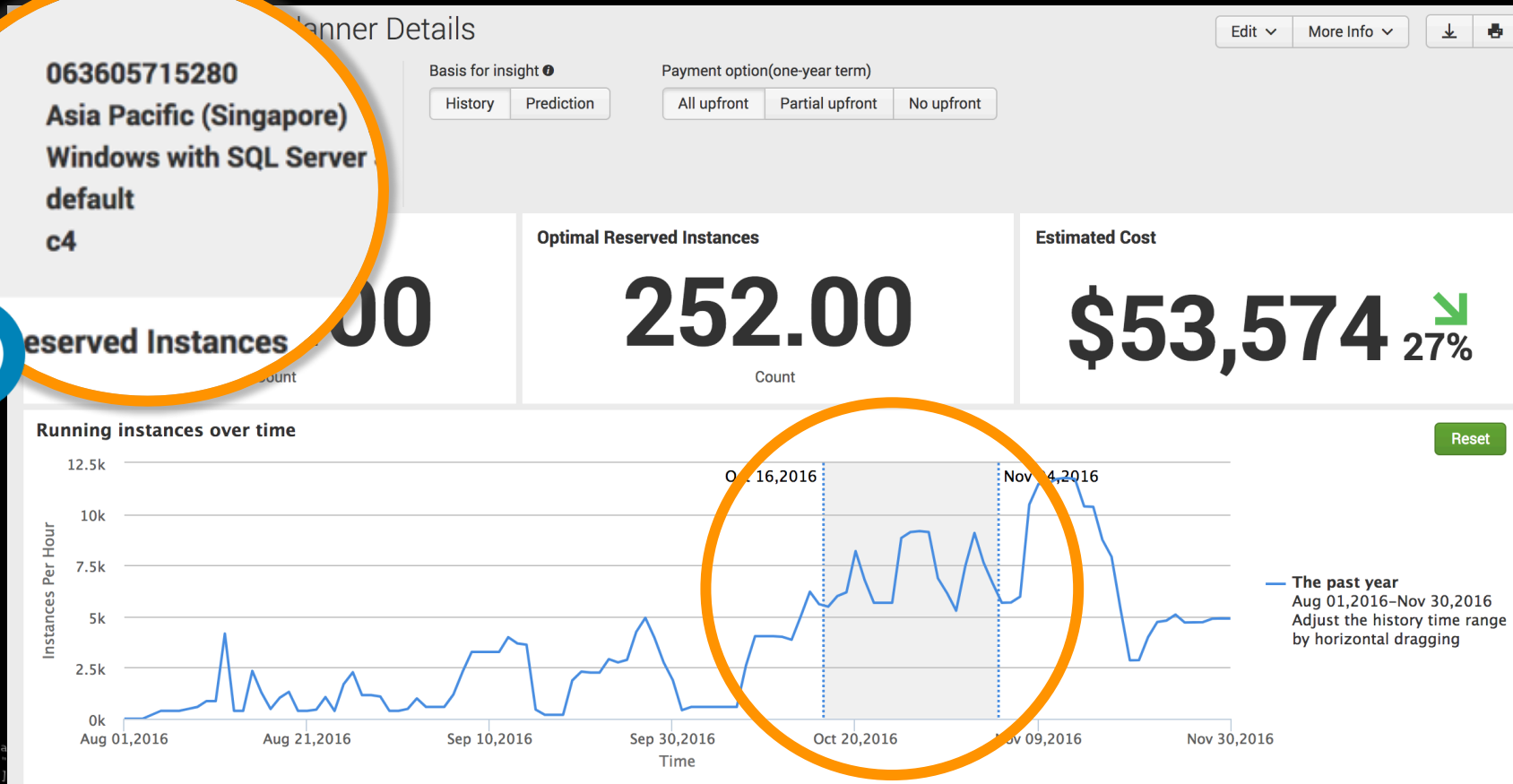
With instance size flexibility, any combination of instance type from the t2 family can get your RI benefit. For example:

- 1 = 4 x 0.25 (nano)
- 1 = 1 x 1 (small)

# Key New Features in AWS App 5.1

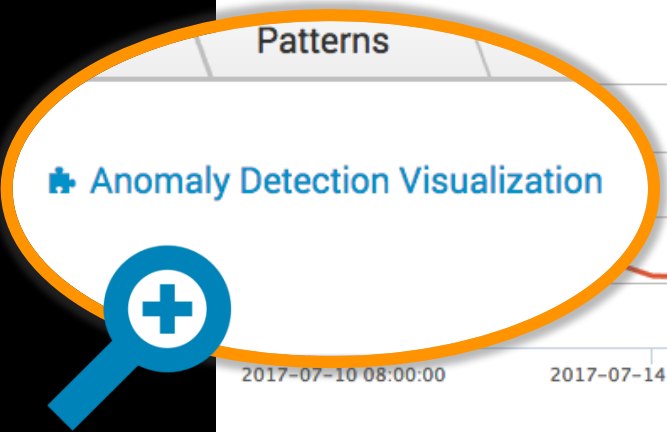
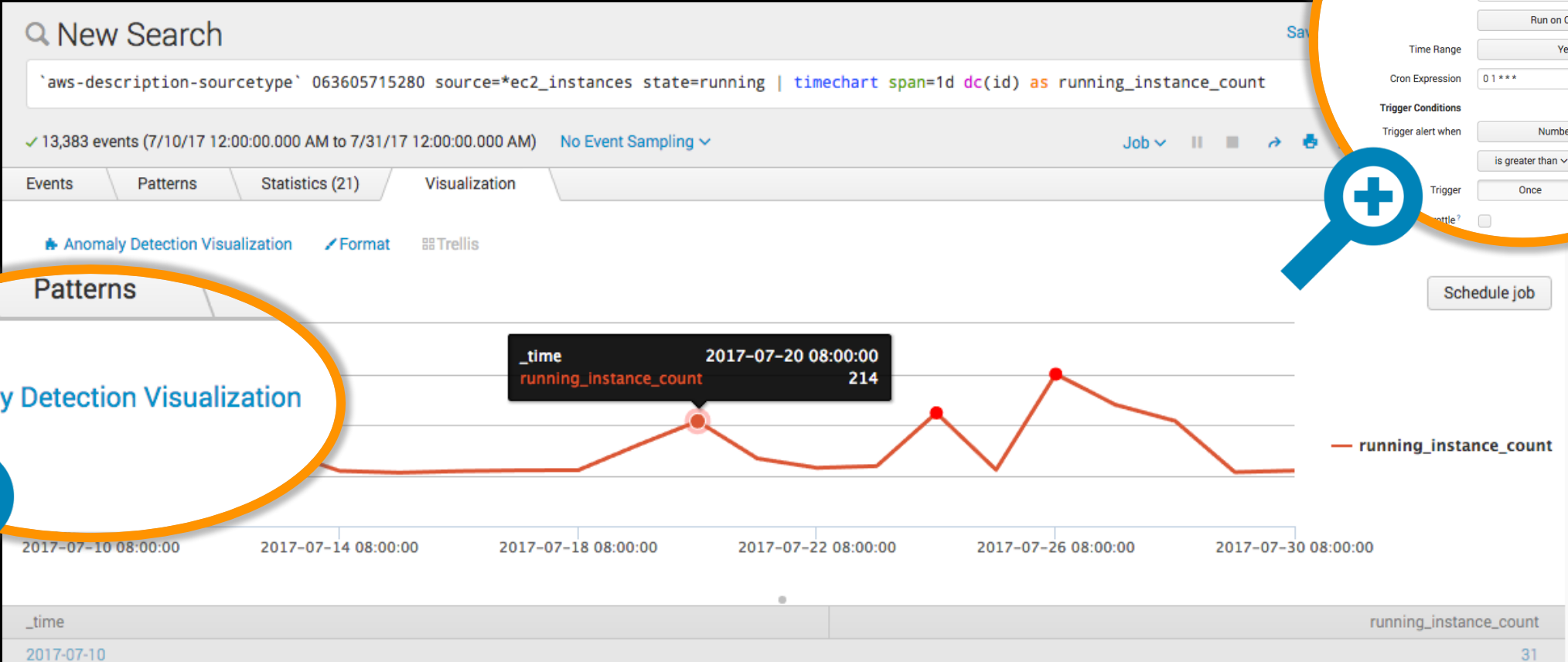
## Reserved Instance Inventory and Planner

- ▶ Add support of Platform and Tenancy in RI planer
- ▶ Support window selection in RI Planer



# Key New Features in AWS App 5.1

## Anomaly Detection Modular Visualization



# Key New Features in AWS App 5.1

## Dedicated Dashboard for Anomaly Detection

Anomaly Detection Overview Edit Export ...

Name:  Priority:  Schedule type:  Tags (match all):  Time Range:  [Hide Filters](#)

**Anomaly Trends**

Date	# of error of API calls grouped by user	# of instance launched	# of running instances
Mon Jul 24 2017	0	0	0
Wed Jul 26	3	1	1
Fri Jul 28	3	0	0
Sun Jul 30	0	0	0

**Latest 100 Anomalies**

_time	Job name	Field name	Value	Severity
2017-07-27	# of error of API calls grouped by user	911	66	High
2017-07-27	# of error of API calls grouped by user	lambda_s3	72	High
2017-07-27	# of error of API calls grouped by user	vpc_policy	18	High
2017-07-26	# of error of API calls grouped by user	azhang	328	Critical
2017-07-26	# of error of API calls grouped by user	lambda_s3	50	Critical
2017-07-26	# of error of API calls grouped by user	zhang	7	Critical
2017-07-26	# of running instances	running_instance_count	400	High
2017-07-26	# of instance launched	runInstancesCount	386	High

**Anomaly Detection Jobs**

i	Name	Priority	Schedule type	Tags	Last anomaly time	Action
✓	# of error of API calls grouped by user	High	Daily	security	2017-07-27 00:00:00	<a href="#">Open in Search</a> <a href="#">Edit</a> <a href="#">Learn more</a>
>	# of instance launched	High	Daily	cloudtrail,ec2	2017-07-26 00:00:00	<a href="#">Open in Search</a> <a href="#">Edit</a>
>	# of running instances	Medium	Daily	ec2	2017-07-26 00:00:00	<a href="#">Open in Search</a> <a href="#">Edit</a>

**Job Details for # of error of API calls grouped by user**

**Job Details**  
 Search: ..... `aws-cloudtrail((aws\_account\_id="063605715280"), (region="\*")) userName="\*" | `cloudtrail\_service("\*, 1") | eval error=(errorCode!="success", 0, 1) | timechart limit=20 useother=false span=1 d sum(error) by userName | fillnull  
 Description: .....

**Alert Settings**  
 Name: ..... AWS 911: Too many error of API calls triggered by specific user  
 App: ..... splunk\_app\_aws  
 Permissions: ..... Private. Owned by power.  
 Alert Type: ..... Scheduled. Cron Schedule.  
 Trigger Condition: ..... Number of events greater than 0.

- ▶ Manage anomaly detection jobs
- ▶ Manage alerts
- ▶ View anomalies detected



# Key New Features in AWS App 5.1

## Decoupled Dependency of AWS Add-on



- ▶ Not available in hybrid environment
- ▶ Not able to connect multiple forwarders

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-2&product_id=K9-CU-01"
ows NT 5.1; SV1: - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SLDE12ADFF9"
//buttercup-shopping_id=RP-LI-02" 468 125.17.14.101:80 [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"
opping.com/purchase&itemId=EST-26&JSESSIONID=SD5SL9FF1ADFF3" 189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1"

```





# Typical Use Cases

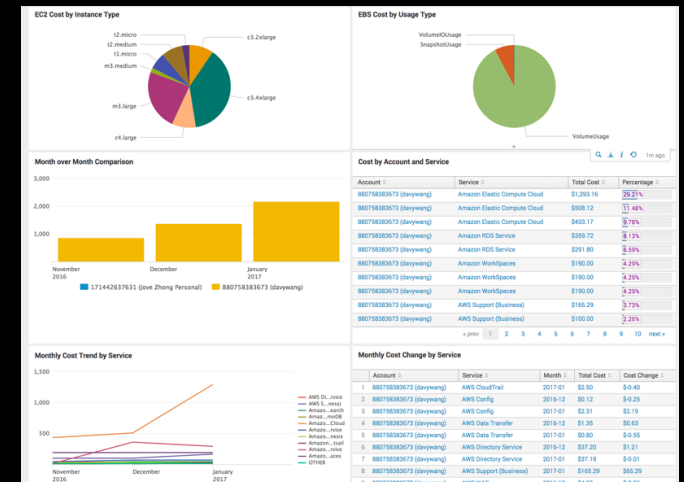
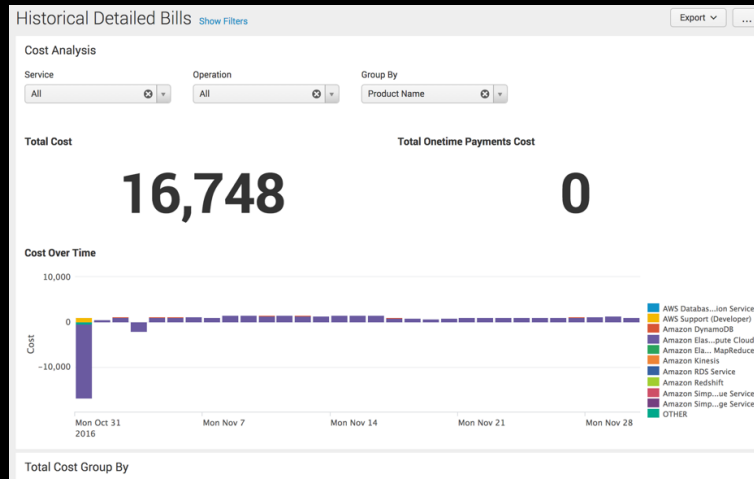
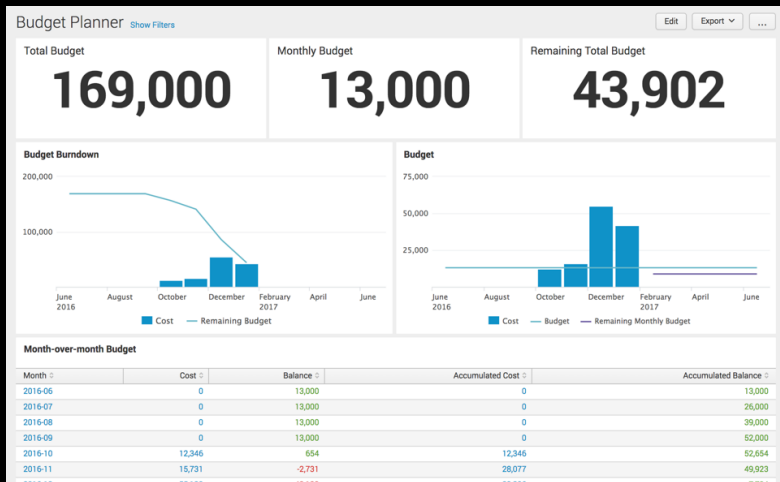
---

# Use Case – Manage Billing Report

## 3 kinds of reports, different granularity

- ▶ CloudWatch Estimated Cost
- ▶ Monthly Report
- ▶ Detailed Billing Report

- Budget planning and tracing
- Cost analysis on different grouping rules
- Cost analysis on customized tags



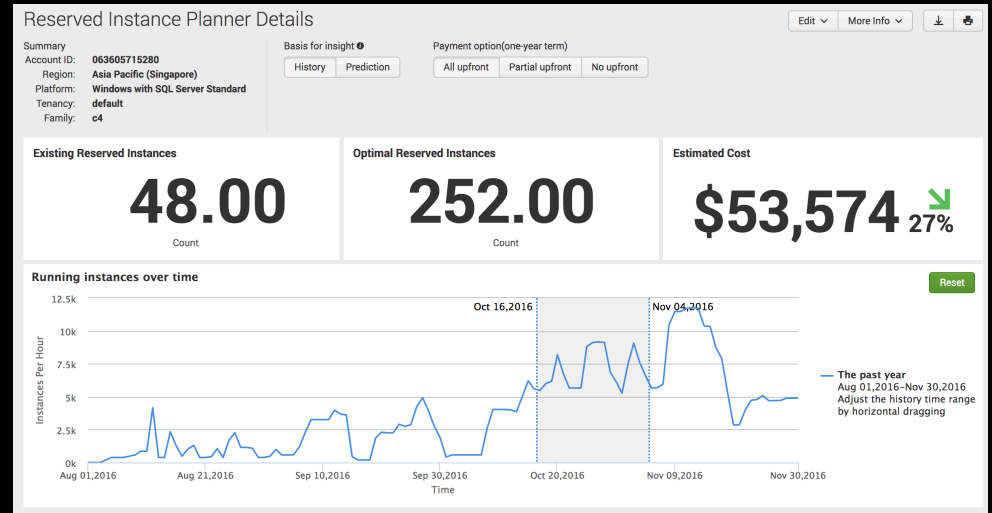
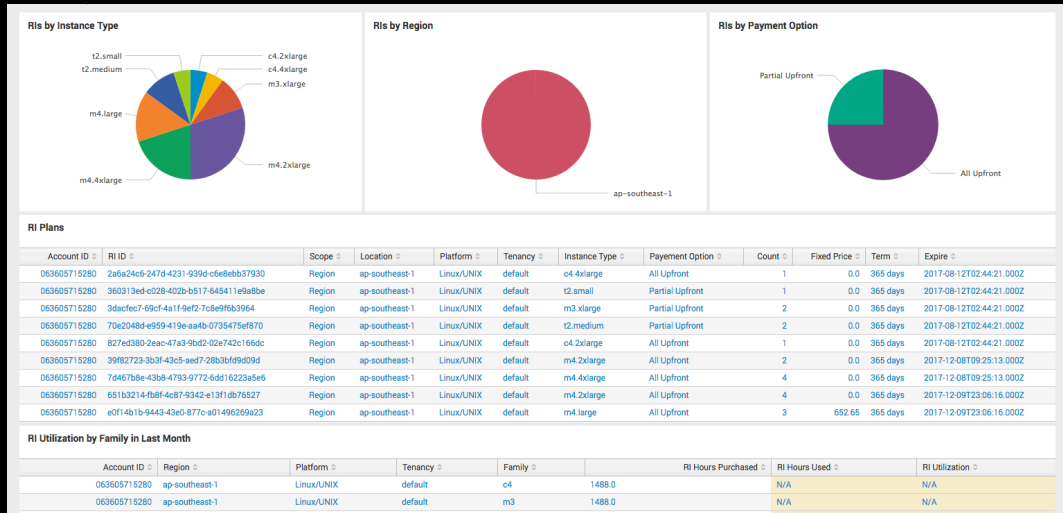
# Case Study – Optimize Reserved Instance

## Statistics of RI

- ▶ Distribution & utilization
- ▶ Detail information

## Best purchase plan of RI

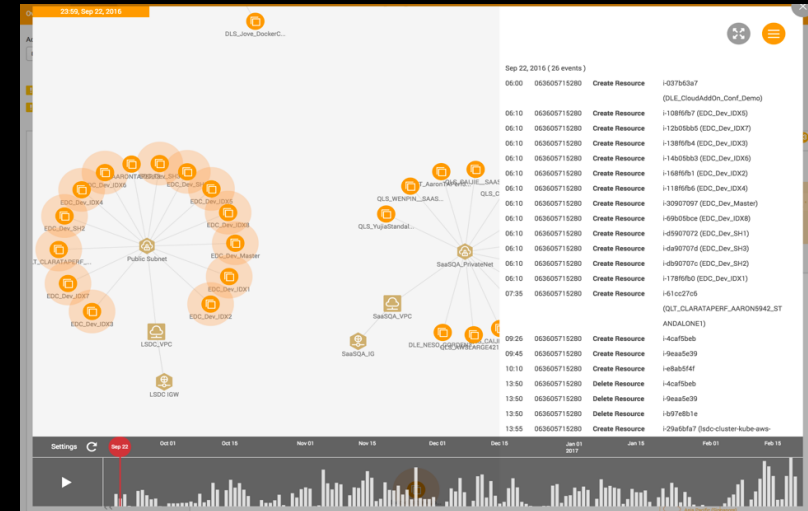
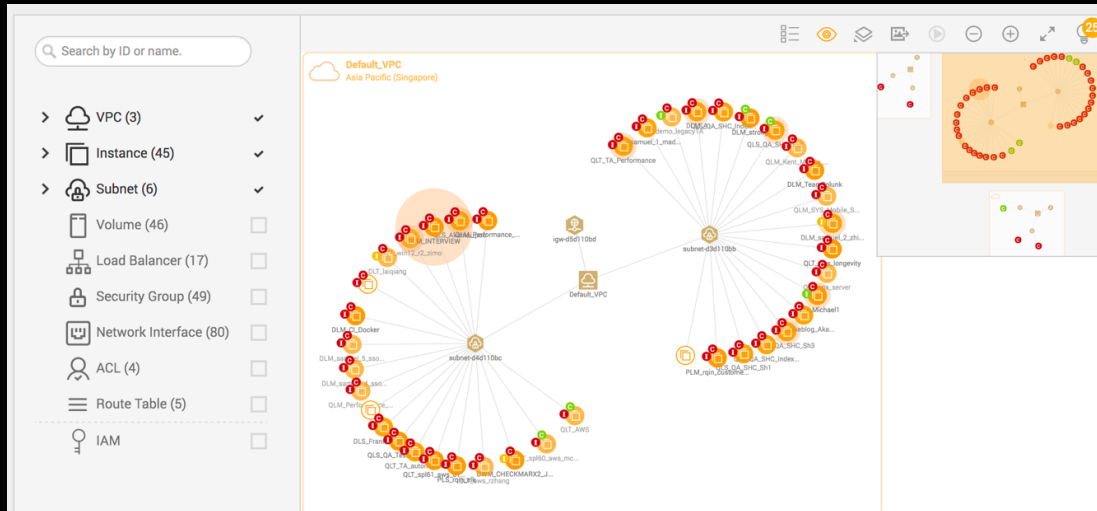
- ▶ Based on historical data
- ▶ Based on forecasting
- ▶ Based on adjusted forecasting
- ▶ Support 3 payment options
- ▶ Support Regional RI
- ▶ Support Size Flexibility



# Case Study – Topology

Interactive network topology  
 Interactive IAM association presenting  
 Export to picture

Multiple overlays  
 Playback of changes



130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FL-SW-01" Operated 20  
 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-20&product\_id=MK11174-0" Operated 20  
 317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-180&product\_id=AV-CB-01&JSESSIONID=SD10SL10E2ADF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item\_id=EST-189" Operated 20  
 125.17.14.10 - - [07/Jan 18:10:56:156] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3" Operated 20  
 468 125.17.14.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3" Operated 20  
 468 125.17.14.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3" Operated 20  
 468 125.17.14.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3" Operated 20  
 468 125.17.14.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3" Operated 20  
 468 125.17.14.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3" Operated 20  
 468 125.17.14.10 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3" Operated 20

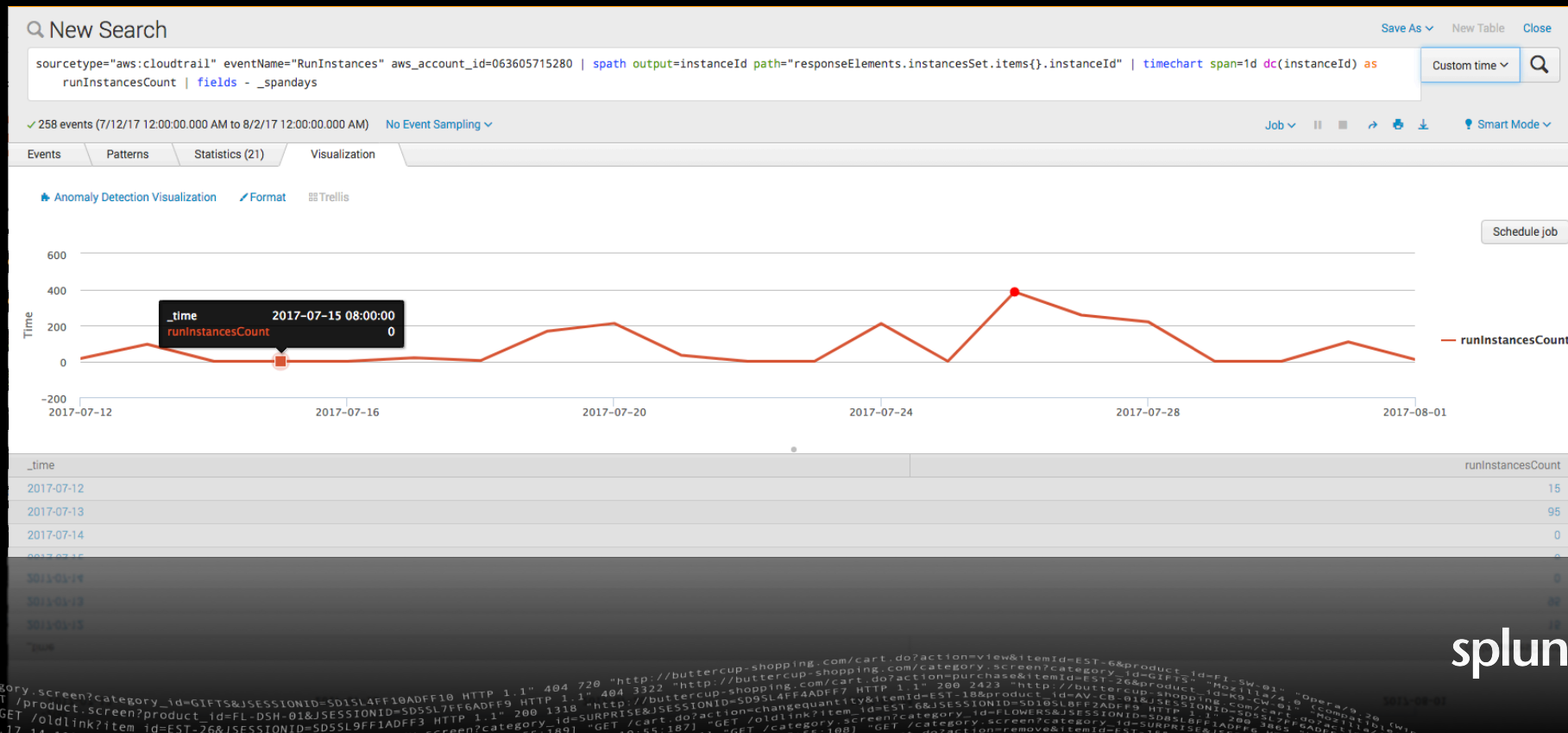
# Case Study – Anomaly Detection

## Custom visualization on any time chart

- ▶ Number of instance launched daily
- ▶ Amount of money spent daily

## Native support of alerting

- ▶ Email, SNS, ServiceNow



# Q&A

---

# Thank You

Don't forget to **rate this session** in the  
.conf2017 mobile app

splunk> .conf2017