splunk> .conf2017

Manage AWS Services

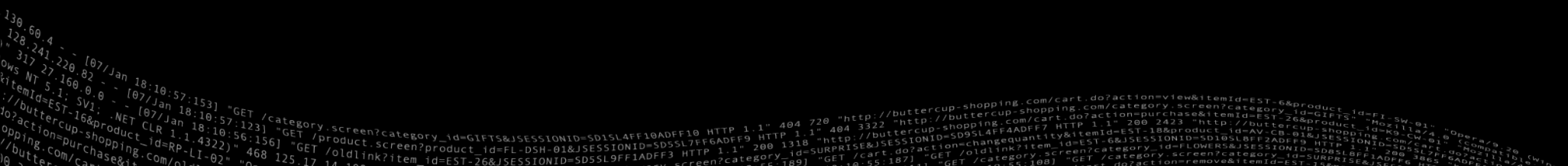
Cost, Security, Best Practice and Troubleshooting

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

September 2017 | Washington, DC

Agenda

- Challenges in Managing Enterprise Level AWS Services
- Get Data In – AWS Add-on
- Data Analysis and Visualization – AWS App
- Case Study
- Q & A



splunk> .conf2017

Challenges

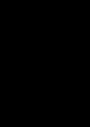
in Managing Enterprise Level AWS Services

Cost Optimization

- Multi accounts
- Budget planning
- RI planning
- Cost forecasting
- Anomaly detection
- Smart alerting

Challenges

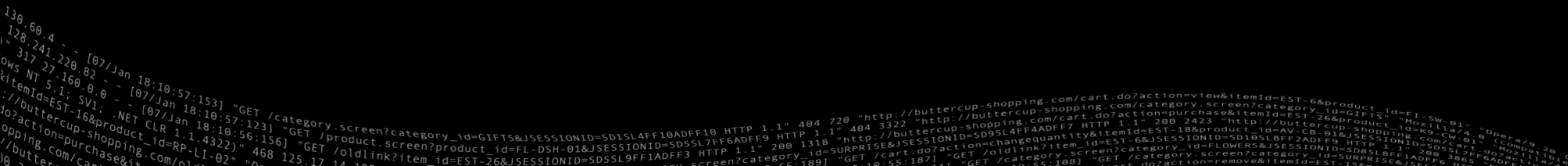
in Managing Enterprise Level AWS Services



Cost Optimization

Security Strategy

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



splunk> .conf2017

Challenges

in Managing Enterprise Level AWS Services

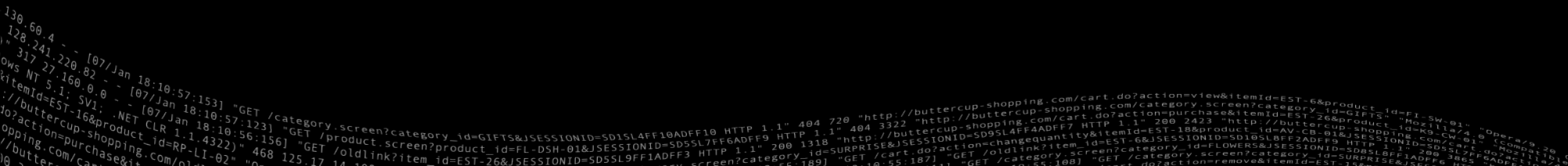
- Cost Optimization
- Security Strategy
- **Best Practice**

- Config Rule
- Inspector
- EC2
- ELB
- EBS
- EIP
- SG
- IAM

Challenges

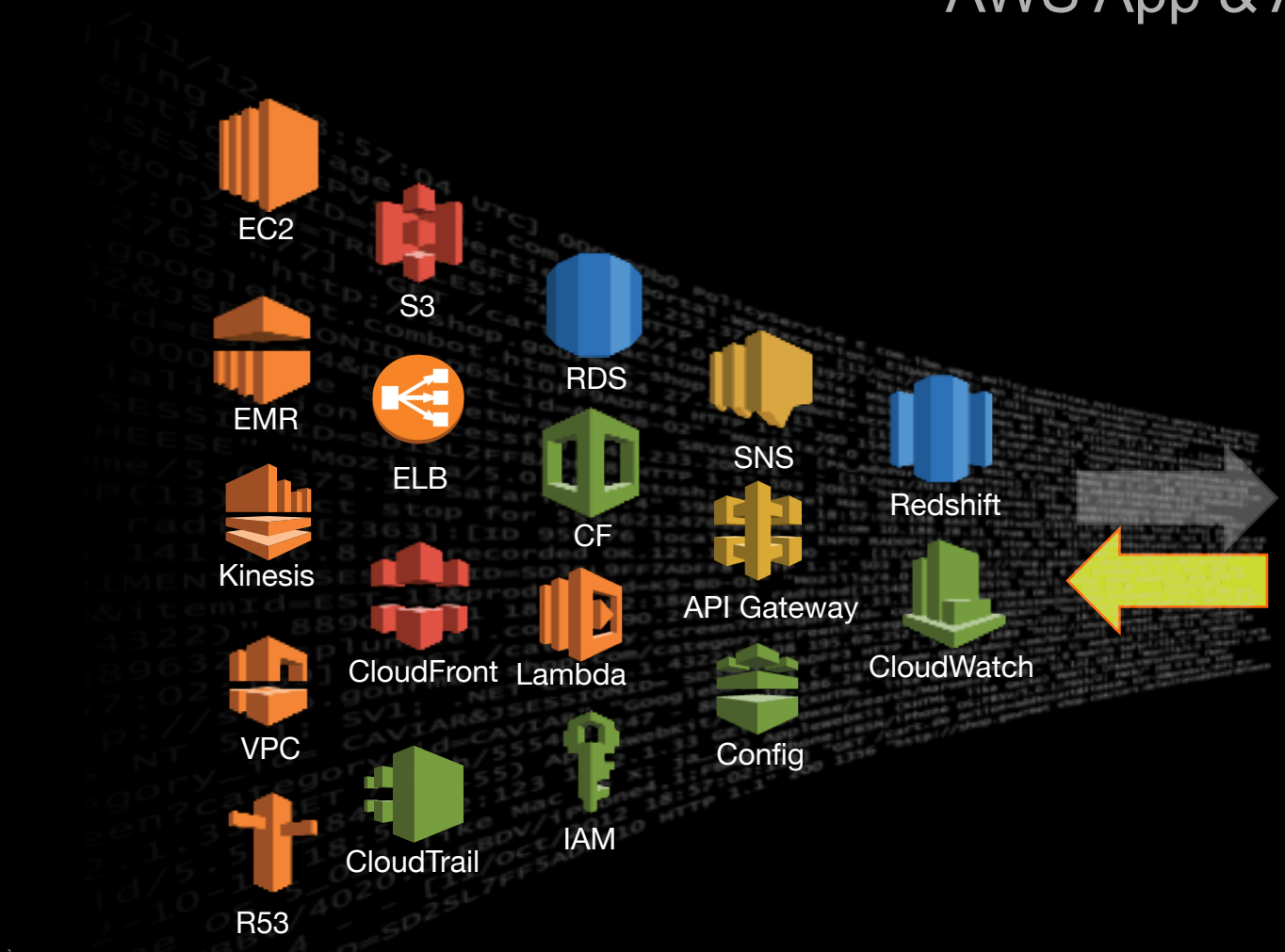
in Managing Enterprise Level AWS Services

- Cost Optimization
- Security Strategy
- Best Practice
- **Troubleshooting**
  - Change management
  - Network topology
  - Association analysis



Splunk Solution

AWS App & Add-on



Explore

Dashboard

Alert

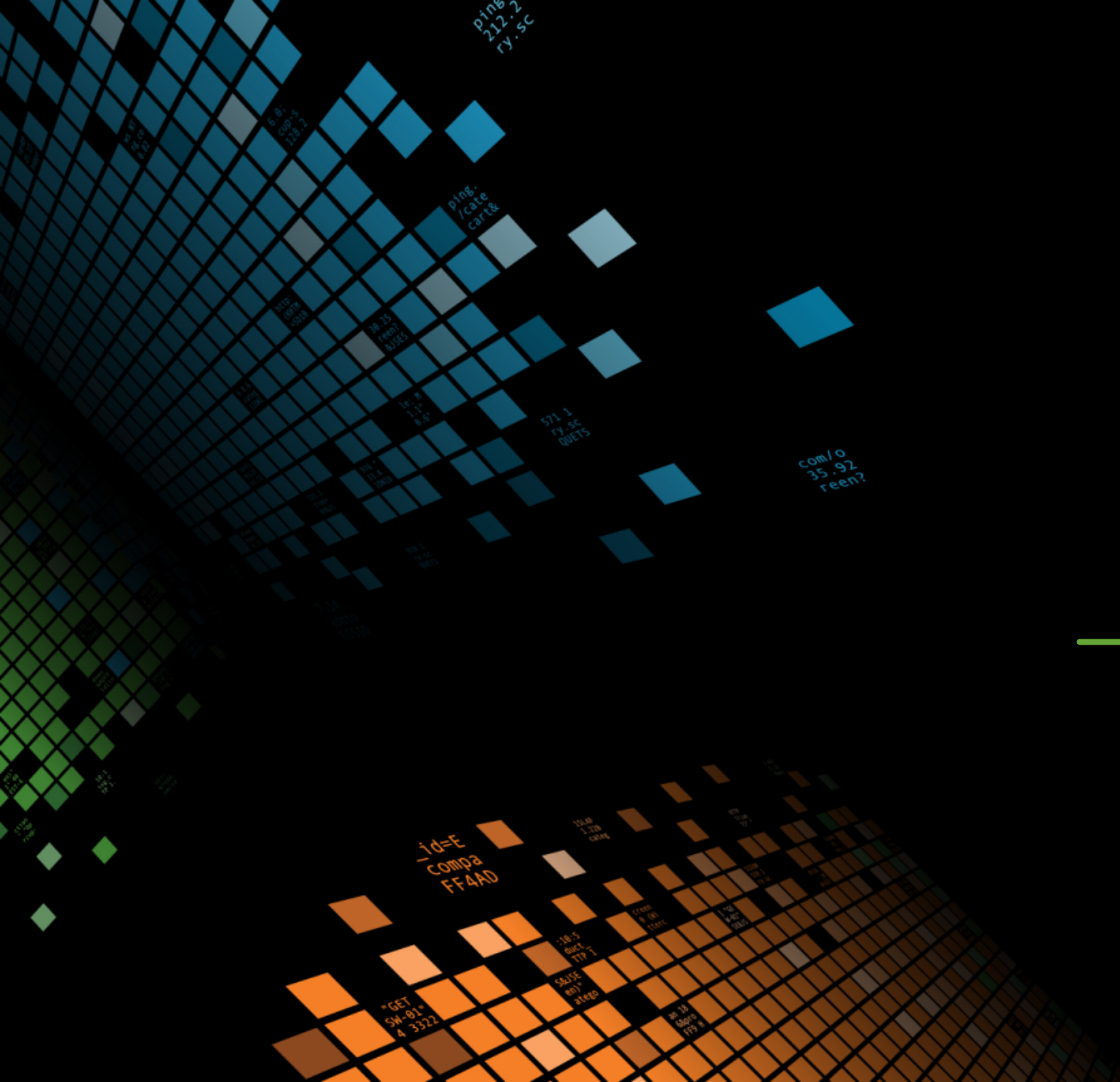
Analyze

Splunk App for AWS

Splunk Add-on for AWS

splunk>

splunk> .conf2017



Get Data In

splunk> .conf2017

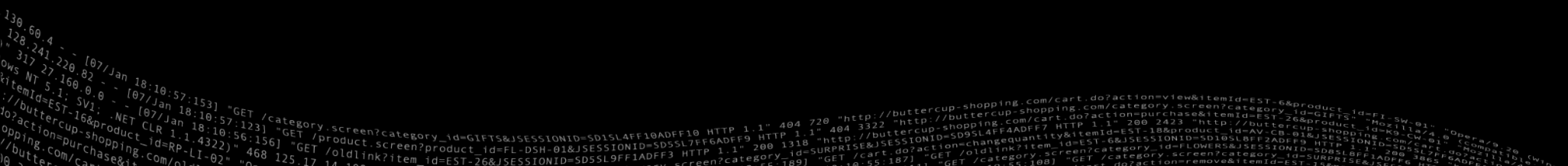
AWS Add-on

Get Data In

- Multi accounts
- Assume Role
- High throughput
- Real-time collection
- Distributed job
- Scale out
- Easy configuration
- Health Monitoring

splunk>

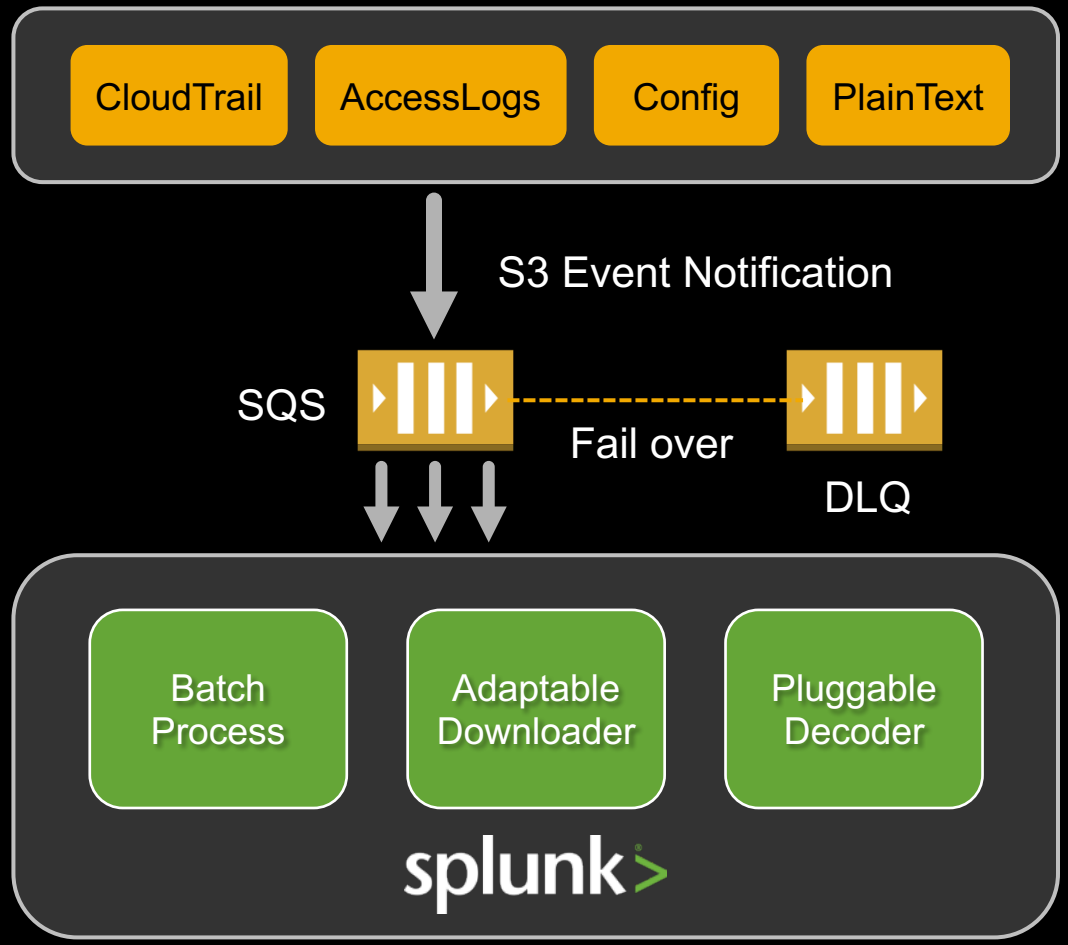
Config | CloudWatch | Kinesis | SQS | CloudTrail | Billing | S3 | ..... More



splunk> .conf2017

Key New Features in AWS Add-on 4.3 and 4.4

New Input: SQS-Based S3

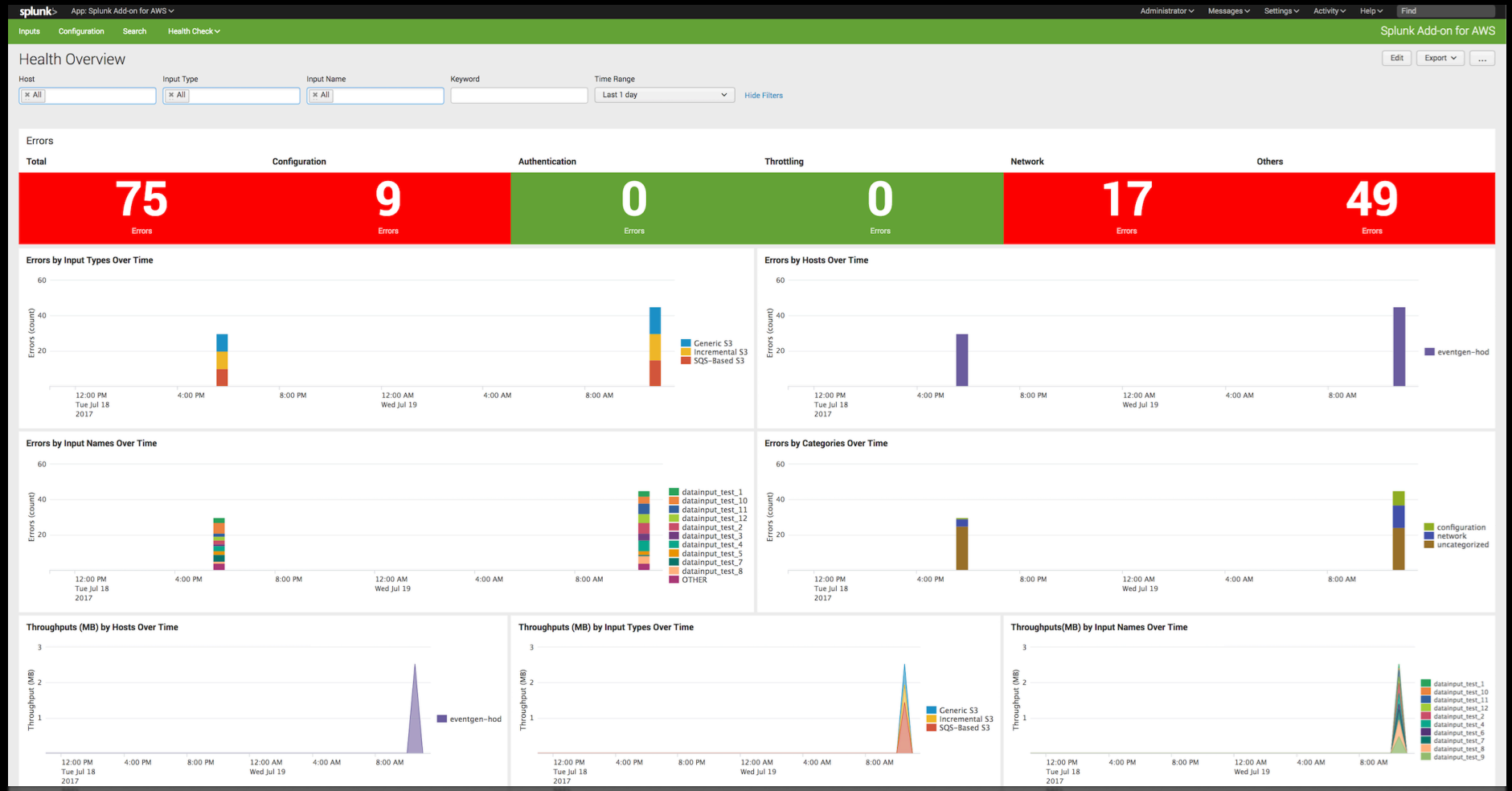


- Higher throughput
- Real-time ingestion
- Cost efficient
- High availability
- Scale out capability

splunk> .conf2017

Key New Features in AWS Add-on 4.3 and 4.4

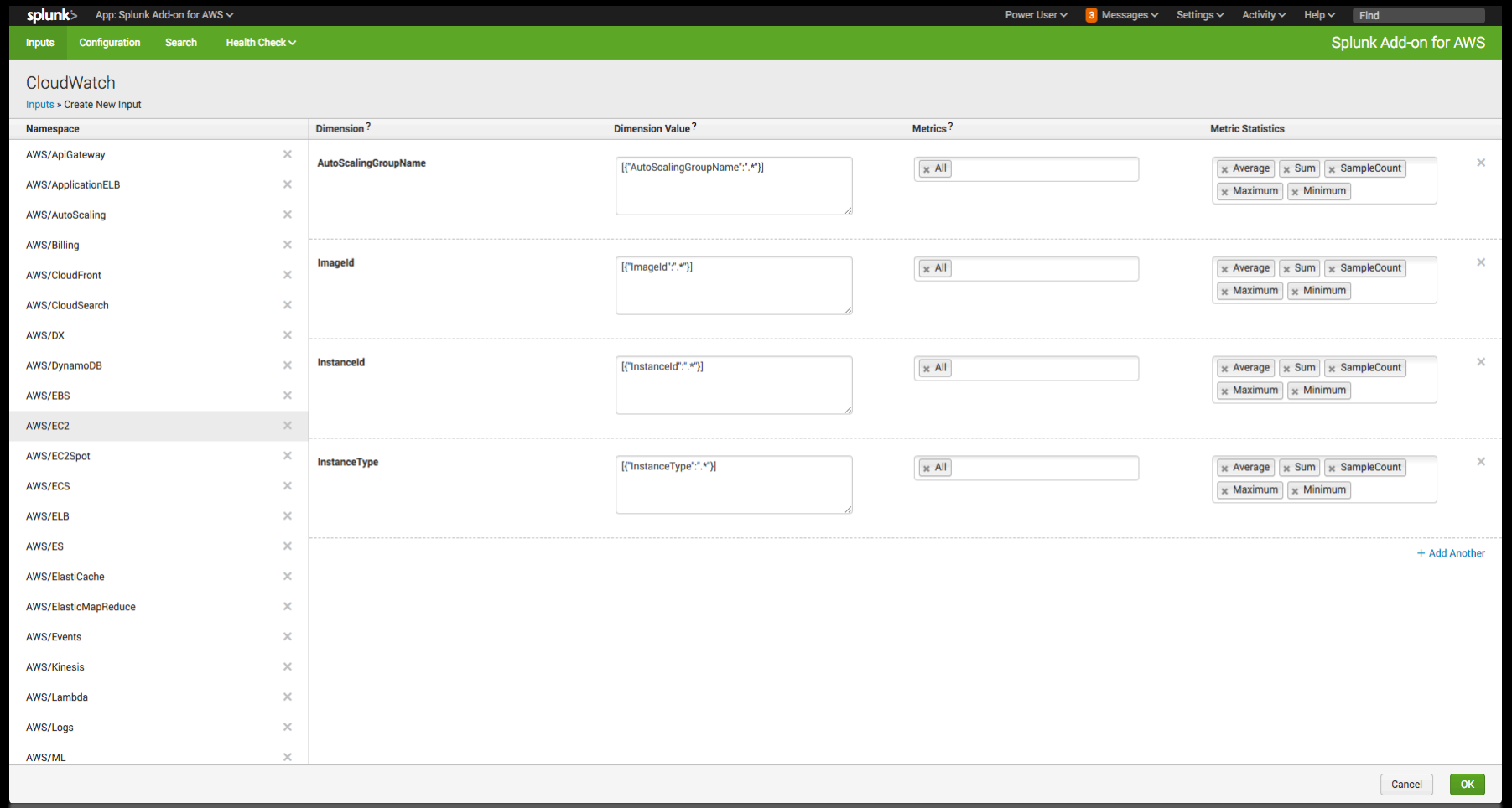
Trouble Shooting: Health Dashboard

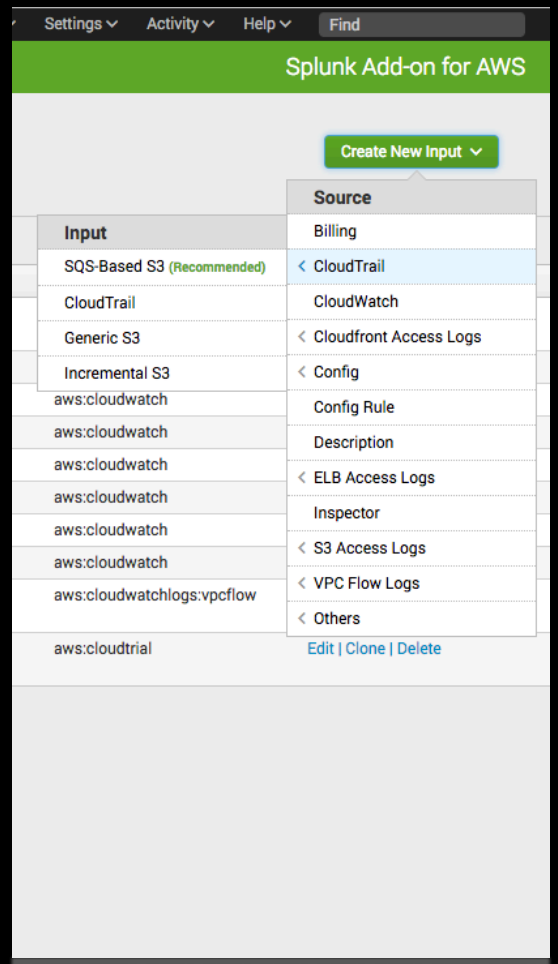


splunk> .conf2017

Key New Features in AWS Add-on 4.3 and 4.4

Easier Configuration: New Designed Configuration GUI

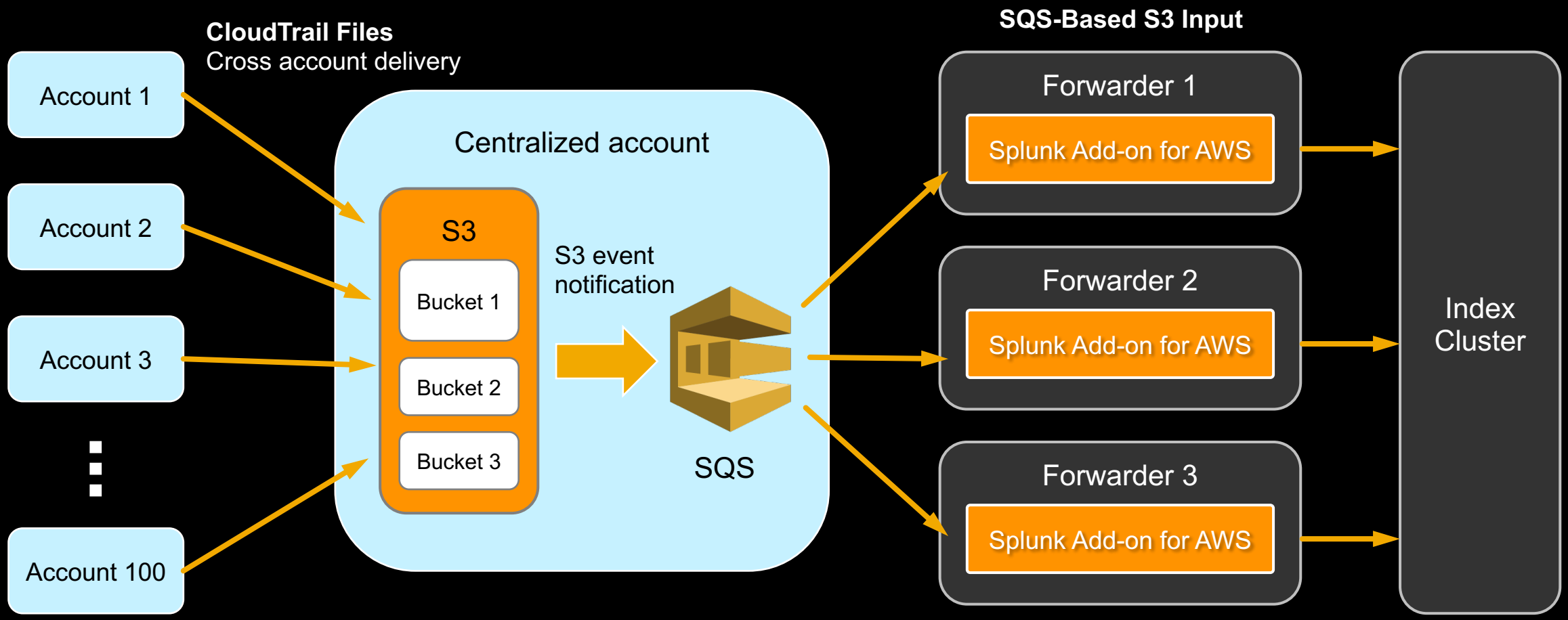




splunk> .conf2017

Best Practice of Get Data In

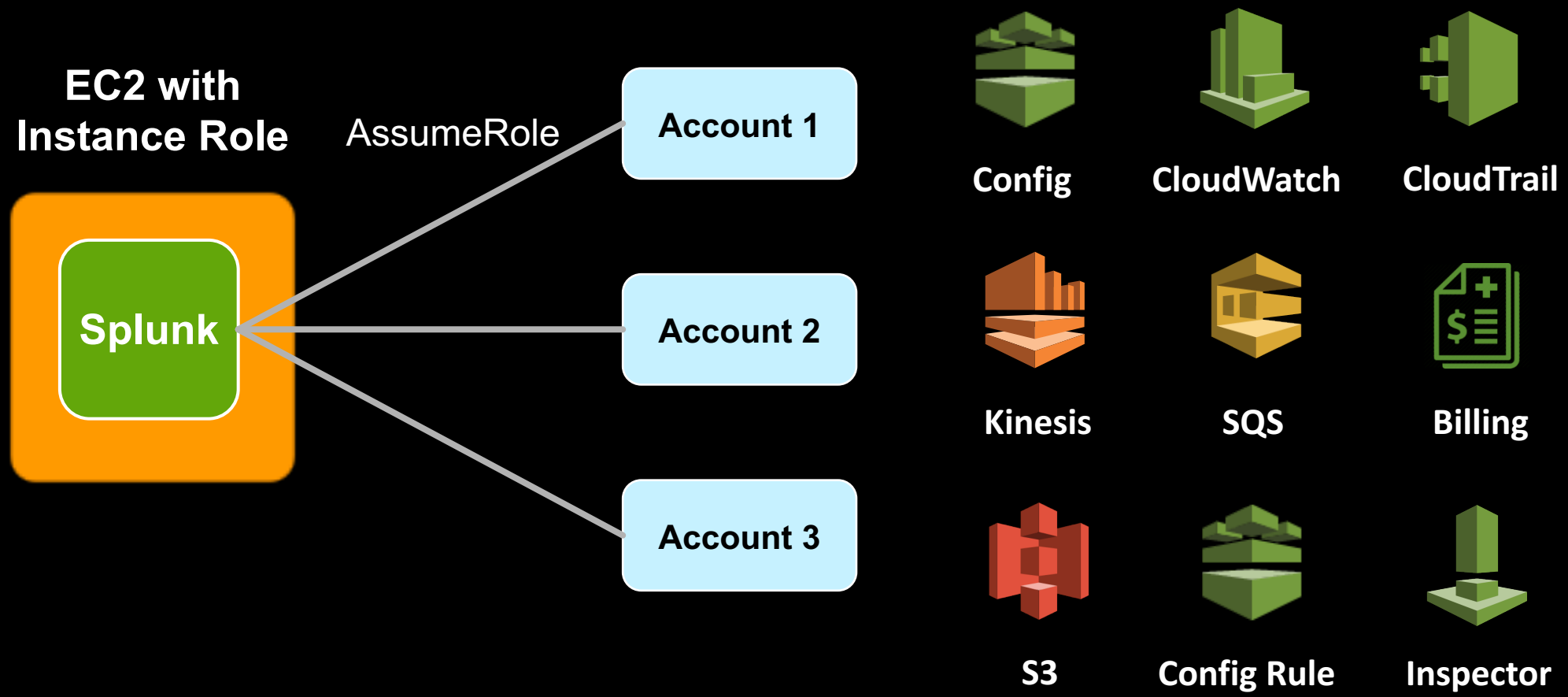
Example 1: Get CloudTrail Data of Hundreds Accounts in Real-time



splunk> .conf2017

Best Practice of Get Data In

Example 2: Get Data More Securely



Data Analysis and Visualization

splunk> .conf2017

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

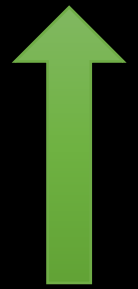
Saved Search

Report Acceleration

Lookup

Data Models

Summary



Data Transformation

Search Acceleration

Machine Learning

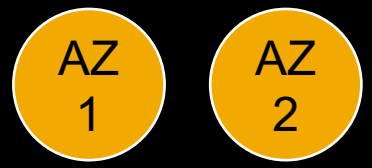
splunk>

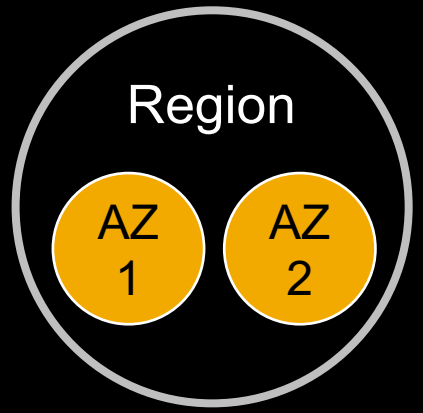
splunk> .conf2017

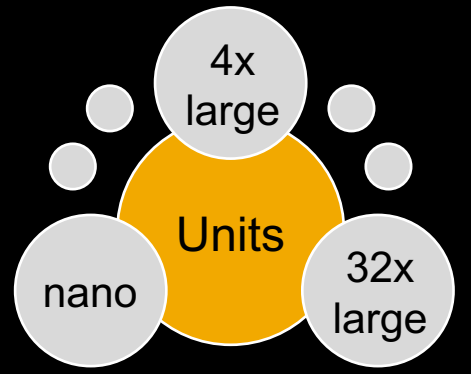
Key New Features in AWS App 5.1

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	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)
v	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.

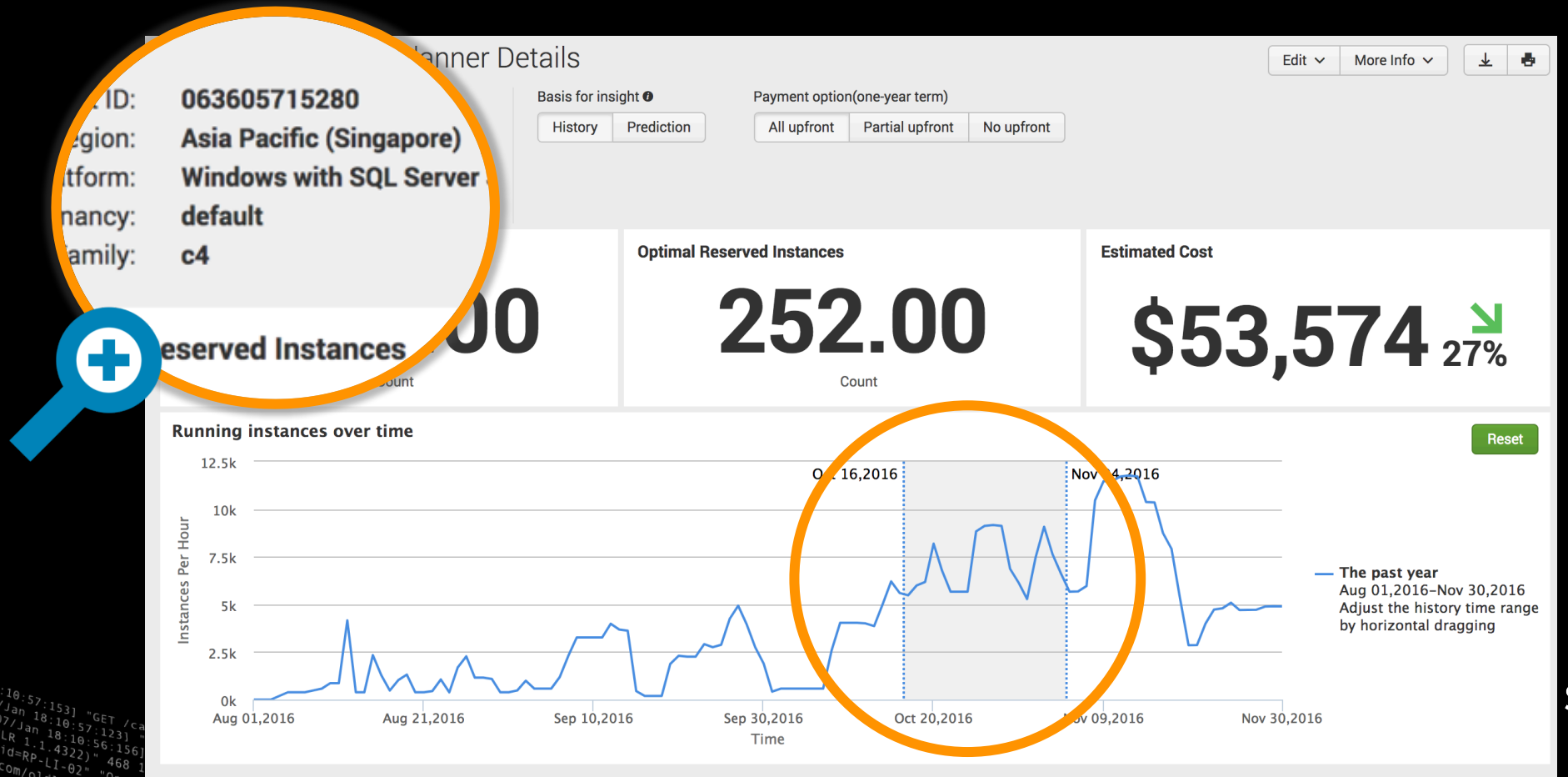
With instance size flexibility, any combination of instance type from the t2 family can get your RI benefit. For example:

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

Key New Features in AWS App 5.1

Reserved Instance Inventory and Planner

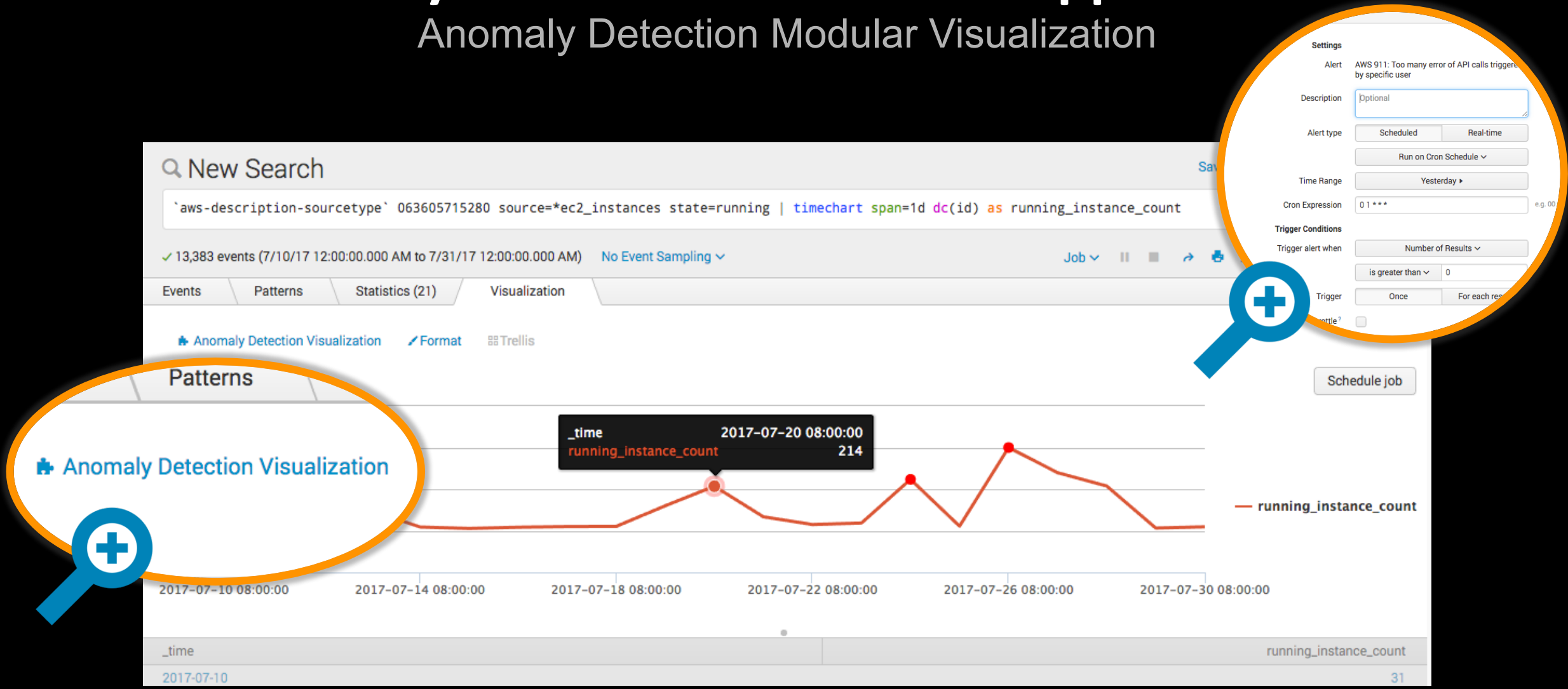
- Add support of **Platform** and **Tenancy** in RI planer
- Support window selection in RI Planer



splunk> .conf2017

Key New Features in AWS App 5.1

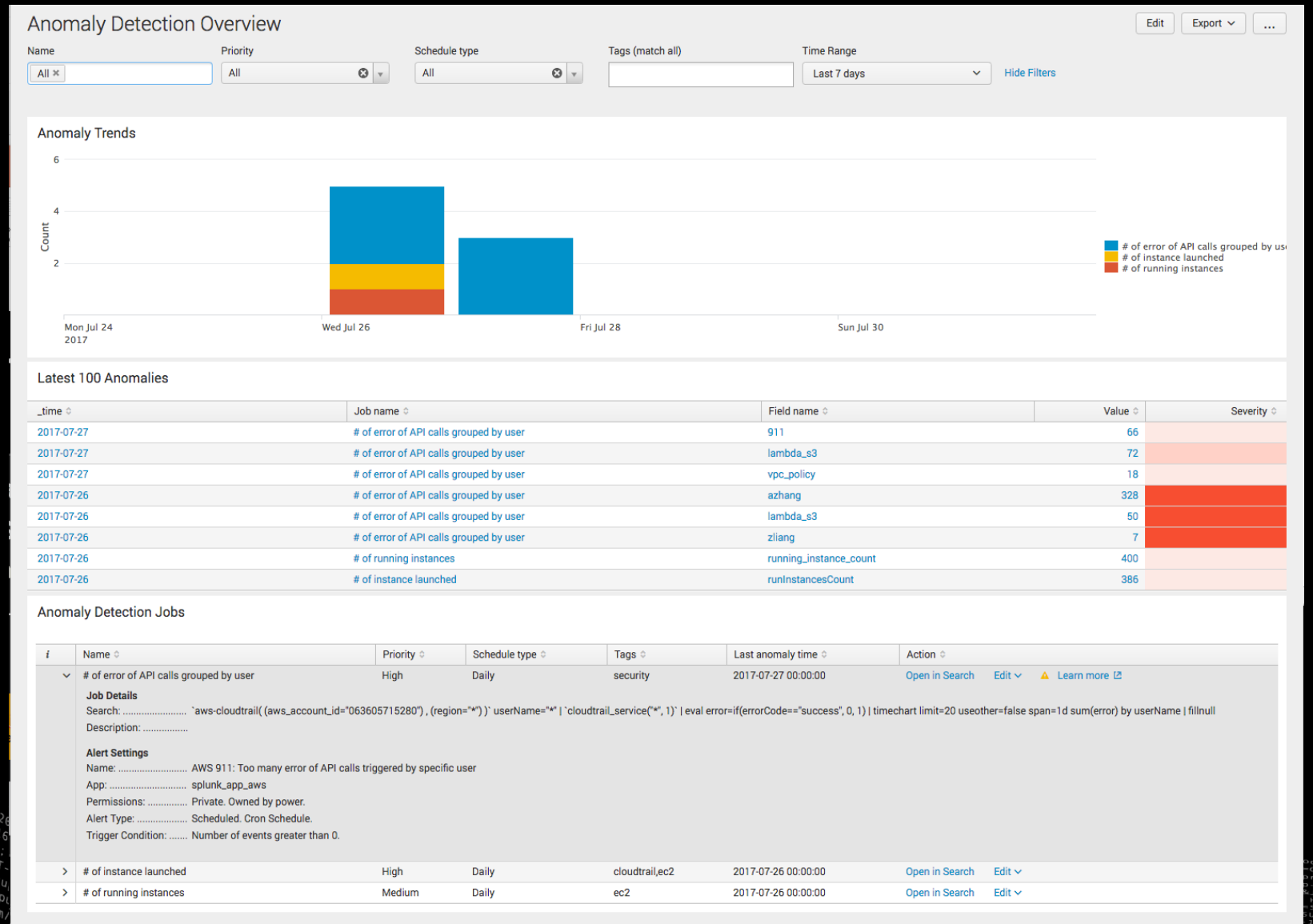
Anomaly Detection Modular Visualization



splunk> .conf2017

Key New Features in AWS App 5.1

Dedicated Dashboard for Anomaly Detection



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

splunk> .conf2017

Key New Features in AWS App 5.1

More Insights

IAM

EIP

ELB

EC2

EBS

SG

COST OPTIMIZING

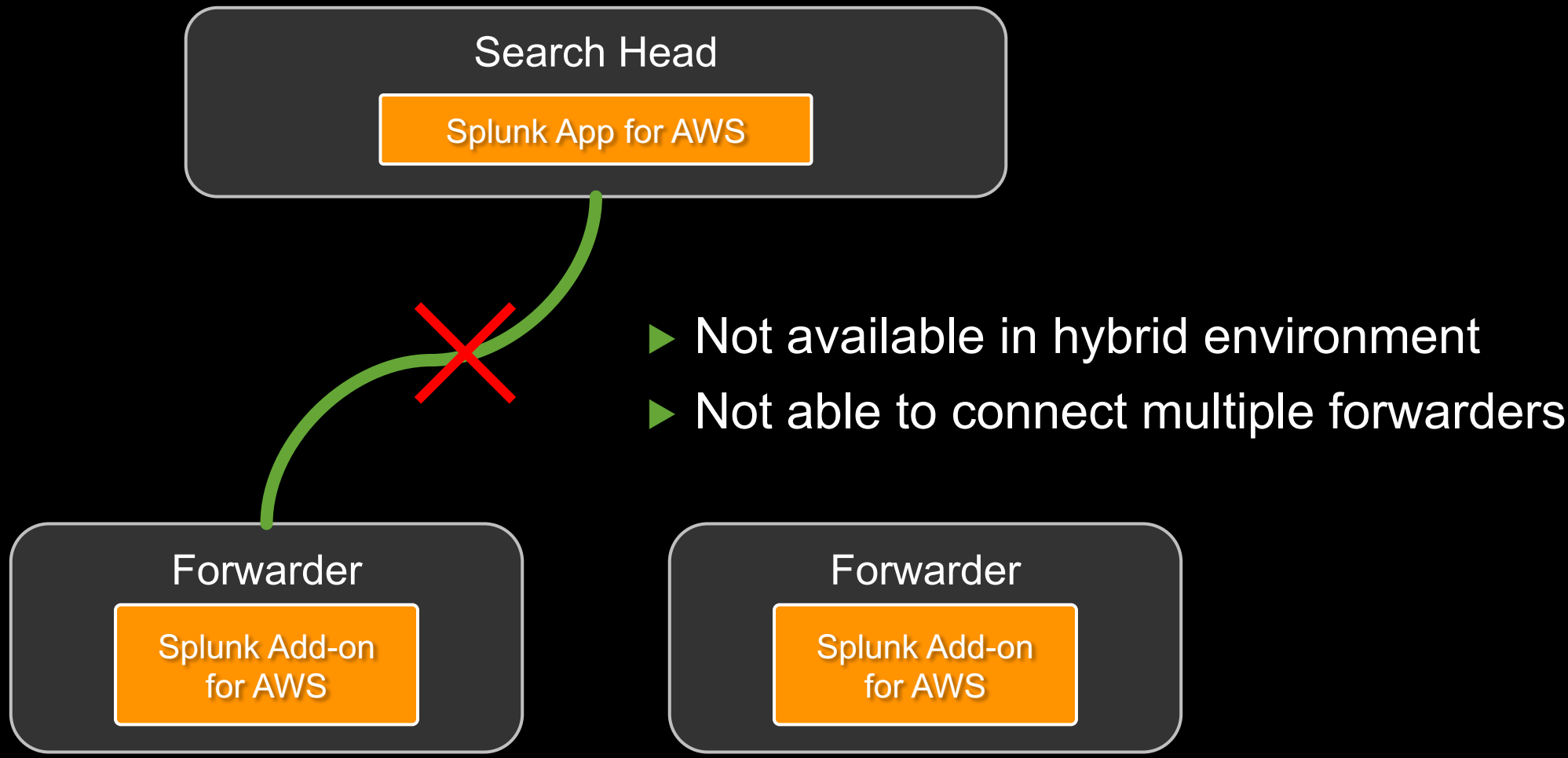
SECURITY

PERFORMANCE

FAULT TOLERANCE

Key New Features in AWS App 5.1

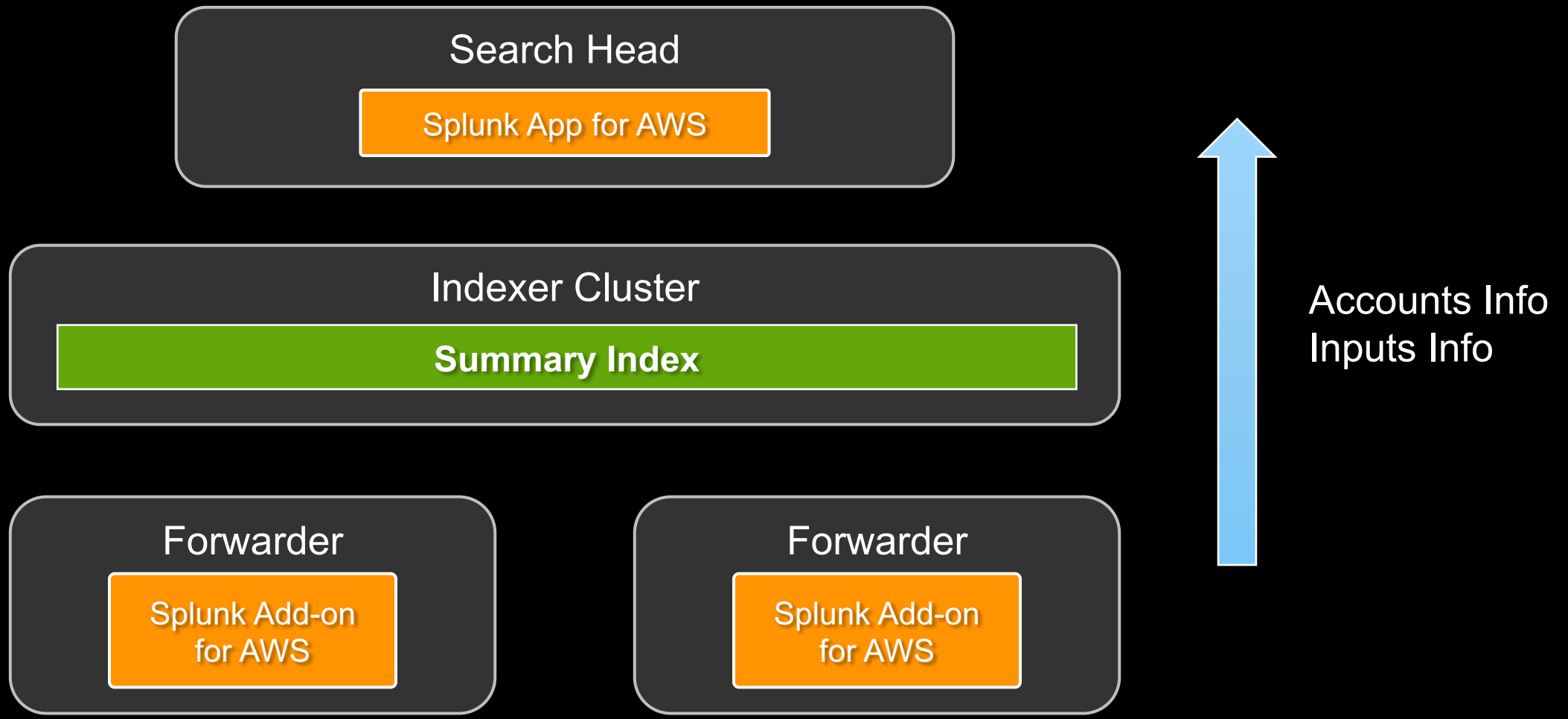
Decoupled Dependency of AWS Add-on



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

Key New Features in AWS App 5.1

Decoupled Dependency of AWS Add-on



Typical Use Cases

Use Case – Manage Billing Report

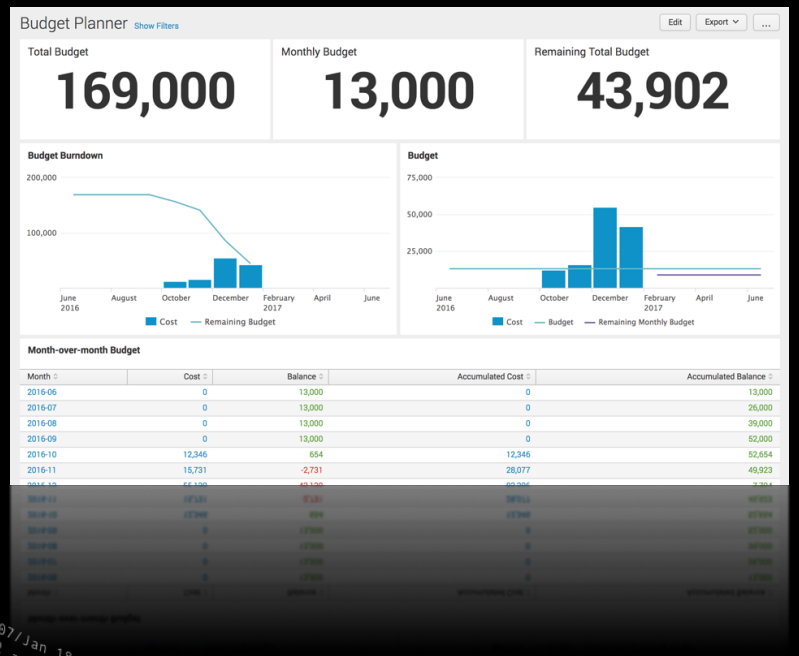
3 kinds of reports, different granularity

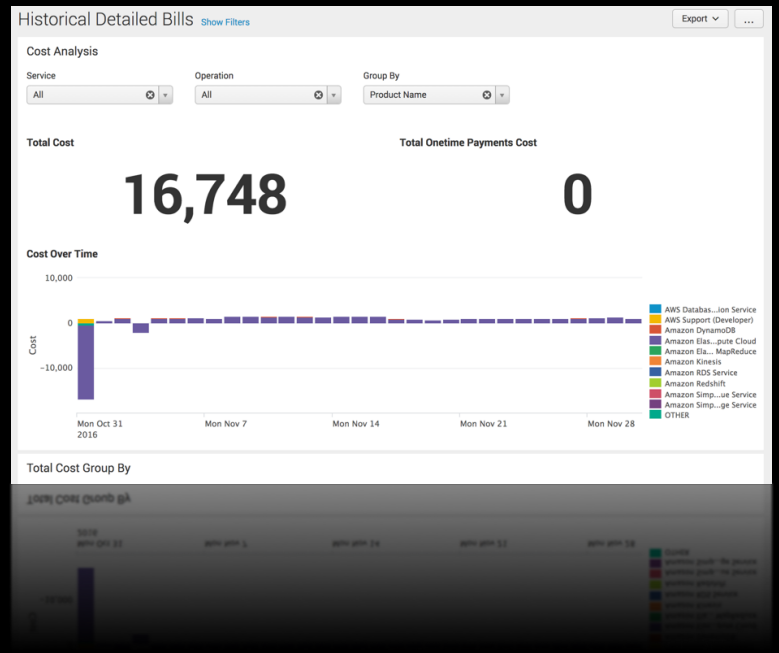
- CloudWatch Estimated Cost
- Monthly Report
- Detailed Billing Report

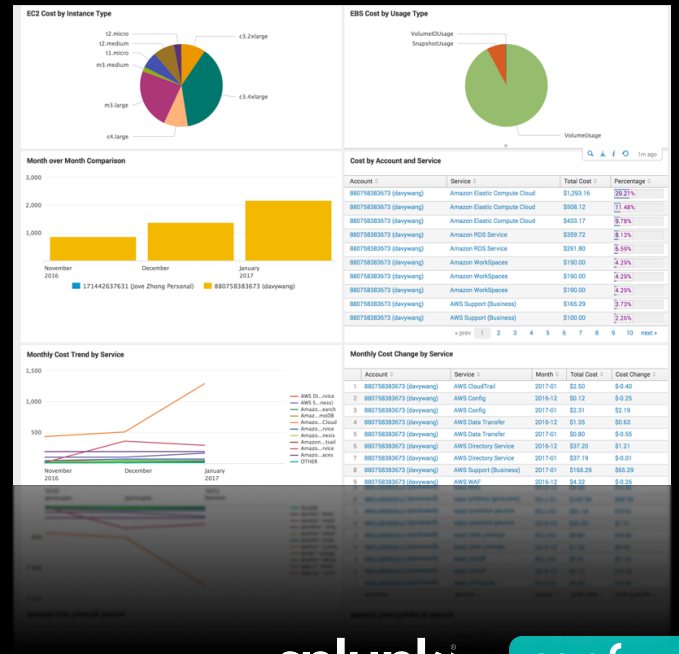
Budget planning and tracing

Cost analysis on different grouping rules

Cost analysis on customized tags







splunk> .conf2017

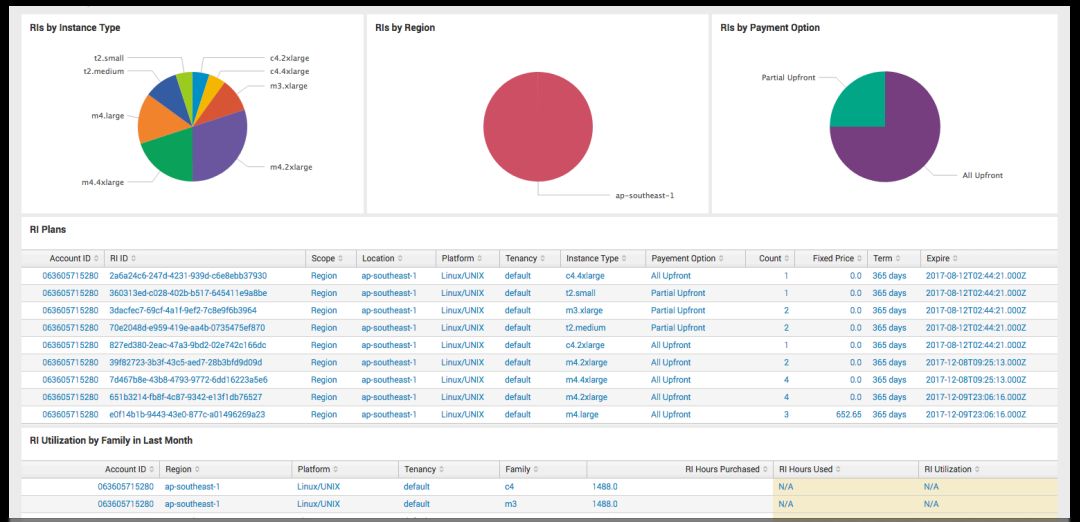
Case Study – Optimize Reserved Instance

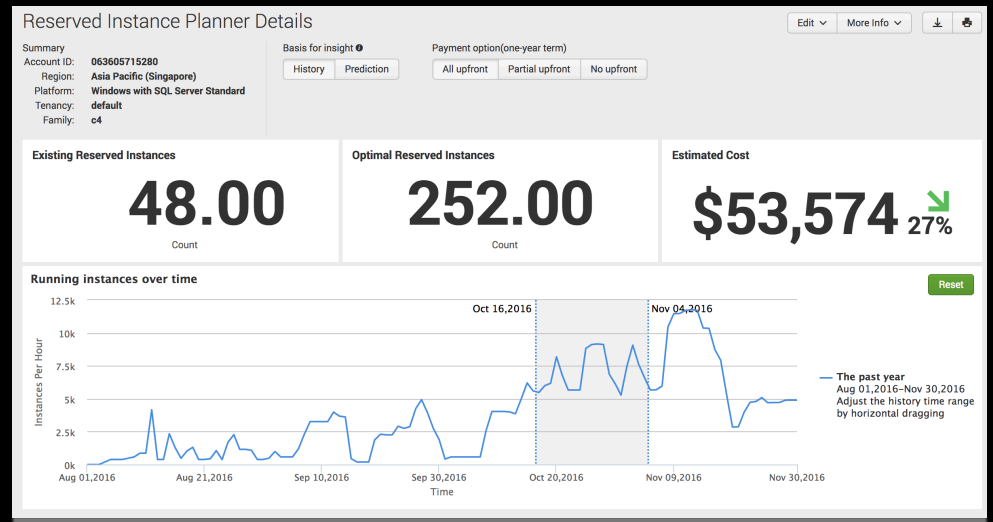
Statistics of RI

- 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





splunk> .conf2017

Case Study – Topology

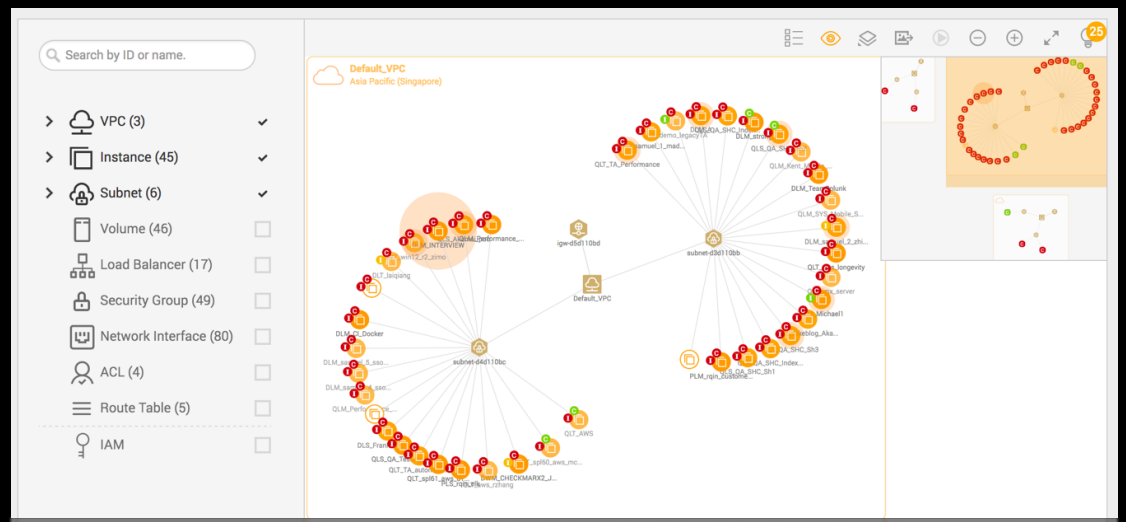
Interactive network topology

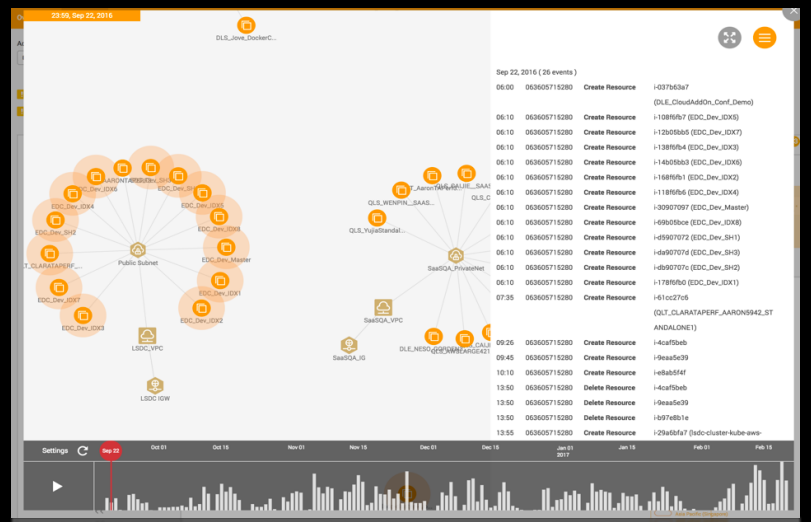
Interactive IAM association presenting

Export to picture

Multiple overlays

Playback of changes





splunk> .conf2017

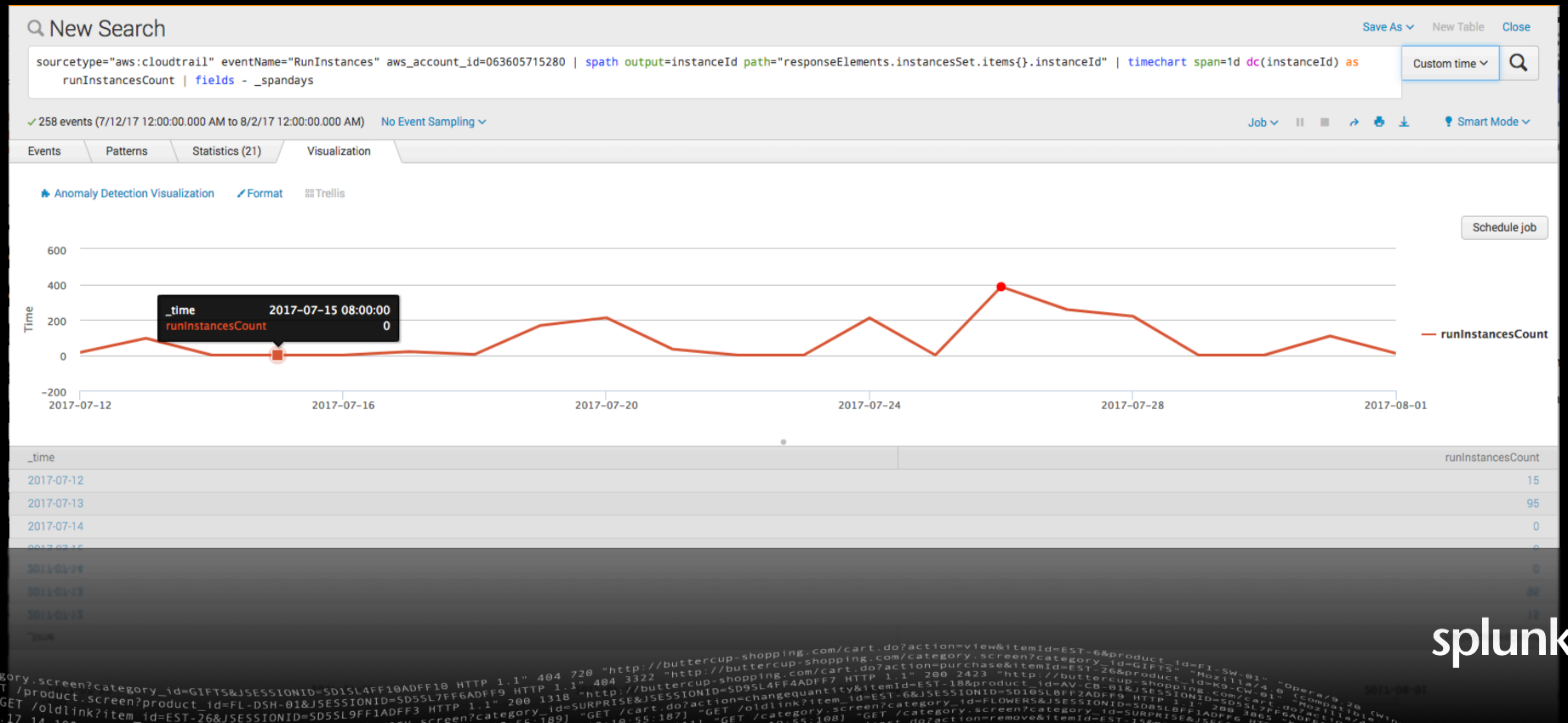
Case Study – Anomaly Detection

Custom visualization on any time chart

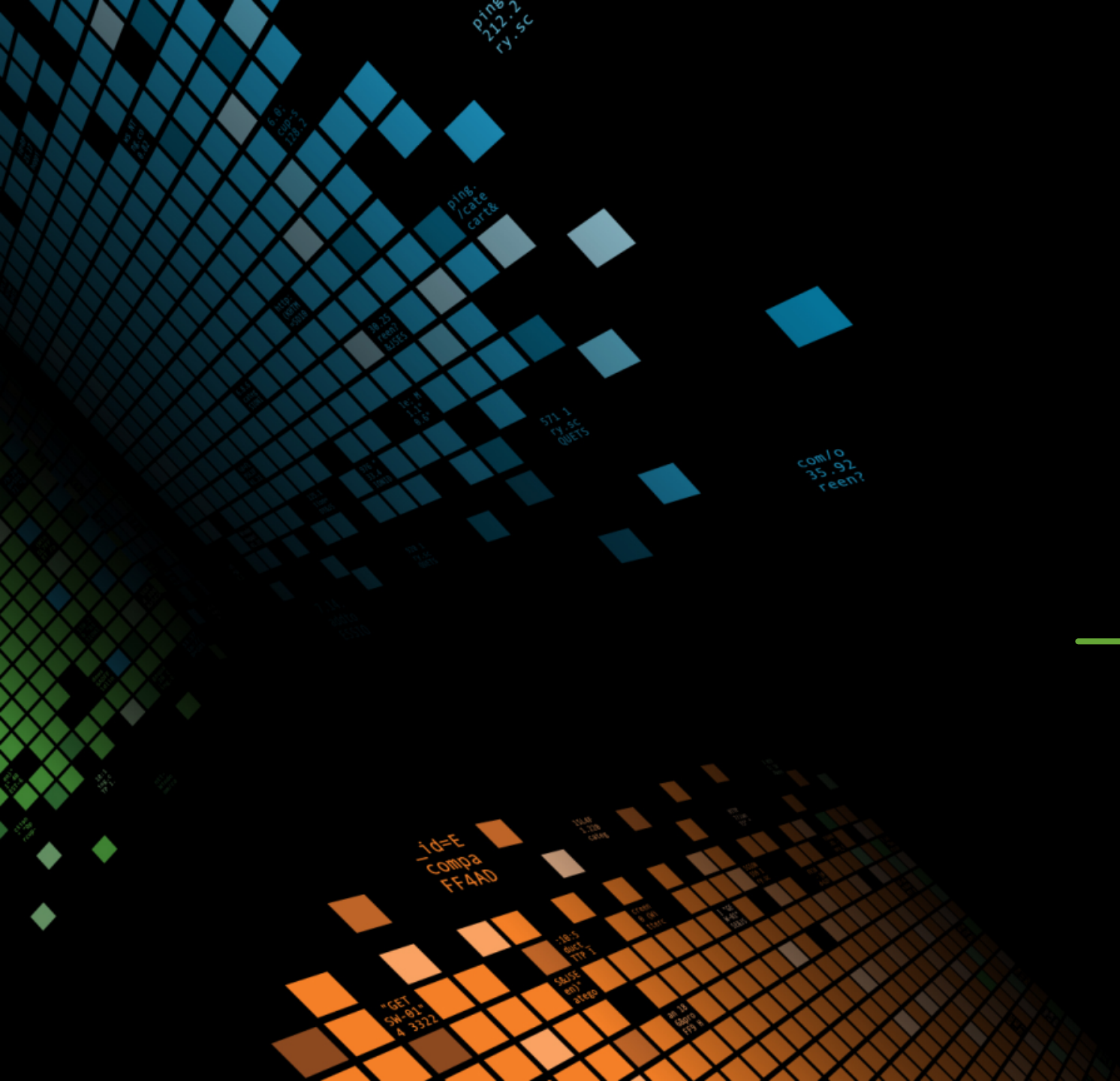
- Number of instance launched daily
- Amount of money spent daily

Native support of alerting

- Email, SNS, ServiceNow



splunk> .conf2017



Q&A

Thank You

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