

 sumologic

 aws

**Ben Newton & Colin Fernandes**  
**AWS Berlin**

Leveraging your **machine data analytics** to manage,  
troubleshoot and secure your **modern apps**

# Who is Sumo Logic?

3 Continents  
6 AWS Regions

2000+ Customers  
50,000+ Users

100+ PetaBytes of  
Machine Data  
Analyzed Daily

20+ Million Searches  
Daily



Multi-tenant,  
microservices-based  
architecture

500+ Trillion Records  
Analyzed Daily

# New Study: Business Value of Machine Data Analytics

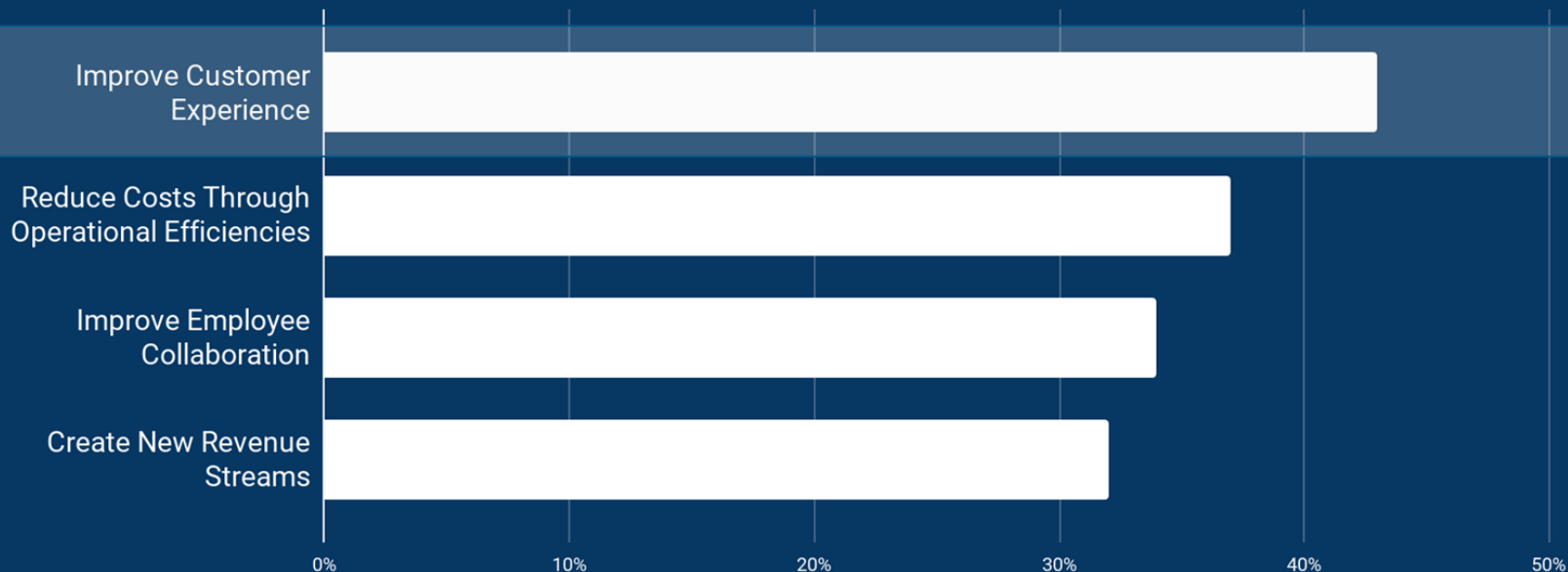
“Businesses that are able to participate in this analytics economy – translating their data into valuable intelligence that gives them competitive advantage – will survive and thrive **Those that don’t will be left behind.**”

**June 12: Download the Study at [sumologic.com](https://sumologic.com)**



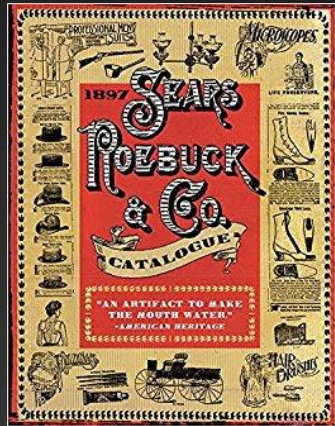
# The Customer Experience Imperative

## Top Drivers of Software Investments



451 Research Voice of the Connected User Landscape: 1H 2017 US Corporate Mobility and Digital Transformation

# The Drive for Convenience and Access



Catalog



Shopping Center



Super Store

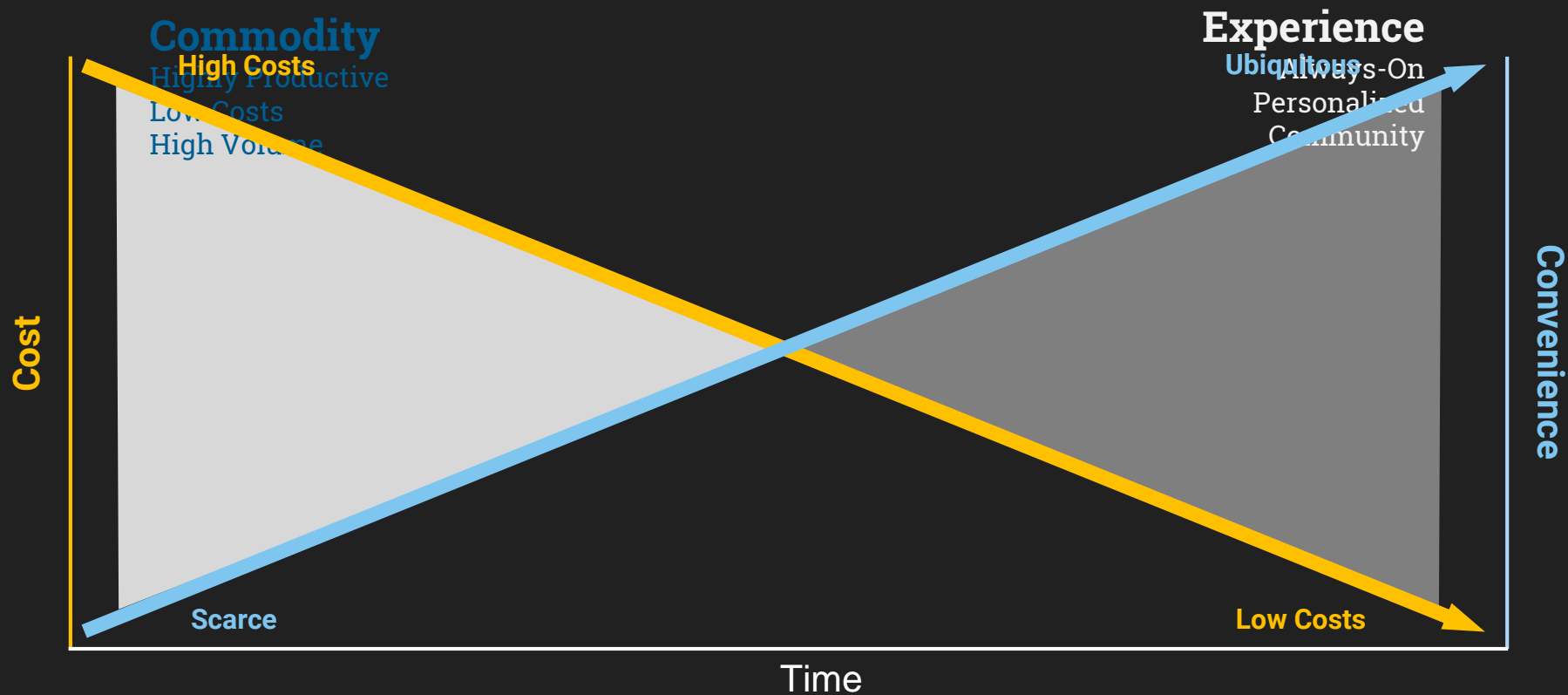


E-Commerce

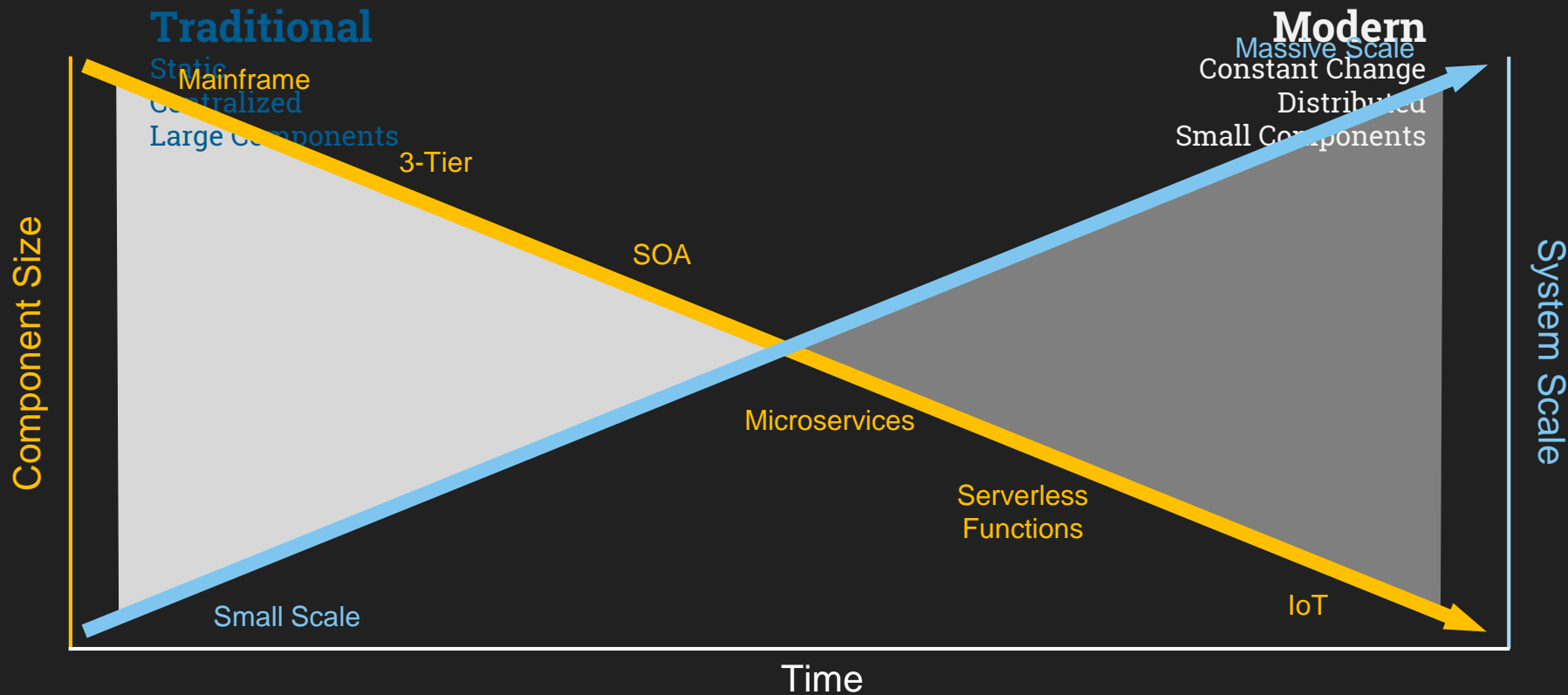


Personalization

# A Shift from Commodity to Experience



# Experience Focus Drives Technology Investments





# Companies are **struggling** with the changes

Lack of  
Visibility



Growing Skills  
Gaps



Data Overload



Legacy Silos





# And they know it...

**Lack of  
Visibility**

**49%**

**Legacy tools  
ineffective**

**Growing  
Skills Gaps**

**63%**

**Requires broader  
technical expertise**

**Data  
Overload**

**51%**

**Cloud staff  
overloaded**

**Legacy Silos**

**57%**

**Require greater  
collaboration**

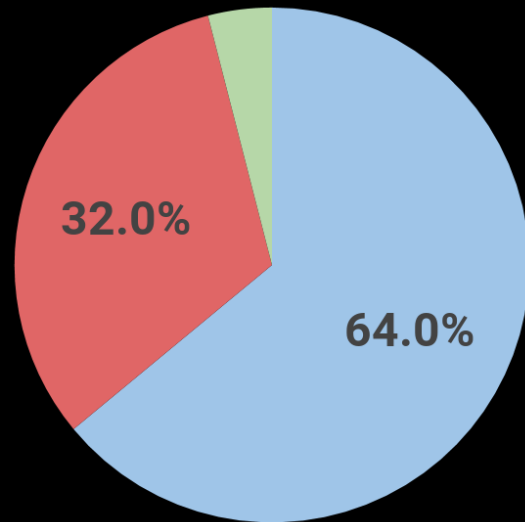
2018 Global Security Trends in the Cloud - Sumo Logic

# Machine Data Analytics is the secret sauce!

Importance of Machine Data Analytics to Customer Experience

Q. How important is machine data to your company's ability to meet its goals?

250 Companies Answered



● Extremely Important ● Important ● Somewhat Important

451 Research: Using Machine Data Analytics to Gain Advantage in the Analytics Economy (June 2018)

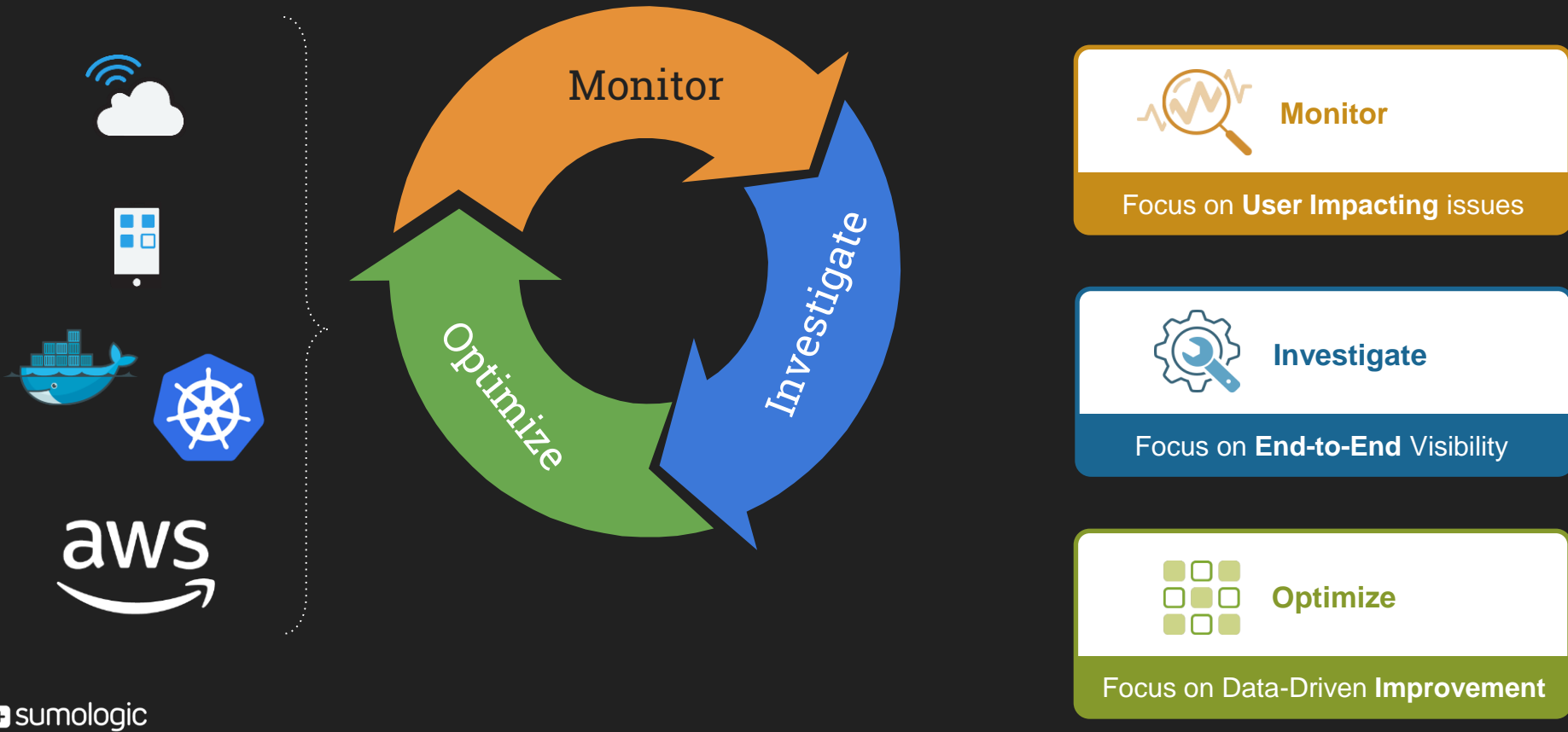
# What's holding us back?

## Biggest Obstacles to Adopting Machine Data Analytics

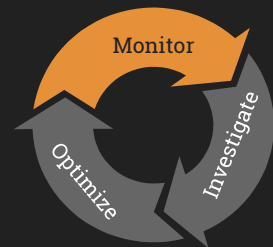


451 Research: Using Machine Data Analytics to Gain Advantage in the Analytics Economy (June 2018)

# A Modern, Integrated Approach to Analytics



# Proactive Real-Time Monitoring



## Threat Intel for AWS - Overview

Welcome to Threat Intel for AWS App

Sumo Logic has partnered with CrowdStrike to help you perform analysis over your logs for potential security threats and Indicators of Compromise (IOCs). Sumo Logic maintains an up-to-date CrowdStrike Threat Intelligence database that you can correlate with your log data through Threat lookup operator. [Learn More](#).

If I don't see any results in any Dashboard, is that a bad thing?

No. No results in your Dashboards can mean that nothing has been identified by CrowdStrike as a threat.

Got more questions? See our [FAQs on Threat Intel](#).

Scanned Events Over Time



CloudTrail

Last 24 Hours

251

VPC

Last 24 Hours

2.43k

ELB

Last 24 Hours

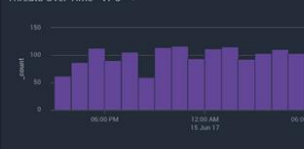
21.4k

Threats Over Time - CloudTrail

Last 24 Hours



Threats Over Time - VPC

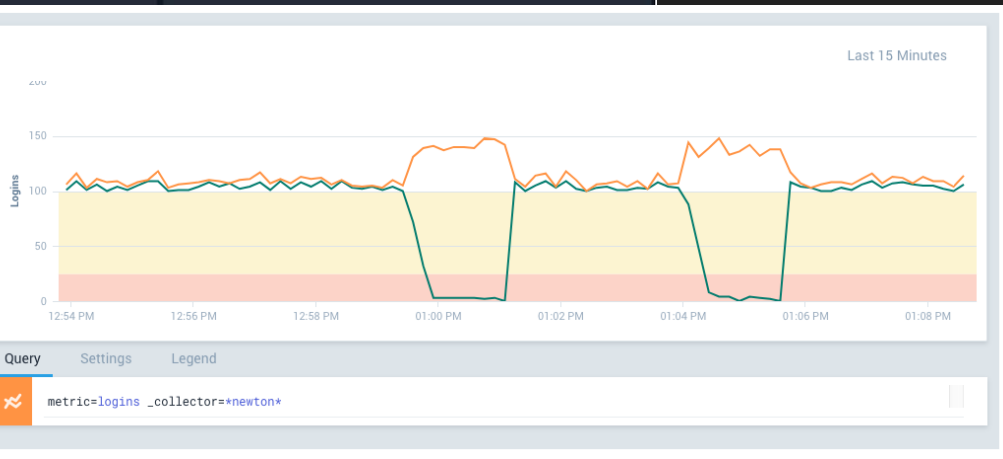


Threat Outlier - CloudTrail

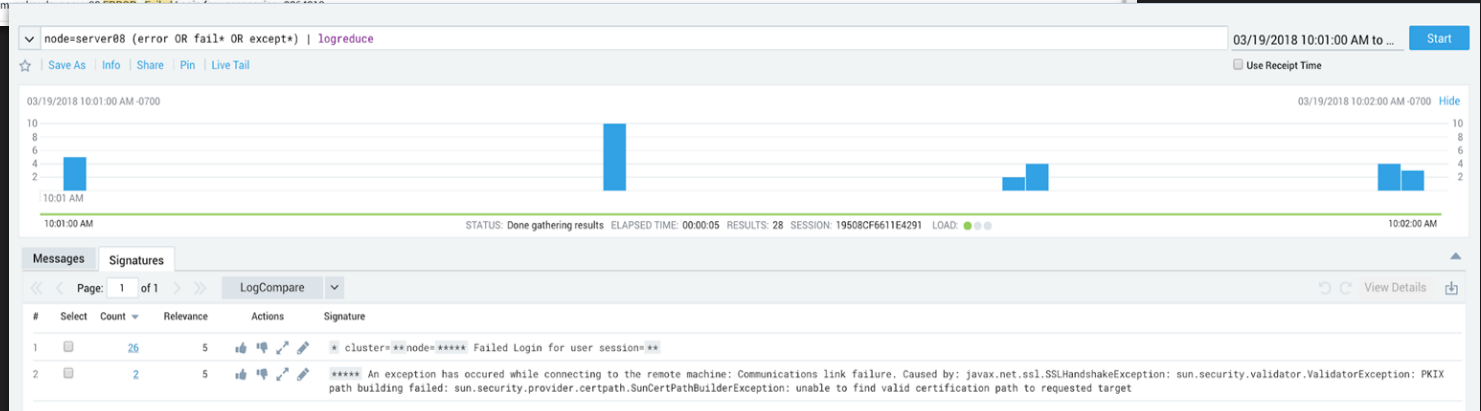
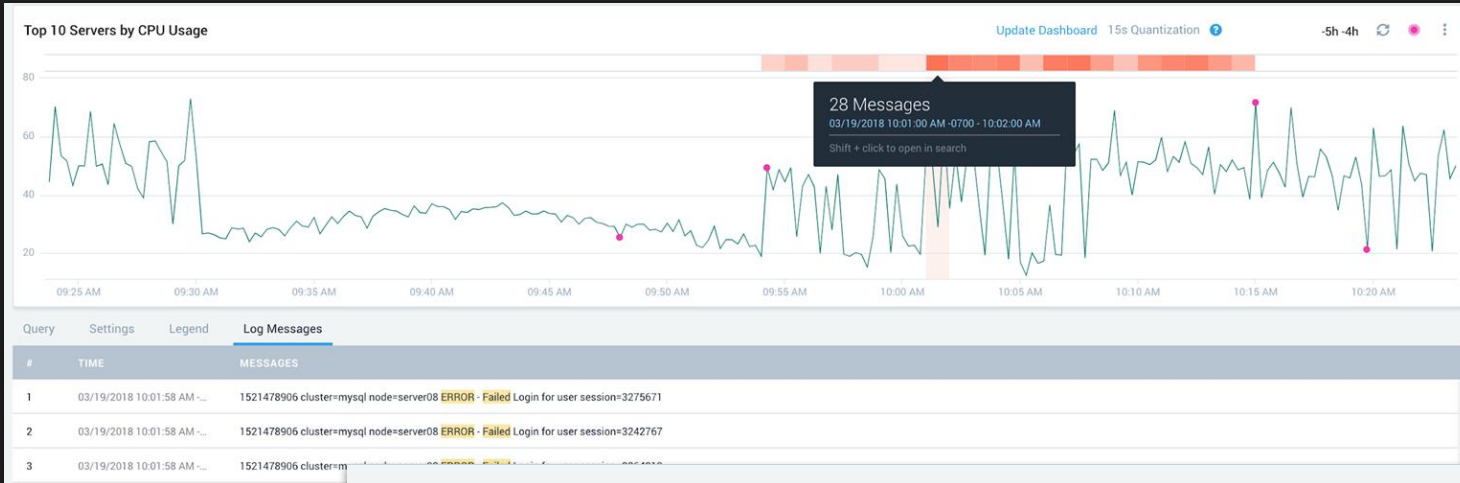
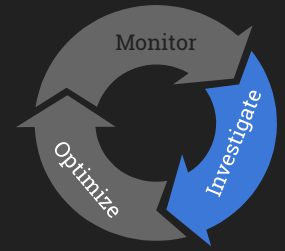
Last 24 Hours



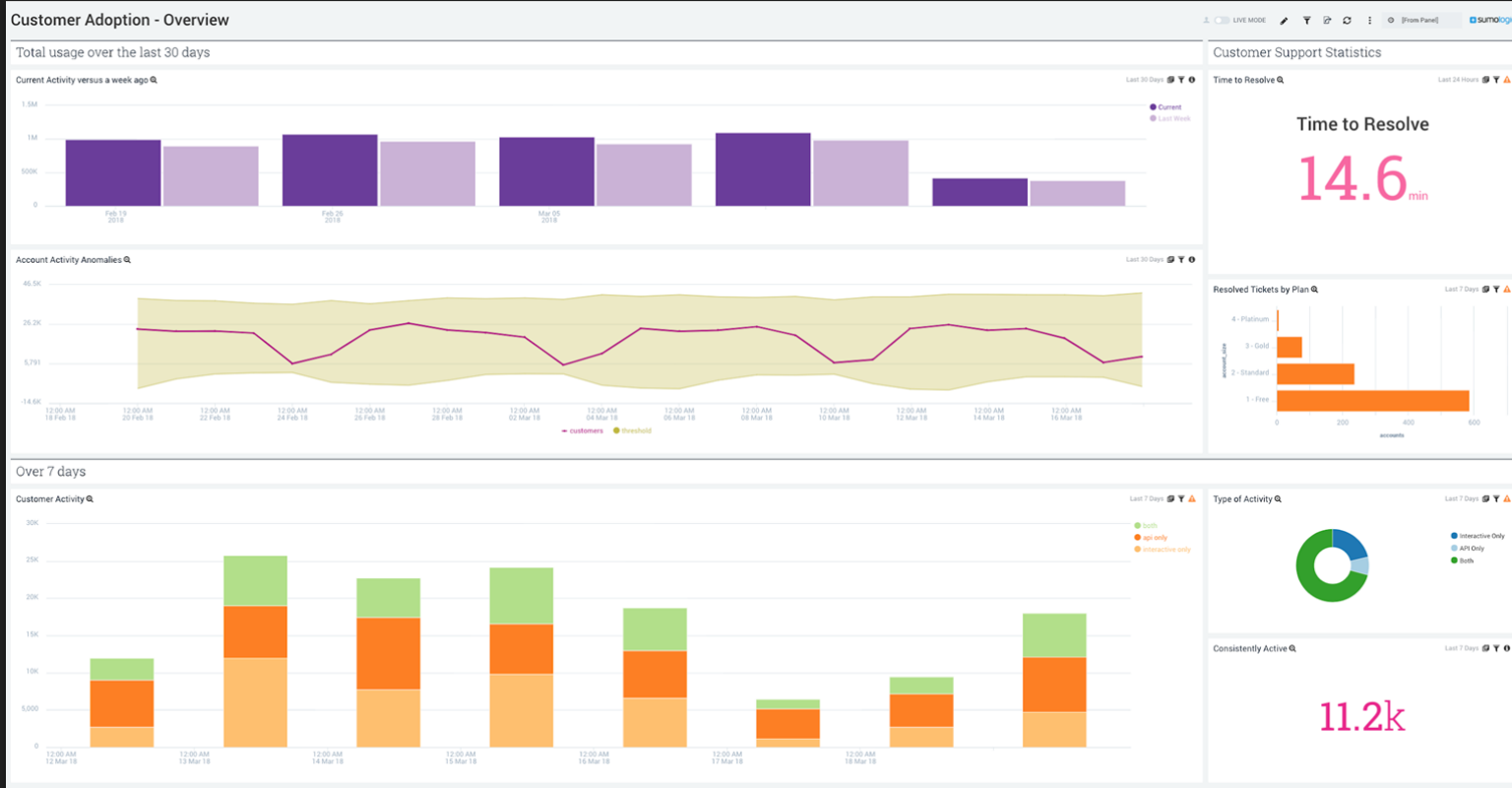
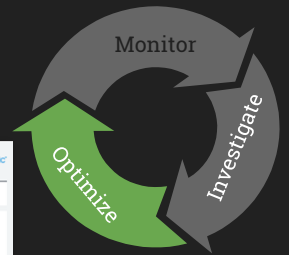
Threat Outlier - VPC



# Effective Investigations



# High-Impact Application Optimization





# Empower the People Powering your Business



**Monitor**

Focus on **User Impacting** Issues



**Investigate**

Focus on **E2E** Visibility



**Optimize**

Focus on **Data-Driven** Improvement



Ops / DevOps



Development /  
Engineering



Ops / DevOps



Development /  
Engineering



Product  
Management



Development /  
Engineering



SecOps



SecOps



Customer  
Support



Marketing /  
Sales



Customer  
Success



**THAT'S NICE. PROVE IT.**

[quickmeme.com](https://www.quickmeme.com)

# Example: Sumo Logic Query Activity Log

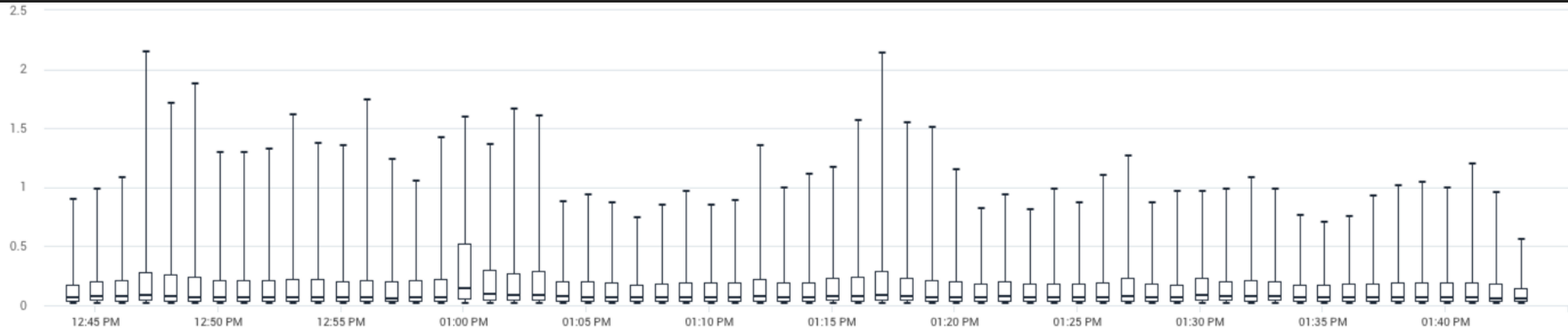
```
2017-08-14 11:33:56,042 -0700 INFO
[LOGTYPE=TELEMETRY.CUSTOMER] [hostId=prod-search-xx]
[module=STREAM]
[logger=stream.internals.EttPlansCache$]
[thread=MTP-RawOutputProcessor-Session-
0.0456958503414473-192C3F406EA0B56D-1]
[auth=xxx:false:DefaultSumoSystemUser:5:UNKNOWN]
[sessionId=xxx] explainJsonPlan.ETT {"version" :
2.0, "customerId" : "xx", "sessionId" : "xx",
"isInteractiveQuery" : false, "exitCode" : 0,
"statusMessage" : "Finished successfully",
"isActiveAggregateQuery" : true, "query" : "SOME QUERY"}
```

# Example: User Query Execution over Time

```
_sourceCategory=*/stream AND explainJsonPlan.ETT  
| parse "explainJsonPlan.ETT *" as json_explain  
| json field=json_explain "executionStartTime" ,  
"executionEndTime"  
| (executionEndTime - executionStartTime) as query_time  
| query_time/1000 as query_time  
| timeslice 1m  
| pct(query_time, 25,50,75), min(query_time),  
pct(query_time, 90) as _max by _timeslice
```

Extract the JSON

Compute a  
histogram



# Example: Correlate Events with Performance



*CPU Load  
correlates to  
User Query  
Activity*

# Example: Searching for Particular Usage

```
_sourceCategory=*/stream AND explainJsonPlan.ETT logreduce by
```

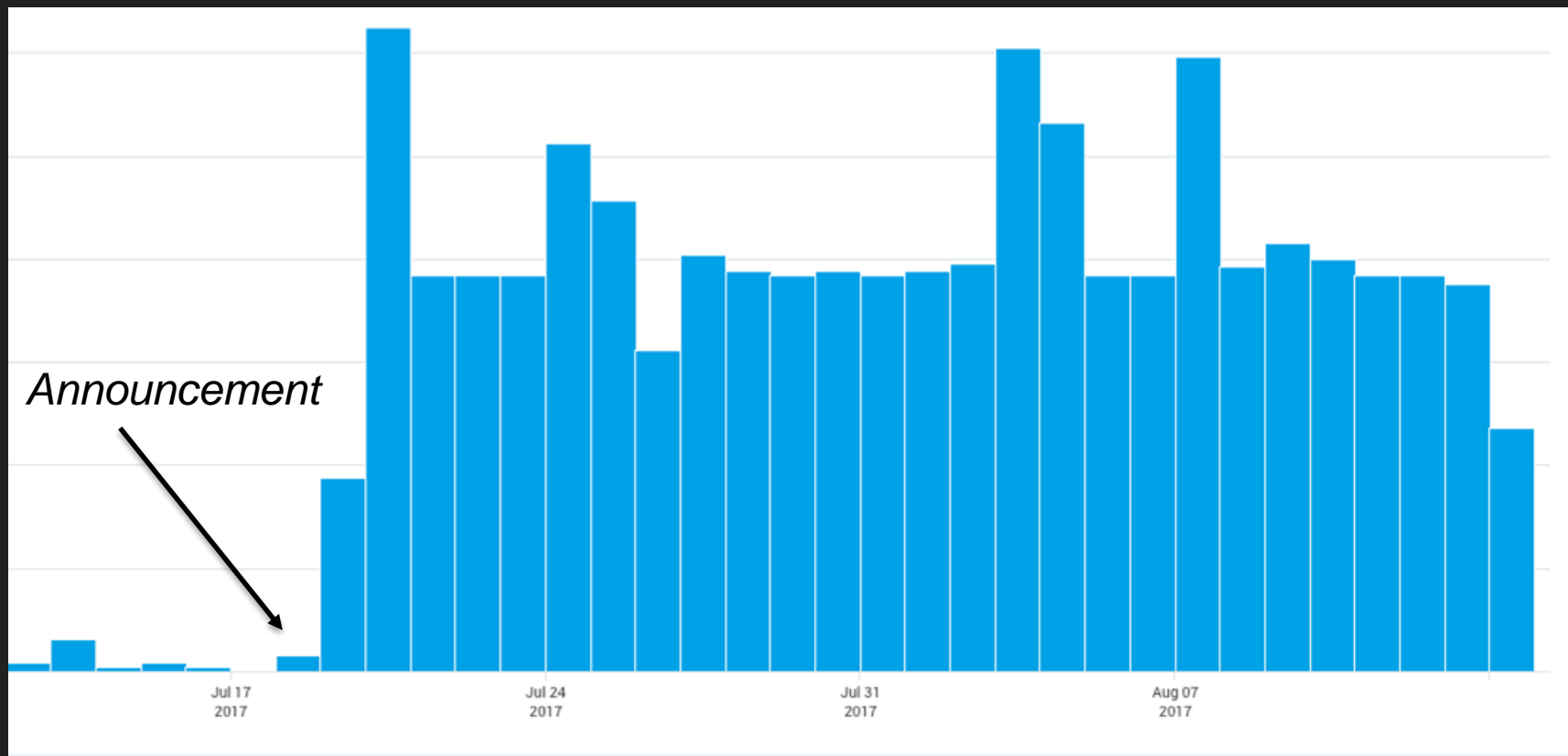
```
| parse "[hostId=*-*]" as deployment, host | parse "[  
explainJsonPlan.ETT *]" as ett
```

```
| json field=ett "rangeDt", "sessionId", "callerModule",  
"statusMessage", "executionDt", "buildEngineDt",  
"customerId", "inputMessageCt",  
"messageCt", "rawCt", "parseRegexTime", "indexCt", "indexCtAfterBloomfi  
lter", "indexBatchCt", "streamProcessingDt", "operatorTime",  
"pauseDt", "gcTime", "executionStartTime", "queryStartTime"
```

```
| where (query matches "*logreduce by *")
```

```
| timeslice by 1d
```

# Example: Understanding a Product Release





# Understanding the Adoption of a New Product Feature

Bento Home - Learn Tab

LIVE MODE

Last 30 Days

Unique Visitors

Last 30 Days

2.61k  
Unique Visitors

Unique Clicks

Last 30 Days

1.22k  
Users Clicking Links

Conversion Percentage

Last 30 Days

46.6%  
Users Clicking Links

Unique Visitors per Day

Last 30 Days



Conversion Percentage by Day

Last 30 Days



Unique Users Clicking per Day

Last 30 Days



Clicks by Destination

Last 30 Days



Doc Pages Viewed

Last 30 Days



Videos being watched

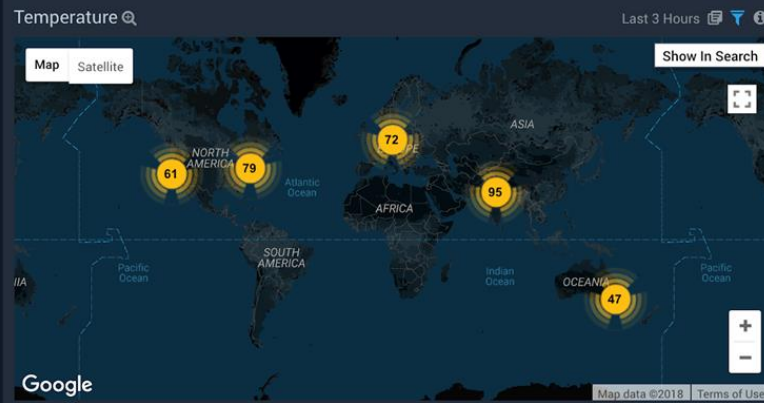
Last 30 Days



# Weather Dashboard

[From Panel]

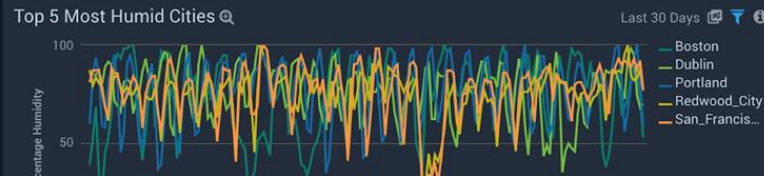
Not  
Just IT  
Either



### Current Weather

Last 3 Hours

city	country	Current Weather	Current Temperature	Current Humidity
Amsterdam	NL	clear sky	68.05	46
Austin	US	broken clouds	88.23	46
Barcelona	ES	few clouds	67.1	88
Beijing	CN	clear sky	55.4	87
Berlin	DE	clear sky	69.8	46
Boston	US	few clouds	78.55	39
Brussels	BE	mist	64.92	88
Chicago	US	scattered clouds	76.01	60
Dallas	US	broken clouds	88.39	46
Denver	US	shower rain	73.99	29



# A Modern Solution for the Modern Application

*"Sumo Logic is the information radiator at SmartThings. Every team at SmartThings finds value with Sumo Logic"*



## Cloud Native



Full visibility  
into App & Infra

## True SaaS



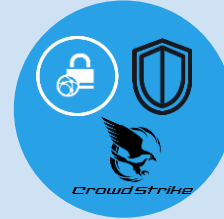
Rapid scale,  
adoption & TTV

## Secure Core



Platform security &  
compliance leader

## Rapid Response



Unified security  
& compliance

## DevSecOps



Accelerated  
innovation &  
transformation



Conversations on the Front Lines of the Data Revolution


[mastersofdata.com](http://mastersofdata.com)

*Available on iTunes and Google Play*



## Bill Burns: A Journey Through Time and Security

CTO, INFORMATICA

Powered by  sumologic



Dr. Nicole Forsgren



Jez Humble

DevOps Research and Assessment (DORA)



## George Gerchow: The New Age of Data Privacy

CSO, SUMO LOGIC

Powered by  sumologic



Christian Madsbjerg  
Author -  
"Sensemaking"

Thank  
You

