Splunking the Transaction Waterfall

Scott Garcia | Principal Architect - Enterprise Solution Delivery, T-Mobile

Andrew Koo | Manager – Enterprise Solution Delivery, T-Mobile

Gary Burgett | Staff Sales Engineer, Splunk

October 1-4 2018 | Orlando, FL

Forward-Looking Statements

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.

Introduction

Agenda

- T-Mobile Splunk @ a Glance
  - Splunk Evolution
  - Fun Facts and Environment
- Journey to Splunk Unlimited
  - IT Transformation
- Waterfall Use Case Walk-Through
- Data Maturity
- Utilizing the Data
  - Searching and Visualizing the Data

T-Mobile @ a Glance

- 1 million+ net customer adds – 19 quarters in a row
- 10s of thousands of employees
- 100s of business and engineering applications
- Splunk customer for 7 years, strategic partner for 5 years
- 100s of teams using Splunk

Evolution of Splunk @ T-Mobile

GEN 1: Initial

- 2 TB license
- Siloed Search Heads

GEN 2: Growth

- 5.5 TB license
- Increased adoption
- Larger, more complex use cases: CDR, Retail

GEN 3: Commoditize Data

- 11.5 TB license
- Bare-metal right-sizing
- Geo redundancy added
- Mediation gen 1 + 2
- Scaling of syslog
- More structured self-serve at scale
- Broad and deep adoption
- Beginning of tiered environments (HW)

GEN 4: Advanced Self-Serve

- ‘Unlimited’ license
- User Engagement
- Advanced Self-Serve
- Launch new analytics capabilities (Viz & ML)
- Streamlined HW provisioning & tiered options
- Improved Availability & Performance
- Workflow Automation
- Show-back Reporting

Fun Facts & Environments

- 45 TB per day INGESTION (+125% Q1-Q2)
- 14,000,000 served SEARCHES (Q1-Q2)
- 112,000 distinct DEVICES supported
- 15,000 supported FORWARDERS
- 1,900 supported DASHBOARDS
- 1,500 supported SOURCETYPES
- 4000 distinct USERS (+18% Q1-Q2)
- 200 supported APPS
- ~ 5 per day ONBOARDINGS

- PCI/Security
- SOX
- Enterprise
  - Class A1
  - Class A2
  - Class B
  - Class X

splunk> .conf18

Journey to Splunk Unlimited

T··Mobile·

splunk> .conf18

IT Transformation

- 3 years ago
  - Utilized an In-house logging application
    - Organization couldn't take full advantage of the data
    - Solutions were developed with a narrow focus
    - Was not scalable and therefore unsustainable
  - Investment front loaded on the network at the expense of IT
    - Disparity in investment can lead to a delay in maturity
  - IT Transformation
    - A multi-year phased introduction of a new Enterprise IT solution
    - Consolidation of 100's of applications through new development and technology

Transition to Splunk Unlimited

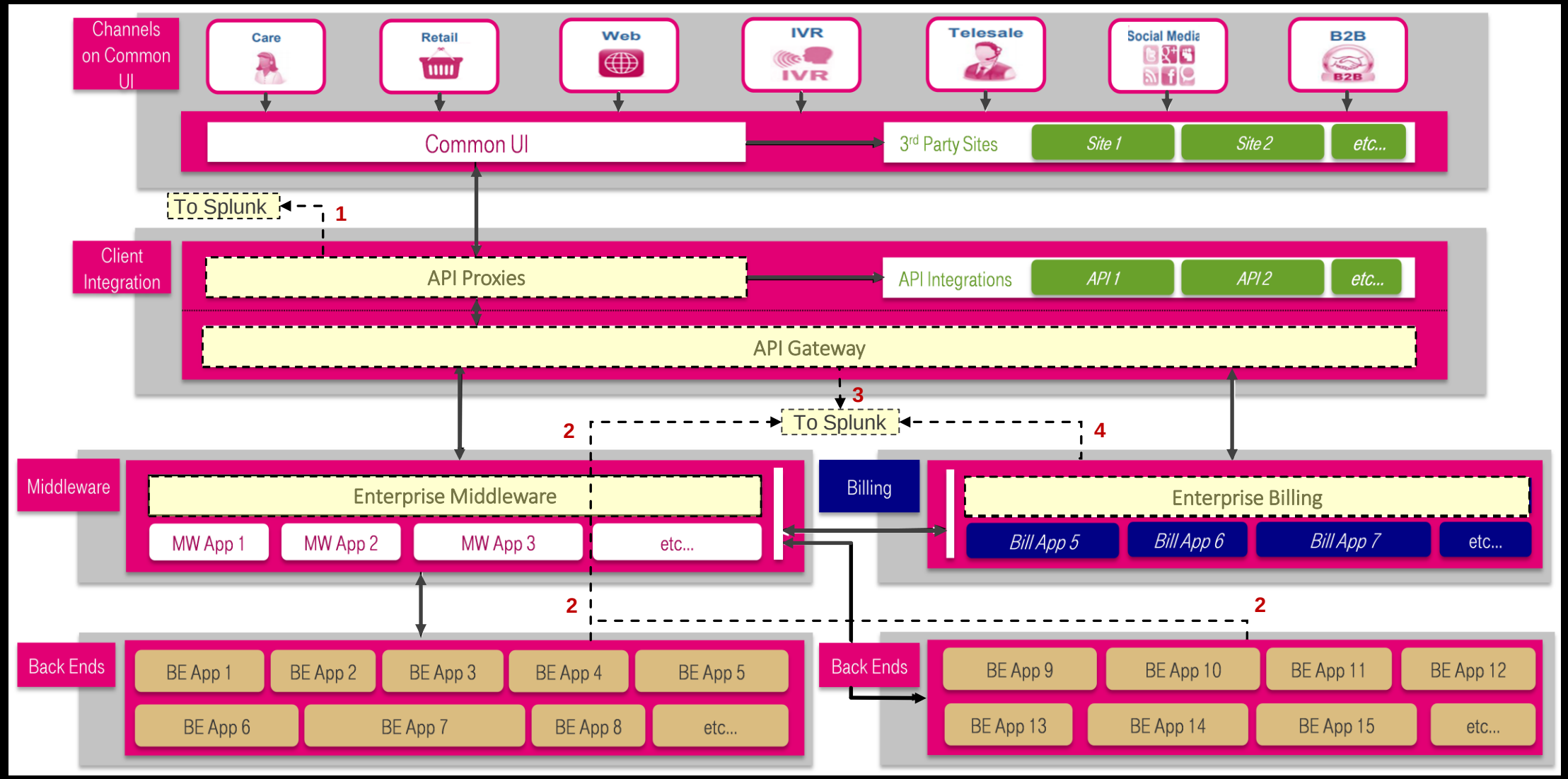
- Next Gen Centralized Logging and Monitoring
  - Value proposition and timing
  - Evaluation of solutions

Splunk named an enterprise solution

- With success came challenges
  - Support of an enterprise solution vs. a targeted solution
  - Splunk knowledge transfer for general use and dashboard development.
  - Infrastructure expansion was needed to support the trend of increasing usage
  - The acceleration of Splunk adoption places pressure on license capacity

Transitioned to an unlimited licensing model – 12/31/17

IT Transformation



T··Mobile·

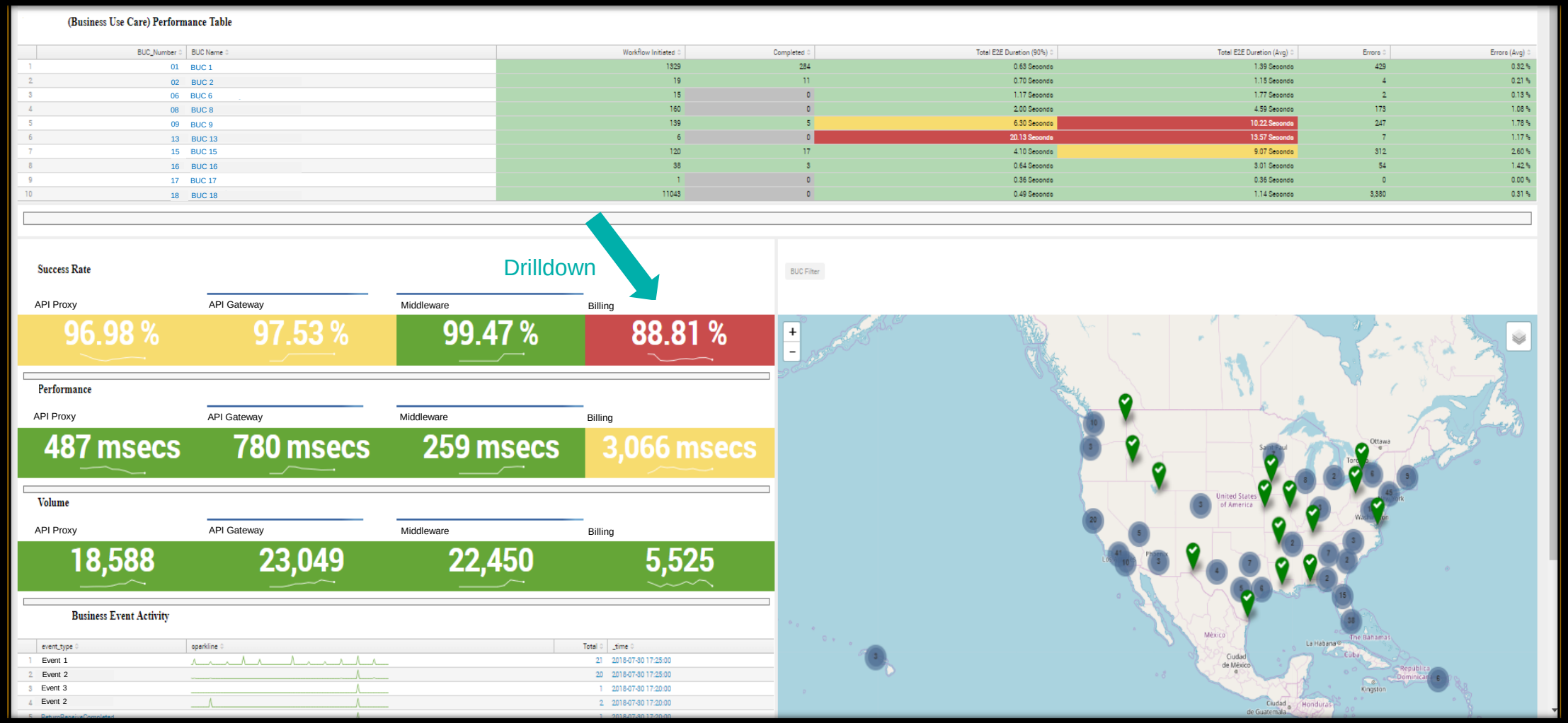
splunk> .conf18

Waterfall Use Case

End to End Transactional Flows

Dashboard

Top Level Performance and Availability Dashboard



(Business Use Care) Performance Table

	BUC_Number	BUC Name	Workflow Initiated	Completed	Total E2E Duration (90%)	Total E2E Duration (Avg)	Errors	Errors (Avg)
1	01	BUC 1	1329	284	0.63 Seconds	1.39 Seconds	429	0.32 %
2	02	BUC 2	19	11	0.70 Seconds	1.15 Seconds	4	0.21 %
3	06	BUC 6	15	0	1.17 Seconds	1.77 Seconds	2	0.13 %
4	08	BUC 8	160	0	2.00 Seconds	4.59 Seconds	173	1.08 %
5	09	BUC 9	139	5	6.30 Seconds	10.22 Seconds	247	1.78 %
6	13	BUC 13	6	0	20.13 Seconds	13.57 Seconds	7	1.17 %
7	15	BUC 15	120	17	4.10 Seconds	9.07 Seconds	312	2.60 %
8	16	BUC 16	38	3	0.64 Seconds	3.01 Seconds	54	1.42 %
9	17	BUC 17	1	0	0.36 Seconds	0.36 Seconds	0	0.00 %
10	18	BUC 18	11043	0	0.49 Seconds	1.14 Seconds	3,380	0.31 %

Drilldown

Success Rate

API Proxy	API Gateway	Middleware	Billing
96.98 %	97.53 %	99.47 %	88.81 %

Performance

API Proxy	API Gateway	Middleware	Billing
487 msecs	780 msecs	259 msecs	3,066 msecs

Volume

API Proxy	API Gateway	Middleware	Billing
18,588	23,049	22,450	5,525

Business Event Activity

	event_type	sparkline	Total	_time
1	Event 1		21	2018-07-30 17:25:00
2	Event 2		20	2018-07-30 17:25:00
3	Event 3		1	2018-07-30 17:20:00
4	Event 2		2	2018-07-30 17:20:00

BUC Filter

Dashboard

1st Level Drilldown – Billing Success Rate

E// Core Apps - Error Messages Resolved as Negative Responses (True) or Not (False)

Negative Response	Target App	PIER Queue	Error Message	# of Errors
FALSE	App 1	Queue 1	Activity timed out	11478
FALSE	App 1	Queue 1	Username or password wrong	52
FALSE	App 1	Queue 1	JE0020: JavaScript error	37
FALSE	App 1	Queue 1	Error From null: Order is NOT allowed. There is already an in-progress Customer level order.	27
FALSE	App 1	Queue 1	; ERROR_MESSAGE_EXPLANATION: UNKNOWN	23
FALSE	App 1	Queue 1	Field im_crm_channel_code is mandatory	23
FALSE	App 1	Queue 1	ON-OC-E00310[validateBusinessLogic]	14
FALSE	App 1	Queue 1	ChannelId is not valid	14

« prev 1 2 3 4 5 6 next »

Drilldown

Success Rate Statistics

Number of Outlier(s)

7

Number of Hourly Intervals Below min Threshold

Errors - (15 minutes)

736

Number of Errors - p/15 min

Success Rate- Avg (15 Minute)

95.68

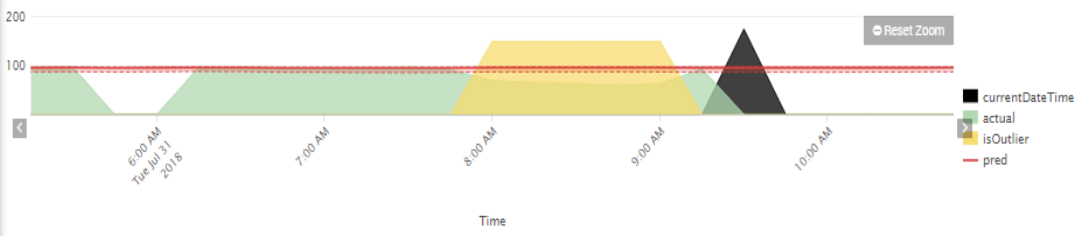
Avg Success Rate - p/15 min

Predicted Success Rate vs Actual

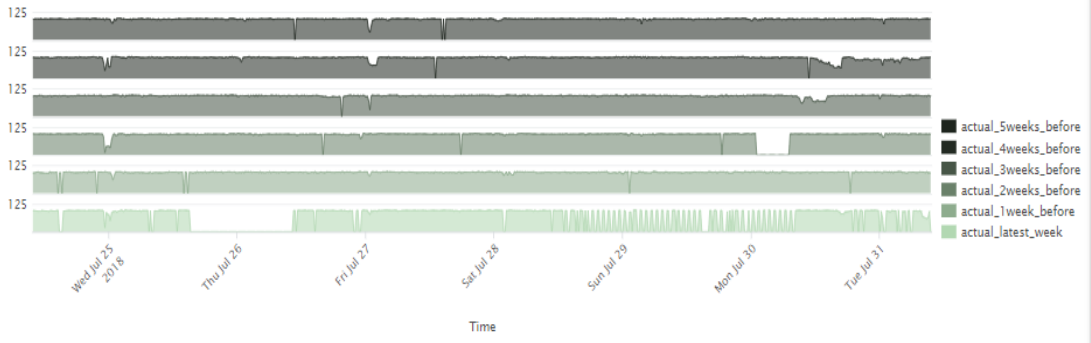
Sensitivity (max 1): .97

Confidence Interval (max 100): 97.5

Include MTC Window:
- Include MTC Window
- Non-MTC Window Only



Weekly Historical View



6m ago

Dashboard

2nd Level Drilldown – Activity Timeout

Time Setting: Custom time | Target Application: APP-1 | Service: Service 1 | Operation: Operation 1 | Error Message: All | Submit | Hide Filters

Error Result Table

	_time	zone	Target	service	operation	result	negative_response	error_message	error_code	rtt	Interaction	end	start
1	2018-09-05 15:45:14.398	Zone 1	APP-1	Service 1	Operation 1	0	FALSE	Activity Timeout	9101086	29	Interaction 1	1536187544.398	1536187484.398
2	2018-09-05 16:15:16.772	Zone 1	APP-1	Service 1	Operation 1	0	FALSE	Activity Timeout	9101086	58	Interaction 2	1536189346.772	1536189286.772
3	2018-09-05 16:15:18.403	Zone 1	APP-1	Service 1	Operation 1	0	FALSE	Activity Timeout	9101086	125	Interaction 3	1536189348.403	1536189288.403
4	2018-09-05 16:27:42.976	Zone 1	APP-1	Service 1	Operation 1	0	FALSE	Activity Timeout	9101086	65	Interaction 4	1536190092.976	1536190032.976
5	2018-09-05 16:06:38.893	Zone 1	APP-1	Service 1	Operation 1	0	FALSE	Activity Timeout	9101086	37	Interaction 5	1536188828.893	1536188768.893

Drilldown

1m ago

Dashboard

3rd Level Drilldown – Waterfall Dashboard

Select a Time Window: Date time range | Select ID: Interaction ID | Value of Selected ID: Interaction 5 | Submit | Hide Filters

U2 Transactions Waterfall

	workflow_id	screen_id	flow_name	service	operation	application	start	end	latency
1	WF-GC-01.01	SC1163	Flow 1		Operation 1	UI	2018-09-05T14:56:11.481	2018-09-05T14:56:11.827	346
2	WF-GC-01.01			Service 1	Operation 2	API Gateway	2018-09-05T14:56:11.792	2018-09-05T14:56:11.815	23
3	WF-GC-01.01	SC1163	Flow 2		Operation 3	UI	2018-09-05T14:56:12.190	2018-09-05T14:56:13.268	1078
4	WF-GC-01.01	SC1163	Flow 3		Operation 4	UI	2018-09-05T14:56:12.333	2018-09-05T14:56:12.667	334
5				Service 2	Operation 5	Middle Ware	2018-09-05T14:56:12.628	2018-09-05T14:56:12.647	19
6				Service 3	Operation 6	Shared Service	2018-09-05T14:56:13.231	2018-09-05T14:56:15.095	1864
7	WF-GC-01.01	SC1432	Flow 4		Operation 7	UI	2018-09-05T14:56:14.587	2018-09-05T14:56:14.966	379
8	WF-GC-01.01			Service 4	Operation 8	Middle Ware	2018-09-05T14:56:14.834	2018-09-05T14:56:14.897	63
9	WF-GC-01.01			Service 5	Operation 9	Shared Service	2018-09-05T14:56:14.917		
10	WF-GC-01.01	SC1432	Flow 5		Operation 10	UI	2018-09-05T14:56:24.706	2018-09-05T14:56:25.662	956
11	WF-GC-01.01			Service 6	Operation 11	Middle Ware	2018-09-05T14:56:25.157	2018-09-05T14:56:25.617	460
12	WF-GC-01.01			Service 7	Operation 12	Shared Service	2018-09-05T14:56:25.646	2018-09-05T14:56:26.627	981
13	WF-GC-01.01	SC1432	Flow 6		Operation 13	UI	2018-09-05T14:56:26.047	2018-09-05T14:56:26.534	487
14				Service 8	Operation 14	Middle Ware	2018-09-05T14:56:26.475	2018-09-05T14:56:26.51	35
15				Service 9	Operation 15	Shared Service	2018-09-05T14:56:26.525	2018-09-05T14:56:28.532	2007
16	WF-GC-01.01	SC1432	Flow 7		Operation 16	UI	2018-09-05T14:56:26.800	2018-09-05T14:56:27.168	368
17	WF-GC-01.01			Service 10	Operation 17	Middle Ware	2018-09-05T14:56:27.106	2018-09-05T14:56:27.138	32
18	WF-GC-01.01			Service 11	Operation 18	Shared Service	2018-09-05T14:56:27.157	2018-09-05T14:56:32.998	5841
19	WF-GC-01.01	SC1432	Flow 8		Operation 19	UI	2018-09-05T14:56:34.010	2018-09-05T14:56:34.469	459
20	WF-GC-01.01	SC1432	Flow 9		Operation 20	UI	2018-09-05T14:56:38.214	2018-09-05T14:56:38.963	749
21				Service 12	Operation 21	API Gateway	2018-09-05T14:56:38.531	2018-09-05T14:56:38.916	385
22				Service 13	Operation 22	Shared Service	2018-09-05T14:56:38.918	2018-09-05T14:56:43.272	4354
23	WF-GC-01.01	SC1161	Flow 10		Operation 23	UI	2018-09-05T14:56:40.136	2018-09-05T14:56:41.320	1184
24	WF-GC-01.01	SC1161	Flow 11		Operation 24	UI	2018-09-05T14:56:40.143	2018-09-05T14:56:40.517	374
25				Service 13	Operation 25	Shared Service	2018-09-05T14:56:40.504	2018-09-05T14:56:41.237	733
26	WF-GC-01.01			Service 14	Operation 26	Shared Service	2018-09-05T14:56:41.260	2018-09-05T14:56:41.525	265
27	WF-GC-01.01			Service 15	Operation 27	Shared Service	2018-09-05T14:56:41.281	2018-09-05T14:56:41.916	635
28									
29									

Waterfall: 0 | 2500 | 5000 | 7500 | 10000 | 12500 | 15000 | 17500 | 20000 | 22500 | 25000 | 27500 | 30000

Sourcetype: ui-sourcetype

Event ID:	123456789ABCDEF
Service Transaction ID:	srv-123456789
Interaction ID:	interaction-123456789
Session ID:	sess-123456789
Result:	Error
Status Code:	500
Error Code:	UI - 9101086
Error Source:	Shared Service
Error Message:	Activity Timeout

T··Mobile·

splunk> .conf18

Waterfall | Value Observed

- Tier 1 and service desk organizations with little knowledge of application processing can easily reference a transactional flow.
- Tier's 2 & 3 are provided with the ability to visually analyze the sequence and contents of events
- The waterfall view is reusable allowing for its integration within many dashboards across T-Mobile's monitoring solutions
- Interactions between Interfaced applications can be observed
- Performance and validation teams are capturing performance related metrics
- Both production and non production teams have access to the waterfall view

Data Maturity

T··Mobile·

splunk> .conf18

Data Maturity

Logging best practices necessary to obtain transactional flows

Data Content Standards

- Cross-platform transaction IDs
- Field naming conventions
- Distribute ownership

Log/Event Structural Standards

- Transport (input) method standards
- Drive data providers to preferred input methods
- Handling complex payloads w/ Complex Event Processing (CEP)

Utilizing the Data

Searching the Data

Now that we have the data, what can we do with it

Different Platforms, Different formats

- Multiple middleware technologies where instrumentation takes place, each with their own format
  - XML
  - JSON
  - Raw text/KV pairs
- Schema-on-the-fly saves the day
- If the information is there, we can normalize it

Rich fields for filtering/grouping

- Sessions
- Activities
- Interactions
- Applications
- Channels
- Customers
- Operations
- Latencies
- Return Codes
- Error Messages

Searching the Data

Now that we have the data, what can we do with it

Consistent Fields = Simple Searches

index=transactions (sourcetype=mw OR sourcetype=core_gw OR sourcetype=core_proxy) cust_id=$cust_id$

Not so simple in practice

Myriad Use Cases

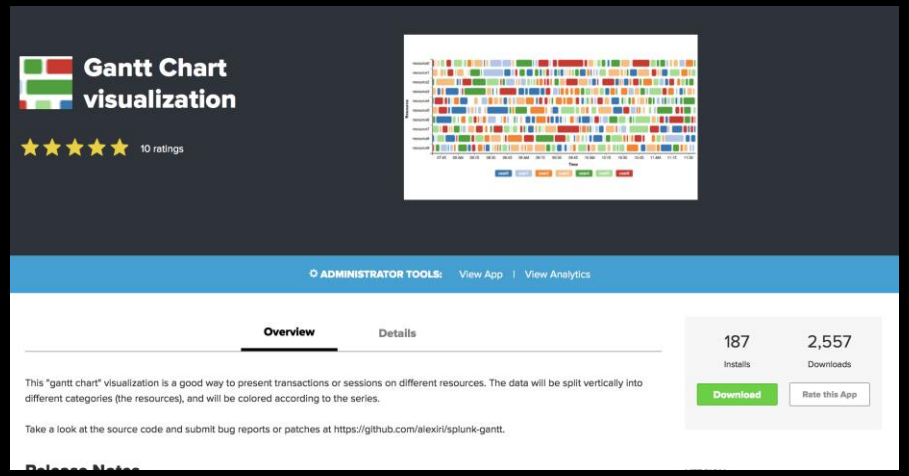
- Support can filter on a particular Customer ID to troubleshoot individual user issues
- Latency and Error Rates can be measured and baselined by Operation, Environment, Channel, etc.
- See individual transactions end-to-end

Visualizing the Data

How do I visualize transaction durations in Splunk?

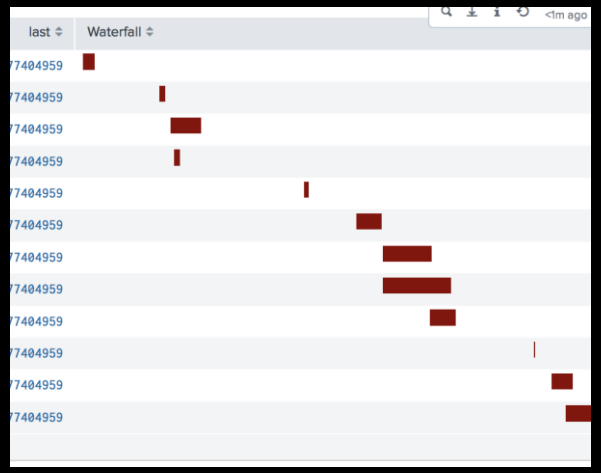
Options for nonstandard viz

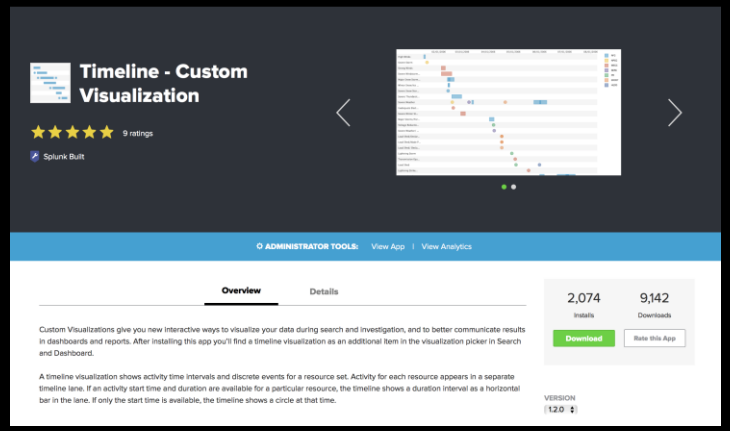
- Splunkbase
- Custom Visualization Framework
- Extend Current Visualizations with JS Extensions



Settled on Extension of Table View

- Simple, minimal code
- Leverage existing functionality
- Data Density



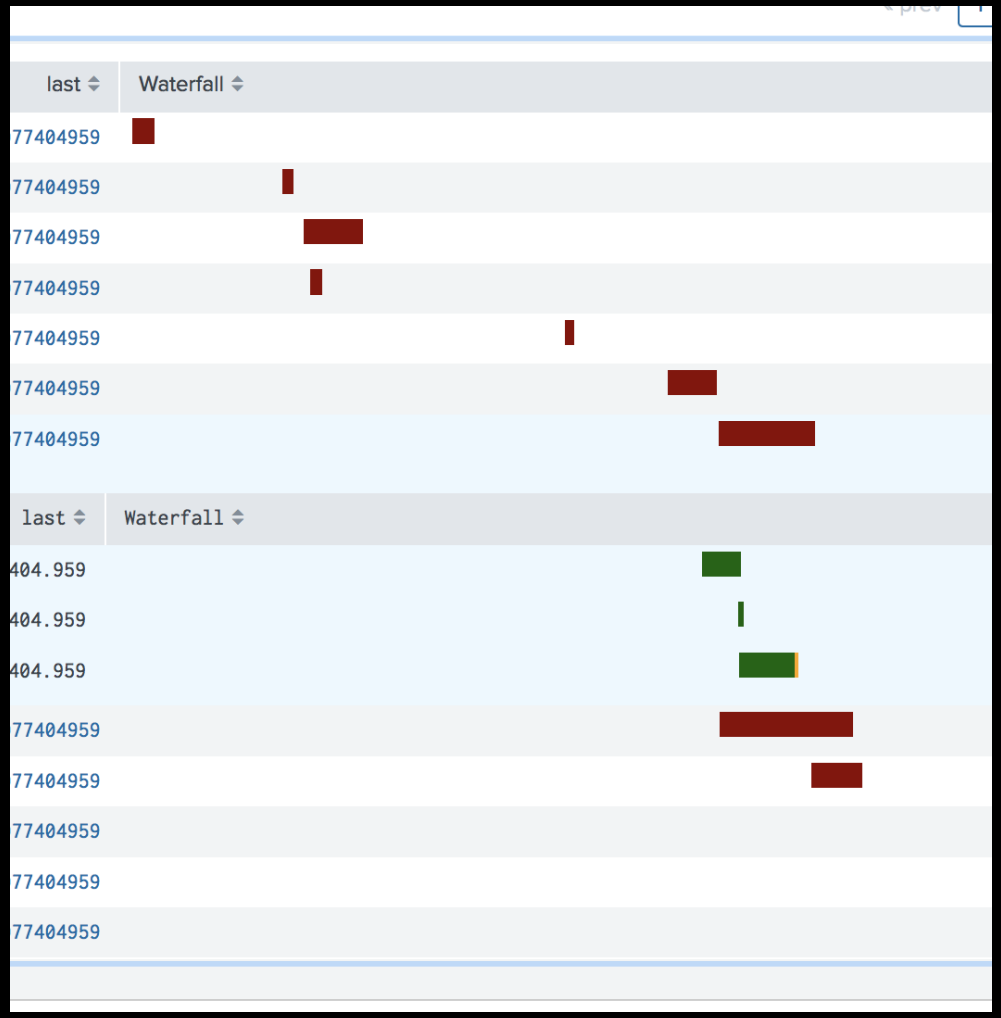


Visualizing the Data

How do I visualize transaction durations in Splunk?

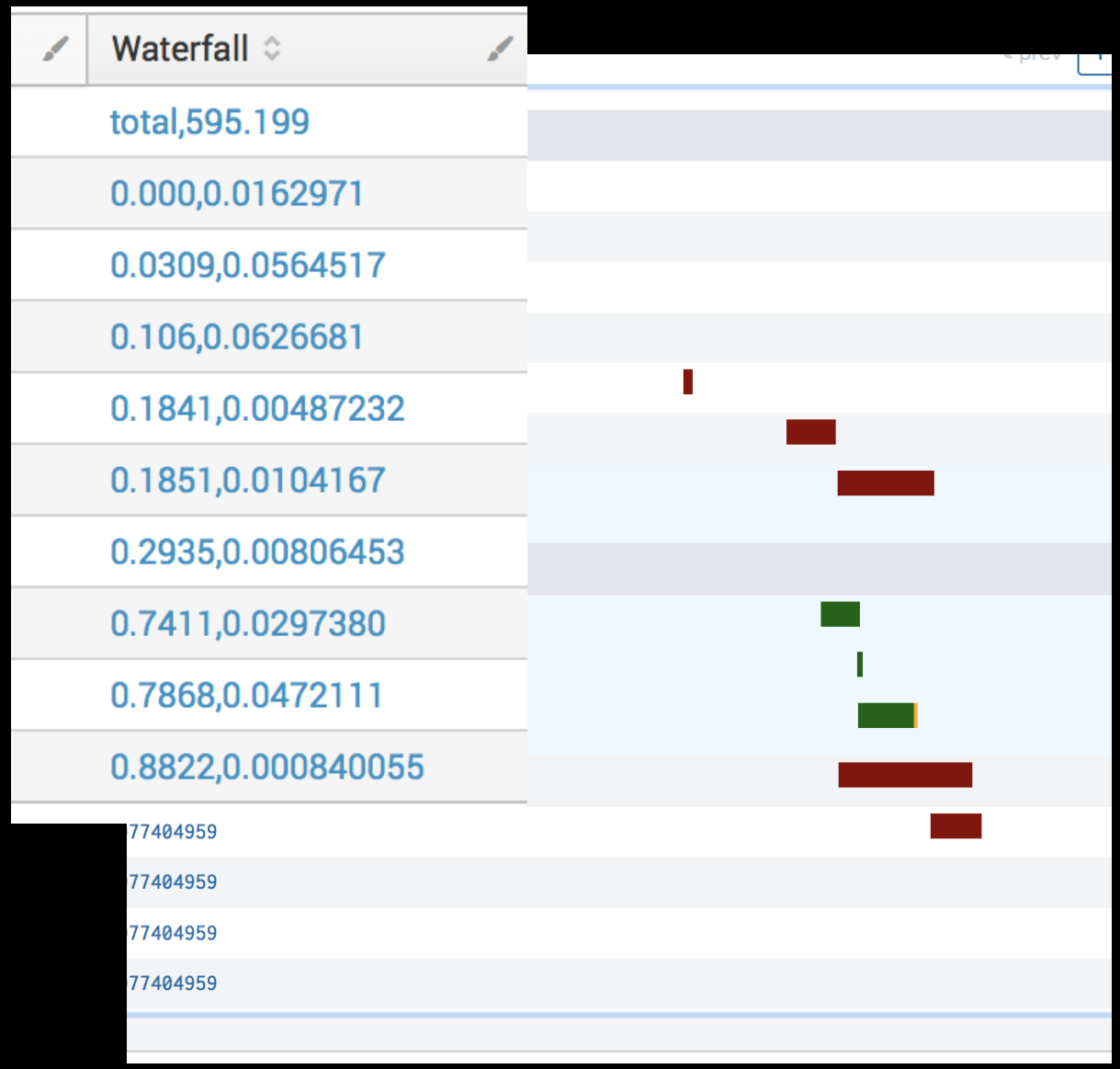
Searching to build the Waterfall

- eval and rex
  - Your best friends for data manipulation
- eventstats
  - Perform aggregate stats while maintaining the original data
- appendpipe
  - Perform aggregate stats and append them to the table



Bring it together

```
index=soa (sourcetype=api_gateway OR
sourcetype=messaging_gateway OR
sourcetype=backend_gateway) transaction_id=e3q29ir1u29zoi
| eventstats first(_time) AS first last(_time) AS last
| eval duration=first-last
| eval buffer=100*(_time-last)/duration
| eval diff=100*latency/(1000*duration)
| reverse
| eval Waterfall=tostring(buffer)+","+tostring(diff)
| eval spent=latency+" ms"
| appendpipe
   [stats max(eval("total," +tostring(duration))) AS Waterfall
max(eval(tostring(duration*1000)+" ms")) AS spent
   | eval buffer=tonumber(-1)]
| appendpipe
   [stats min(eval("markers,"+tostring(duration))) AS Waterfall
   | eval buffer=tonumber(101)]
| sort buffer | fields - buffer, diff
```



Key Takeaways

Good Logging Practices

1. Employ Good Logging Practices

2. Related Splunk .conf2018 Sessions

- **IT1256 - Zipkin & Splunk: Tracing Transactions Across Your Ecosystem**

Tuesday, Oct 02, 4:45 p.m. - 5:30 p.m.

Tom Martin, Staff Practitioner, Splunk

- **IT1847 - Splunking Application Performance: Traditional APM and Beyond**

Wednesday, Oct 03, 12:45 p.m. - 1:30 p.m.

Gary Burgett, Staff Sales Engineer, Splunk

T··Mobile·

splunk> .conf18

Q&A

Scott Garcia
Andrew Koo
Gary Burgett

T··Mobile·

splunk> .conf18

Thank You

Don't forget to rate this session in the .conf18 mobile app