

How Splunk Uses Telemetry to Improve Our Products and Services



Archana Ganapathi - Director, Data Strategy

Tracy Knight - Director, Product Performance

Miranda Luna - Senior Product Manager

Bharath Aleti - Director, Product Management

David Alward - Senior Escalation Manager

Kevin Louther - Products Data Analyst

Forward-Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

What is Telemetry?

Data that Splunk collects from Enterprise deployments

Contains license utilization, deployment topology, configuration, performance, search types, pageviews, apps, sourcetypes, etc.

Aggregated and sent nightly

Customers have choice to share:

Opt-out/in at first launch, can modify later

Helping You Get More Value from Splunk Software

Splunk Inc. collects aggregated product usage data so that we can enhance the value of your investment in Splunk software. This product usage data does not include any data you ingest into your deployment. Examples of what we collect:

- Feature usage
- Deployment topology
- Infrastructure and operating environment
- Performance

We use this data to optimize your deployment, prioritize our features, improve your experience, notify you of patches, and develop high-quality product functionality.

Sharing of product usage data from this deployment is set to ON. You can change your data collection preferences at any time in your [instrumentation Settings](#).

[Learn more](#) [↗](#) about what we collect, how we securely transmit data, and how we store the data. For details on Splunk's data practices, see the [Splunk Privacy Policy](#) [↗](#).

We are dedicated to helping you get the most out of your investment. Thank you for helping us make Splunk's products even better.

Got it!

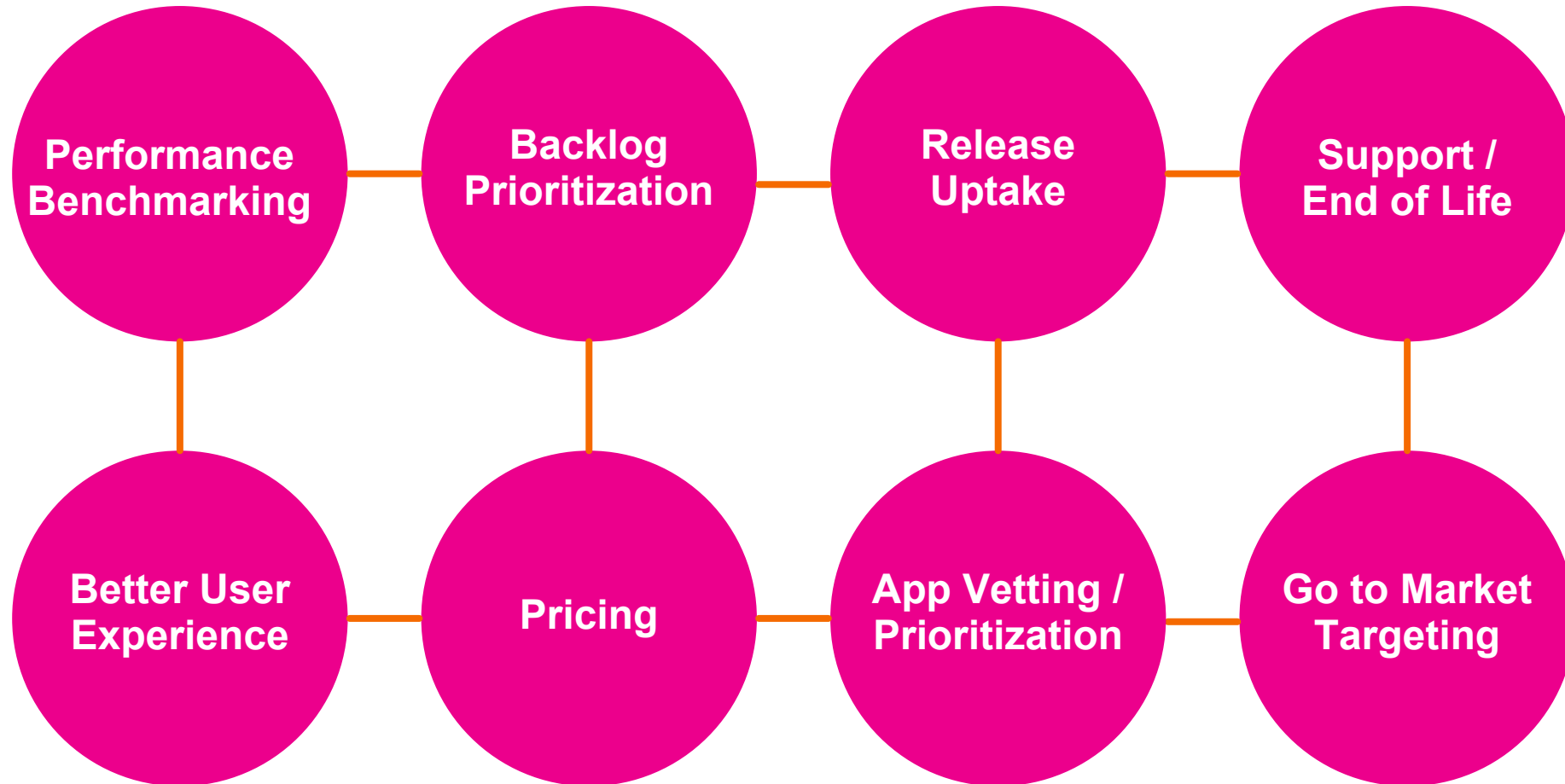
What Does Telemetry Look Like?

i	Time	Event
>	9/12/19 11:29:18.000 PM	<pre>{ [-] component: app.session.session_start data: { [+] } deploymentID: acad1ffb-9da1-5e72-80ef-595d4d700f6d eventID: d4165591-b34e-5734-5675-2c80c81ed06d experienceID: 7fb86762-64e3-3e7e-669e-801f5a3457aa timestamp: 1568330958 userID: 4c99702b43c02b7c01b0ebdc7d888a702e8e138efd4d4433190c6fa495457793 version: 3 visibility: anonymous,support }</pre> <p>Show as raw text</p> <p>host = acad1ffb-9da1-5e72-80ef-595d4d700f6d source = app.session.session_start sourcetype = _json</p>
>	9/12/19 11:29:05.000 PM	<pre>{ [-] component: app.session.session_start data: { [+] } deploymentID: acad1ffb-9da1-5e72-80ef-595d4d700f6d eventID: 3f684344-2641-4a00-84e7-5d376b3cedee experienceID: 0e900ef6-f866-f6b7-c4b2-43d19d343576 timestamp: 1568330945 userID: 4c99702b43c02b7c01b0ebdc7d888a702e8e138efd4d4433190c6fa495457793 version: 3 visibility: anonymous,support }</pre> <p>Show as raw text</p> <p>host = acad1ffb-9da1-5e72-80ef-595d4d700f6d source = app.session.session_start sourcetype = _json</p>

What Does Telemetry Look Like?

i	Time	Event
>	9/12/19 11:29:18.000 PM	<pre>{ [-] component: app.session.session_start data: { [-] app: search browser: Chrome browserVersion: 76.0.3809.100 device: MacIntel guid: B8E7D0B9-BB6E-41DB-928B-411ABBA5AD90 locale: en-US os: Mac OS X osVersion: 10. page: search splunkVersion: 7.3.1 } deploymentID: acad1ffb-9da1-5e72-80ef-595d4d700f6d eventID: d4165591-b34e-5734-5675-2c80c81ed06d experienceID: 7fb86762-64e3-3e7e-669e-801f5a3457aa timestamp: 1568330958 userID: 4c99702b43c02b7c01b0ebdc7d888a702e8e138efd4d4433190c6fa495457793 version: 3 visibility: anonymous,support } Show as raw text host = acad1ffb-9da1-5e72-80ef-595d4d700f6d source = app.session.session_start sourcetype = _json</pre>

What Has Splunk Used Telemetry For?








Deployment Health and Monitoring Console

Bharath Aleti
Director, Product Management

Health Overview and Alerts

Overview of Splunk Enterprise 8.0.0

Anomalies

Status	Description	Feature	Actions
	The number of extremely lagged searches (1) over the last hour exceeded the red threshold (1) on this Splunk instance	Search Scheduler Search Lag	Investigate
	The percentage of high priority searches delayed (33%) over the last 24 hours is very high and exceeded the red thresholds (10%) on this Splunk instance. Total Searches that were part of this percentage=3. Total delayed Searches=1	Search Scheduler Searches Delayed	Investigate
	The percentage of high priority searches skipped (33%) over the last 24 hours is very high and exceeded the red thresholds (10%) on this Splunk instance. Total Searches that were part of this percentage=3. Total skipped Searches=1	Search Scheduler Searches Skipped	Investigate

Deployment Topology





3 Indexers	1 Search Head
1 Cluster Master	3 License Masters
10 Indexes	

Deployment Metrics

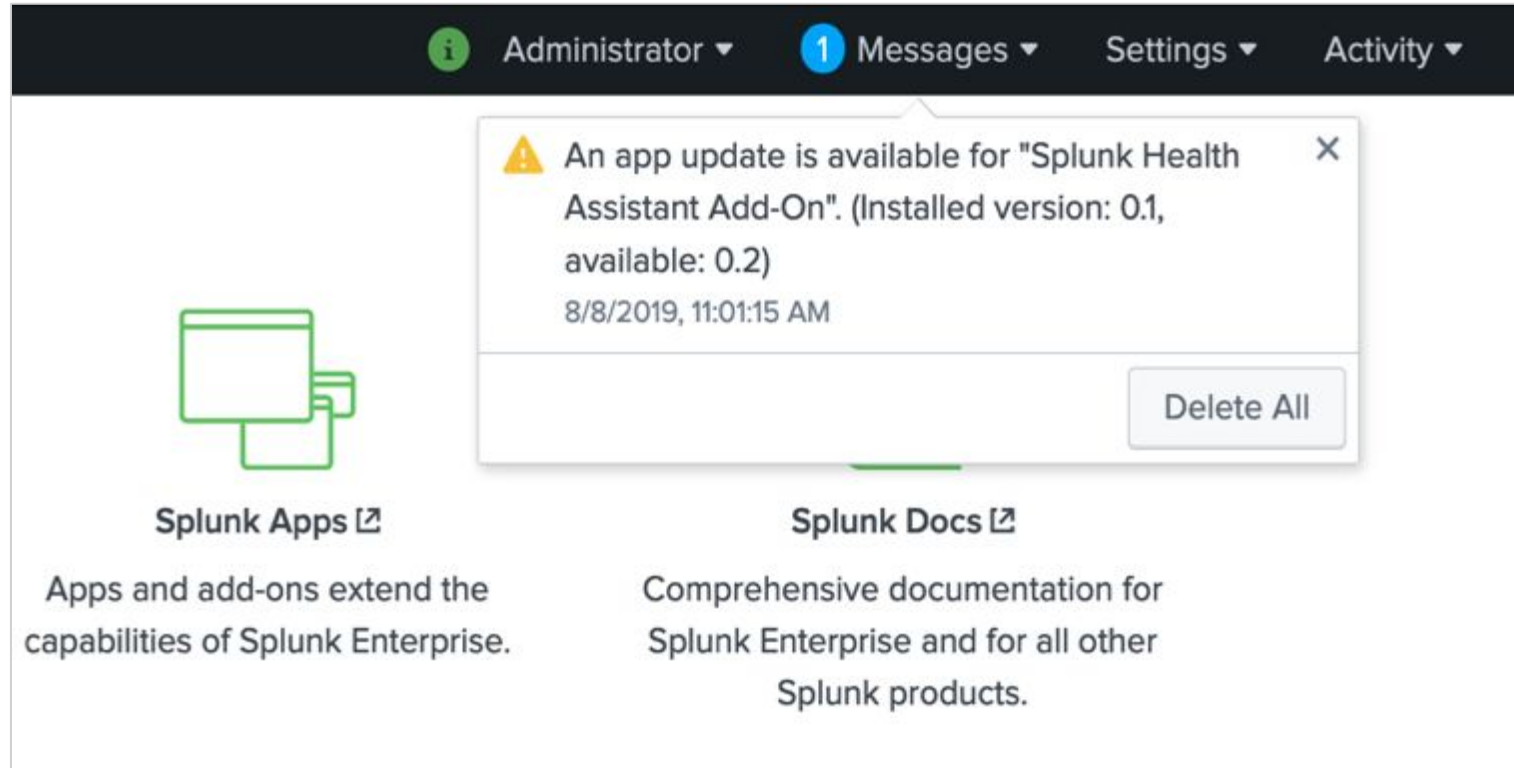
Last 24 hours Edit Panel

Avg. CPU Usage: All Indexers	20.67%
Avg. Mem Usage: All Indexers	45%
Avg. Skipped Searches	88.20%

Deployment Components

File Monitor Input	
Index Processor	
Indexer Clustering	
Search Scheduler	

Proactive Notification



The screenshot shows the Splunk web interface. At the top, there is a navigation bar with 'Administrator', 'Messages' (with a notification count of 1), 'Settings', and 'Activity'. A notification box is open, displaying a warning icon and the text: 'An app update is available for "Splunk Health Assistant Add-On". (Installed version: 0.1, available: 0.2) 8/8/2019, 11:01:15 AM'. A 'Delete All' button is located at the bottom right of the notification box. Below the notification, there are two main sections: 'Splunk Apps' and 'Splunk Docs'. 'Splunk Apps' includes an icon of overlapping documents and the text 'Apps and add-ons extend the capabilities of Splunk Enterprise.' 'Splunk Docs' includes an icon of a document and the text 'Comprehensive documentation for Splunk Enterprise and for all other Splunk products.'

Search Usage Statistics

Overview Summary Health Check Instances Indexing Search Resource Usage Forwarders Settings Run a Search Monitoring Console

Search Usage Statistics: Instance

Group: All Search Heads Instance: fool01.sv.splunk.com Time Range: Last 4 hours Only Ad Hoc Searches: Yes No [Hide Filters](#)

Search Activity by User (1)

User	Search Count	Median Runtime	90th Percentile Runtime	Cumulative Runtime	Last Search
1 splunk-system-user	2	5.77	9.79	11.53	2019-09-12 08:17:00

Frequently Run Searches

User: All

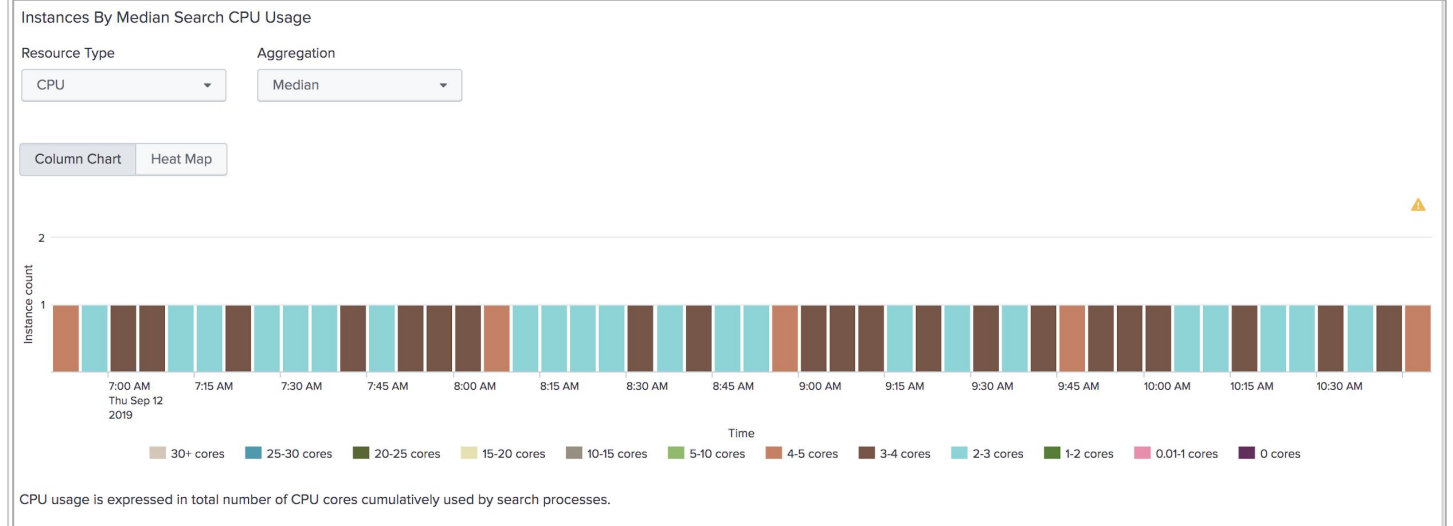
Search	Count	Median Runtime	Max Runtime	User
1 ' copybuckets json="{\"providers\": {}, \"vixes\": {}}"'	2	5.77s	10.80s	splunk-system-user

Long-running Searches

User: All

Search	Search Runtime	Search Start	Earliest Time	Latest Time	Type	User
1 ' copybuckets json="{\"providers\": {}, \"vixes\": {}}"'	10.80s	09/12/2019 08:17:00 -0700	all time	all time	ad hoc	splunk-system-user
2 ' copybuckets json="{\"providers\": {}, \"vixes\": {}}"'	0.73s	09/12/2019 07:17:02 -0700	all time	all time	ad hoc	splunk-system-user

Search Resource Usage



Top 20 Memory-Consuming Searches

	Name	Provenance	Memory Usage (MB)	Instance	Runtime	Started	Type	Mode	App	User	Role
1	test_sk_B	scheduler	954.52	mrt.sv.splunk.com	8min 50.84s	Thu Sep 12 07:06:55 PDT 2019	scheduled	historical batch	search	splunk-system-user	head
2	test_sk_A	scheduler	925.85	mrt.sv.splunk.com	8min 20.63s	Thu Sep 12 07:14:55 PDT 2019	scheduled	historical batch	search	splunk-system-user	head
3	test_lagged_a	scheduler	908.99	mrt.sv.splunk.com	7min 56.78s	Thu Sep 12 06:50:05 PDT 2019	scheduled	historical batch	search	splunk-system-user	head
4	test_sk_C	scheduler	834.42	mrt.sv.splunk.com	8min 41.23s	Thu Sep 12 06:58:25 PDT 2019	scheduled	historical batch	search	splunk-system-user	head
5	test_sk_D	scheduler	833.88	mrt.sv.splunk.com	9min 7.78s	Thu Sep 12 06:50:05 PDT 2019	scheduled	historical batch	search	splunk-system-user	head
6	test_lagged_a	scheduler	793.68	mrt.sv.splunk.com	7min 10.11s	Thu Sep 12 08:55:05 PDT 2019	scheduled	historical	search	splunk-system-user	head
7	N/A	unknown	39.02	mrt.sv.splunk.com	2.06s	Thu Sep 12 10:43:16 PDT 2019	ad-hoc	historical batch	splunk_monitoring_console	admin	head
8	N/A	unknown	36.59	mrt.sv.splunk.com	2.78s	Thu Sep 12 07:31:25 PDT 2019	ad-hoc	historical	splunk_archiver	splunk-system-user	head
9	N/A	unknown	34.97	mrt.sv.splunk.com	8.57s	Thu Sep 12 07:56:45 PDT 2019	scheduled	historical	search	splunk-system-user	head
10	N/A	unknown	34.56	mrt.sv.splunk.com	1.26s	Thu Sep 12 10:43:16 PDT 2019	ad-hoc	historical	splunk_monitoring_console	admin	head



Deployment Sizing and Performance Benchmarking

Tracy Knight
Director, Product Performance

Splunk Sizing Calculator

Helps Customer capacity planning

Populate workload default based on 80th% customer usage patterns

Splunk Sizing Calculator v1.0 - Beta

Hello, Splunker

Splunk Enterprise & App Version

Server Specifications

Index and Search

Cluster & Storage

Parallelization Tuning

SFDC Ticket Info

Workload Specification

Index Volume Range (1000-5000 GB/day)

Daily Indexing Volume

3000 GB

Daily Search Count

70000

1 SEARCH HEAD

11 INDEXERS

Total Physical CPU Cores: 24

Total Physical CPU Cores: 264

Calculate Export Reset

Daily Total Volume: 3,000 GB | 272.73 GB/Indexer

Result Analysis Resource Usage Storage Details

Topology

Distributed Non-Clustered Deployment (D1 / D11)

Search Tier

SH

Management

DS

LM

MC

Indexing Tier

Indexer

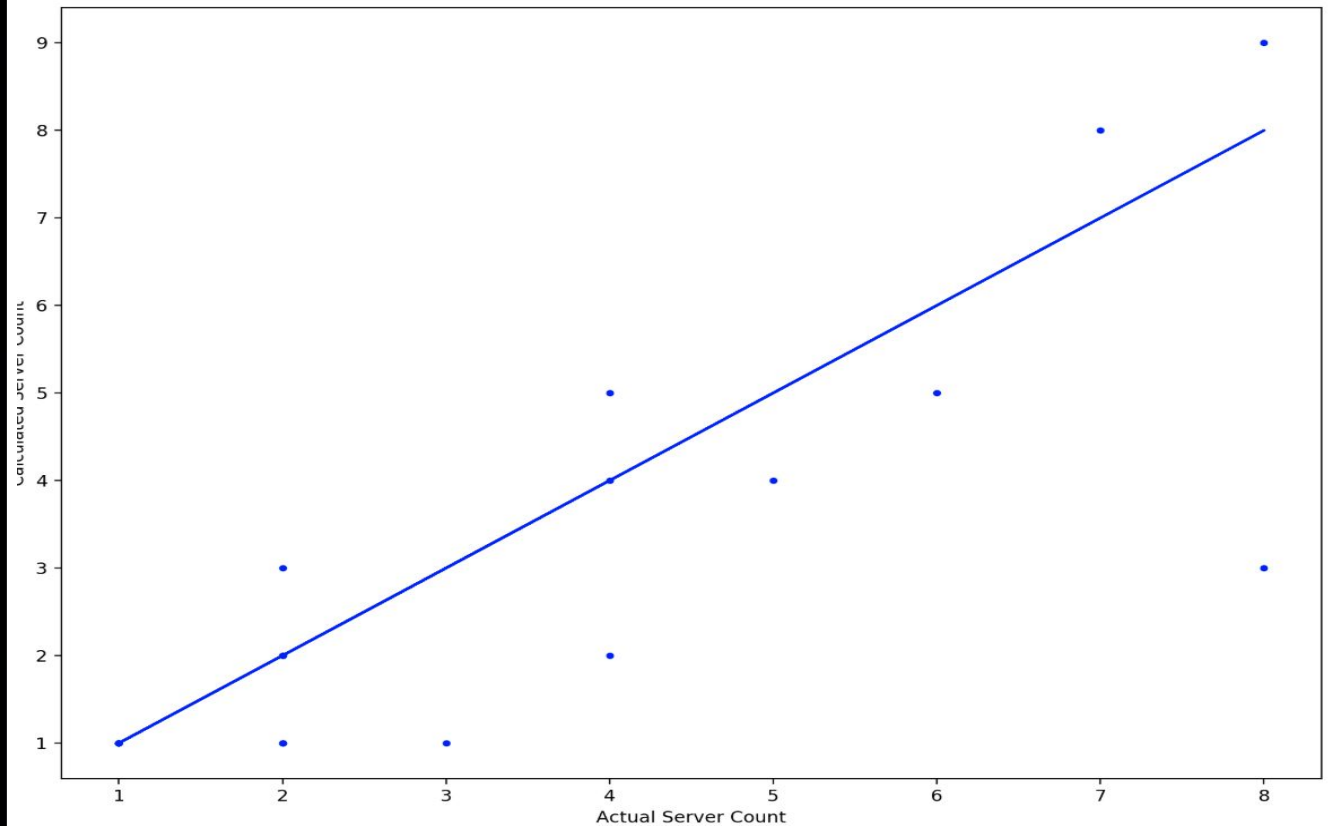
Indexer

Indexer

Splunk Sizing Calculator

Accuracy Validation

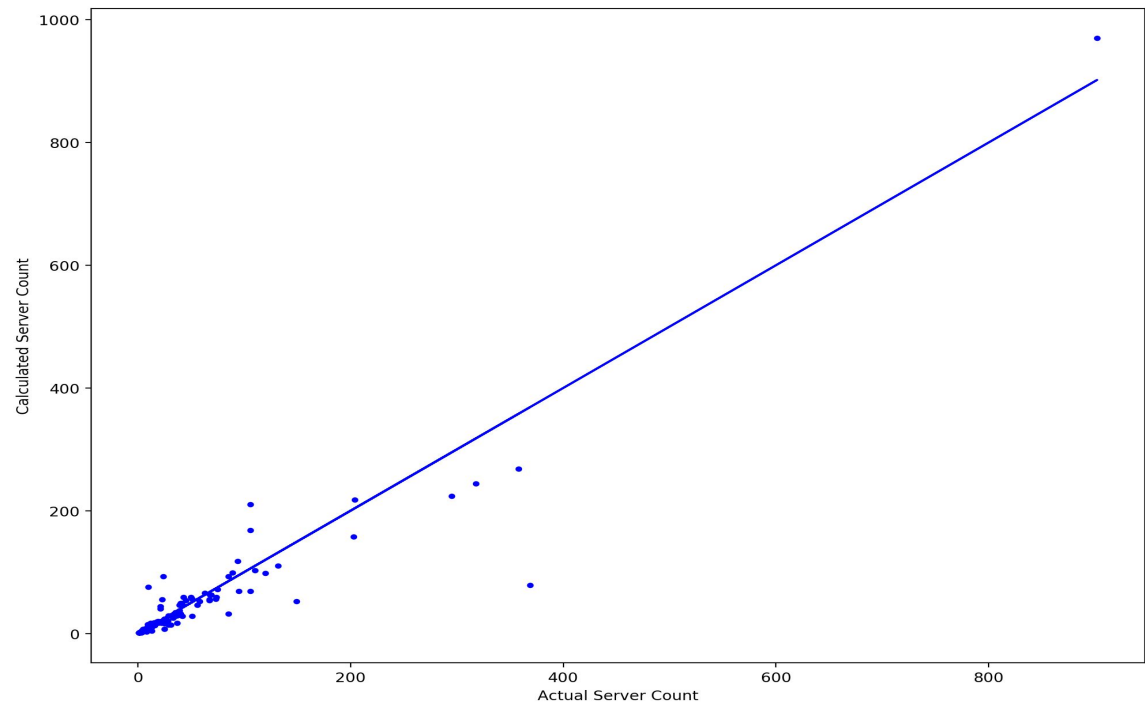
Leverage anonymous
telemetry data



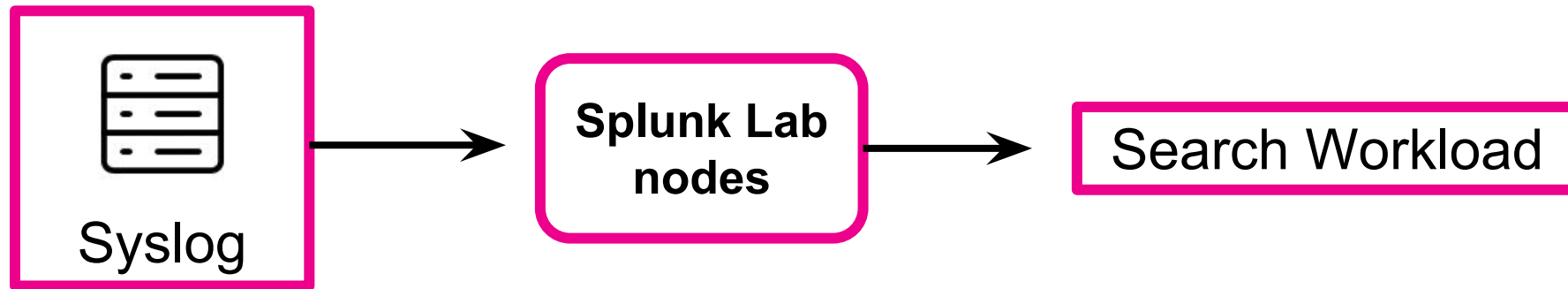
Splunk Sizing Calculator

Accuracy Validation

Leverage anonymous
telemetry data



We listen to data through telemetry

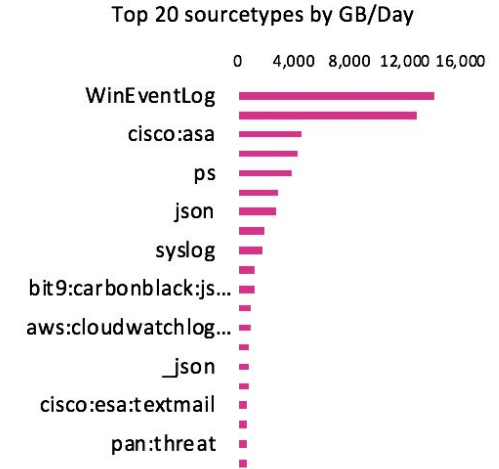
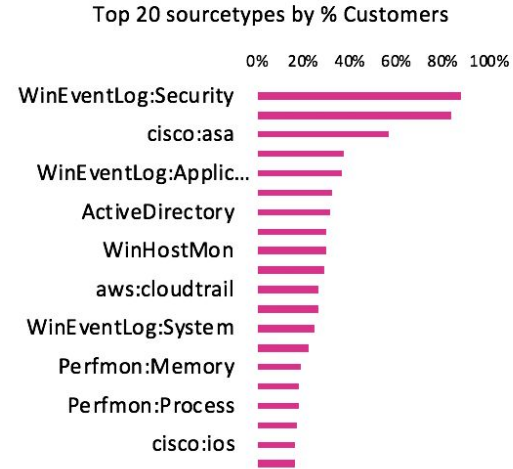
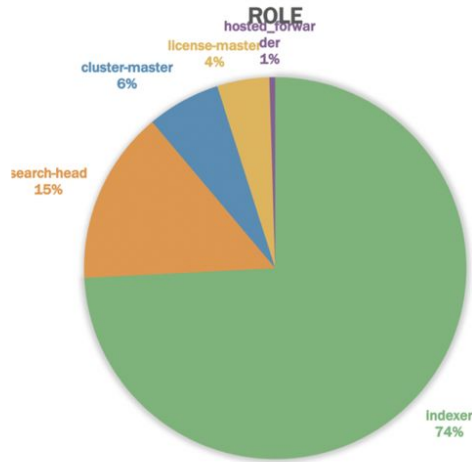


Performance Benchmark Design

We listen to data through telemetry

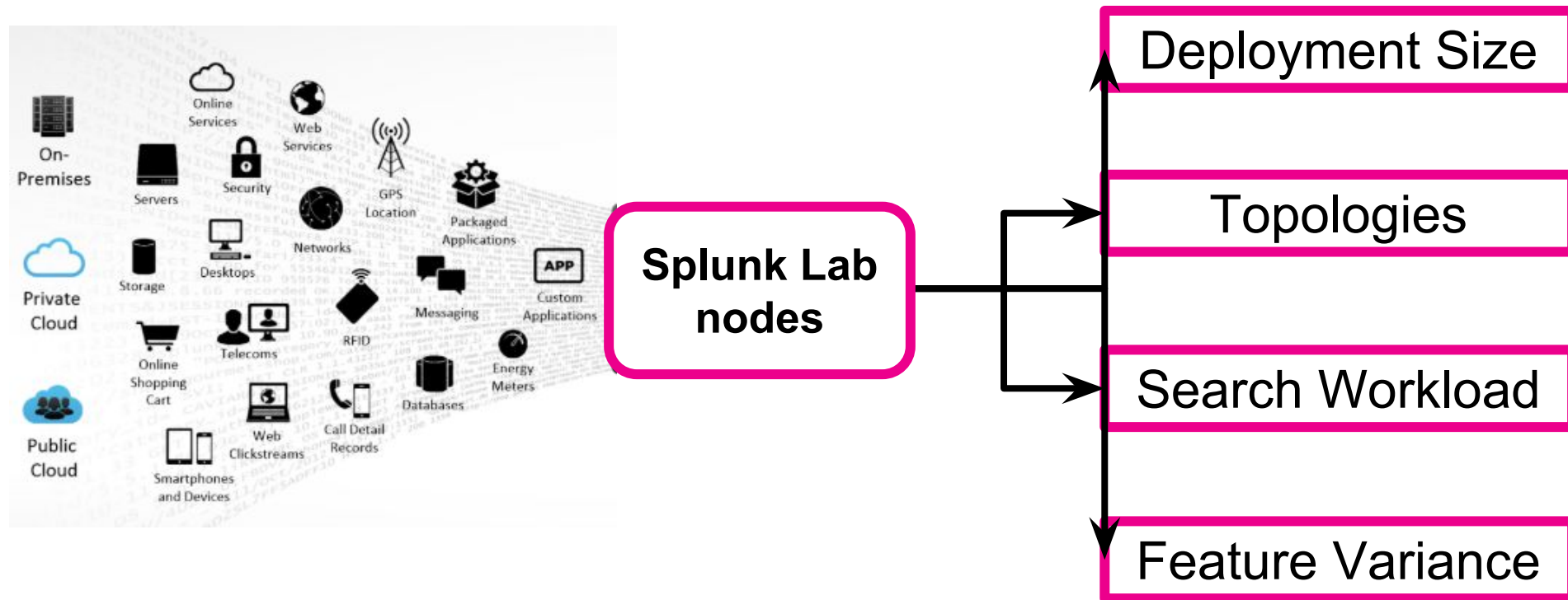
Telemetry data analysis

Enhance Performance benchmarks based on a generalization of statistics by Telemetry



Search Load	Saved Searches	DMA	Correlation	User-defined	Ingest Rate
AVG	40	22	12	6	358
MAX	257	164	93	78	4,265
80-PERCENTILE	64	31	23	7	448
90-PERCENTILE	88	53	33	12	738

We listen to data through telemetry



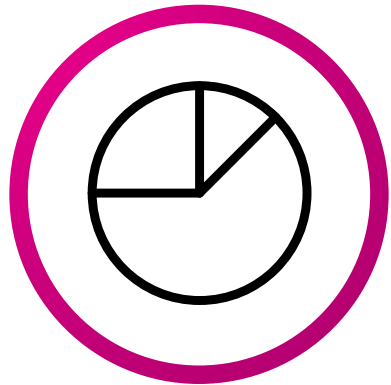


Product Analytics

Kevin Louther
Data Analyst

Common Questions

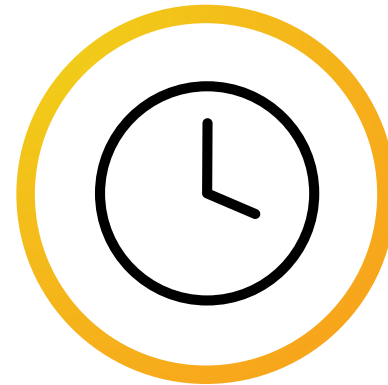
How many users
are using my
app?



What is the most
used operating
system?



How much time is
spent in my app?



What is the most
common Splunk
version?



Raw Telemetry

i	Time	Event
>	9/12/19 11:42:31.000 PM	<pre>{ [-] component: app.session.dashboard.load data: { [+] } deploymentID: 0099ff91-5d36-525f-8b40-9924168f9c12 eventID: b23e2199-c22a-fdb0-bc45-3c446f3ff477 experienceID: 61c1aacc-0b18-128d-4465-91a7477db3a2 timestamp: 1568331751 userID: 448e81fd88cca1fb9edf8bc4ca77962187585c670f08834991e2842510cb7fb0 version: 3 visibility: anonymous,support }</pre> <p>Show as raw text</p> <p>host = 0099ff91-5d36-525f-8b40-9924168f9c12 source = app.session.dashboard.load sourcetype = _json</p>
>	9/12/19 11:42:30.000 PM	<pre>{ [-] component: app.session.pageview data: { [+] } deploymentID: 0099ff91-5d36-525f-8b40-9924168f9c12 eventID: 093454c6-95d5-6ab7-e83d-dbe8caffa972 experienceID: 61c1aacc-0b18-128d-4465-91a7477db3a2 timestamp: 1568331750 userID: 448e81fd88cca1fb9edf8bc4ca77962187585c670f08834991e2842510cb7fb0 version: 3 visibility: anonymous,support }</pre> <p>Show as raw text</p> <p>host = 0099ff91-5d36-525f-8b40-9924168f9c12 source = app.session.pageview sourcetype = _json</p>

App Usage

App Usage

Edit Export ▾ ...

Previous month ▾

Customer Type
Paying ▾

Find My App (SPL)
*

Uncheck to Hide Help

Hide Filters



Help

- For Telemetry information please see: [Inventory of Existing Product Telemetry](#)
- For further questions please e-mail: products-datainsights@splunk.com
- Note: Telemetry data searchable from June 2018

Click Row For Per App Details

App Name ↕	appid ↕	Number of Deployments ↕	Number of Users ↕
launcher	launcher	2570	13070
search	search	2538	13321
splunk_monitoring_console	splunk_monitoring_console	1131	8926
Splunk DB Connect	splunk_app_db_connect	341	4447
Lookup File Editor	lookup_editor	310	4161
SplunkEnterpriseSecuritySuite	SplunkEnterpriseSecuritySuite	278	2837
Splunk App for Windows Infrastructure	splunk_app_windows_infrastructure	244	1569
Splunk Security Essentials	Splunk_Security_Essentials	219	1451
Splunk Add-on for Amazon Web Services	Splunk_TA_aws	192	2151
Splunk Dashboard Examples	simple_xml_examples	175	2305

« prev 1 2 3 4 5 6 7 8 9 10 next »

Splunk Versions JSON

```
> 9/12/19      { [-]
  11:49:49.000 PM  component: app.session.session_start
                   data: { [-]
                     app: $SPLUNK_PLATFORM
                     browser: Chrome
                     browserVersion: 47.0.2526.69
                     device: Linux armv7l
                     guid: 09EC3DF1-428B-4D51-A0CC-B278FF05FCF2
                     locale: en-US
                     os: Linux
                     osVersion: not available
                     page: embed
                     splunkVersion: not available
                   }
  deploymentID: 7a0afc65-15b4-5718-b508-86eb31febf5
  eventID: 6e6677db-8079-6af7-a37a-b7d982373036
  experienceID: 1db7f460-496c-57a3-4e3d-64529cc282f5
  timestamp: 1568332189
  userID: a42214201707b8ab7f83afd1da167b237a982a25ee364d913fdec11594efa34
  version: 3
  visibility: anonymous,support
}
Show as raw text
host = 7a0afc65-15b4-5718-b508-86eb31febf5 | source = app.session.session_start | sourcetype = _json
```

Splunk Versions

Splunk Versions

Click on Deployment ID to get Splunk version details

Deployment ID ↕	Splunk Versions on Deployment ↕
23b7a19d-7b6d-5172-9744-089802ecc1b8	3
24EEF8FC77928FC32BF3165B5C26E3	3
2643d57c-26f3-5260-9b53-aaf594534c99	3
2778C7223A449264120A767DAE8120	3
278a811e-4119-52c1-a433-0186882a94b9	3
297cf77f-ed9a-5515-b9af-aaf9249d142a	3
299f0fe9-d0f4-502f-84f7-be1cb161ff28	3

Splunk Version Details

Node Version Search

Forwarder Version Search

Search Head Version

To search for specific versions, search in the respective box above

Node Versions ↕

7.1.1

Search Head Versions ↕

7.1.1

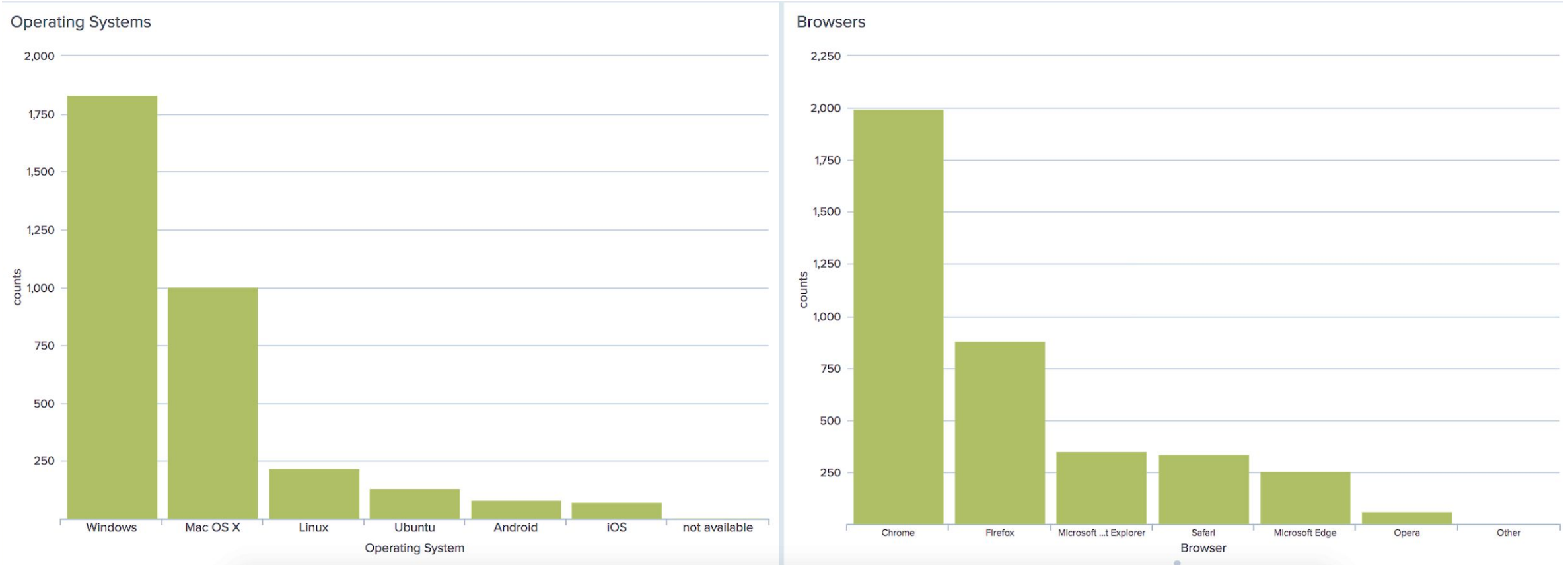
Forwarder Versions ↕

7.1.1

7.1.2

7.3.0

OS + Browser Versions

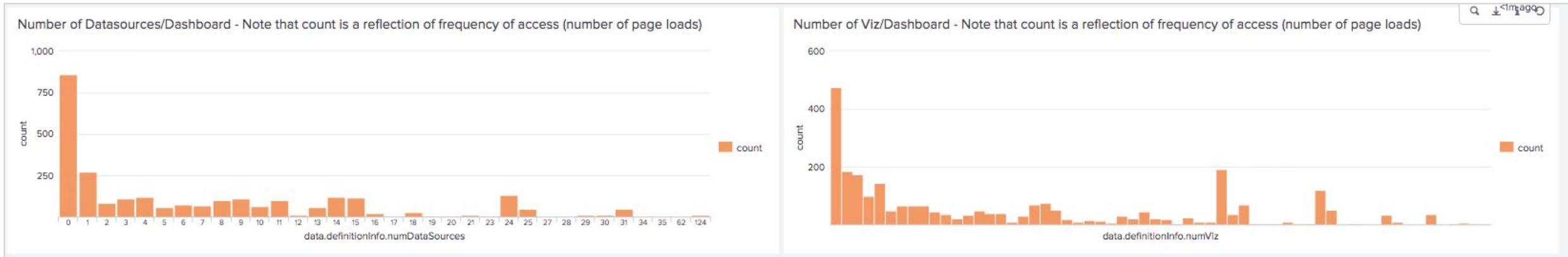




User Interface and Dashboard Framework

Miranda Luna
Senior Product Manager

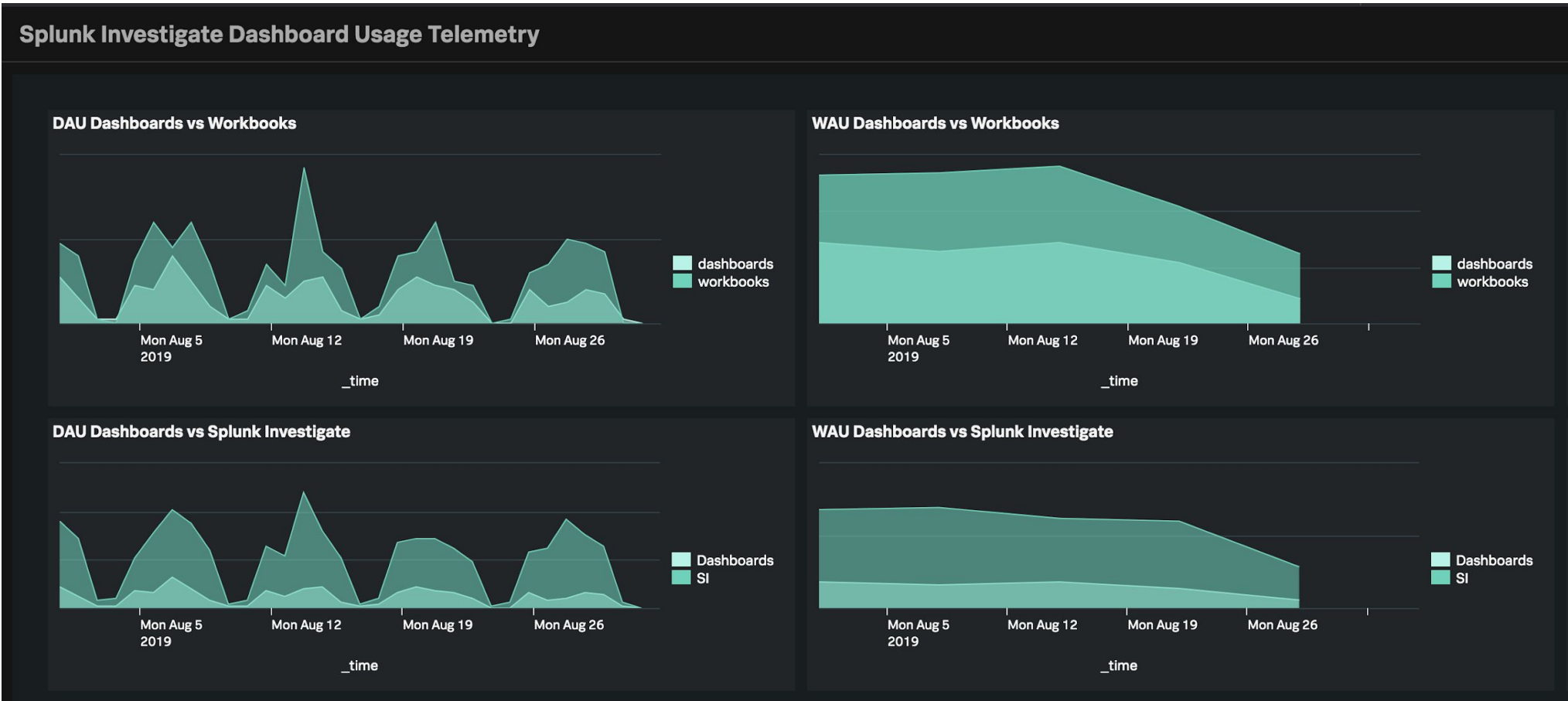
What are the Key Elements to Storytelling?



What Inputs to Prioritize for Simple XML Transition?



Are We Enabling All Users to Become Storytellers?





Enhanced Support

David Alward
Senior Escalation Manager

Instrumentation

Configure automated reporting settings, view collected data, export data to file, work with diagnostic files, and send data to Splunk. [Learn More](#)

Usage Data ⚙️

Sharing your software usage data helps Splunk Inc. optimize your deployment, prioritize our features, improve your experience, notify you of patches, and develop high quality product functionality.

[Learn more](#) ↗️

Aggregated Usage Data

Enabled

To improve our products and offerings, we collect aggregated data about feature usage, performance, deployment topology, infrastructure, and operating environment. This data is not linked to your account. [Learn more](#) ↗️

Support Usage Data

Enabled

To provide you enhanced support and help you troubleshoot and improve your implementation, we collect aggregated data about feature usage, performance, deployment topology, infrastructure, and operating environment. This data is linked to your account using your license GUID. [Learn more](#) ↗️

License Usage Data

To ensure compliance with your purchased offering, we collect data about your license consumption. This data is linked to your account using your license GUID. [Learn more](#) ↗️

Automatically enabled

Software Version Data

To understand the number of customers using older versions of Splunk software, we collect anonymized software version data. [Learn more](#) ↗️

Automatically enabled

Share Telemetry for Enhanced Support

Settings

➔ Instrumentation
➔ Usage Data

Python 3 Readiness

Deployment ID ↕	Unsupported Apps ↕	Number of Unsupported Apps ↕	Total Apps Being Used ↕
00180209-f9b8-539f-90d7-95f56dea3734	Cisco eStreamer eNcore Add-on for Splunk CyberSponse Add-on for Splunk Lookup File Editor SSL Certificate Checker Sideview Admin Tools Sideview Utils (free internal use license)	6	54
00bf7c17-8ddf-5685-92eb-e0bd5ac81265	Lookup File Editor Website Monitoring	2	10
013c7314-722f-5254-87fe-e47d7d278073	CylancePROTECT App for Splunk Demisto App for Splunk F5 Networks - LTM FireEye App for Splunk Enterprise v3 G Suite For Splunk Google Apps for Splunk Input Add On for G Suite App Input Add On for Netskope Lookup File Editor MAC Address Vendor Scripted Lookup Microsoft Log Analytics Add-on (Formerly Known as OMS)	15	67

Enterprise Security EOL

deploymentID	host	data.name	data.version	data.splunkVersion	ES	ES_compatibility	ES_compatible
16b903d2-f4cd-54ea-b9a3-892982dde3d0	16b903d2-f4cd-54ea-b9a3-892982dde3d0	SplunkEnterpriseSecuritySuite	5.2.2	7.2.3	Yes	5.3.1, 5.3.0, 5.2.2, 5.2.1, 5.2.0, 5.1.1	Yes
172ba4ad-c13b-54f2-b116-a44f766a3d82	172ba4ad-c13b-54f2-b116-a44f766a3d82	SplunkEnterpriseSecuritySuite	5.3.1	7.2.7	Yes	5.3.1, 5.3.0, 5.2.2, 5.2.1, 5.2.0, 5.1.1	Yes
1DC20527E077A07317C532BF150FB2	1DC20527E077A07317C532BF150FB2	SplunkEnterpriseSecuritySuite	4.5.3	7.2.4	Yes	5.3.1, 5.3.0, 5.2.2, 5.2.1, 5.2.0, 5.1.1	No
1a0ff5a5-d606-544b-a3f4-0e16cc7f67dc	1a0ff5a5-d606-544b-a3f4-0e16cc7f67dc	SplunkEnterpriseSecuritySuite	4.7.2	7.1.3	Yes	5.3.1, 5.3.0, 5.2.2, 5.2.1, 5.2.0, 5.1.1, 5.1.0	No
1b117c87-43d3-5fa1-a8c4-aa72c2558f13	1b117c87-43d3-5fa1-a8c4-aa72c2558f13	SplunkEnterpriseSecuritySuite	5.2.2	7.2.4	Yes	5.3.1, 5.3.0, 5.2.2, 5.2.1, 5.2.0, 5.1.1	Yes
1b2fdab0-10a3-5997-ae7b-0e5565fb3124	1b2fdab0-10a3-5997-ae7b-0e5565fb3124	SplunkEnterpriseSecuritySuite	5.3.1	7.3.1	Yes	5.3.1, 5.3.0	Yes



Archana Ganapathi
Director, Data Strategy



David Alward
Senior Escalation Manager



Tracy Knight
Director, Product Performance



Bharath Aleti
Director, Product Management



Miranda Luna
Senior Product Manager



Kevin Louther
Products Data Analyst



splunk>

Thank

You



Go to the .conf19 mobile app to

RATE THIS SESSION

