



splunk&gt;

# App Dev's Introduction to SDC

Tristan Fletcher | Architect, IT Markets

October 2018



# 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.

Splunk, Splunk>, Listen to Your Data, 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. © 2018 Splunk Inc. All rights reserved.



**Tristan**  
**tfletcher@splunk.com**

## ► About

- Formerly: Manager, UI/Systems/QA Engineer
- San Francisco, sometimes Santana Row
- Worked at Splunk for 7 years
- Surprise Villain at the Splunk Roll20 DnD Group

# Goals



Understand the difference in how apps are deployed on SDC v Classic



Understand the motivation and general design behind SDC



Know where to go for more information



# Agenda

## 1. Big Honkin' Overview

## 2. Core Services

## 3. Data Ingestion

## 4. Search Technology

## 5. Apps

## 6. Q&A

# Big Honkin' Overview

---

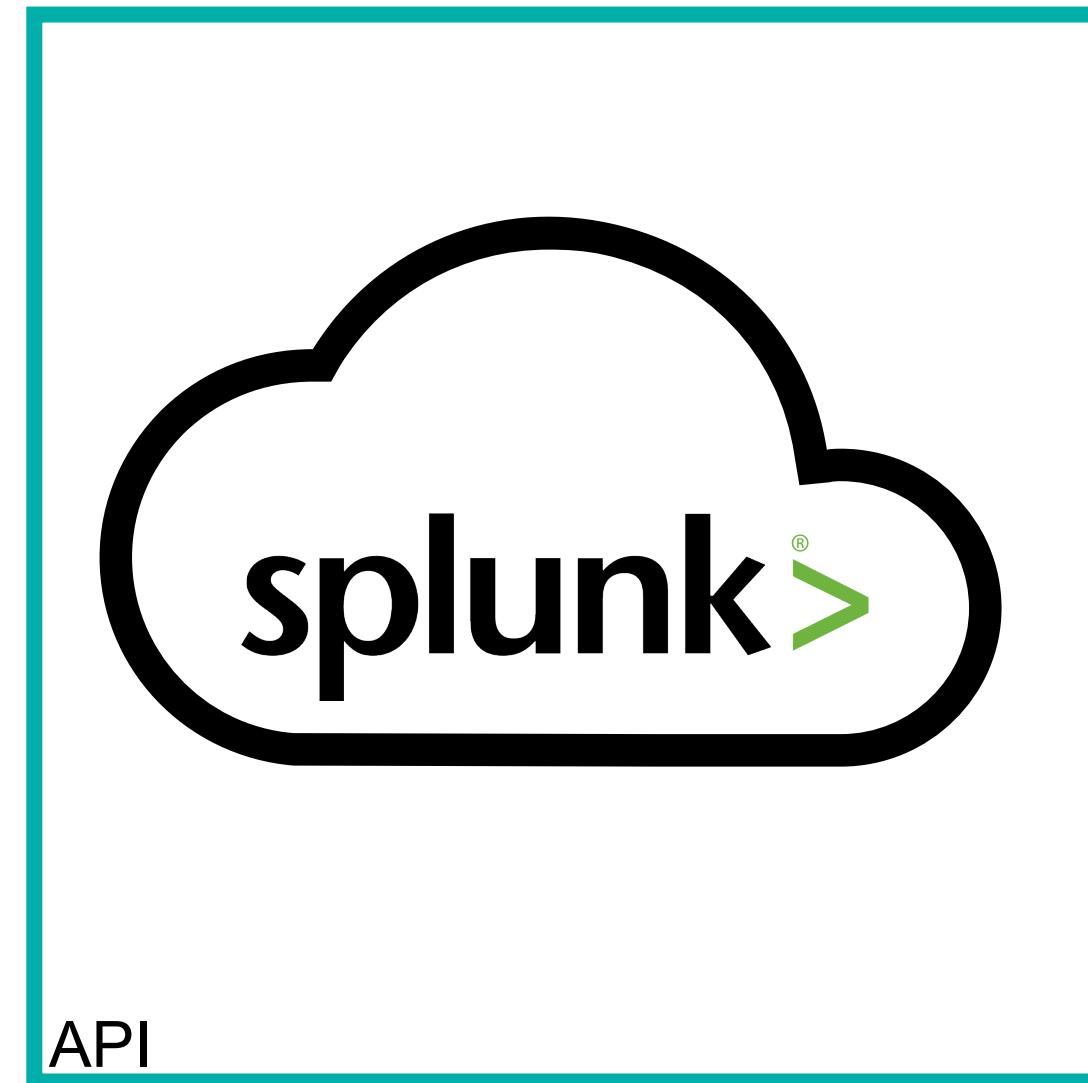
## AKA WTF (is) SDC



# What's different about developing in SDC?



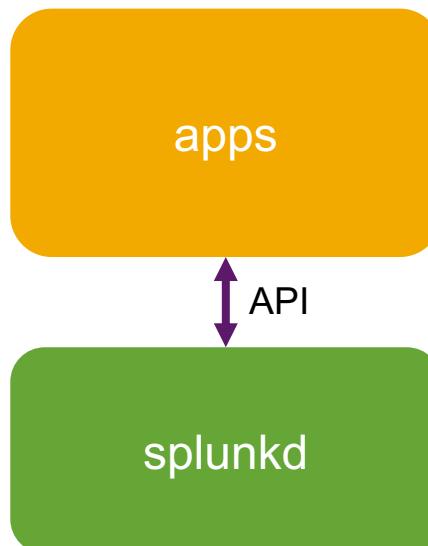
# WTF is SDC



AP

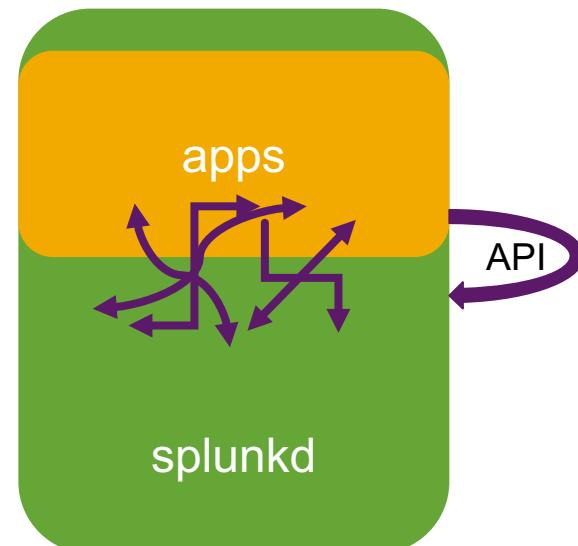
# But Splunk Enterprise is API-driven...

# Perception



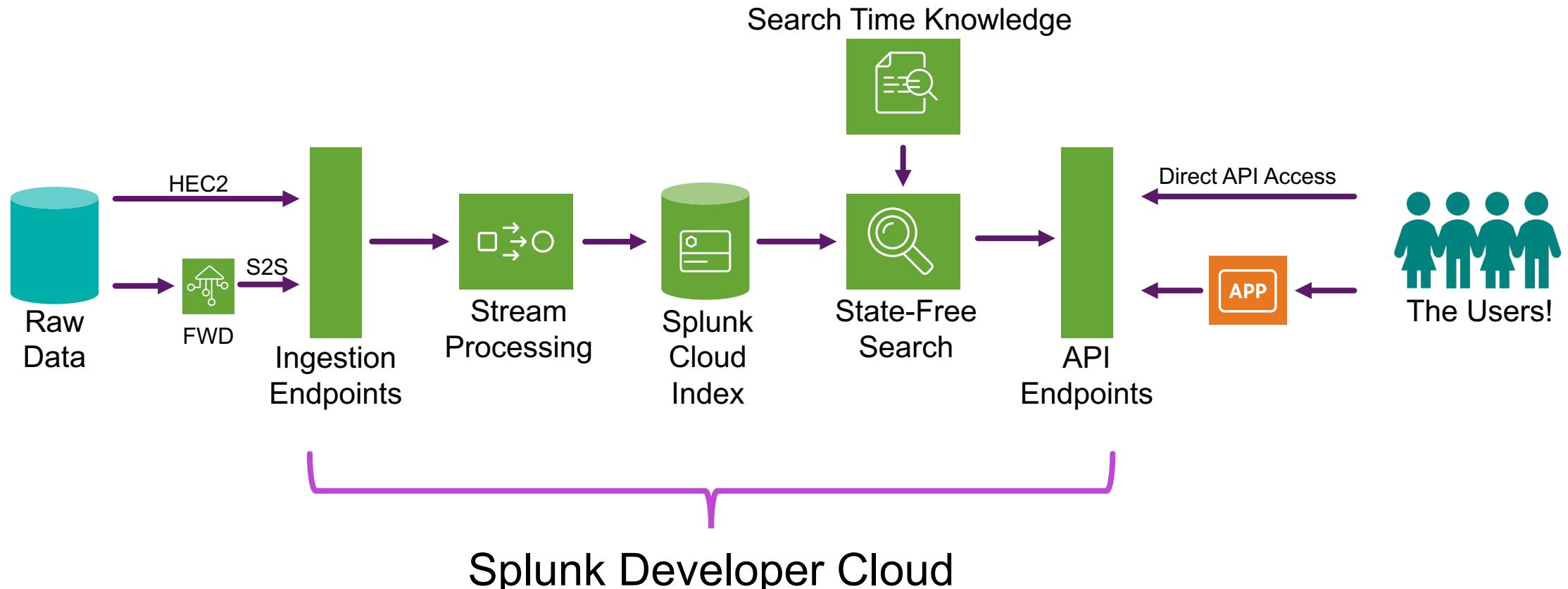
**We want to  
get here**

## Reality



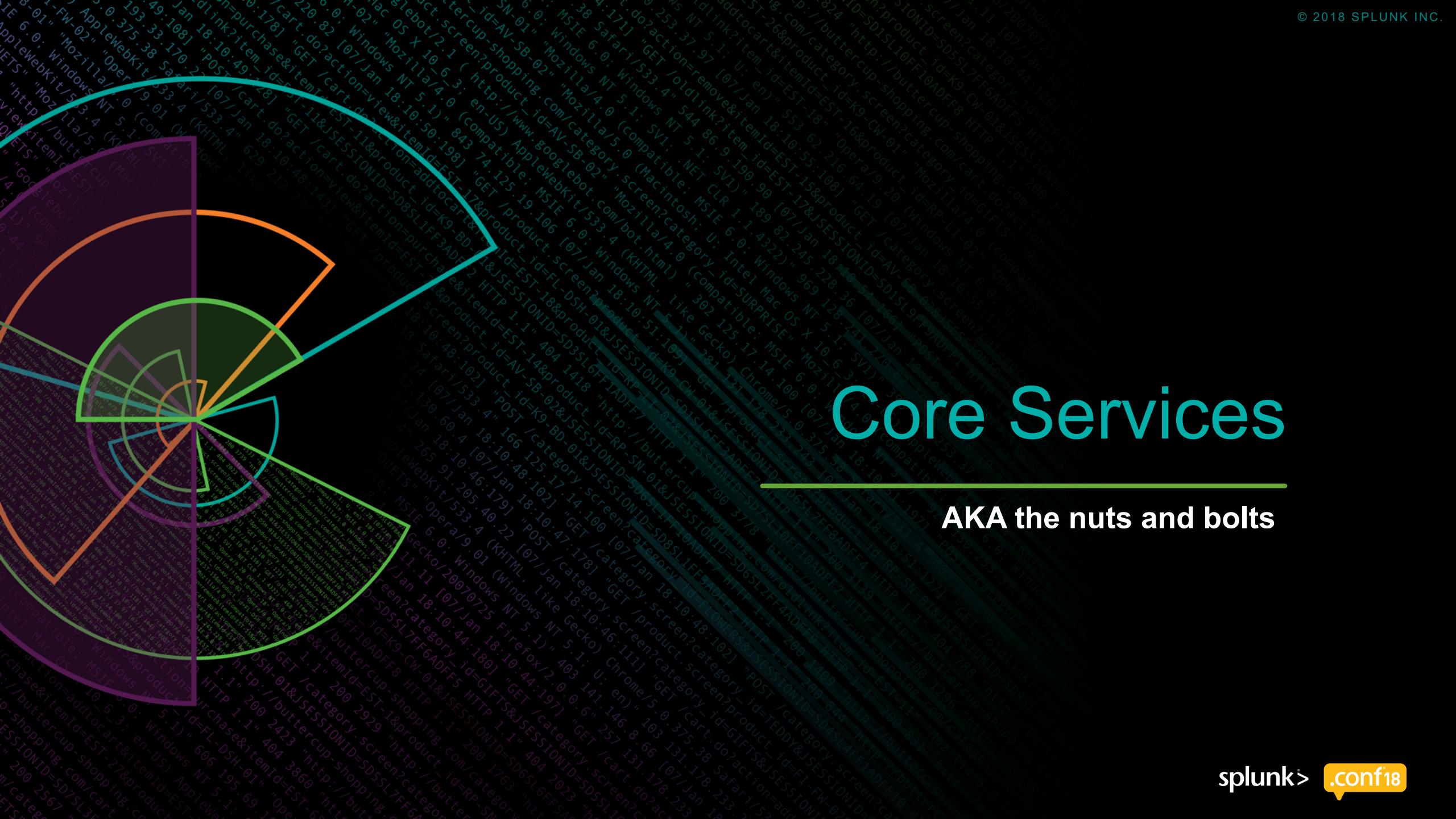
- ▶ Developing apps in Splunk Enterprise is not a delightful experience
    - Lacks significant functionality that apps are forced to “re-invent” every time
    - Too many implementation and deployment details are exposed (e.g. search head clustering)
    - Many interactions outside of the API (e.g. apps write to the file system, use of deployer, etc.)
    - Very limiting authorization model

# A Day in the Life of Data

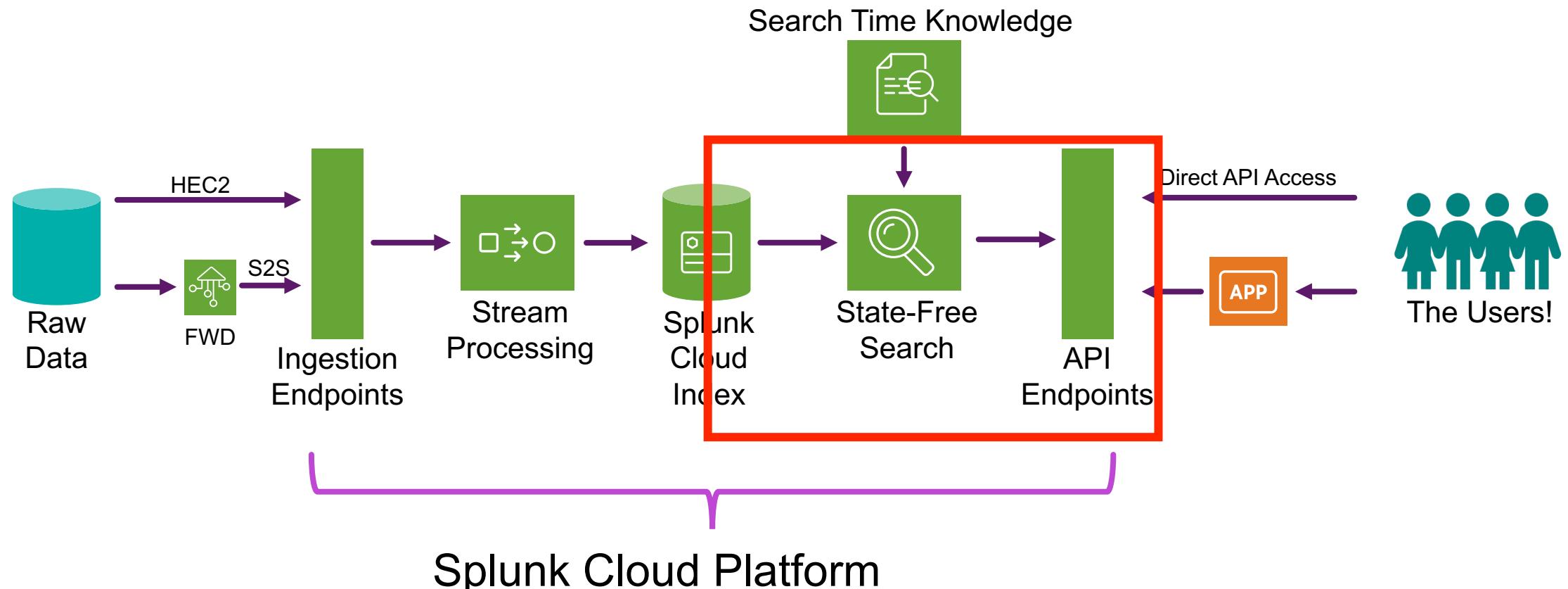


# Core Services

AKA the nuts and bolts



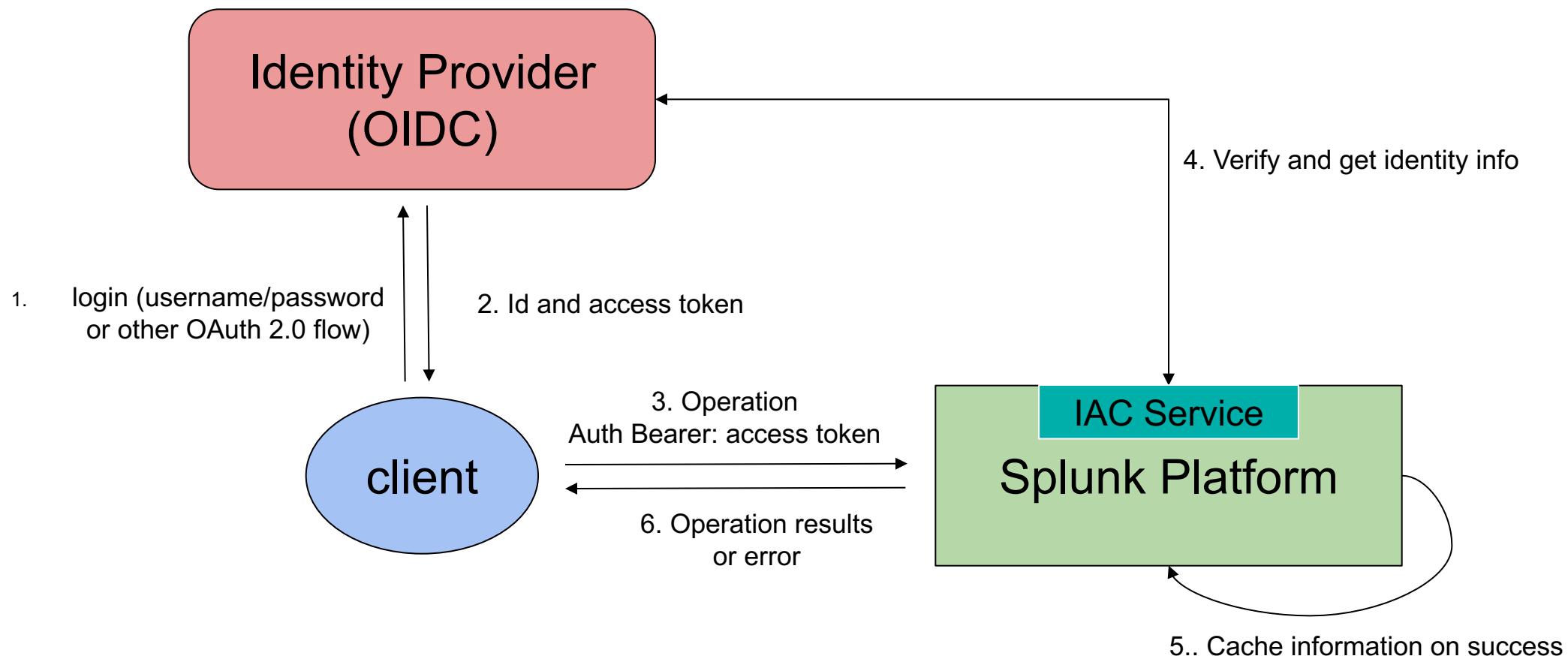
# A Day in the Life of Data



```

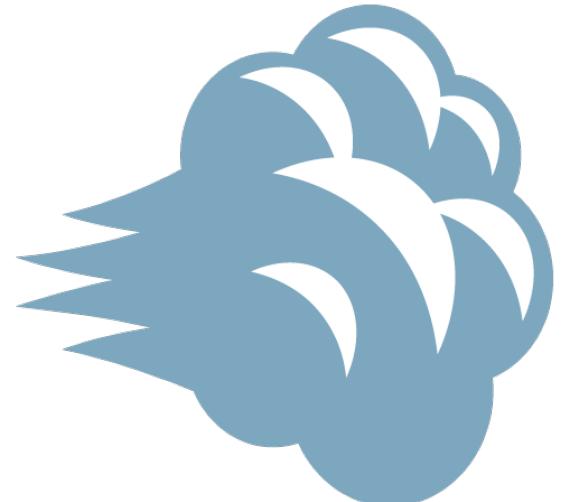
138.60.4 - - [07/Jan/18:10:57:153] "GET /category.screen?categoryId=EST-0&productId=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-0&productId=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 404 3322 "http://buttercup-shopping.com/cart.do?action=putInCart&itemId=EST-2&productId=S059L4FFA0DFE" HTTP/1.1 200 2423 "http://buttercup-shopping.com/cart.do?action=putInCart&itemId=EST-2&productId=S059L4FFA0DFE" HTTP/1.1 200 3865 "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST-18&productId=S059L4FFA0DFE" HTTP/1.1 200 3865 "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST-6&productId=S059L4FFA0DFE" HTTP/1.1 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&productId=S059L4FFA0DFE" HTTP/1.1 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-6&productId=S059L4FFA0DFE" HTTP/1.1 200 3865
    ...
  
```

# Cloud Authentication Workflow

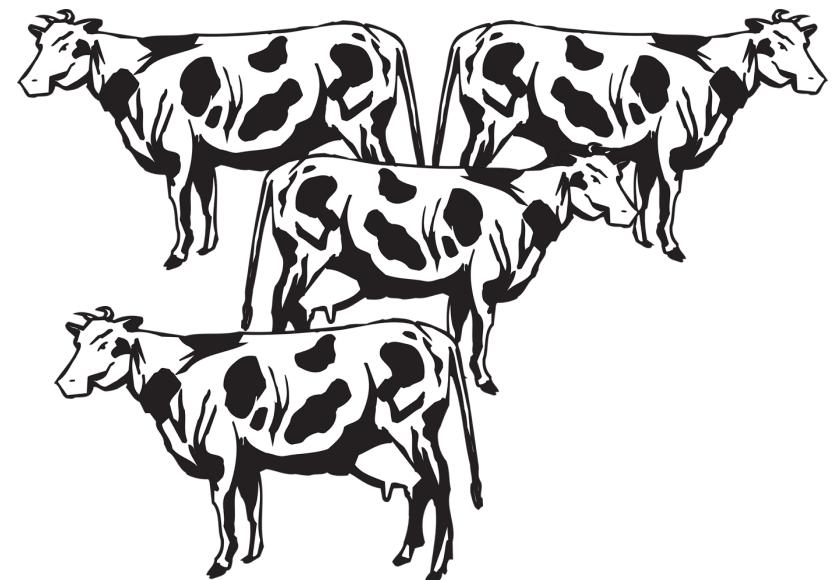


# Cloudifying Deployment Scaling

**splunk>enterprise**  
► SHC, Search Peers



**splunk>Developer Cloud**  
► State-Free Search



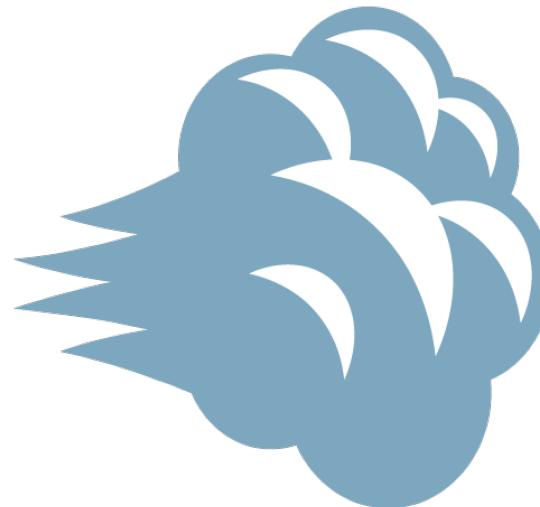
```

138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_0&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "128.241.220.82 - - [07/Jan 18:10:57:153]" "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 332 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_2&product_id=F1-ZZ1111/4.0" "Scomparti 2013/01/09 09:55:1891" "GET /oldlink?item_id=EST_26&product_id=EST_6&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 4318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST_18&productId=EST_18&product_id=AU-COOL-SESSIONID=SD55L8BF2D0EFFF HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changecount?itemId=EST_6&JSESSIONID=SD55L8BF2D0EFFF HTTP 1.1" 200 3865 "GET /category.screen?category_id=EST_0&product_id=EST_0&JSESSIONID=SD55L8BF2D0EFFF HTTP 1.1" 200 3865
    
```

# Cloudifying KV Store

splunk>enterprise

- ▶ KV Store
  - (collections.conf)



splunk> Developer Cloud

- ▶ KV Store
  - (Dataset in Catalog)



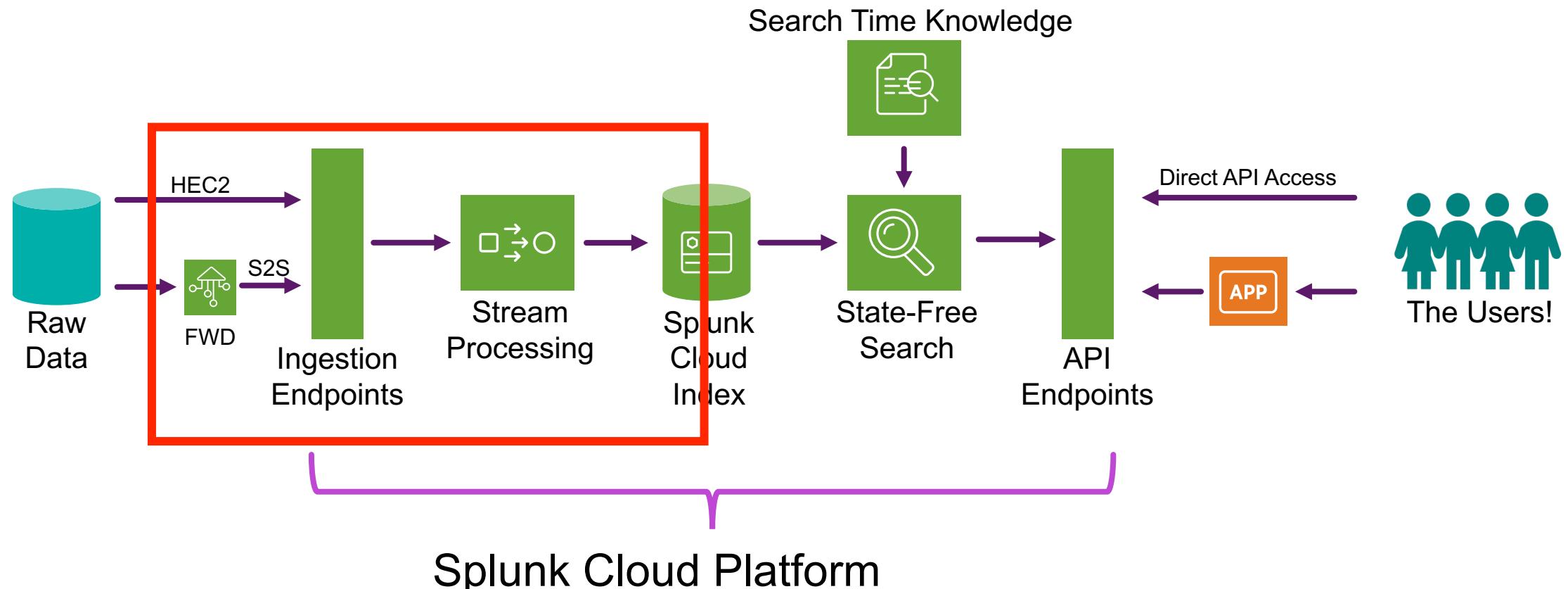
```
138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322) AppleWebKit/4.0 (KHTML, like Gecko) Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07/Jan 18:10:57:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=updateSession" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 4318 "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST-18&product_id=EST-6&SESSIONID=SD55L8FF2ADFF5 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=oldlink?item_id=EST-18&product_id=EST-6&SESSIONID=SD515LBFF2ADFF5" [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-6&product_id=EST-26&SESSIONID=SD55L8FF2ADFF5 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&SESSIONID=SD55L8FF2ADFF5" [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07/Jan 18:10:57:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=updateSession" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 4318 "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST-18&product_id=EST-6&SESSIONID=SD55L8FF2ADFF5 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=oldlink?item_id=EST-18&product_id=EST-6&SESSIONID=SD515LBFF2ADFF5 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&SESSIONID=SD55L8FF2ADFF5"
```

# Data Ingestion

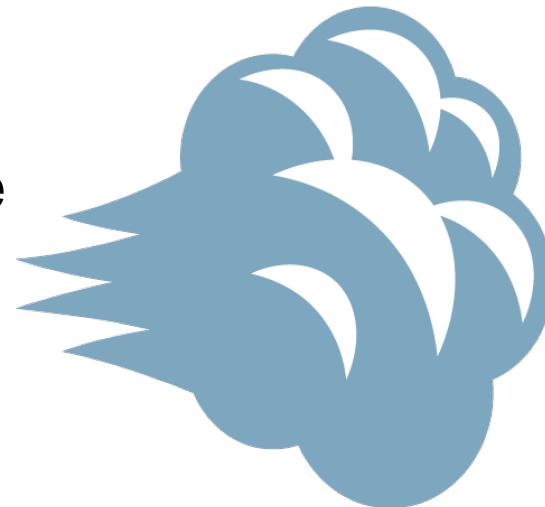
AKA data, it's what apps crave



# A Day in the Life of Data



# Cloudifying Index Transforms



# splunk>enterprise

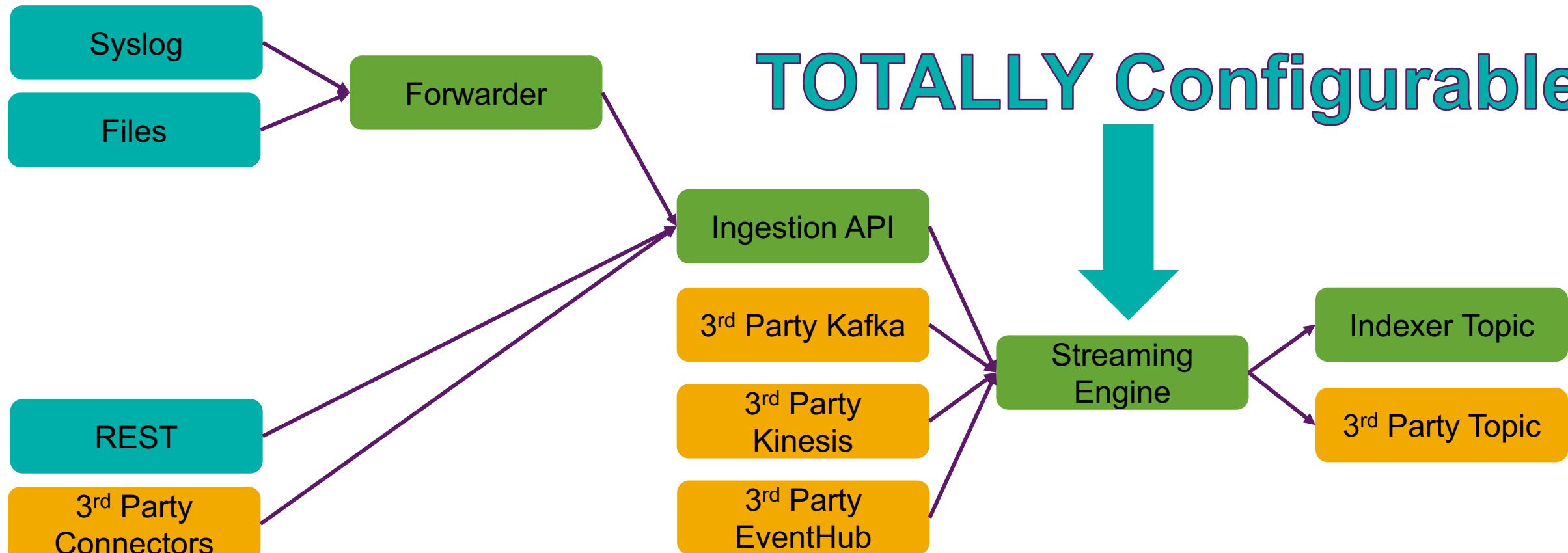
- ## ► Indexed Fields, Null Queue

# splunk> Developer Cloud

- ## ► BLAM Pipelines

  - (Data Availability APIs)

# Overview



# Stream Processing – Why?

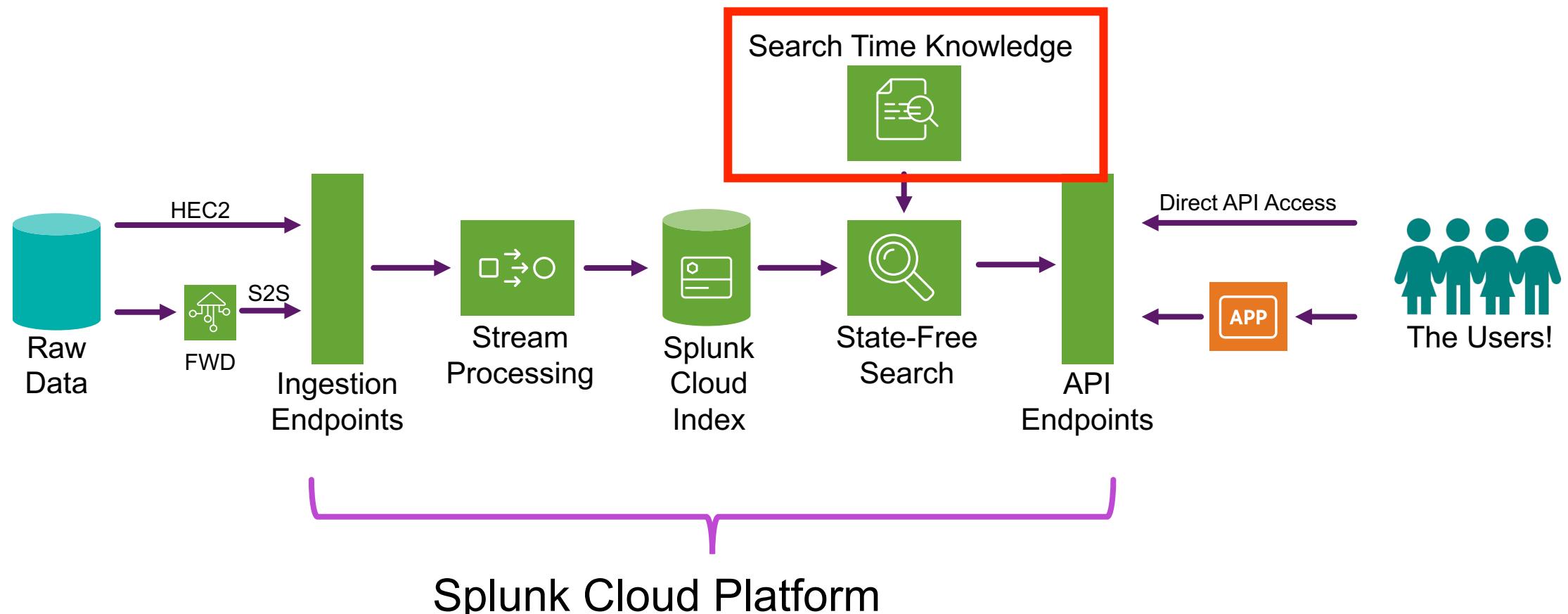
- ▶ Complement Splunk's query-time data wrangling with ingest-time wrangling
    - Building metrics from events
    - Pre-extract and enrich to make common queries simpler
    - Advanced routing of events
    - Enforce data quality standards
    - “Really realtime” searches and metrics
    - Move expensive saved searches to ingest-time triggers

# Search Technology

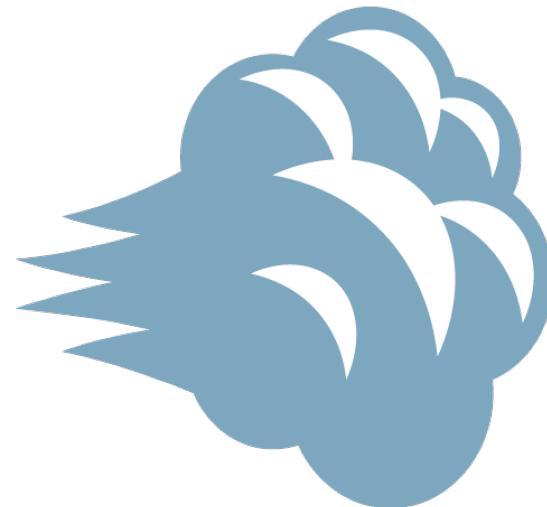
AKA accessing data



# A Day in the Life of Data



# Cloudifying Data Storage



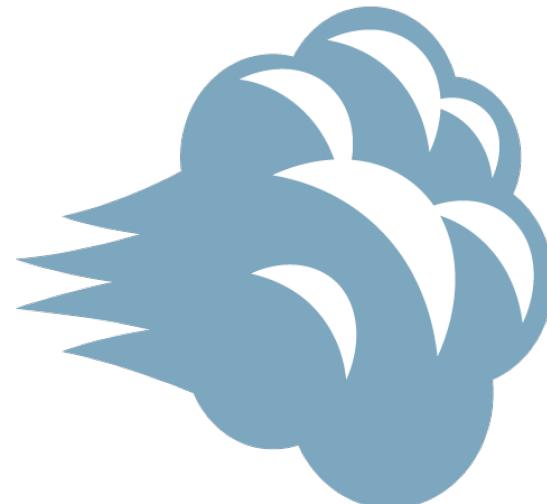
# splunk>enterprise

- ▶ Indexes, Collections, Saved Searches
    - (`indexes/savedsearches/collections.conf`)

# splunk> Developer Cloud

- ## ► Datasets in Catalog

# Cloudifying Search Time Knowledge



# splunk>enterprise

- ▶ Field Extractions, Aliases etc.
    - (props/transforms.conf)

# splunk> Developer Cloud

- ## ► Rules and Actions in Catalog

# Cloudifying Search Time Knowledge

# splunk>enterprise

# splunk> Developer Cloud

```
[sourcetype::testlog]
FIELDALIAS-user = uid as user
EXTRACT-errors = dvc=\[w+\](?<err_id>[^:]++)
EVAL-company = coalesce(company, "NA")
LOOKUP-product_info = products ID AS pid OUTPUT Name
AS product_name
KV MODE = auto
```

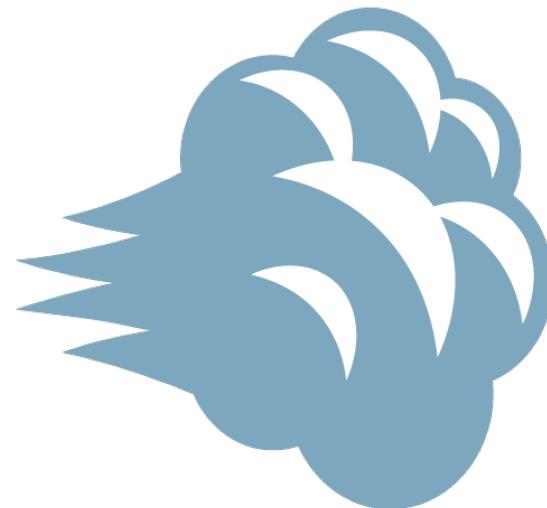
```
{  
    "id": "#id#",  
    "name": "#name#",  
    "module": "#module#",  
    "match": "sourcetype::testlog",  
    "actions": [ ... ]  
        { ...,  
        { "id": "#id#",  
            "id": "#id#,AS",  
            "kind": "AUTOKV",  
            "mode": "AUTO"products ID AS pid OUTPUT  
                }]}product_name, Category as product_category",  
}        "owner": "user"  
        }, ... ]  
}
```

# Cloudifying Lookups

# splunk>enterprise

# ► Lookup

- (transforms.conf,  
collections.conf, csv)



# splunk> Developer Cloud

## ► Datasets in Catalog

- (Only KV Store based)

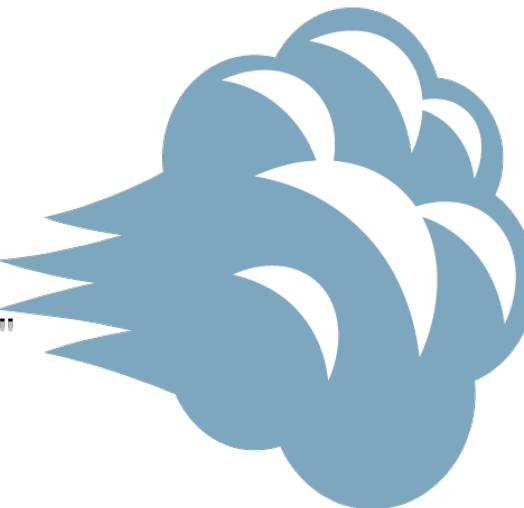
# Cloudifying SPL

**splunk>enterprise**  
► SPL

```
index=main err*
| head 100

| mstats latest(_value) AS cost
WHERE index=metrics metric_name="cpu"
BY host span=1s
```

```
index=main
| stats count BY host
```



**splunk>Developer Cloud**  
► SPLv2

```
| from index:main
| search err*
| head limit=100

| from metric:metrics
WHERE metric_name="cpu"
GROUP BY host, span(_time, 1m)
SELECT latest(_value) as cost, host

| from index:main
GROUP BY host
SELECT count(), host
```

# Cloudifying App Namespaces

**splunk>enterprise**  
► App Namespaces



**splunk> Developer Cloud**  
► Modules

To learn more go to:  
[Intro to SPLv2, the Module System and the Catalog](#) Thu 1:30pm

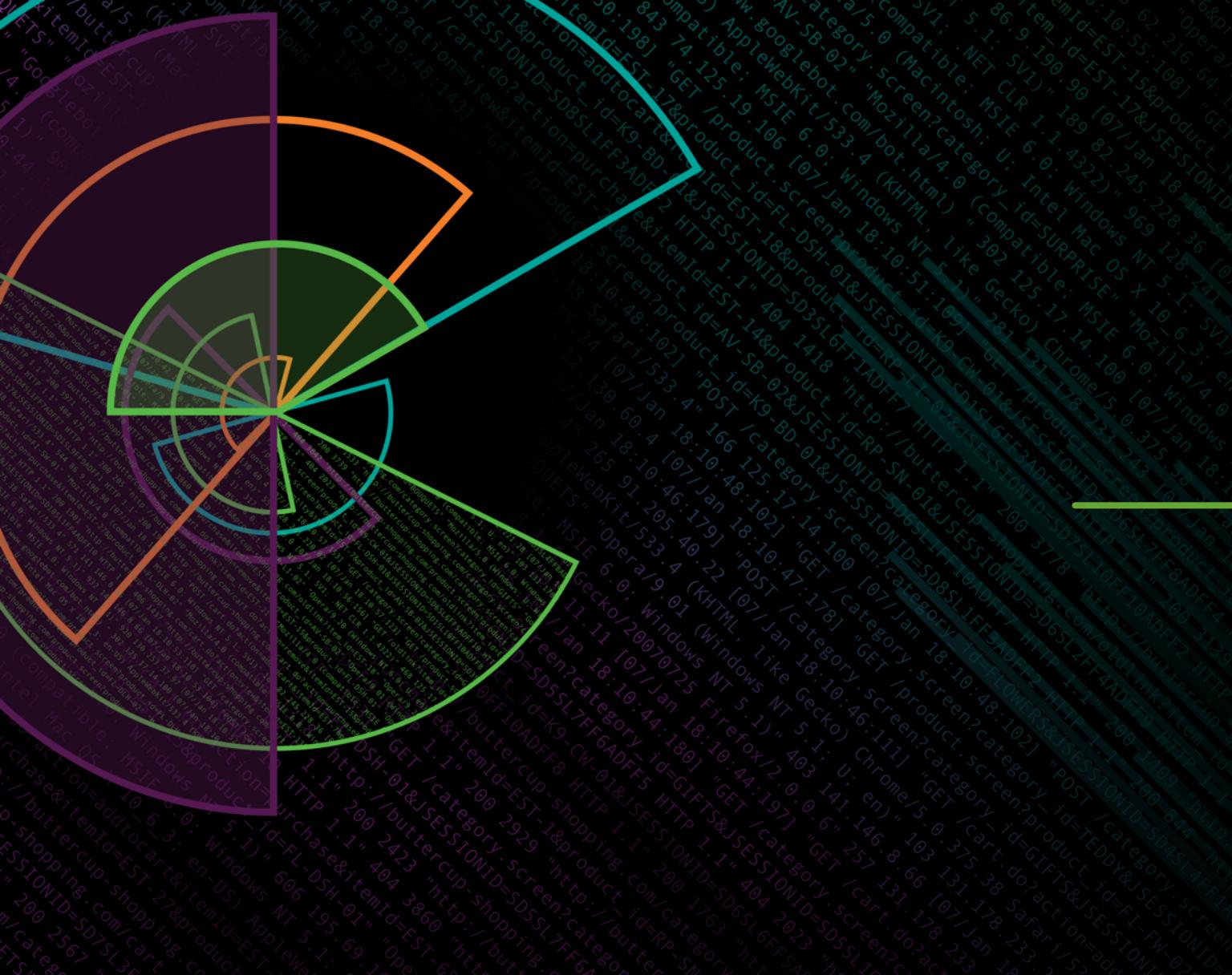
# No Clear Analog

- ▶ Search Scheduling
- ▶ Eventtypes/Tags
- ▶ EAI REST Interfaces
- ▶ Modular Inputs

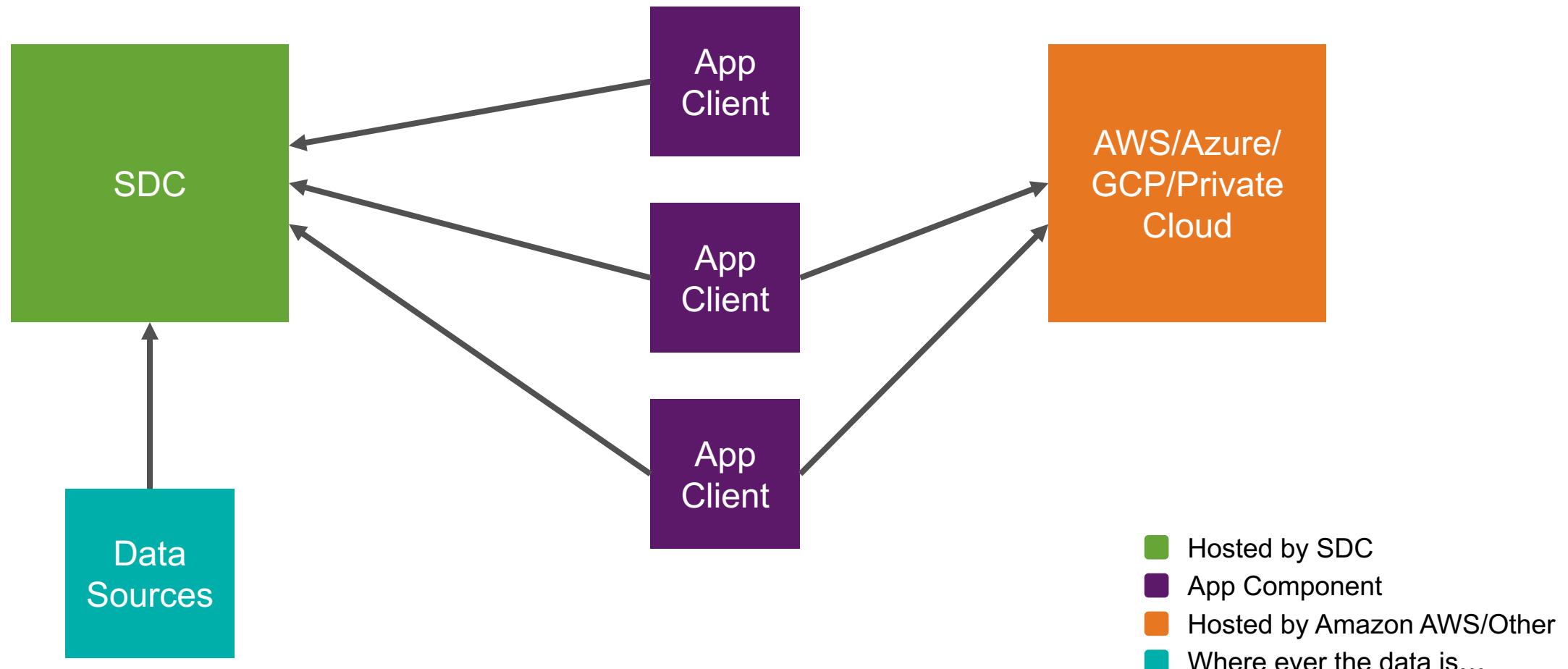


# Apps

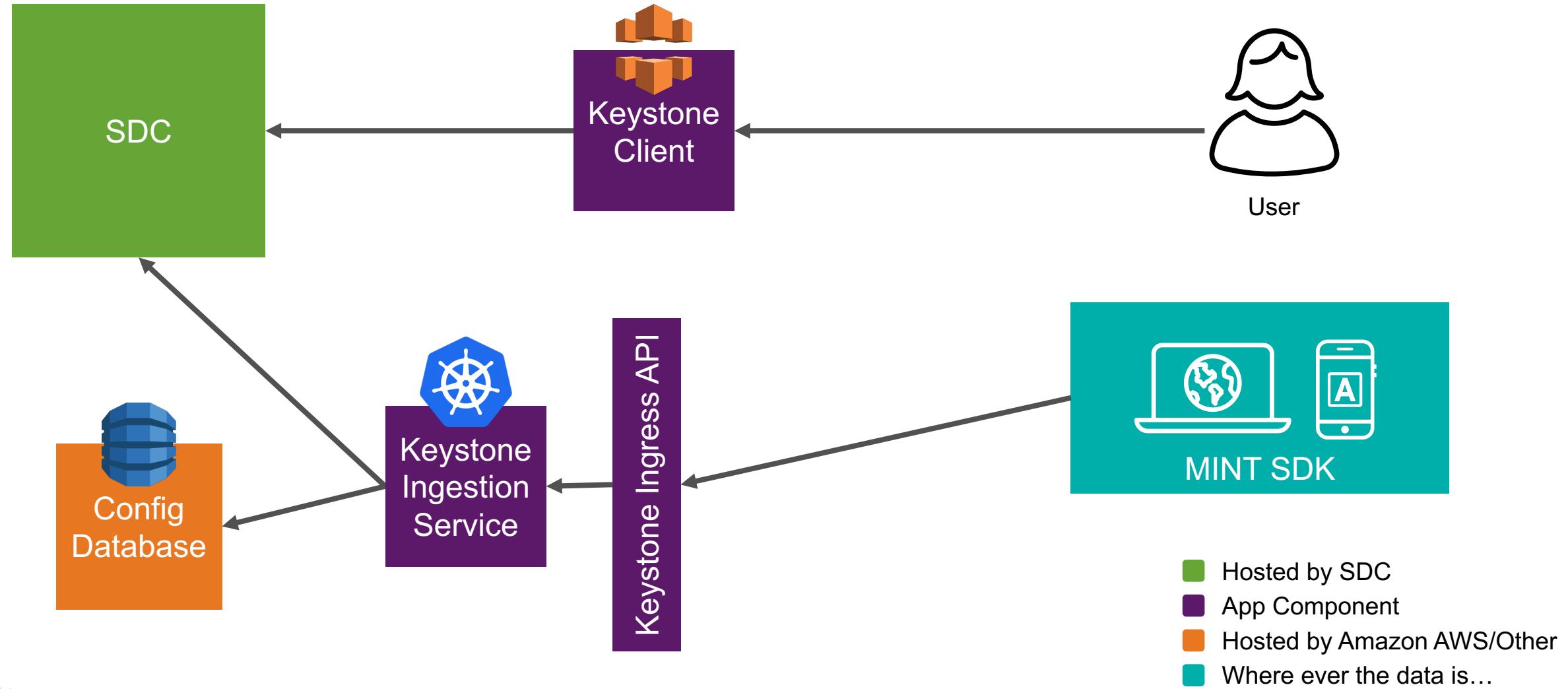
AKA what you build!



# Future of App Deployments



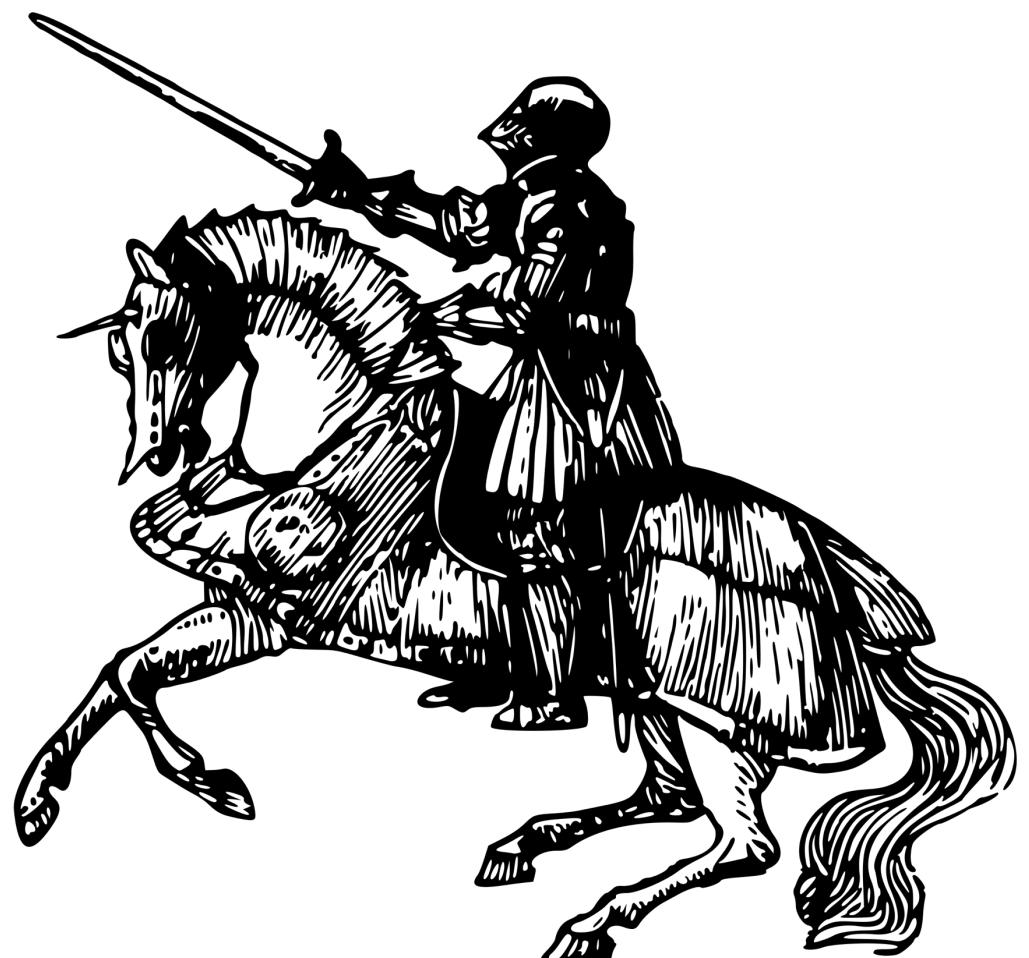
# Splunk Insights for Web and Mobile Apps Architecture



- Hosted by SDC
- App Component
- Hosted by Amazon AWS/Other
- Where ever the data is...

# Where To Go For More

- ▶ Dev Portal on SDC ([SIGN UP!](#))
- ▶ Other talks
  - 12:45pm [Splunk Developer Cloud Services and Features](#)
  - 2:00pm [Developer Tools for Splunk Developer Cloud](#)
  - 3:15pm [Partners Build Apps on Splunk Developer Cloud](#)
  - 4:30pm [Dashboards and Analysis UI Components for Developers](#)
  - Thu 1:30pm [Intro to SPLv2, the Module System and the Catalog](#)



Thank You



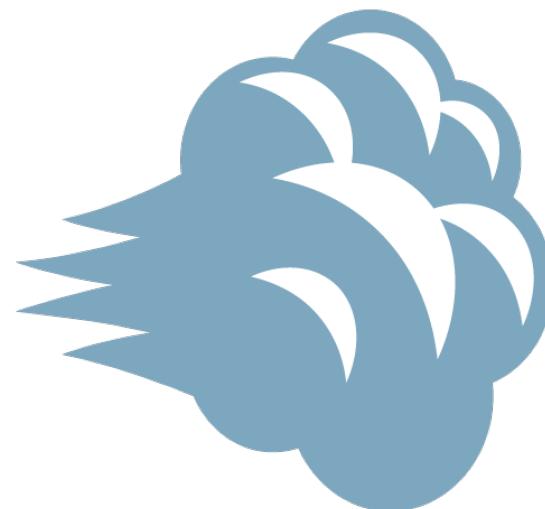
# Q&A



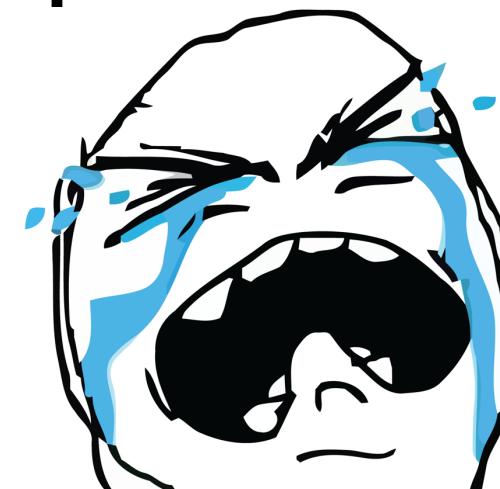
# Cloudifying Custom Search Commands

splunk>enterprise

- ▶ Custom Commands
  - (code and commands.conf)



splunk>SDC



*for now...*

```
338.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFFF0 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_B&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 104  
1, 317 27.160.0.0 - - [07/Jan 18:10:57:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=updateSession?itemId=EST_26&productId=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 104  
1, 317 27.160.0.0 - - [07/Jan 18:10:57:159] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 4318 "http://buttercup-shopping.com/cart.do?action=changeQuantity?itemId=EST_18&productId=AU-CUP-18-SHOPPING-CW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 104  
1, 317 27.160.0.0 - - [07/Jan 18:10:57:162] "GET /oldlink?item_id=EST_6&JSESSIONID=SD16SLBFF2ADFF7 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove?itemId=EST_26&productId=SD16SLBFF2ADFF7" 468 125.17 14 104  
1, 317 27.160.0.0 - - [07/Jan 18:10:57:165] "GET /oldlink?item_id=EST_6&JSESSIONID=SD16SLBFF2ADFF7 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove?itemId=EST_26&productId=SD16SLBFF2ADFF7" 468 125.17 14 104  
1, 317 27.160.0.0 - - [07/Jan 18:10:57:168] "GET /category.screen?category_id=EST_SURPRISES&JSESSIONID=SD16SLBFF2ADFF7 HTTP/1.1" 404 366 "http://buttercup-shopping.com/cart.do?action=remove?itemId=EST_26&productId=SD16SLBFF2ADFF7" 468 125.17 14 104  
1, 317 27.160.0.0 - - [07/Jan 18:10:57:171] "GET /category.screen?category_id=EST_SURPRISES&JSESSIONID=SD16SLBFF2ADFF7 HTTP/1.1" 404 366 "http://buttercup-shopping.com/cart.do?action=remove?itemId=EST_26&productId=SD16SLBFF2ADFF7" 468 125.17 14 104
```