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> .conf18

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

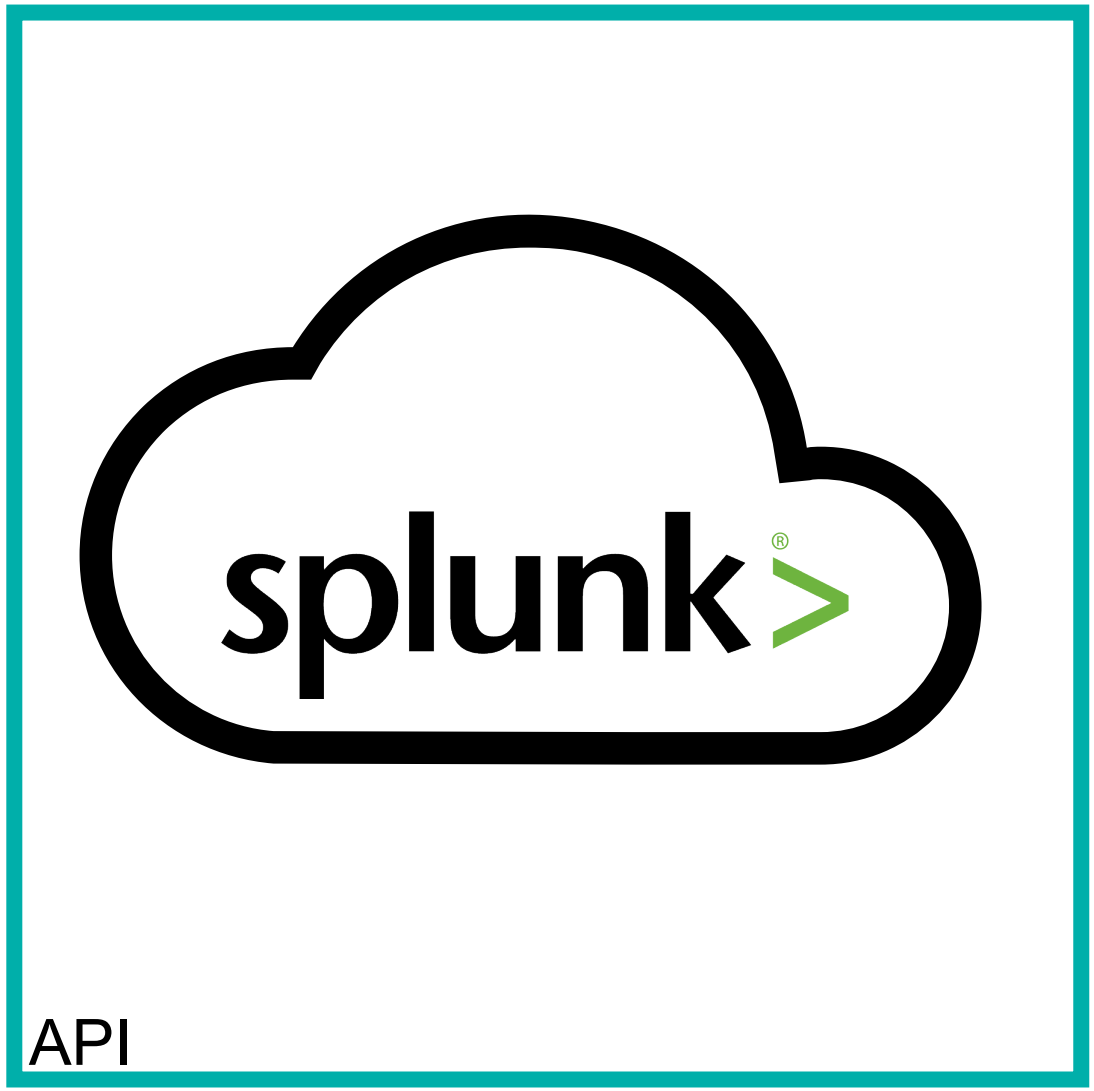
Big Honkin' Overview

AKA WTF (is) SDC

splunk> .conf18

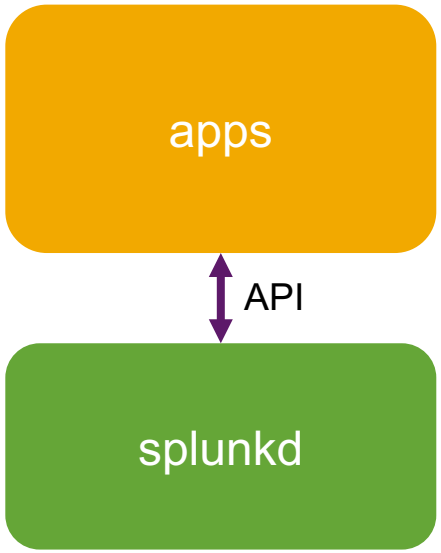
What's different about developing in SDC?

WTF is SDC



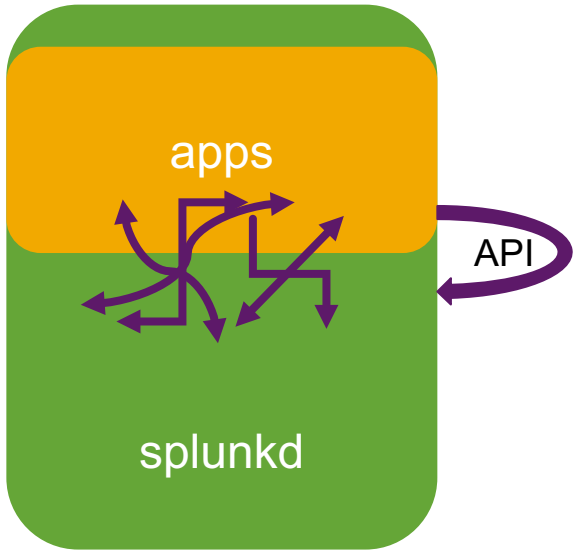
But Splunk Enterprise is API-driven…

Perception



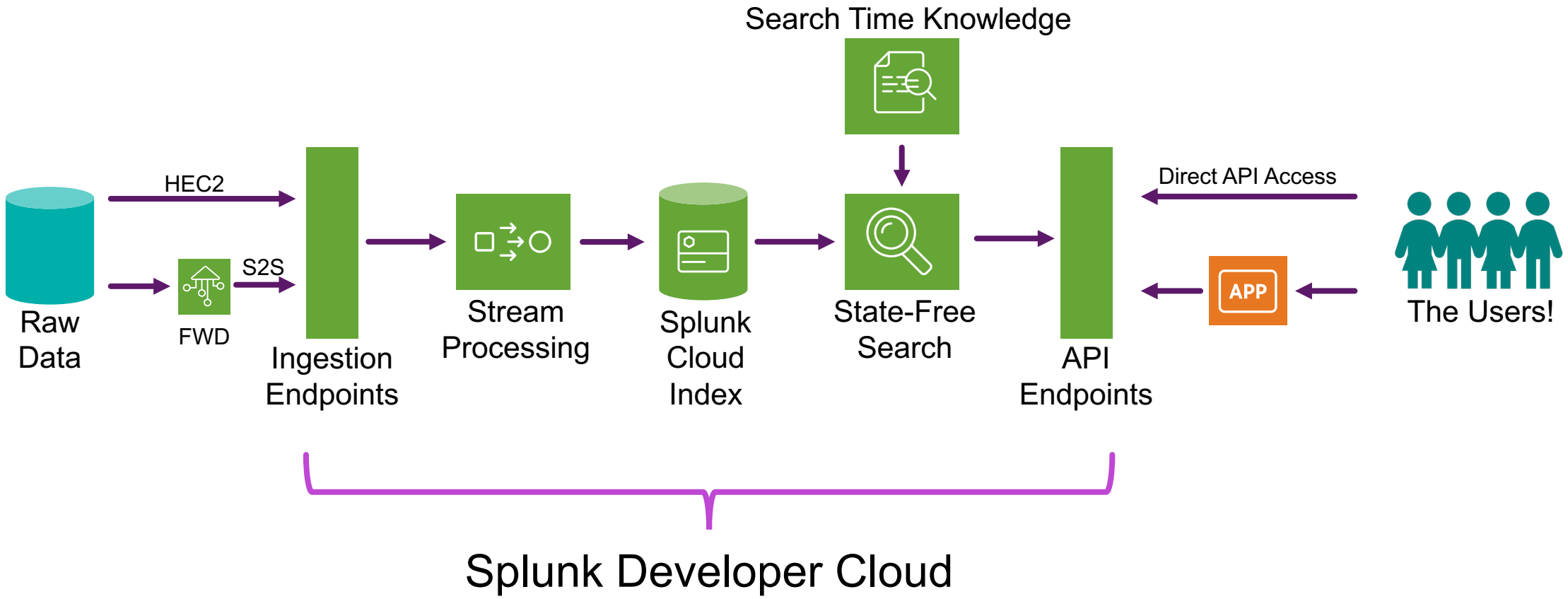
We want to get here

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

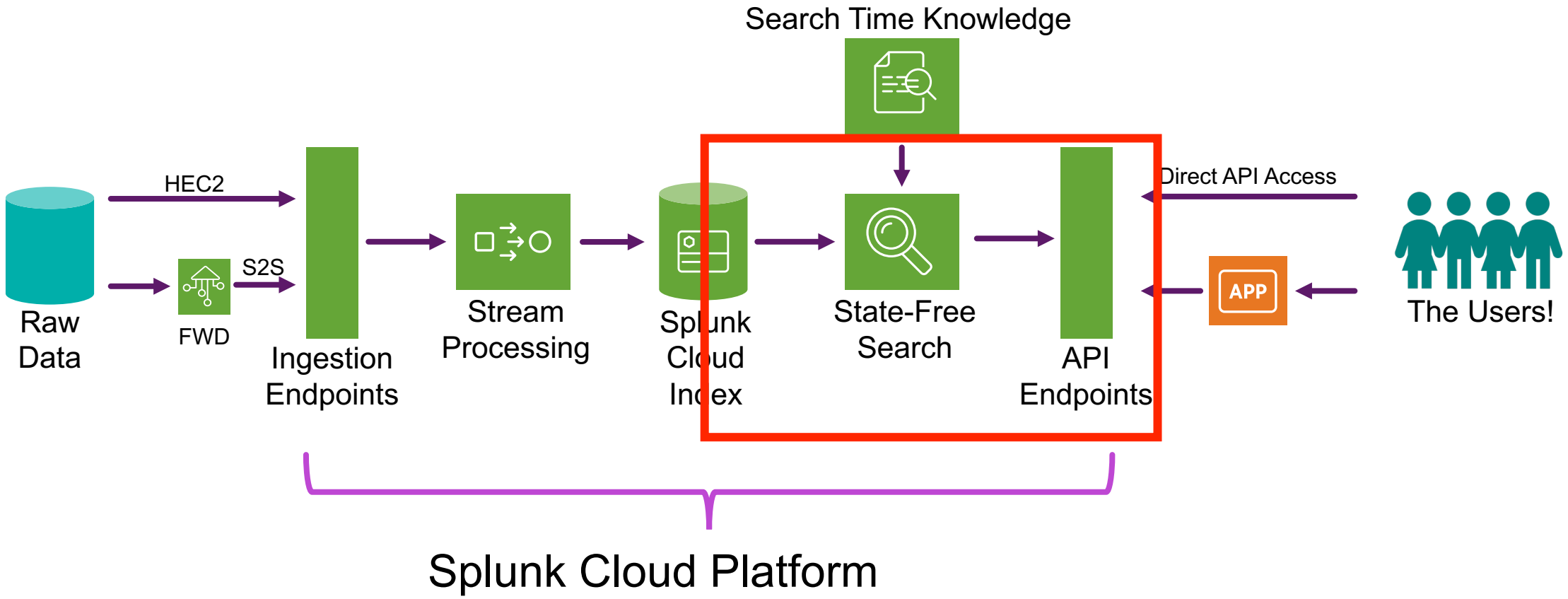
A Day in the Life of Data



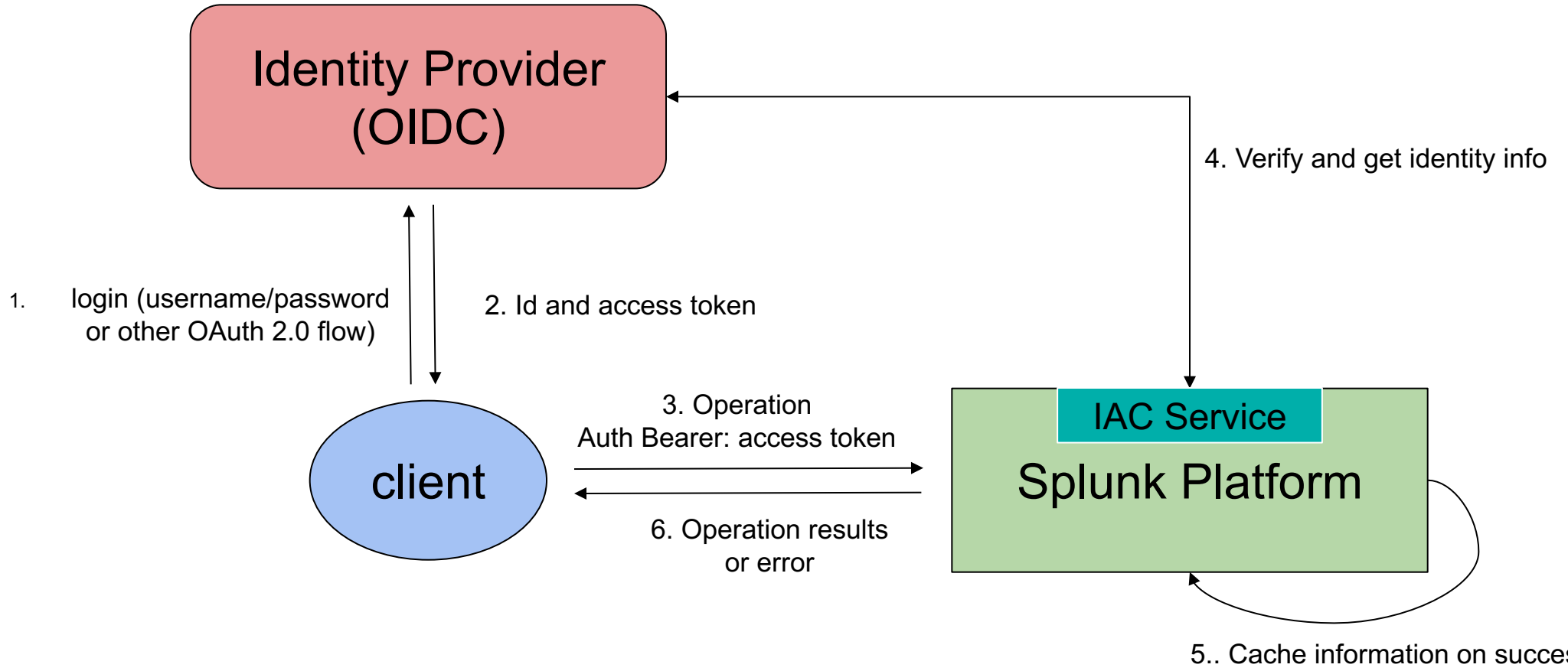
Core Services

AKA the nuts and bolts

A Day in the Life of Data



Cloud Authentication Workflow



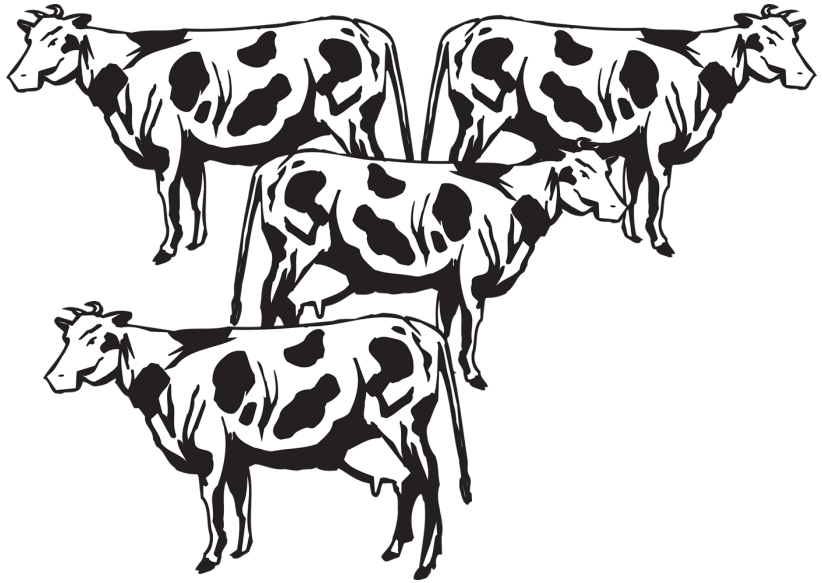
Cloudifying Deployment Scaling

splunk>enterprise

- SHC, Search Peers

splunk> Developer Cloud

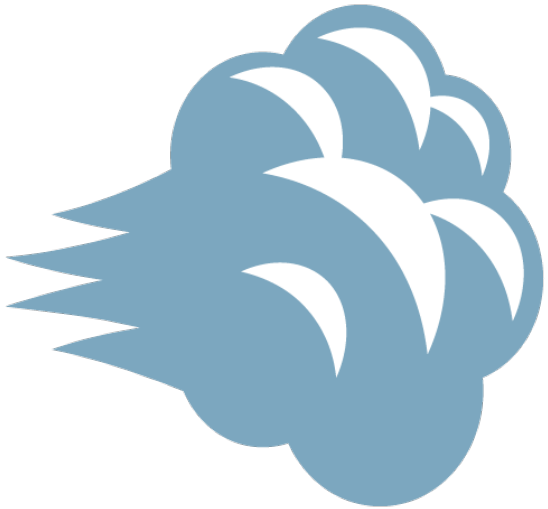
- State-Free Search



Cloudifying KV Store

splunk>enterprise

- KV Store
  - (collections.conf)



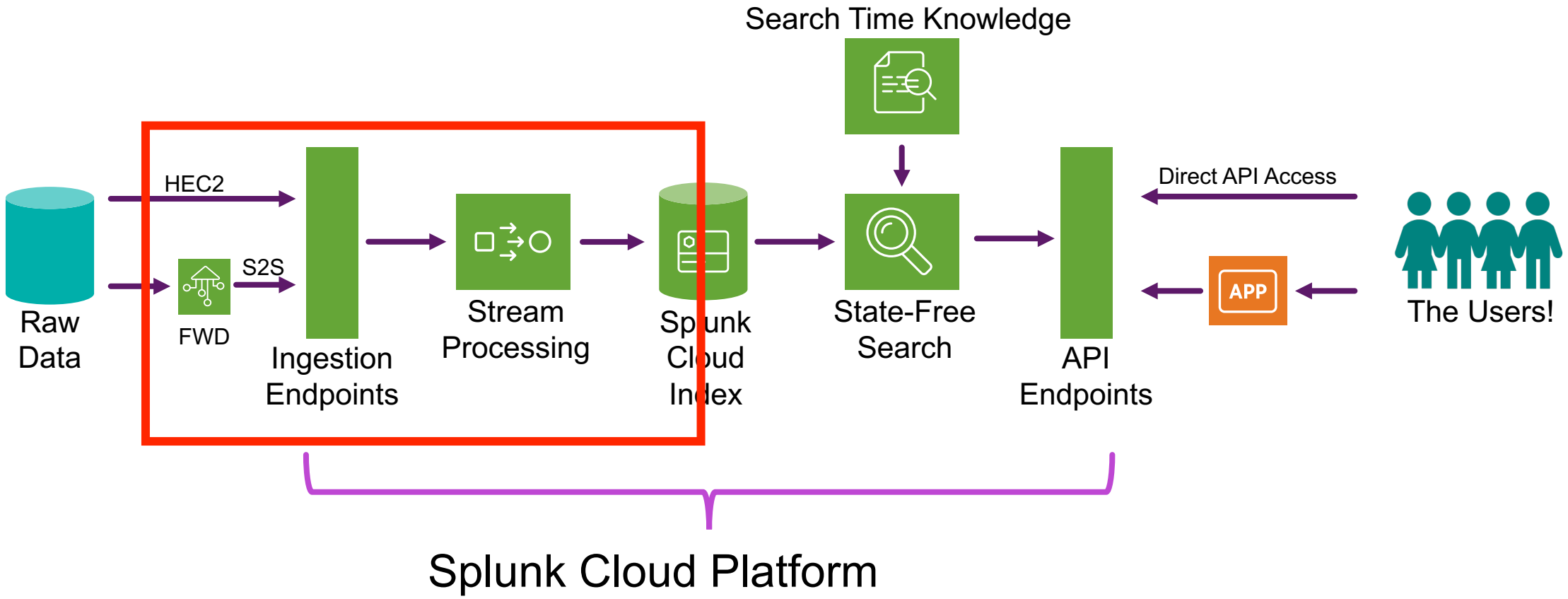
splunk> Developer Cloud

- KV Store
  - (Dataset in Catalog)

Data Ingestion

AKA data, it's what apps crave

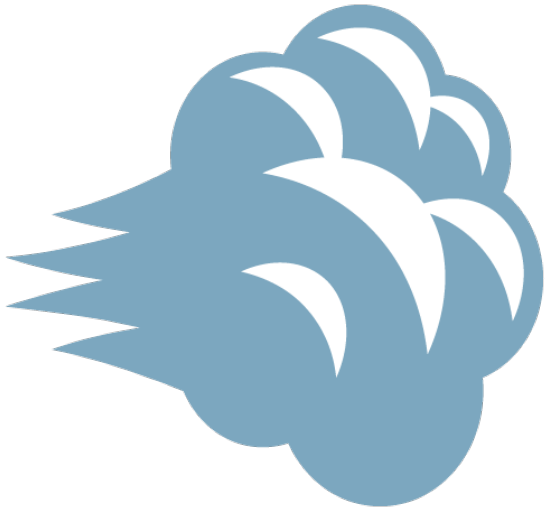
A Day in the Life of Data



Cloudifying Index Transforms

splunk>enterprise

- Indexed Fields, Null Queue
  - (props/transforms/fields.conf)

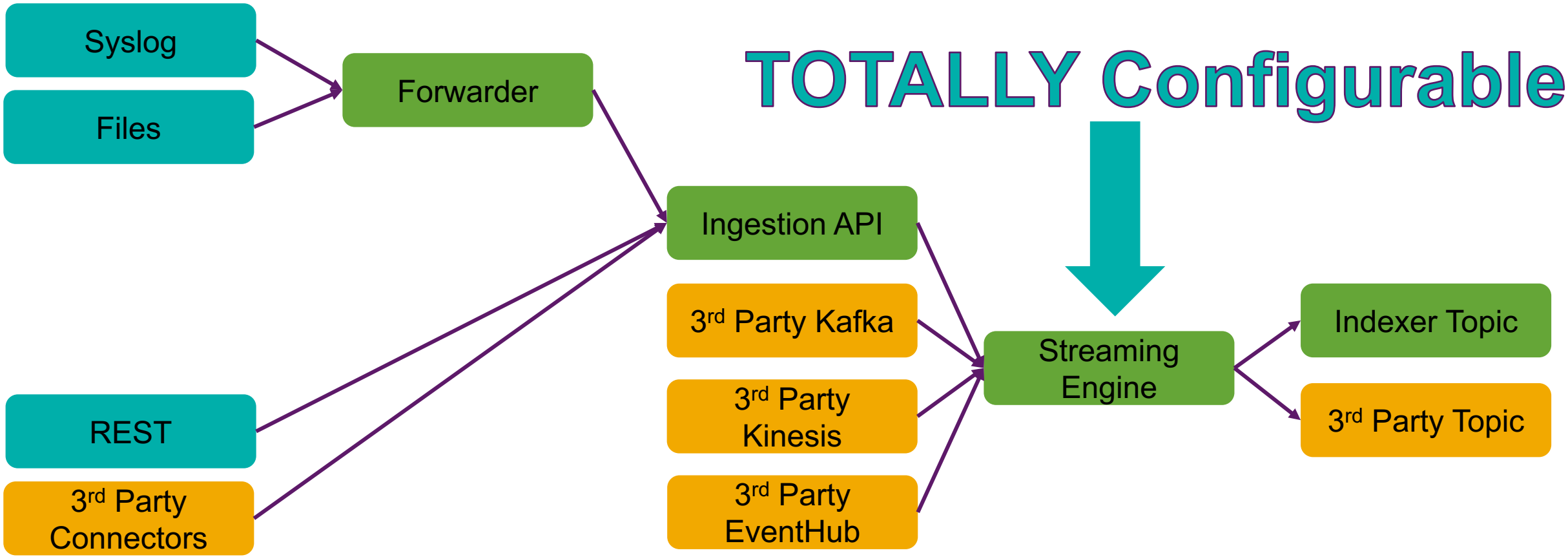


splunk> Developer Cloud

- BLAM Pipelines
  - (Data Availability APIs)

splunk> .conf18

Overview



Stream Processing – Why?

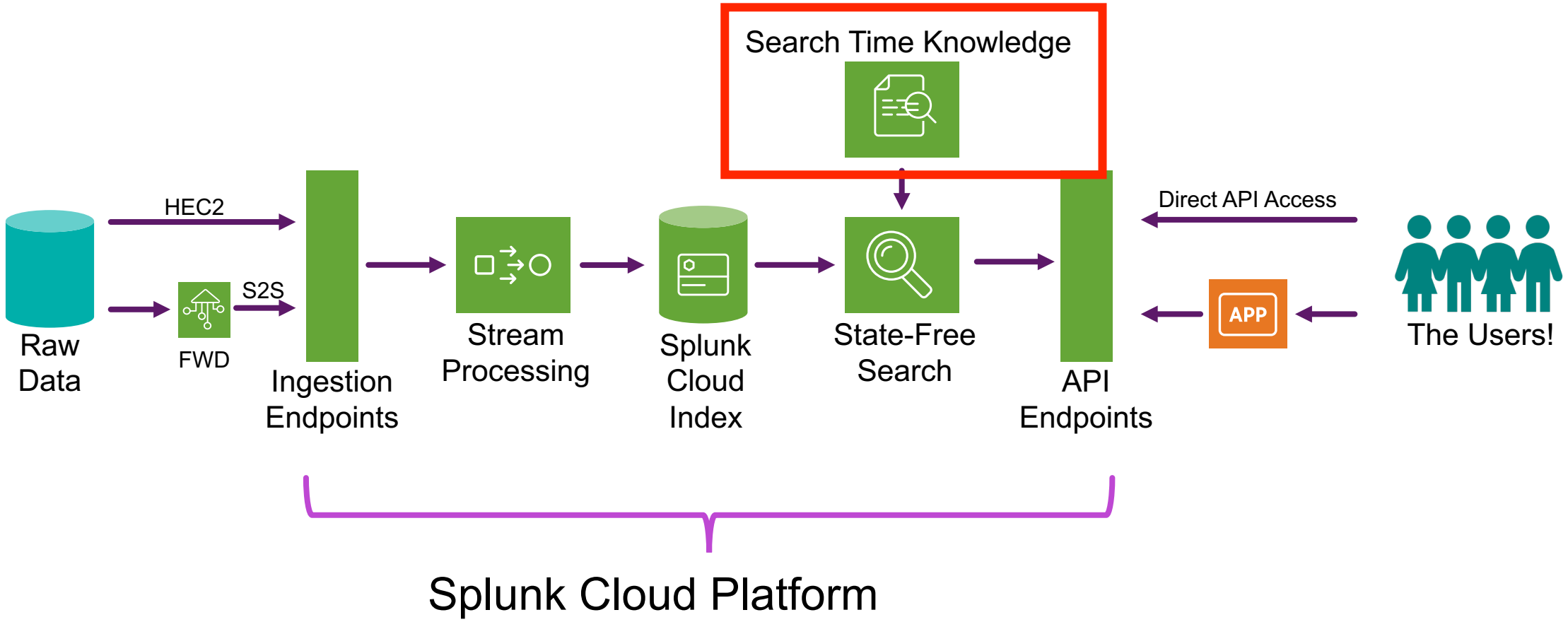
- *Complement* Splunk's query-time data wrangling with ingest-time wrangling
  - Building metrics from events
  - Pre-extract and enrich to make common queries simpler
  - Advanced routing of events
  - Enforce data quality standards
  - "Really realtime" searches and metrics
  - Move expensive saved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

Search Technology

AKA accessing data

splunk> .conf18

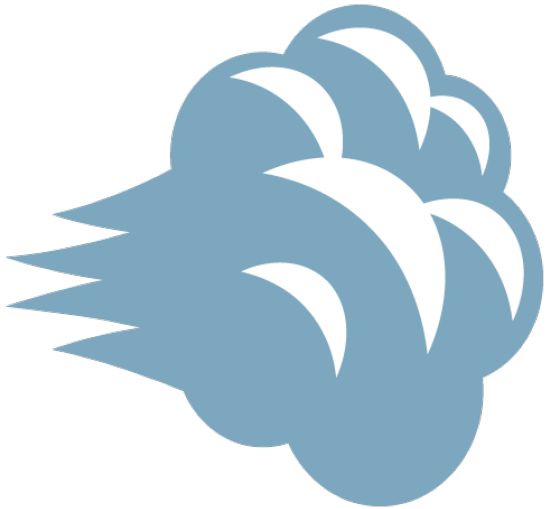
A Day in the Life of Data



Cloudifying Data Storage

splunk>enterprise

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



splunk> Developer Cloud

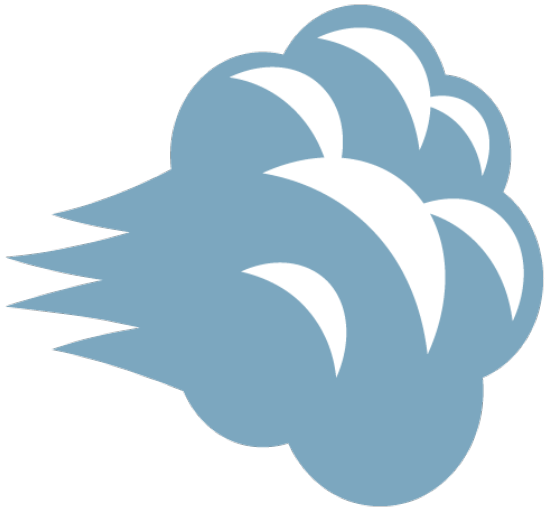
- Datasets in Catalog

splunk> .conf18

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

```
[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
```

splunk> Developer Cloud

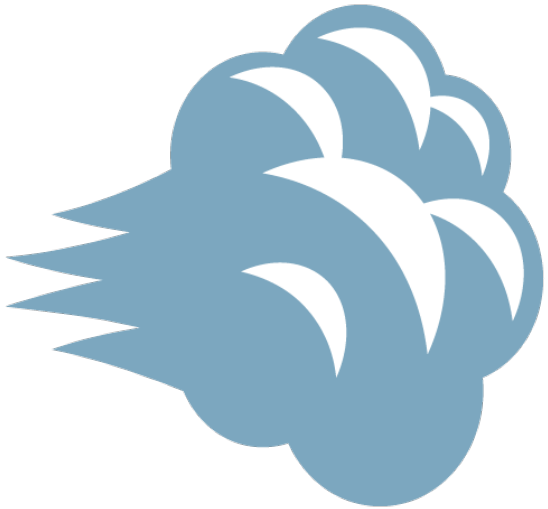
```
{
    "id": #id#,
    "name": #name#,
    "module": #module#,
    "match": "sourcetype::testlog",
    "actions": [ ... ]
        {..,
        { "id": #id#,
          "id": #id#,AS",
          "kind": "AUTOKV",
          "mode": "AUTO"products ID AS pid OUTPUT
        }oduct_name, Category as product_category",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

splunk> .conf18

Cloudifying Lookups

splunk>enterprise

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



splunk> Developer Cloud

- Datasets in Catalog
  - (Only KV Store based)

Cloudifying SPL

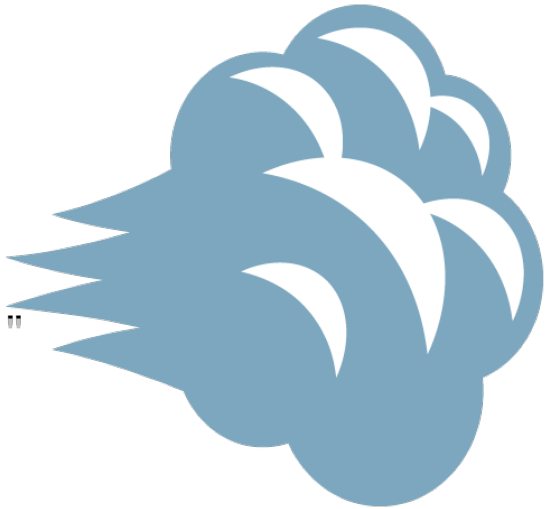
splunk>enterprise

- 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
```

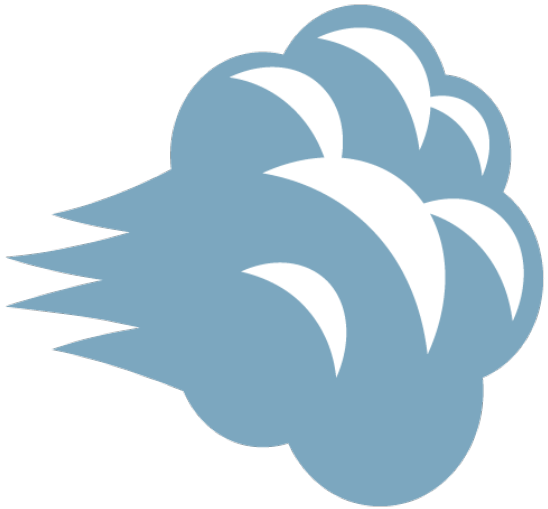
```
| from metric:metrics
WHERE metric_name="cpu"
GROUP BY host, span(_time, 1m)
SELECT latest(_value) as cost, host
```

```
| 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

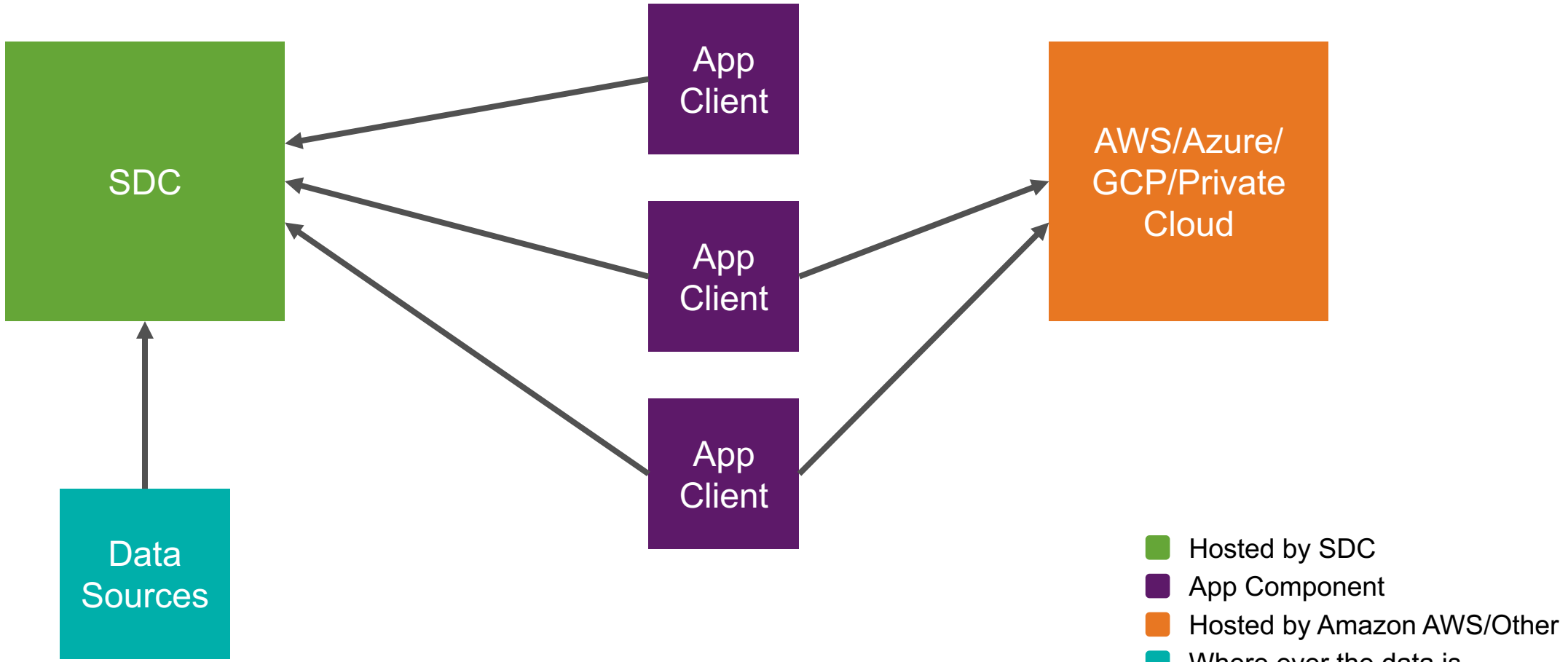
No Clear Analog

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

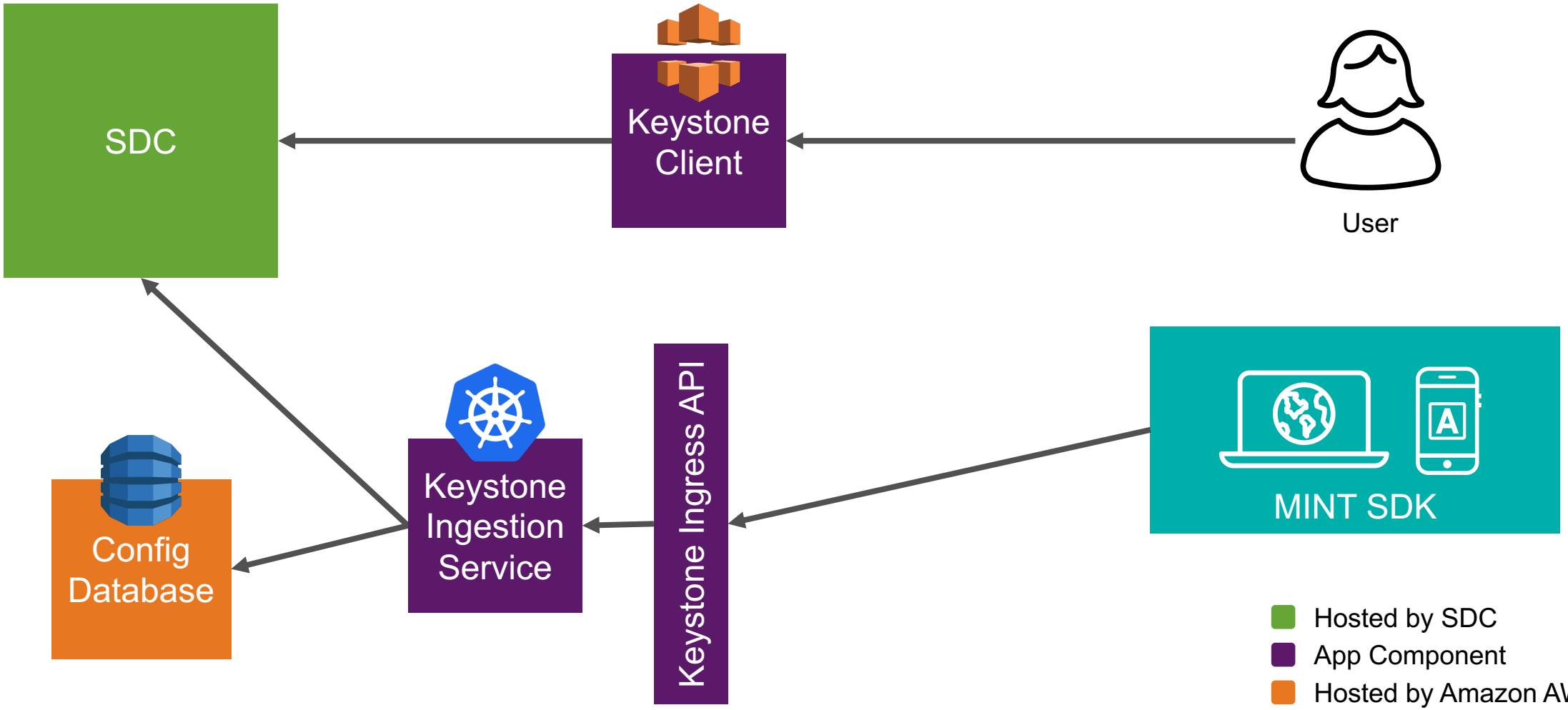
Apps

AKA what you build!

Future of App Deployments

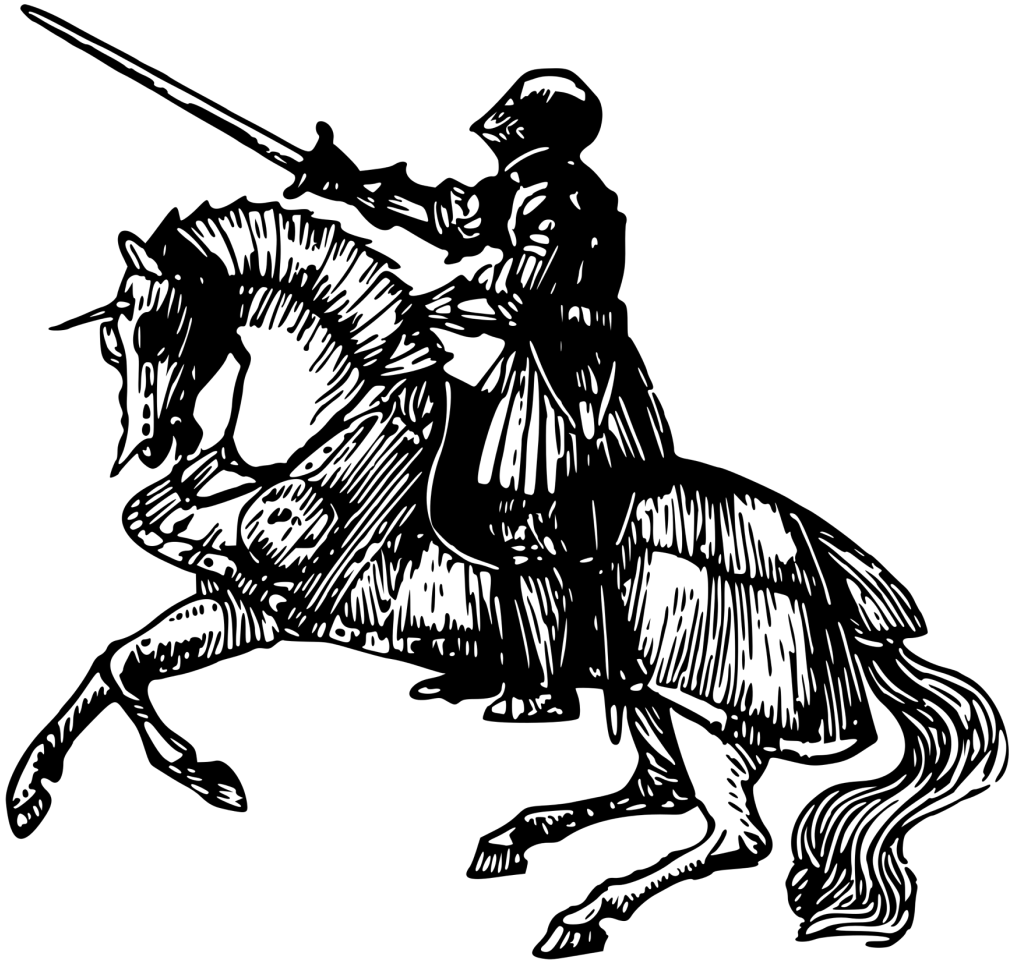


Splunk Insights for Web and Mobile Apps Architecture



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 Catalaog



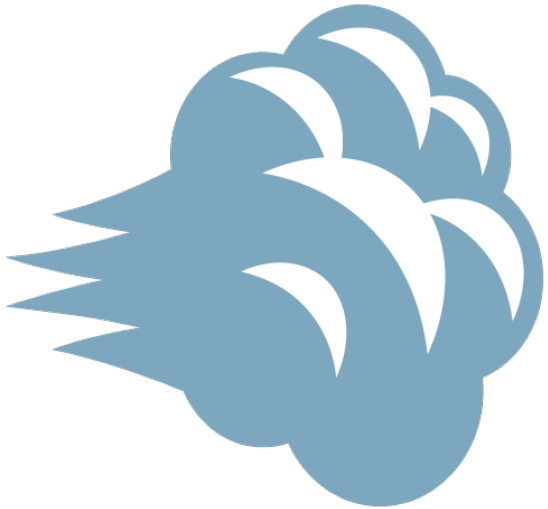
Thank You

Q&A

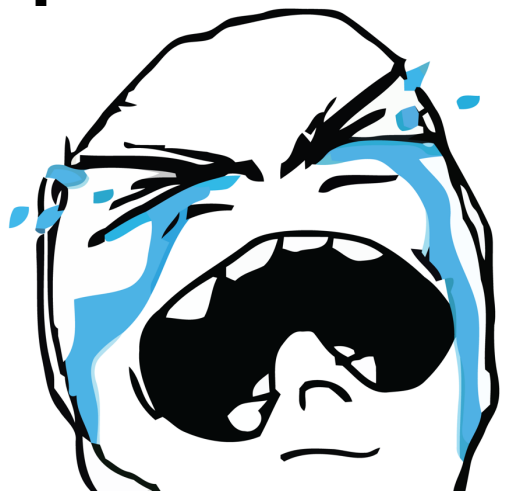
Cloudifying Custom Search Commands

splunk>enterprise

- Custom Commands
  - (code and commands.conf)



splunk> SDC



for now…