Using Splunk as a Monitoring Solution for MuleSoft's API Platform

October 2018

Our Speakers

JUAN GOMEZ

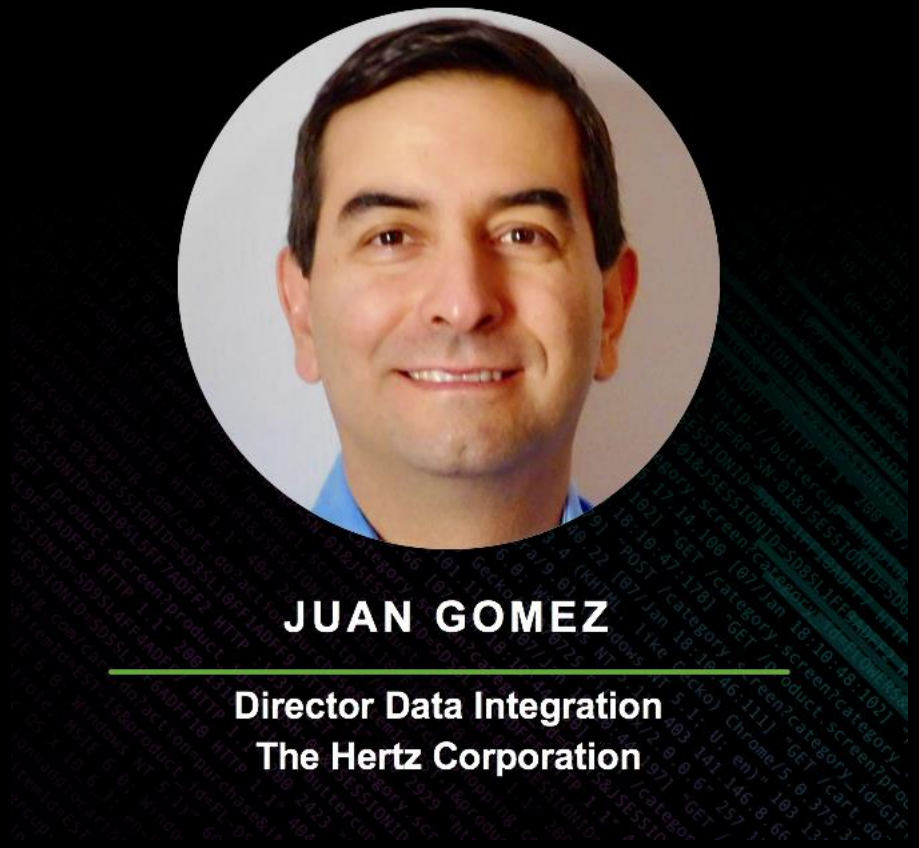
Director Data Integration
The Hertz Corporation

TOLGA TOHUMCU

Staff Architect, Splunk
@TolgaTohumcu

splunk> .conf18

Juan Gomez

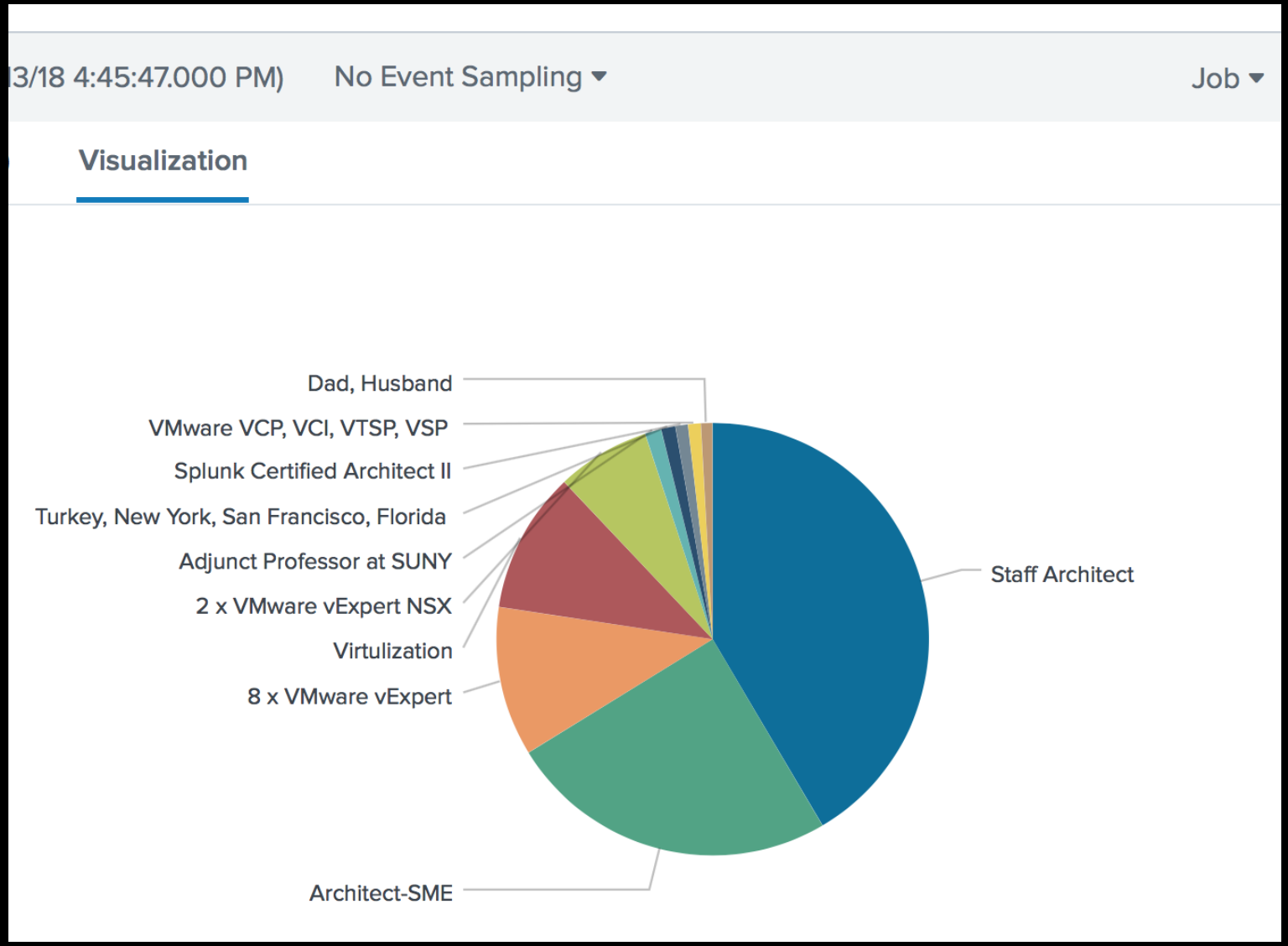


- Splunk user since 2011
- Working with MuleSoft since 2008
- Managing and architecting MuleSoft deployment for Hertz digital transformation program
- Enjoy working with data integration, API architecture, stream processing and analytics

Tolga Tohumcu

TOLGA TOHUMCU

Staff Architect, Splunk
@TolgaTohumcu



"Hertz is transforming the entire rental car experience through new digital offerings.

MuleSoft delivers a unified, global platform that creates a better experience for our customers.

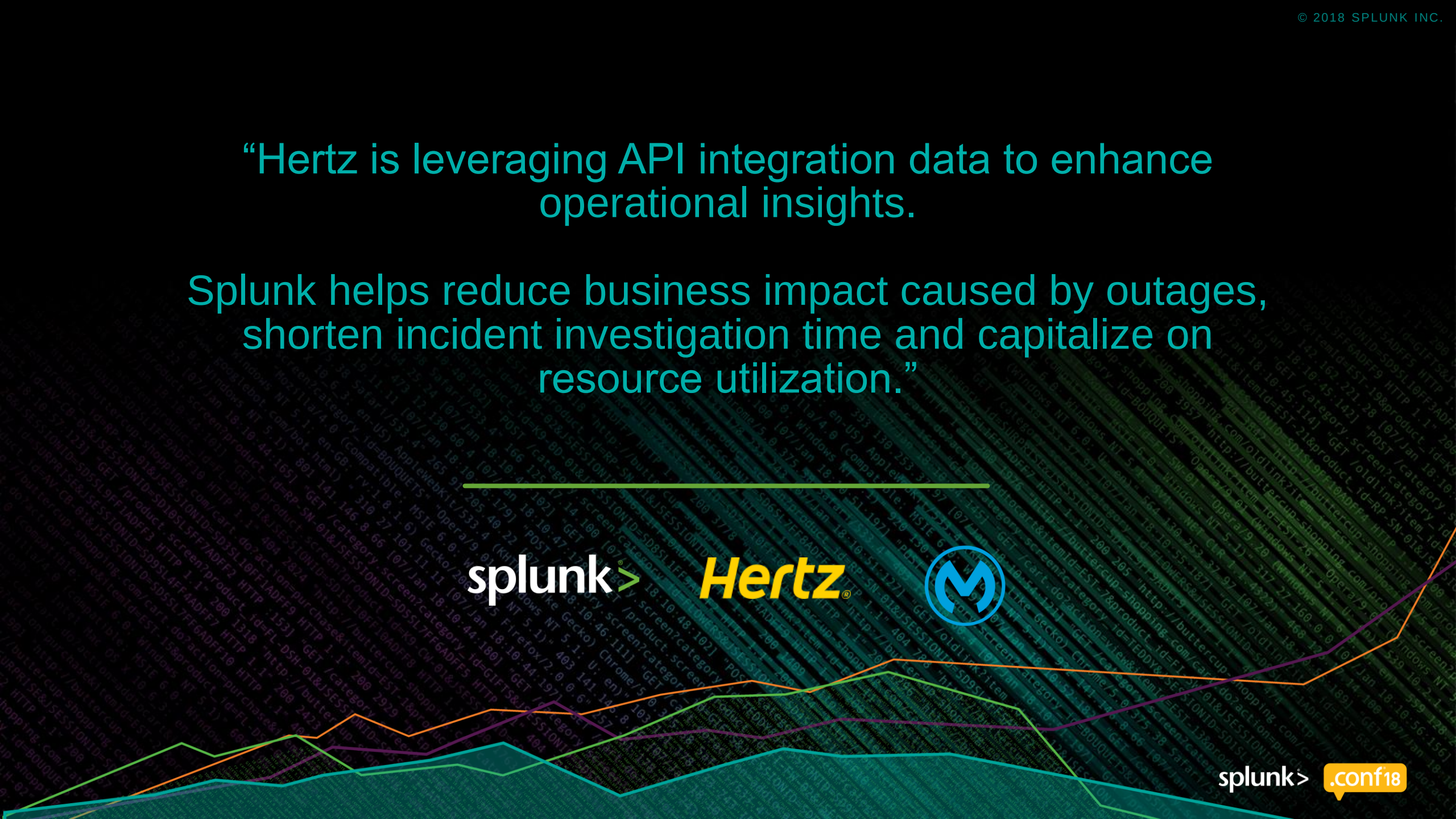
This global ecosystem provides greater flexibility, increased productivity and enhanced capabilities"

splunk> Hertz

"Hertz is leveraging API integration data to enhance operational insights.

Splunk helps reduce business impact caused by outages, shorten incident investigation time and capitalize on resource utilization."

splunk> Hertz



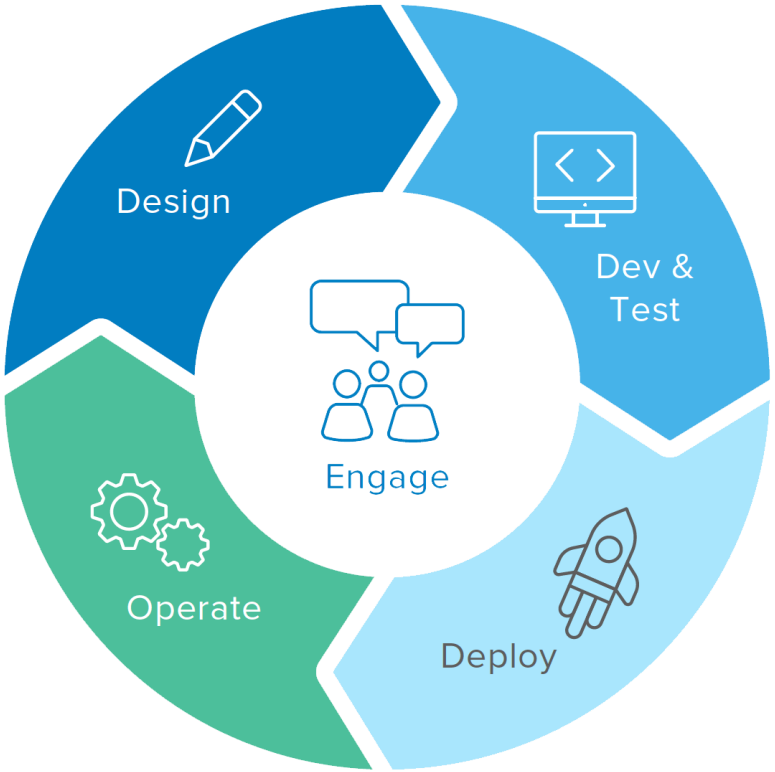
splunk> .conf18

“Monitoring MuleSoft APIs is challenging when running in Hybrid Cloud”

“By leveraging Splunk Cloud, we successfully monitor MuleSoft APIs running in Hybrid Cloud”

splunk> .conf18

Intro: MuleSoft as Integration Platform



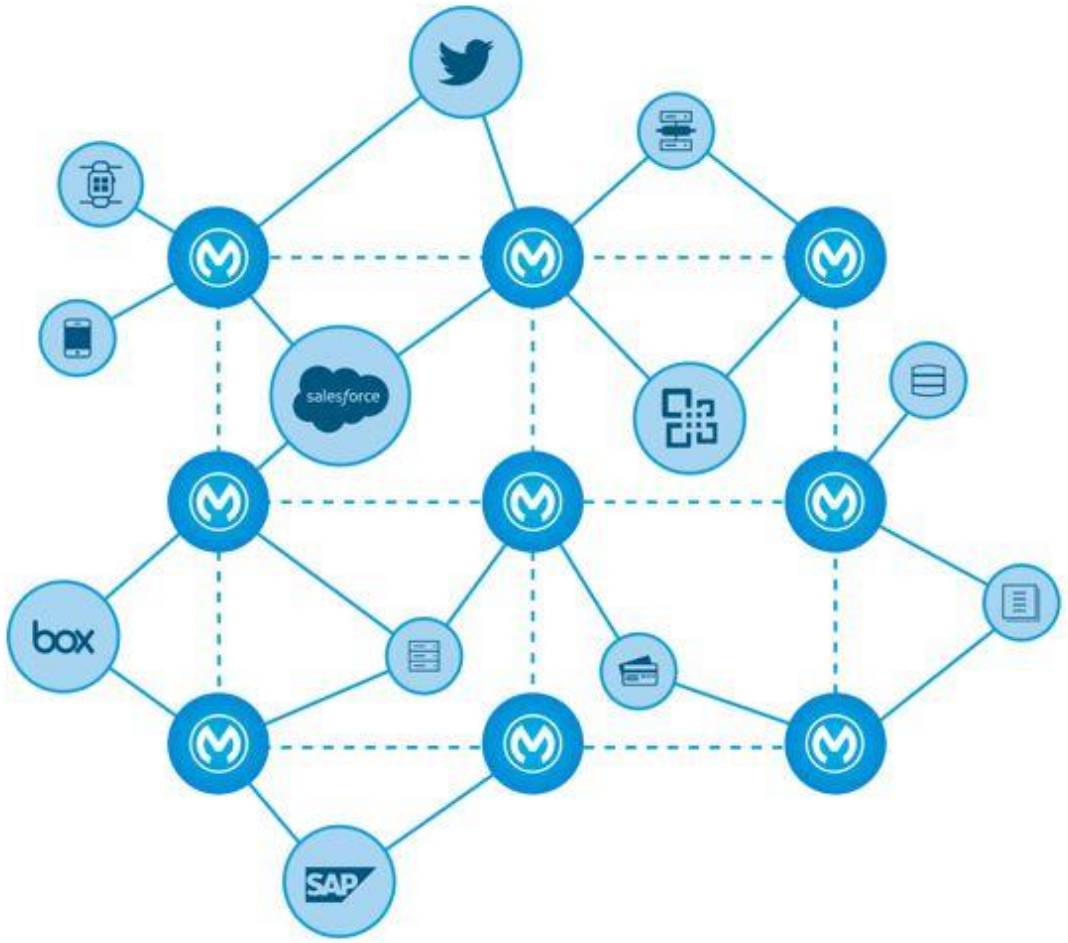
Full API Lifecycle Management with MuleSoft's Anypoint Platform

- Rapid Development
- Easily Connect to any System (pre-build connectors, SDK)
- Collaborate and Publish
- Flexible Runtime (cloud, on-premise, containers)
- API Governance and Monitor

Intro: API Integration with MuleSoft

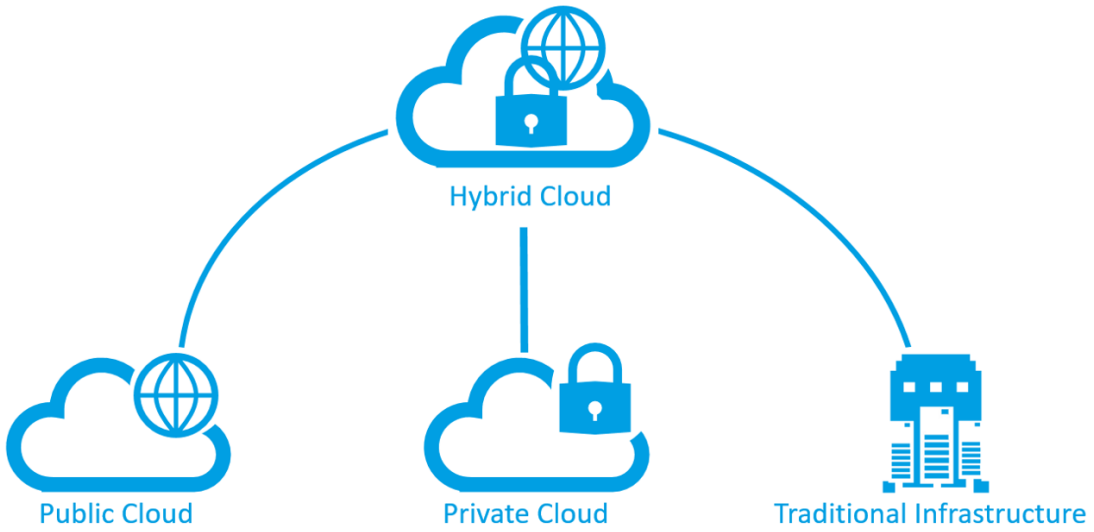
"Using an API lead integration approach IT can deliver today's projects faster than before, while also building re-usable assets that are easily adaptable to future changes in the enterprise."

Intro: The MuleSoft Application Network



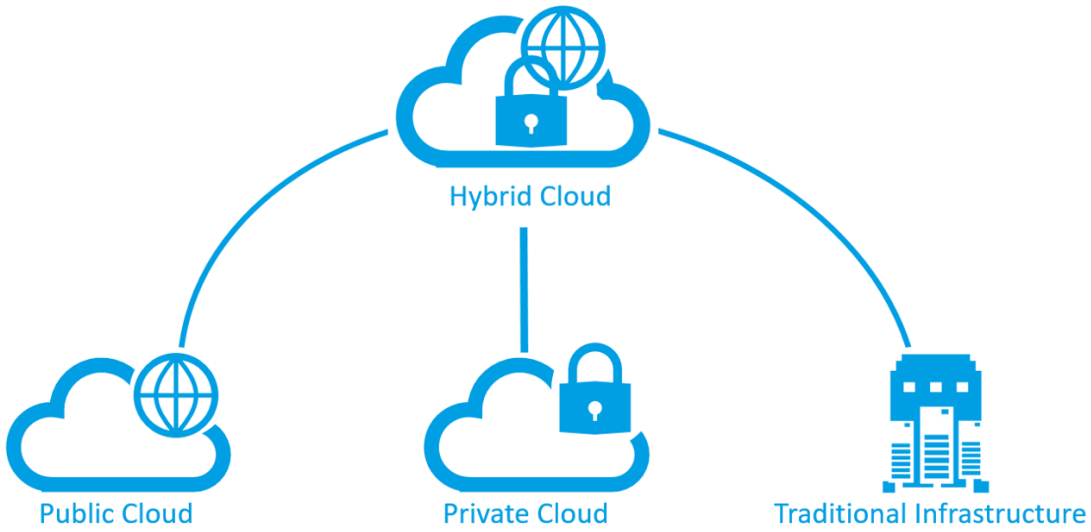
- Re-usable patterns
  - Efficiency, Consistency
- De-coupled architecture
  - Flexibility
- Scalable designs
  - Goodbye Monoliths
- Connect or expose
  - Build for the future

MuleSoft Running in Hybrid Cloud



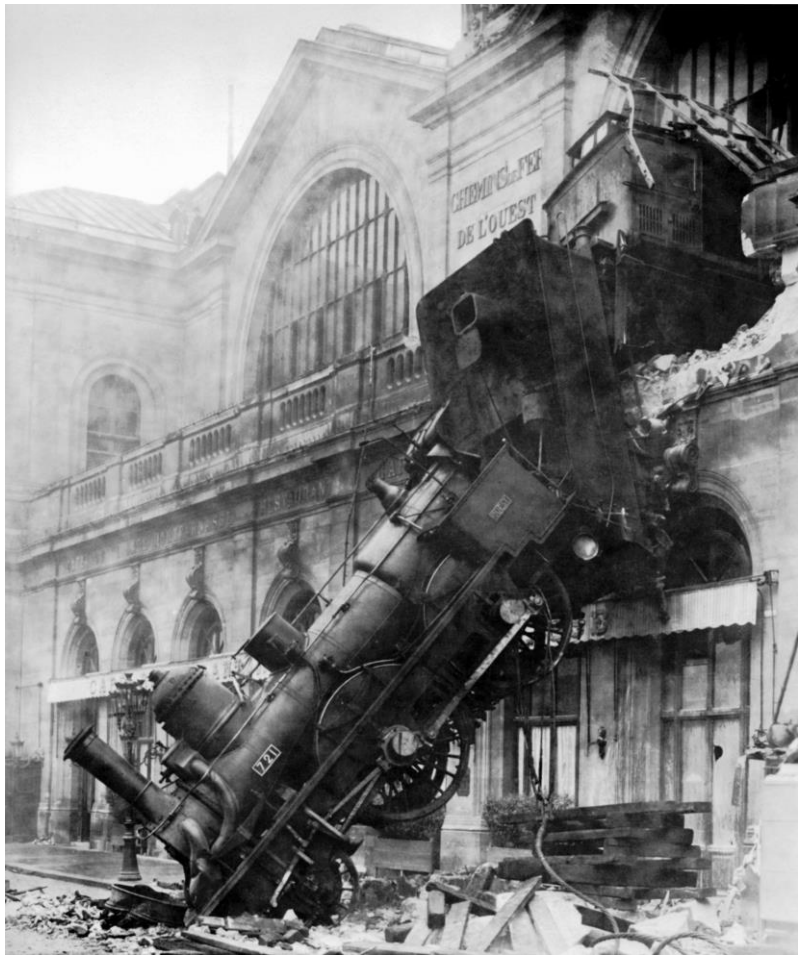
- Anypoint Platform supports the deployment of APIs on Multiple Cloud environments
- Anypoint Cloudhub
  - Offers an integration platform as a service that answers concerns of scalability, security and governance
  - Allows for global deployment of APIs
  - Runtimes updated seamlessly

MuleSoft Running in Hybrid Cloud



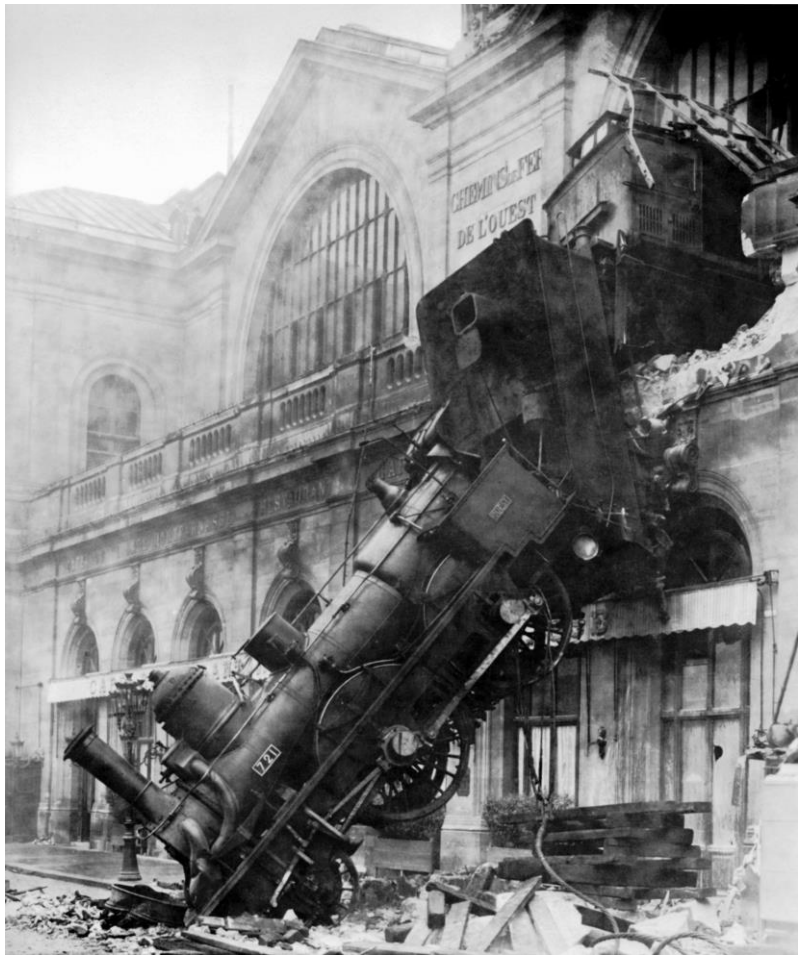
- On-Premise Runtimes
  - Traditional deployment mode, provides maximum control when Cloud is not the first option
- Greater flexibility with support for multiple deployment scenarios

What about Log Management?



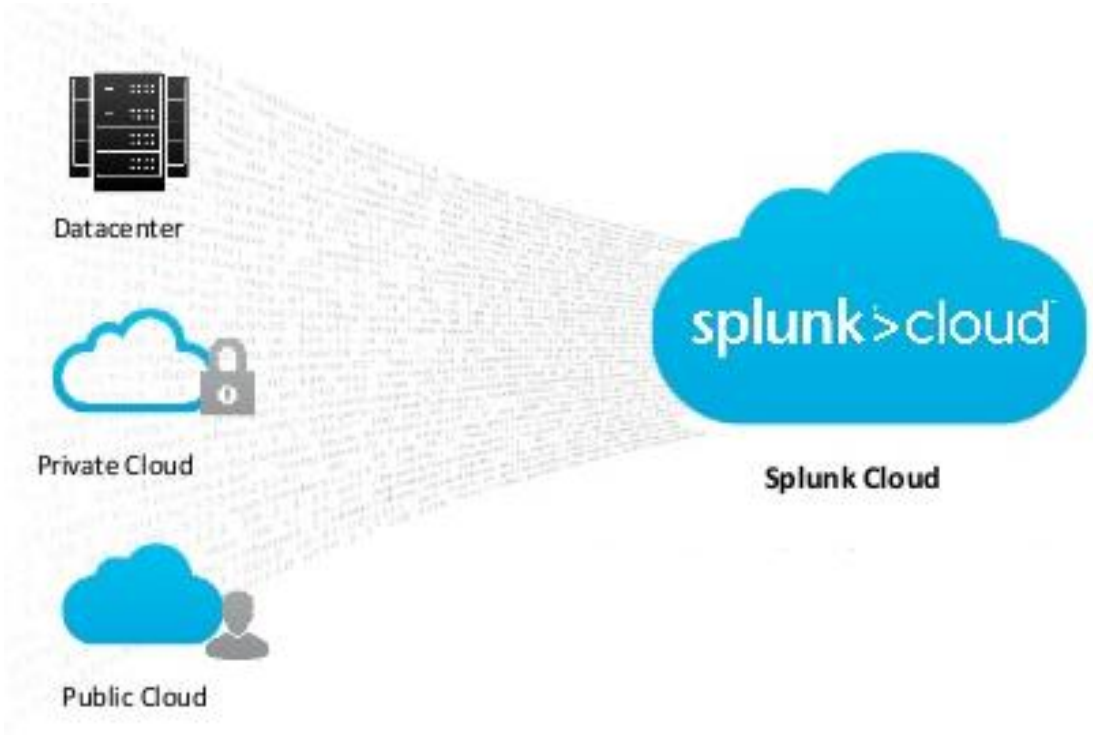
- Challenges introduced by running in Hybrid Cloud
  - No central place to aggregate logs
  - On-premise: full control of logging, but limitations on storage
  - Cloud: logs are spread across each application, some limitations on storage
- Multiple cloud locations to troubleshoot issues

What about Log Management?



- Challenges introduced by using API lead integration
  - Small APIs compose an application, thus many logs entries will encompass a single transaction
  - Requires strategy for stitching the transaction

Splunk Cloud to Solve these Challenges



A platform like Splunk Cloud allows you to:

1. Centrally aggregate logs
2. Ingest logs from diverse cloud environments
3. Create a single view of transaction
4. Perform schema-less log ingestion
5. Scale in the Cloud as required

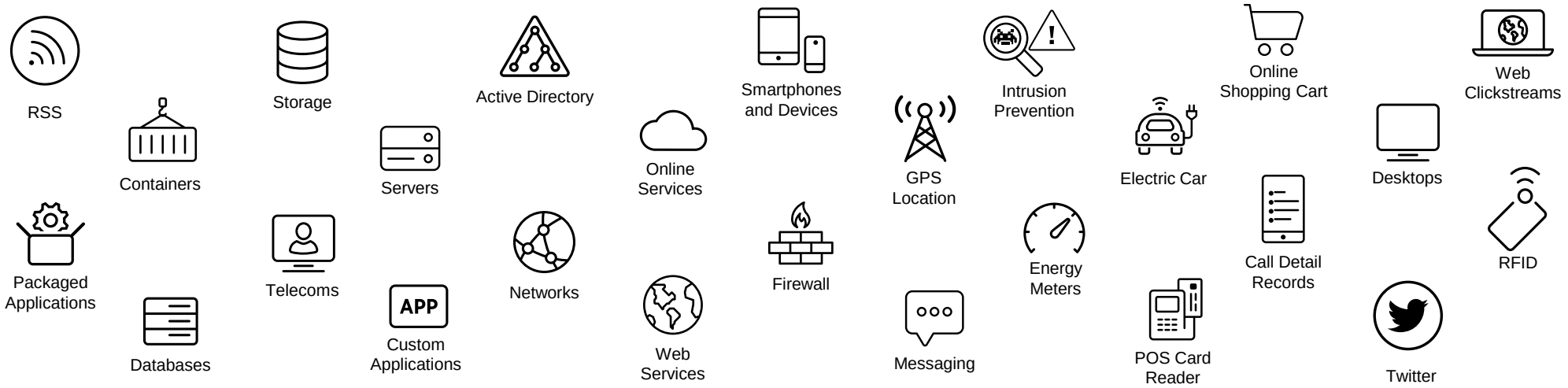
Benefits of Splunk Cloud

Maximizes Value from limited resources

Eliminates Infrastructure Requirements

Fastest Time to Value

Extensive Ecosystem of Splunk



splunk>

7+ PB/Day | Real Time | Mission Critical | Schema on Read

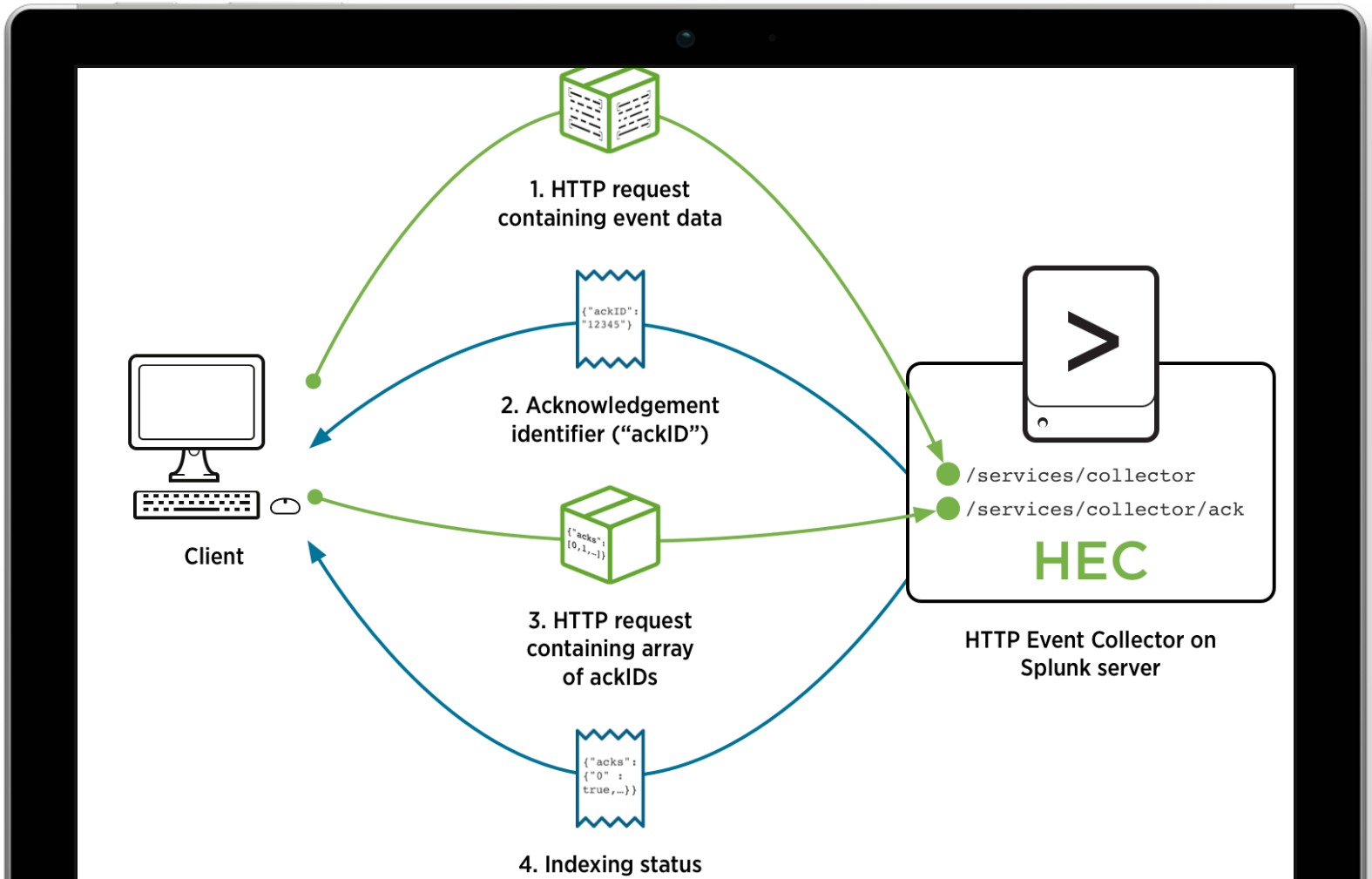
splunk> .conf18

Splunk Cloud Functionality

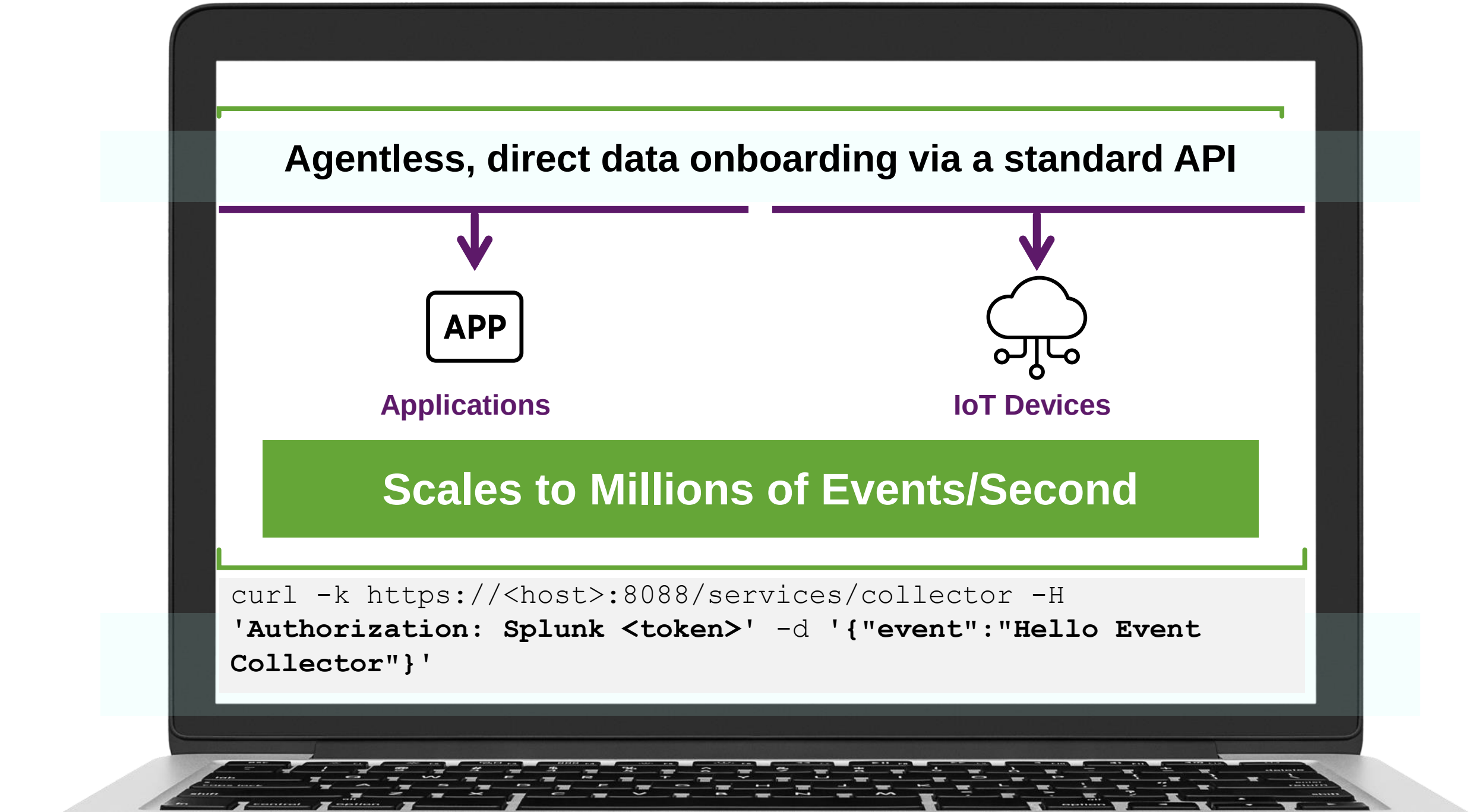
- Enhanced Splunk Metrics
  - Turn logs into events with mcollect
- Upgrade with Minimal Downtime
  - Search,monitor, alert during upgrades
- Self-Service install
  - Supporting SHC, better performance and availability
- Self-Storage
  - Tiered data storage to S3
- Investigate on ANY machine data
  - Splunk Add-on for AWS Firehose
  - Splunk Connect for Apache Kafka
  - Splunk Connect for Docker
  - Splunk Connect for Kubernetes
- AI through Machine Learning
  - MLTK
  - Experiment Management Framework

splunk> .conf18

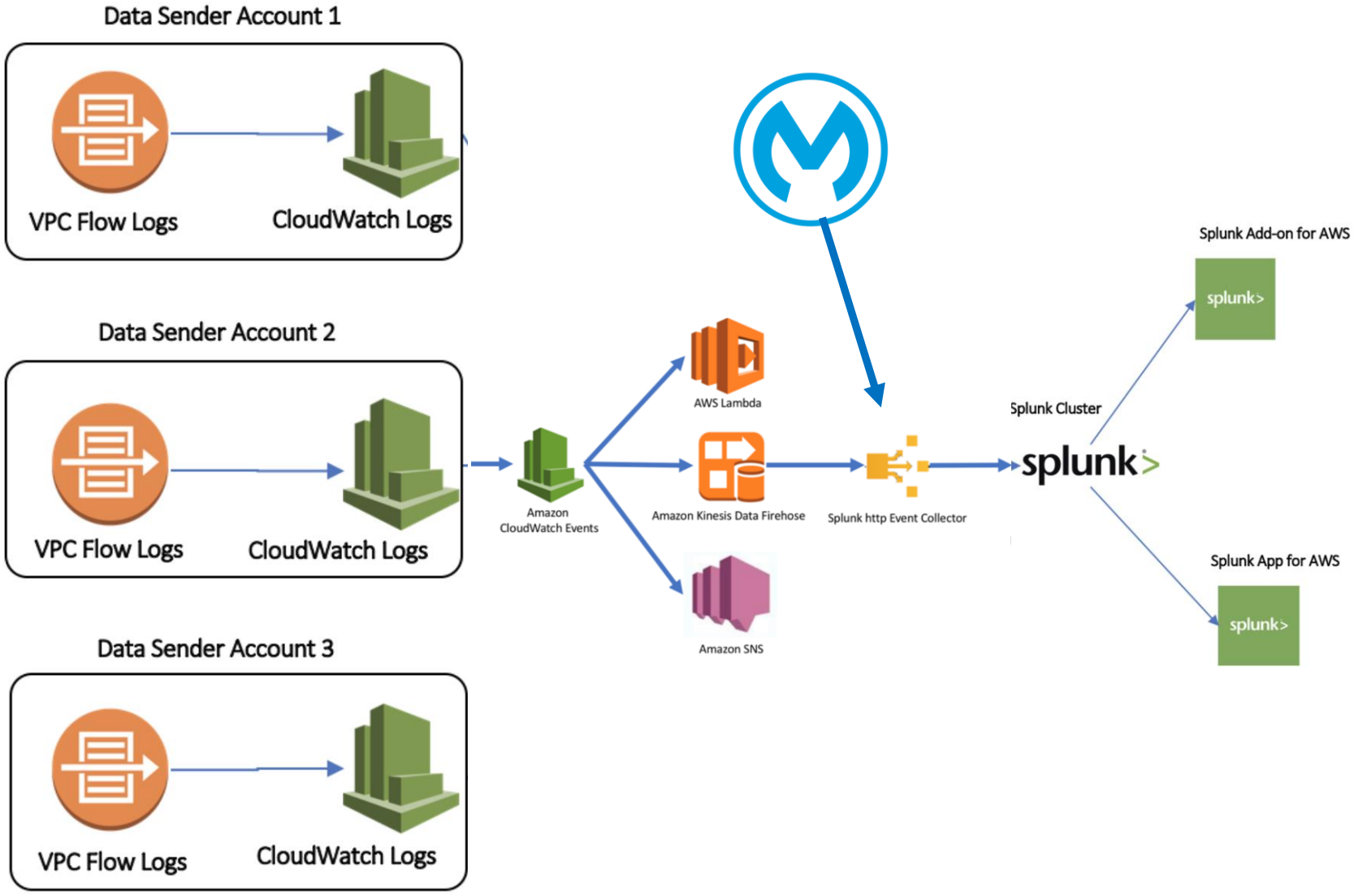
HTTP Event Collector (HEC)



- Simple HTTP endpoint for pushing data
- Send events directly from anywhere
- Easy to configure and secure
- Highly scalable and performant
- Advanced features
  - Sourcetype, index, ACK



Leveraging AWS Logs with MuleSoft using HEC



Improving Performance by Indexed Field Extractions

You can trigger indexed field extractions of JSON fields in two ways. As part of main “event” or separate from the “event”

Use nested JSON inside the “event” property

{"sourcetype":"_json", "event":"{\"uuid\":\"2ab7b65e-4d87-43d0-8cef-87b6b429086b\",\"action\":\"test-http-event-collector\"}"}

Or add a “fields” property at the top JSON level

{"sourcetype":"_json","event":"hello world!","fields":{"uuid":"2ab7b65e-4d87-43d0-8cef-87b6b429086b","action ":"test - http - event "}}

Use tstats command to leverage indexed fields and speed up your search

| tstats count where index=xyz api=123 by _time, a, b, c

splunk> .conf18

Improving Performance SPL and Search Optimization

Retrieve only the required data | **Move as little data as possible** | **Parallelize as much work as possible** | **Set appropriate time windows**

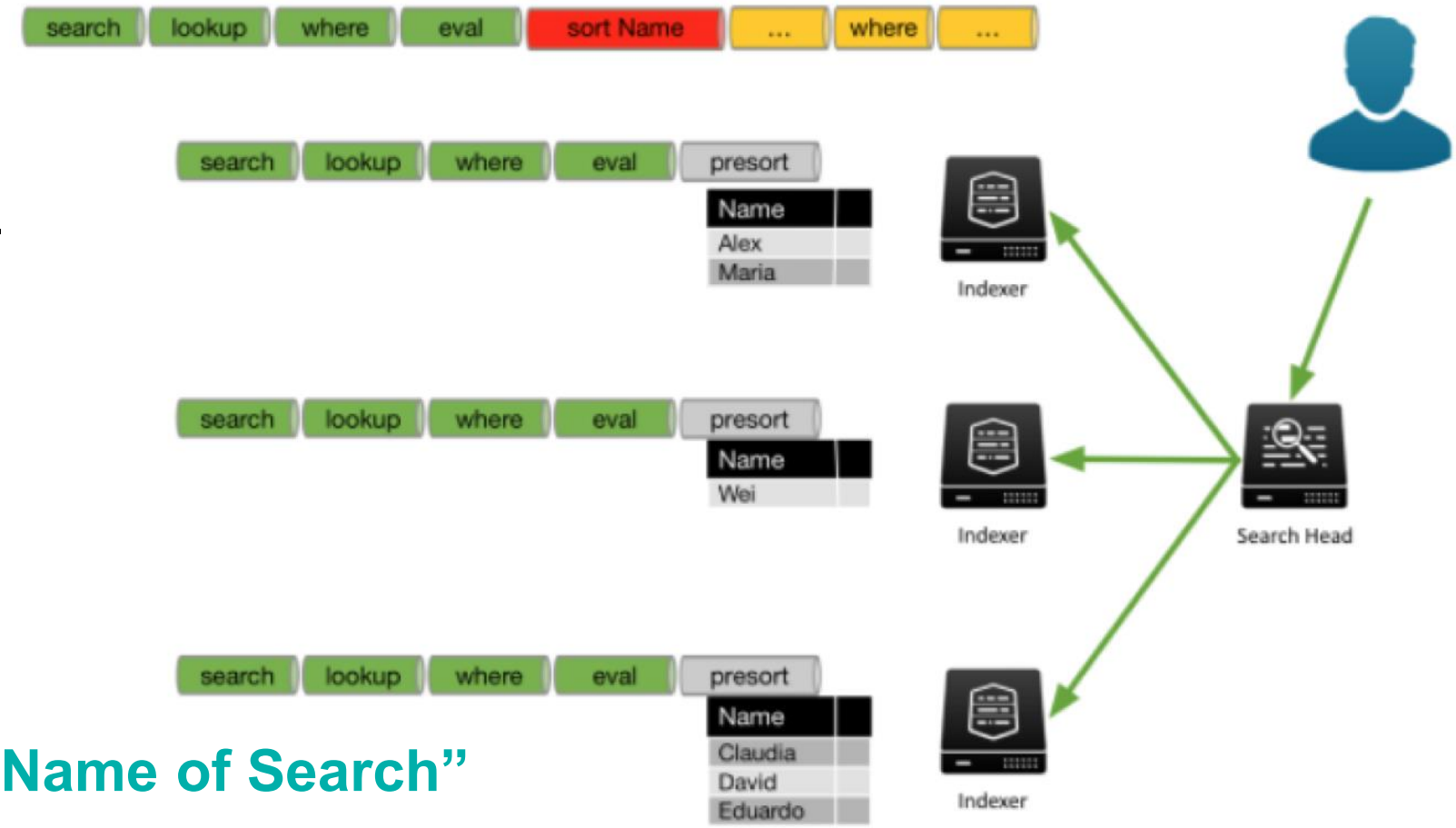
search and filter | munge | report | cleanup

```
sourcetype=access*

| eval KB=bytes/1024

| stats sum(KB) dc(clientip)

| rename sum(KB) AS "Total KB" dc(clientip) AS "Unique Customers"
```

splunk> .conf18

Command Order with One Search, Many Panels

- LoadJob
  - Loads events or results of a previously completed search.
  - Identified by
    - Search ID
    - Scheduled Search Name



| loadjob savedsearch="Name of Search"

Splunk IT Service Intelligence (ITSI)

- Predict and Prevent Outages
- Create a 360-degree view
- Find Problems Faster
- Predict Health Scores in Advance
- Reduce MTTR

splunk> .conf18

Key Takeaways

1. Log Management in Hybrid Cloud can be challenging, define a strategy early on
2. Leverage tried and tested tools like Splunk
3. Leverage HEC for visibility to your own VPC
4. Leverage people's time with value rather than administration

Q&A

Juan Gomez

Tolga Tohumcu

Thank You

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