splunk> .conf2017

Splunk Project Nova

Analyzing logs (and more!) from your microservices

Sam Gazitt, Nikhil Mungel, Brian Krueger

September 2017

Disclaimer

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.

Who **We** Are

Sam Gazitt

Director of Product Management

sgazitt@splunk.com

Nikhil Mungel

Principal Software Engineer
Incubation & Innovation Engineering

nikhil@splunk.com

Brian Krueger

Senior Software Engineer
Incubation & Innovation Engineering

bkrueger@splunk.com

Ledio Ago

Senior Director
Incubation & Innovation Engineering

ledio@splunk.com

Who **You** Are

IT/Operations

Can Nova help me enable my development teams more quickly?

Enterprise Developer

Is Nova something I can use quickly to aggregate my app logs?

How does Nova help me observe and analyze the behavior of my services?

Startup Developer

If it’s not on HackerNews, it doesn’t exist to me.
Also, tabs > spaces!

Other

Am I in the right room?
Where is the coffee?

What **You** Will Learn

IT/Operations

Project Nova can help me unblock my developers as my company moves to the cloud!

Enterprise Developer

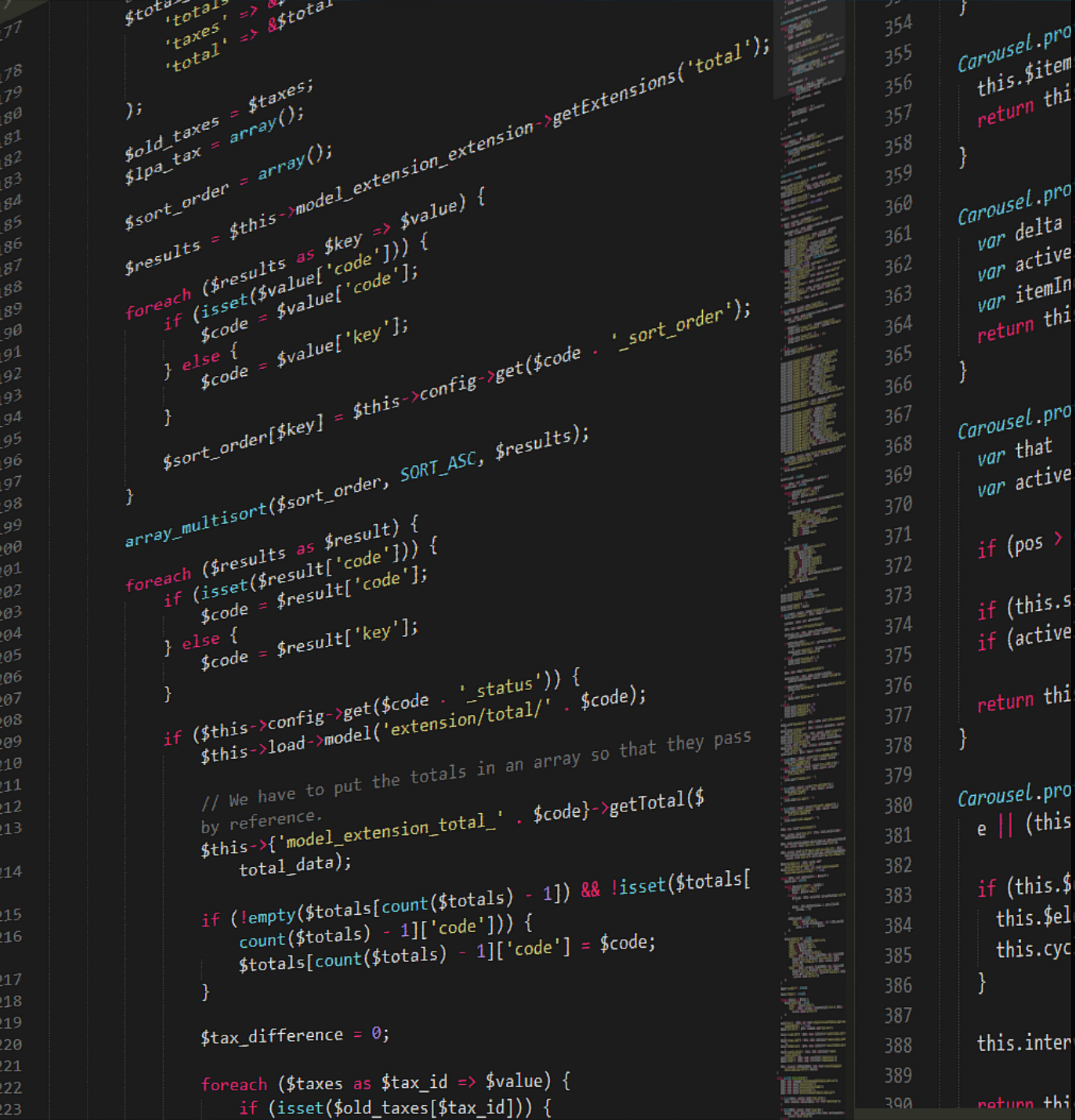
Project Nova can help me understand the quality, availability, and performance of my microservices across their entire lifecycle

Startup Developer

I'll be reading comments about Project Nova on HackerNews sometime soon. Cool!

Other

The closest coffee is out the door, to the left, and down to the end of the hall. ☺



Building Microservices

Beyond just writing code…

- Manage complex dependencies between services
- Measure and improve availability
- Manage continuous delivery of updates
- Design for resiliency and elasticity
- Manage container orchestration

⚠ Not enough time to manage logging and monitoring tools

Splunk Project Nova

Cloud APIs that remix Splunk technology into a developer’s world

Splunk Technology Remixed

Nova REST APIs integrated into dev tools and ecosystems

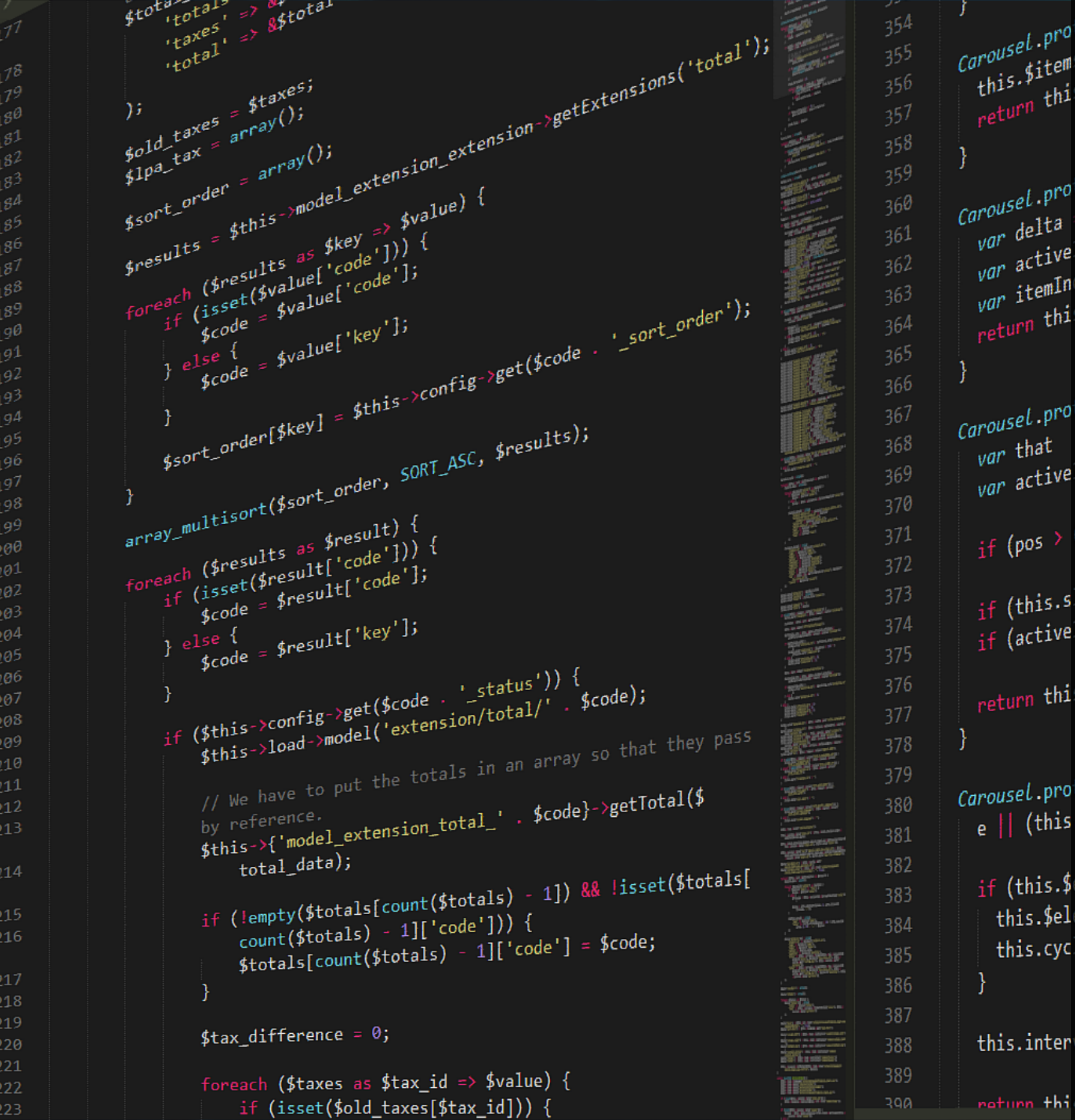
Dev Communities

Visualization

CLIs and SDKs

Cloud Platforms

Open Source Tools



Building Microservices

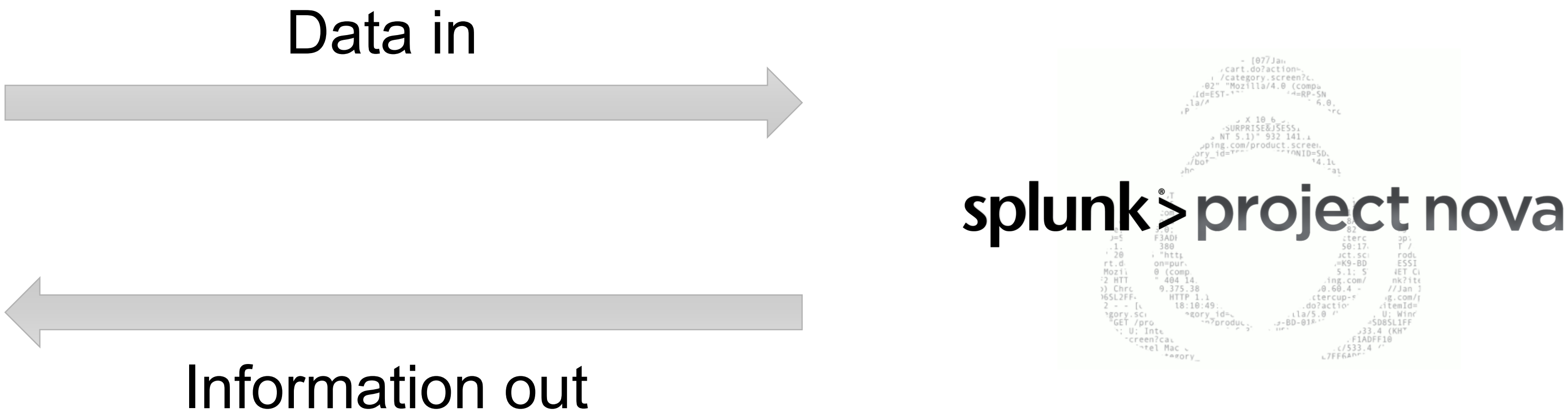
Use Splunk Project Nova to…

- Trace requests across services
- Analyze API access logs
- Track build and deployment health
- Quickly capture and debug errors
- Monitor the logs and metrics from cloud platforms

✓ Use Splunk Project Nova’s cloud APIs instead of managing your own tools

The journey of a thousand miles begins with a single step.

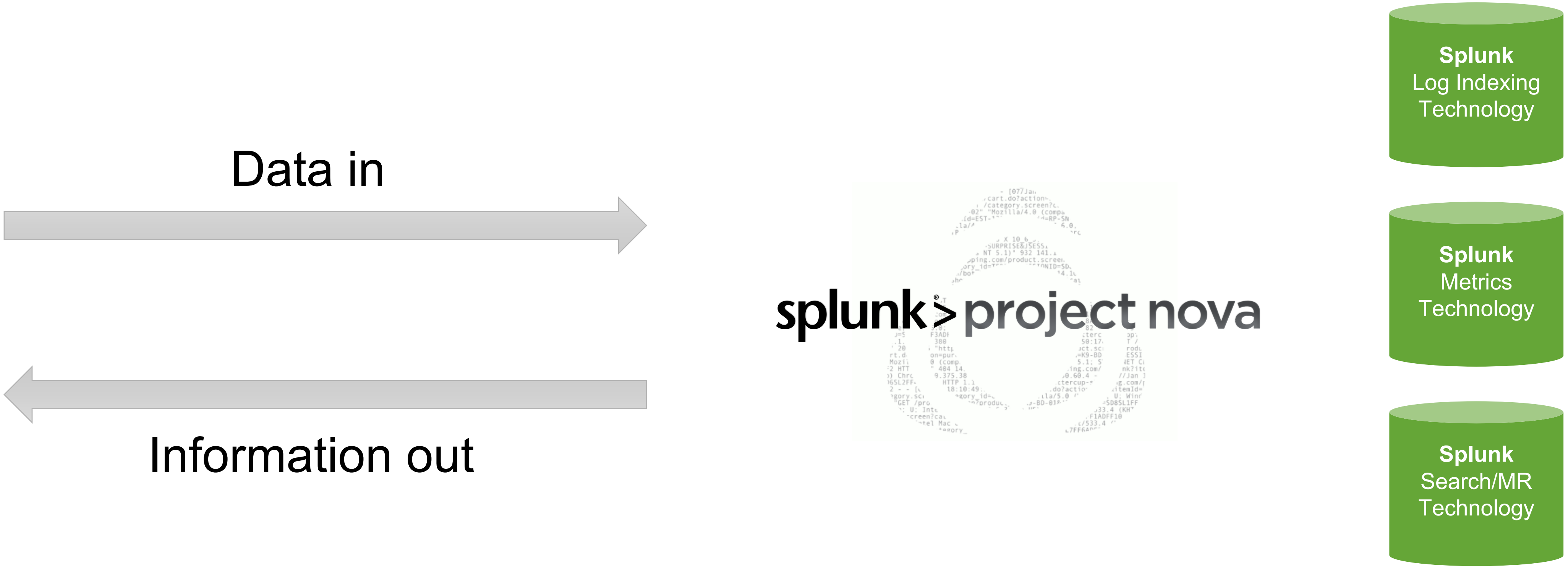
Lao Tzu



Data in

splunk> project nova

Information out



Data in

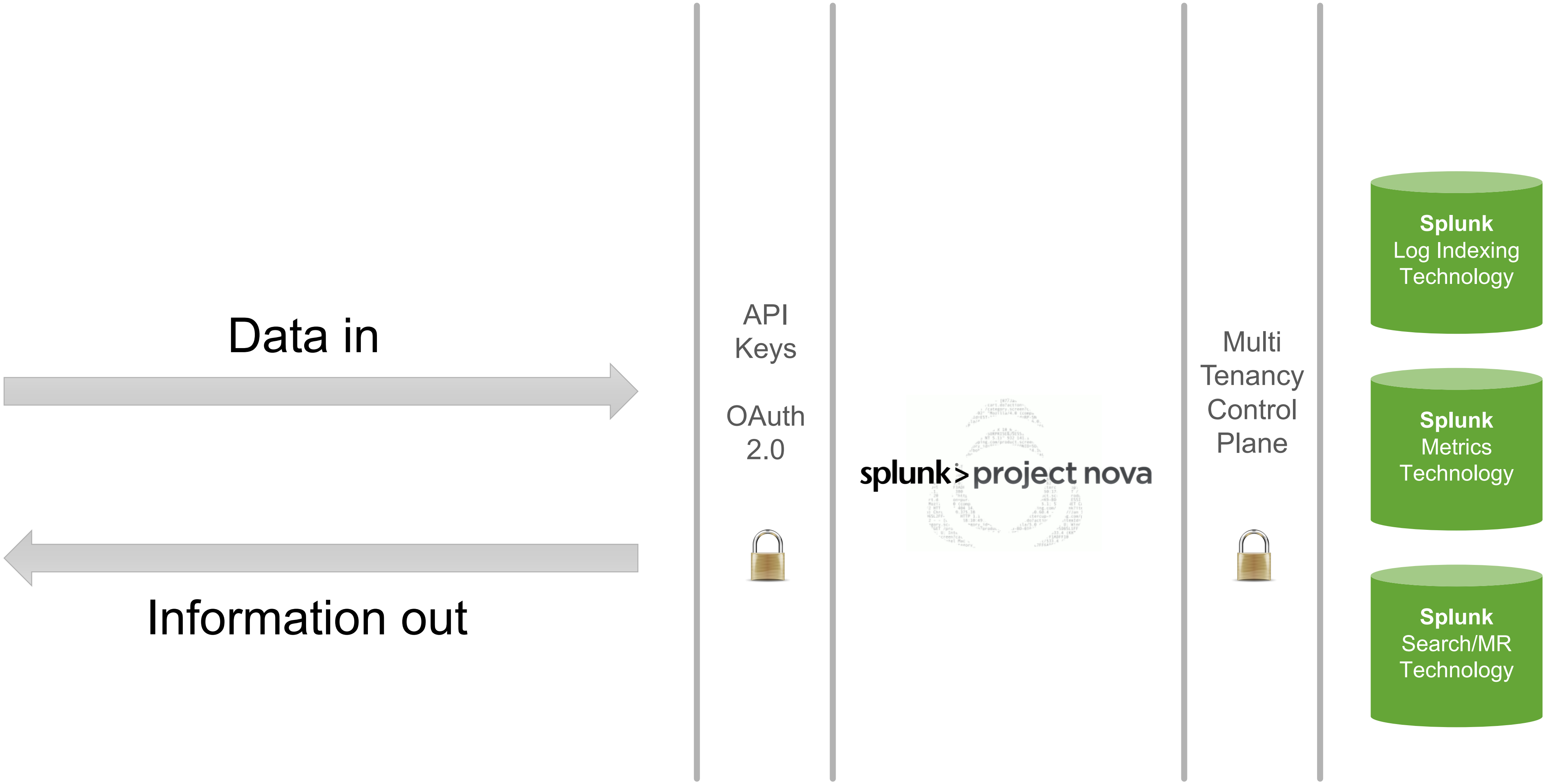
Information out

splunk> project nova

Splunk
Log Indexing Technology

Splunk
Metrics Technology

Splunk
Search/MR Technology



Data in

Information out

API Keys

OAuth 2.0

splunk> project nova

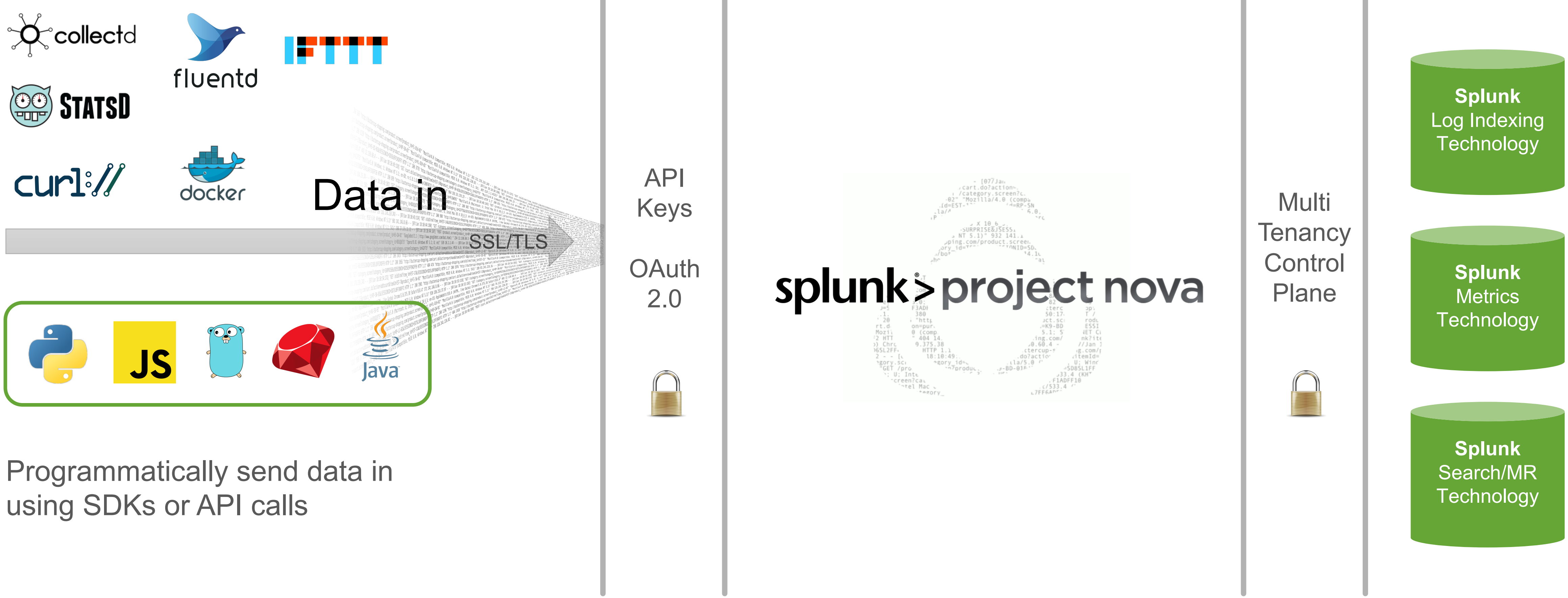
Multi Tenancy Control Plane

Splunk Log Indexing Technology

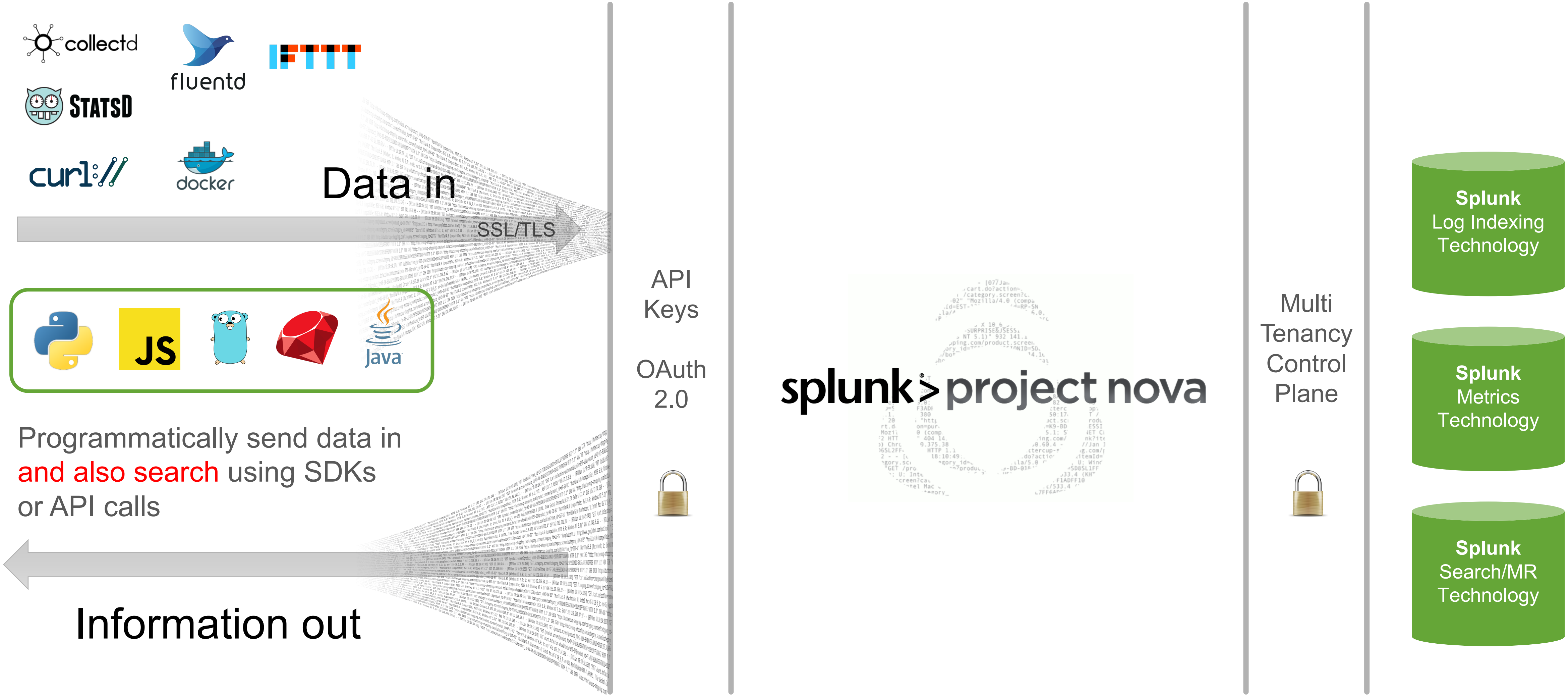
Splunk Metrics Technology

Splunk Search/MR Technology

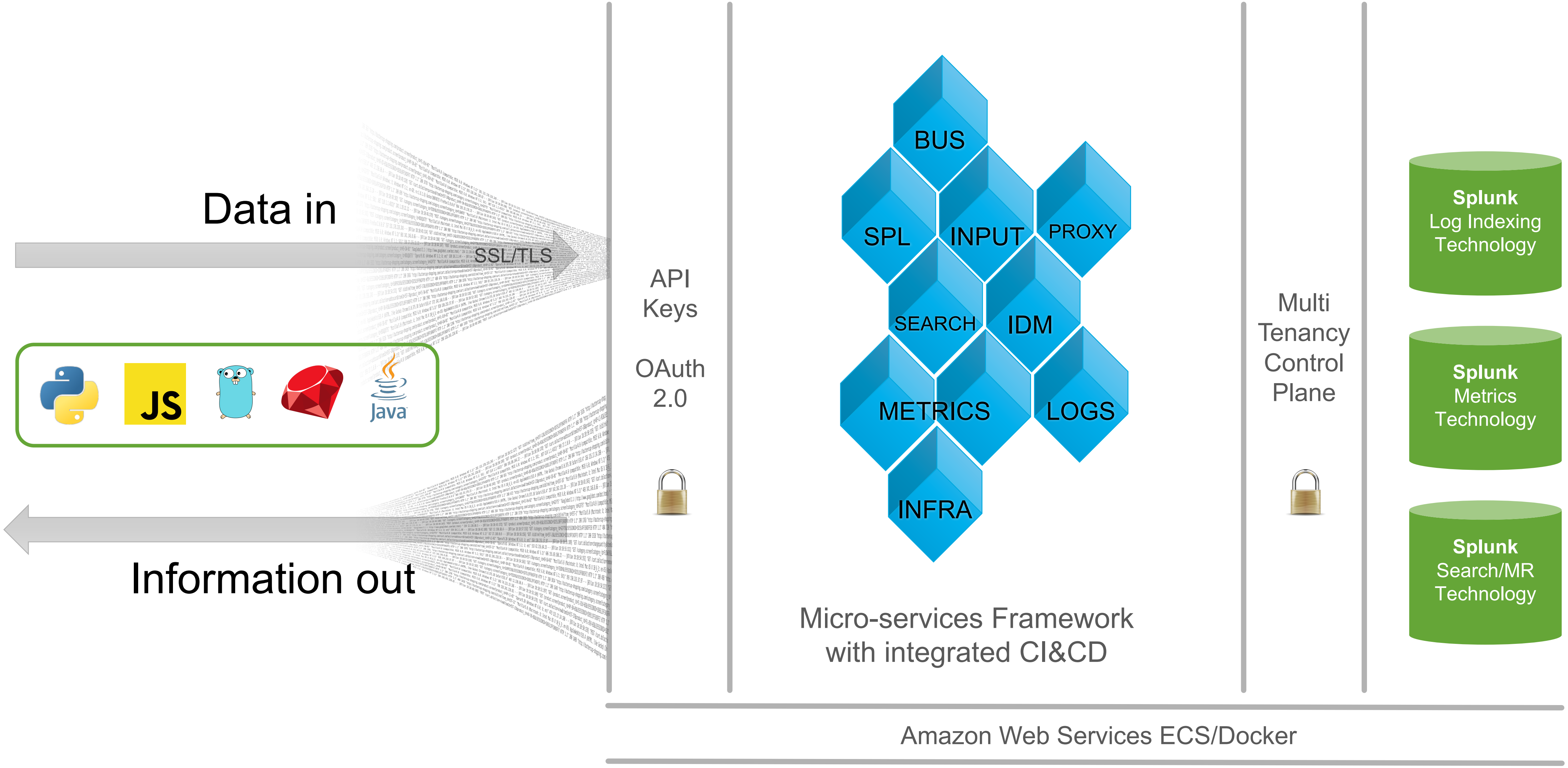
Send data using collectors & logging drivers*


collectd
fluentd
IFTTT
STATSD
curl://
docker
Data in
SSL/TLS
JS
Java
API Keys
OAuth 2.0
splunk> project nova
Multi Tenancy Control Plane
Splunk Log Indexing Technology
Splunk Metrics Technology
Splunk Search/MR Technology

Programmatically send data in using SDKs or API calls



Programmatically send data in and also search using SDKs or API calls



Data in

SSL/TLS

Information out

API Keys

OAuth 2.0

BUS

SPL

INPUT

PROXY

SEARCH

IDM

METRICS

LOGS

INFRA

Micro-services Framework with integrated CI&CD

Multi Tenancy Control Plane

Splunk Log Indexing Technology

Splunk Metrics Technology

Splunk Search/MR Technology

Amazon Web Services ECS/Docker

REST API

Fig 1.1: How to troll a developer

REST API

- Nova was built with developers, integrations and automation in mind
- Unified and versioned API resides at **https://api.splunknova.com/v1/**
- Open API (Swagger) compliant REST API
- Auto-generated clients* and integrations

**Your mileage may vary with auto generated libraries*

REST API

For Structured Events

HTTP POST /v1/events

```
[
  {
    "entity":     "52.52.52.52",
    "source":     "app1",
    "module":     "web",
    "processing": "started",
    "user":       "abc1def"
  }
]
```

HTTP GET /v1/events

- *How many times did we process a particular user*
  `/events/?keywords="abc1def"&report="stats count by processing"`

- *How many unique users did we see*
  `/events/?keywords="*"&report="stats dc(user)"`

REST API

For Custom Metrics

HTTP POST /v1/metrics

```
{
  "fields": {
    "source":      "52.52.52.52",
    "entity":      "app1",
    "metric_name": "pageLoadTime",
    "_value":      1.2345,
    "user":        "abc1def",
    "location":    "DC"
  }
}
```

HTTP GET /v1/metrics

- *Mean page load time*
  `/metrics/pageLoadTime/mean`
- *Get the 95th percentile slowest*
  `/metrics/pageLoadTime/perc95`
- *Median load time by location*
  `/metrics/pageLoadTime/median/`
  `?group_by=location`

REST APIs

Fig 1.2: Assembly required

Integrations!

Dev Communities

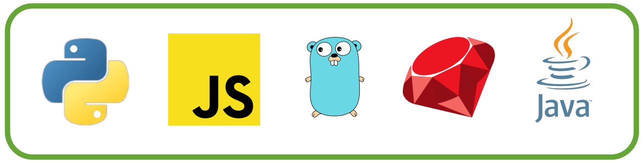
Visualization

CLIs and SDKs

Cloud Platforms

Open Source Tools

- An official CLI client that allows you to quickly get started with sending and searching structured events.
- Automatically generated swagger SDKs for language level integration for sending data and searching.



- Also log directly from your language runtime by using logging drivers.

CLIs and SDKs

Visualization

CLIs and SDKs

Cloud Platforms

Open Source Tools

- You can use agents like collectd, fluentd, telegraf, etc. to send data

```
#Sample Collectd Config
<Plugin write_http>
       <Node "example">
              URL https://api.splunknova.com/v1/metrics
              User "API_CLIENT_ID"
              Password "API_CLIENT_SECRET"
              Format "JSON"
              Metrics true
              Notifications false
              BufferSize 4096
              LogHttpError true
       </Node>
</Plugin>
```

Open Source Tools

Visualization

CLIs and SDKs

Cloud Platforms

Open Source Tools

- Have your serverless application directly dispatch data to SplunkNova
- Compatible with AWS Lambda, Google Cloud Functions, or Azure Functions

amazon web services

Google Cloud Platform

Microsoft Azure

- Docker logging driver can be used from any container service

Cloud Platforms

Visualization

CLIs and SDKs

Cloud Platforms

Open Source Tools

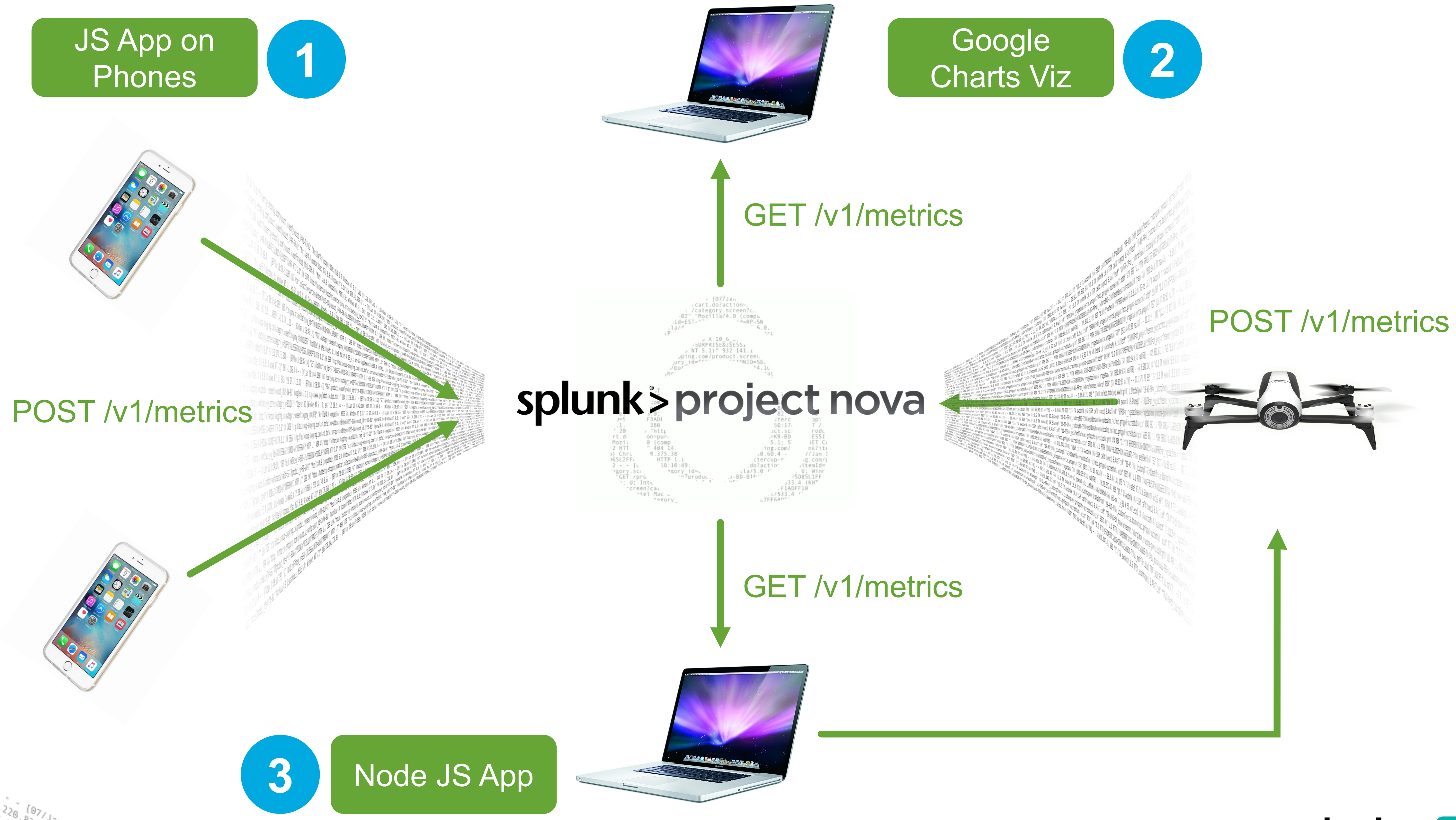
- SplunkNova has its own charting library for first class support*
- It's also compatible with most charting solutions like D3.js, Google Charts, or Highcharts!

Visualization

Fun with Integrations

- Home Automation
  - CURL data about Philips Hue lights, other Zigbee devices, or any home automation devices from a controller to SplunkNova.
  - Write an Alexa skill or another tool to action on this data!
- IFTTT
  - Use IFTTT to trigger events based on data in SplunkNova.
  - Integration available online!
- Slack Bot (or Hubot)
  - Have a bot POST an event to SplunkNova every time someone mentions a certain phrase (e.g. "Error", or "Throttled").
  - Mine this data to optimize or correct your processes.

Demo time!!!



JS App on Phones 1

Google Charts Viz 2

GET /v1/metrics

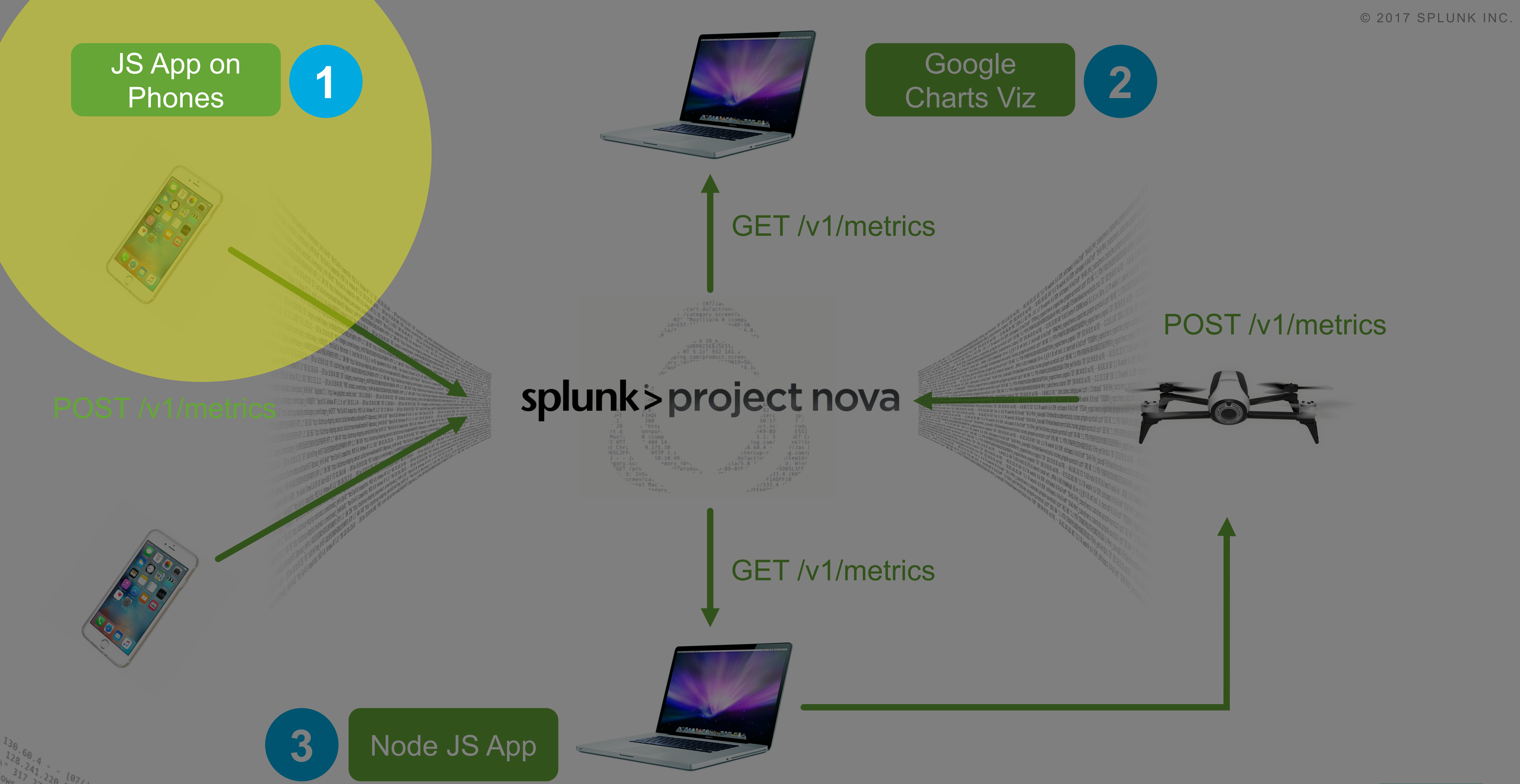
POST /v1/metrics

splunk> project nova

POST /v1/metrics

GET /v1/metrics

3 Node JS App



JS App on Phones 1

Google Charts Viz 2

Node JS App 3

POST /v1/metrics

GET /v1/metrics

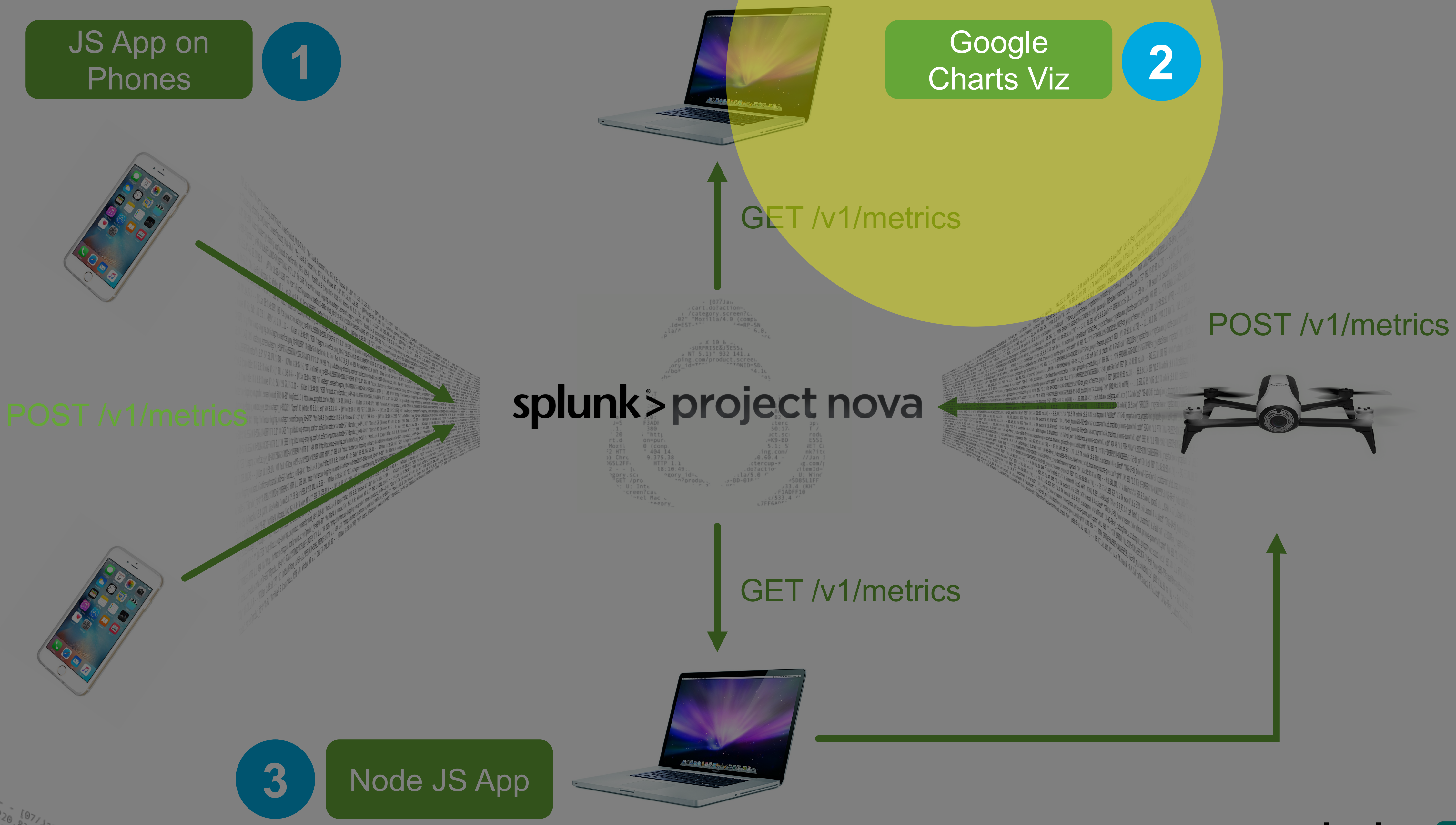
POST /v1/metrics

GET /v1/metrics

splunk> project nova

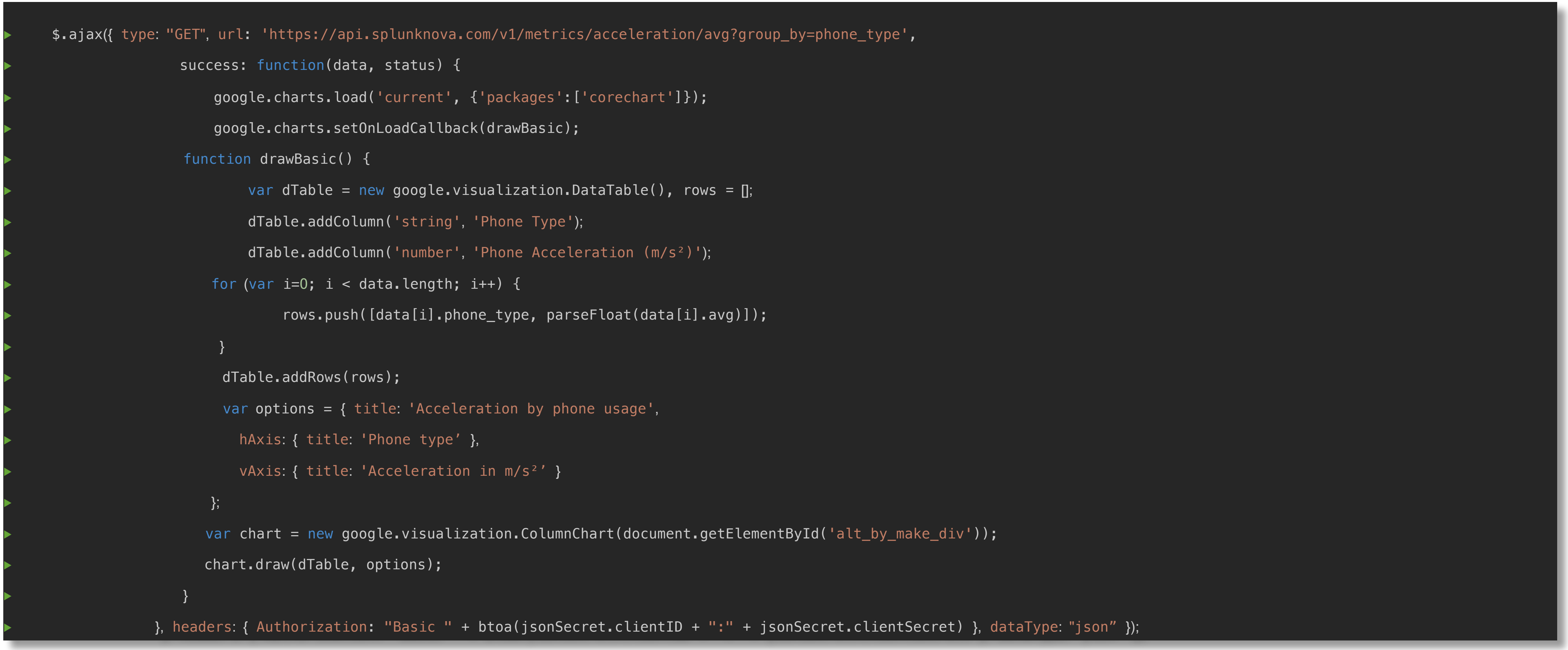
1 Sending Metrics in from the Phone App

```
$.ajax({
          method: "POST",
          url: ”https://api.splunknova.com/v1/metrics",
          data: JSON.stringify({
            "fields": {
                "metric_name": "acceleration",
                "_value": e.acceleration,
                "phone_type": getMobileOperatingSystem(),
                "uuid": e.uid
          }
      }),
      headers: {
          Authorization: "Basic " + encodedSecret
      },
      success: function(e, t, r) { console.log("Sent data!"); }
});
```

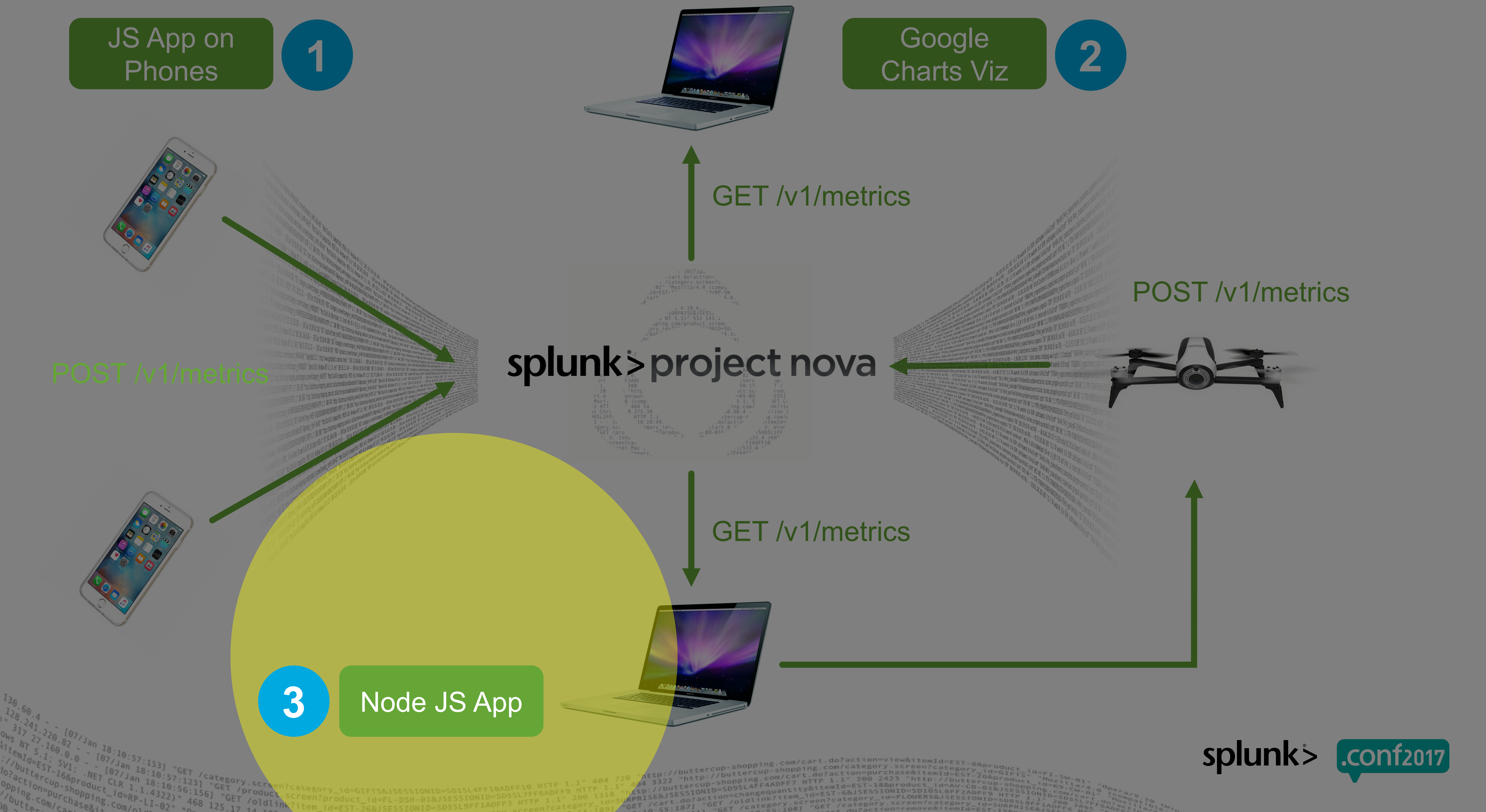


splunk> .conf2017

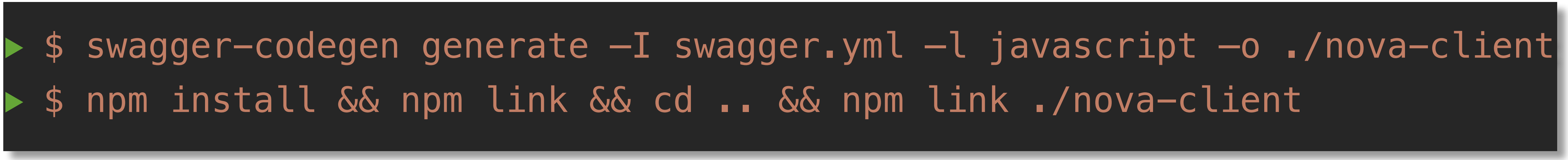
2 Visualizing Metrics Data with Google Charts



```
$.ajax({ type: "GET", url: 'https://api.splunknova.com/v1/metrics/acceleration/avg?group_by=phone_type',
               success: function(data, status) {
                   google.charts.load('current', {'packages':['corechart']});
                   google.charts.setOnLoadCallback(drawBasic);
                function drawBasic() {
                       var dTable = new google.visualization.DataTable(), rows = [];
                       dTable.addColumn('string', 'Phone Type');
                       dTable.addColumn('number', 'Phone Acceleration (m/s²)');
                   for (var i=0; i < data.length; i++) {
                           rows.push([data[i].phone_type, parseFloat(data[i].avg)]);
                    }
                    dTable.addRows(rows);
                    var options = { title: 'Acceleration by phone usage',
                      hAxis: { title: 'Phone type’ },
                      vAxis: { title: 'Acceleration in m/s²’ }
                   };
                  var chart = new google.visualization.ColumnChart(document.getElementById('alt_by_make_div'));
                  chart.draw(dTable, options);
                }
            }, headers: { Authorization: "Basic " + btoa(jsonSecret.clientID + ":" + jsonSecret.clientSecret) }, dataType: "json” });
```


JS App on Phones
1
Google Charts Viz
2
GET /v1/metrics
POST /v1/metrics
POST /v1/metrics
splunk> project nova
GET /v1/metrics
3
Node JS App
splunk> .conf2017

Setting up Node.js Client from Swagger



```
▶ $ swagger-codegen generate -I swagger.yml -l javascript -o ./nova-client
▶ $ npm install && npm link && cd .. && npm link ./nova-client
```

3

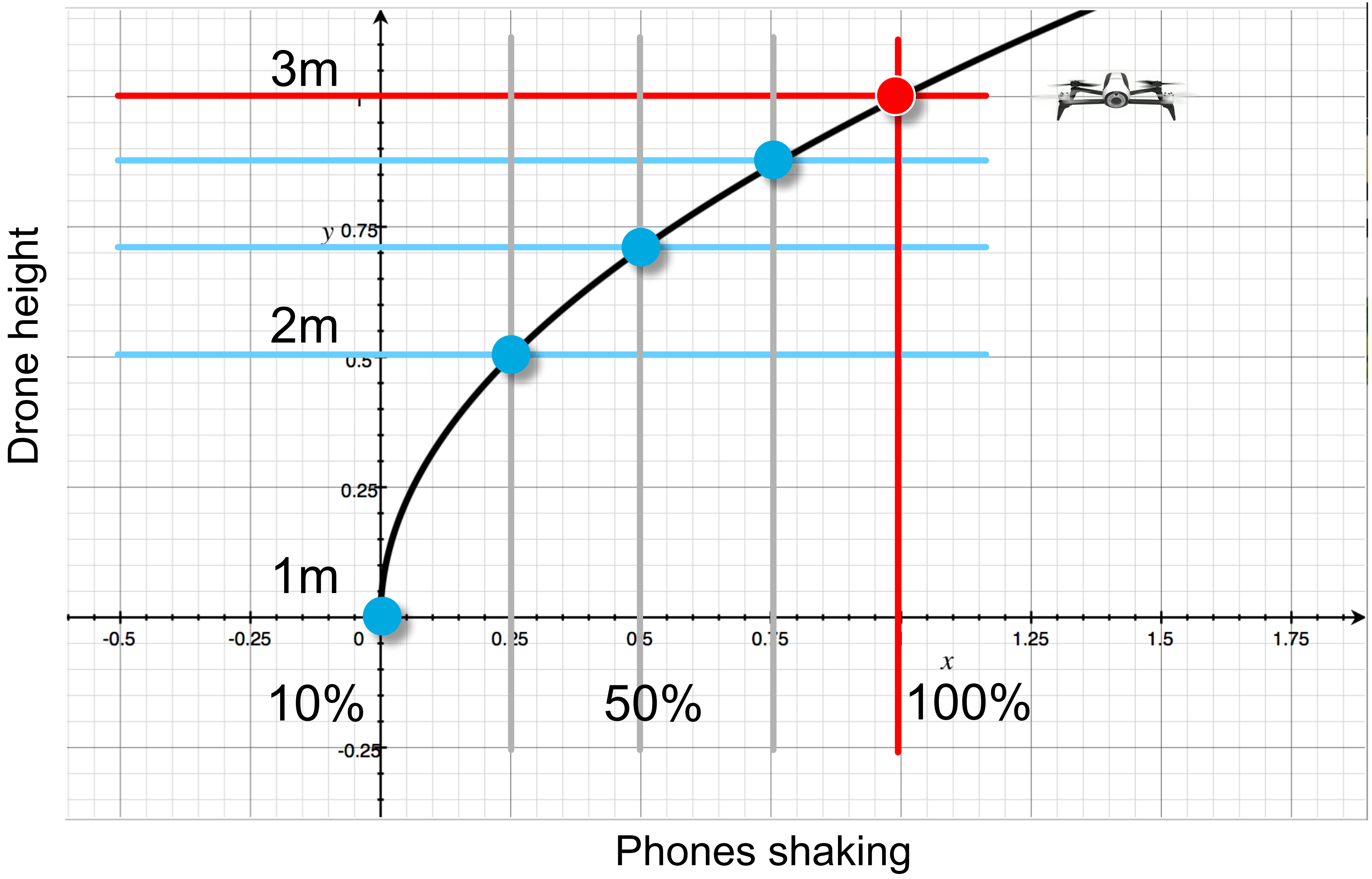
Getting Metrics with a Node.js Generated Client

```
var NovaDeveloperApi = require('nova_developer_api'),
    basicAuth = defaultClient.authentications['basicAuth'];
// Configure HTTP basic authorization: basicAuth;
basicAuth.username = secrets.clientID;
basicAuth.password = secrets.clientSecret;
var apiInstance = new NovaDeveloperApi.MetricsApi();
var getMetrics = function() {
    var metricNames = "acceleration"; // String | comma separated list of dotted notation metric names
    var aggregations = "avg"; // String | comma separated aggregation operations like 'avg', 'max' etc.
    var opts = {
            'span': "2s", // String | time span to split aggregated metrics by. e.g. '1m', '1d' etc.
            'pageCount': 1, // Number | number of metrics to return, sorted by most recent first.
            'pageIndex': 0 // Number | return metrics starting at index, 0 is most recent.
     };
     apiInstance.metricsMetricNamesAggregationsGet(metricNames, aggregations, opts, handleMetricResult);
};
```

demo.splunknova.com

On your phone or tablet

Data-Driven Drone



Recap

IT Operations

Project Nova can help me unblock my developers as my company moves to the cloud!

Enterprise Developer

Project Nova can help me understand the quality, availability, and performance of my microservices across their entire lifecycle

Startup Developer

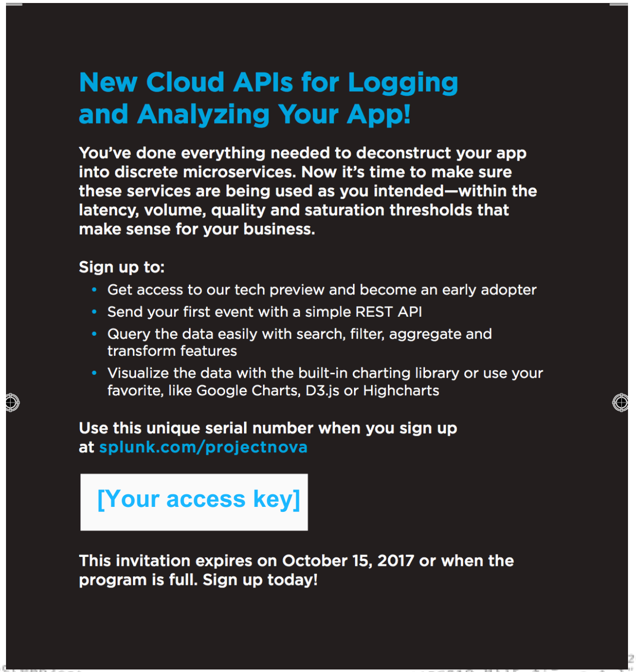
I’ll be reading comments about Project Nova on HackerNews sometime soon. Cool!

Other

The closest coffee is out the door, to the left, and down to the end of the hall. ☺

Get rewarded for helping out!

- Accept your tech preview invitation at splunknova.com
- The **first 50 people** who provide feedback will **get $25 gift cards**!
- Stop by the booth and show us what you've built to collect your gift card.
- Join our slack community at community.splunknova.com



New Cloud APIs for Logging and Analyzing Your App!

You've done everything needed to deconstruct your app into discrete microservices. Now it's time to make sure these services are being used as you intended—within the latency, volume, quality and saturation thresholds that make sense for your business.

Sign up to:

- Get access to our tech preview and become an early adopter
- Send your first event with a simple REST API
- Query the data easily with search, filter, aggregate and transform features
- Visualize the data with the built-in charting library or use your favorite, like Google Charts, D3.js or Highcharts

Use this unique serial number when you sign up at splunk.com/projectnova

[Your access key]

This invitation expires on October 15, 2017 or when the program is full. Sign up today!

Demo links

- Repository links:
  - https://github.com/swagger-api/swagger-codegen - For generating your own clients
  - https://api.splunknova.com/swagger.json - Our REST definition
  - https://nodejs.org/en/ - Node
  - https://github.com/hybridgroup/node-bebop -- Drone API
  - https://developers.google.com/chart/ - For creating your own charts

Thanks!

Don't forget to **rate this session** in the .conf2017 mobile app

splunk> .conf2017