

# splunk® > live!

APRIL 20, 2017 | MINNEAPOLIS, MN

# splunk® > live!

APRIL 20, 2017 | MINNEAPOLIS, MN

**Delivering New Visibility and Analytics for IT Operations**

Brett Knudson | Senior Sales Engineer, Named Accounts

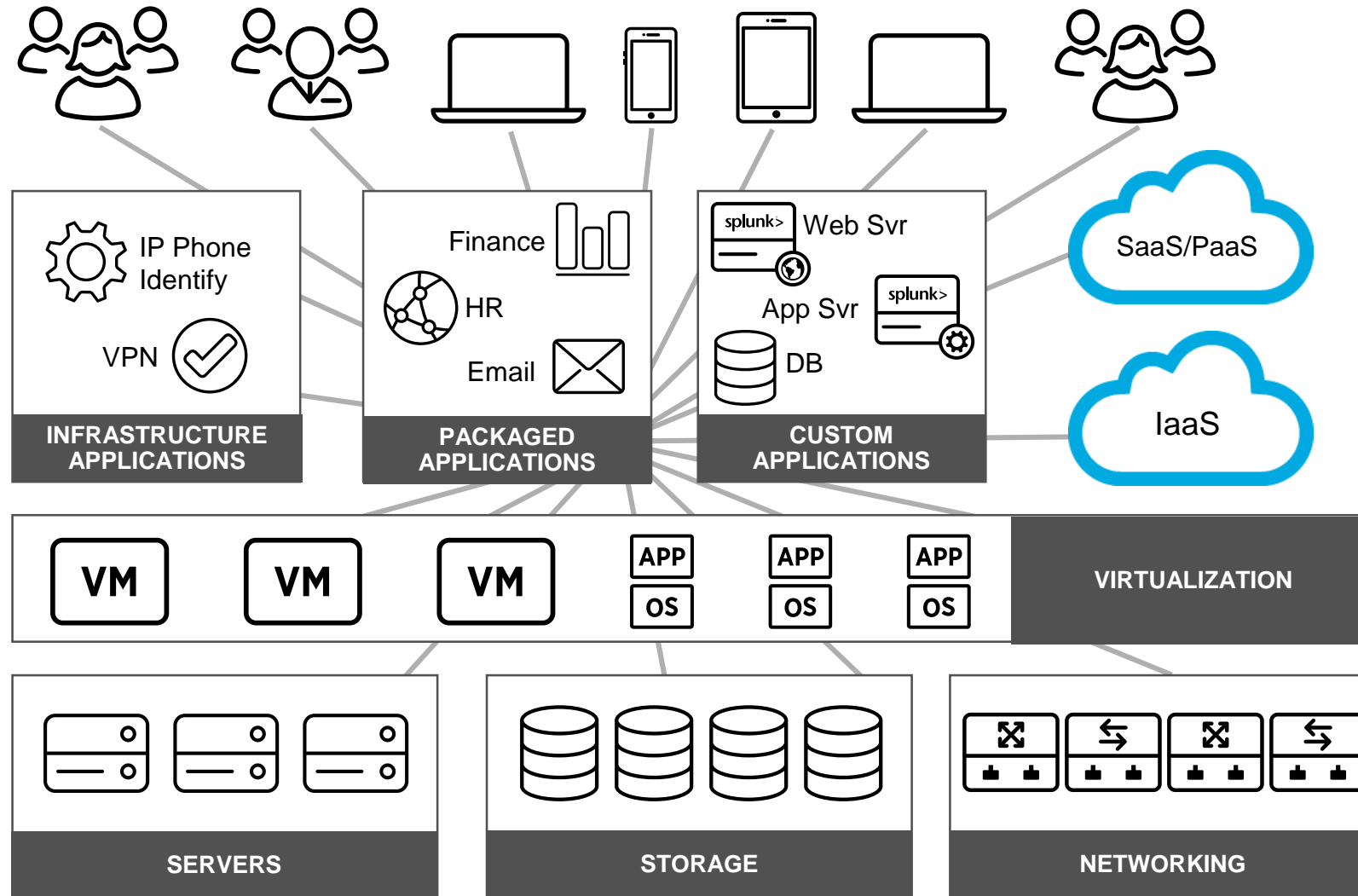
# Safe Harbor Statement

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.

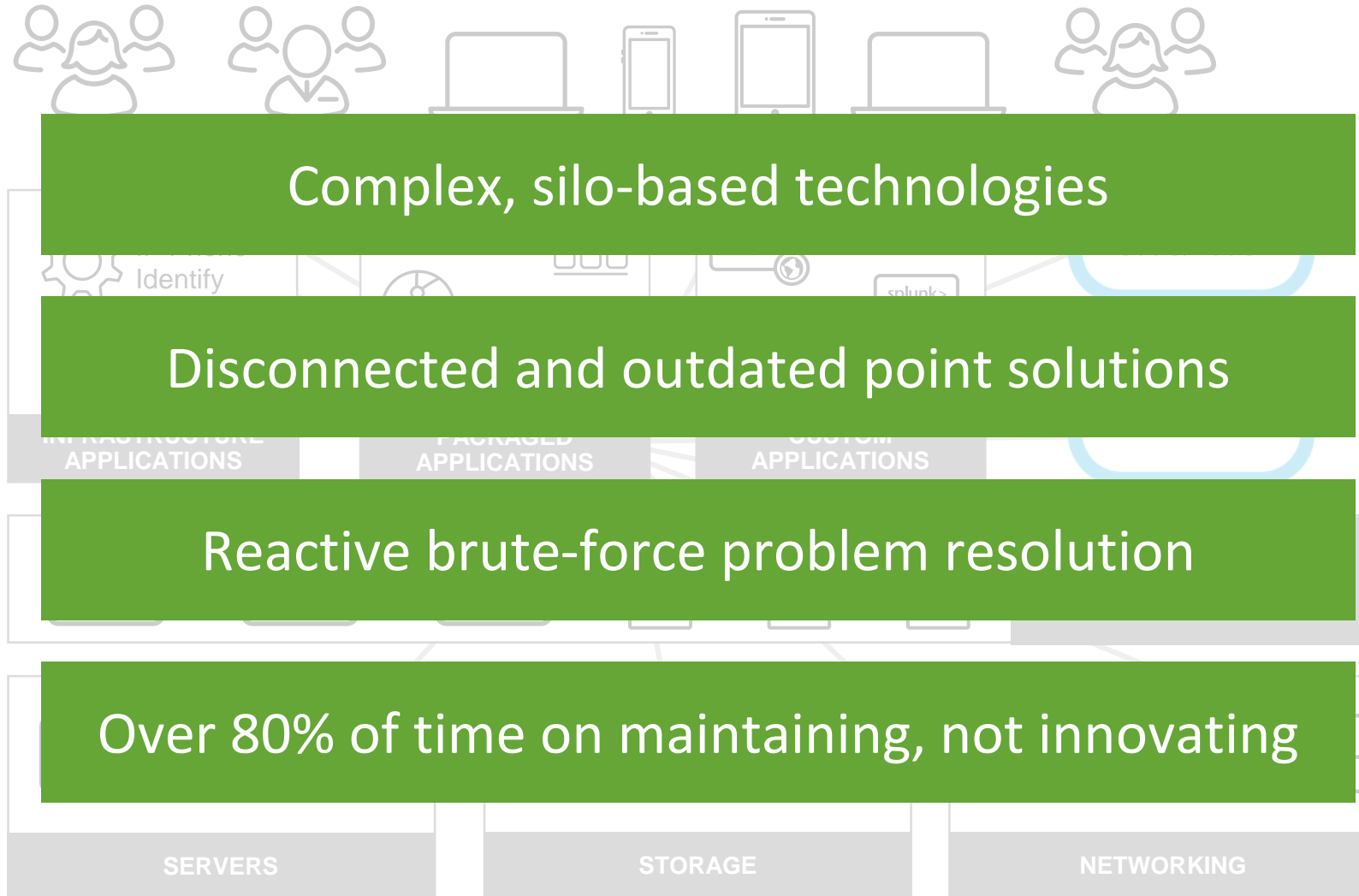
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements 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. © 2017 Splunk Inc. All rights reserved.

# Escalating IT Complexity...



# Escalating IT Complexity...





# Industry-Leading Platform for Machine Data

## Any Machine Data



## Operational Intelligence

Search and Investigation

Proactive Monitoring

Operational Visibility

Real-Time Business Insights

splunk>enterprise

splunk>cloud

Enterprise Scalability

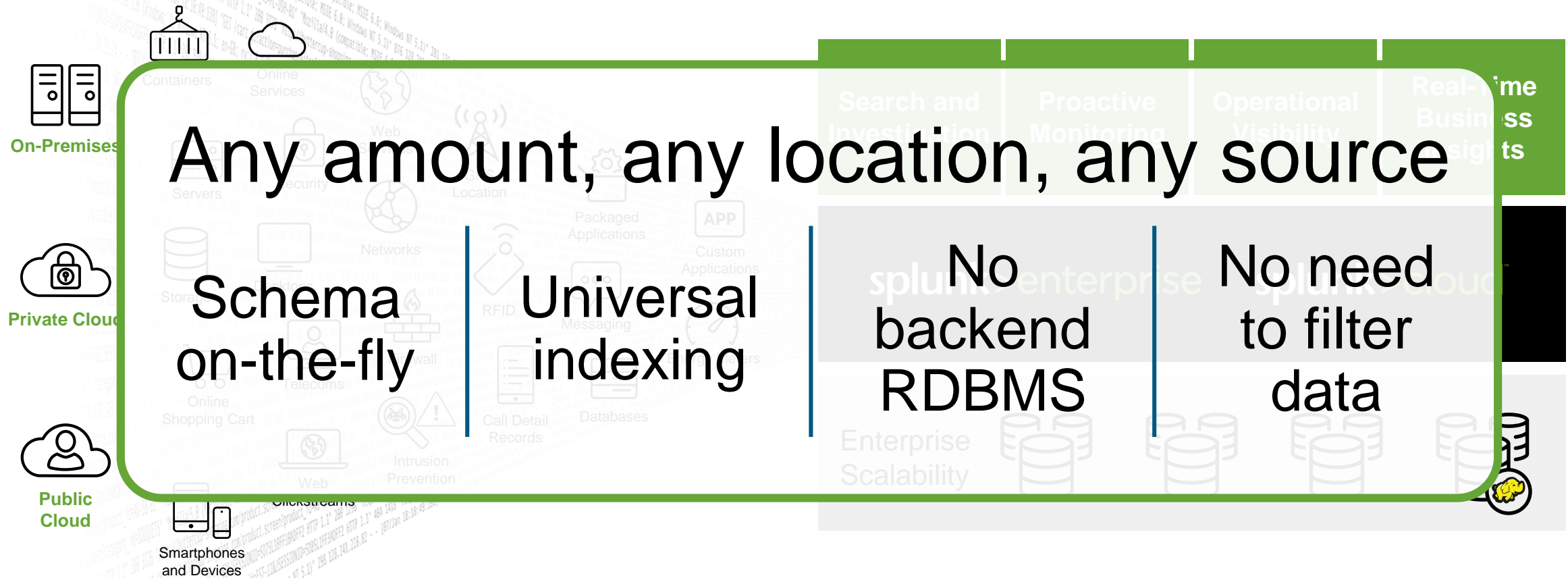


splunk>live!

# Industry-Leading Platform for Machine Data

Any Machine Data

Operational Intelligence



# The Focus

Application  
Delivery

IT  
Operations

Security,  
Compliance  
and Fraud

Business  
Analytics

Internet of  
Things and  
Industrial  
Data

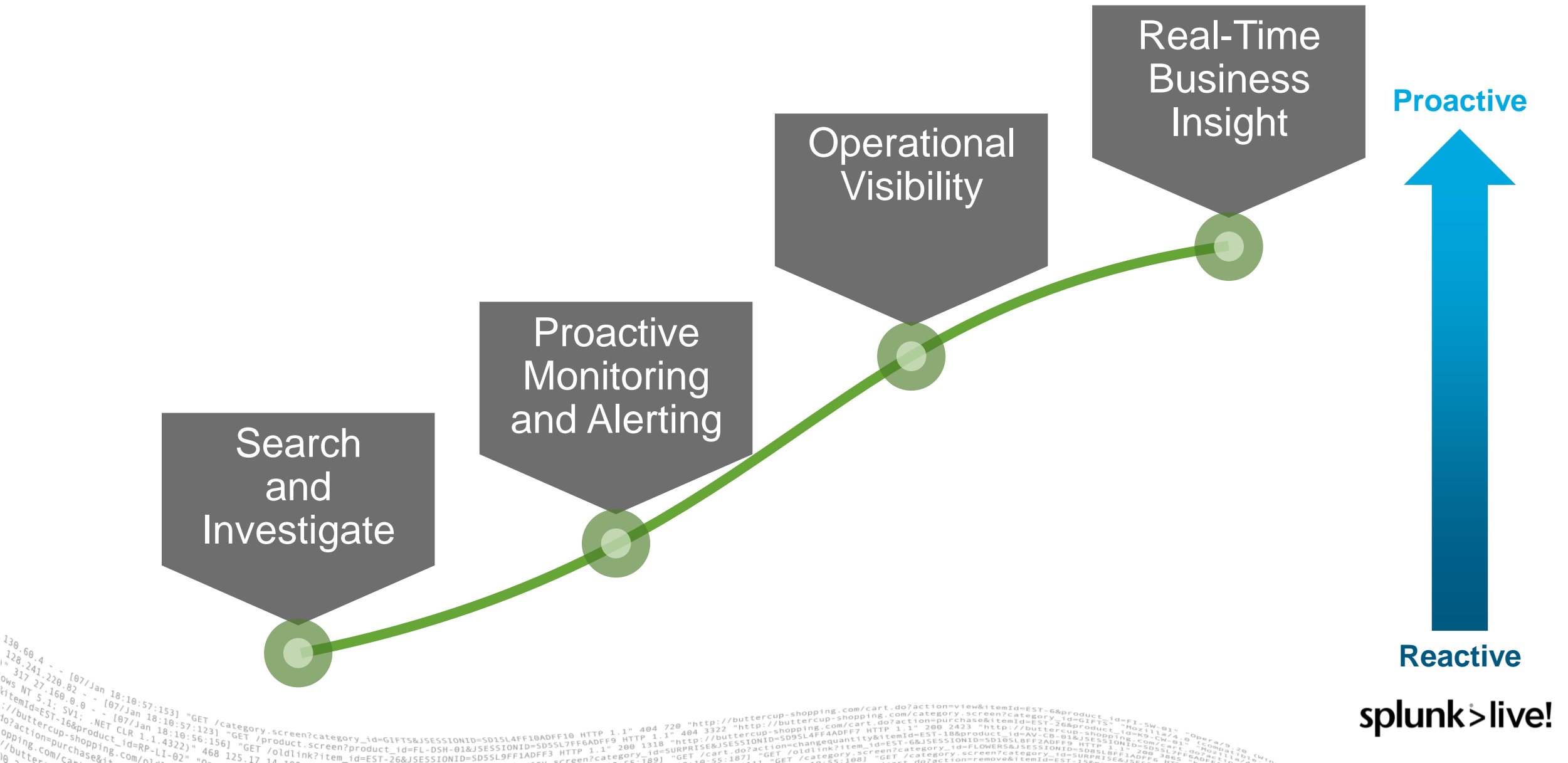
Developer Platform (REST API, SDKs)

**splunk**> Platform for Operational Intelligence

**splunk**>live!

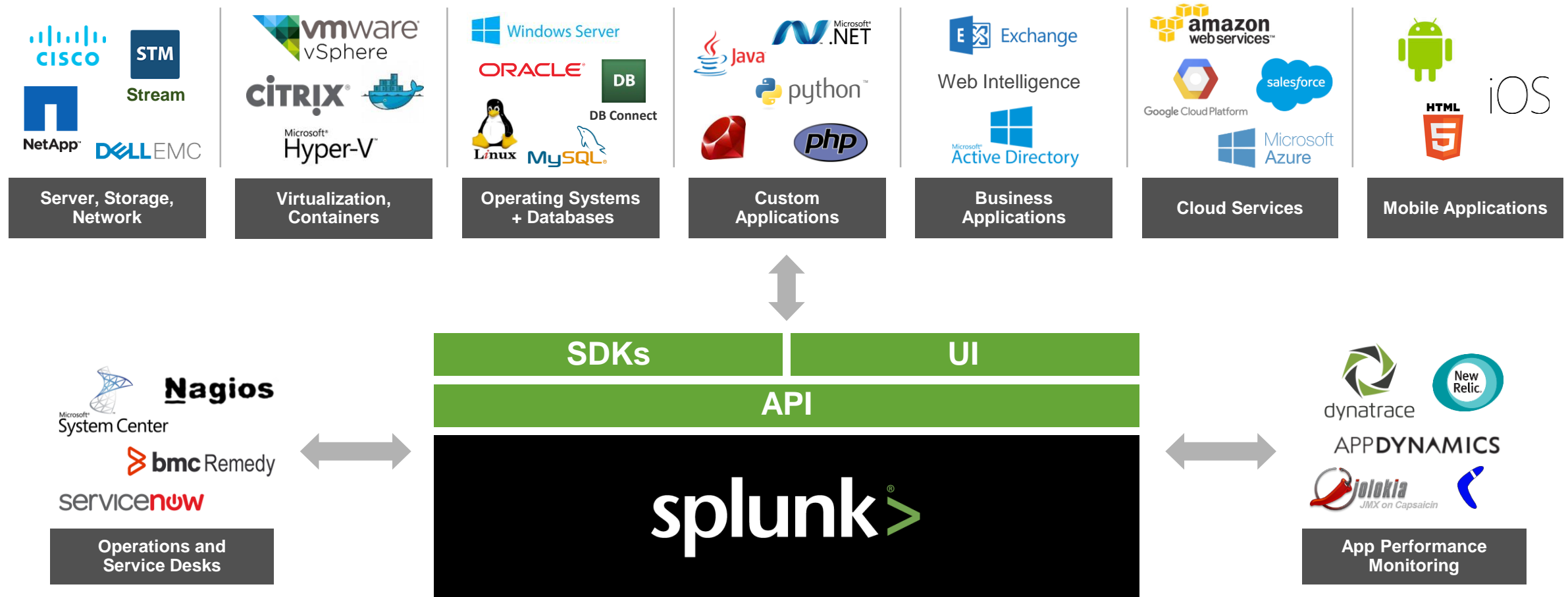


# Turning Machine Data Into Operational Intelligence



# Index and Analyze Data Across Your Technology Stack

Splunk Add-Ons, Templates and Apps Accelerate Value From Machine Data

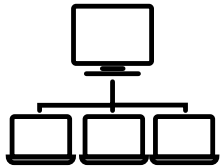


*No rigid schemas – add in data from any other source.*

**splunk>live!**

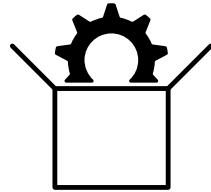
# Splunk Quick Start

A quick and easy way to deploy Splunk Enterprise at a low price



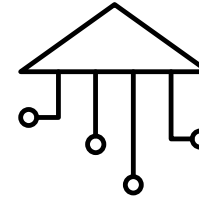
**Splunk  
Enterprise  
License**

**Discounted  
by volume**



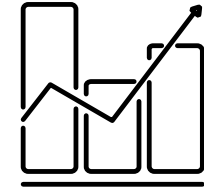
**Tailored Selection  
of Splunk Apps  
and Add-ons**

**Index and visualize  
the data sources  
you need**



**Splunk Education  
Credits and  
.conf Passes**

**Everything you need  
to get your team  
Splunk Certified**



**Personalized  
Support**

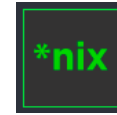
**Customer Success  
Manager to help you  
get up and running  
in 1 week**

# Quick Start for Infrastructure Monitoring

Fast time-to-results and success for a low entry price



Tailored  
Apps are



Active Directory



vmware  
vSphere



Add-On  
Builder



Windows Server



Expert Guidance and Customer  
Success Manager



Education Credits  
and .conf Passes

splunk>enterprise

splunk>live!

# Quick Start for Application Management

Fast time-to-results and success for a low entry price



**Tailored Selection of Apps and Add-ons**



Machine Learning



MINT



Active Directory



Stream



Add-On Builder



**Expert Guidance and Customer Success Manager**



**Education Credits and .conf Passes**

**splunk>enterprise**

**splunk>live!**



# Let's Get Hands-On

Install Splunk if you haven't

Start Splunk

splunk start — accept-license

Log in

<http://localhost:8000>

Credentials: [admin/changeme](#)

Install app

Click the widget next to “Apps”

Install app from file

Choose the app from the USB key

Restart Splunk

## ► Cloud Instances

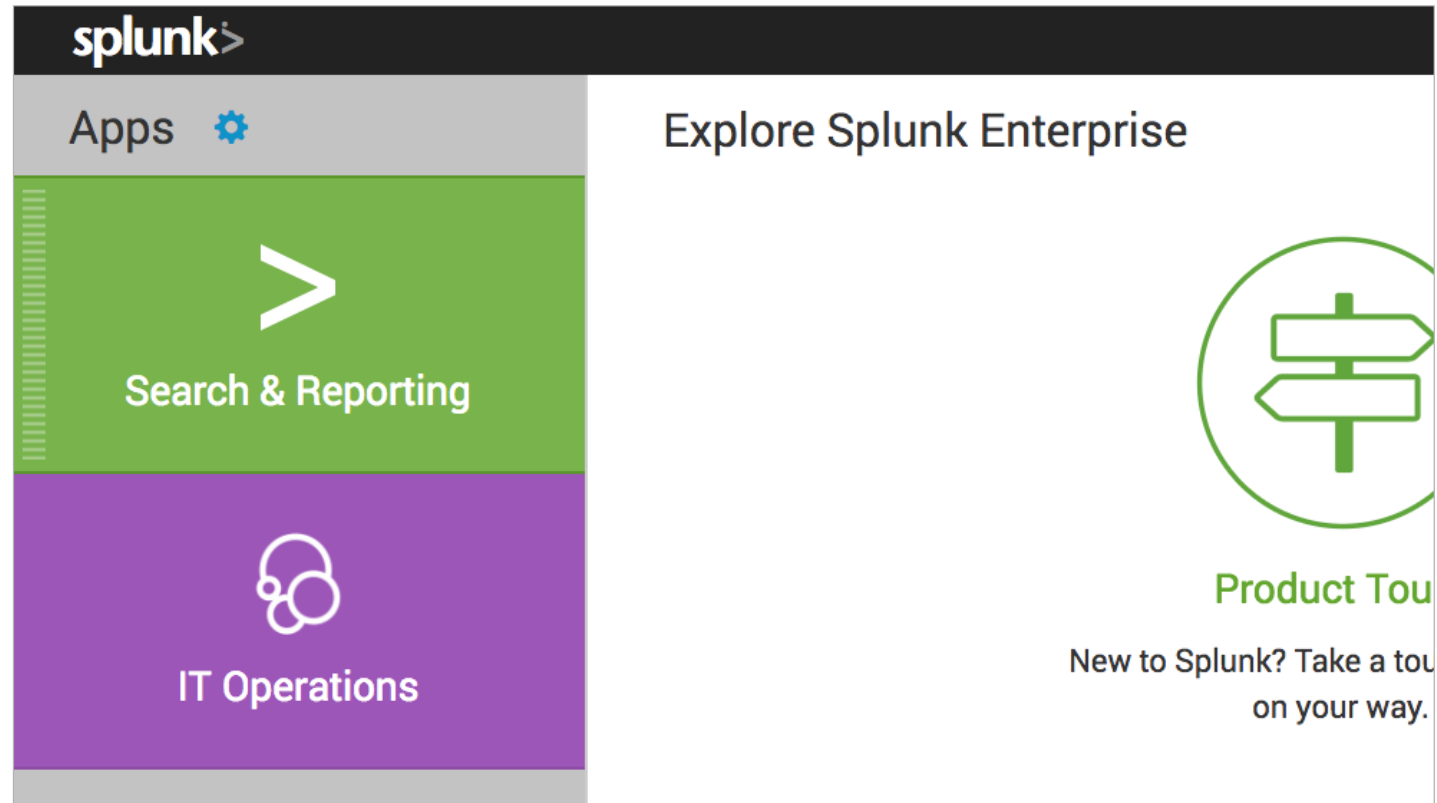
- <https://od-sl-mpls-itops-01.splunkoxygen.com>
- <https://od-sl-mpls-itops-02.splunkoxygen.com>

## ► Log in

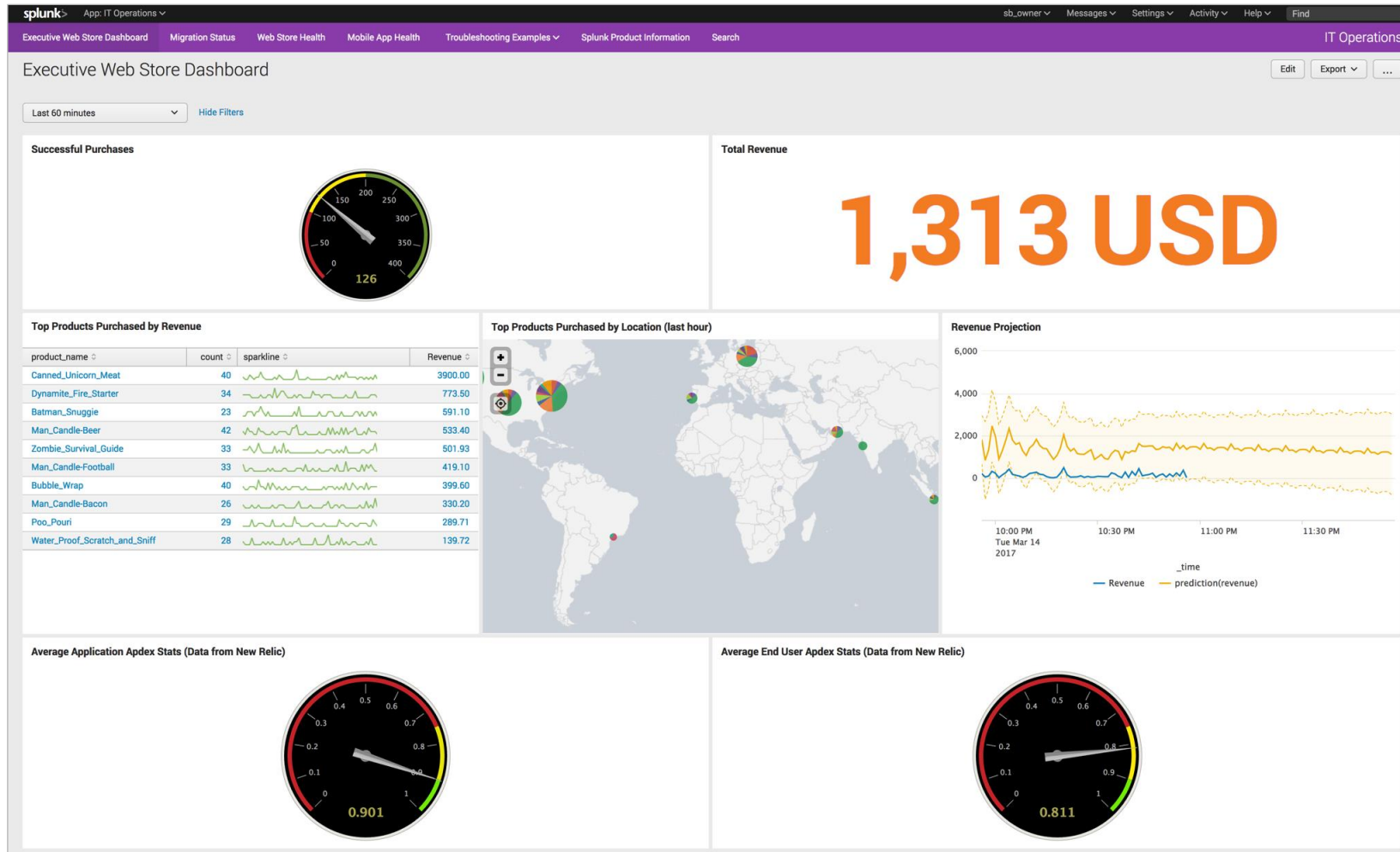
- Credentials: user[01-10]/changeme[01-10]

# Welcome to Splunk

- ▶ **Click IT Operations**  
to get started using Splunk!



# Dashboards



# Errors on the website!

- ## Our job: find the root cause!


# Our Dashboard

At the top of the screen,  
*click* on **Troubleshooting Examples**,  
 then *click* on **IT Troubleshooting Basics 1 – Web Site Errors**

IT Troubleshooting Basics 1 - Web Site Errors
Edit
Export
...

### Background

One of the most common ways that people use Splunk is for searching and investigating issues, using their data to find the root cause of problems. In this example, we'll be looking for issues in web access logs.



Machine data can come in many different formats, but Splunk can ingest it all and make it searchable. Splunk Add-ons help you get started with Splunk faster by providing configurations that you can use to ingest and parse data. Splunk Apps can provide reports and visualizations to help you use that data.

Splunk takes your *events* and extracts *fields* from it. For example, in a typical web log event, you might expect to find a field for the status code.

### Resources

- Splunk Add-on for Apache Web Server
- Splunk Add-on for IBM WebSphere
- Splunk Add-on for NGINX
- Splunk Add-on for IIS

### Key Techniques

This example leverages the following useful techniques:

- Basic searching
- Understanding events
- Understanding fields
- Aggregating data using the *stats* command

### Next Steps

Once you've identified the "bad" server, try to find the problem using [search](#)!

Some hints on how to proceed:

- What data is available for the server?
- What *fields* from that data may be useful?

If you're new to Splunk, click [HERE](#) for a more guided experience



# Our Search

Scroll to the **Line by Line** section,  
then *click* on **Load search to this point**  
to load the search results in a new tab.

**Line by Line**

**Pull Specific and Relevant Data**

```
sourcetype=apache:access status=503
```

[Load search to this point](#)



**Click Here!**

# Raw Events

**New Search** Save As ▾ Close

sourcetype=apache:access status=503 ← Our search Last 60 minutes ▾ Q

✓ 26 events (1/19/17 9:42:00.000 AM to 1/19/17 10:42:06.000 AM) No Event Sampling ▾ Job ▾ || ■ → ⬇ ⬆ Smart Mode ▾

Events (26) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 minute per column

List ▾ Format ▾ 20 Per Page ▾ Events < Prev 1 2 Next >

< Hide Fields All Fields

**Fields** ←

Selected Fields

- host 3
- source 1
- sourcetype 1

Interesting Fields

- action 4
- # bytes 22
- # bytes\_in 23
- # bytes\_out 23
- category 1
- code 7
- cost 7

i	Time	Event
>	1/19/17 10:39:39.453 AM	53.64.80.116 www.buttercup.com - jdunno 443 [19/Jan/2017 10:39:39:453994] "POST /cart?action=update&product_name=Batman_Snuggie&JSESSIONID=ECF5F0F929F0 HTTP 1.1" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML; like Gecko) Chrome/30.0.1599.66 Safari/537.36" 183 515 247870 host = web-05   source = /opt/apache/log/access.log   sourcetype = apache:access
>	1/19/17 10:38:49.306 AM	128.10.106.118 www.buttercup.com - pramosm 443 [19/Jan/2017 10:38:49:306843] "GET /login?JSESSIONID=3F3F7FF35FFF HTTP 1.1" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)" 202 502 276965 host = web-05   source = /opt/apache/log/access.log   sourcetype = apache:access
>	1/19/17 10:30:58.039 AM	170.75.96.119 www.buttercup.com - cjacksonr 443 [19/Jan/2017 10:30:58:039776] "POST /cart?action=add&product_name=Dynamite_Fire_Starter&JSESSIONID=DD0092D6FBF0 HTTP 1.1" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML; like Gecko) Chrome/30.0.1599.69 Safari/537.36" 218 591 315633 host = web-05   source = /opt/apache/log/access.log   sourcetype = apache:access
>	1/19/17 10:29:17.760 AM	5.195.54.127 www.buttercup.com - halvarezs 443 [19/Jan/2017 10:29:17:760340] "POST /orderstatus?JSESSIONID=E9FA4EFE5F2F HTTP 1.1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML; like Gecko) Chrome/29.0.1547.76 Safari/537.36" 215 499 245832 host = web-05   source = /opt/apache/log/access.log   sourcetype = apache:access

# Analyzing the Data

- *Scroll* to the **Line by Line** section again, then *click* on **Load search to this point** for the **second** search to load the results in a new tab.

## Line by Line

### Pull Specific and Relevant Data

```
sourcetype=apache:access status=503
```

[Load search to this point](#)

- **What:** Pull in the web logs, and filter to those with an error status
- **Why:** We know that our site is having an issue - let's see if we can

### Analyze the Data to Find the Rogue Server

```
| stats count by host
```

[Load search to this point](#)

**Click Here!**

# Search Results

**New Search** Save As Close

sourcetype=apache:access status=503 | stats count by host Last 60 minutes Q

✓ 21 events (1/19/17 9:59:00.000 AM to 1/19/17 10:59:36.000 AM) No Event Sampling Job || ■ → 📄 ⬇ 💡 Smart Mode

Events Patterns Statistics (2) Visualization

20 Per Page Format Preview

host	Count
web-03	1
web-05	20

**Our search** (points to the search bar)

**Hosts** (points to the host column)

**Count** (points to the count column)

Note: your search results may look different than the screen shot

# Wrapping Up on Web Errors

Full Search Results	
host	count
web-01	1
web-03	3
web-05	15

We've found our problem server... Now what?

## Next Steps

Once you've identified the "bad" server, try to find the problem using [search!](#)

Some hints on how to proceed:

- What data is available for the server?
- What *fields* from that data may be useful?

If you're new to Splunk, click [HERE](#) for a more guided experience

**Click Here!**

Scroll up to the **Next Steps** section and *click* the link to **search**.

Note: your search results may look different than the screen shot



# Next Steps

New Search

host=web-05 | stats count by sourcetype

Save As Close

Last 60 minutes

3,533 events (1/19/17 11:39:00.000 AM to 1/19/17 12:39:36.000 PM) No Event Sampling

Job

Smart Mode

Events Patterns Statistics (8) Visualization

20 Per Page Format Preview

sourcetype	count
apache:access	45
aws:cloudwatch	7
bandwidth	118
cpu	177
df	118
iostat	236
ps	2773
vmstat	59

We'll be taking a shortcut – *click* on **Troubleshooting Examples**, then *click* **IT Troubleshooting Basics 2 – Server Issues**

# An Infrastructure Problem



## SERVER'S DOWN

WE'RE WORKING ON IT

Line by Line

Pull Specific and Relevant Data

```
sourcetype=cpu host=web*
```

[Load search to this point](#)

**Click here!**

Which **fields** might help us find the problem?

# Analyzing the Data

Full Search Results	
host	max(cpu_load_percent)
web-01	59.08
web-02	65.48
web-03	63.09
web-04	66.84
web-05	85.71

## Next Steps

Now that you've identified the "bad" server, explore some different ways to visualize the results in the [search app](#)!

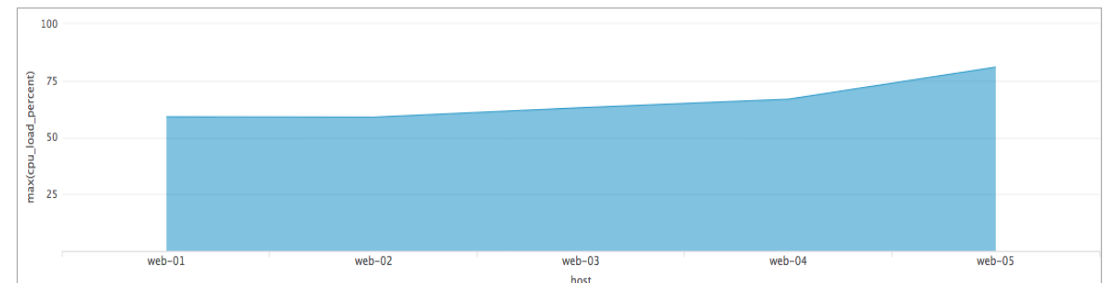
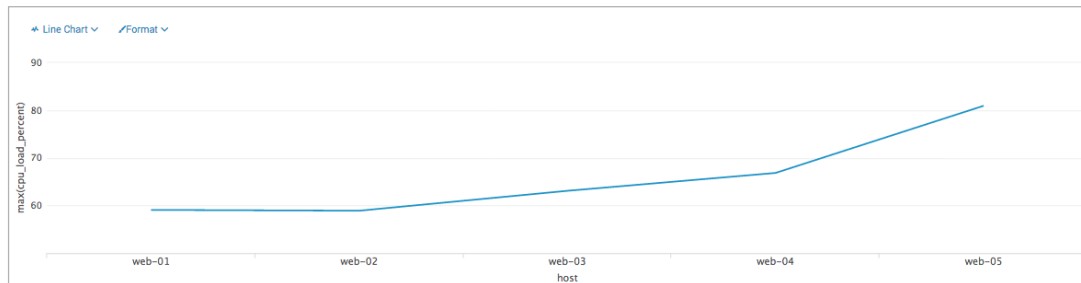
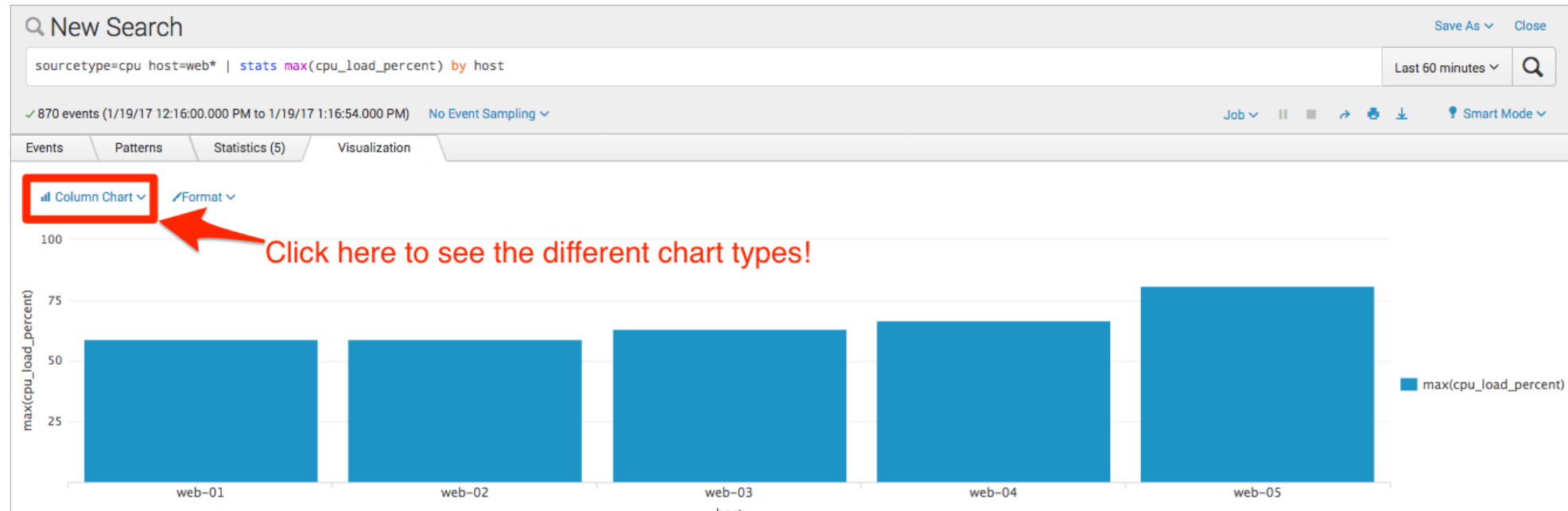
Some tips on how to proceed:

- What visualizations work well with this data?

If you're new to Splunk, click [HERE](#) for a more guided experience

**Click here!**

# Visualizations





# Reports

IT Operations

Click here! → Save As ▼ Close

Then here! → Report

Dashboard Panel

Alert

Event Type

Job ▼ || ▶ ↻ 🖨

Save As Report

Title

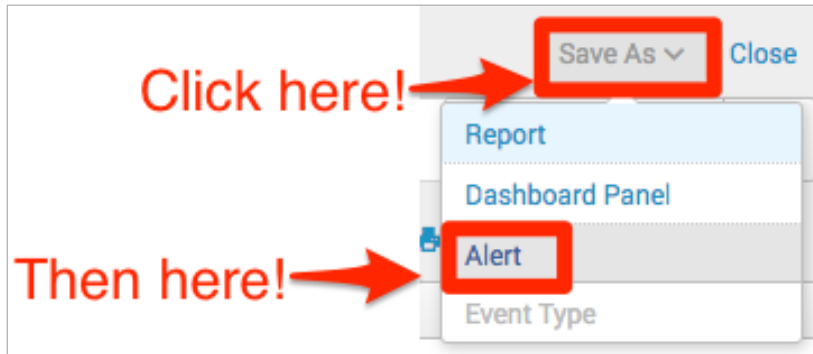
Description

Content

Time Range Picker

Cancel Save

# Alerts



Save As Alert

Settings

Title

Title

Description

Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run every week ▼

On

Monday ▼

at

6:00 ▼

Trigger Conditions

Trigger alert when

Number of Results ▼

is greater than ▼

0

Trigger

Once

For each result

Throttle?

Trigger Actions

+ Add Actions ▼

Cancel

Save

# Mobile App Issues

Click on **Troubleshooting Examples**,  
then *click* **IT Troubleshooting Basics**  
**3 – Mobile App Errors**



Line by Line

Pull Specific and Relevant Data

```
sourcetype=mint:network
```

[Load search to this point](#)



Click here!

# Raw Events

**New Search**

sourcetype=mint:network

✓ 428 events (1/19/17 12:41:00.000 PM to 1/19/17 1:41:12.000 PM) [No Event Sampling](#) ▾

Events (428) [Patterns](#) [Statistics](#) [Visualization](#)

[Format Timeline](#) ▾ [Zoom Out](#) [Zoom to Selection](#) [Deselect](#)

[List](#) ▾ [Format](#) ▾ [20 Per Page](#) ▾

		i	Time	Event
		>	1/19/17 1:39:40.000 PM	<pre>{ [-]   appVersionName: 5.8   carrier: Sprint   device: Kindle Fire HDX 8.9   extraData: {"jsessionId": "E8EEF7D1E352"}   latency: 357728   platform: android   remoteIP: 8.52.238.154   state: connected   statusCode: 200   timestamp: 1484861980   url: /orderstatus   userIdentifier: hmasonx   uuid: f1b09027-99a0-4922-8e74-37ce960c078c }</pre> <p><a href="#">Show as raw text</a></p> <p>host = splunk_sh-01   source = mint   sourcetype = mint:network</p>

< Hide Fields [All Fields](#)

Selected Fields

- host 1
- source 1
- sourcetype 1

Interesting Fields

- appVersionName 5
- carrier 4
- date\_hour 2
- date\_mday 1
- date\_minute 59
- date\_month 1
- date\_second 60

# Mobile App Problems

| chart count over appVersionName by statusCode

## Full Search Results

appVersionName	200	401
4.2	77	0
5.5	60	0
5.6	64	0
5.8	205	0
6.0	0	29

## Next Steps

Once you've identified the "bad" app version, try to change the search to find the impacted platform using the [search](#) app!

Some hints on how to proceed:

- What field in the MINT data might be helpful?

If you're new to Splunk, click [HERE](#) for a more guided experience

 Click here!

# Mobile App Issue Wrap Up

New Search Save As Close

sourcetype=mint:network | **chart** **count** **over** appVersionName **by** statusCode Last 60 minutes Q

✓ 427 events (1/19/17 1:13:00.000 PM to 1/19/17 2:13:08.000 PM) No Event Sampling Job || ■ → 🖨 ↓ Smart Mode

Events Patterns Statistics (5) Visualization

20 Per Page Format Preview

appVersionName	200	401
4.2	65	0
5.5	61	0
5.6	66	0
5.8	212	0
6.0	0	23

New Search Save As Close

sourcetype=mint:network | **chart** **count** **over** **platform** **by** statusCode Last 60 minutes Q

✓ 418 events (1/19/17 1:16:00.000 PM to 1/19/17 2:16:20.000 PM) No Event Sampling Job || ■ → 🖨 ↓ Smart Mode

Events Patterns Statistics (3) Visualization

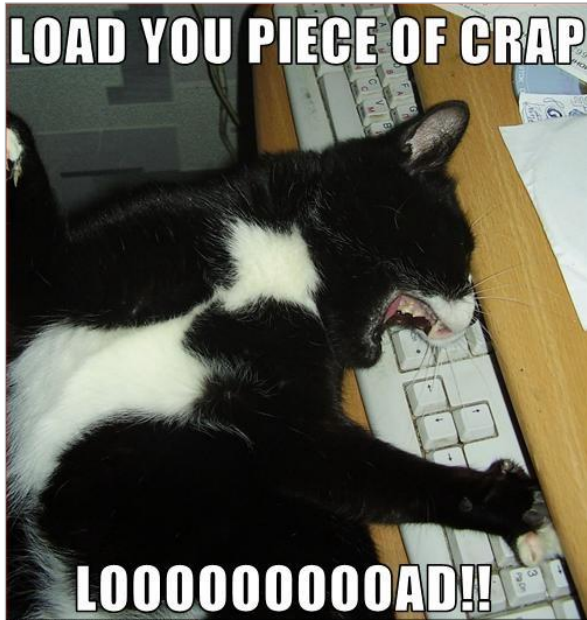
20 Per Page Format Preview

platform	200	401
WP	5	0
<b>android</b>	132	<b>22</b>
iOS	259	0



# Using APM Data

Click on **Troubleshooting Examples**, then *click* **IT Troubleshooting Basics 4 – Using APM Data**



## Line by Line

## Pull Specific and Relevant Data

```
sourcetype=newrelic_account
```

Load search to this point [🔗](#)

Click here!

# Raw Events

New Search

sourcetype=newrelic\_account

Last 60 minutes

855 events (3/6/17 12:39:00.000 PM to 3/6/17 1:39:53.000 PM) No Event Sampling

Events (855) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

Prev 1 2 3 4 5 6 7 8 9 ... Next

< Hide Fields All Fields

Selected Fields

- a host 1
- a source 2
- a sourcetype 1

Interesting Fields

- a eventtype 1
- a index 1
- # key\_transaction.application\_summary.apdex\_score 12
- # key\_transaction.application\_summary.apdex\_target 2
- # key\_transaction.application\_summary.error\_rate 9
- # key\_transaction.application\_summary.host\_count 6
- # key\_transaction.application\_summary.instance\_count 6
- # key\_transaction.application\_summary.response\_time 100+
- # key\_transaction.application\_summary

i	Time	Event
✓	3/6/17 1:39:30.000 PM	<pre>{ [-]   key_transaction: { [-]     application_summary: { [-]       apdex_score: 1.0       apdex_target: 0.3       error_rate: 0.0       host_count: 3       instance_count: 3       response_time: 0.19       throughput: 2     }     end_user_summary: { [-]       apdex_score: 0.94       apdex_target: 0.5       response_time: 0.22       throughput: 2     }     health_status: green     id: 19320     name: API Order Status     reporting: true     transaction_name: API Order Status   } }</pre>

Show as raw text

Event Actions

# APM Data

```
| stats latest(key_transaction.health_status) by key_transaction.name
```

## Full Search Results

key_transaction.name	latest(key_transaction.health_status)
API Add to Cart	green
API Checkout	orange
API Order Status	orange
API Product Details	orange
API Remove from Cart	green
API Update Cart	
API View Cart	
Authorization API	
Search API	
Web Add to Cart	

## Analyze the Data

```
| stats latest(key_transaction.health_status) by key_transaction.name
```

[Load search to this point](#)

**Click here!**

[illegible]



# Splunk Delivers on Top CIO Priorities

## Increasing Enterprise Growth

“Splunk is at the heart of CloudShare’s business. We use Splunk to get visibility into customer behavior and drive business growth.”

— **Elad Gotfrid**, Director of IT



## Delivering Business Solutions

“Splunk lets us quickly correlate and debug performance issues so we can track our critical SLAs in pre-production and double our velocity.”

— **Amit Sehgal**, Performance and Scalability Engineer



## Analytics and Business Intelligence

“Splunk delivered executive dashboards showing activations by minute, by channel, by market, by device type in hours—not weeks or months.”

— **Ty Prinkki**, Senior Operations Manager



## Improving Customer Experience

“Splunk tracks any interference with customer experience on our website and proactively finds underperforming components.”

— **Jon Abend**, Senior Manager of Enterprise Architecture





# Dramatic Results, Rapid ROI



**90% Reduction in Time  
to Track Deliveries**



**200% ROI  
Usage Analytics**



**200% ROI  
Better Customer Experience**



**MTTR (-70%)  
Tools Consolidation**



# Now What?

Feel free to keep working with the data from your USB key

splunk>enterprise

---

Full-featured platform for real-time Operational Intelligence  
Download **Splunk Enterprise** for free at [www.splunk.com/download](http://www.splunk.com/download)

---

splunk>cloud

---

Splunk Enterprise as a cloud service  
Try **Splunk Cloud** with a free trial at [www.splunk.com/cloud](http://www.splunk.com/cloud)

---

splunk>

---

Learn more about **Splunk quick start bundles** at  
[www.splunk.com/bundles](http://www.splunk.com/bundles)

---

splunk>live!

# Workshops: Get Splunk Hands-on Experience

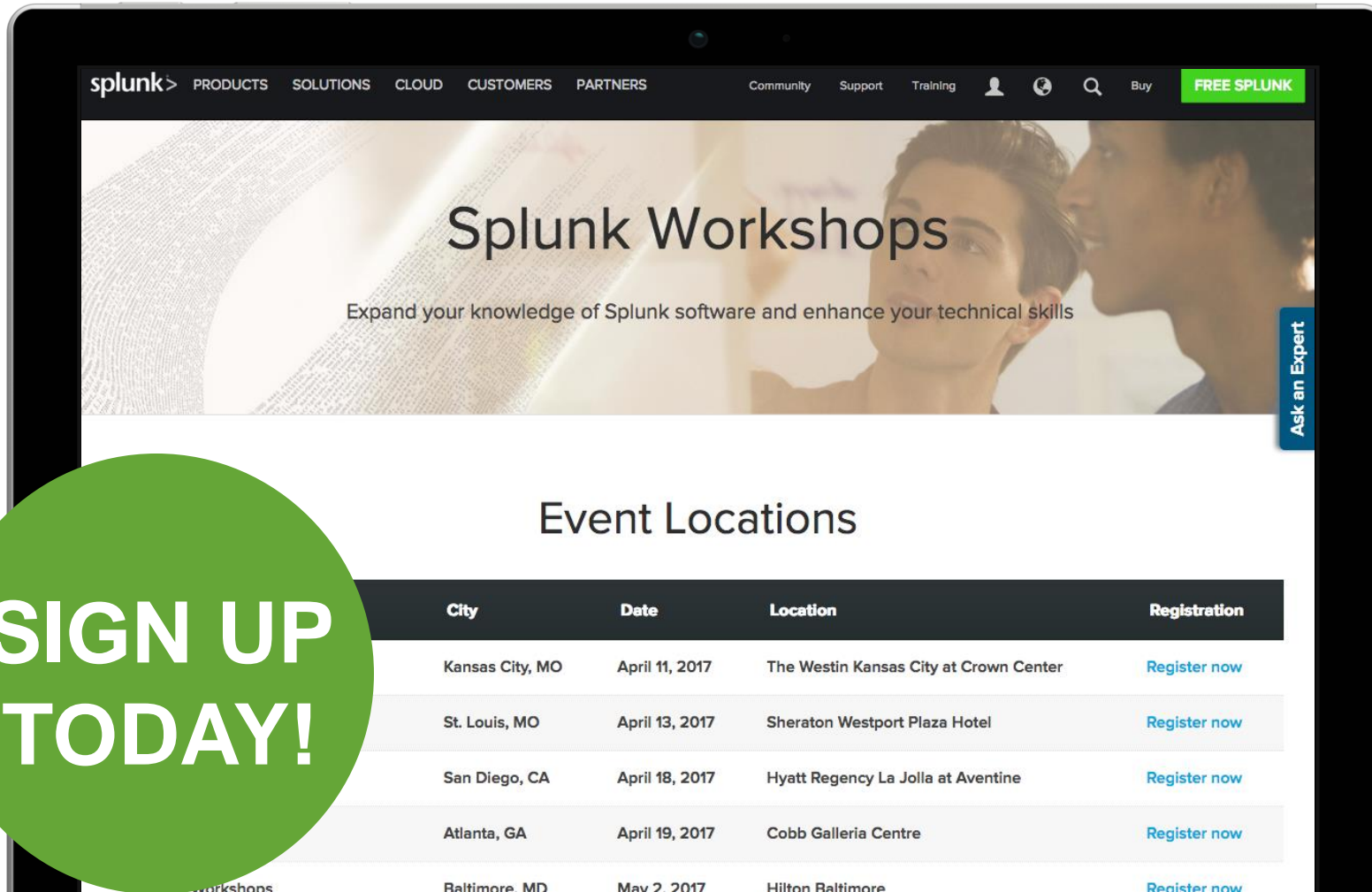
Attend a Splunk Workshop

[splunk.com/workshops](https://splunk.com/workshops)

## June 14: Minneapolis

- ▶ **Venue:** Hyatt Regency Minneapolis
- ▶ **Time:** 8:30am
- ▶ Register Soon!
  - [splunk.com/workshops](https://splunk.com/workshops)

**SIGN UP  
TODAY!**



### Event Locations

City	Date	Location	Registration
Kansas City, MO	April 11, 2017	The Westin Kansas City at Crown Center	<a href="#">Register now</a>
St. Louis, MO	April 13, 2017	Sheraton Westport Plaza Hotel	<a href="#">Register now</a>
San Diego, CA	April 18, 2017	Hyatt Regency La Jolla at Aventine	<a href="#">Register now</a>
Atlanta, GA	April 19, 2017	Cobb Galleria Centre	<a href="#">Register now</a>
Baltimore, MD	May 2, 2017	Hilton Baltimore	<a href="#">Register now</a>

**.conf2017**

The 8<sup>th</sup> Annual Splunk Conference

**SEPT 25-28, 2017**

Walter E. Washington Convention Center  
Washington, D.C.

**SAVE OVER \$450**

You will receive an email after registration opens with a link to save over \$450 on the full conference rate.

You'll have 30 days to take advantage of this special promotional rate!

**conf.splunk.com**

**splunk > live!**

## A stylized, symmetrical face with a wide, toothy grin, large eyes, and a central vertical line, resembling a mask or a stylized animal head. The face is composed of thick black outlines on a white background. It has a large, open mouth showing two rows of teeth. The eyes are large and almond-shaped, with a single dot in each. A thick vertical line runs down the center of the face, separating the two sides. The top of the head is rounded with small, pointed ears on either side.



Complete the survey for  
your chance to win a  
.conf2017 pass



# THANK YOU