

Splunk4Industry: Financial Services Industry

Workshop

X #Splunk4Industry

splunk>



Forward-Looking Statements



This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk, Splunk> and Turn Data Into Doing 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. © 2023 Splunk Inc. All rights reserved.

Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?



Workshop Agenda

- Building Digital Resilience with Splunk
- Splunk in the Financial Services Industry
- Labs 1-6:
 - Onboarding data
 - Exploring the data / gaining insights
- Demo: Splunkbase + Essentials App
- Lab 7:
 - Exploring FSI use cases
- Demo: Service Intelligence - Payments
- Labs 8-10:
 - Intro to Service Monitoring
 - Expanding Visibility
 - Build Your Own!



There's a lot more to Splunk

- Clustering
- Data Models
- Alerting
- Pivot
- SDKs
- APIs
- DB Connect

- Advanced Searches
- SOAR
- Machine Learning (ML)

- Splunk Stream
- Deployment Server
- Federated Search
- Metrics

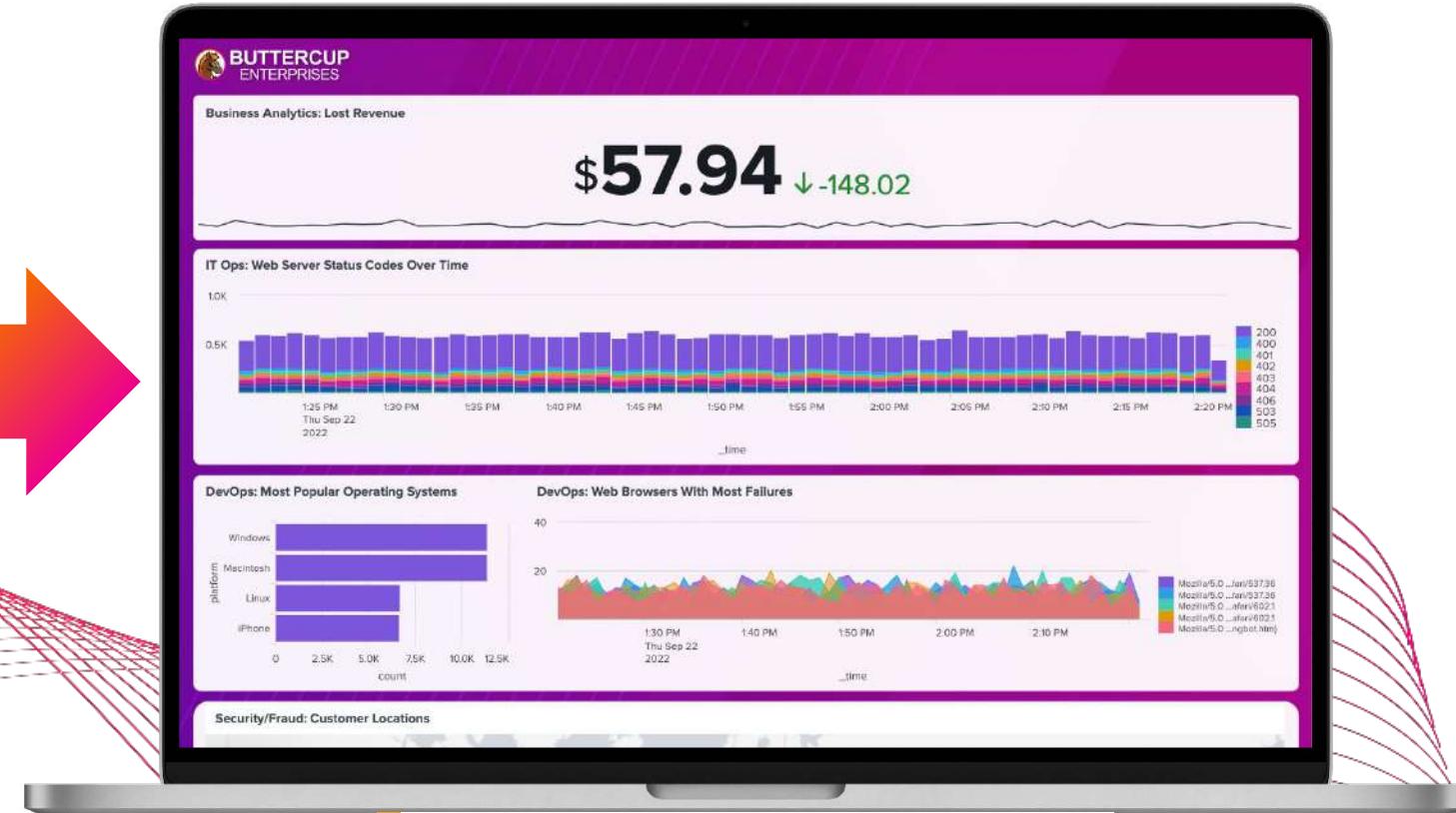
- Custom Visualisations
- HTTP Event Collector (HEC)
- Data Filtering
- Transformations
- Architecture

- Report Acceleration
- Common Information Model (CIM)
- Containers
- Best Practices
- And much more...

Objective for Today: Pt1



Go from messy machine data...

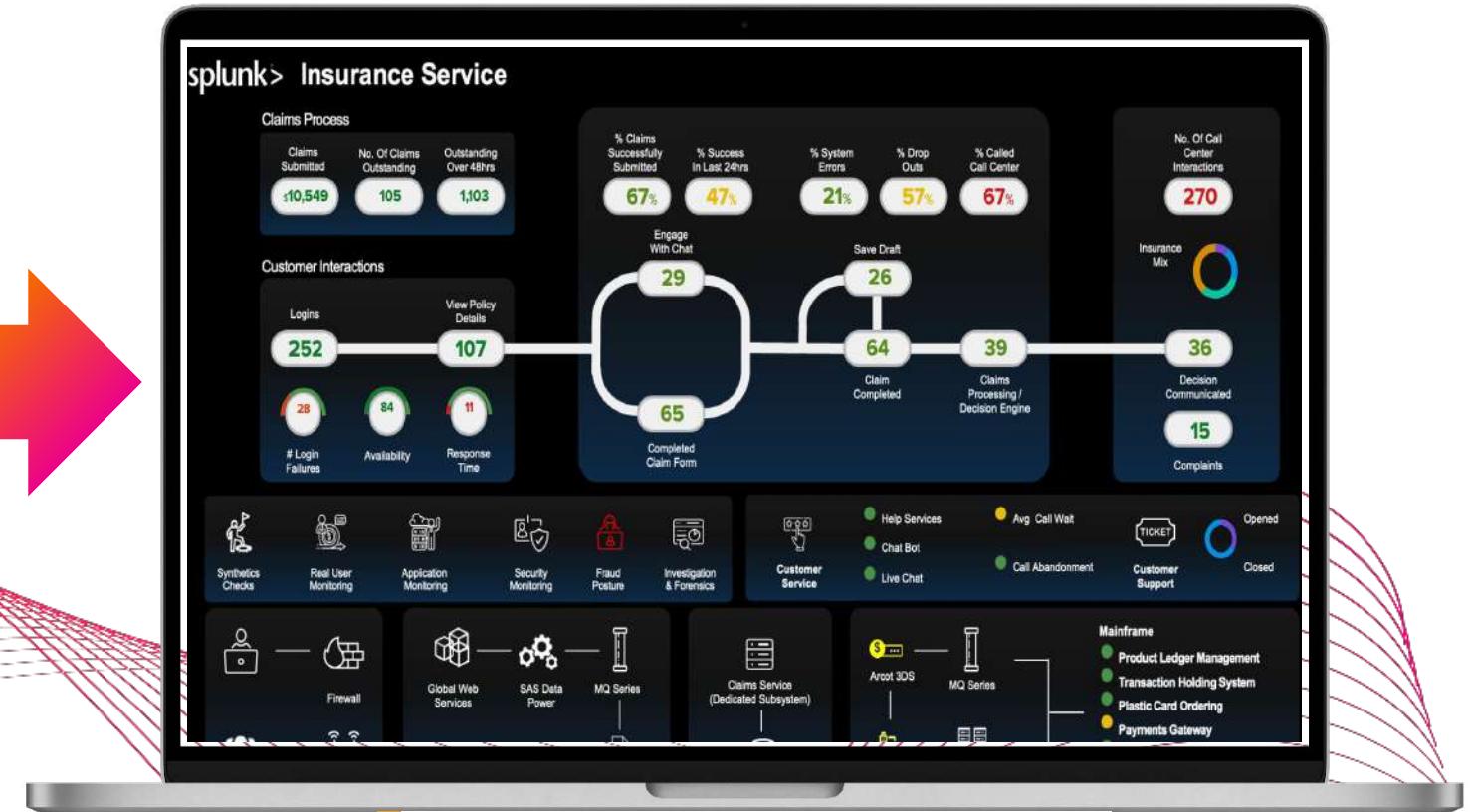


...to a dynamic, interactive dashboard!

Objectives for Today: Pt2



How does IT align to the Business?



...to holistic view of services



Obtain the Materials for Today's Workshop

Tasks

1. Get your instance details from your host
2. Download the hands-on lab guide:
<https://splk.it/FSI-Lab-Guide>
Contains step-by-step instructions
for all of today's exercises!
3. Download a copy of today's slide deck:
<https://splk.it/FSI-Attendee>

Goal

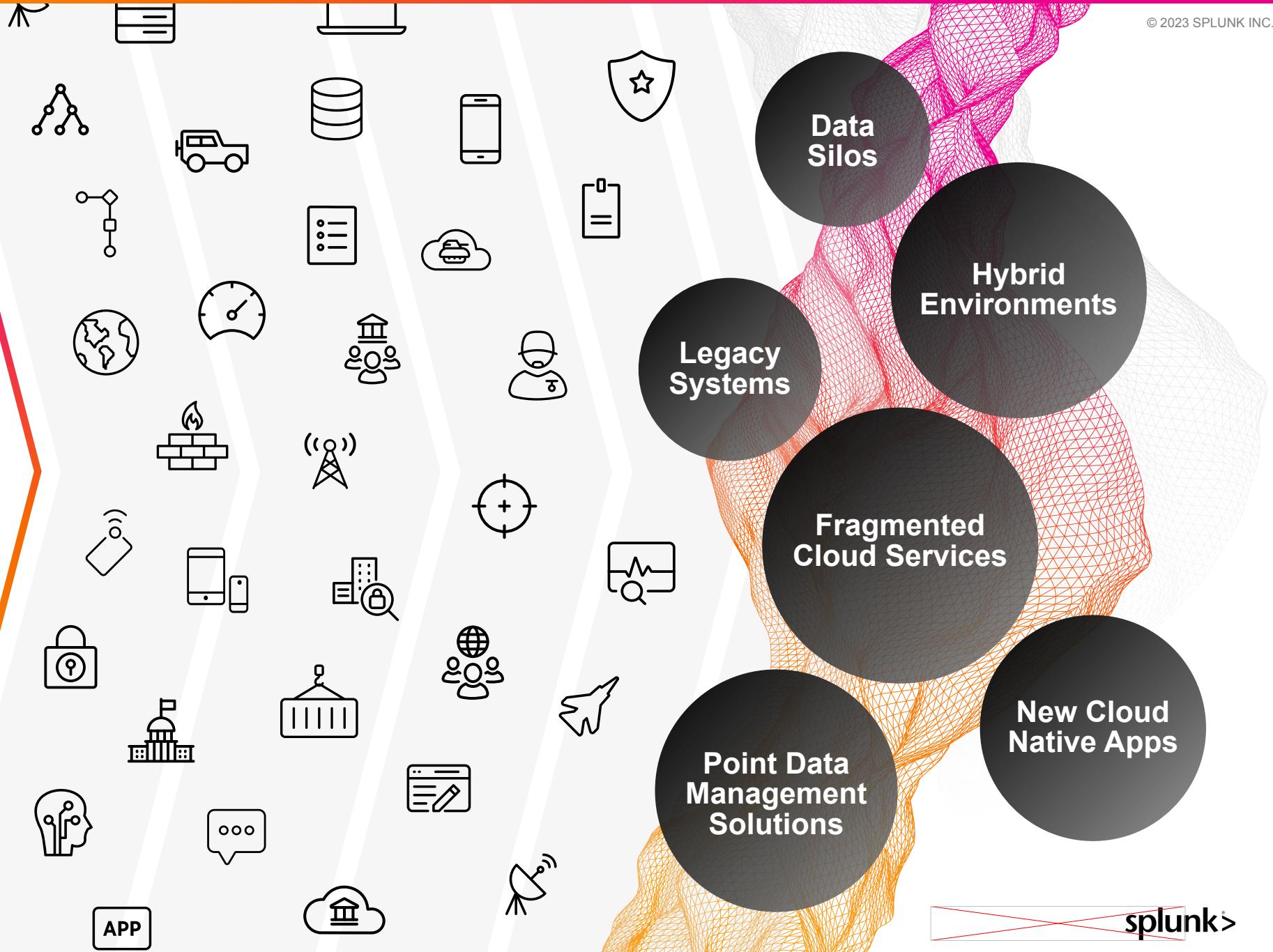
adminUsername	adminPassword	url
admin	changeme	https://i-07701533c62d97ab5.splunk.show
admin	changeme	https://i-01527c2526e8e3719.splunk.show
admin	changeme	https://i-0802422ed1f20c671.splunk.show
admin	changeme	https://i-0ef3ac2950177bc26.splunk.show
admin	changeme	https://i-03475a6ebca7d779d.splunk.show

Put your name against one
of the instances in the list

Data is your Competitive Advantage

Data isn't just a record.
Data makes things happen.
Splunk makes it possible.

Turning Real-time Data Into Action is Hard



The Power of Splunk

Delivering Unified Security and Observability

See

End-to-end visibility

No sampling or blind spots

Act

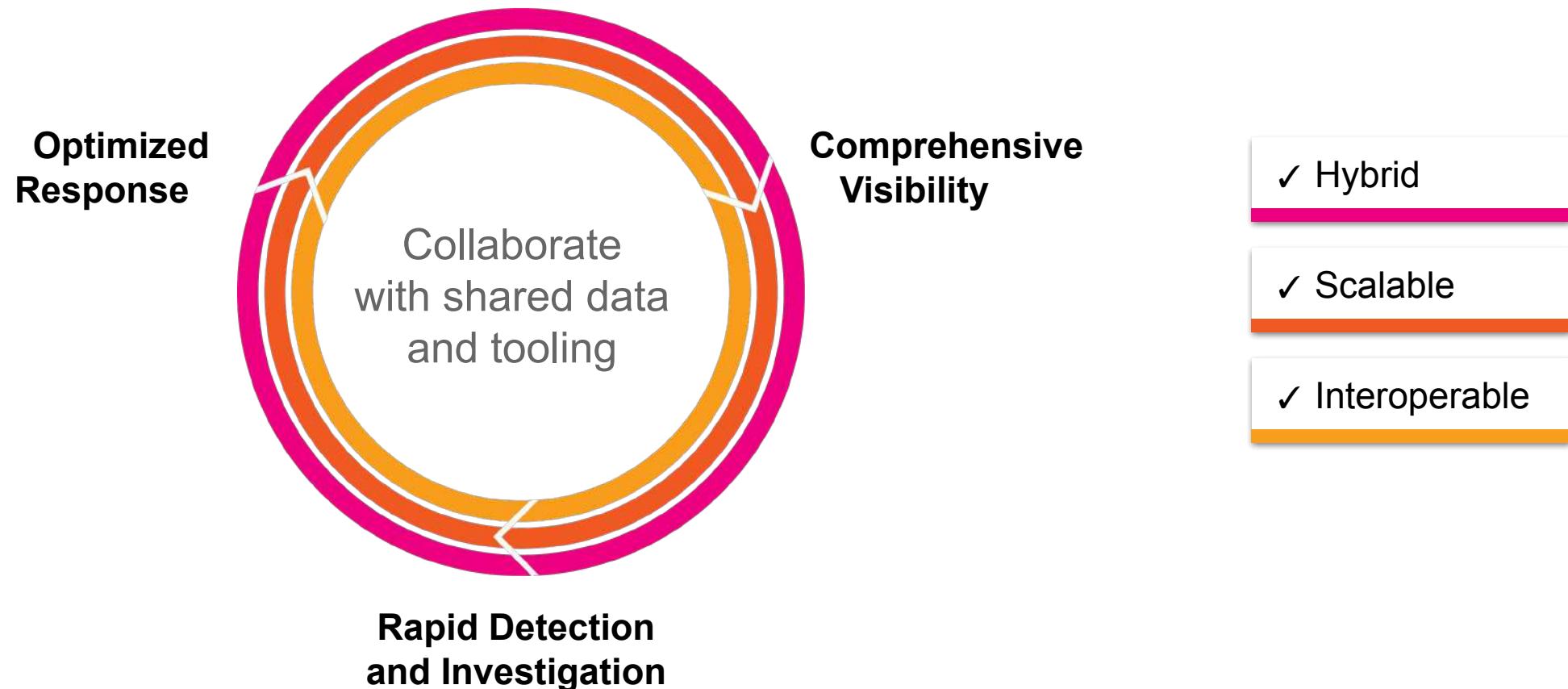
Investigate across massive data sets and take **action** fast

Extend

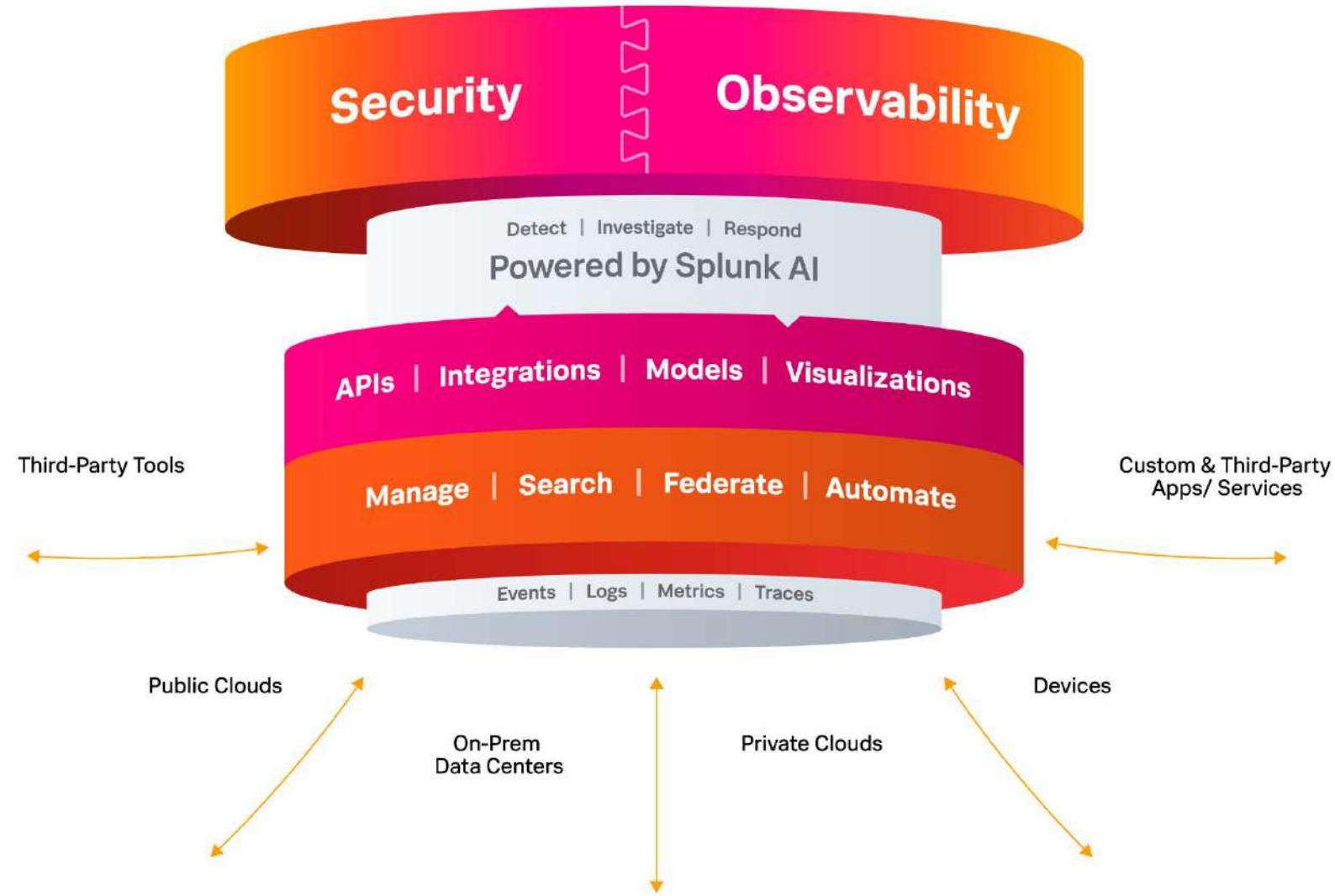
Extend the **platform** to use data to solve problems across the business



Splunk enables faster detection, investigation and response



The Unified Security and Observability Platform

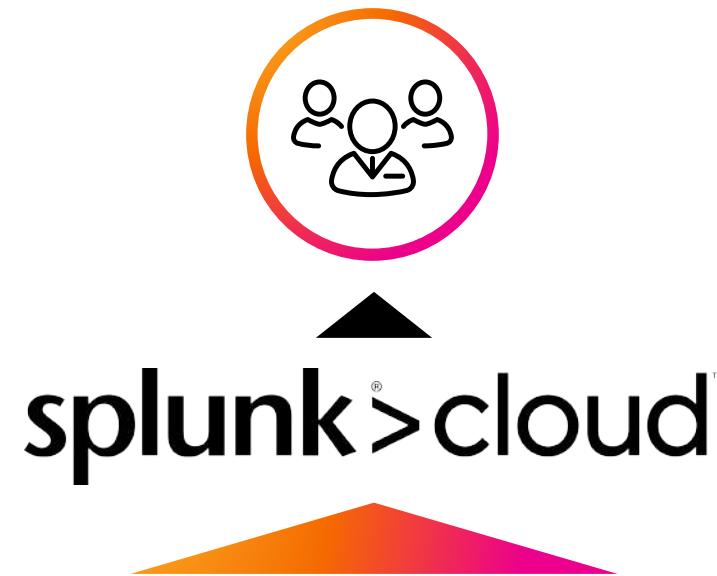


Splunk as a Service

Fastest time to value | Minimum Infrastructure | Maximum Value

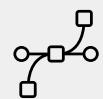
3 Simple Steps

1. Onboard data
2. Onboard users
3. Get value from your data



- **Fastest time to value**
- **Software as a service** - AWS or GCP
- **Secure** - ISO 27001, SOC 2 Type II, PCI DSS, HIPAA, FedRAMP Moderate, DoD IL5, IRAP
- **Encryption-in-transit** - plus optional encryption-at-rest
- **Resilient infrastructure**
- **100% uptime guarantee**
- **24/7 NOC/SOC support team**

Flexible options for data collection and forwarding



Wire Data



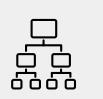
API



SDKs



HEC



TCP/UDP



RDBMS



Containers



Apps



Cloud Services



OpenTelemetry

Splunk
Forwarders

Splunk Cloud Service Description: <https://splk.it/SplunkCloudServDesc>

splunk>

What is a Splunk Universal Forwarder?

- Reliable collection of data from remote locations
- Includes methods for collecting from a variety of data sources
- Lightweight but powerful:
 - Buffering / guaranteed delivery
 - Encryption
 - Compression
 - Load balancing
 - And more!
- Very small footprint
- Just forwards data – no parsing beforehand!

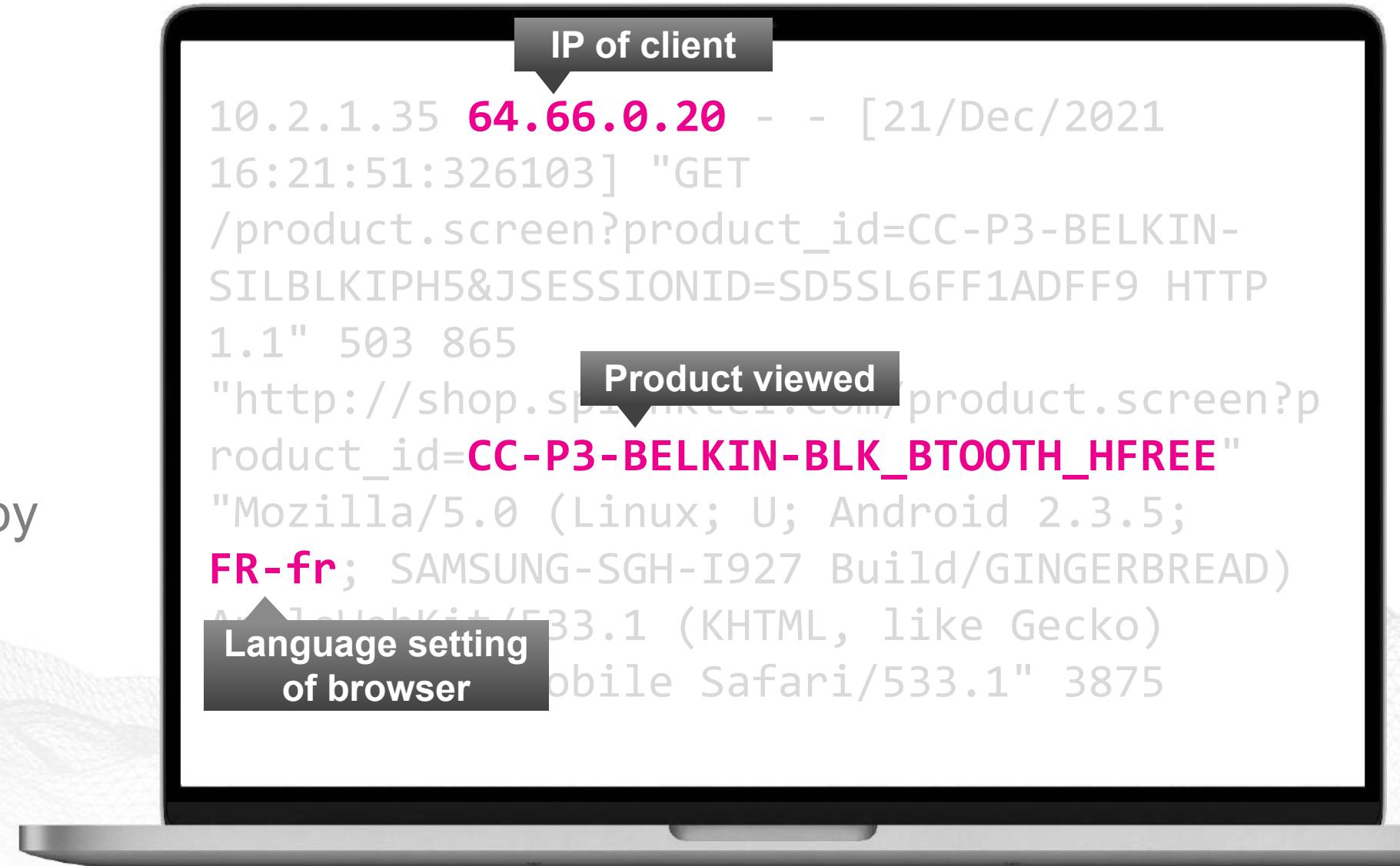


**Machine data
is valuable
not complex!**

```
10.2.1.35 64.66.0.20 - - [21/Dec/2021  
16:21:51:326103] "GET  
/product.screen?product_id=CC-P3-BELKIN-  
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP  
1.1" 503 865  
"http://shop.splunktel.com/product.screen?p  
roduct_id=CC-P3-BELKIN-BLK_BT0OTH_HFREE"  
"Mozilla/5.0 (Linux; U; Android 2.3.5;  
FR-fr; SAMSUNG-SGH-I927 Build/GINGERBREAD)  
AppleWebKit/533.1 (KHTML, like Gecko)  
Version/4.0 Mobile Safari/533.1" 3875
```

Marketing Use Case

Show the top
products viewed by
language



DevOps Use Case

Which mobile handsets should I test the most before releasing my new app?

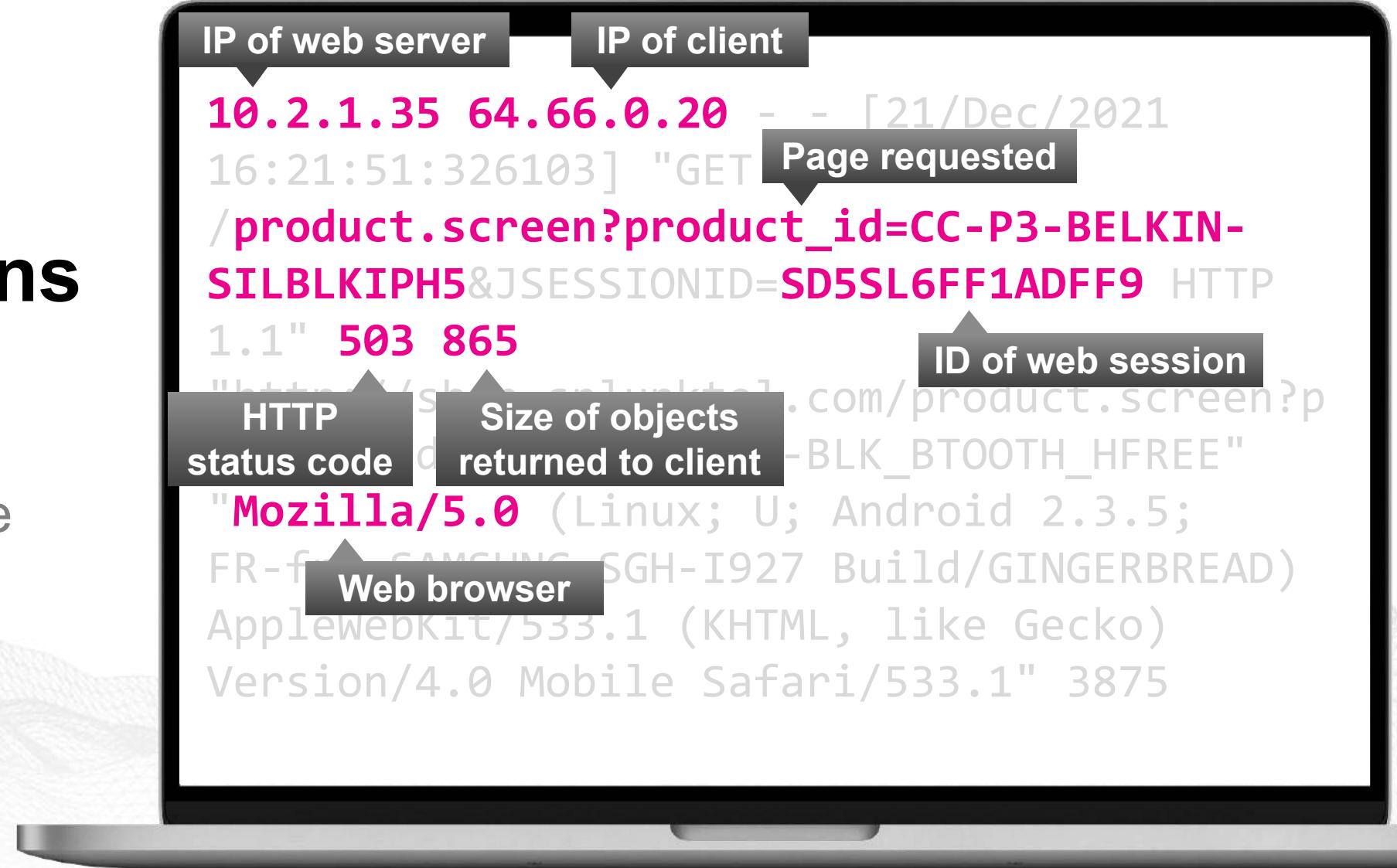
```
10.2.1.35 64.66.0.20 - - [21/Dec/2021  
16:21:51:326103] "GET  
/product.screen?product_id=CC-P3-BELKIN-  
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP  
1.1" 503 865  
"http://shop.splunktel.com/product.screen?p  
roduct_id=CC-P3-BELKIN-BLK_BRIGHT_FREE"  
Mozilla/5.0 (Linux; U; Android 2.3.5;  
FR-fr; SAMSUNG-SGH-I927 Build/GINGERBREAD)  
AppleWebKit/533.1 (KHTML, like Gecko)  
Version/4.0 Mobile Safari/533.1" 3875
```

Platform

Handset model

IT Operations Use Case

Which web pages
are generating the
most errors?



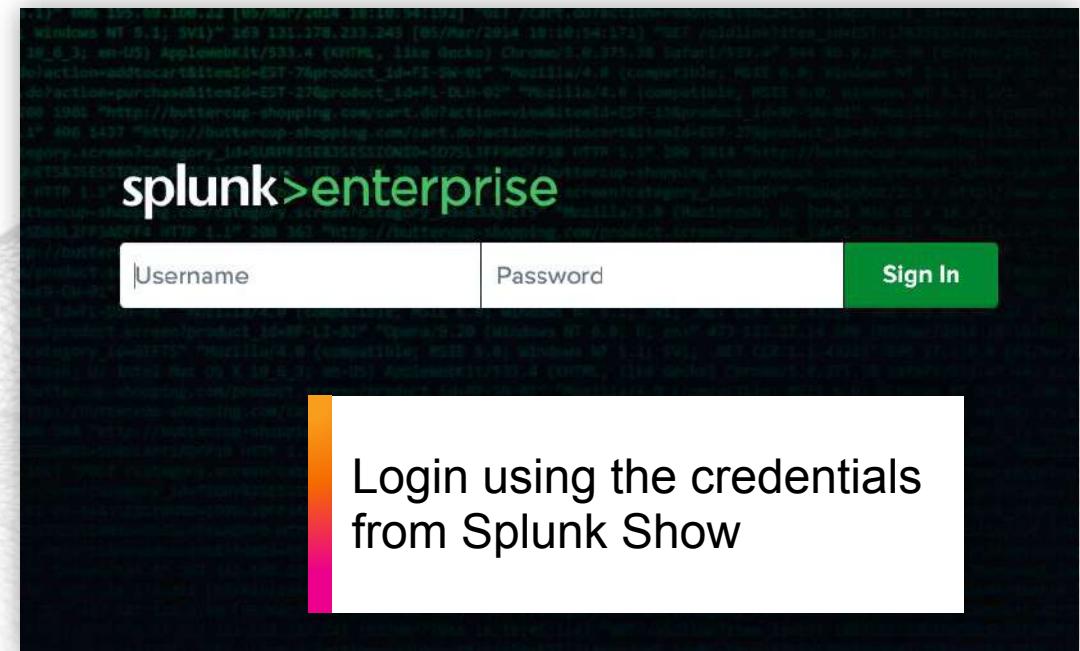
Login to Splunk

Locate your instance URL and credentials
in the list provided

adminUsername	adminPassword	url
admin	<password>	https://i-07701533c62d97ab6.splunk.show
admin	<password>	https://i-01527c2526e8e3712.splunk.show
admin	<password>	https://i-0802422ed1f20c670.splunk.show
admin	<password>	https://i-0ef3ac2950177bc25.splunk.show
admin	<password>	https://i-03475a6ebca7d779e.splunk.show

Locate your instance URL
in the list provided - make sure
you use the one with your
name next to it!

Log in to your Splunk instance



Login using the credentials
from Splunk Show



Create an App and Add Some Data

Tasks

1. Create a new app
2. Monitor a directory: `/var/log/weblogs`
3. Select a source type: `access_combined`
4. View your data in Splunk

Select source

- var
- backups
- cache
- crash
- lib
- local
- lock
- log
 - apt
 - audit
 - dist-upgrade
 - fsck
 - landscape
 - squid3
 - unattended-upgrades
 - upstart
 - weblogs
- alternatives.log

Reminder
Download the [lab guide](#) for step-by-step instructions!

Open your app and have a play!

The currently selected app

Search bar – type anything here to search

Event histogram

Event timestamp

Raw event data

Metadata fields extracted at search time

The screenshot shows the Splunk Enterprise interface. At the top, it displays the selected app as "Splunk 4 Rookies". Below the header, there's a "New Search" bar containing the query "action=purchase status=200". To the right of the search bar is a "Time picker" set to "Last 60 minutes". The main search results are shown in a table under the "Events (261)" tab. The first event listed is from "flowershop.com" with timestamp "15/05/2018 08:49:08.127". The table includes columns for Time, Event, and source. A sidebar on the left lists "INTERESTING FIELDS" such as action, bytes, category_id, clientip, date_hour, date_mday, date_minute, date_month, and date_second. The bottom right corner features the Splunk logo.

Time	Event
15/05/2018 08:49:08.127	12.130.60.5 - - [15/May/2018 08:49:08:127] "GET /cart.do?action=purchase&itemId=EST-20&product_id=RP-SN-01&JSESSIONID=SD1SL2FF10 flowershop.com/category.screen?category_id=GIFTS" "Googlebot/2.1 (http://www.googlebot.com/bot.html) " 873 host = ip-172-31-31-62 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined
15/05/2018 08:48:54.193	12.130.60.4 - - [15/May/2018 08:48:54:193] "POST /product.screen?product_id=FL-DLH-02&JSESSIONID=SD7SSL2FF3ADFF8 HTTP/1.1" 200 629 "http://www.myflowershop.com/cart.do? action=purchase&itemId=EST-20&product_id=FL-DLH-02" "Googlebot/2.1 (http://www.googlebot.com/bot.html) " 256 host = ip-172-31-31-62 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined
15/05/2018 08:48:46.196	203.92.58.136 - - [15/May/2018 08:48:46:196] "GET /cart.do?action=purchase&itemId=EST-15&product_id=K9-BD-01&JSESSIONID=SD1SL10FF1ADFF7 HTTP/1.1" 200 3031 "http://www. myflowershop.com/category.screen?category_id=BOUQUETS" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safari/533.4" 897 g/weblogs/noise_apache_1.log sourcetype = access_combined

Start Exploring Your Data

Example searches

503 purchase

Find all events that contain the words “503” and “purchase”

503 pur*

Find all events containing “503” and words beginning with “pur”

503 (purchase OR addtocart)

Boolean operators (AND/OR/NOT) – must be UPPERCASE!

status=503 action=purchase

Use *fieldname = value* to ensure accurate search results

How would you find events with a status code of 200 that are NOT purchase events?

status=200 **NOT** action=purchase

status=200 action!=purchase

Splunk's Search Processing Language (SPL)

Search Terms

Commands

index=main action=purchase | stats count by status | rename count as "number of events"

Pipe character: Output
of left is input to right

e.g. index=main action=purchase

Time	Event
15/09/2022 09:12:53.163	12.130.60.5 - - [15/Sep/2022 09:12:53:163] "GET /product.screen?product_id=MGB-5&JSESSIONID=\$D4SL3F18ADFF4 HTTP/1.1" 401 3810 "http://www.buttercupenterprises.com/cart.do?action=purchase&itemId=EST-27&product_id=MGB-5" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36" 299
	host = ip-172-31-39-95 source = /var/log/weblogs/noise_apache_2.log sourcetype = access_combined
15/09/2022 09:12:48.184	128.241.220.82 - - [15/Sep/2022 09:12:48:184] "GET /cart.do?action=purchase&itemId=EST-21&product_id=ZSG-2&JSESSIONID=\$D4SL5FF3A0FF10 HTTP/1.1" 404 2946 "http://www.buttercupenterprises.com/product.screen?product_id=ZSG-2" "Mozilla/5.0 (iPhone; CPU iPhone OS 7_0 like Mac OS X) AppleWebKit/537.51.1 Version/7.0 Mobile/11A465 Safari/9537.53 BingPreview/1.0b" 661
	host = ip-172-31-39-95 source = /var/log/weblogs/noise_apache_3.log sourcetype = access_combined
15/09/2022 09:12:42.194	141.146.8.66 - - [15/Sep/2022 09:12:42:194] "POST /cart.do?action=purchase&itemId=EST-19&product_id=MGB-8&JSESSIONID=\$D3SL4FF18ADFF8 HTTP/1.1" 505 3349 "http://www.buttercupenterprises.com/cart.do?action=purchase&itemId=EST-19&product_id=MGB-8" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_1) AppleWebKit/537.36 Chrome/56.0.2914.3 Safari/537.36 OPR/45.0.2431.8 (Edition developer)" 891
	host = ip-172-31-39-95 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined
15/09/2022 09:12:42.176	281.3.128.132 - - [15/Sep/2022 09:12:42:176] "POST /cart.do?action=purchase&itemId=EST-16&product_id=MCF-3&JSESSIONID=\$D3SL7FF3A0FF3 HTTP/1.1" 200 3542 "http://www.buttercupenterprises.com/product.screen?product_id=MCF-3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_1) AppleWebKit/537.36 Chrome/57.0.2959.8 Safari/537.36" 236

Functions

| stats count by status | rename count as "number of events"

status	count
200	850
400	81
401	76
402	50
403	57

status	number of events
200	850
400	81
401	76
402	50
403	57

Want to know more? Check out:

Splunk Quick Reference Guide: <https://splk.it/SplunkQuickRef>

Search manual: <https://splk.it/SplunkSearchManual>

Splunk in FSI

Charles Adriaenssens: FinServ Industry Specialist



Today's Intro Scenario | Buttercup Enterprises

Your Company

- Buttercup Enterprises is a large national online retailer operating in the US, which sells a variety of books, clothing and other gifts through its online webstore
- Buttercup Enterprises have recently invested in Splunk and now they want to start making use of it across the business

Your Role

- You are one of the chosen few: a Splunk power user!
- Your responsibility is to provide insights to users throughout the company
- The teams you support include:
 - **IT Operations**
 - **DevOps**
 - **Business Analytics [Splunk4Rookies only]**
 - **Security/Fraud**



What Does the Business Want to See?

We Need to Create a Dashboard With Four Views



IT Operations team: Investigate successful vs unsuccessful web server requests over time



DevOps team: Show the most common customer operating systems and which web browsers are experiencing the most failures



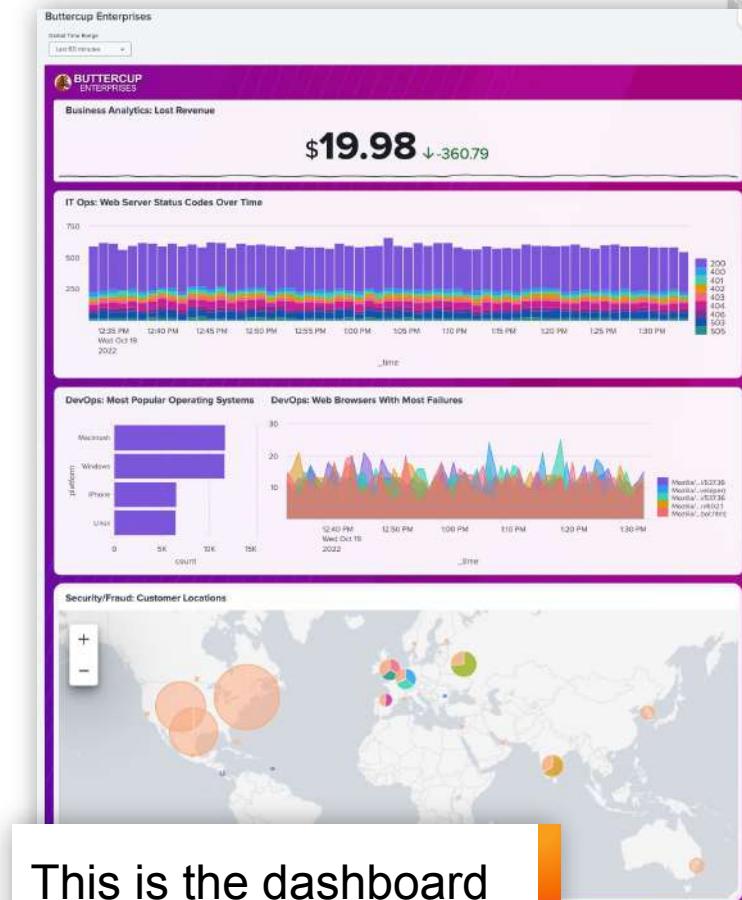
Business Analytics team: Show lost revenue from the Buttercup Enterprises website



Security/Fraud team: Show website activity by geographic location



Buttercup Enterprises: Add all of this to a single dashboard with a custom background image



This is the dashboard we're aiming for!



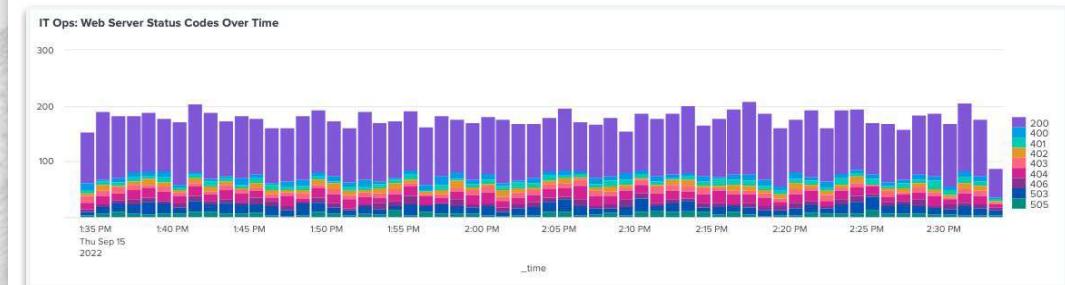
IT Operations Team

Investigate Successful Versus Unsuccessful Web Server Requests Over Time

Tasks

1. Show successful vs unsuccessful web server requests over time
2. Use a stacked column chart visualisation
3. Add your chart to a new dashboard
4. Choose ‘Dashboard Studio’ and use ‘Absolute’ layout mode to allow for future dashboard customisation!

Goal



Splunk Dashboards

Classic Dashboards (Simple XML)



- Easy to deploy a **wide variety of visualisations**, but **hard to craft a story**
- **Flexible and extensible**, but **time consuming** to build something truly beautiful (e.g. custom JS, CSS)
- **PDF export loses look/feel** of dashboard

Dashboard Studio



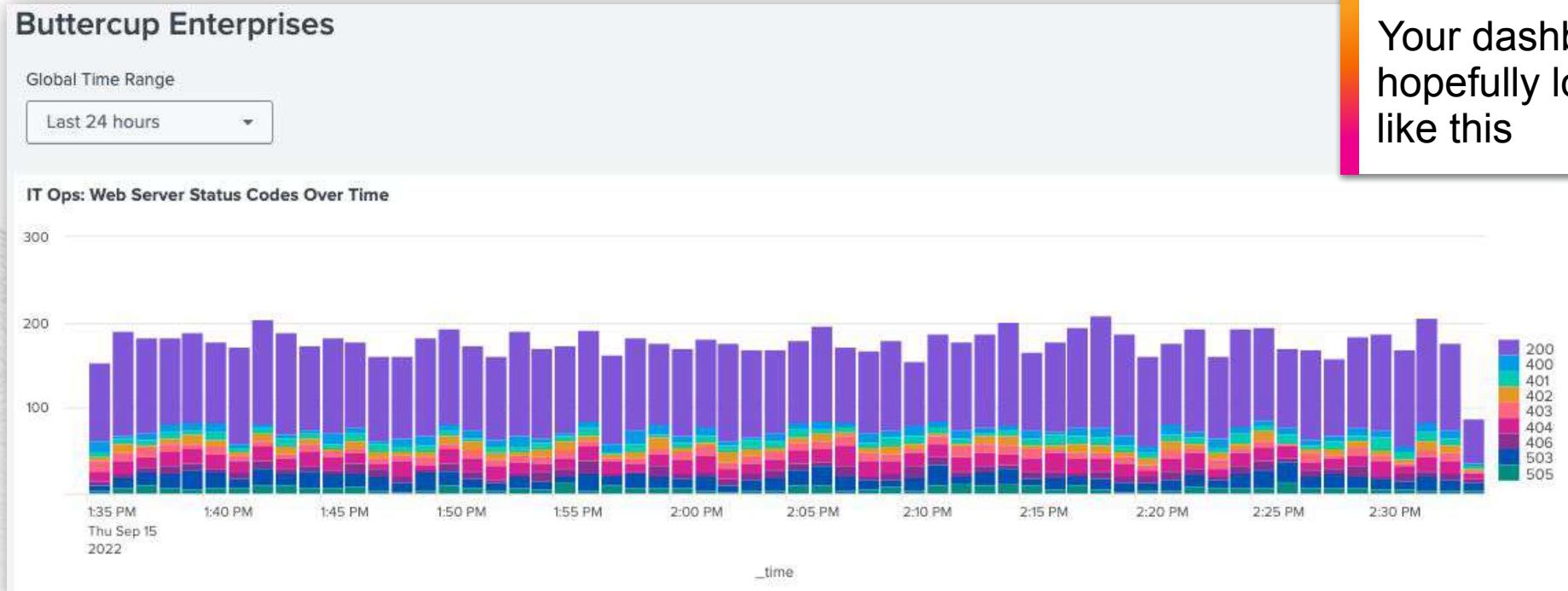
- Create **powerful, story-telling dashboards** with **advanced visualisation tools**
- **Streamlined editing experience** with **flexible layouts**
- Support for **images, text boxes, shapes, lines** and **icons**, with **intact PDF export**
- **No custom code required**



Your Dashboard So Far

Solution

```
index=main sourcetype=access_combined | timechart count by status limit=10
```



Your dashboard should hopefully look something like this

DevOps Team

Show the Most Common Customer Operating Systems and Which Web Browsers are Experiencing the Most Failures

Step 1: Show the most common customer operating systems

The screenshot shows a Splunk search interface. The search bar contains the query `index=main sourcetype=access_combined`. The results table has columns for i (Info icon), Time, and Event. One event row is highlighted, showing a timestamp of 03/04/2023 15:10:51.000 and an event details pane. The event details pane shows the host as 1.19.11.11, the source as ADFF9, the protocol as HTTP/1.1, the status code as 200, the response length as 1474, the URL as "http://www.buttercupenterprises.com/product.screen?product_id=MCF-3", the user agent as "Mozilla/5.0 Macintosh Intel Mac OS X 10_12_2 AppleWebKit/537.36 Chrome/54.0.2840.98 Safari/537.36", and the session ID as SD2SL10FF10. A callout box points to the operating system information in the event details pane with the text: "We can see operating system information in our events but we don't currently have a field we can use to report on".

i	Time	Event
>	03/04/2023 15:10:51.000	1.19.11.11 -- [03/Apr/2023 15:10:51] "GET /cart.do?action=purchase&product_id=ZSG-2&JSESSIONID=SD2SL10FF10 ADFF9 HTTP/1.1" 200 1474 "http://www.buttercupenterprises.com/product.screen?product_id=MCF-3" "Mozilla/5.0 Macintosh Intel Mac OS X 10_12_2 AppleWebKit/537.36 Chrome/54.0.2840.98 Safari/537.36" 313 host = Domain sourcetype =

We can see operating system information in our events but we don't currently have a field we can use to report on



Extracting a New Field

1. Click on the arrow to expand an event

Time Event
03/04/2023 1.19.11.11 - -
15:10:51.000 ADFF9 HTTP 1.1
(Macintosh; In
Event Actions ▾
Build Event Type
Extract Fields

2. Click on Event Actions

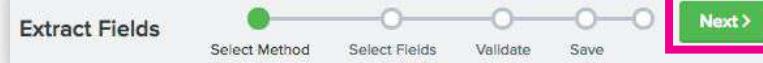
3. Click on Extract Fields

(.*?)

Regular Expression

Splunk Enterprise will extract fields using
a Regular Expression.

4. Click on Regular Expression



5. Click Next

Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

89.167.143.32 - - [04/Apr/2023:15:10:51-0700] "GET / HTTP/1.1" 200 12345
6&JSESSIONID=SD8SL4FF2ADFAE8C
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 OPR/43.0.2431.0
Extract
Field Name platform
Sample Value Macintosh
Add Extraction

6. Highlight the part of the event that is of interest

7. Give the new field a name, lowercase is recommended



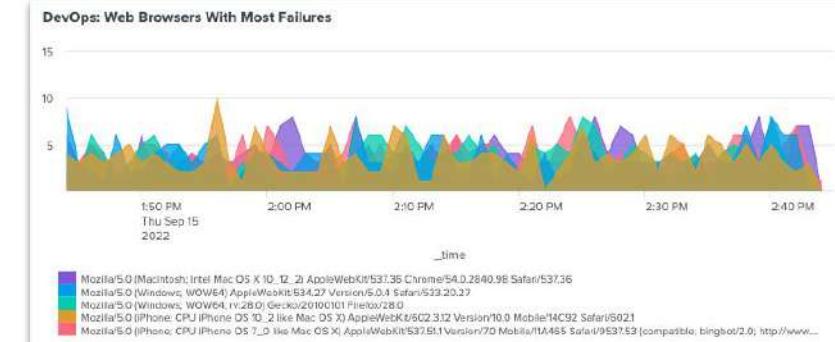
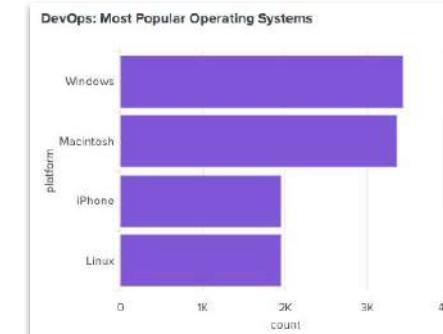
DevOps Team

Show the most common customer operating systems and which web browsers are experiencing the most failures

Tasks

1. Extract a new **platform** field
2. Show the top values using a bar chart visualisation
3. Create an area chart showing the top 5 web browsers that are experiencing the most failures over time
4. Add your charts to your existing dashboard

Goal



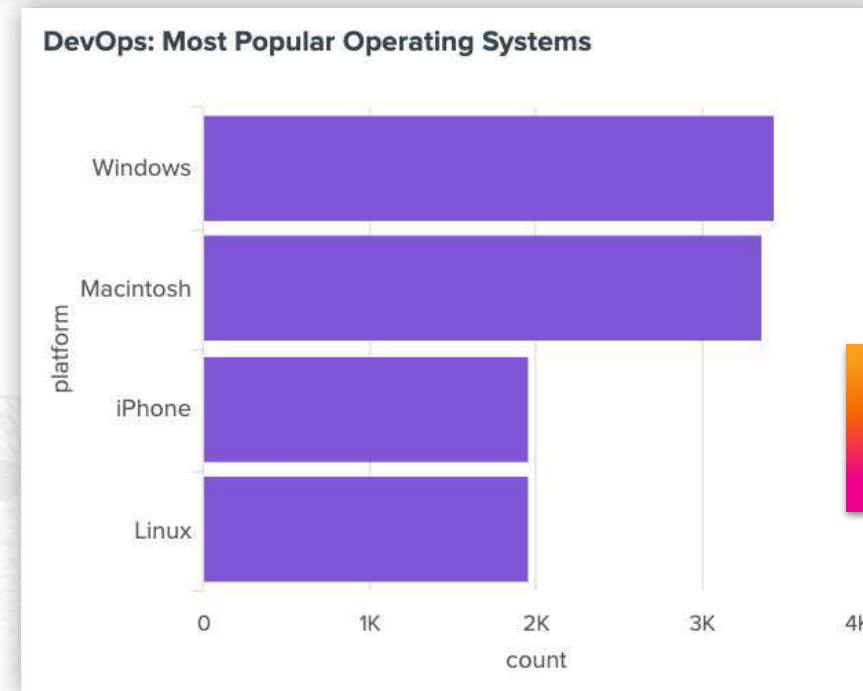


DevOps Team

Show The Most Common Customer Operating Systems

Solution

```
index=main sourcetype=access_combined | top limit=20 platform showperc=f
```



When you're happy with your chart add it to your dashboard!

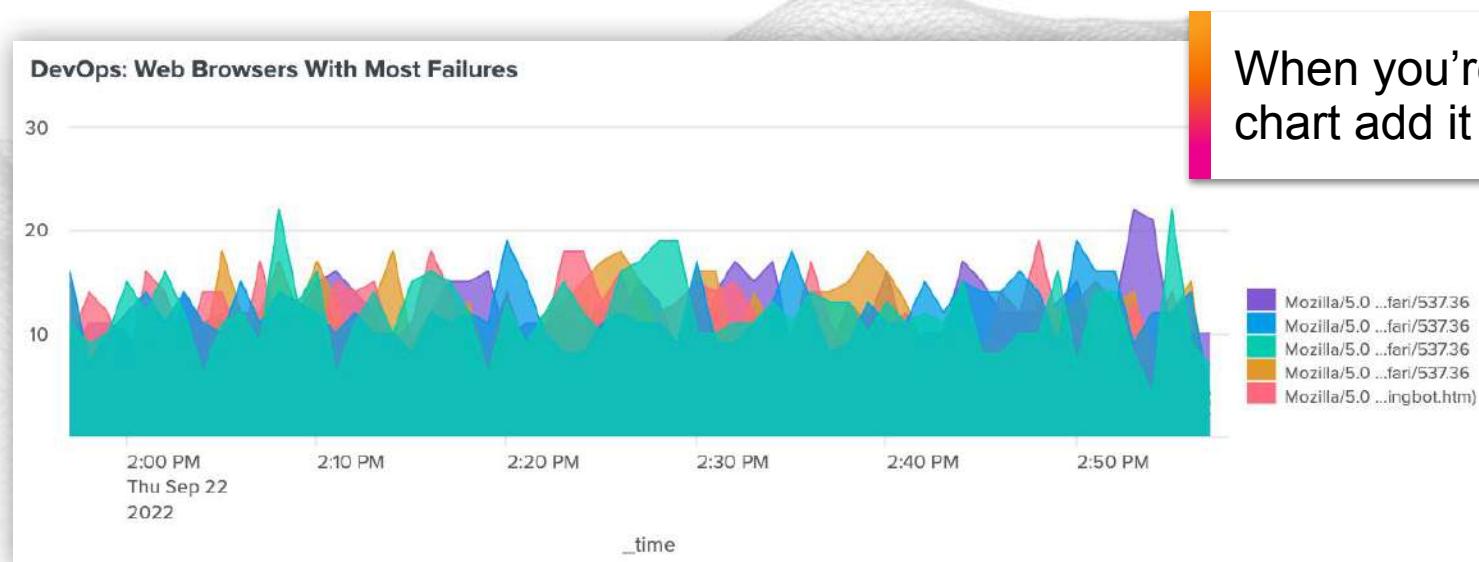


DevOps Team

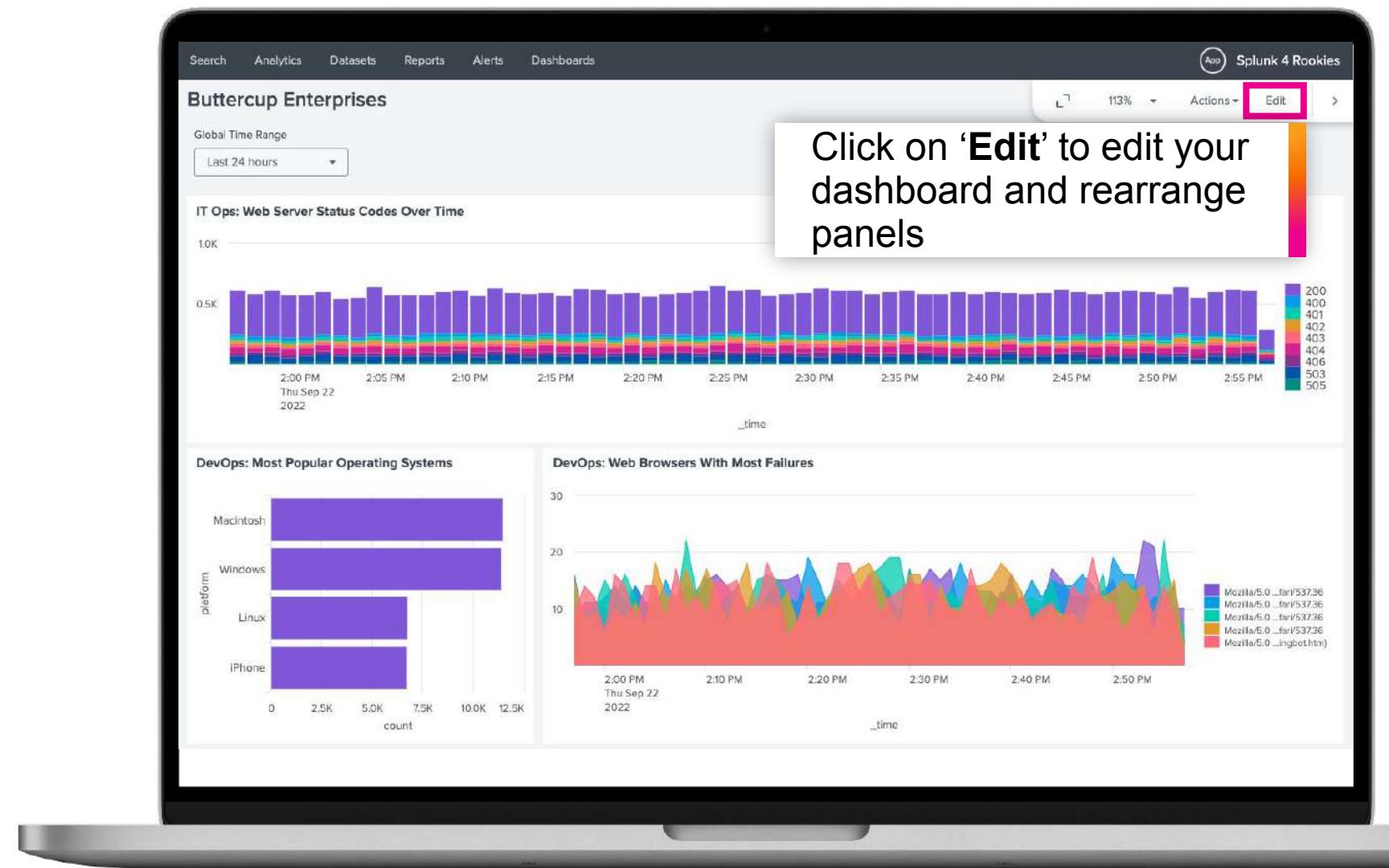
Create A Graph Showing the Top 5 Web
Browsers That Are Experiencing the Most Failures Over Time

Solution

```
index=main sourcetype=access_combined status>=400  
| timechart count by useragent limit=5 useother=f
```



Your Dashboard so far...



Obtaining Location Information with the `iplocation` and `geostats` Commands

Usage:

```
<your search> | iplocation clientip | geostats count by <field>
```

The name of a field in your data that contains IP addresses

Generates the ‘tiles’ that will be rendered on the map when visualised

Split your results by a specific field for more detailed analysis

Enriches IP data on-the-fly with location data

a City 54
a Country 23
lat 56
lon 56
a Region 41

The `iplocation` command produces additional fields containing geographic data





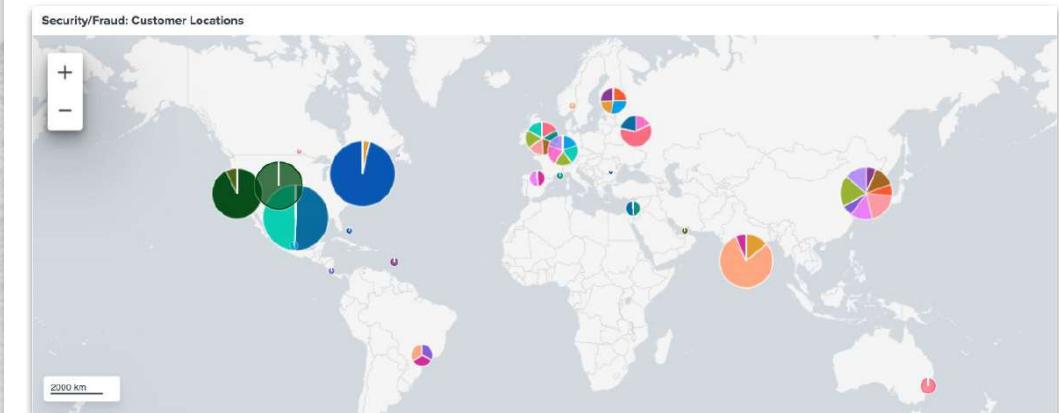
Security and Fraud Teams

Show Website Activity by Geographic Location

Tasks

1. Use the [iplocation](#) command to enrich the events with location data
2. Generate a world map showing the geographic location of all website activity down to the city level
3. Add your visualisation to your existing dashboard

Goal



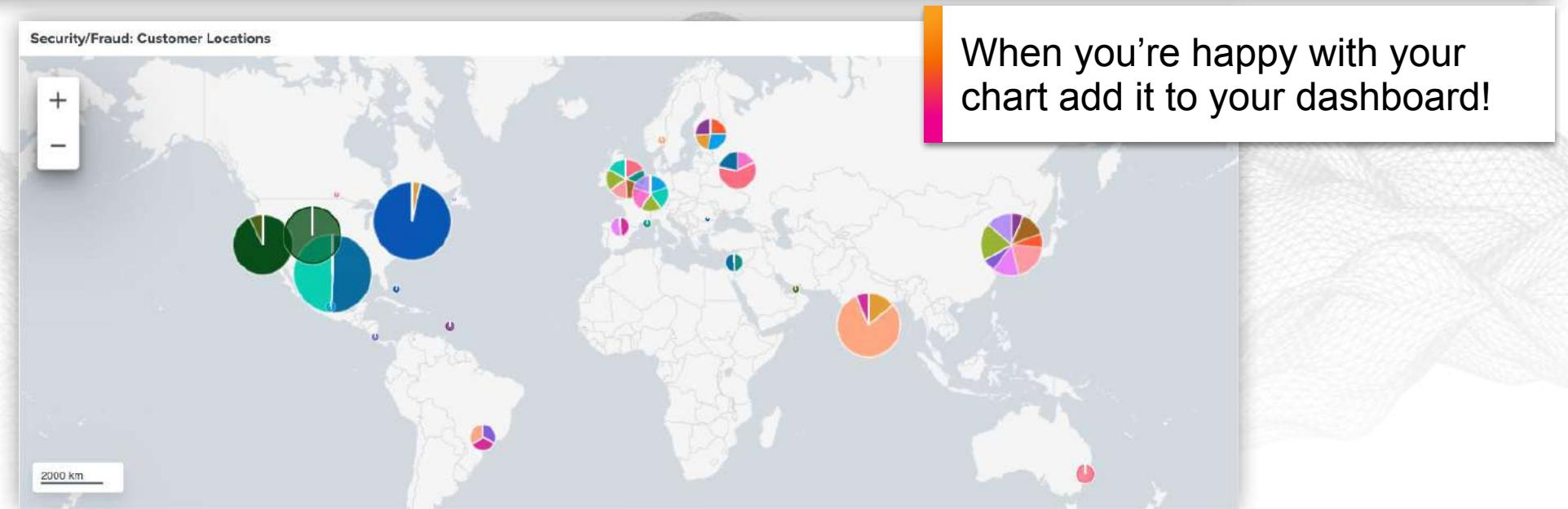


Security and Fraud Teams

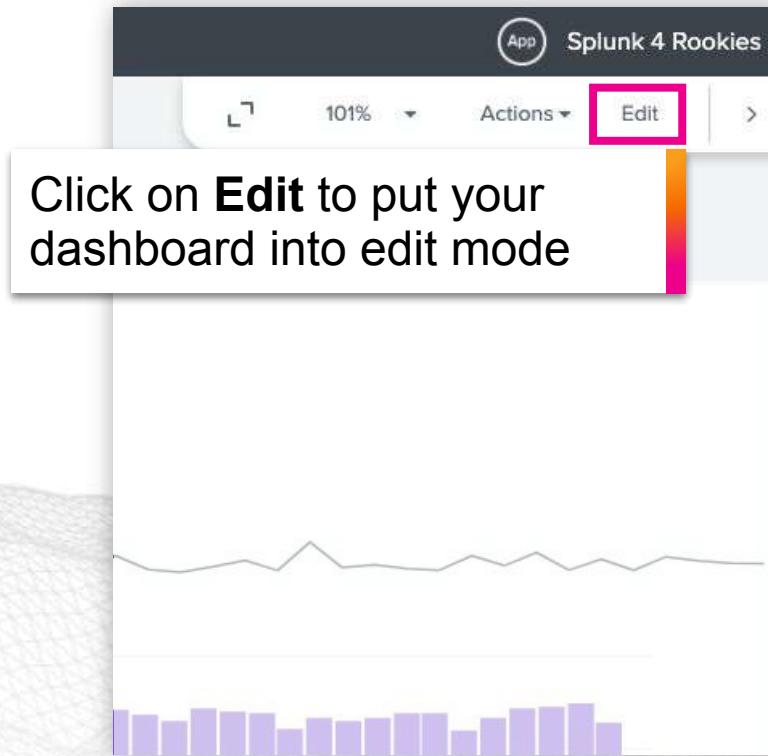
Show Website Activity by Geographic Location

Solution

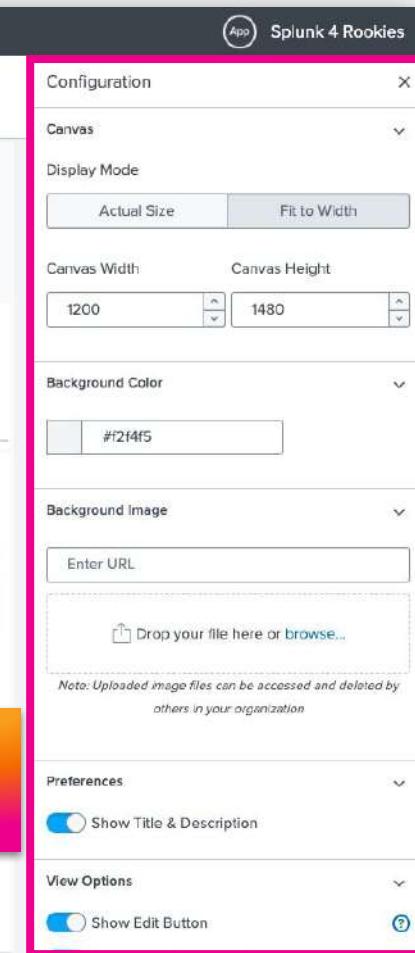
```
index=main sourcetype=access_combined  
| iplocation clientip | geostats count by city
```



Customise Your Dashboard



Add new dashboard elements from the editing toolbar



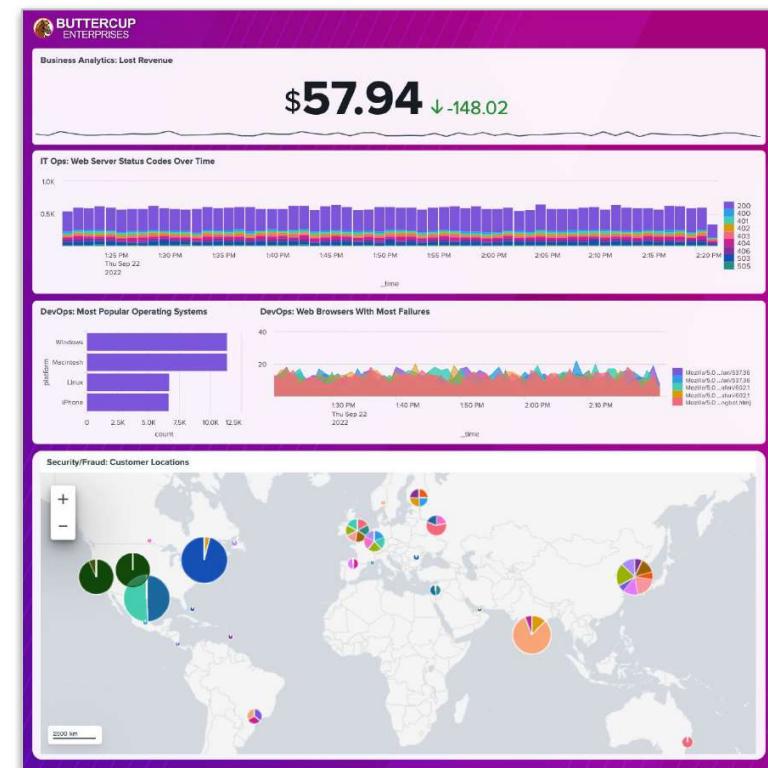


Customise Your Dashboard

Tasks

1. Add a custom background image provided by the Buttercup Enterprises Marketing team (<https://splk.it/ButtercupBackground>)
2. Resize your dashboard panels to fit within the boxes on the background image
3. Link your dashboard panels to the global time picker

Goal



Apps and Add-ons

- 3000+ free apps and add-ons available from <https://splunkbase.splunk.com/>
- Built either by Splunk, our technology partners or members of our user community
- Prebuilt packages that help to enhance and extend the Splunk platform
- Provide content and capabilities – such as reports, dashboards and integrations – for a specific technology, purpose or use case, with the flexibility to customise for your own needs

Apps

Content designed to bring fast time-to-value from your data in Splunk, including pre-built **dashboards**, **reports**, **alerts**, **visualisations** and **workflows**



Add-ons

Provide specific capabilities to Splunk, such as **getting data in**, **mapping data**, or providing **saved searches** and **macros**



Essentials for Financial Services

Demo

Splunkbase: [link](#)



Experimenting with FSI use cases and data



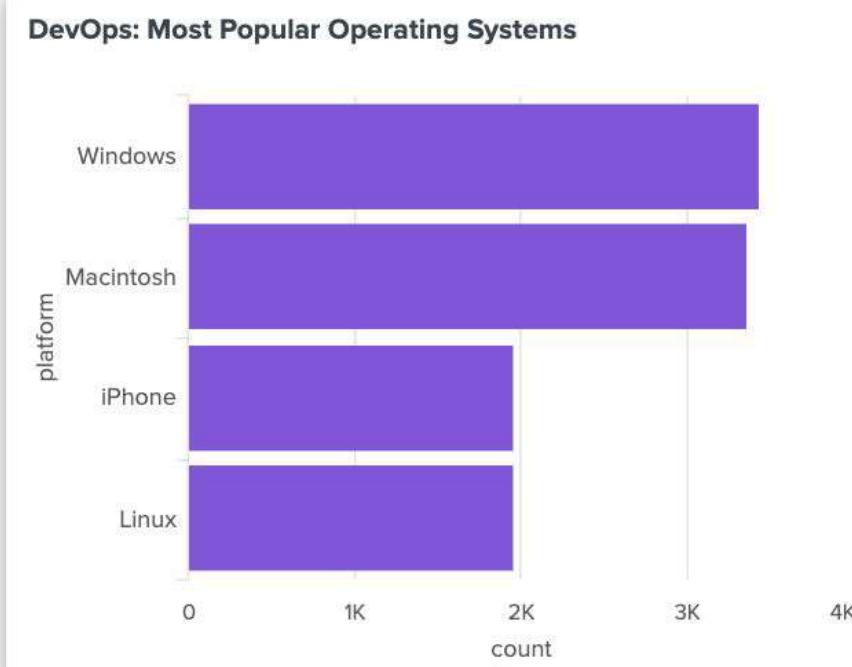


Example searches across FSI use cases

Tasks

1. Create a new app and index for this lab
2. Add FSI sample data into environment
3. Add searches to a new custom dashboard

Goal [to be updated]



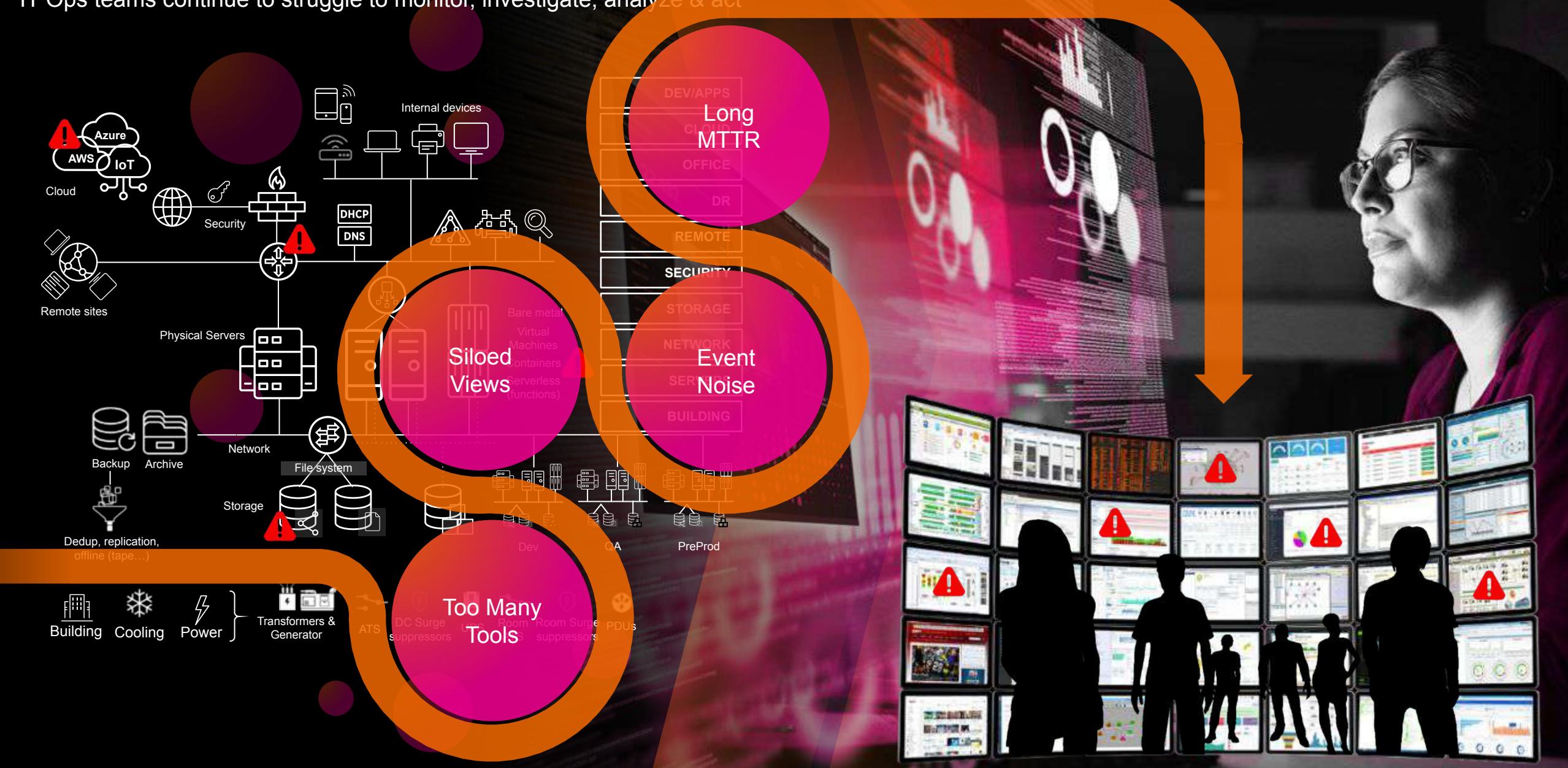
Service Intelligence



splunk>

Complexity obscures the data you need

IT Ops teams continue to struggle to monitor, investigate, analyze & act



The impact can be significant

Putting revenue, customer experience, employee effectiveness & innovation at risk



Lost Revenue

Outages and incidents impact the services and apps driving revenues



Poor Customer Experiences

Customers click away and brand reputation is damaged



Decreased Employee Effectiveness

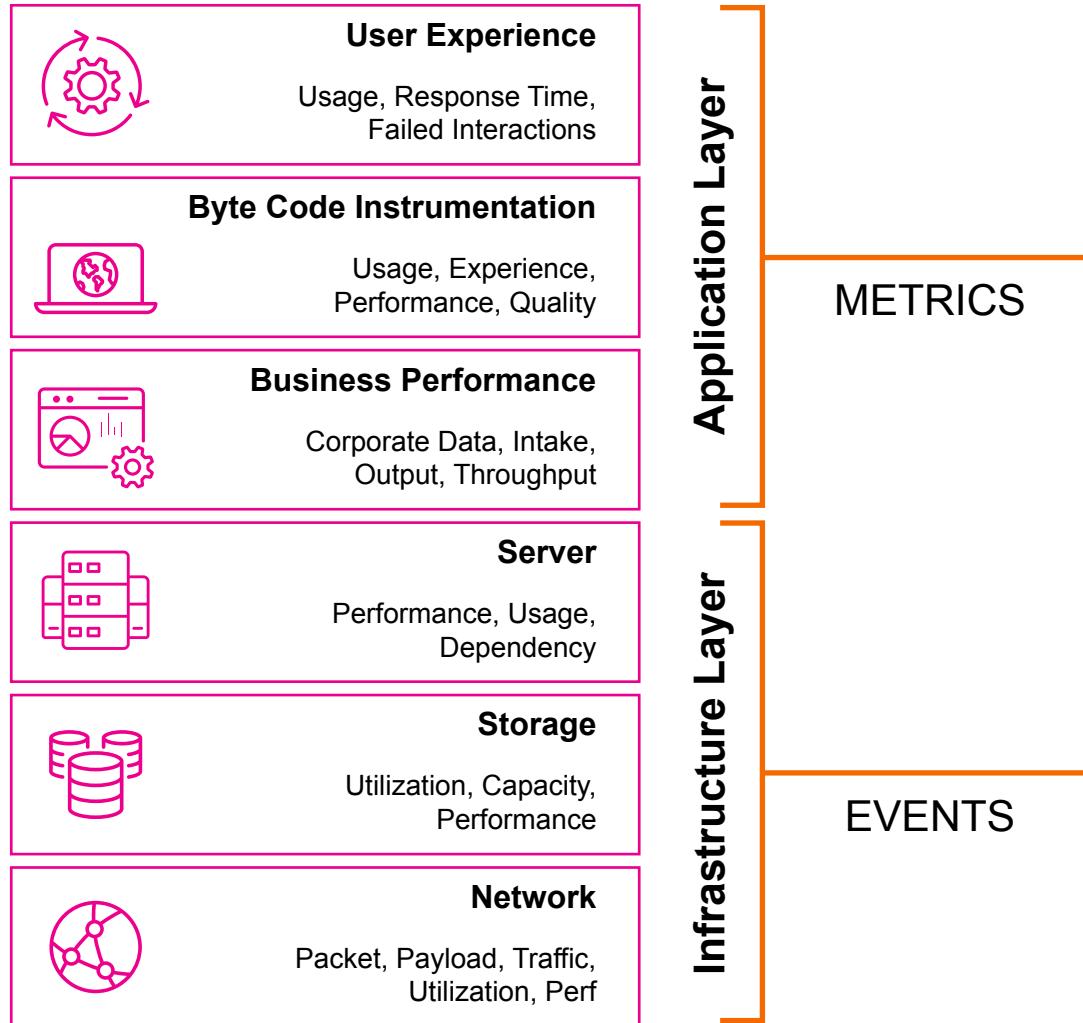
Teams thrash, finger-point, and key employees leave



Struggle to Innovate

IT spends too much time fixing problems instead of innovating and transforming

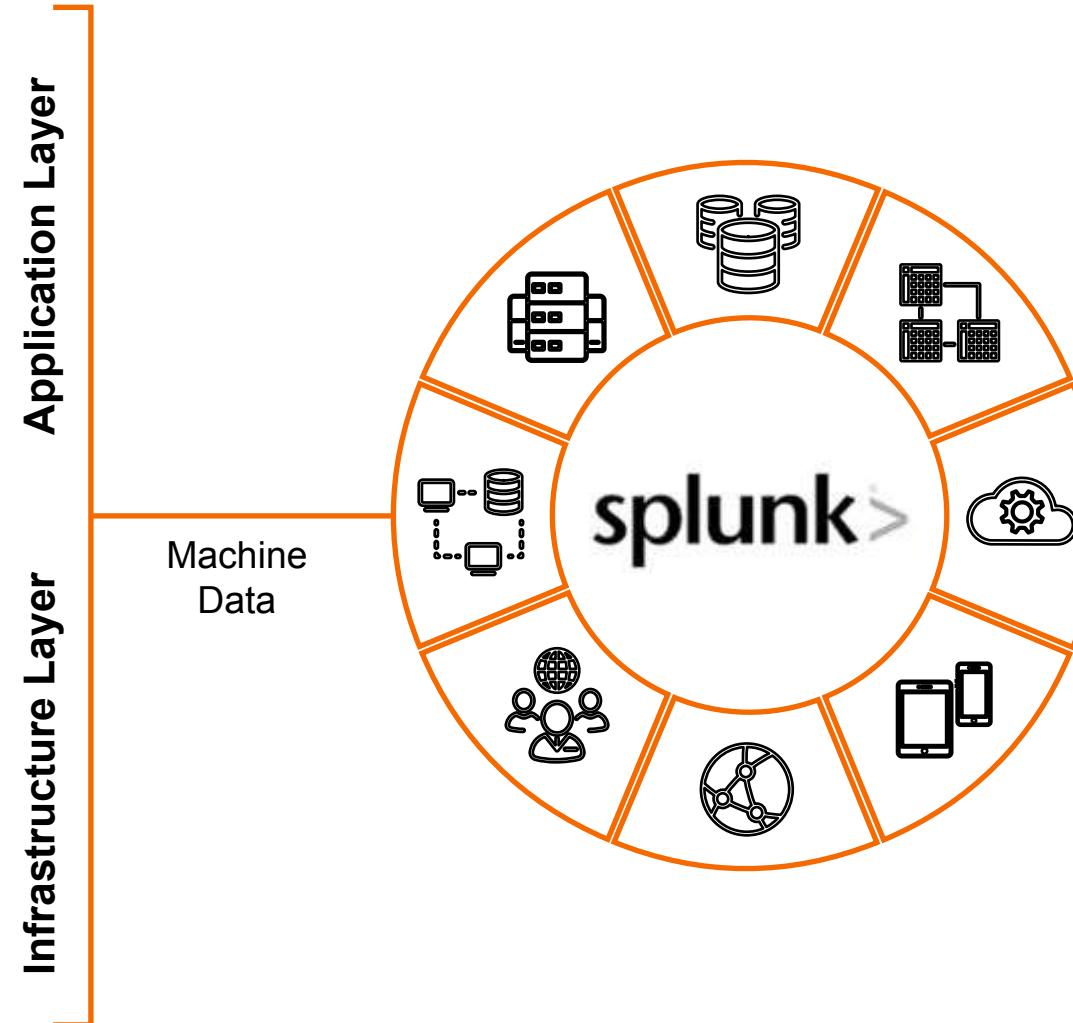
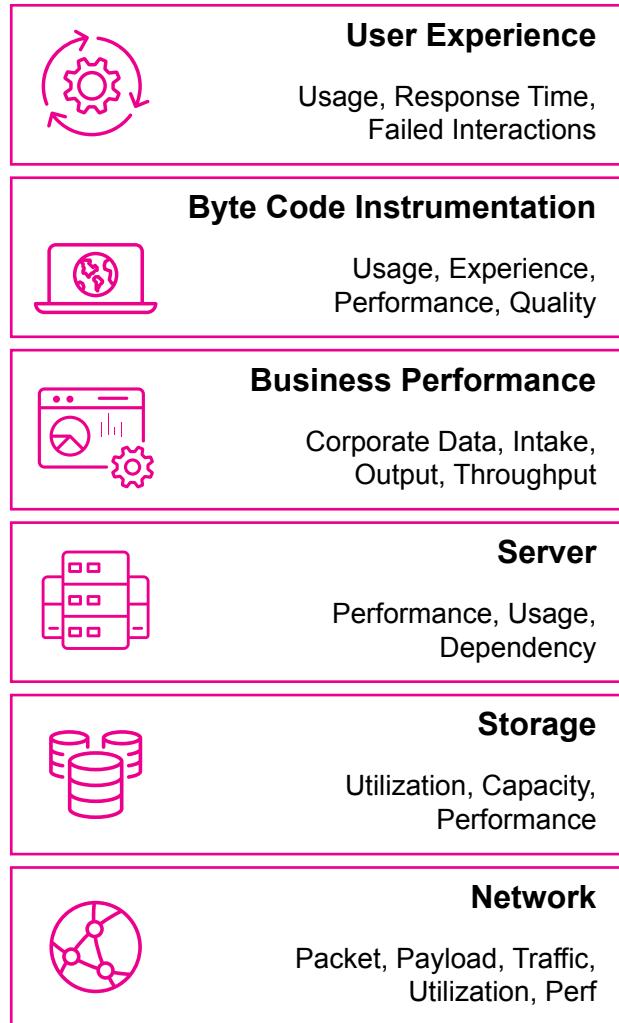
The Old Ways Disappoint



Challenges

- Many disparate components
- Brittle integrations
- Data is summarized and lost
- Longer root-cause identification
- End-to-end view challenging
- Labor-intensive to manage
- Not agile for digital business

Splunk IT Service Intelligence Platform Approach



Splunk Approach:

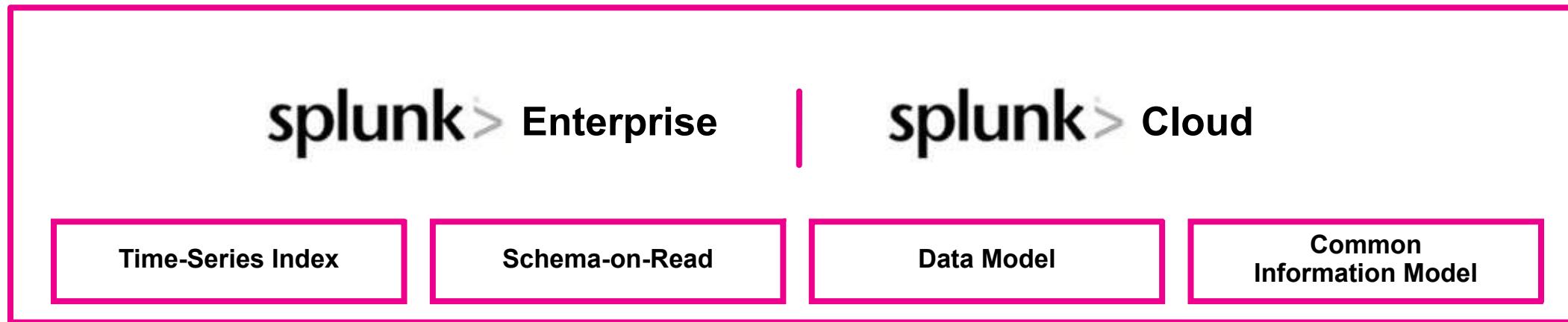
- Repository for **ALL** data
- Data in original raw format
- Machine learning
- Simplified architecture
- Fewer resources to manage
- Collaborative approach

Splunk IT Service Intelligence

Data-driven service monitoring and analytics



Machine
Learning



Service Intelligence Demo



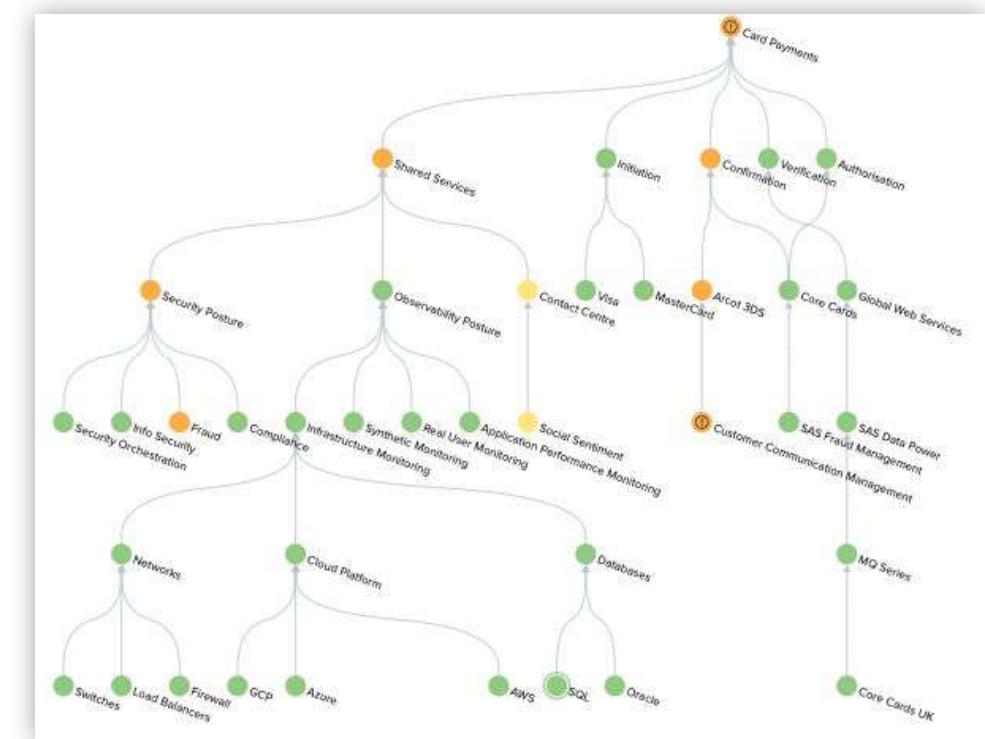


Explore the ITSI capability

Tasks

1. Explore Glass Tables
2. Explore Service Analyzer
3. Explore Deep Dive

Goal





Building a new service view

Tasks

1. Build your own service hierarchy
2. Add KPIs, generate Health Scores
3. Build some custom Glass Tables

Goal



Creating Services via Import Demo



splunk>



Building your own service!

Tasks

1. Use what you've learned today to build something that relates to your role or team
2. Be creative, ask for help, and share ideas

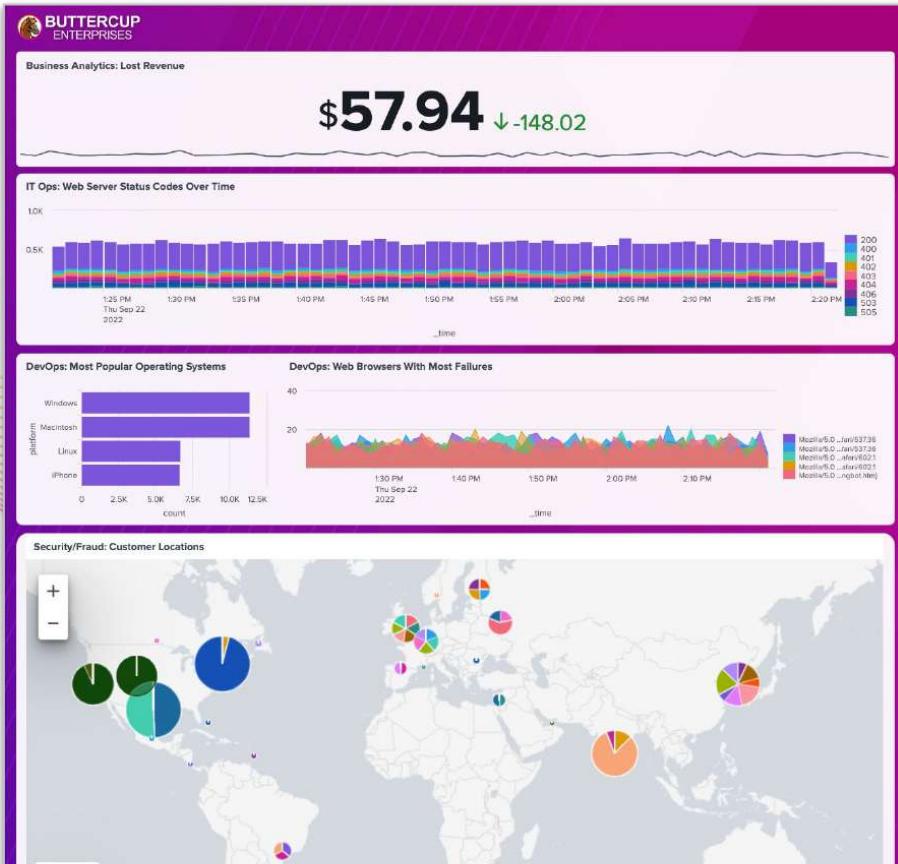
Goal

You Finished the Hands-on Exercises!

You made it!



How Did You Do?



Did you end up like this?...



Or this?



Splunk Resources

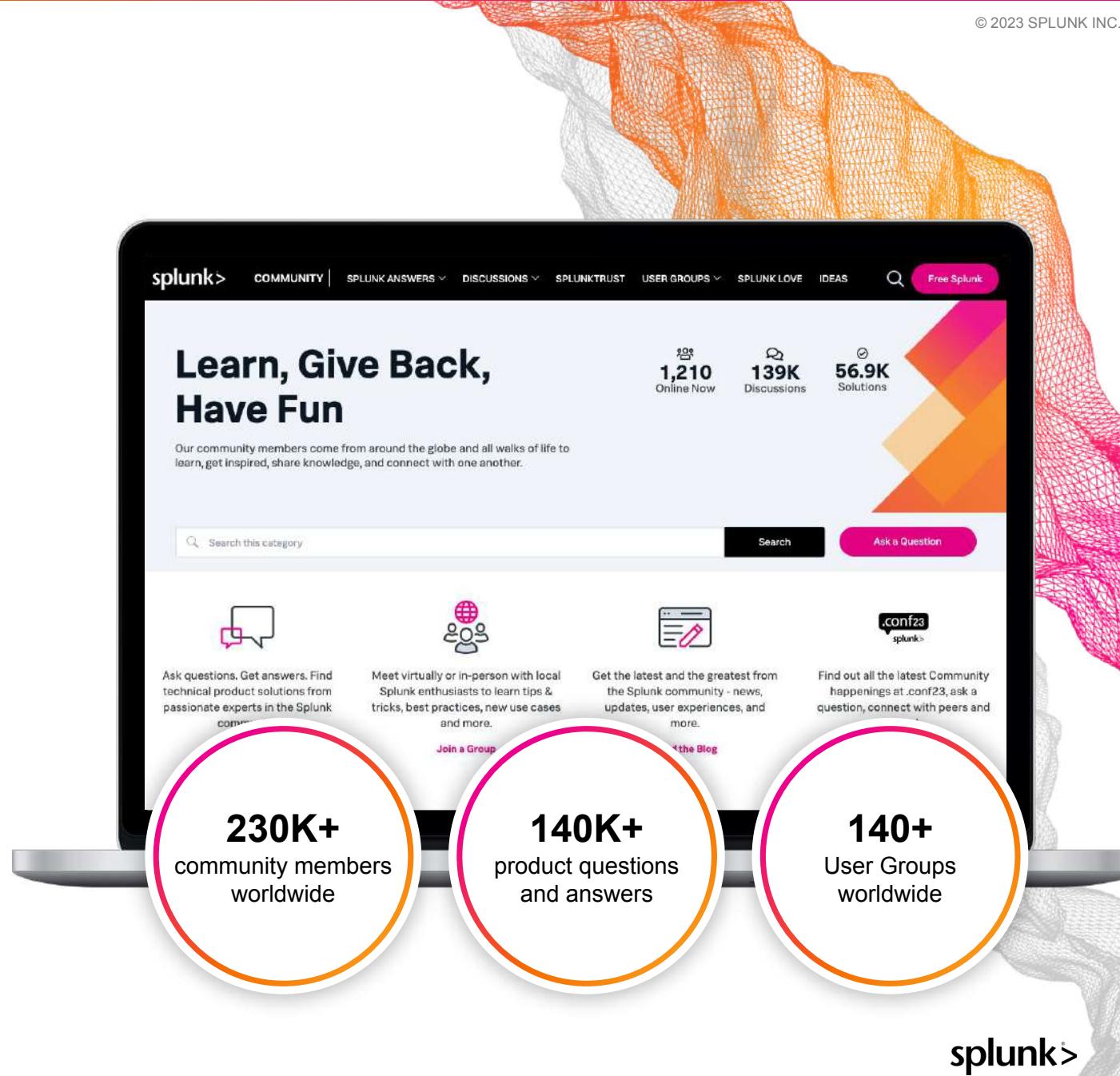
Where to go after
today's workshop

splunk>

Splunk Community

<https://community.splunk.com>

- A free way to connect, learn, have fun, and find success with Splunk
- Ask questions, get answers, and find solutions from passionate experts in the community
- Meet in-person or virtually with like-minded enthusiasts, in your area or by interest
- Search for, vote on, or submit your own ideas for new enhancements for any product or solution



Splunk Events

<https://events.splunk.com>

- Expand your network and connect with the global and local Splunk community



<https://conf.splunk.com>

- Join us at .conf24!
- Hundreds of on-demand sessions from product updates to learning new Splunk skills!

A screenshot of a tablet displaying the Splunk Events website. The top navigation bar includes links for Products, Solutions, Why Splunk?, Resources, Support, and a Free Splunk button. The main header reads "Splunk Events" with a subtext: "Join us at an event near you to gain new skills, expand your network and connect with the Splunk Community." On the left, there's a sidebar with a search bar and filters for "Filter all", "Regions", "Event Types", and "Solutions". The main content area is titled "Featured Events" and lists three events: "Gartner IT SYMPOSIUM Xpo" (Industry Event, Orlando), "KubeCon + CloudNativeCon North America 2023" (Industry Event, Chicago, IL), and "AWS re:Invent" (Partner Event, Las Vegas, NV). Below this is a section titled "Upcoming Events".

The screenshot shows a tablet displaying the Splunk Events website. The page features a header with the Splunk logo and navigation links. The main content area is titled "Splunk Events" and encourages users to join events for skill gain and networking. It highlights "Featured Events" like Gartner IT SYMPOSIUM Xpo, KubeCon, and AWS re:Invent. A sidebar on the left provides filtering options for regions, event types, and solutions. The overall design is clean and modern, utilizing a color palette of orange, white, and grey.

Documentation

<https://docs.splunk.com>

- Search reference for SPL

- Step-by-step tutorials

Search:

<https://splk.it/SplunkSearchTutorial>

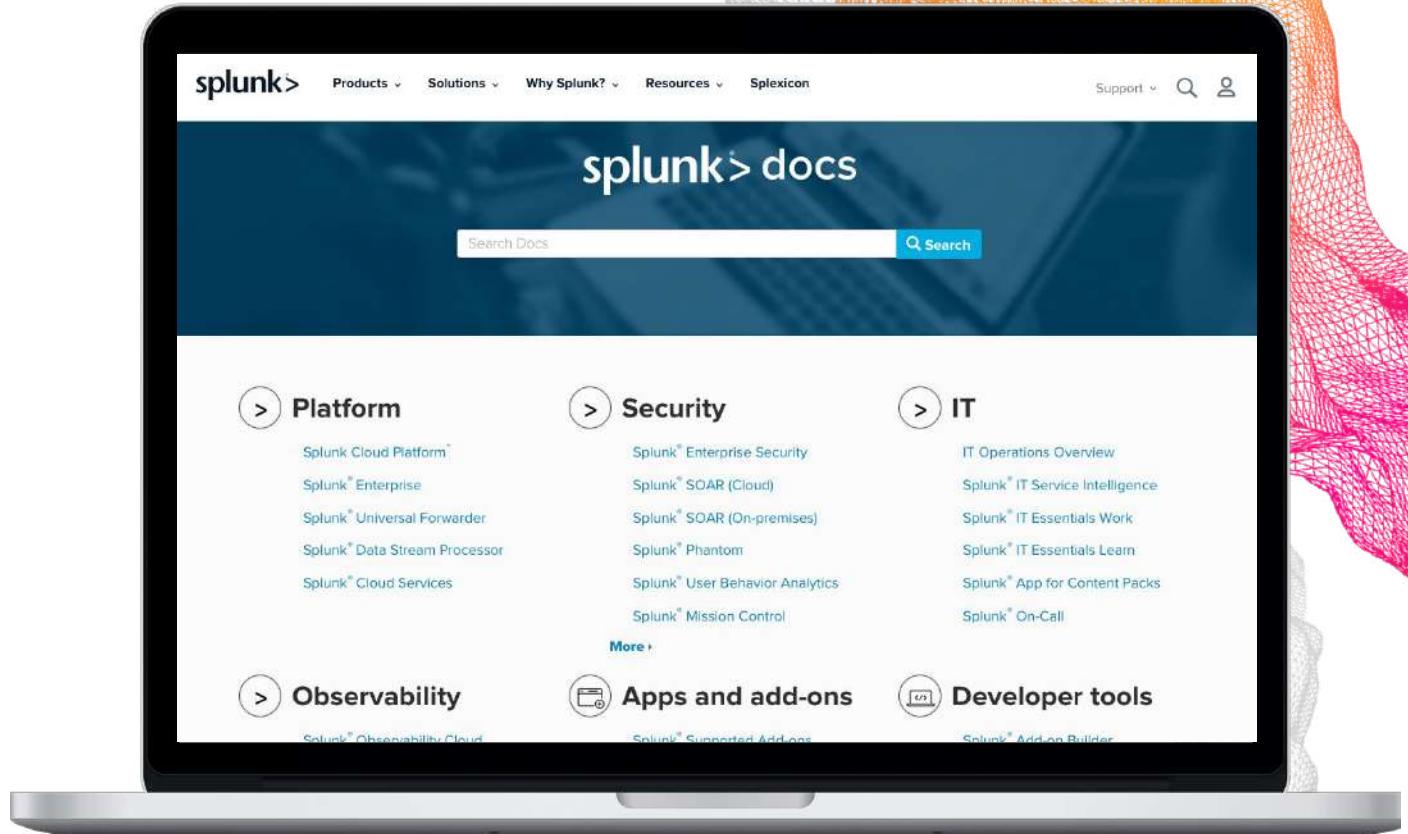
Dashboard Studio:

<https://splk.it/SplunkDashStudioTutorial>

- Product references

- Procedures/guides

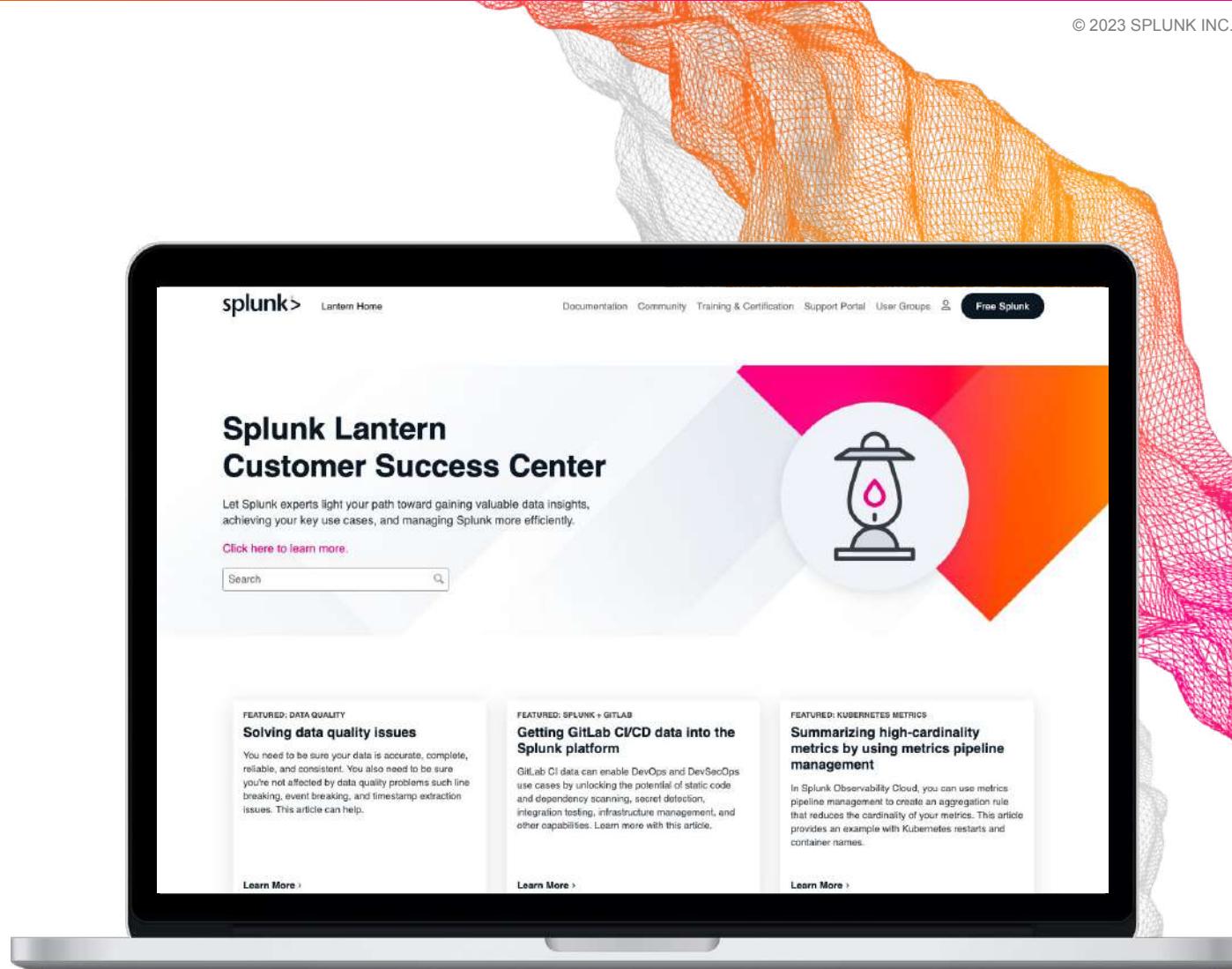
- And more!



Splunk Lantern

<https://lantern.splunk.com>

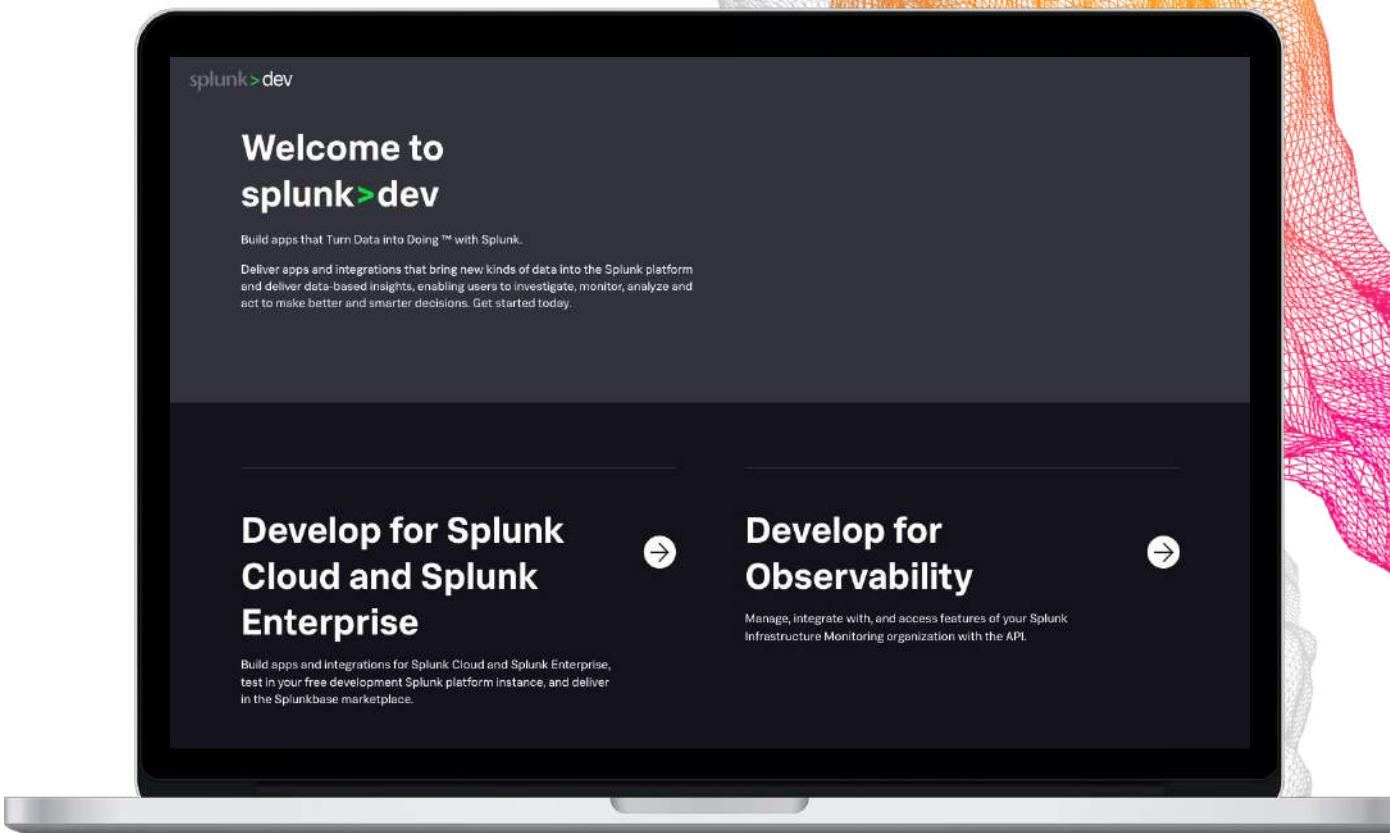
- Use case library
- Step-by-step procedures
- Map use cases to data sources
- Splunk Success Framework to realize value across your organisation



Developer Resources

<https://dev.splunk.com>

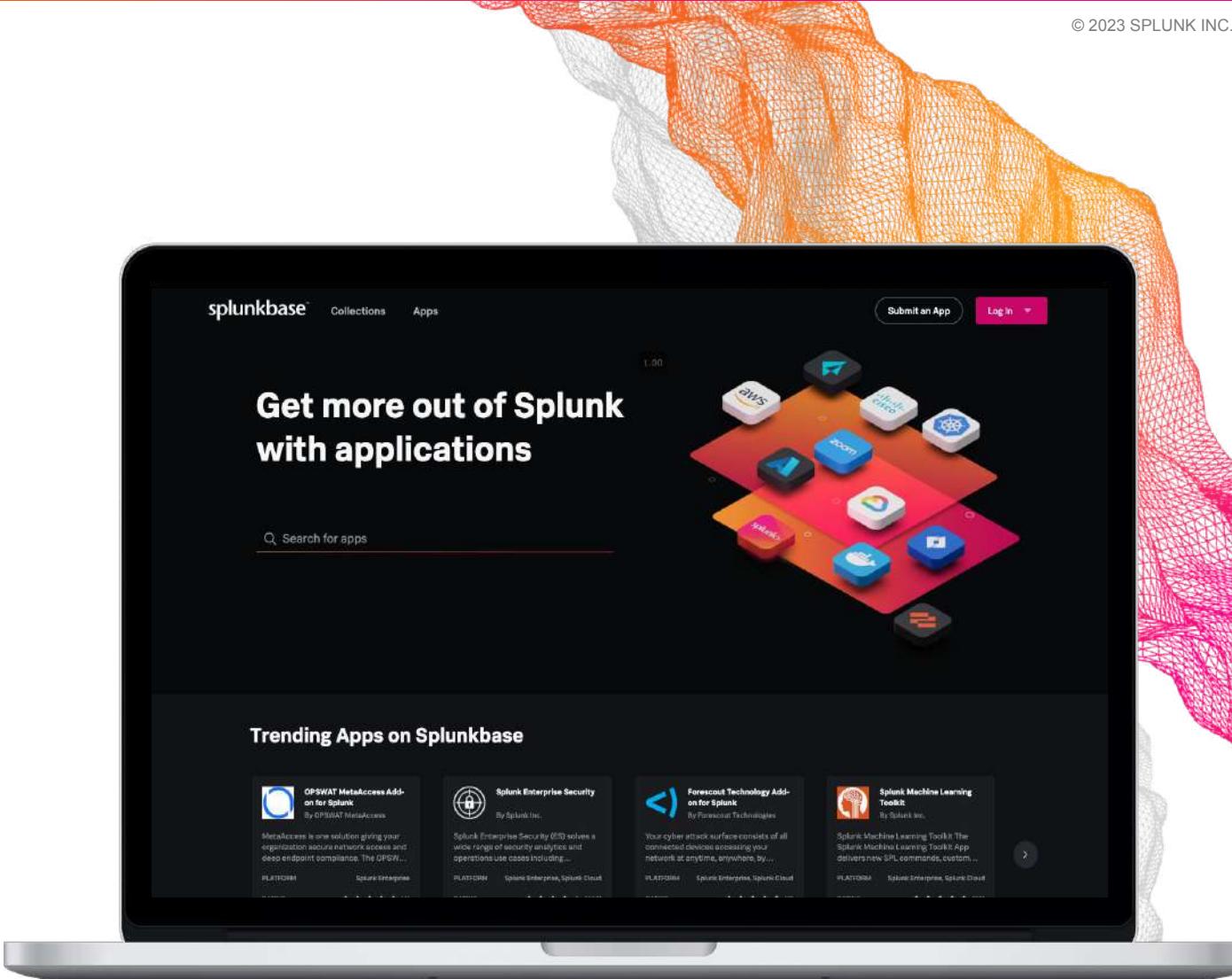
- Developer Guide
- API Reference
- Tutorials
- Downloads
APIs, libraries, tools
- Code examples
- Free Developer licence



Splunk Apps & Add-ons

<https://splunkbase.splunk.com/>

- 3000+ apps and add-ons
- Pre-built searches, reports, visualisations and integrations for specific use cases and technologies
- Download apps and customise them based on your requirements
- Fast time to value from your data
- Build and contribute your own apps!



Training & Certification

<https://splunk.com/training>

Online education classes

Instructor-led and self-paced eLearning

Certification tracks for different roles

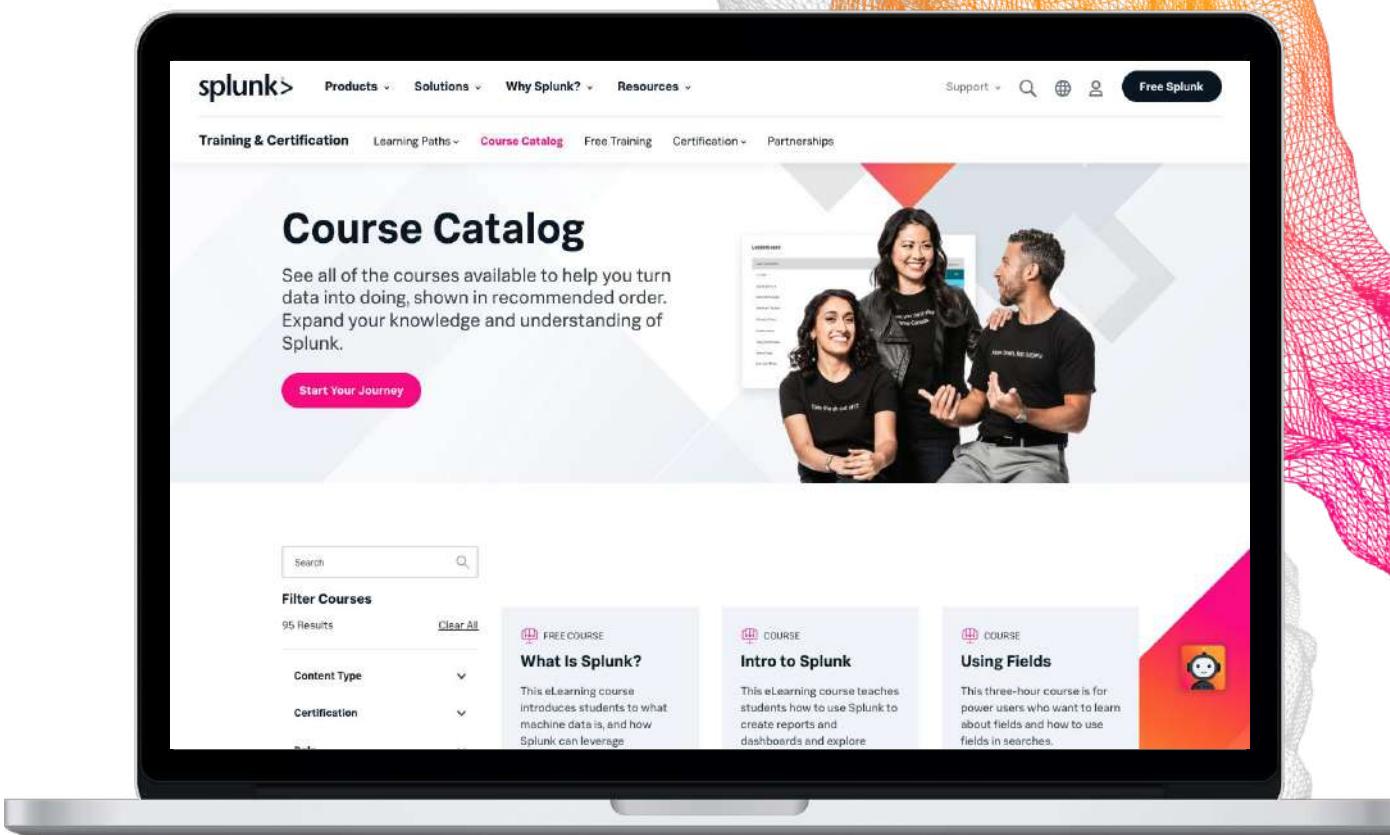
User, Power User, Admin, Architect and Developer

Splunk Education Rewards

Complete training and receive points that you can redeem for Splunk swag!

Free education!

Free single-subject eLearning courses to kick start your Splunk learning



Thank You!

