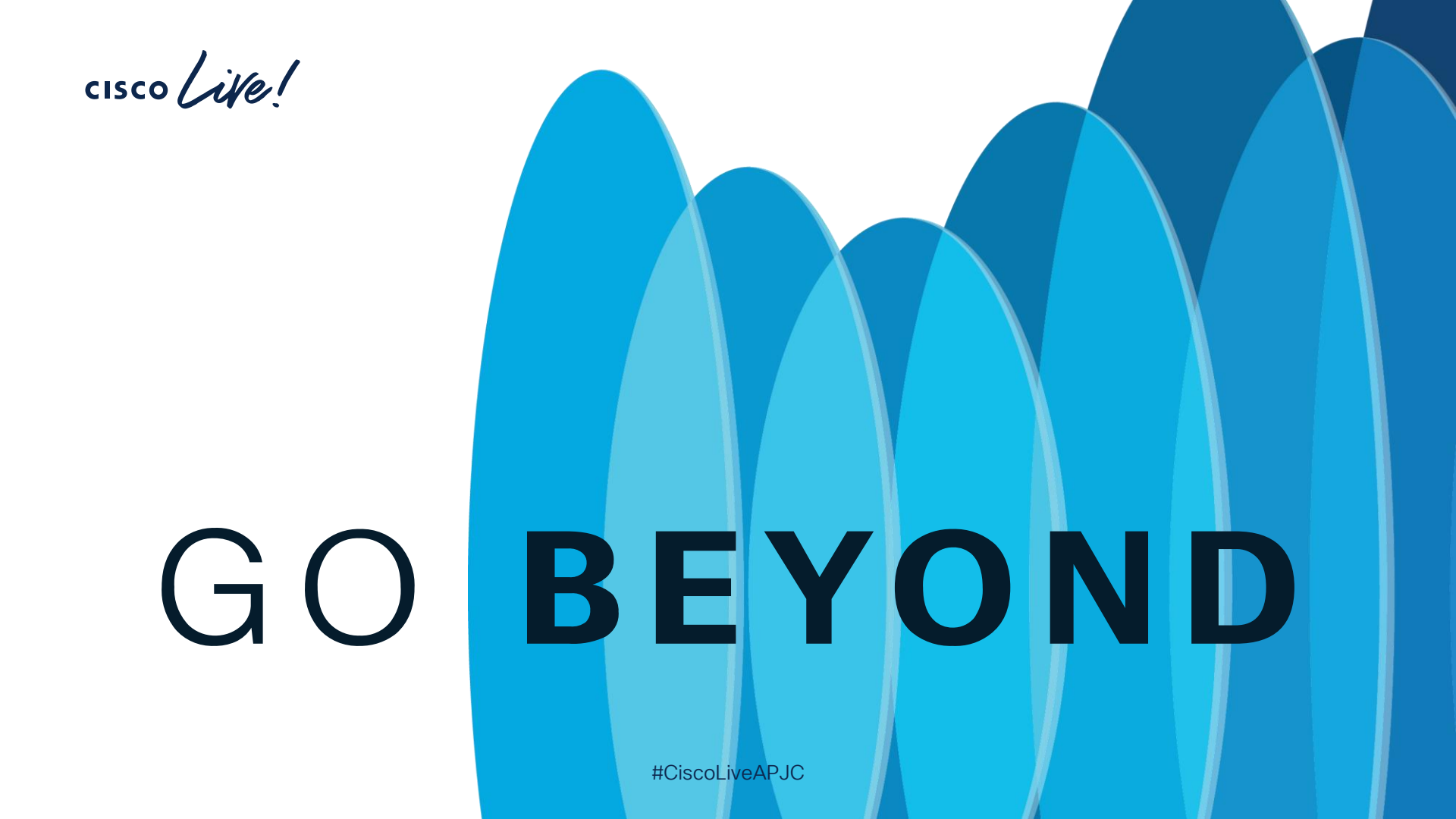

cisco Live!
GO BEYOND
#CiscoLiveAPJC

Splunk Platform Insights

A Guide for Network Engineers

Russell Uman
Cloud Staff Solutions Architect – Splunk Singapore

BRKGEN-1624

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKGEN-1624

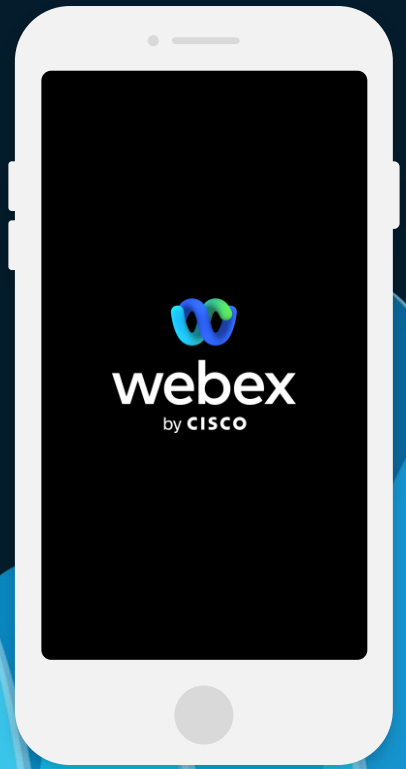
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



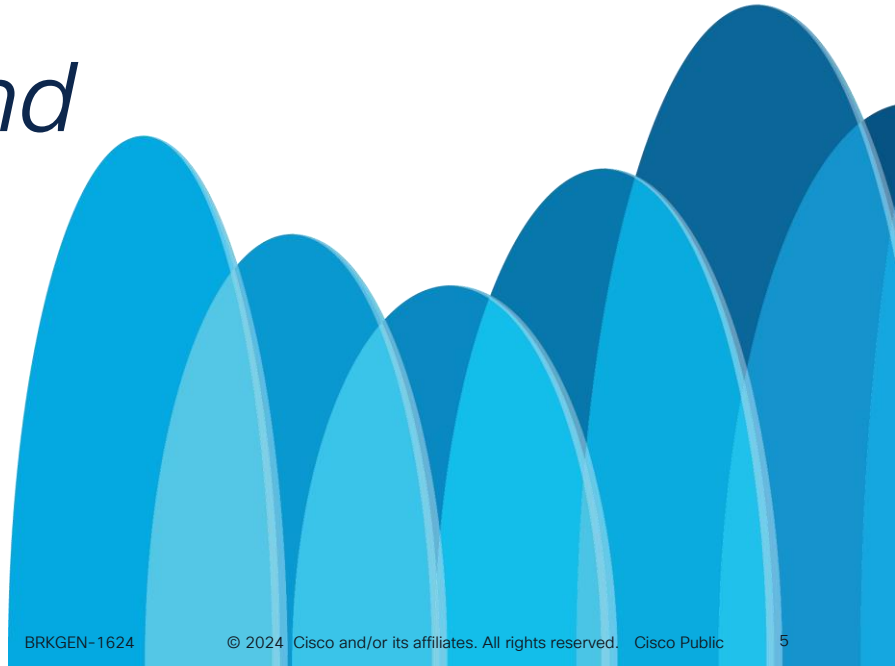
cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk turns data into actions by making machine data accessible, usable and valuable

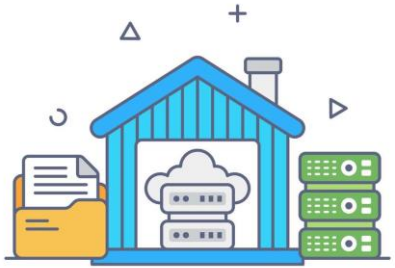
What is Splunk?

How do we help?



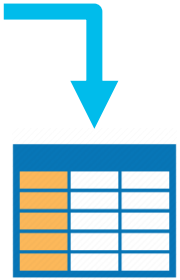
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data Classification



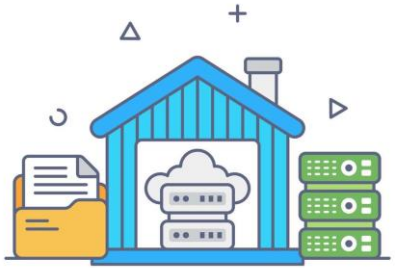
Data Warehouse

- Business
- Reporting



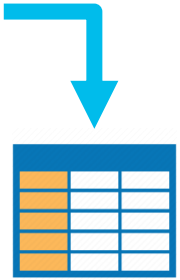
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data Classification



Data Warehouse

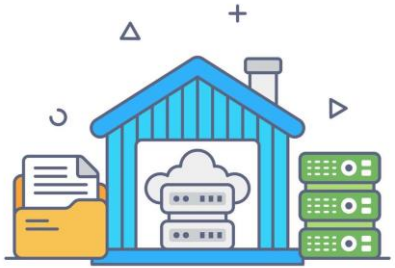
- Business
- Reporting



Files and Documents

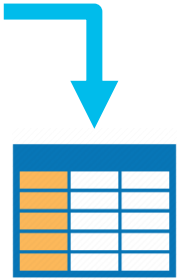
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data Classification

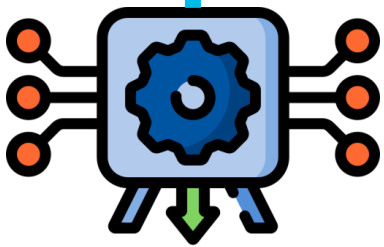


Data Warehouse

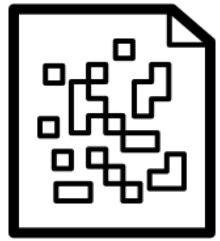
- Business
- Reporting



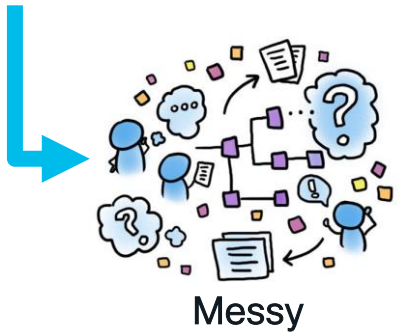
Files and Documents



Machine Data



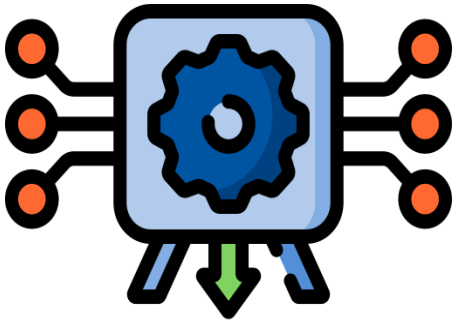
Unstructured



Messy

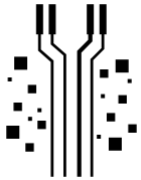
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Machine Data “Valuable Complex Data”



Machine Data

Machine Interactions



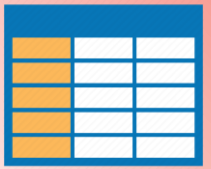
Streaming

Transactional

- Metrics
- Events
- Logs
- Traces

Unstructured

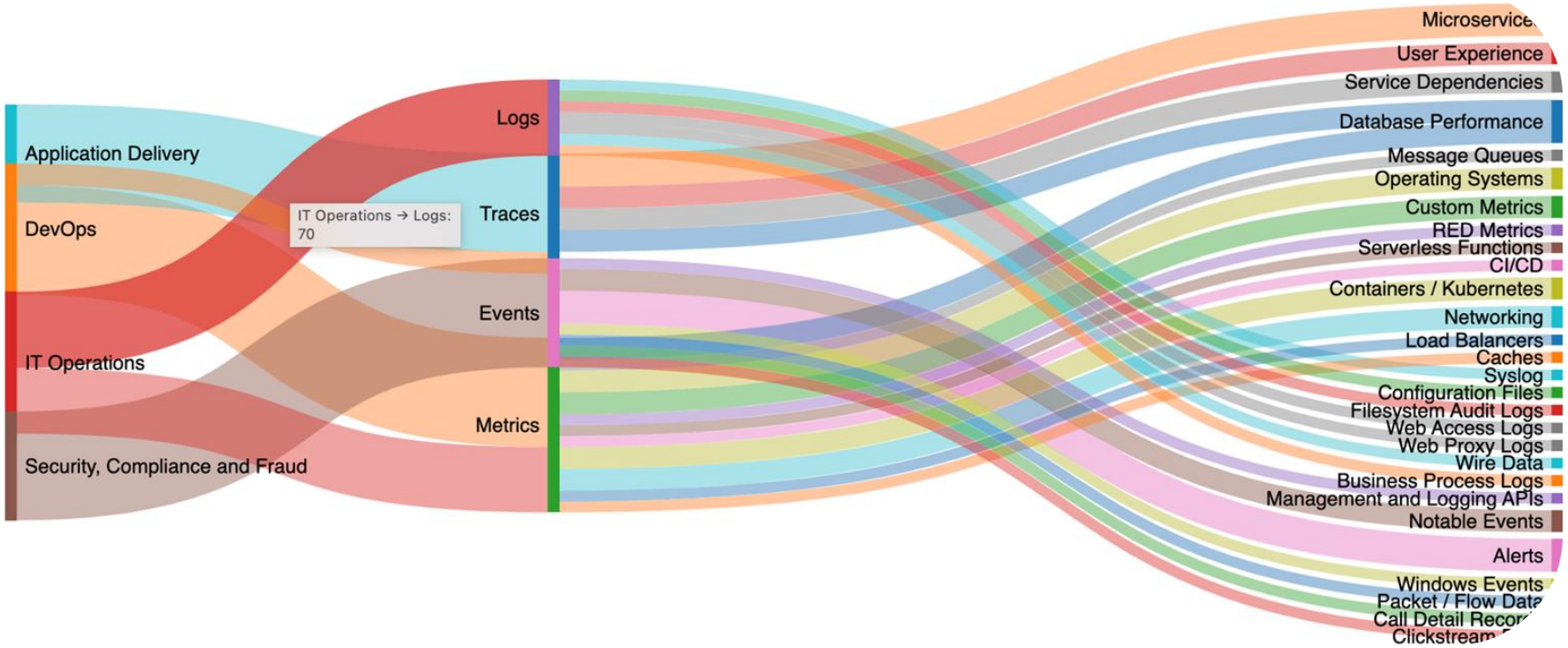
Messy



Structured
Semi - Structured

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Multiple Use Cases On Common Data

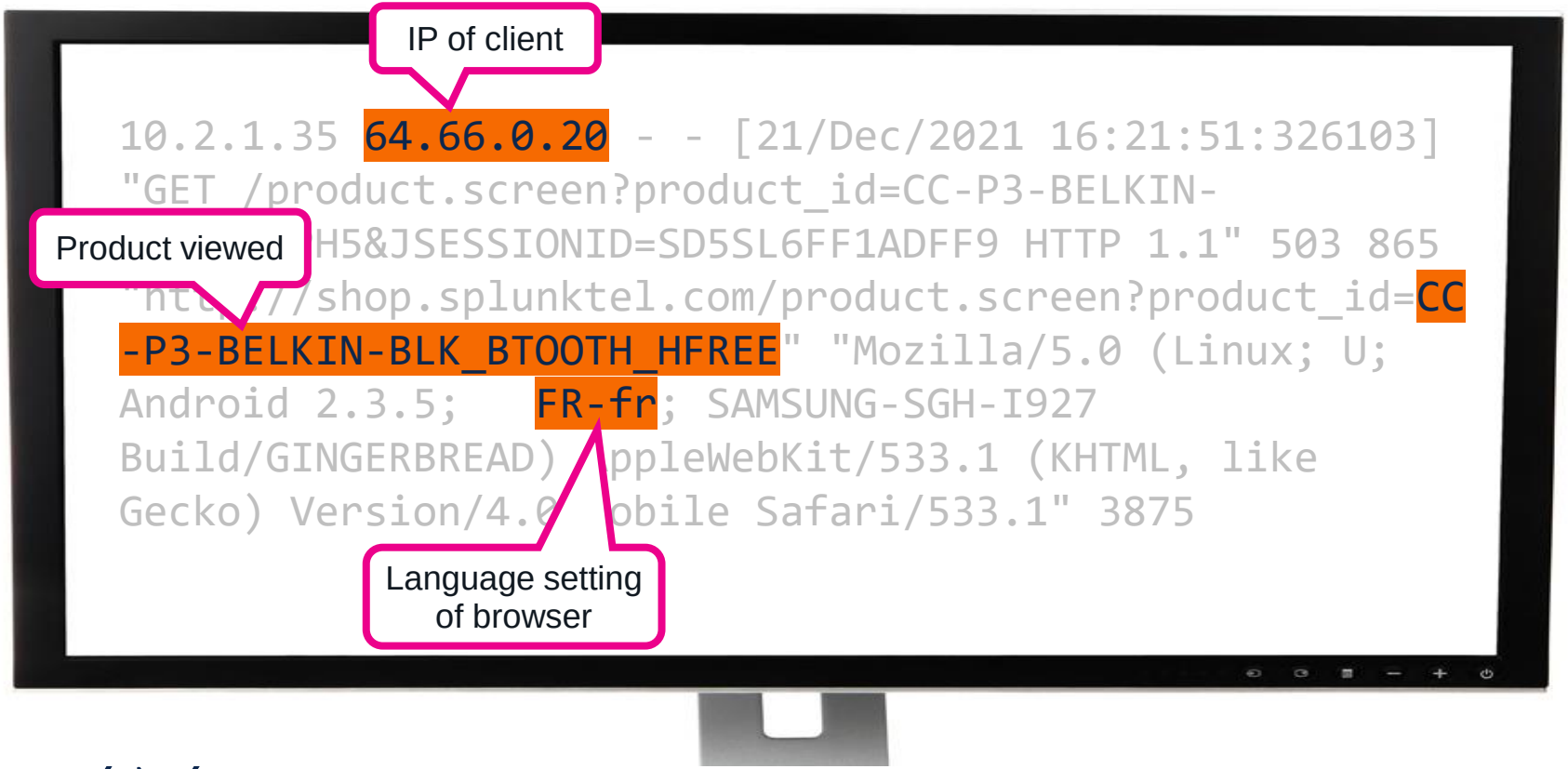


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Machine Data is ~~Complex~~ VALUABLE!

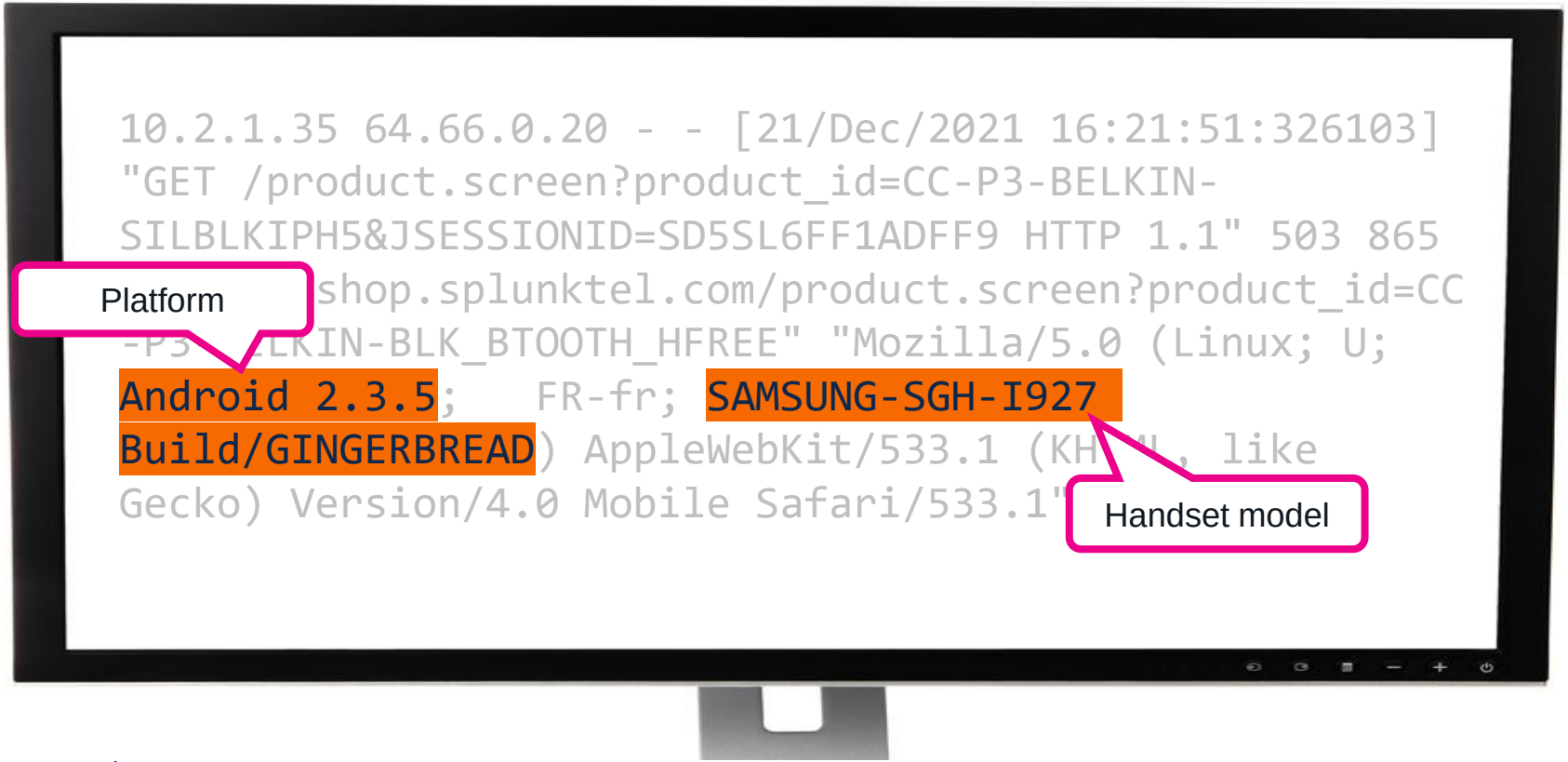
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Marketing Use Case:
Show the top products viewed by language



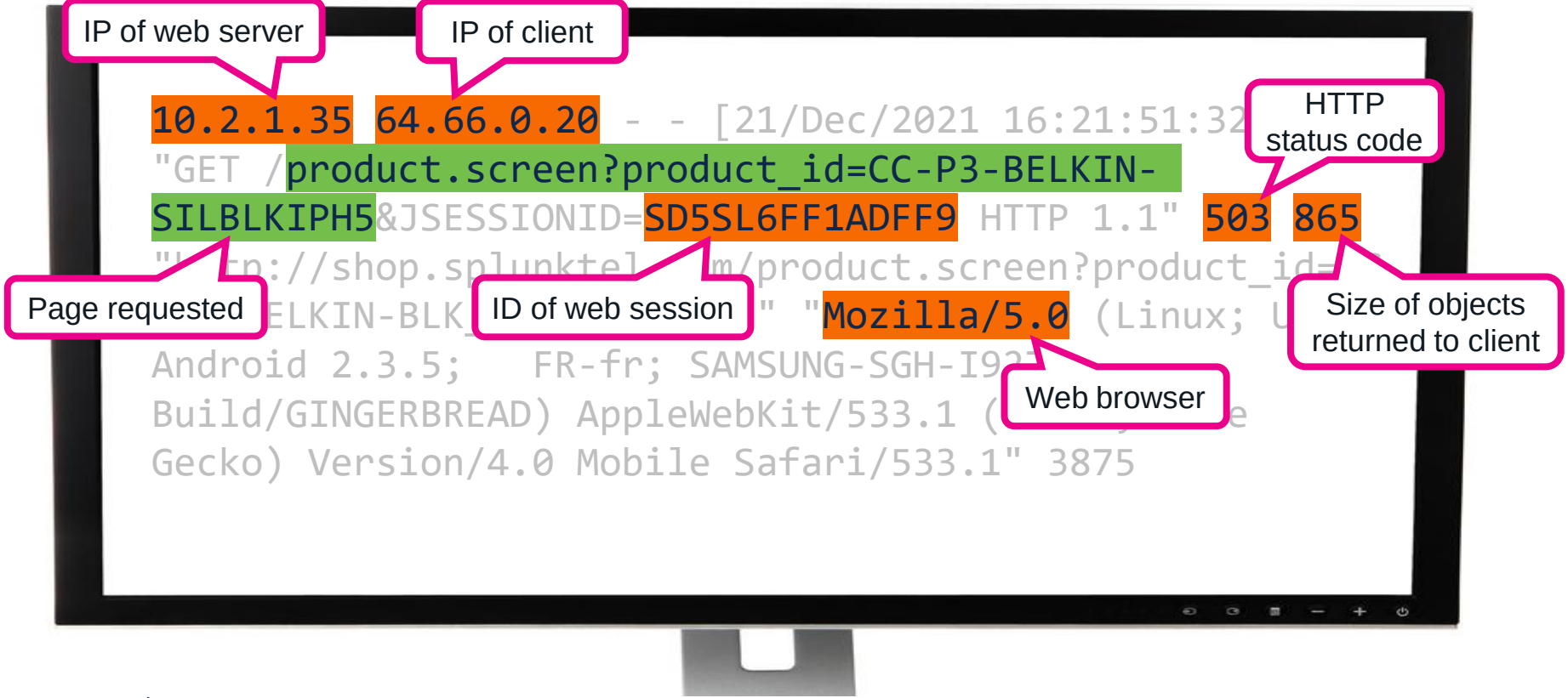
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

DevOps Use Case: Which mobile handsets should I test the most before releasing my new app?



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

IT Operations Use Case: Which web pages are generating the most errors?



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk, since 2003.

Founded by 3 geeks (Rob, Michael and Erik)

Vision to make a tool to manage massive amount of machine logs as simple as you searching it on a webpage (GOOGLE FOR LOG SEARCH)

Splunk SIEM : Enterprise Security Launched

First premium app was launched to provide advance security data analytics and SIEM

Splunk Cloud Launched

O11y Cloud Launched

Major feature updates across platform, security and o11y space

Data streaming was launched

2003 — 2006 — 2011 — 2012 — 2013 — 2020 — 2024

Splunk Enterprise

Splunk 1.0 Launched

Splunk launched its first product, Splunk 1.0. It was marketed as a search engine for log files and machine data, enabling users to troubleshoot and monitor their IT systems.

Evolution of product : Splunk 1.0 to Splunk 4.0

- *SPL Language for advance analysis*
- *Index optimisation for scale*
- *Data manipulation based searches*
- *Analytics and real time search*
- *Distributed search*
- *Splunk app base launch and APPS GENERATION AT SCALE STARTED*

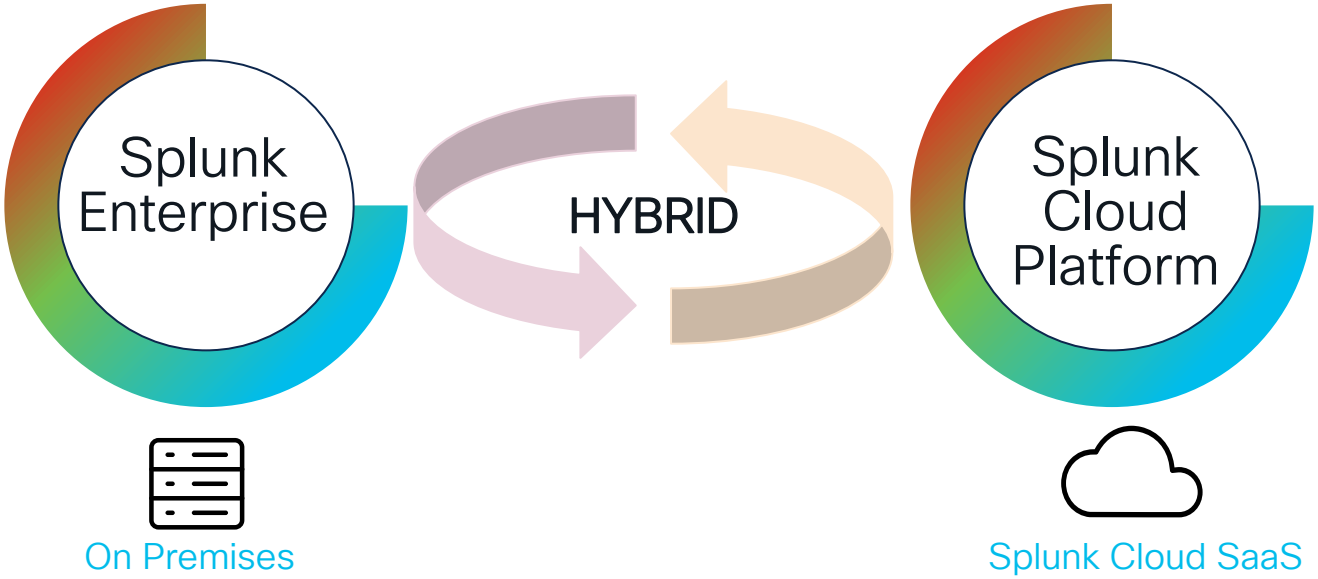
Product Evolution & Market Leadership

- *ITSI Launched*
- *More than 8 acquisitions made (Phantom, SignalFx, Rocana etc)*
- *Emerged as technology leader in security, ITOps and o11y*
- *Splunkbase grown from 400 to 1800 apps*
- *Reached PB / day scale milestone*

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk Platform

Deployment Choices



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk’s way of doing things.

Getting data in.

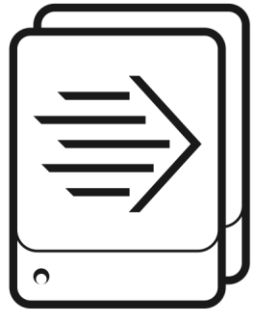
Forwarders

Universal Forwarder

- Inputs
  - File reader
  - Network (TCP/UDP)
  - Simple scripts
- Outputs
  - Splunk2Splunk
  - HEC
  - Raw/Syslog

Heavy Forwarder

- Data Collection
  - Complex scripts (modular inputs)
  - APIs
  - External databases



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Receivers

Heavy Forwarder

- Intermediate forwarder to bridge networks or offload parsing.

Indexers

- Receive data, index data, and search data.
- Most parsing happens on the first receiver.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk Connect For...

Syslog

- Containerized fast/efficient alternative to UF + Syslog server.

SNMP

- Containerized light-weight collector for SNMP sources.

Kubernetes

- Otel Collector for Kubernetes is a Helm chart that simplifies sending logs and metrics to K8s clusters to Splunk and Splunk IM.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

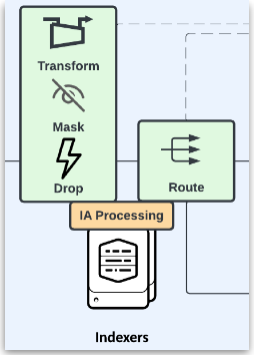
Splunk Stream

- Full-featured collector for network events
  - Passively capture streams of network data
  - Capture metadata and full packet streams for multiple network protocols
  - Collect NetFlow protocol data
- Runs as a component of a forwarder to collect local network data
- Runs as a stand-alone collector to capture wire data.

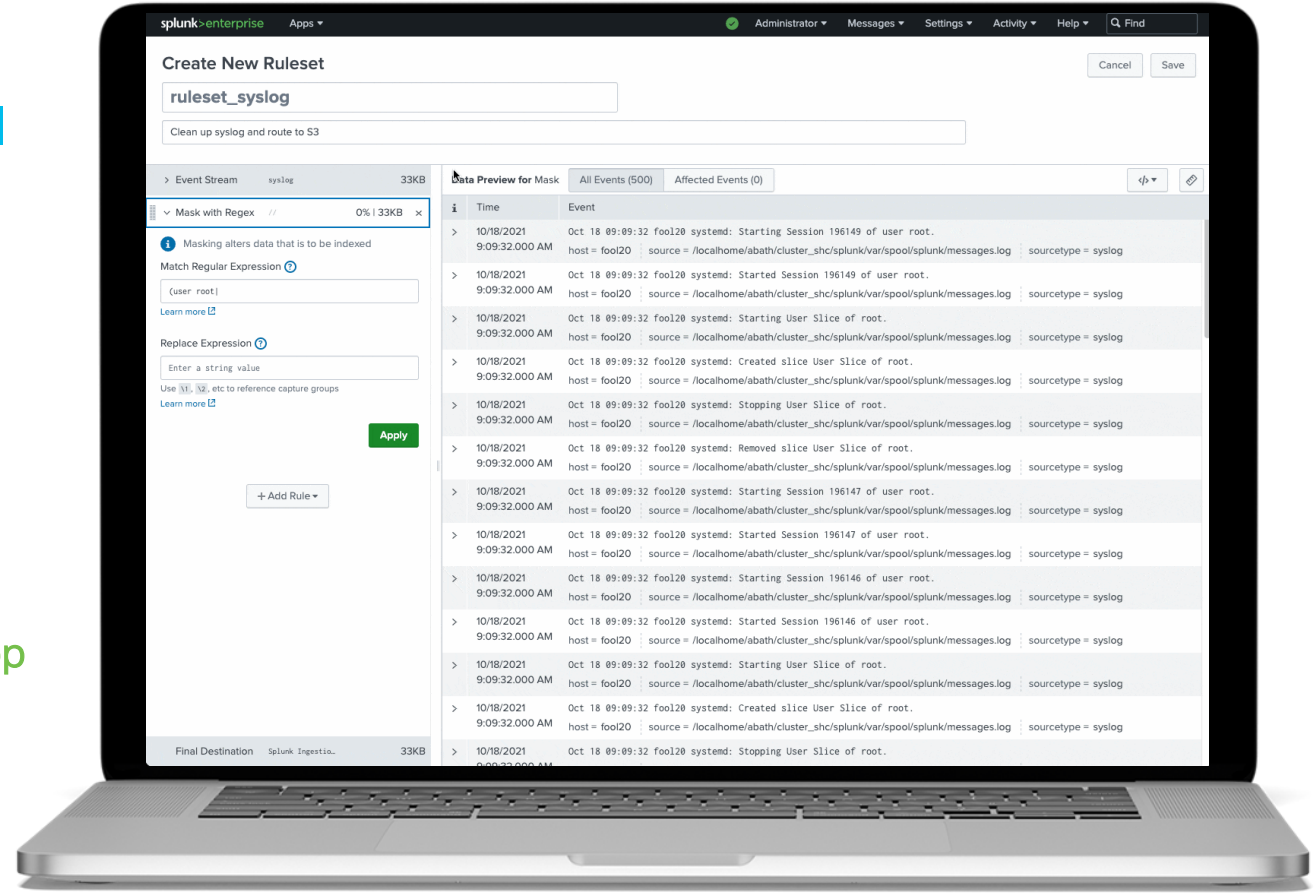
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ingest Actions

Transform & Control Your Data



→Mask
→Filter & Drop
→Enrich
→Route
(Splunk, 3rd parties)

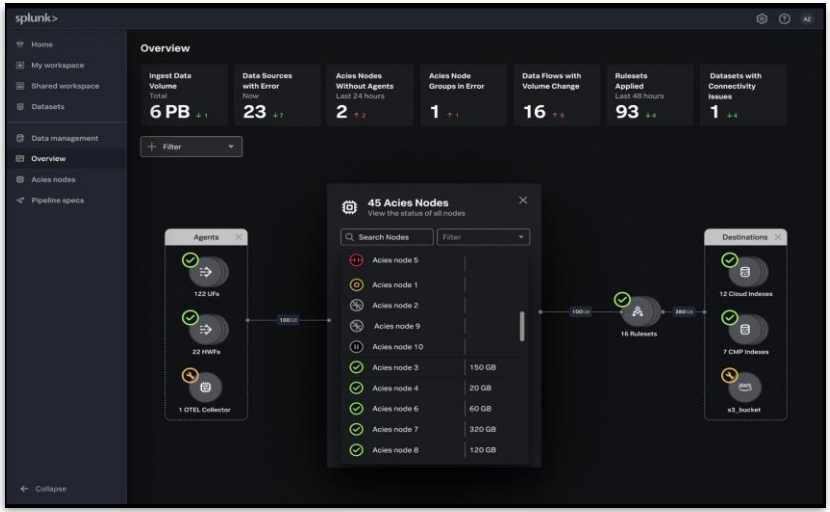


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Edge Processor

Centrally managed next-generation data processor at the Edge.

- Customer-managed edge instances for ingest processing -Single command line deployment on hosts of your choice
- Cloud-based control plane for simple authoring and pipeline deployment
- Easy to author data processing **pipelines** with data preview
- Visibility of inbound and outbound streams, with metrics
- Serves as "Intermediate Forwarding Tier" for customers who need ingest processing at the edge



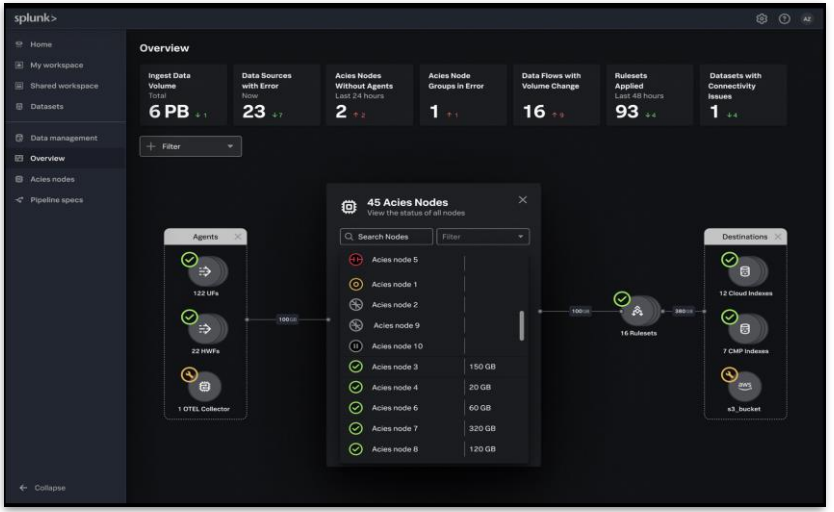
- Available to Splunk Cloud customers and supports both Cloud and Enterprise deployments
- Supported processing: filter, enrichment, transform, drop & routing
- Supported data sources: UF/HWF, HEC, Syslog
- Supported destinations: Splunk® Cloud Platform, Splunk® Enterprise, Amazon S3

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ingest Processor

Fully-managed next generation data processor

- Send data directly to Ingest Processor service.
- Easy to author data processing **pipelines** with data preview
- Visibility of inbound and outbound streams, with metrics



- Available to Splunk Cloud customers and supports Cloud deployments
- Supported processing: filter, enrichment, transform, drop & routing
- Supported data sources: UF/HWF, HEC, Syslog
- Supported destinations: Splunk® Cloud Platform, Splunk® Enterprise, Amazon S3

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data indexing.

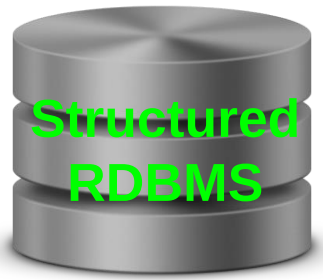
Splunk Approach to Machine Data

Traditional

Schema at Write

SQL

ETL



Splunk

Schema at Read

Search

Universal Indexing

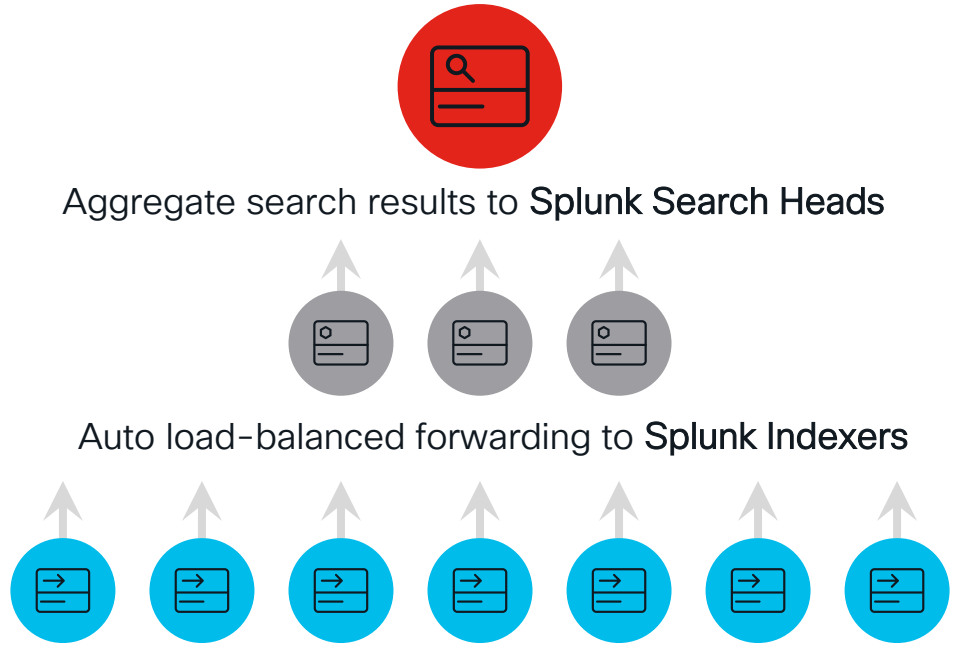
Unstructured & Structured

Volume Variety

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

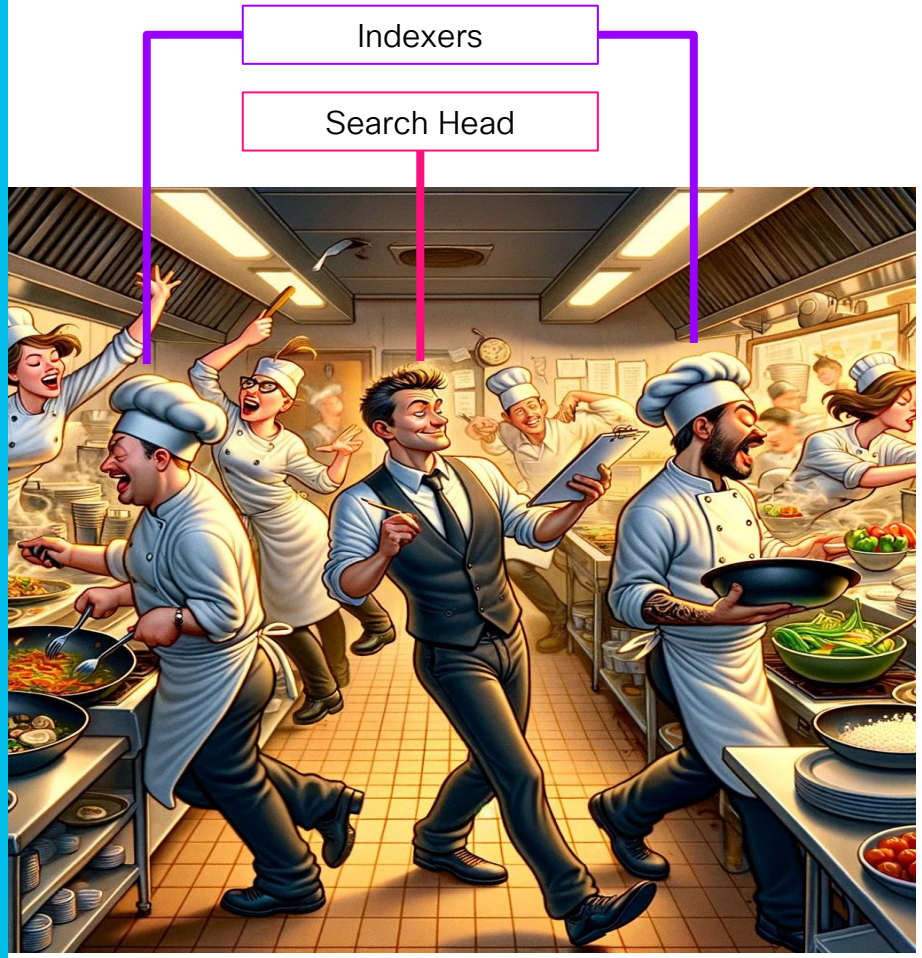
Scales to PBs/Day

Enterprise-Class Scale, Resilience and Interoperability



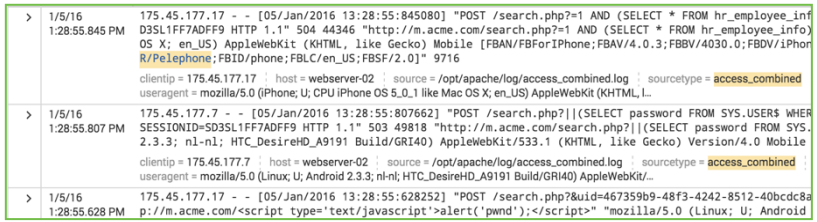
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Recipe to scale cooking process



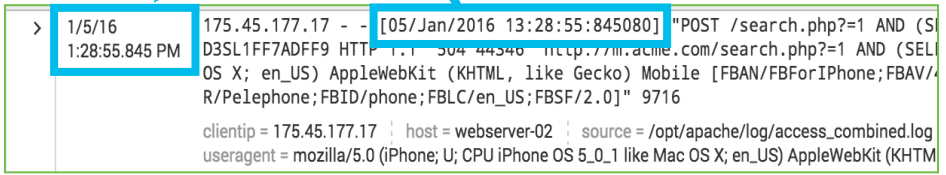
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Inside Universal Indexing

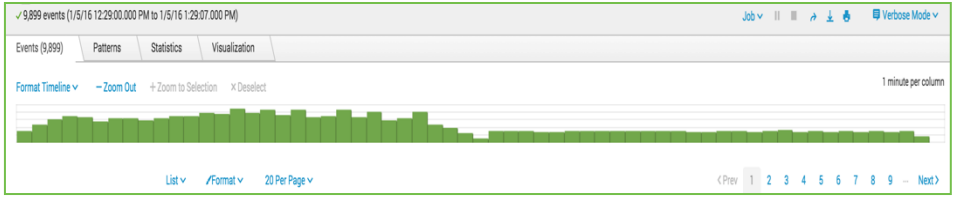


Automatic event boundary identification

Automatic timestamp normalization

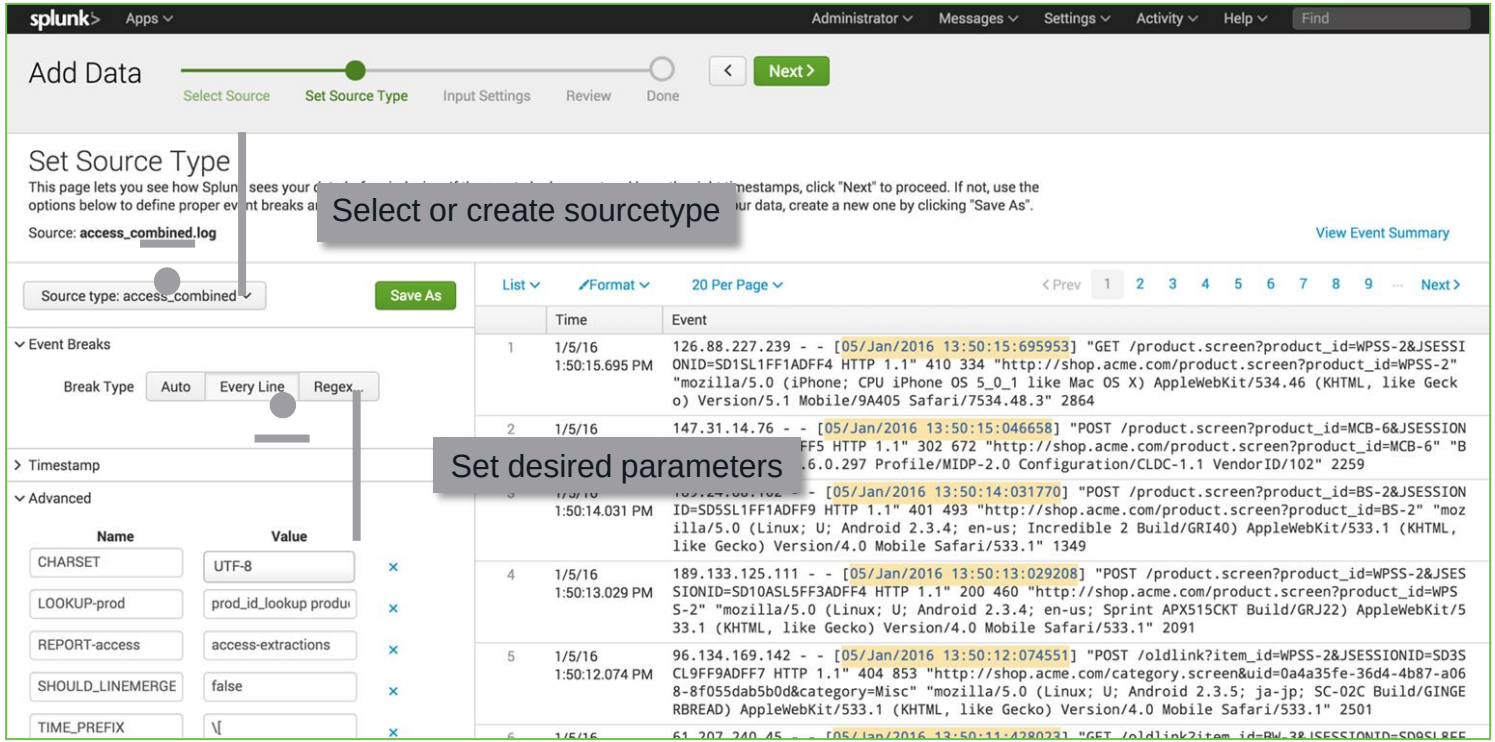


Accurate searching and trending by time across all data



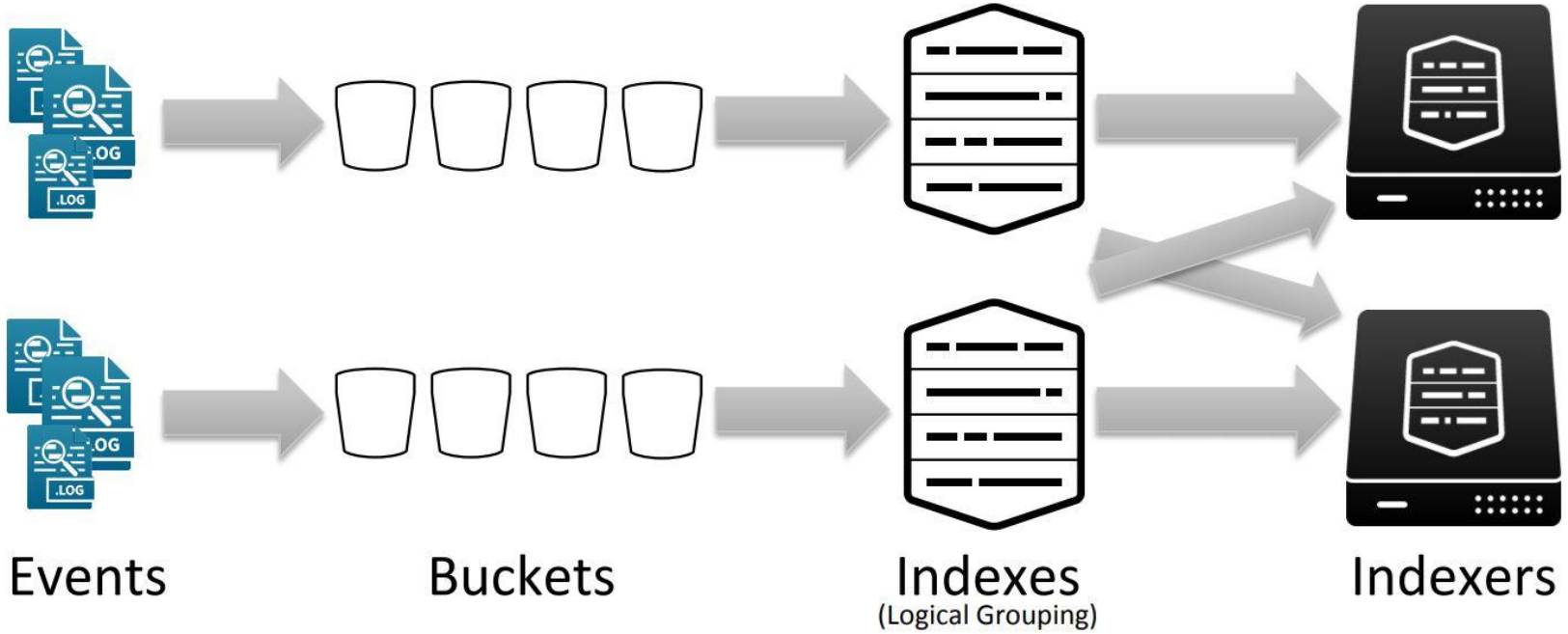
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data Onboarding



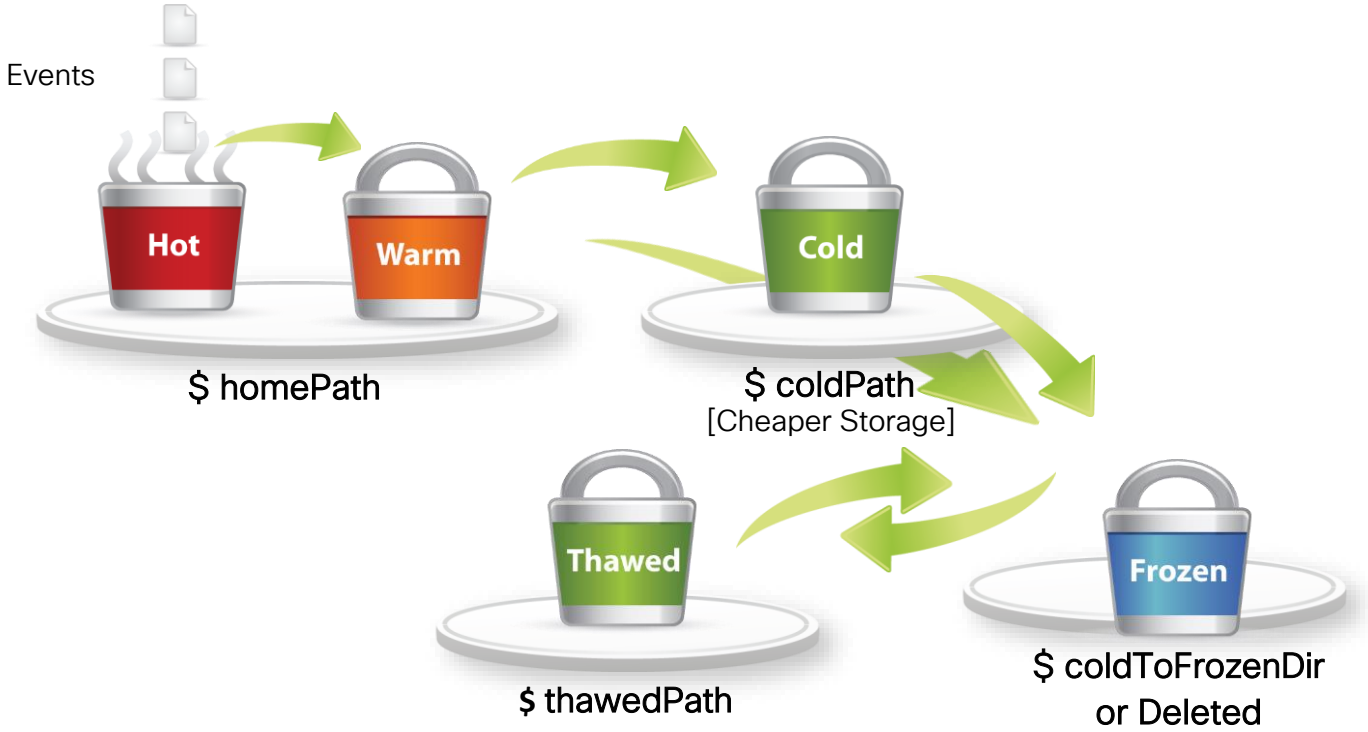
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How Splunk Stores Data



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk Storage : Bucket States

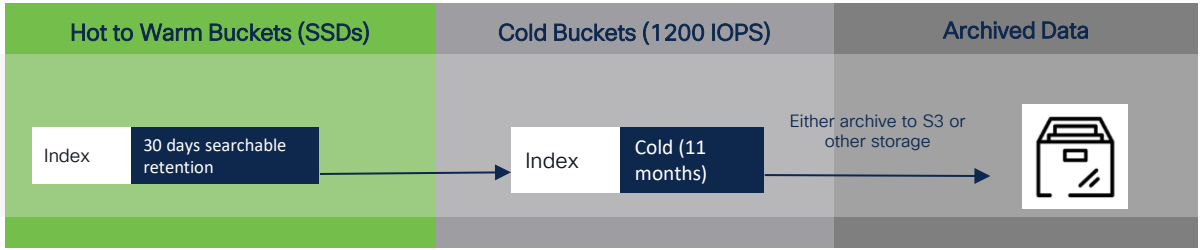


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk Storage Example

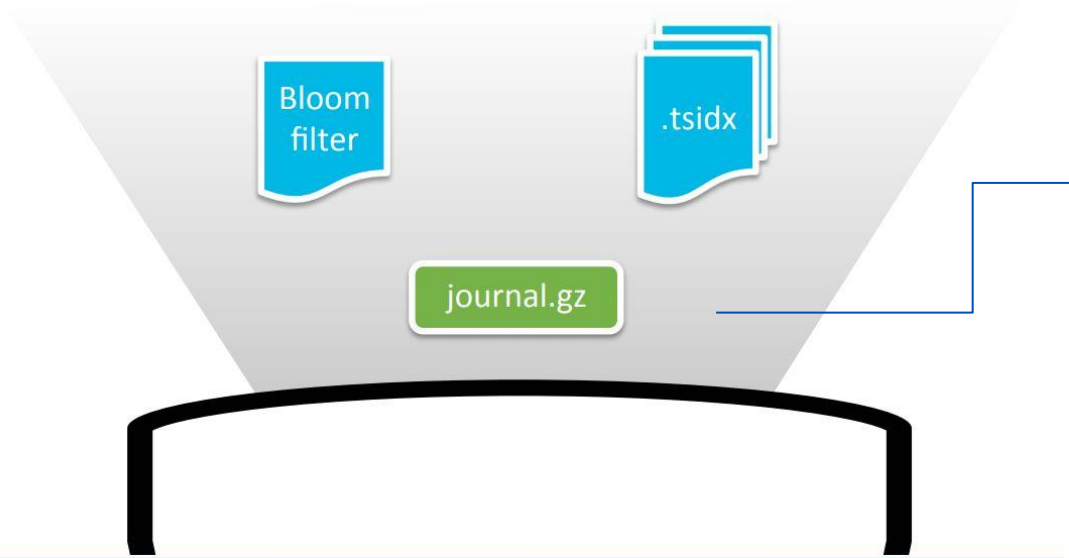
Index Configuration:

- 365 days total
- 30 days hot/warm
- Rest cold for 11 months, archive afterwards



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is in a Bucket



- Your events go here
- Journal.gz is made up of many smaller compressed slices
- Raw data is collected and saved into slices
  - ~128kb of uncompressed data make up a slice.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

TSIDX

Time Series Index (C++)

- Inverted index optimized for time
- Two basic components
  - Lexicon
  - Arrays of information about events

Why: Given a time range and query, where's my matching data?

Raw Events
Jim likes Mickey
Suzie likes Donald
Pat likes Pluto

Unique terms from the raw events are written to the lexicon

Lexicon

Term	Postings List
Donald	1
Jim	0
likes	0,1,2
Mickey	0
Pat	2
Pluto	2
Suzie	1

The postings list tells us where we can find a specific term in the values array

Values Array

Posting Value	Seek Address
0	34
1	87
2	132

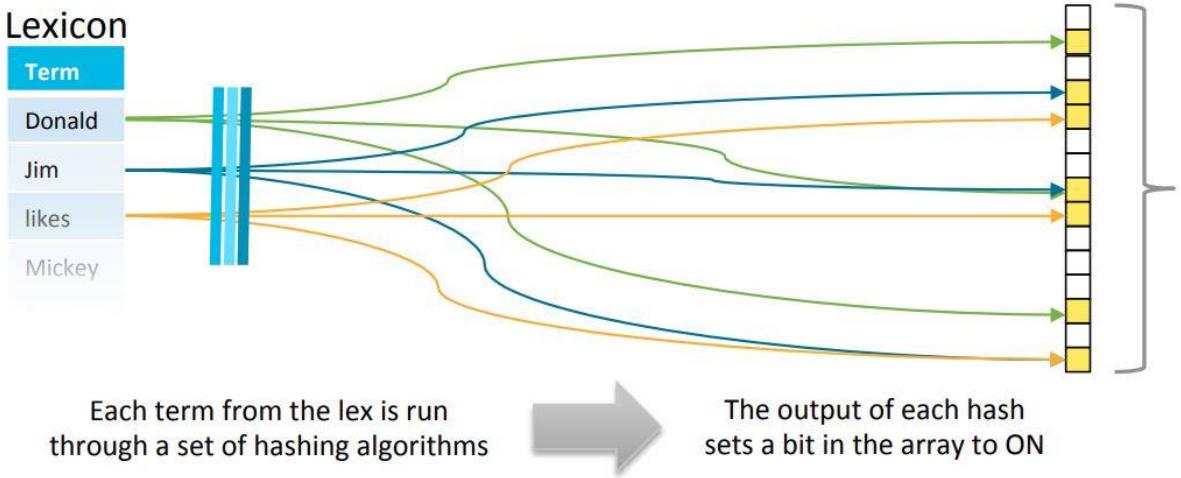
The seek address tells us where we can find the matching event(s) in the journal.gz slices

*The overall structure of a TSIDX file has been simplified for illustrative purposes

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

TSIDX : Bloom Filters
Needle in a haystack

- Determines whether a term is likely to exist in the TSIDX of a bucket
  - False positives are possible, false negatives are not

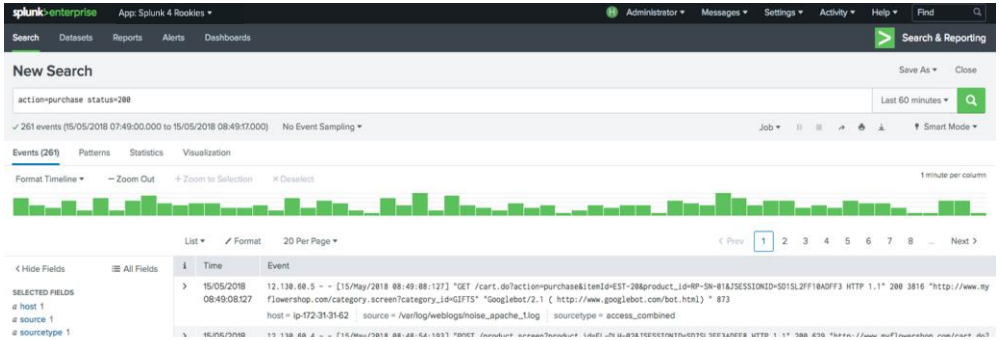


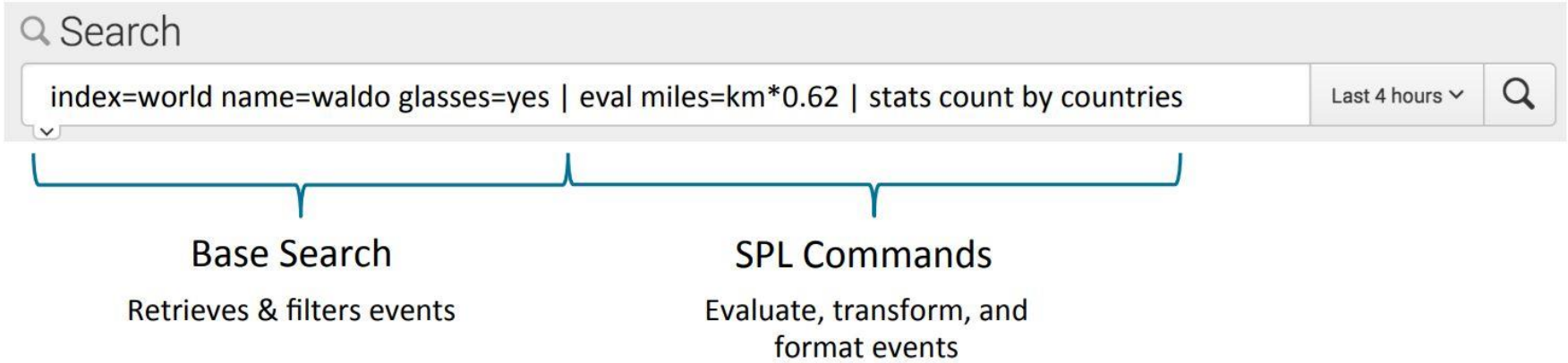
- Regardless of the # of terms, bit array size remains fixed
- Binary format
- Fast to read vs. TSIDX, which grows with more unique terms

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Searching, alerting, reporting.

How Search Works



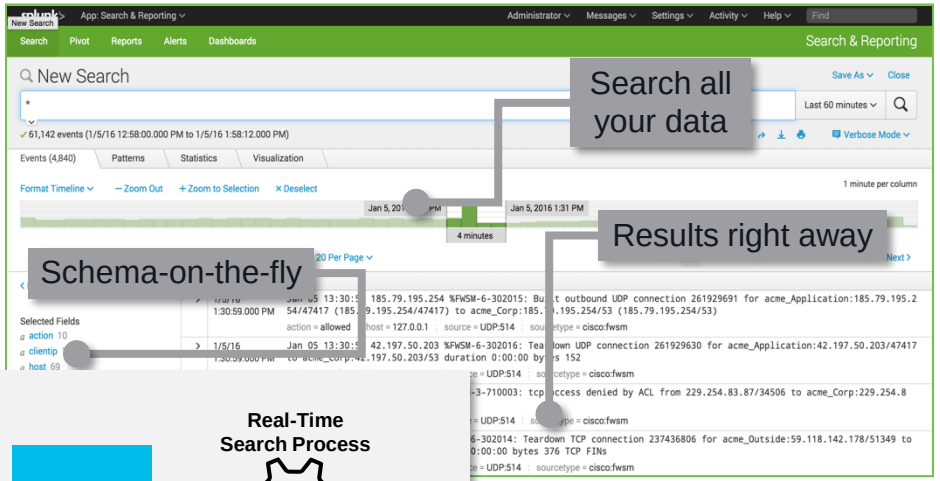


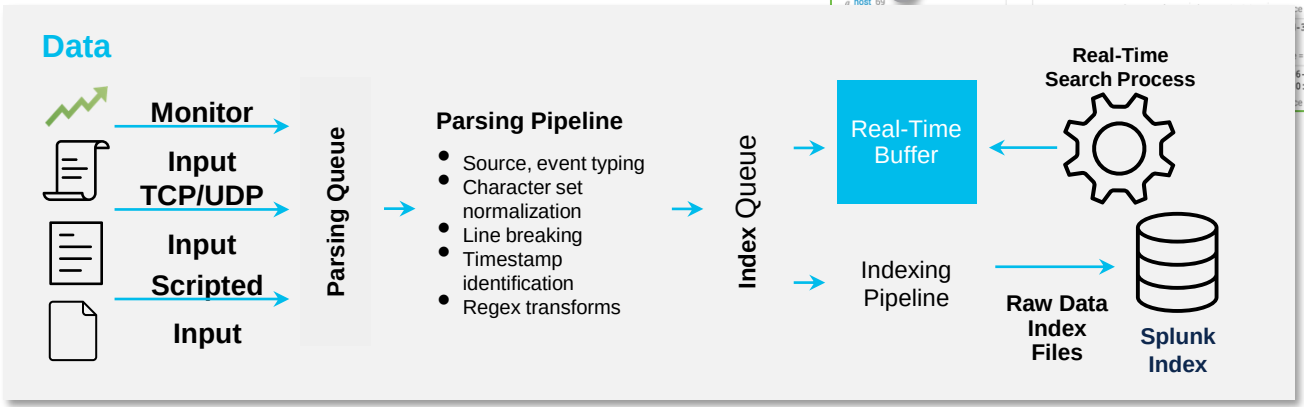
Events are retrieved → Results move linearly through SPL commands

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Search All Your Machine Data

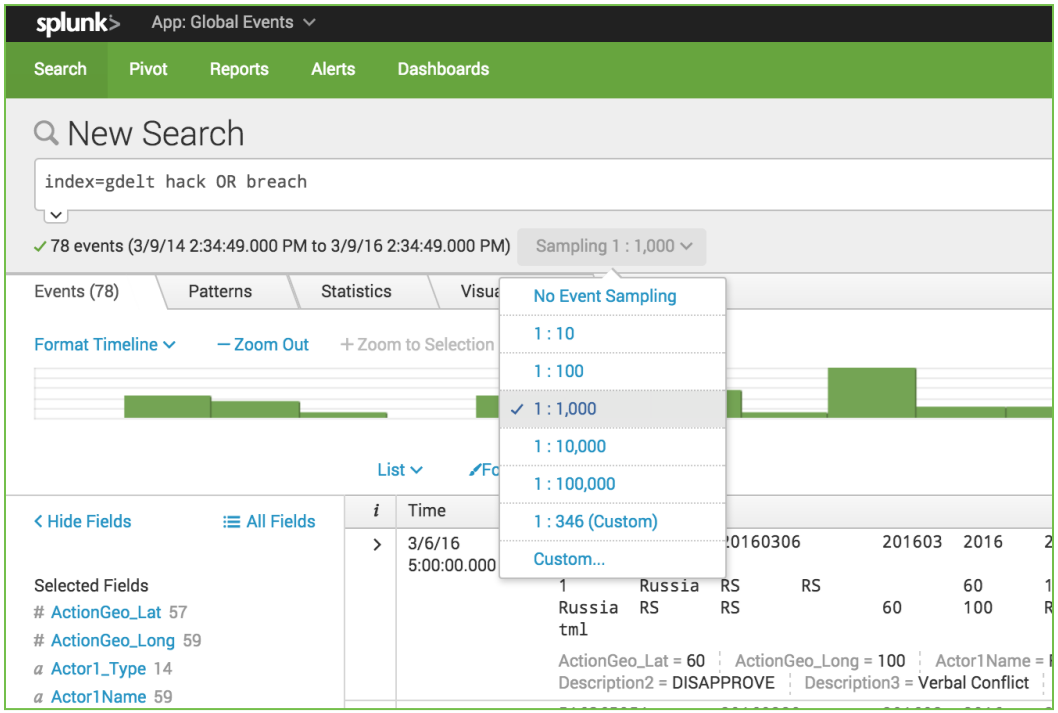
- Real-time and historical data on-premises, in the cloud or both
- Over 200 commands including anomaly detection and machine learning





© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

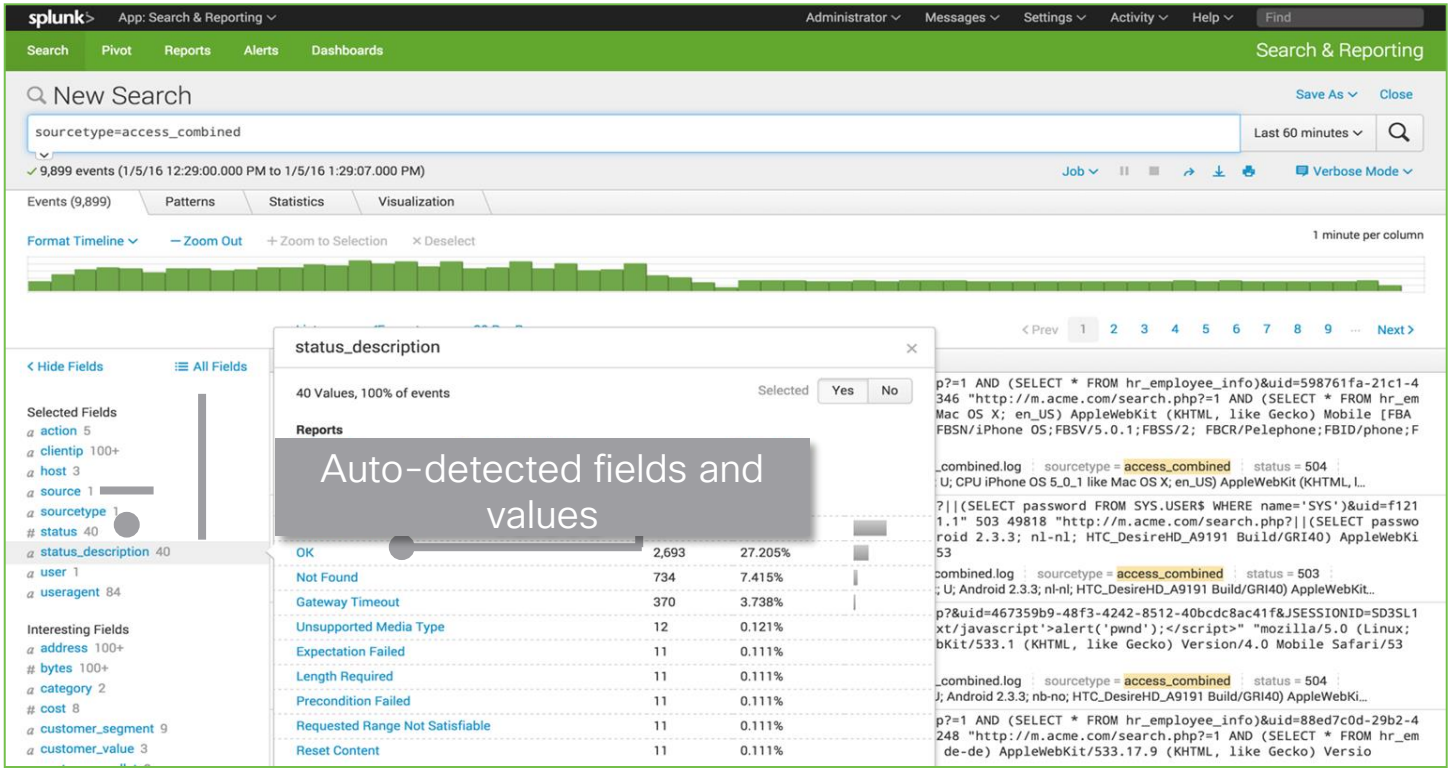
Event Sampling



- Sample Random Events
  - Powerful search option provides unbiased sample results
  - Useful to quickly determine dataset characteristics
  - Speeds large-scale data investigation and discovery

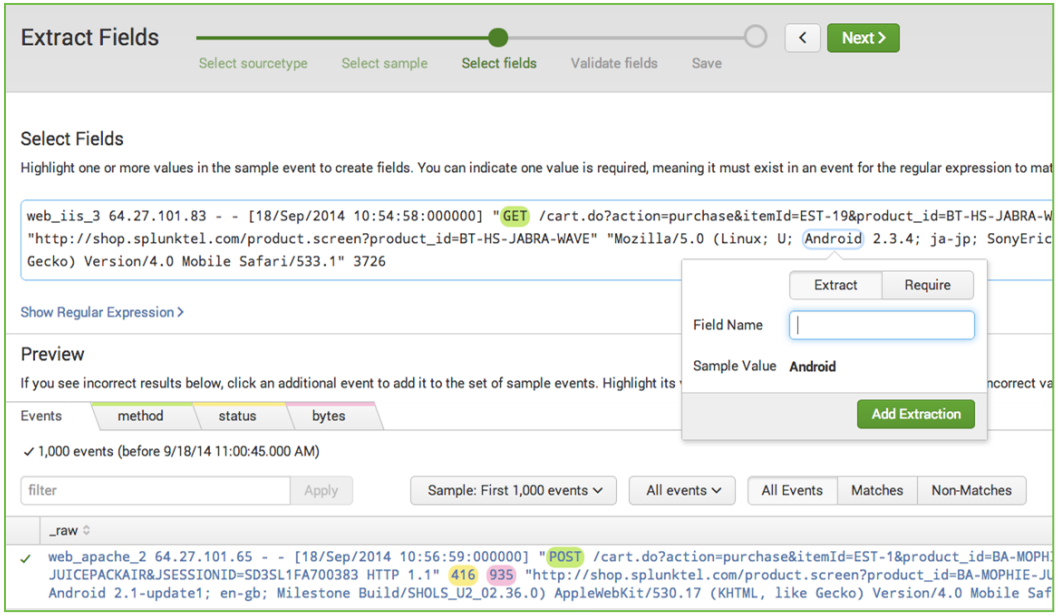
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Schema-on-the-Fly



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Extract Fields Anytime

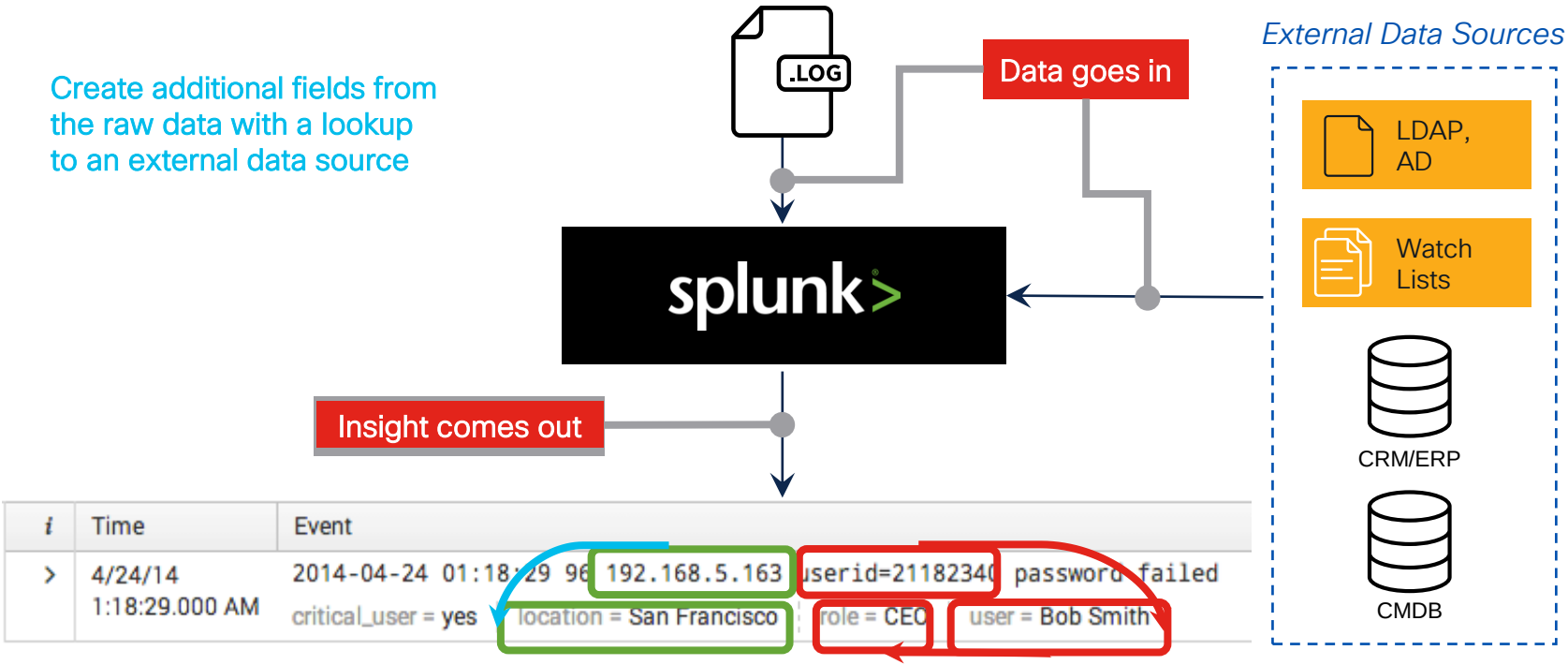


- Simple field extraction
  - Highlight-to-extract multiple fields at once
  - Apply keyword search filters
  - Specify required text in extractions
  - View diverse and rare events
  - Validate extracted values with field stats

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enrich Raw Data to Make It More Meaningful

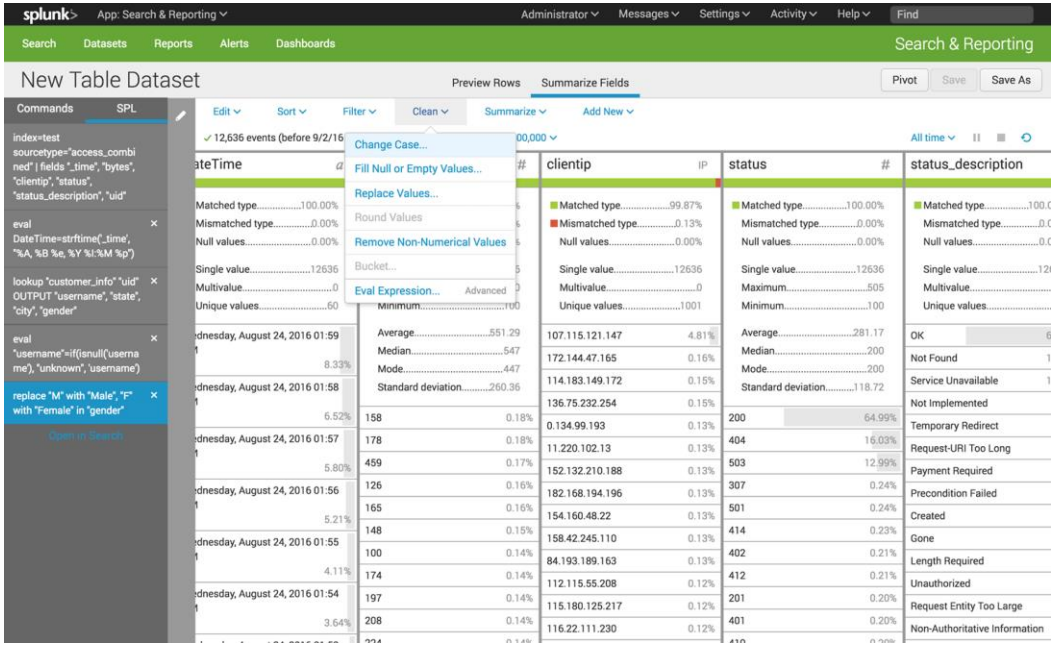
Create additional fields from the raw data with a lookup to an external data source



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data Preparation & Analysis With Tables

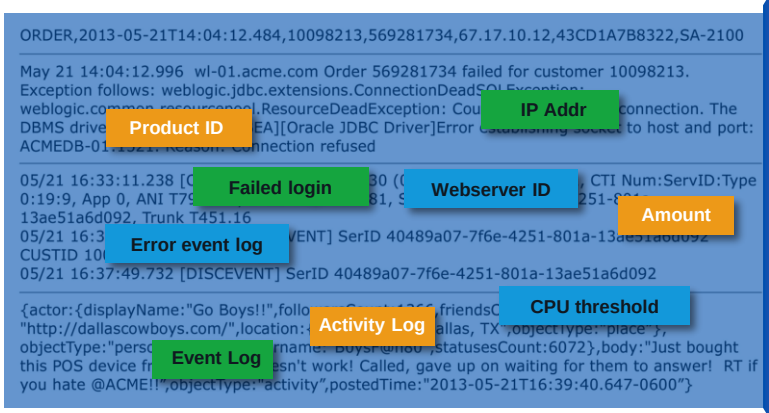
Fast and simple analysis for a wide range of users



- Tabular data views speed analysis for specialist and occasional users
- Intuitive interface to prepare and analyze data without using Splunk Search Processing Language (SPL)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Structured View Into Unstructured Data



IT Ops

Server Name	Uptime %	Avg Response Time	Errors	CPU	Disk
web_bc01	.88	35ms	1	22%	33%
web_bc02	.65	2990ms	43	100%	31%

Business Analytics

Product ID	Number of Orders	Total Sales	Average Checkout time	Avg Site Visit Time	Abandoned Carts	CSAT
Prod A	301	$6622	:45	3:04	301	60
Prod B	450	$10350	:35	2:21	450	70

Security

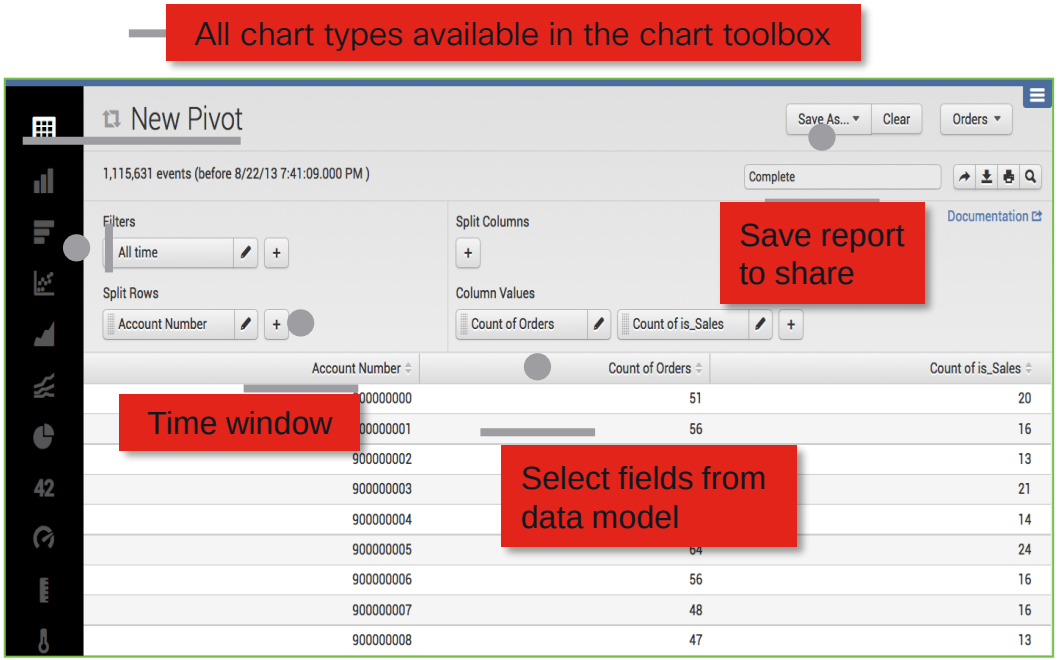
Server Name	IP Addr	Failed Logins	Security Event Logs	Network Activity	Notable Events
web_bc01	67.17.10.12	4	22	Normal	2
web_bc02	67.17.10.13	631	1030	Suspicious	13
web_bc03	67.17.10.14	12	27	Normal	0
prdstg_01	67.17.10.15	0	0	Normal	0
prddb_01	67.17.10.16	1	5	Normal	1

Table Datasets: Empower users with focused data views

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Easy-to-Use Analytics

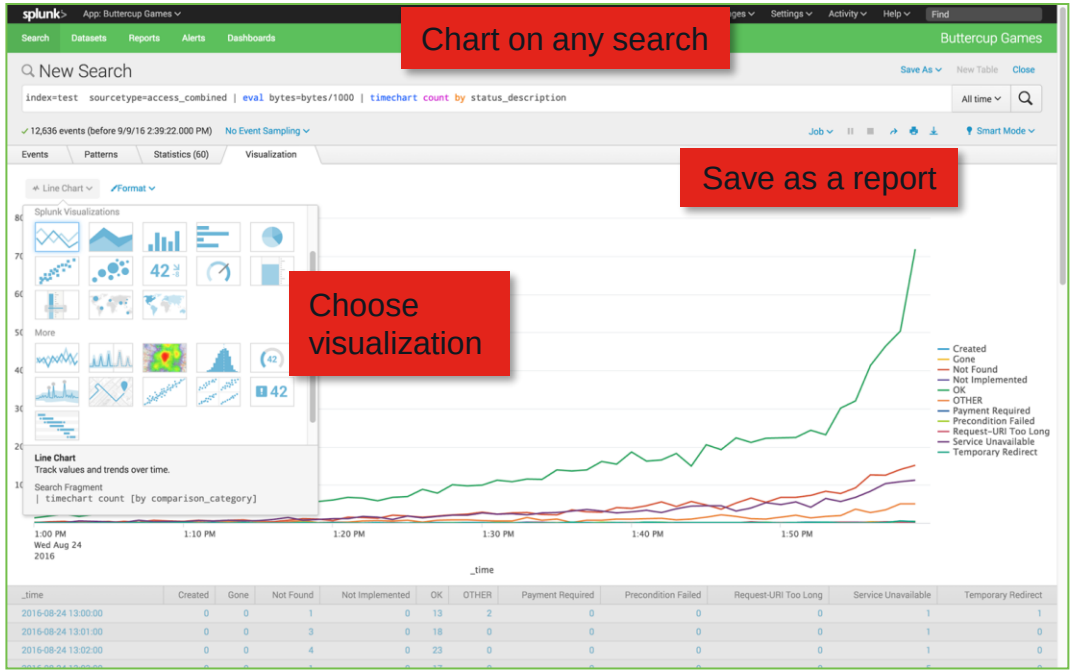
- Pivot
  - Drag-and-drop interface enables any user to analyze data
  - Create complex queries and reports without learning search language
  - Click to visualize any chart type; reports dynamically update when fields change



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

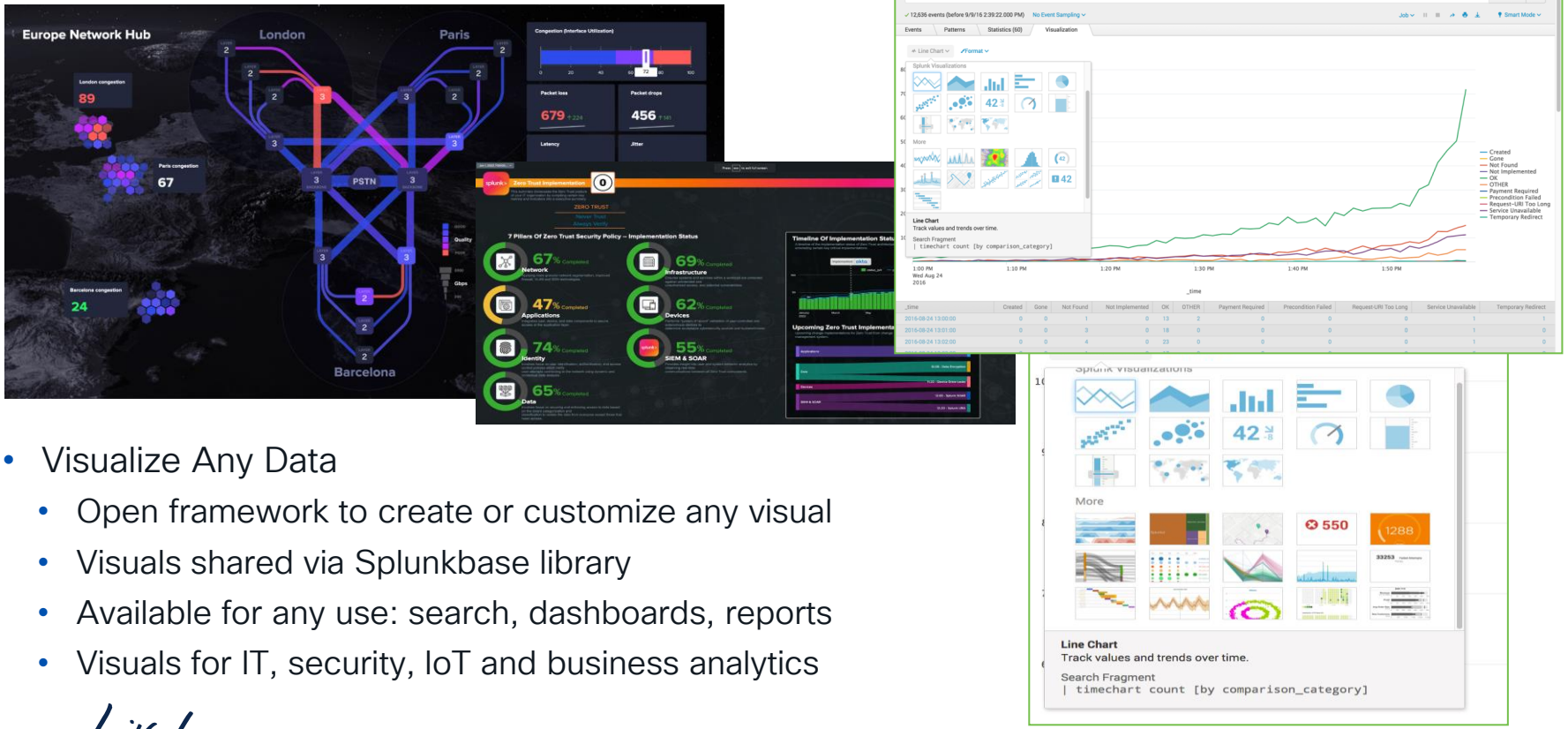
Dynamic Reporting

- Reports
  - Visually represent the results of a search
  - Run on an ad hoc basis or save the report to view later
  - Share it with others on the team or a different group
  - Add reports to a new or existing dashboard



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Reporting & Visualizations



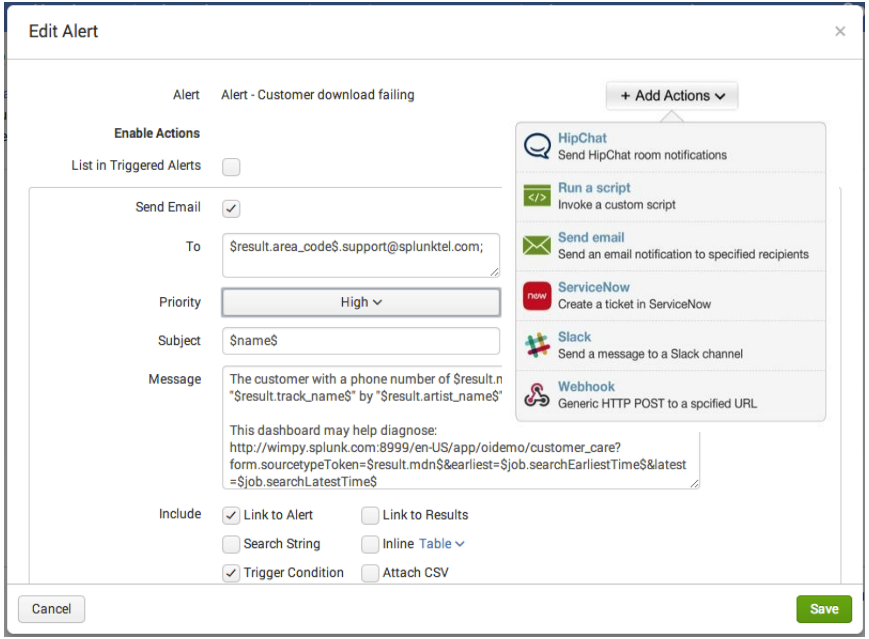
- Visualize Any Data
  - Open framework to create or customize any visual
  - Visuals shared via Splunkbase library
  - Available for any use: search, dashboards, reports
  - Visuals for IT, security, IoT and business analytics

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Actionable Alerting

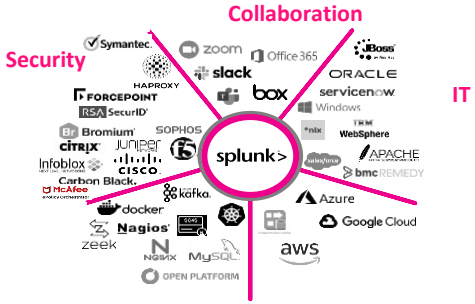
Alerts

- Create alerts based on any search
- Customize content and format of email alerts
- Trigger a script
- Custom Alert Actions
  - Allows packaged integration with third-party applications
  - Enable custom workflows
  - Developers can build, package and publish alert actions



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Apps and Add-ons



Apps	Add-on
A packaged solution containing a collection of knowledge objects and extensions for a specific technology or use case	An App that provides custom configurations or data inputs to support other Splunk apps. (ex. data ingestion and parsing.)

Public Apps

Splunk, Partner, and community developed Apps and TAs offered for community reuse*.

- Splunkbase apps vetted via App Inspect

Splunkbase

- 1,000+ Splunk Cloud Certified Public apps
- Splunk 1st-Party Apps are already vetted

Splunk Admin

App Inspect

Splunk AppInspect service automatically checks for security compliance of Splunk Apps

Private Apps

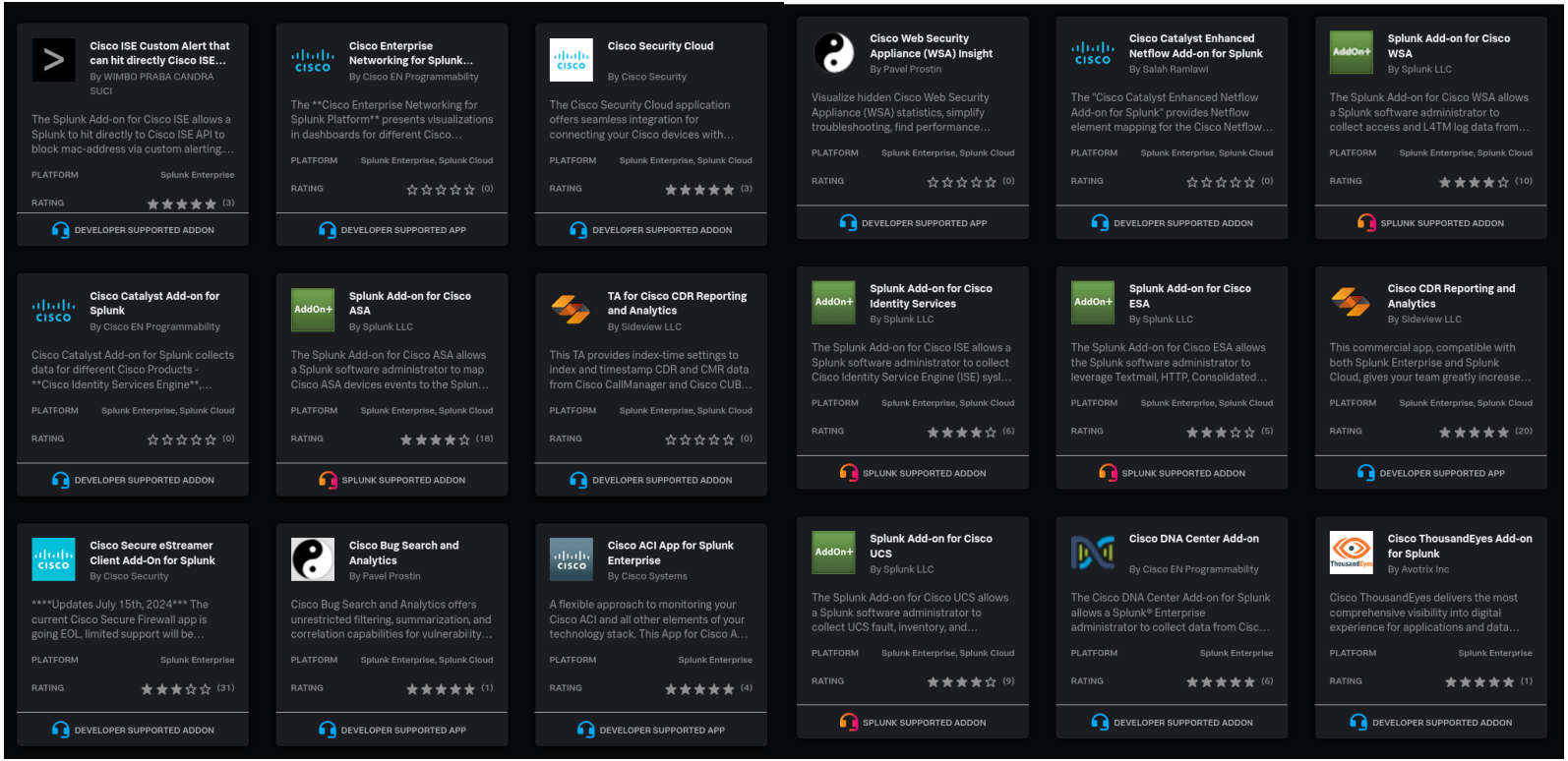
Customer developed Apps and TAs private to your organization.

- Private apps installed via Splunk Cloud UI or Admin Config Service (ACS)

* Some Apps are offered as part of paid offerings.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

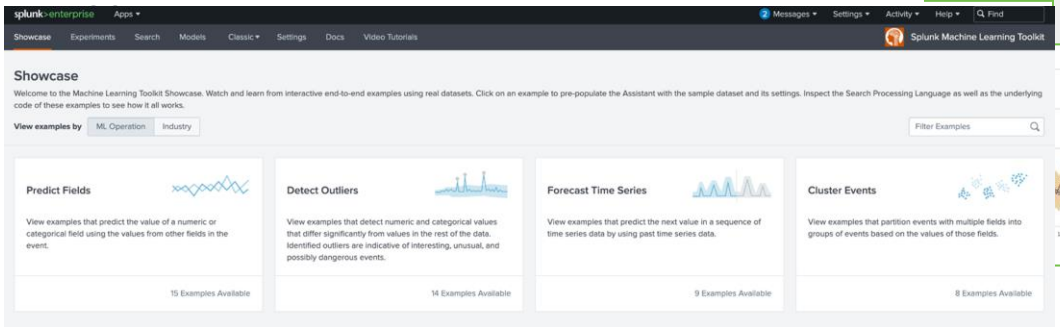
Cisco Apps

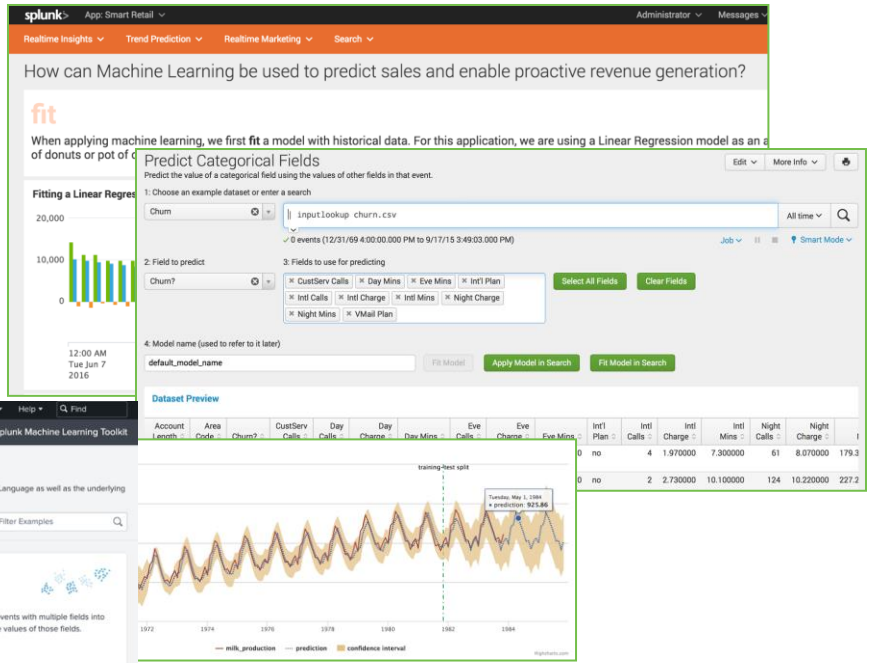


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk Machine Learning Toolkit

- **Assistants:** Guide model building, testing & deployment for common objectives
- **Showcases:** Interactive examples for typical IT, security, business, IoT use cases
- **SPL ML Commands:** New commands to fit, test and operationalize models
- **Python for Scientific Computing Library:** 300+ open source algorithms available for





Build custom analytics for any use case

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco Live!

Keynote Deep Dives

Wednesday
10:30am –11:30am

Experiences Amplified: How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106

Smart, Secure, Seamless: Transforming Experiences with Next-Generation Networking

Level 2
Room 204

Harness a Bold New Era: Transform Data Centre and Service Provider Connectivity

Level 2
Room 203

Securing User to Application and Everything in Between

Level 2
Melbourne Room 2

Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

Complete your surveys in the **Cisco Live mobile app**.

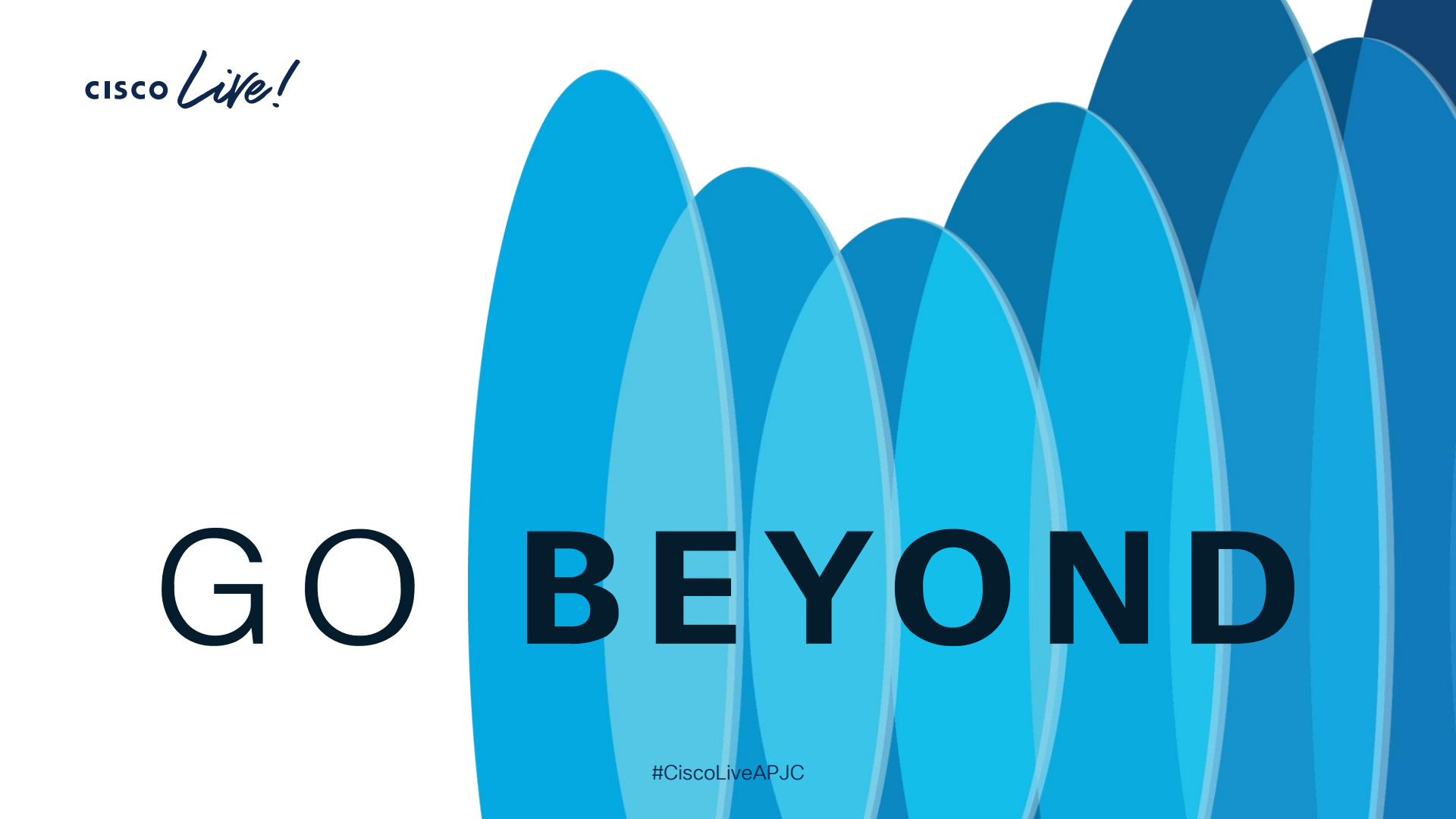
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC