



splunk®

What's New in Splunk Enterprise and Splunk Cloud

Todd Untrecht | VP Product Management

October 2, 2018

Action Packed Session



Live Demos



Audience Challenges



Learn More “Pop Outs”

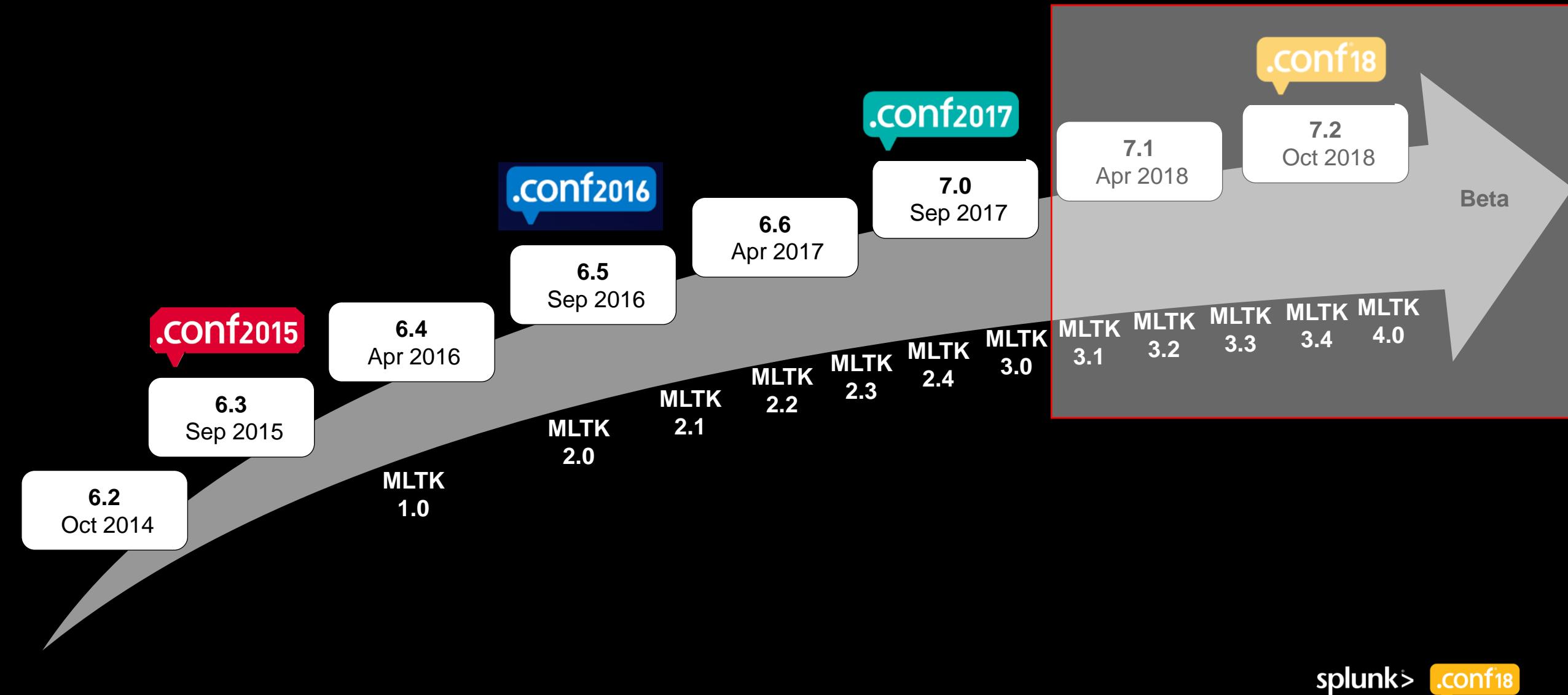
Forward-Looking Statements

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. © 2018 Splunk Inc. All rights reserved.

Splunk Enterprise Releases

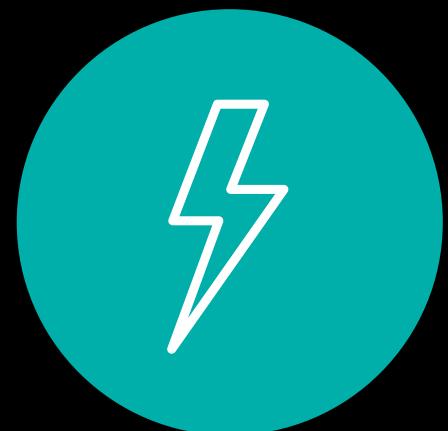




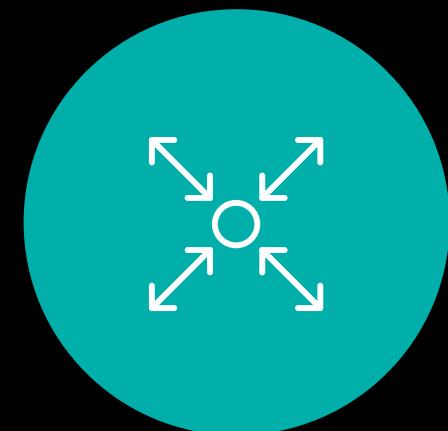
Artificial intelligence and machine learning integrated throughout platform



Limitless exploration and investigation



Leadership in performance, scale and manageability



Splunk and expansive ecosystem

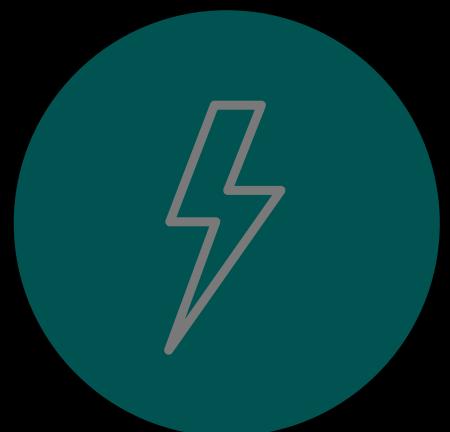
Solve problems faster

Grow more easily

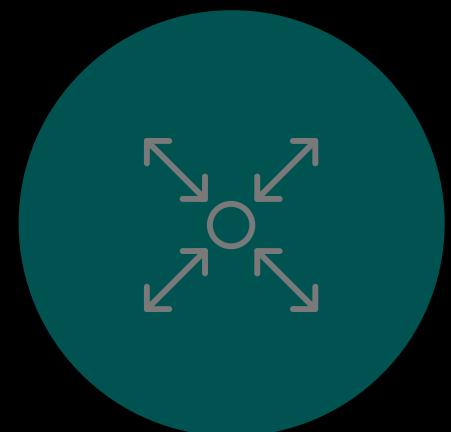
Leverage more data



Limitless exploration and investigation



Leadership in performance, scale and manageability



Splunk and expansive ecosystem

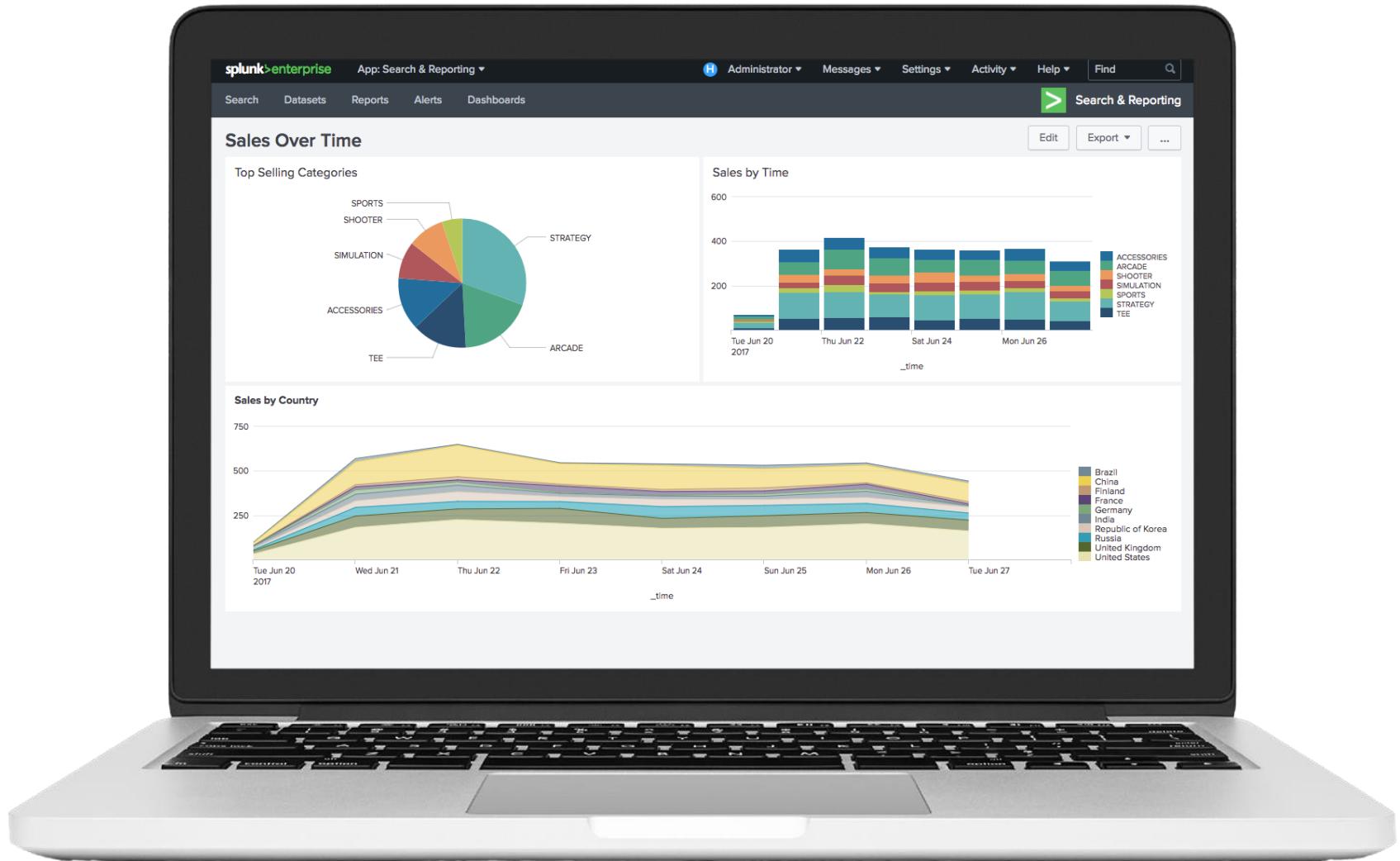
Solve problems faster

Visual Refresh

Modernized user interface

Refreshed User Interface

Crisp and consistent UI spanning Splunk products and Splunk.com



7.1

Increased Legibility to Events

Old

Search & Reporting

New Search
index=_internal | head 100

Events (100) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 100 milliseconds per column

List ▾ Format ▾ 20 Per Page ▾

Time	Event
6/12/16 2:32:04.297 PM	2016-06-12 14:32:04,297 ERROR pid=31059 tid=MainThread file=csv_parser.py:_get_stanza_filename_map:252 Unknown exception when locating lookup table file for a CSV threatlist stanza. stanza="fb-tx_file_intel" Traceback (most recent call last): File "/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/bin/parsers/csv_parser.py", line 246, in _get_stanza_filename_map transform_name = transform_rx.findall(content['url'])[0] IndexError: list index out of range host = soln-esnightly4.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager
6/12/16 2:32:04.184 PM	2016-06-12 14:32:04,184 INFO pid=31065 tid=MainThread file=app_permissions_manager.py:run:313 status="exitin g" exit_status="0" host = soln-esnightly4.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/app_permissions_manager.log sourcetype = app_permissions_manager
6/12/16 2:32:04.184 PM	2016-06-12 14:32:04,184 INFO pid=31065 tid=MainThread file=app_permissions_manager.py:run:295 No permissions changes needed. host = soln-esnightly4.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/app_permissions_manager.log sourcetype = app_permissions_manager
6/12/16 2:32:04.184 PM	2016-06-12 14:32:04,184 INFO pid=31065 tid=MainThread file=app_permissions_manager.py:detect_changes:149 status="No app_permissions.conf changes detected" host = soln-esnightly4.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/app_permissions_manager.log sourcetype = app_permissions_manager
6/12/16 2:32:04.129 PM	2016-06-12 14:32:04,129 INFO pid=31077 tid=MainThread file=__init__.py:execute:927 Execute called host = soln-esnightly4.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/python_modular_input.log sourcetype = python_modular_input
6/12/16 2:32:04.077 PM	2016-06-12 14:32:04,077 INFO pid=31065 tid=MainThread file=app_permissions_manager.py:get_updated_apps:98 Excluding imported_apps which are disabled: set(['SA-UEBA']) host = soln-esnightly4.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/app_permissions_manager.log sourcetype = app_permissions_manager
6/12/16 2:32:04.069 PM	2016-06-12 14:32:04,069 WARNING module='Timer' sample='linux.diskio': Generator Queue Full, looping host = soln-esnightly4.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/eventgen.log sourcetype = eventgen
6/12/16 2:32:04.042 PM	2016-06-12 14:32:04,042 INFO pid=31065 tid=MainThread file=app_permissions_manager.py:run:209 status="retrieved_checkpoint_data" task="merged" host = soln-esnightly4.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/app_permissions_manager.log sourcetype = app_permissions_manager

Selected Fields
a host 1
a source 8
a sourcetype 8

Interesting Fields
a alert_actions 1
a app 9
a bytes 37
a clientip 2
a component 1
date_hour 1
date_mday 1
date_minute 1
date_month 1
date_second 4
a date_wday 1
date_year 1
a date_zone 2
digest_mode 1
dispatch_time 5
a events 1
a eventtype 5
a file 17
a host_is_expected 1
a host_pci_domain 1
a host_requires_av 1
a host_should_timesync 1
a host_should_update 1
idm_flags 2
a index 1
a level 2
linecount 1
a message 15
a module 2
a punct 16
a sample 35
a splunk_server 1
a status 4

New

enterprise App: Search & Reporting

New Search
index=_internal | head 100

Events (100) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 100 milliseconds per column

List ▾ Format ▾ 20 Per Page ▾

Time	Event
6/12/16 2:36:12.245 PM	2016-06-12 14:36:12,245 WARNING module='Timer' sample='oracle_incident': Generator Queue Full, looping host = soln-esnightly2.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/eventgen.log sourcetype = eventgen
6/12/16 2:36:12.166 PM	2016-06-12 14:36:12,166 WARNING module='Timer' sample='linux.diskio': Generator Queue Full, looping host = soln-esnightly2.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/eventgen.log sourcetype = eventgen
6/12/16 2:36:12.125 PM	2016-06-12 14:36:12,125 WARNING module='Timer' sample='DeviceControl.sophos': Generator Queue Full, looping host = soln-esnightly2.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/eventgen.log sourcetype = eventgen
6/12/16 2:36:12.081 PM	2016-06-12 14:36:12,081 WARNING module='Timer' sample='oracle_xml_listener': Generator Queue Full, looping host = soln-esnightly2.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/eventgen.log sourcetype = eventgen
6/12/16 2:36:12.022 PM	2016-06-12 14:36:12,022 WARNING module='Timer' sample='smtp_sample.txt': Generator Queue Full, looping host = soln-esnightly2.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/eventgen.log sourcetype = eventgen
6/12/16 2:36:11.962 PM	2016-06-12 14:36:11,962 WARNING module='Timer' sample='Security.680.windows': Generator Queue Full, looping host = soln-esnightly2.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/eventgen.log sourcetype = eventgen
6/12/16 2:36:11.960 PM	2016-06-12 14:36:11,960 WARNING module='Timer' sample='bro.ssl.log': Generator Queue Full, looping host = soln-esnightly2.sv.splunk.com source = /usr/local/bamboo/splunk-install/current/var/log/splunk/eventgen.log sourcetype = eventgen

Selected Fields
a host 1
a source 6
a sourcetype 6

Interesting Fields
date_hour 1
date_mday 1
date_minute 1
a date_month 1
date_second 4
a date_wday 1
date_year 1
a date_zone 2
a eventtype 4
a host_is_expected 1
a host_pci_domain 1
a host_requires_av 1
a host_should_timesync 1
a host_should_update 1
idm_flags 2
a index 1
a level 2
linecount 1
a message 15
a module 2
a punct 16
a sample 35
a splunk_server 1
a status 4

7.1

Cleaner Listing Pages

Old

Search & Reporting

Dashboards
Dashboards include searches, visualizations, and input controls that capture and present available data.

82 Dashboards

i	Title ^	Actions	Owner	App	Sharing
>	Access Anomalies	Edit ▾	nobody	DA-ESS-AccessProtection	Global
>	Access Center	Edit ▾	nobody	DA-ESS-AccessProtection	Global
>	Access Search	Edit ▾	nobody	DA-ESS-AccessProtection	Global
>	Access Tracker	Edit ▾	nobody	DA-ESS-AccessProtection	Global
>	Account Management	Edit ▾	nobody	DA-ESS-AccessProtection	Global
>	Asset Center	Edit ▾	nobody	SA-IdentityManagement	Global
>	Bro	Edit ▾	nobody	Splunk_TA_bro	Global
>	Content Profile	Edit ▾	nobody	SplunkEnterpriseSecurity...	Global
>	Create Concept	Edit ▾	nobody	Splunk_SA_ExtremeSear...	Global
>	Create Data-Driven Context	Edit ▾	nobody	Splunk_SA_ExtremeSear...	Global
>	Create User-Defined Context	Edit ▾	nobody	Splunk_SA_ExtremeSear...	Global
>	Data Model Audit	Edit ▾	nobody	Splunk_SA_CIM	Global
>	Data Protection	Edit ▾	nobody	SA-AuditAndDataProtect...	Global
>	Default Account Activity	Edit ▾	nobody	DA-ESS-AccessProtection	Global
>	Discover Trend	Edit ▾	nobody	Splunk_SA_ExtremeSear...	Global
>	Display Concept	Edit ▾	nobody	Splunk_SA_ExtremeSear...	Global
>	Display Context	Edit ▾	nobody	Splunk_SA_ExtremeSear...	Global
>	DNS Activity	Edit ▾	nobody	DA-ESS-NetworkProtecti...	Global
>	DNS Search	Edit ▾	nobody	DA-ESS-NetworkProtecti...	Global
>	Email Activity	Edit ▾	nobody	DA-ESS-NetworkProtecti...	Global
>	Email Search	Edit ▾	nobody	DA-ESS-NetworkProtecti...	Global
>	Endpoint Changes	Edit ▾	nobody	DA-ESS-EndpointProtecti...	Global
>	ES Configuration Health	Edit ▾	nobody	SplunkEnterpriseSecurity...	Global
>	Eventgen Logs	Edit ▾	nobody	SA-Eventgen	Global
>	Eventgen Performance	Edit ▾	nobody	SA-Eventgen	Global
>	Facebook Threat Exchange	Edit ▾	nobody	Splunk_DA-ESS_Faceboo...	Global
>	Find Best Concept	Edit ▾	nobody	Splunk_SA_ExtremeSear...	Global
>	Find Best Concept Via Search	Edit ▾	nobody	Splunk_SA_ExtremeSear...	Global
>	Forwarder Audit	Edit ▾	nobody	SA-AuditAndDataProtect...	Global
>	HTTP Category Analysis	Edit ▾	nobody	DA-ESS-NetworkProtecti...	Global
>	HTTP User Agent Analysis	Edit ▾	nobody	DA-ESS-NetworkProtecti...	Global
>	Identity Center	Edit ▾	nobody	SA-IdentityManagement	Global
>	Incident Review Audit	Edit ▾	nobody	SA-ThreatIntelligence	Global

Create New Dashboard

New

enterprise App: Search & Reporting

Dashboards
Dashboards include searches, visualizations, and input controls that capture and present available data.

111 Dashboards

i	Title ^	Actions	Owner	App	Sharing
>	Access Anomalies	Edit ▾	nobody	DA-ESS-AccessProte...	Global
>	Access Center	Edit ▾	nobody	DA-ESS-AccessProte...	Global
>	Access Search	Edit ▾	nobody	DA-ESS-AccessProte...	Global
>	Access Tracker	Edit ▾	nobody	DA-ESS-AccessProte...	Global
>	Account Management	Edit ▾	nobody	DA-ESS-AccessProte...	Global
>	Anomalous System Uptime	Edit ▾	nobody	Splunk_DA-ESS_PCIC...	Global
>	Asset Center	Edit ▾	nobody	SA-IdentityManagem...	Global
>	Bro	Edit ▾	nobody	Splunk_TA_bro	Global
>	Content Profile	Edit ▾	nobody	SplunkEnterpriseSec...	Global
>	Create Concept	Edit ▾	nobody	Splunk_SA_ExtremeS...	Global
>	Create Data-Driven Context	Edit ▾	nobody	Splunk_SA_ExtremeS...	Global
>	Create User-Defined Context	Edit ▾	nobody	Splunk_SA_ExtremeS...	Global
>	Credit Card Data Found	Edit ▾	nobody	Splunk_DA-ESS_PCIC...	Global
>	Data Model Audit	Edit ▾	nobody	Splunk_SA_CIM	Global
>	Data Protection	Edit ▾	nobody	SA-AuditAndDataProt...	Global
>	Default Account Access	Edit ▾	nobody	Splunk_DA-ESS_PCIC...	Global
>	Default Account Activity	Edit ▾	nobody	DA-ESS-AccessProte...	Global
>	Discover Trend	Edit ▾	nobody	Splunk_SA_ExtremeS...	Global
>	Display Concept	Edit ▾	nobody	Splunk_SA_ExtremeS...	Global
>	Display Context	Edit ▾	nobody	Splunk_SA_ExtremeS...	Global
>	DNS Activity	Edit ▾	nobody	DA-ESS-NetworkProt...	Global
>	DNS Search	Edit ▾	nobody	DA-ESS-NetworkProt...	Global
>	Email Activity	Edit ▾	nobody	DA-ESS-NetworkProt...	Global
>	Email Search	Edit ▾	nobody	DA-ESS-NetworkProt...	Global
>	Endpoint Changes	Edit ▾	nobody	Splunk_DA-ESS_PCIC...	Global

Create New Dashboard

7.2

New Dashboard Dark Mode

Heightens visual contrast; optimized for NOC/SOC environments



The image displays two laptops side-by-side, illustrating the visual difference between the Light Theme and Dark Theme of the Splunk 7.2 dashboard. Both laptops show the 'Game Statistics' dashboard for the 'ButtercupGo' game.

Light Theme (Left Laptop):

- Header:** splunk>enterprise, App: Search & Reporting, Administrator, Messages, Settings, Activity, Help, Find.
- Dashboard Metrics:**
 - Total Games Played: 22,482
 - Average Score: 17
 - Top Score: 101
 - Total Users: 93
- Leaderboard:** A table showing user names, scores, and games played. Top users include e-LOR, Aayla Secura, Admiral Ackbar, Admiral Thrawn, Ahiska Tano, Anakin Solo, Asajj Ventress, Aurra Sing, Barriss Offee, and Bastilla Shan.
- Browser Trend:** A line chart showing the number of games played over time from September 2016 to March 2017. The trend shows a peak in September followed by a decline and then a slight increase towards March.
- Play Times:** A line chart showing play times per day of the week. The chart shows a general upward trend from Friday to Tuesday, with a significant peak on Tuesday.
- Peak Usage Times:** A bubble chart showing usage times across different days of the week. The size of the bubbles indicates the volume of activity, with higher volumes occurring on weekdays.

Dark Theme (Right Laptop):

- Header:** splunk>enterprise, App: Search & Reporting, Administrator, Messages, Settings, Activity, Help, Find, Dark Theme, Edit, Export.
- Dashboard Metrics:**
 - Total Games Played: 22,482
 - Average Score: 17
 - Top Score: 101
 - Total Users: 93
- Leaderboard:** Same data as the Light Theme.
- Browser Trend:** Same data as the Light Theme.
- Play Times:** Same data as the Light Theme.
- Peak Usage Times:** Same data as the Light Theme.

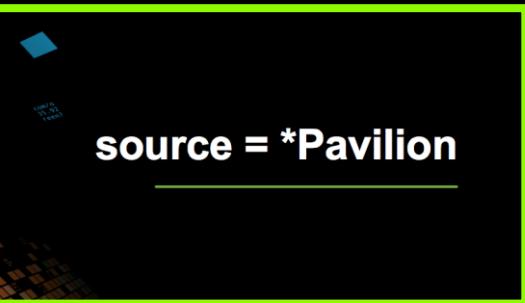
Dashboards Powered by Apple TV

More secure and cost-effective option for SOCs and NOCs

[Learn More](#)

Product and Technology Keynote

Wednesday, October 3, 2018 | 9:00 AM-10:30 AM
ESPN Arena



source = *Pavilion



Accessibility for Users With Disabilities

Section 508 compliance

Splunk Enterprise Accessibility Advances



User Testing for Web Accessibility

- ▶ Hundreds of changes to improve accessibility for users with disabilities
- ▶ Optimized usage for multiple screen reader technologies
- ▶ Updated Voluntary Product Accessibility Template (VPAT) documenting support for Section 508 requirements
- ▶ Integrated into internal release and testing processes

 **Section508.gov**
GSA Government-wide IT Accessibility Program



Play Screen Reader Video

Splunk Metrics Workspace

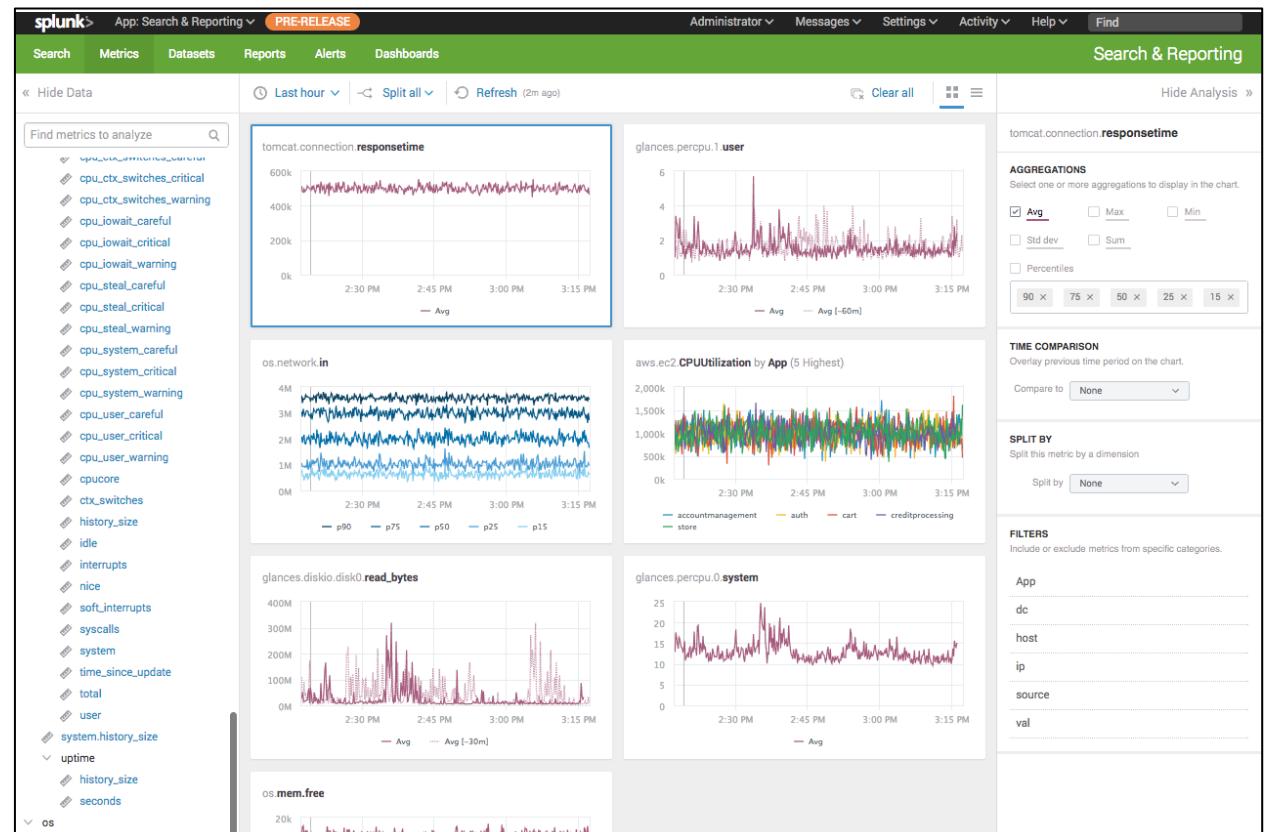
Explore metrics and accelerated datasets without SPL



New Metrics Workspace



- ▶ Query time series from events and metrics in the same environment without SPL
 - ▶ Set up alerts through the UI without writing SPL
 - ▶ Quickly visualize, aggregate and analyze any indexed metric
 - ▶ Support for multiple dimensions allows for easy grouping and filtering



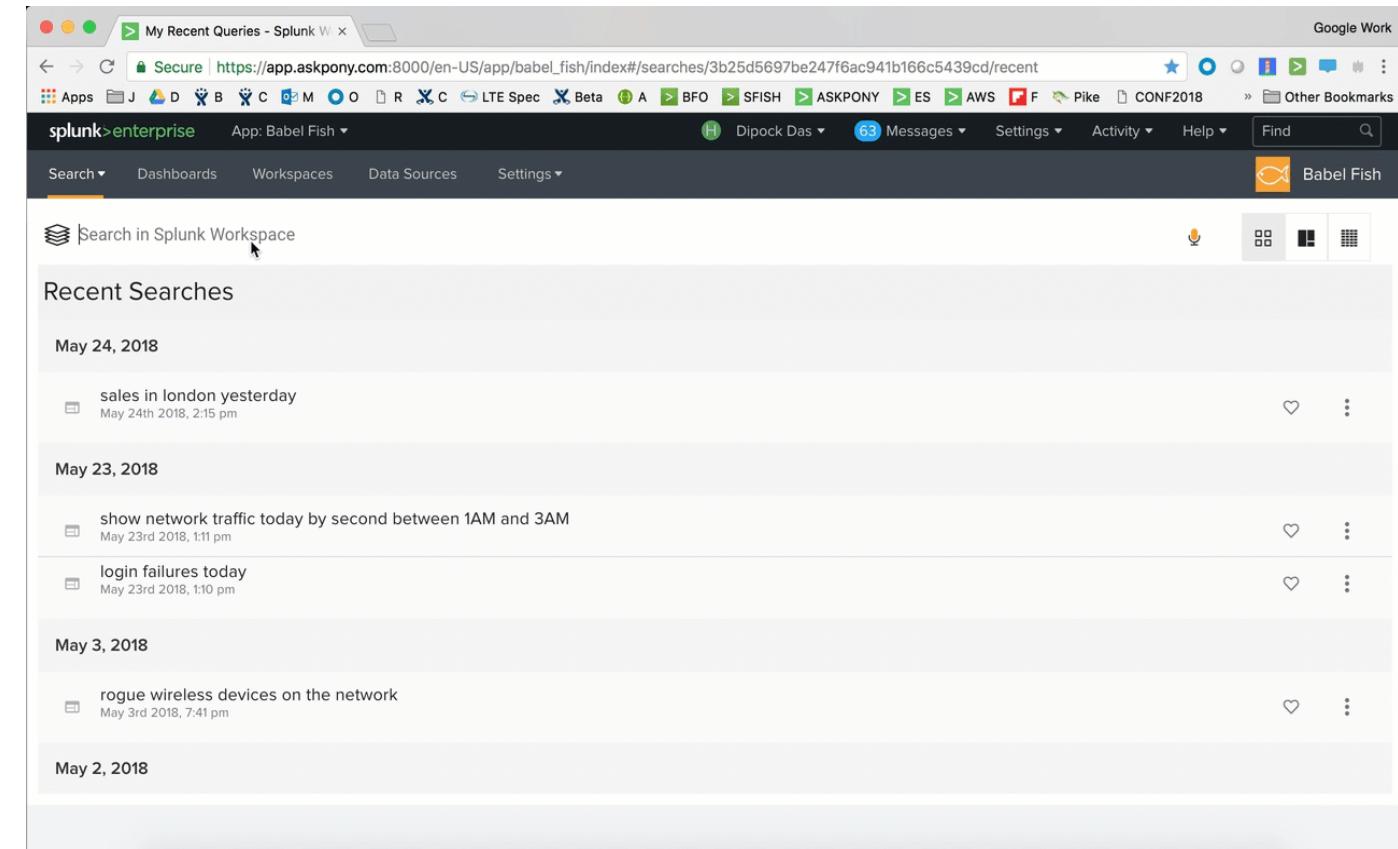
Natural Language Search



Natural Language Processing

Ask Splunk questions using browser, mobile and voice-enabled services

- ▶ Query a system and ask questions of Splunk without knowing SPL
- ▶ Get answers instantly in charts and text without having to format the results
- ▶ Leverage mobile and voice-enabled services



Mobile and Augmented Reality

New Mobile and Augmented Reality Offerings



Rich, actionable
alerts



Augmented
reality

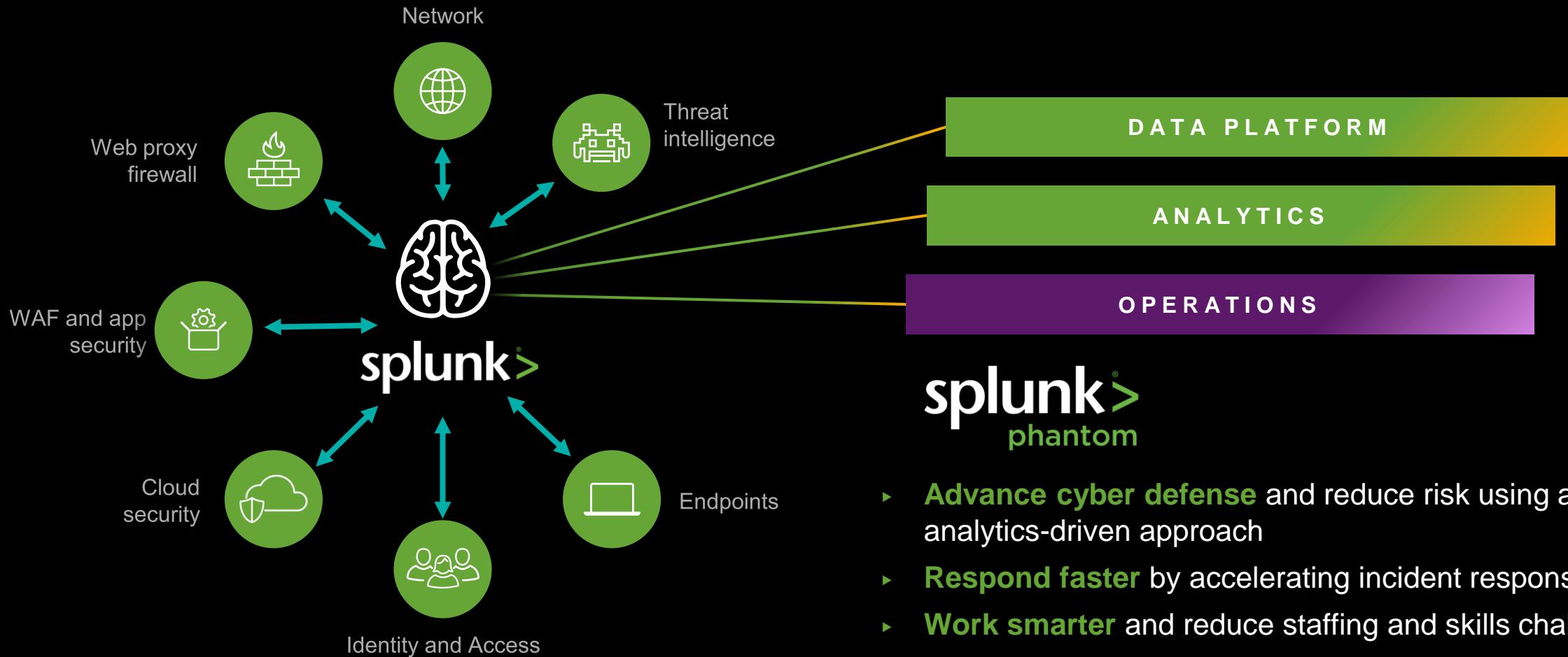
Phantom Integration

Taking action



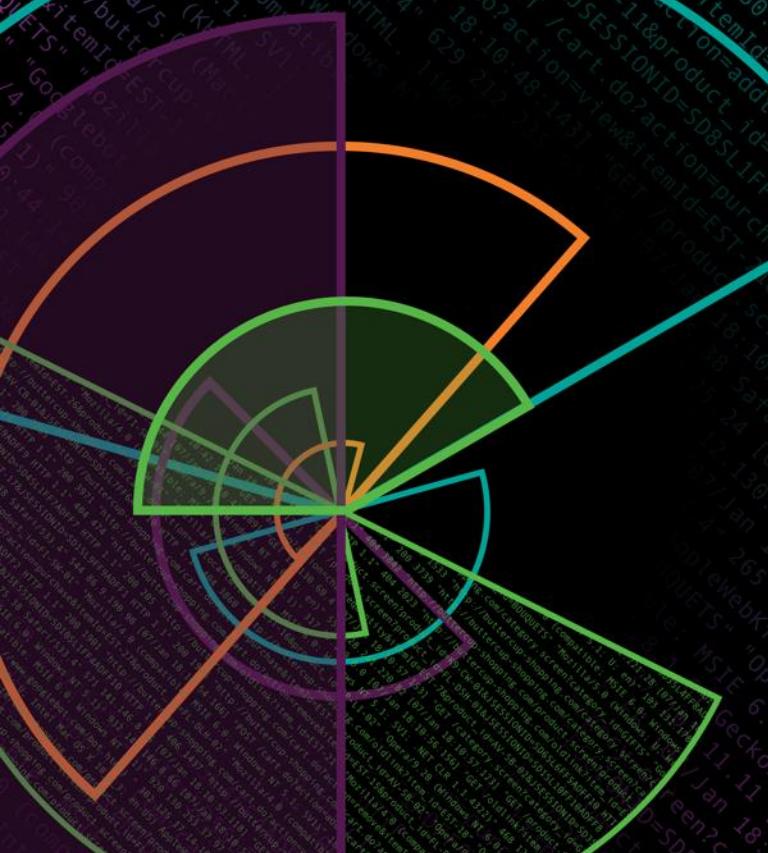
Phantom and Splunk — Unified Vision

How does Phantom help Splunk's nerve center security vision?



VictorOps Integration

Taking action



VictorOps and Splunk

Making on-call suck less



Timeline Reports Settings Help ▾

Customize View ▾ @walterwhite ▾ Greymatter Inc.

People

Teams Users

All Users On-call Engaged Teammates

- Lydia Rodarte-Quayle @lydiarq Production Blue
- Todd Alquist @talquist Carwash, Production Blue
- Ted Beneke @ted.beneke Ciudad Juarez Cartel
- Gale Boetticher @gboetticher Ciudad Juarez Cartel
- Mike Ehrmantraut @mehrmantraut
- Steve Gomez @sgomez
- Tyrus Kitt @tyruss.kitt

Timeline

post an update... Filters ▾

#13289 Resolved Jun. 11 - 8:42 AM
Just bounced the server. Looks like it's fixed.

#13289 Resolved Jun. 11 - 8:40 AM
Splunk: Splunk Alert - Fleetwood Bounder CRITICAL
Policies alerted: Tech Ops, App Alerts
Resolved by: ted.beneke

1 Annotation 4 Alerts show details

Ted Beneke RESOLVED #13289 for Splunk Jun. 11 - 8:40 AM

#13289 Acked Jun. 11 - 8:42 AM
With your knowledge of how the books got the way they are, maybe there's some way you could undo what's in there.

Paging cancelled for Ted Beneke Jun. 11 - 8:40 AM

#13289 Triggered Jun. 11 - 8:40 AM
Splunk: Splunk Alert - Fleetwood Bounder CRITICAL
Policies alerted: Tech Ops, App Alerts
Paging: ted.beneke

1 Annotation 4 Alerts show details

Paging Ted Beneke Feb 1 - 7:21 AM
Contacting Ted Beneke for incident #13289, sending Email, Sending SMS

#13289 Triggered Jun. 11 - 8:40 AM
Splunk: Splunk Alert - Fleetwood Bounder CRITICAL
Policies alerted: Tech Ops, App Alerts
Paging: ted.beneke

1 Annotation 4 Alerts show details

Incidents

Incident #13289

#13289 Resolved Jun. 11 - 8:40 AM

Resolved: Splunk: Splunk Alert - Fleetwood Bounder CRITICAL
Policies alerted: Tech Ops, App Alerts
Resolved by: ted.beneke

Details Timeline Annotations (3)

1. Link to runbook
2. Report: whenever the issue occurs
4. System Load Graph

(Host filter can be applied)

2

1

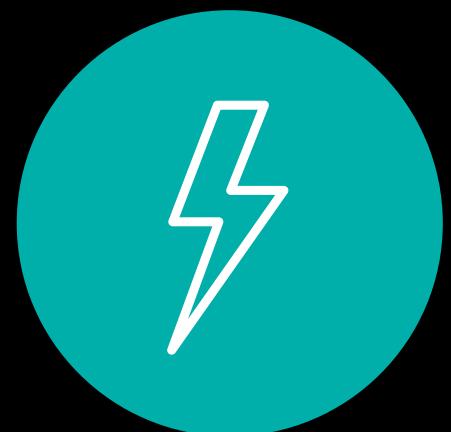
12:00 PM Mon Nov 9 2015 1:00 PM 2:00 PM 3:00 PM

_time

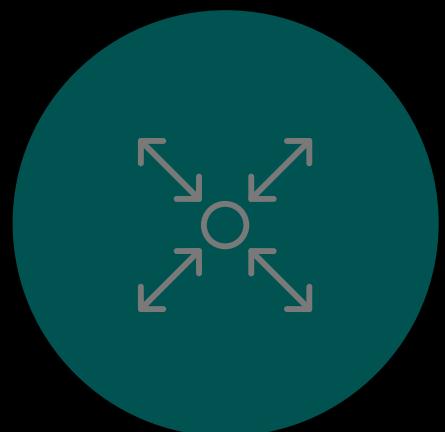
...Load10min: 192.168.2.4 ...mLoad1min: 192.168.2.4
...mLoad5min: 192.168.2.4



Limitless exploration and investigation



Leadership in performance, scale and manageability



Splunk and expansive ecosystem

Grow more easily

Splunk Metrics Performance

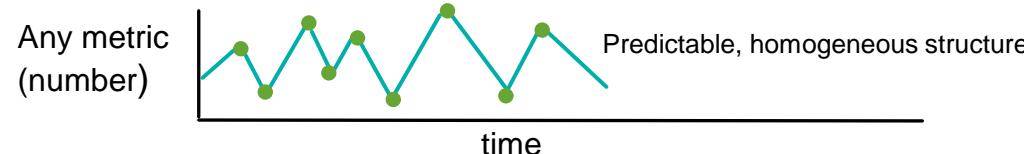


Metrics and Events

New, high-speed metrics engine that integrates seamlessly with events

Metrics

- ▶ Set of numbers describing a particular process or activity measured over an interval of time — i.e., *time series data*
- ▶ Virtually unlimited number of use cases



- ▶ Common metrics sources:
 - System metrics (CPU, memory, disk), sensor data (temperature)
 - Infrastructure metrics (AWS CloudWatch), web tracking (Google Analytics)
 - Application agents (application performance monitoring, error tracking)

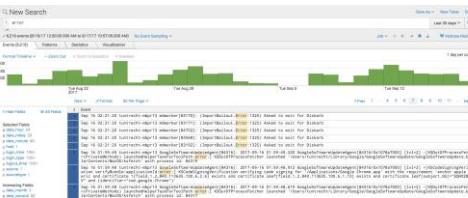
Sample Metric



Events

- ▶ Traditional Splunk — typically text, binary, un/structured data that describe a set of discrete events that happen over time
- ▶ Virtually unlimited number of use cases

Traditional
Splunk

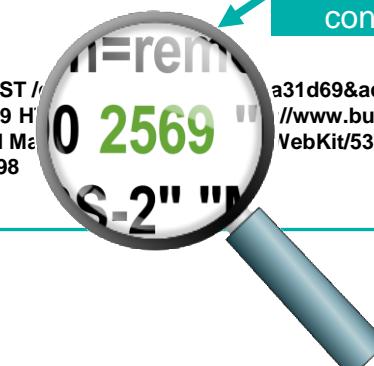


Common event sources:

- System and server logs (syslog, journald), APIs (Twitter, Wunderground)
- Firewall data (Palo Alto Networks, etc)
- Application, platform and other logs (log4j, log4net, Apache, MySQL, AWS)

Sample Log

[29/Aug/2017 08:47:05:316503] "POST /<redacted>?JSESSIONID=SD6SAL4FF1ADFF9 H product_id=BS-2" "Mozilla/5.0 (Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2957.0 Safari/537.36" 98



Metrics in Splunk Enterprise

Lightning-fast performance when searching on metrics

- ▶ Up to **2,000x** speed improvement against the same search (query) on logs with Splunk Enterprise 6.6
- ▶ All Splunk Platform benefits apply:
 - Visualizations and alerting
 - Role-based access controls
 - Data onboarding
 - Clustering, scaling, alerting
 - Leverage open source for existing source types (statsd, collectd)

Metrics – great for high volume data and large number of searches in one dashboard



Turn Event Data Into Metrics



Turning Events into Metrics

Using the mcollect command



Which airline has the longest delays into Orlando?

1. Start with a public airline dataset and put into traditional Splunk event index
2. Look at the shape of the data
3. Create a new metrics index
4. Push event data into the metrics index using mcollect command
5. Query the metrics index to find our answer

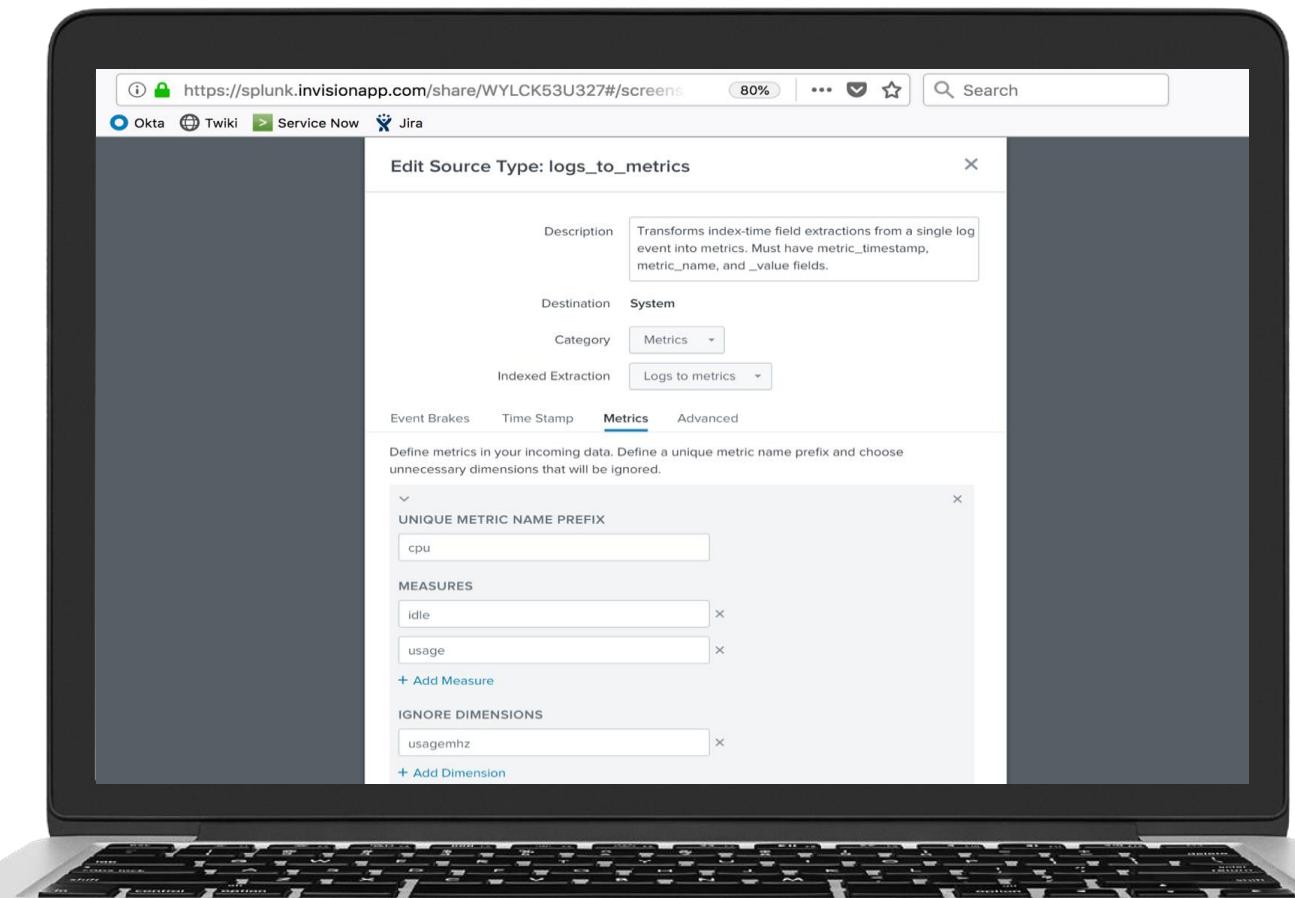
```
index=airline_data
| stats avg(ArrDelay) as AvgDelay by Dest, Origin, UniqueCarrier
| eval _value=AvgDelay
| eval metric_name="AvgDelay"
| table Dest, Origin, UniqueCarrier, metric_name, _value
| mcollect index=airline_metrics_index
```

```
| mstats avg(AvgDelay) as AvgDelay WHERE index=airline_metrics_index
Dest=MCO Origin=IAD by UniqueCarrier
| sort -AvgDelay
```

Logs to Metrics

Take advantage of metrics performance by converting your logs to metrics

- ▶ Intuitive interface for converting logs to metrics
 - ▶ Take advantage of Splunk metrics performance – 2,000X faster alerting and monitoring – as well as the new Splunk Metrics Workspace



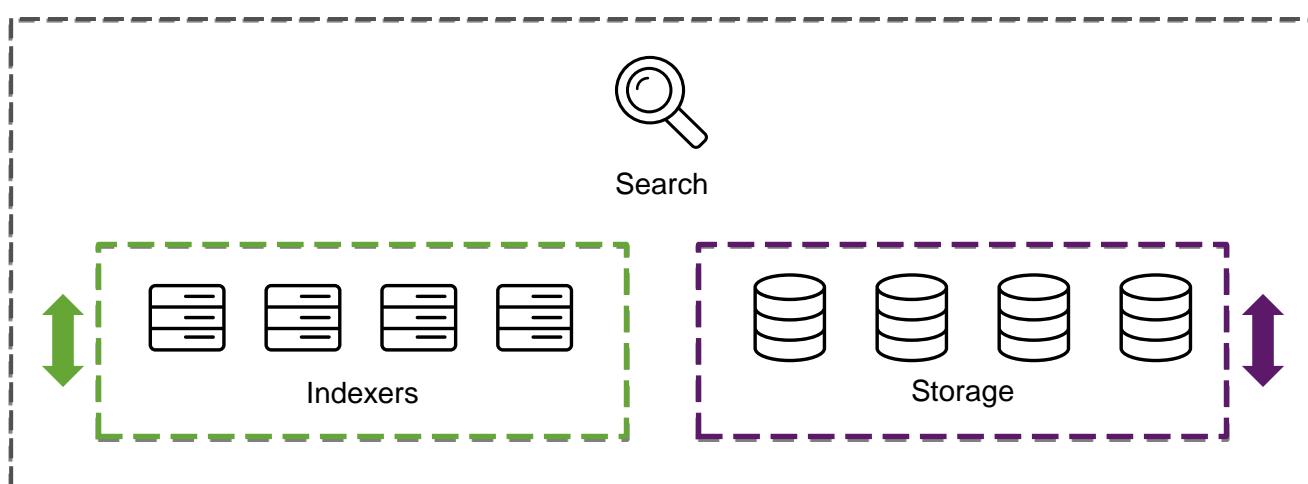
Splunk Management Improvements



SmartStore

Independently scale storage and compute – maintain performance and availability while lowering TCO

- ▶ Independently scale up/down compute (CPUs) and data storage based on business demands
 - ▶ Automatically evaluates users' data access patterns (via app-aware cache) – places actively accessed data in local storage for real-time analytics; inactive data to low-cost, remote storage



Proactive Splunk Component Monitoring

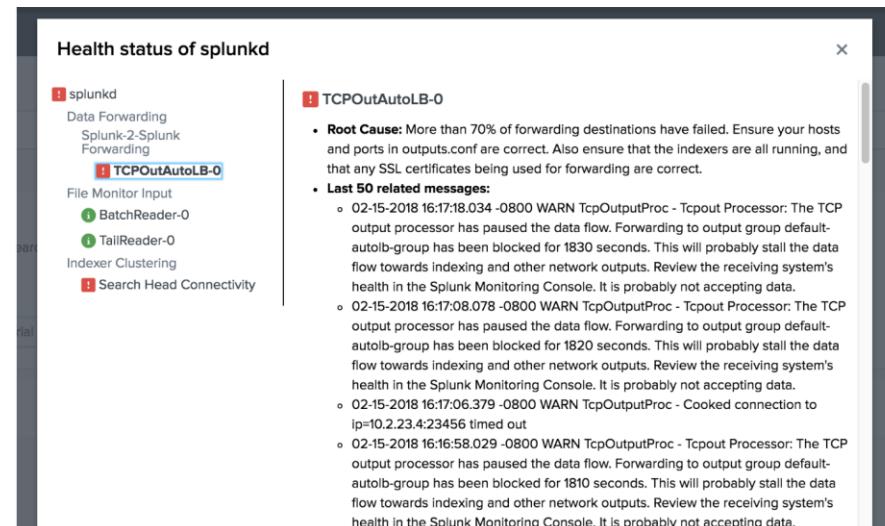
The screenshot shows the Splunk 7.1 interface. At the top, there's a navigation bar with links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search bar. Below the navigation is a secondary header with 'Search & Reporting' and a 'Search' button. The main content area is titled 'Search' and contains a search bar with placeholder 'enter search here...', a time range selector 'Last 24 hours', and a green search button. To the left, there's a 'How to Search' section with a link to documentation and a 'Tutorial'. On the right, there's a 'What to Search' summary showing '109,864 Events' indexed from '12 days ago' to '5 days ago'. At the bottom, there's a 'Search History' section.

- ▶ Get health status of Splunk components via REST API calls
- ▶ Provides both top-level and drill-down views of the deployment
- ▶ Provides root cause and guidance on resolving the problem

Splunk health status pop up



Forwarding alert with root cause and related messages



Workload Management

Prioritize and manage search and ingestion resources to meet business needs

ronnie.sv.splunk.com:8003/en-US/manager/system/workload_management

splunk>enterprise Apps ▾ i Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Search

Workload Management

View and edit configurations of workload management.

Disable Add Workload Pool Add Workload Rule Apply

i Message will go here

Workload Pool	CPU Group	Memory Group	Default Pool	Ingest Pool	Actions	Applied
pool_1	/sys/fs/cgroup/cpu/pool_1	/sys/fs/cgroup/memory/pool_1	✓		Edit Delete	<input type="checkbox"/>
pool_2	/sys/fs/cgroup/cpu/pool_2	/sys/fs/cgroup/memory/pool_2		✓	Edit Delete	<input type="checkbox"/>
pool_3	/sys/fs/cgroup/cpu/pool_3	/sys/fs/cgroup/memory/pool_3			Edit Delete	<input type="checkbox"/>
pool_4	/sys/fs/cgroup/cpu/pool_4	/sys/fs/cgroup/memory/pool_4			Edit Delete	<input type="checkbox"/>

Order	Workload Rule	Type	Type Value	Workload Pool	Actions	Applied
-------	---------------	------	------------	---------------	---------	---------

Password Management



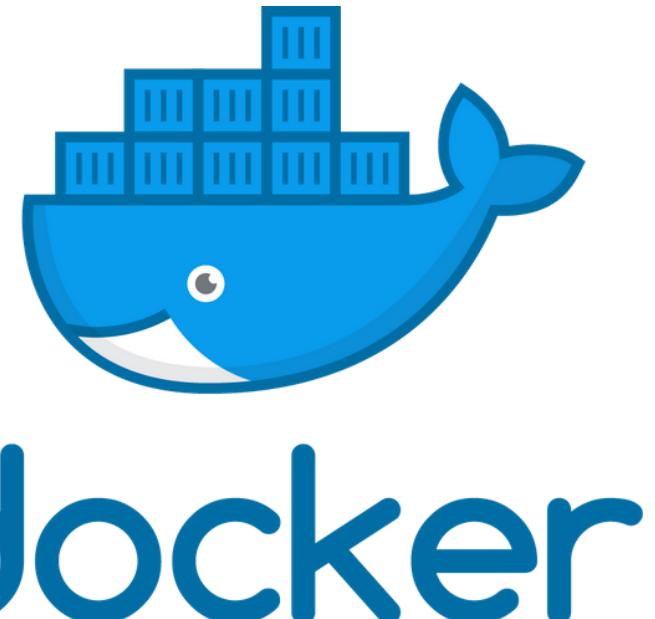
Password Management



Splunk on Docker

Fast deployments. Easily expandable. Lower TCO.

- ▶ Official Splunk Support for Enterprise 7.2 deployments in Docker containers
 - ▶ All the benefits of Docker...
 - Fast deployments
 - Easily expand (or contract) Splunk footprint; onboard new teams and users
 - Lower TCO via decreased hardware, OS and hypervisor requirements



Splunk Cloud Compliance

Announcing new compliance attestations of compliance: HIPAA and PCI

- ▶ New Splunk Cloud SKU featuring:
 - Splunk Cloud subscription with HIPAA and/or PCI compliance
 - Encryption at rest
 - Splunk Standard Success Plan
 - ▶ Assurance Splunk Cloud will manage customer data in accordance with strict regulations:
 - Health Insurance Portability and Accountability Act (HIPAA), the standard for organizations in the USA that deal with sensitive patient data
 - Payment Card Industry Data Security Standard (PCI DSS), security standards designed to ensure all organizations that accept, process, store or transmit credit card information maintain a secure environment



Dynamic Data

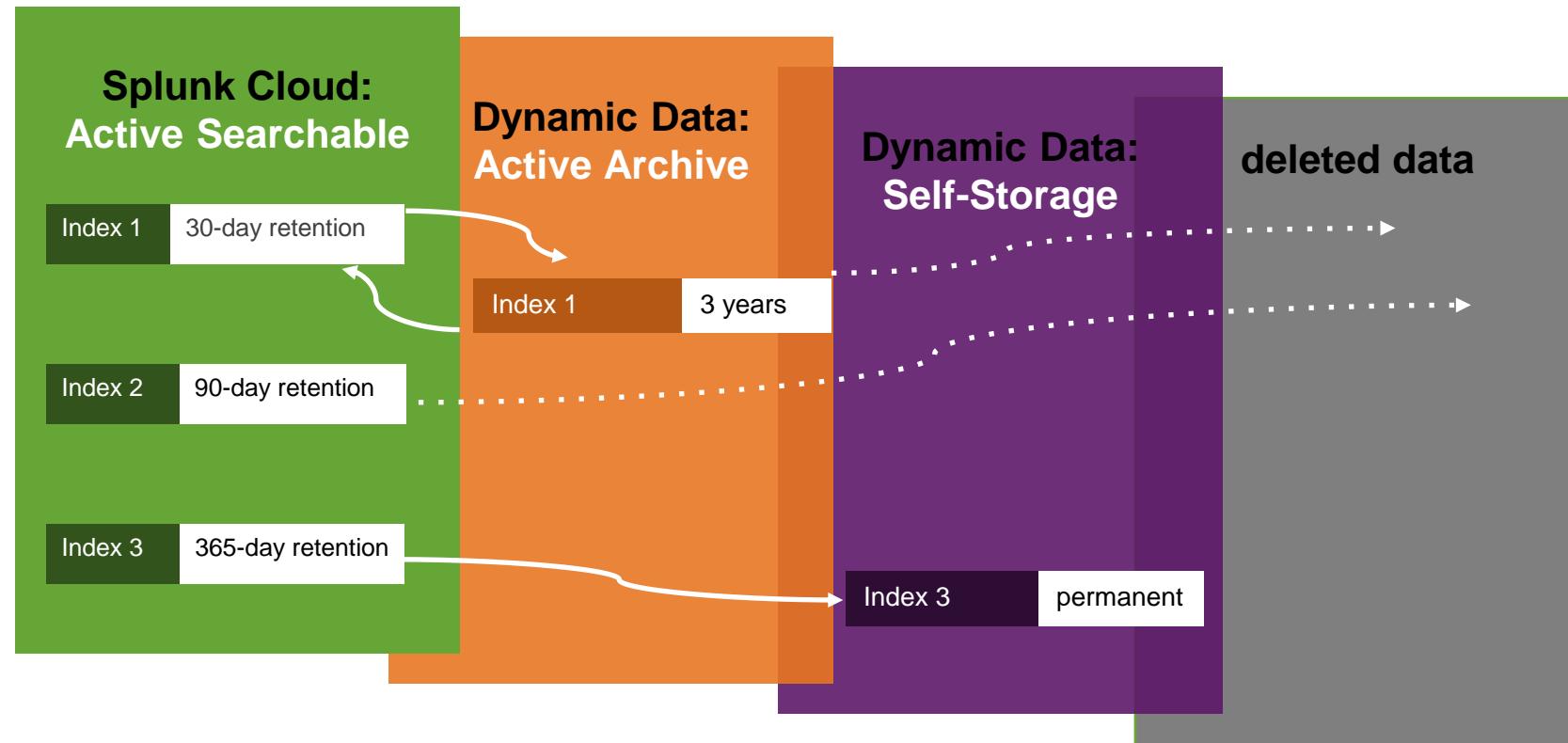
Retain **infrequently accessed** data to meet compliance requirements.
Easily resurrect to **search when required**.

Dynamic Data: Active Archive

- ▶ New with Splunk Cloud release 7.2
- ▶ Move less-frequently accessed data to cost-effective, Splunk-managed data archive
- ▶ Easily restore data into Splunk Cloud (i.e., it becomes “warm”)

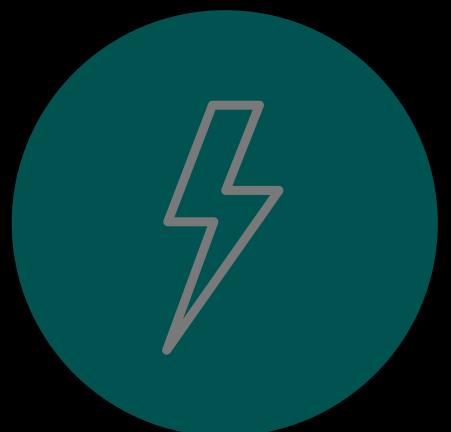
Dynamic Data: Self-Storage

- ▶ Introduced with Splunk Cloud release 7.1
- ▶ Tiered data storage service empowers you to move data from Splunk Cloud to your own Amazon S3 environment
- ▶ Data no longer accessible via Splunk Cloud (i.e., it becomes “frozen”)

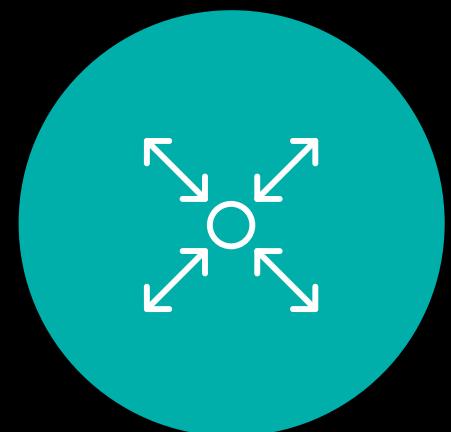




Limitless exploration and investigation



Leadership in performance, scale and manageability



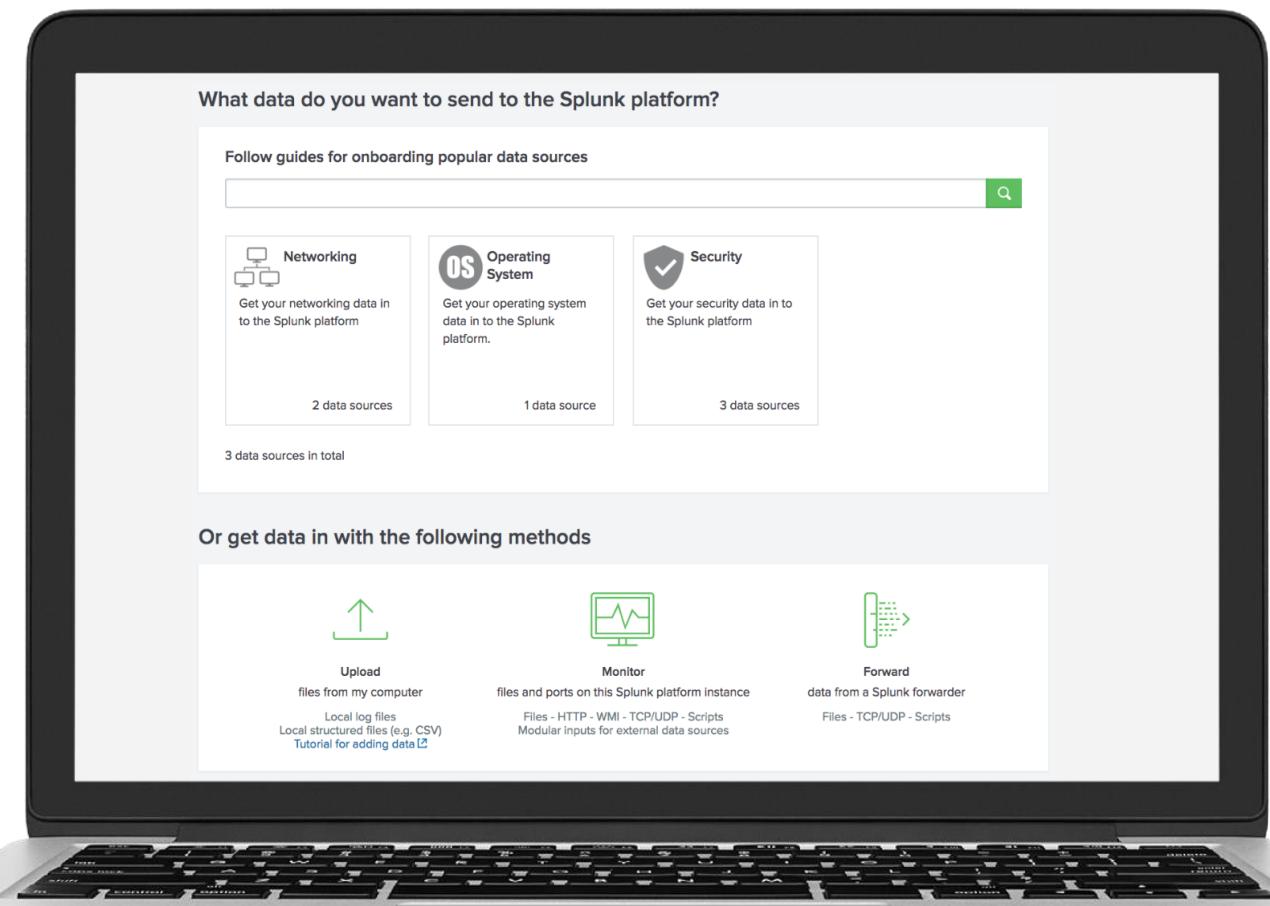
Splunk and expansive ecosystem

Leverage more data

Guided Data Onboarding

Intuitive interface for getting data into Splunk

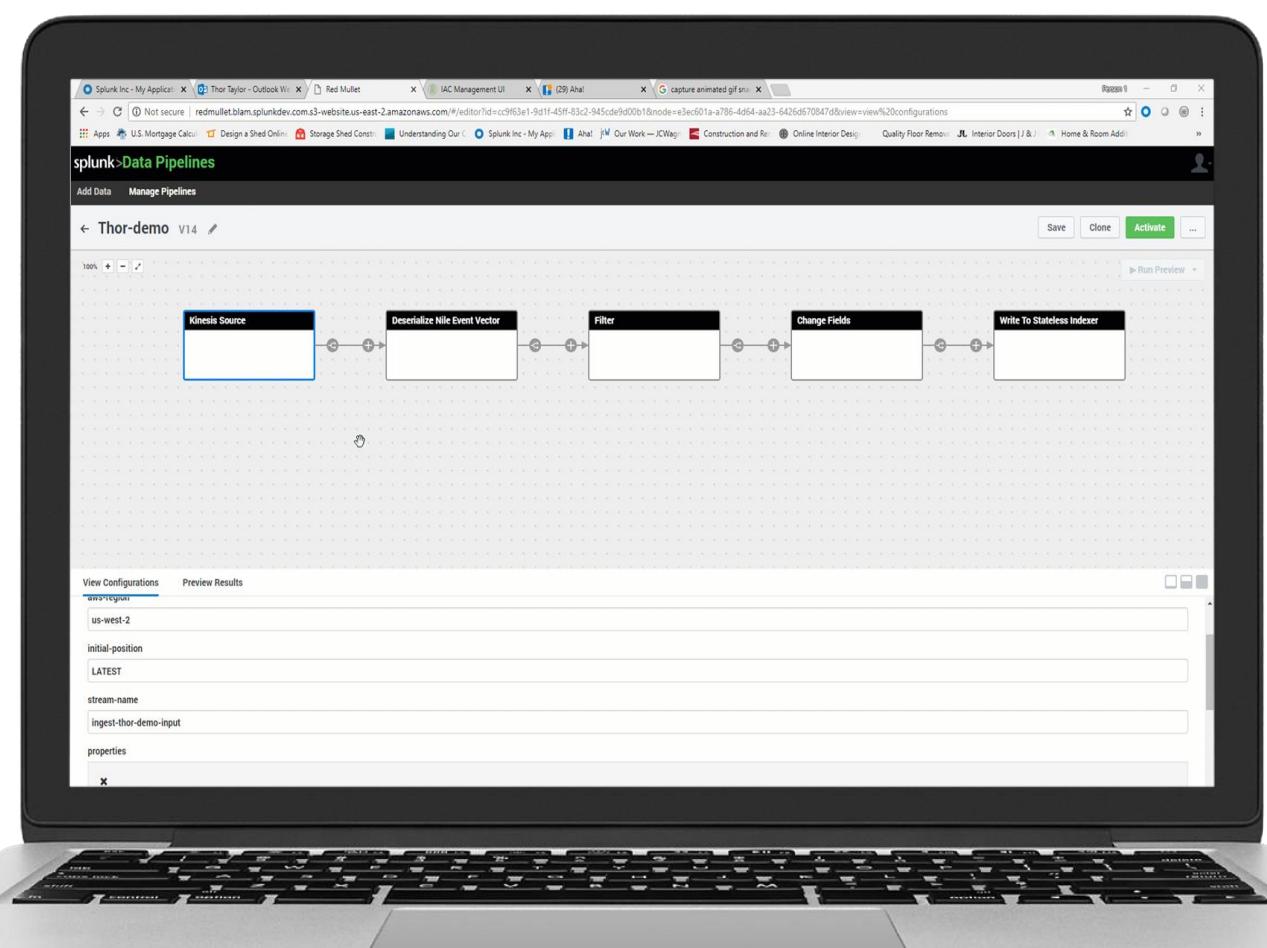
- ▶ Helps users understand the crucial concepts related to getting data into Splunk
- ▶ Data onboarding methodologies based on users' specific Splunk architecture: single instance, single search head with clustered indexers, or Splunk Cloud
- ▶ Addresses most common data sources: networking, OS, security, servers



Data Stream Processor

Explore and transform data at rest and in flight (while it's streaming)

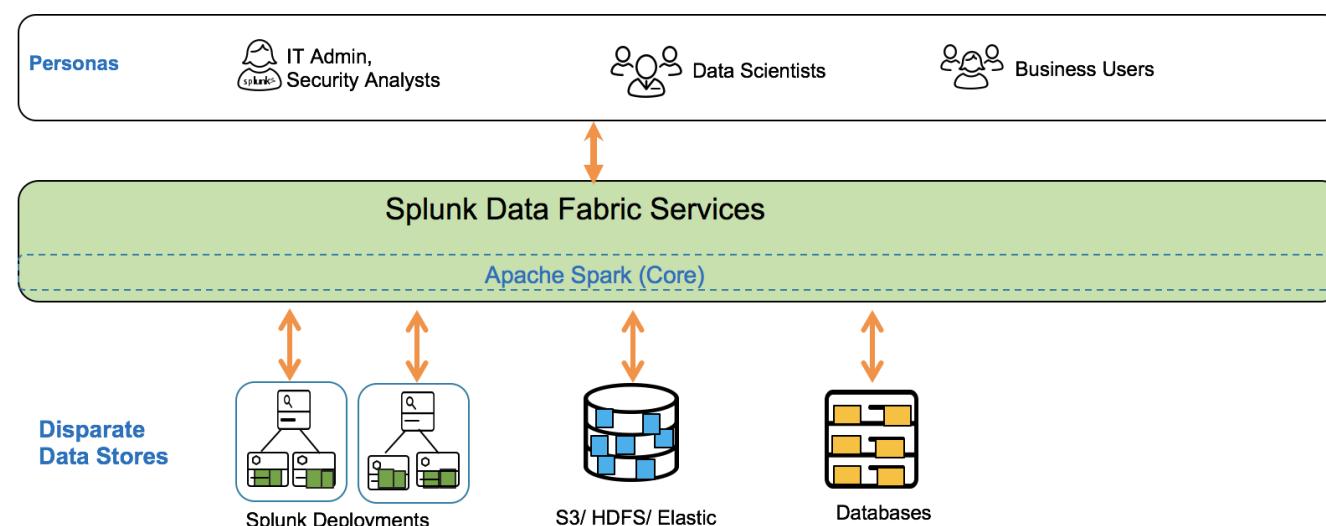
- ▶ Customize capabilities and meet specific use cases using our open APIs
- ▶ Connect to any data — at rest or streaming
- ▶ Refine, modify or adjust data before it reaches its destination
- ▶ Track data through the entire pipeline, and ensure it successfully reaches the intended destination



Data Fabric Search

Search trillions of events at ease — single instance or Splunk 2 Splunk

- ▶ Search and retrieve significantly larger amounts of data with much higher performance, easily scaling to billions or trillions of events
 - ▶ Run federated searches across multiple Splunk deployments as easily as if it were a single deployment
 - ▶ Expand your federated searches to disparate data sources across a wider data fabric, viewing all the data in a unified way through Splunk dashboards

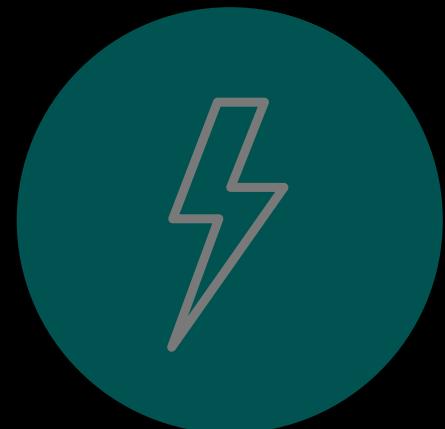




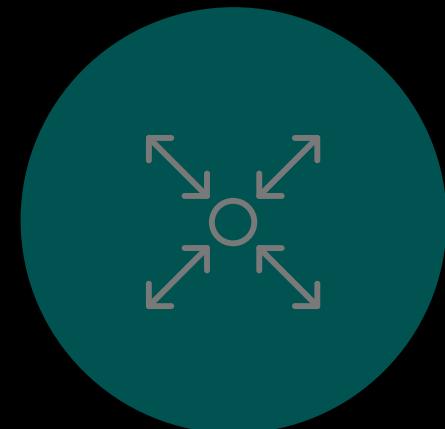
Artificial intelligence and machine learning integrated throughout platform



Limitless exploration and investigation



Leadership in performance, scale and manageability



Splunk and expansive ecosystem

AI Powered by Machine Learning

Splunk premium solutions deliver AI powered by ML out-of-the-box;
Splunk platform is designed for expansive and customizable AI and ML use cases

AIOps



Splunk IT Service
Intelligence™

Analytics-driven Security



Splunk User Behavior
Analytics™

- ▶ Designed for IT and security practitioners
- ▶ Machine learning embedded; users select data sets and adjust the model
- ▶ Does not require a data scientist

Splunk Premium Solutions

Out-of-the-box AI and ML experience for specific use cases

Machine Learning



Machine Learning Toolkit
(MLTK)

- ▶ Codeless, step-by-step ML
- ▶ Integrates with open source algorithms
- ▶ Launch inside any Splunk search/query pipeline
- ▶ Requires Splunk and analytics expertise

Splunk Platform

Customizable AI and ML for all use cases

New with MLTK 4.0



1. Splunk Community for MLTK Algorithms on GitHub

Enables Splunk MLTK users to share code and custom algorithms, get feedback and tips from fellow Splunk MLTK users, as well as the Splunk team and other GitHub community members.

2. Splunk MLTK Container for TensorFlow

Extends the value of Splunk MLTK with additional contributions and functionality provided by TensorFlow, the OSS library for high performance numerical computation.

3. Splunk Machine Learning Toolkit Connector for Apache Spark

Allows users to leverage their own Spark clusters for fitting models on large data sets using Spark infrastructure vs. the Splunk search head, delivering faster computation on certain algorithms, easier scaling and high elasticity. New Spark and Splunk configuration UI facilitates testing of the Spark connection and set up. Support for additional [MLlib](#) algorithms out-of-the-box.

The screenshot shows the Splunk Enterprise interface with the "Machine Learning Toolkit" tab selected. The main area displays a grid of experiment cards. One card is highlighted with a blue border, showing details for an experiment named "Expt_Predict_Sales". It includes fields for "Predict Numeric Fields" (5), "Predict Categorical Fields" (1), "Detect Numeric Outliers" (2), "Detect Categorical Outliers" (2), "Forecast Time Series" (1), and "Cluster Numeric Events" (3). Below the grid, there are sections for "EXPERIMENT SETTINGS" and "PREPROCESSING STEPS".

The screenshot shows a "FieldSelector" configuration dialog. It includes a "Preprocess method" dropdown set to "FieldSelector", a "Select the field to predict" dropdown set to "median_house_value", and a "Select the predictor fields" dropdown containing several fields: "avg_rooms_per_dwelling", "business_acres", "charles_river_dojacency", "crime_rate", "distance_to_employment_center", "highway_accessibility_index", "land_zone", "nhticoxide_concentration", "property_tax_rate", "pub_teachr_ratio", and "units_prior_1940". A "Mode" dropdown is set to "Kbest" with a value of "3". At the bottom, there is an "Apply" button and a note: "FieldSelector has identified the following fields: avg_rooms_per_dwelling, crime_rate, nhticoxide_concentration. Use 'X' to select them all."

The diagram illustrates the process of creating a vector-space representation from documents. It starts with a stack of documents on the left, which are mapped to a "Vector-space representation" on the right. This representation is shown as a grid of numbers (D1 to D5) for terms (complexity, algorithm, entropy, traffic, network). Below this grid is a "Term-document matrix".

	D1	D2	D3	D4	D5
complexity	2	3	2	3	
algorithm	3		4	4	
entropy	1			2	
traffic	2	3			
network	1	4			

Term-document matrix

New with MLTK 3.2



- 1. Experiment management framework**
This new, intuitive interface gives you the ability to view, control, share and monitor the status of your machine learning experiments.
- 2. FieldSelector pre-processing algorithm**
Speeds-up the process of identifying the most relevant data fields to train, and increases the accuracy of your machine learning models.
- 3. New X-means algorithm**
Useful for clustering unlabeled data without requiring knowledge of how many groups there should be.

The screenshot shows the Splunk Machine Learning Toolkit's Experiment management interface. It displays a grid of experiments with columns for Predict Numeric Fields, Predict Categorical Fields, Detect Numeric Outliers, Detect Categorical Outliers, Forecast Time Series, and Cluster Numeric Events. Each experiment entry includes a preview of the data, the algorithm used (e.g., LinearRegression, XMeans), and various configuration settings like EXPRESSION SETTINGS, PROCESSING STEPS, and MODEL DETAILS.

The screenshot shows the FieldSelector pre-processing algorithm interface. It lists the field to predict (median_house_value) and the predictor fields selected by the Kbest mode (avg_rooms_per_dwelling, business_acres, crime_rate, distance_to_nearest_center, highway_accessibility_index, land_zone, nitric_oxide_concentration, property_tax_rate, pub_teacher_ratio, units_prior). A note at the bottom indicates that FieldSelector has identified the fields: "avg_rooms_per_dwelling", "crime_rate", "nitric_oxide_concentration".

The diagram illustrates the X-means algorithm for document clustering. It shows a flow from 'Documents' to 'Vector-space representation' and then to a 'Term-document matrix'. The term-document matrix is represented as a table:

	D1	D2	D3	D4	D5
complexity	2	3	2	3	
algorithm	3		4	4	
entropy	1			2	
traffic	2	3			
network	1	4			

Below the matrix is the text: "Term-document matrix".

Thank You

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

