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”

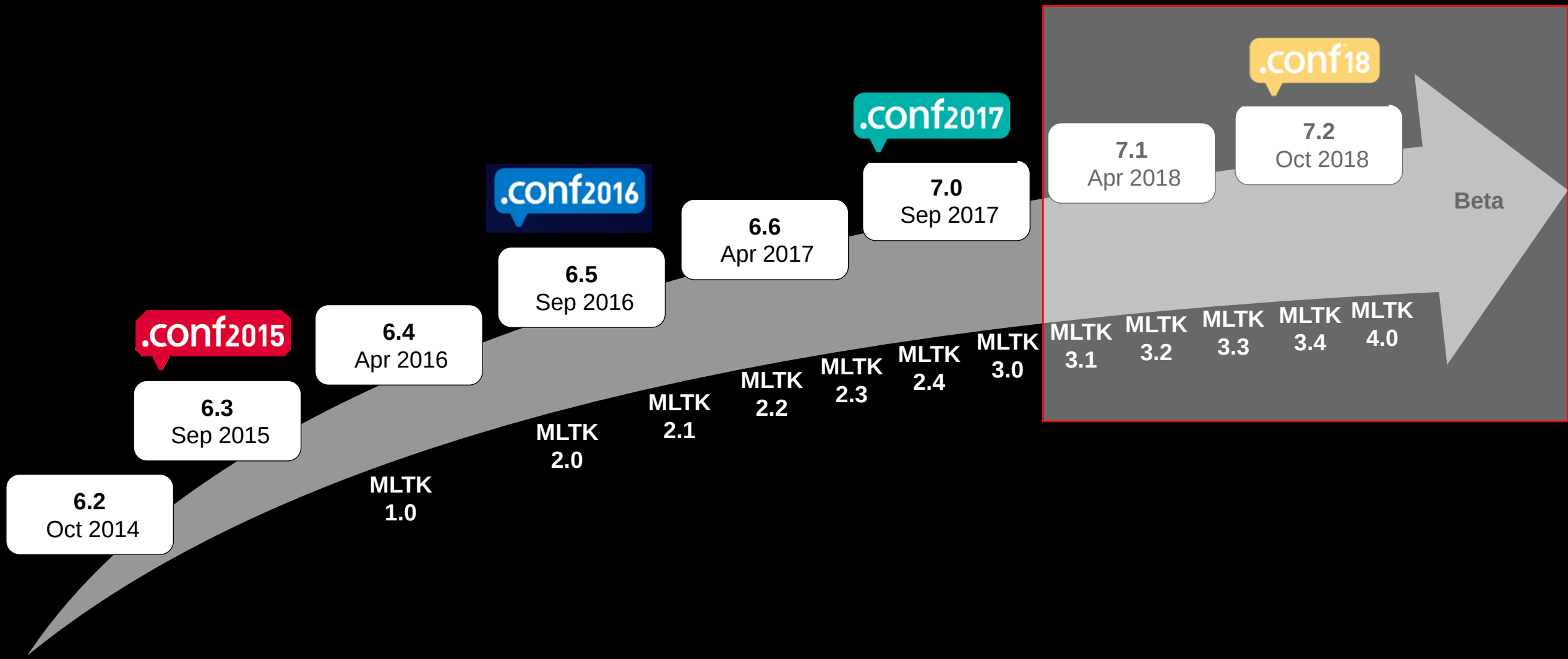
Forward-Looking Statements

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> .conf18

Splunk Enterprise Releases



splunk> .conf18

Artificial intelligence and machine learning integrated throughout platform

Limitless exploration
and investigation

Solve problems faster

Leadership in performance,
scale and manageability

Grow more easily

Splunk *and*
expansive ecosystem

Leverage more data

Limitless exploration
and investigation

Leadership in performance,
scale and manageability

Splunk *and*
expansive ecosystem

Solve problems faster

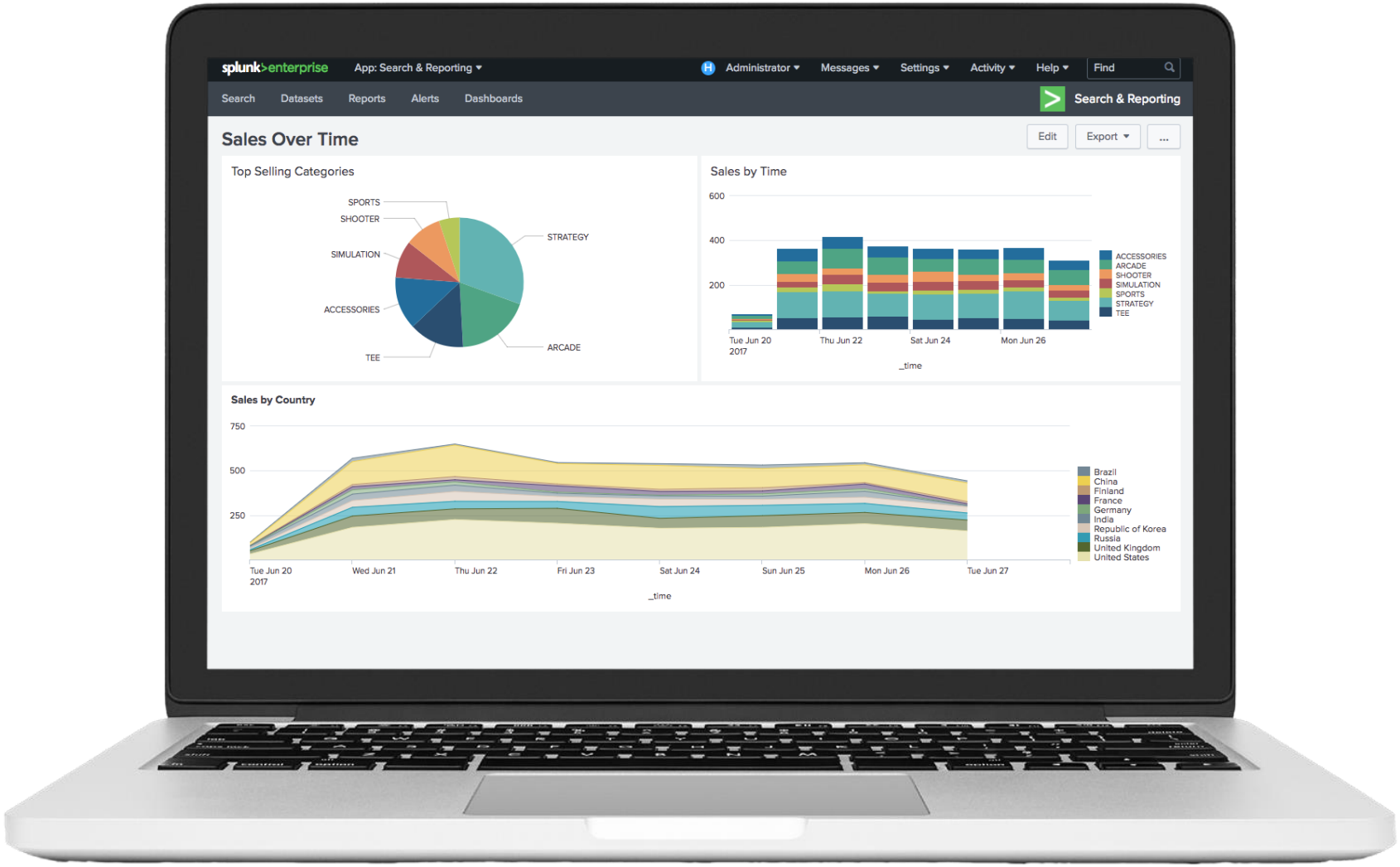
splunk> .conf18

Visual Refresh

Modernized user interface

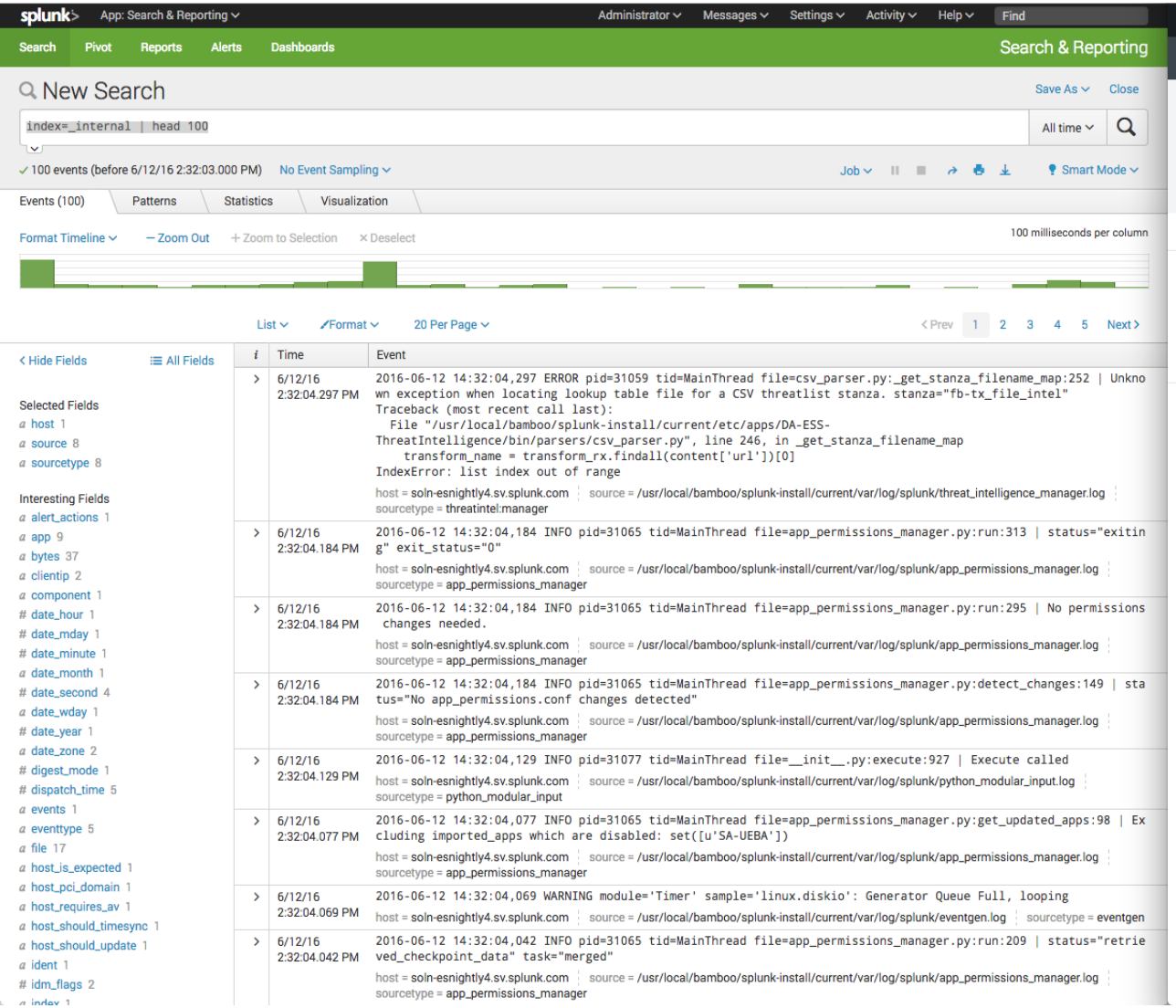
Refreshed User Interface

Crisp and consistent UI spanning Splunk products and Splunk.com

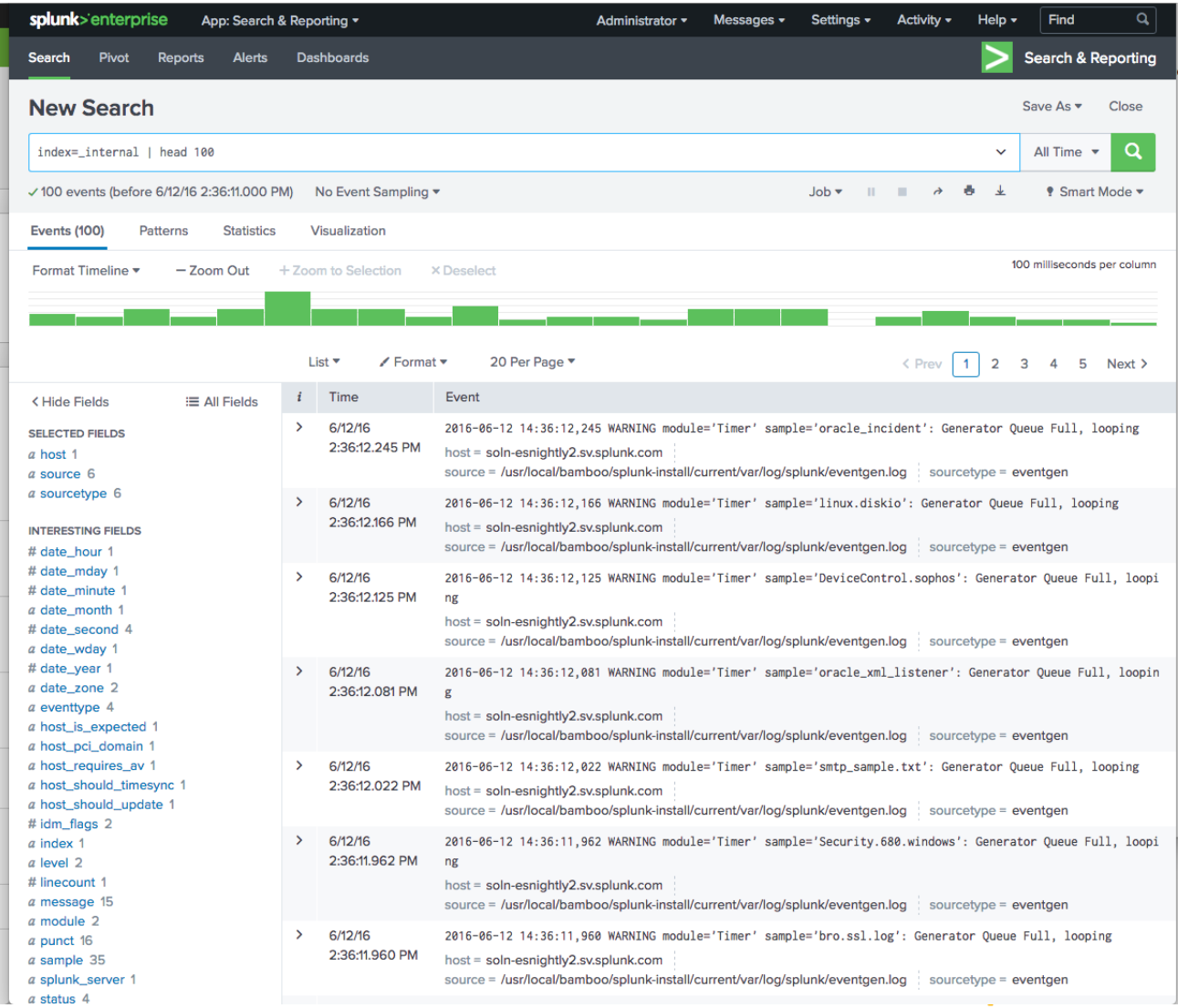


Increased Legibility to Events

Old

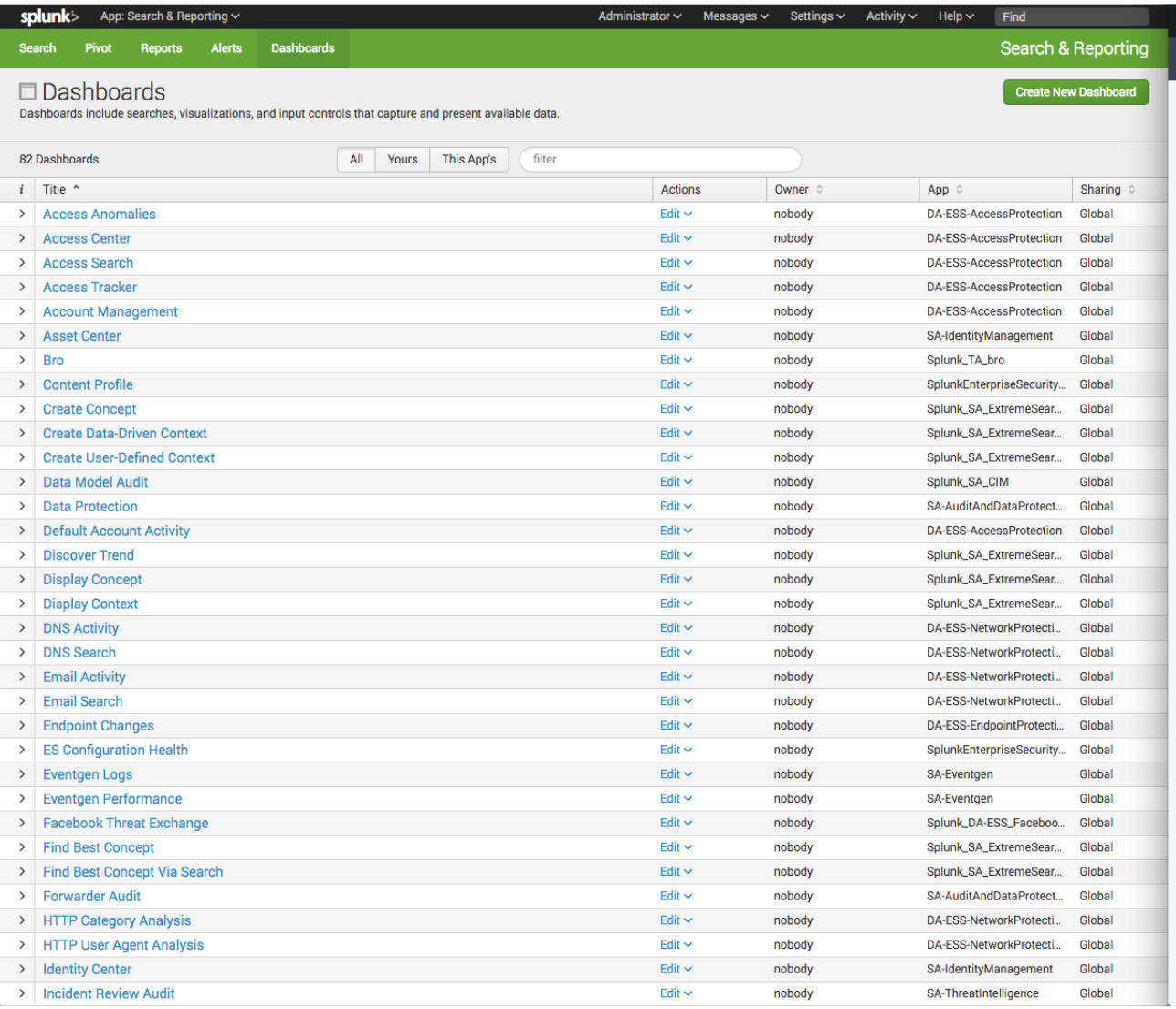


New

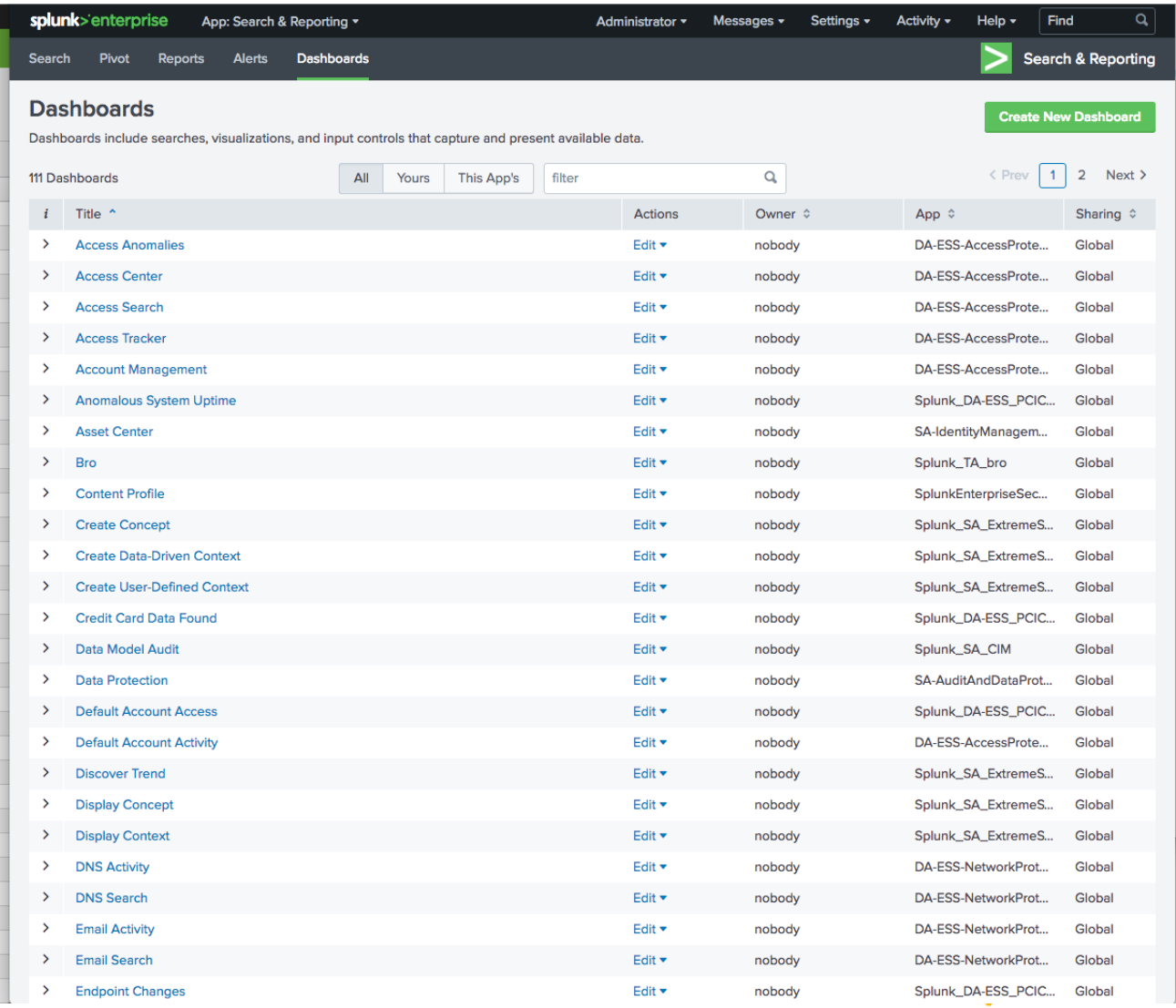


Cleaner Listing Pages

Old

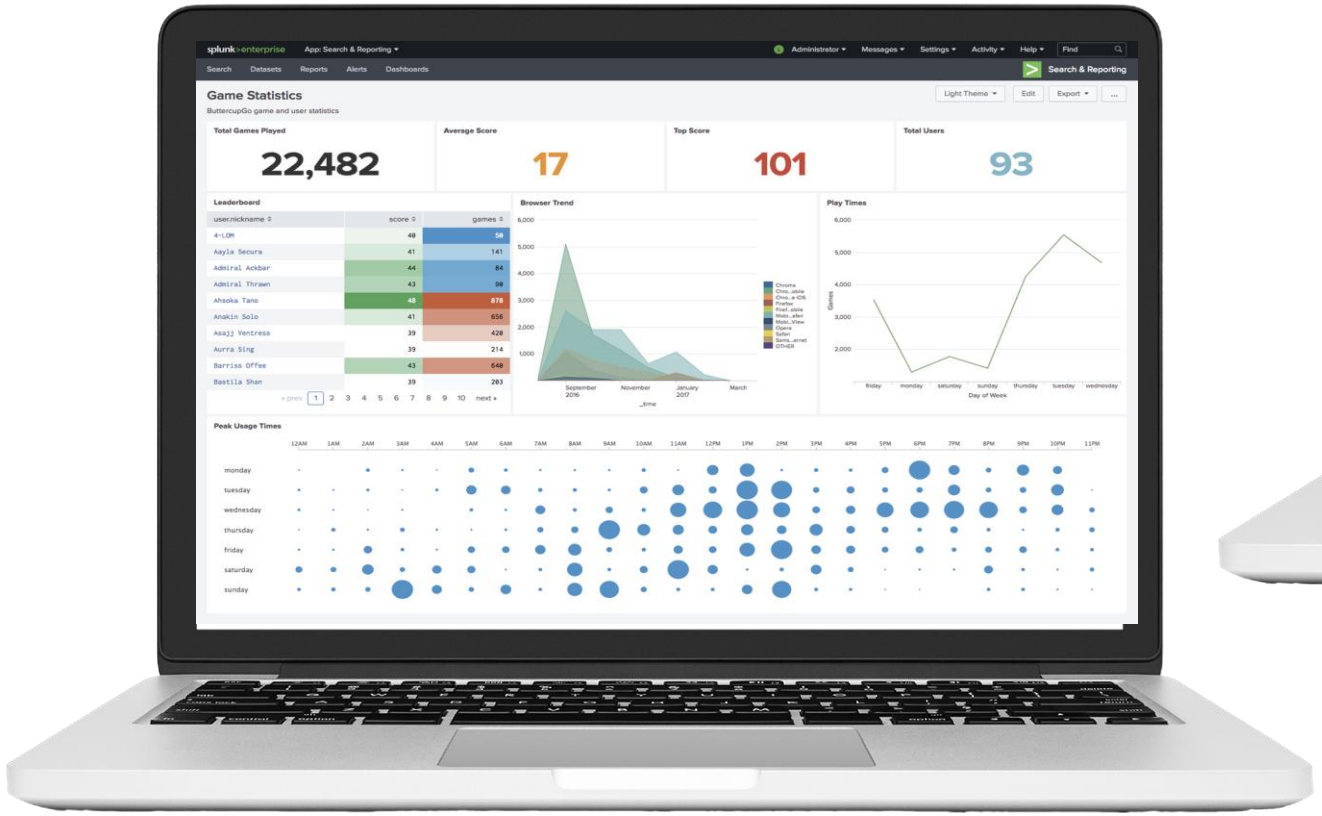


New



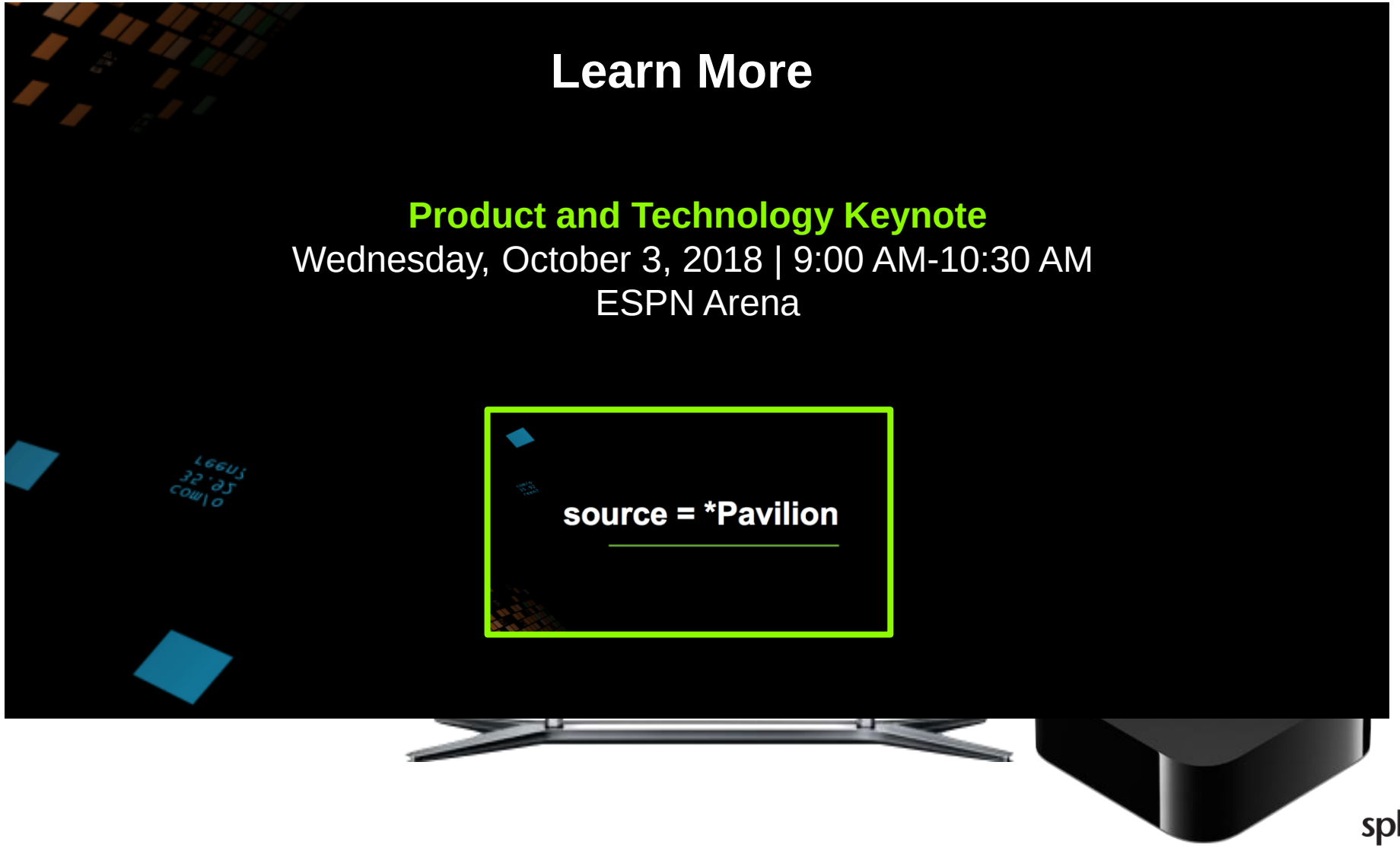
New Dashboard Dark Mode

Heightens visual contrast; optimized for NOC/SOC environments



Dashboards Powered by Apple TV

More secure and cost-effective option for SOCs and NOCs



splunk> .conf18

Accessibility for Users With Disabilities

Section 508 compliance

splunk> .conf18

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

Play Screen Reader Video

Section508.gov
GSA Government-wide IT Accessibility Program

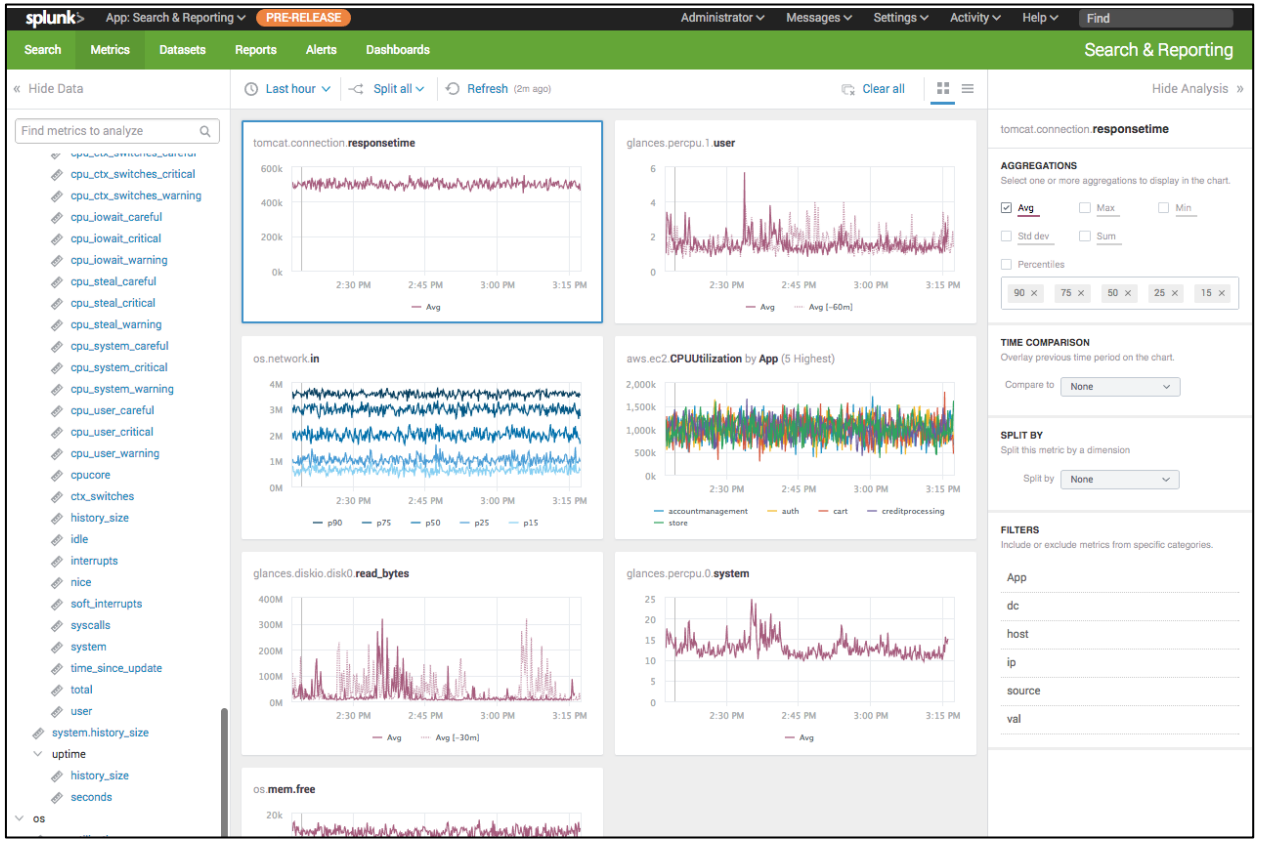
Splunk Metrics Workspace

Explore metrics and accelerated datasets without SPL

splunk> .conf18

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

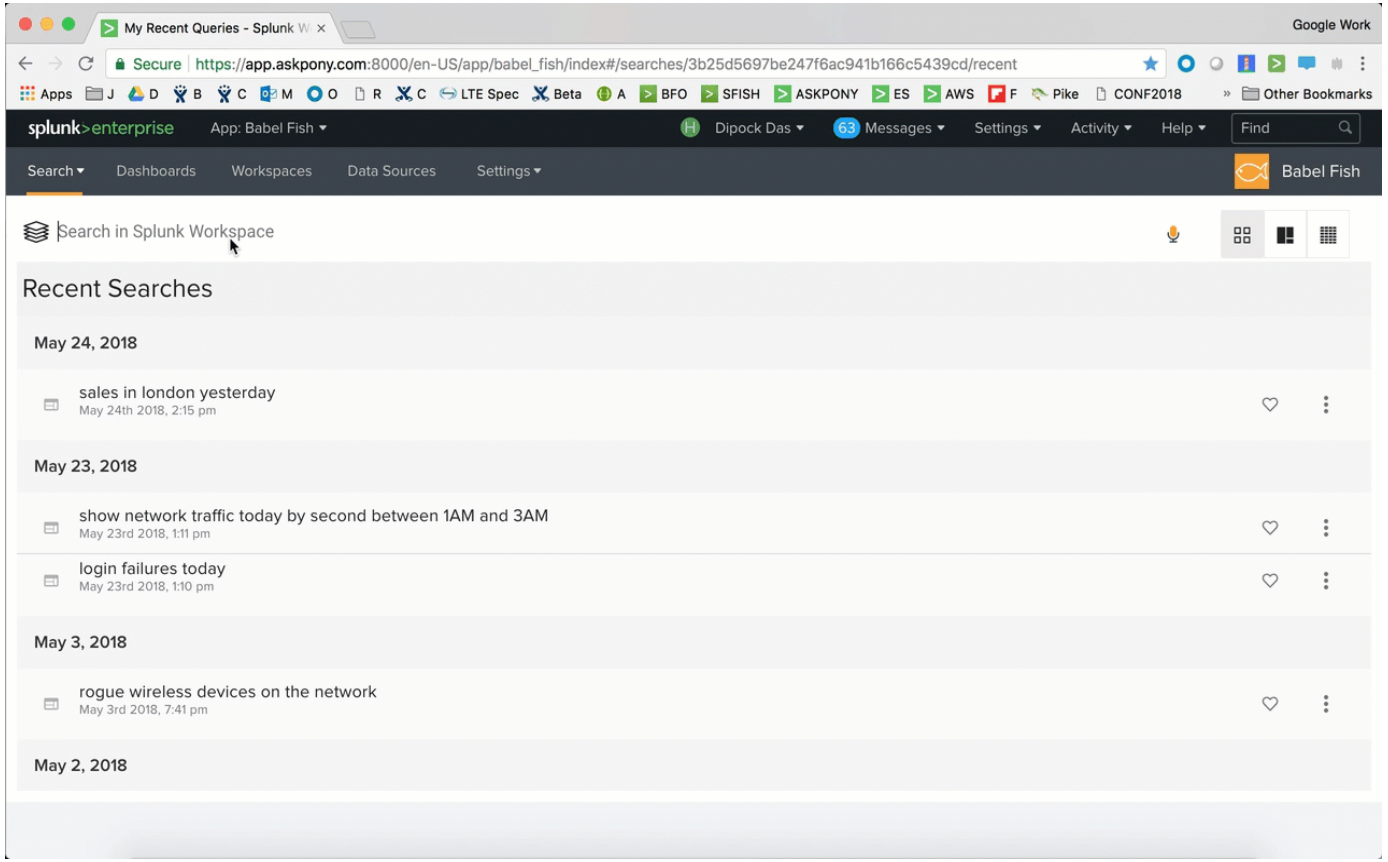
splunk> .conf18

BETA

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



splunk> .conf18

Mobile and Augmented Reality

splunk> .conf18

BETA

New Mobile and Augmented Reality Offerings

Rich, actionable alerts

Augmented reality

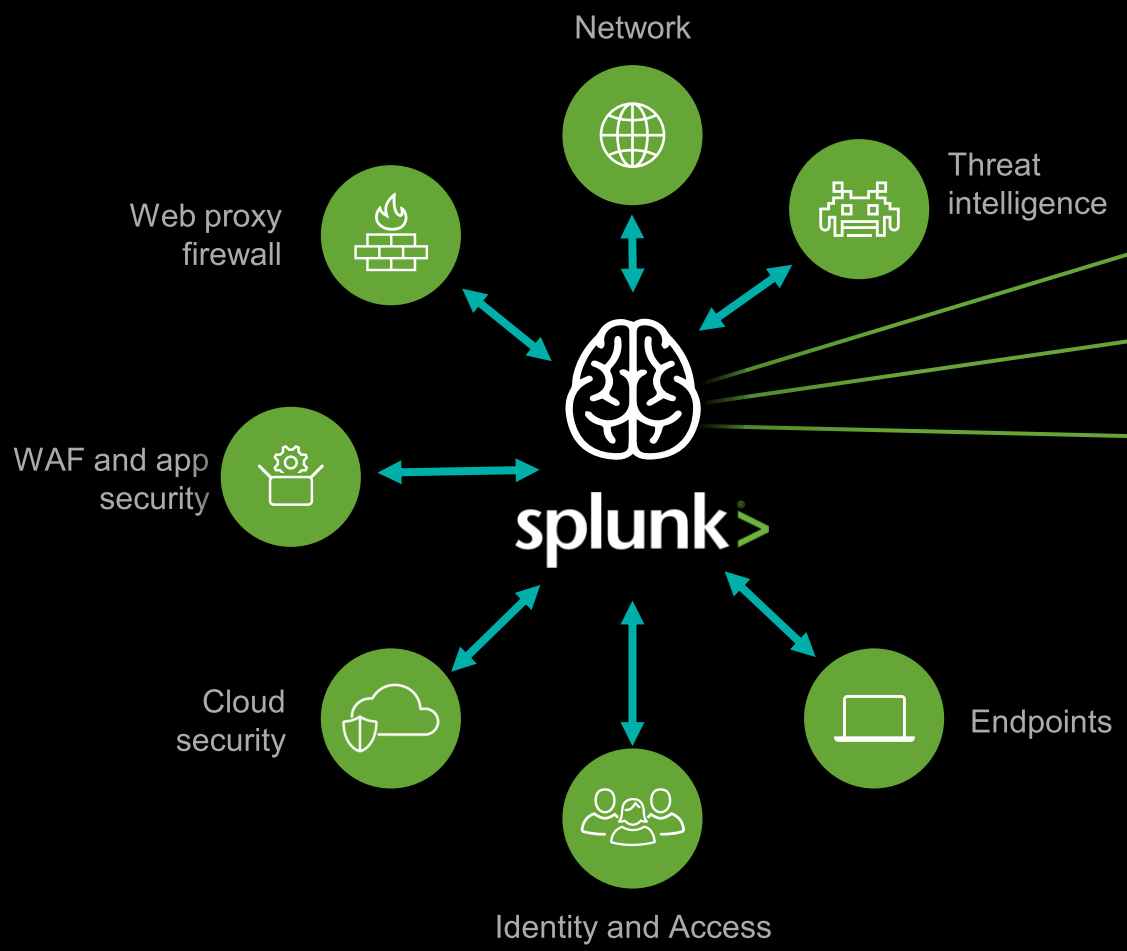
Phantom Integration

Taking action

splunk> .conf18

Phantom and Splunk — Unified Vision

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



DATA PLATFORM

ANALYTICS

OPERATIONS

splunk> phantom

- **Advance cyber defense** and reduce risk using an analytics-driven approach
- **Respond faster** by accelerating incident response
- **Work smarter** and reduce staffing and skills challenges

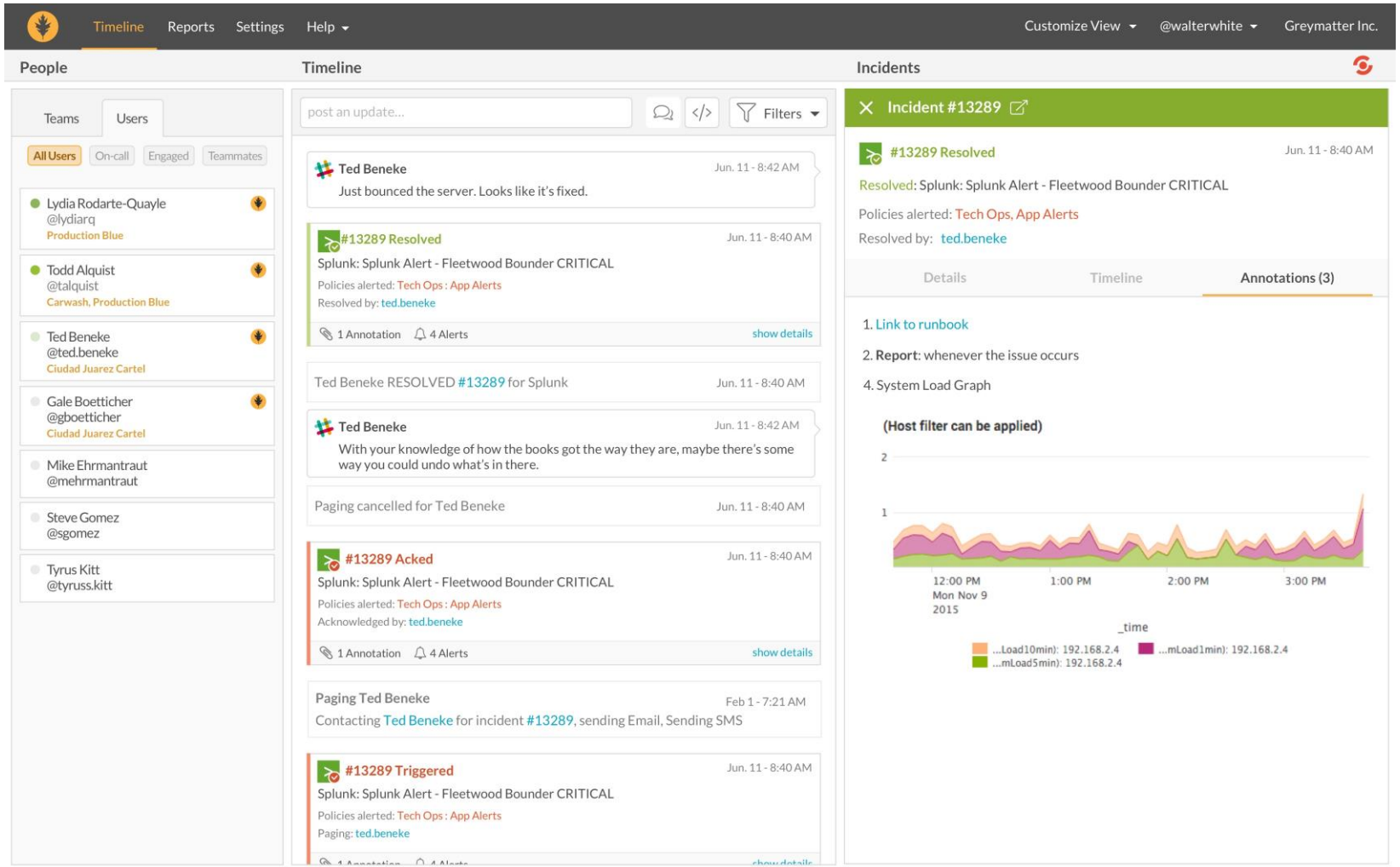
VictorOps Integration

Taking action

splunk> .conf18

VictorOps and Splunk

Making on-call suck less



splunk> .conf18

Limitless exploration
and investigation

Leadership in performance,
scale and manageability

Splunk *and*
expansive ecosystem

Grow more easily

Splunk Metrics Performance

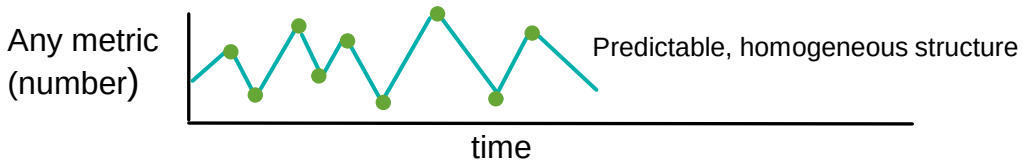
splunk> .conf18

Metrics and Events

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

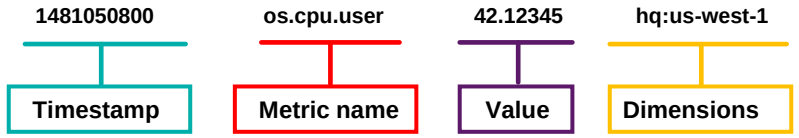
Metrics

- 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)

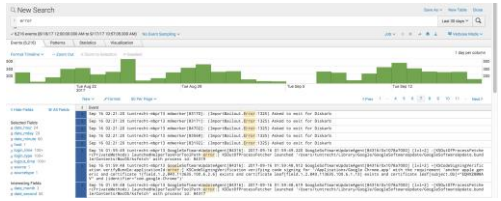
Sample Metric



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

Of course can also contain numbers

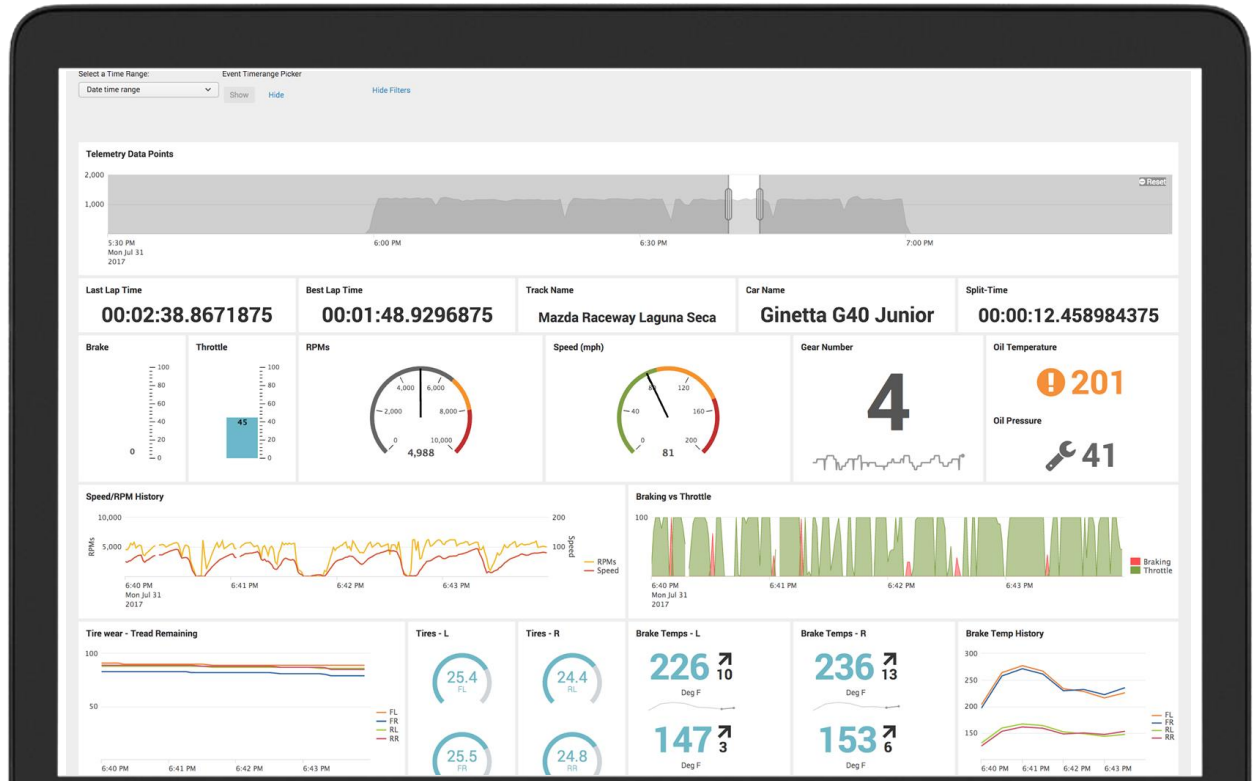
splunk> .conf18

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

splunk> .conf18

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

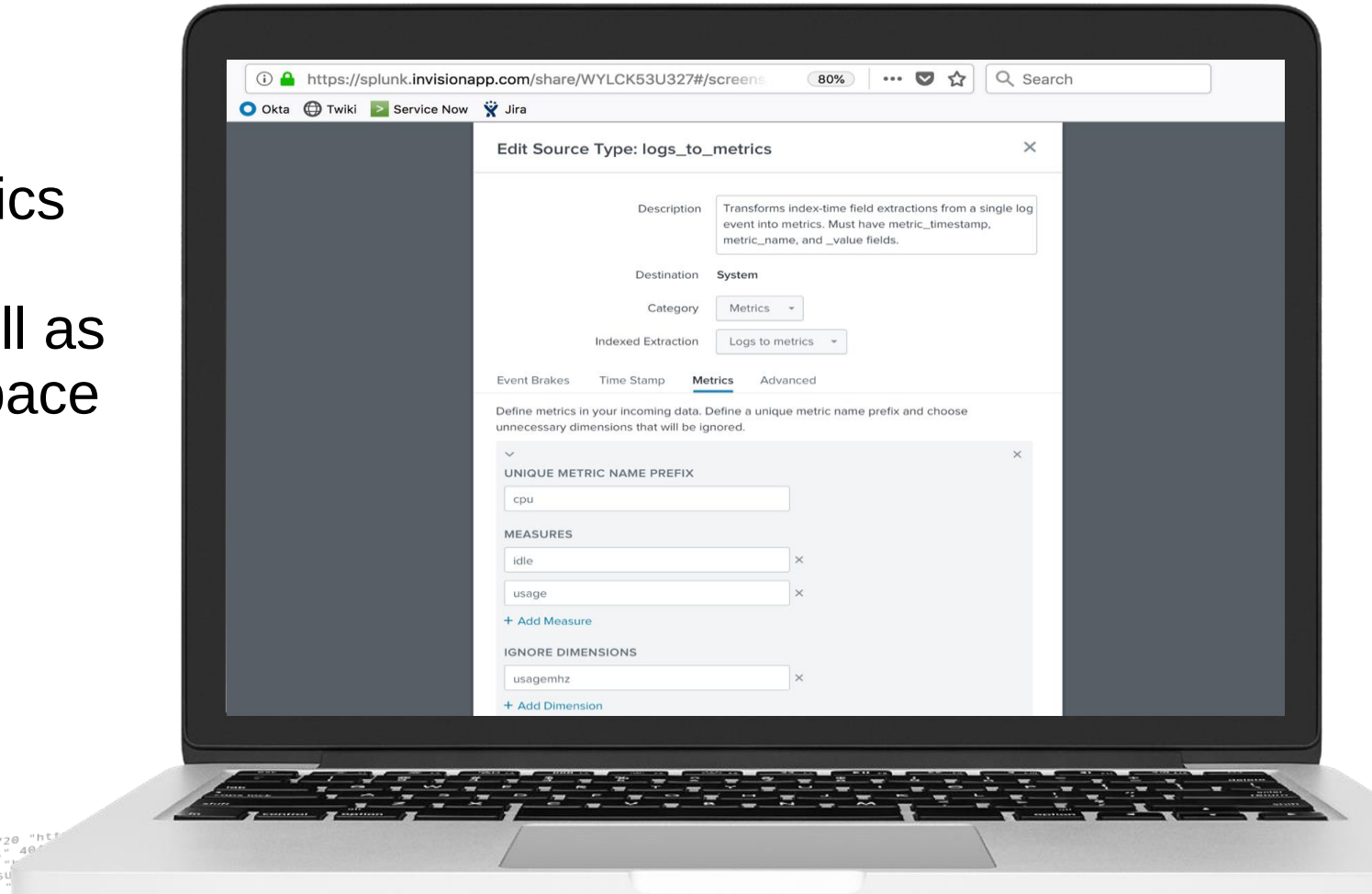
```
index=airline_data
| stats avg(ArrDelay) as AvgDelay by Dest, Origin, UniqueCarrier
| eval _value=AvgDelay
| eval metric_name="AvgDelay"
| table Dest, Origin, UniqueCarrier, metric_name, _value
| mcollect index=airline_metrics_index
```

```
| 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



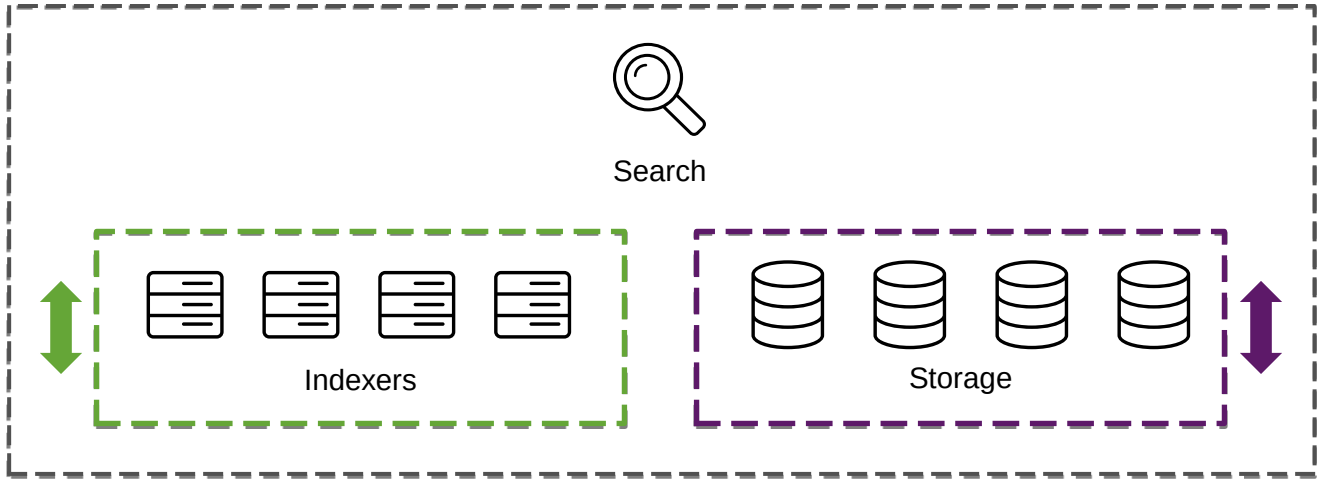
Splunk Management Improvements

splunk> .conf18

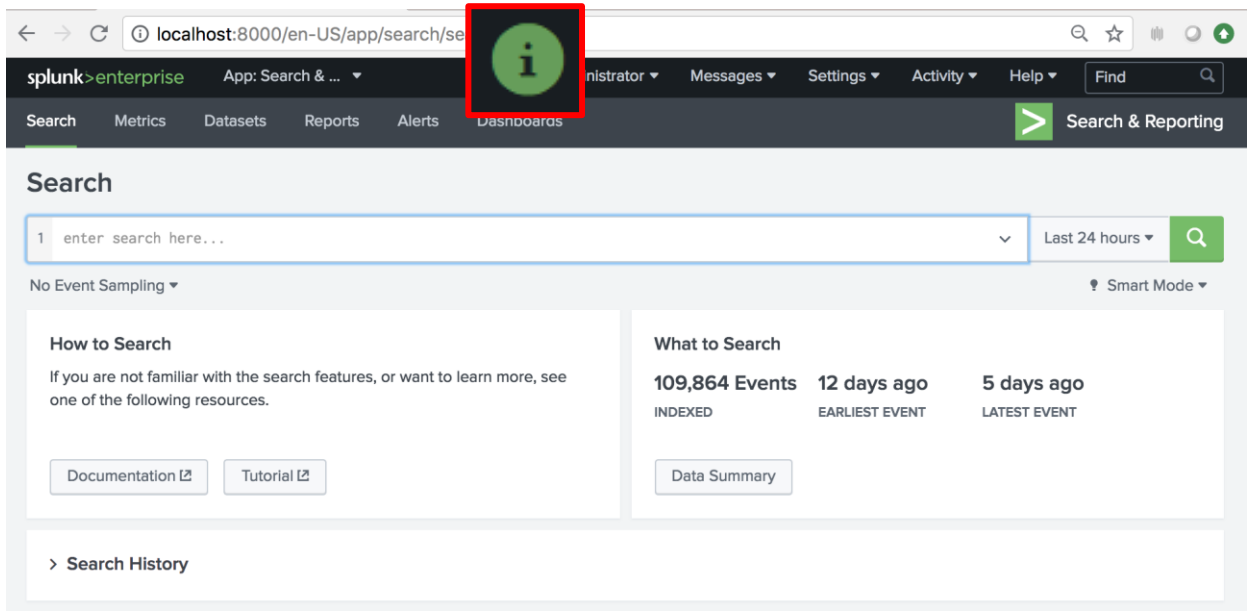
SmartStore

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



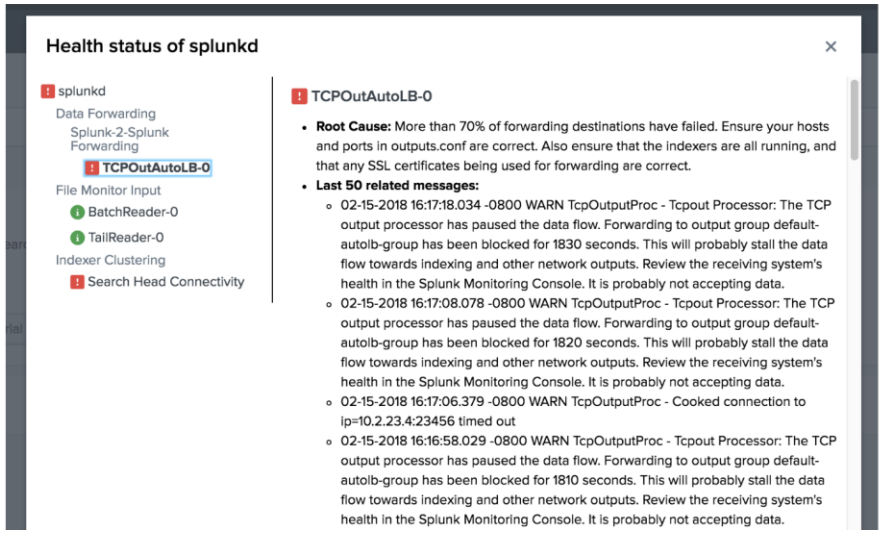
Proactive Splunk Component Monitoring



- 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

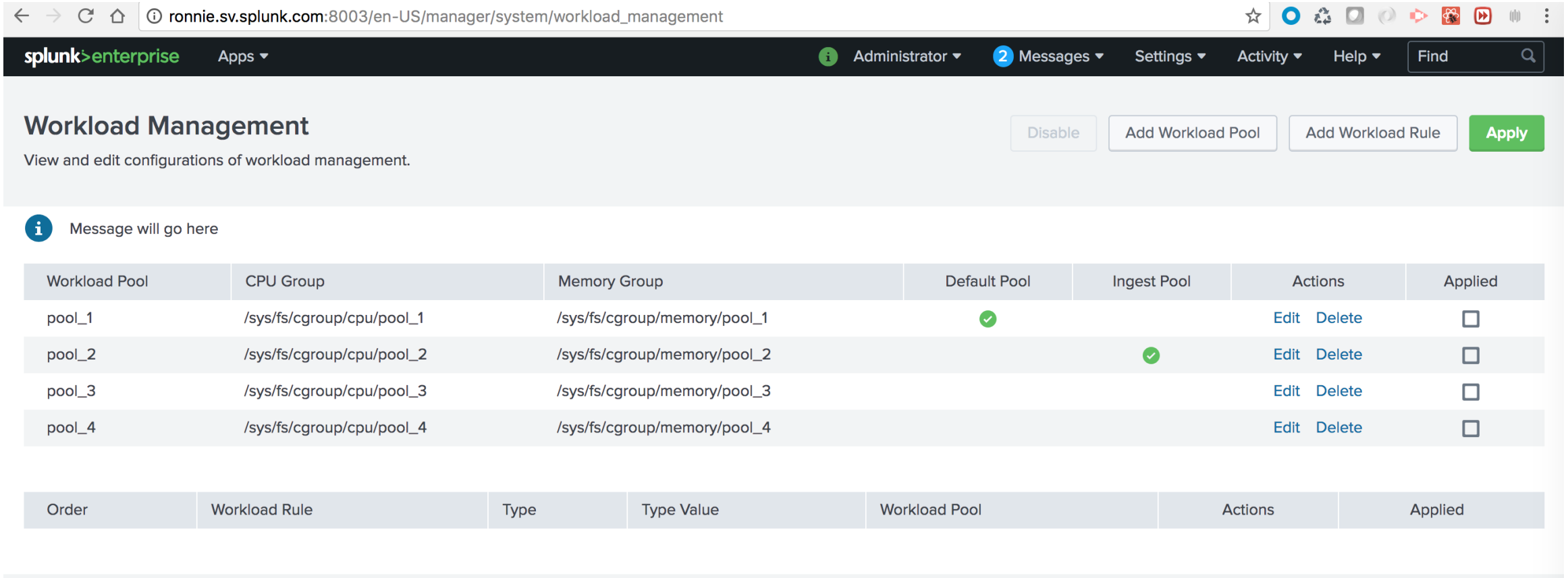
Splunk health status pop up

Forwarding alert with root cause and related messages



Workload Management

Prioritize and manage search and ingestion resources to meet business needs



splunk> .conf18

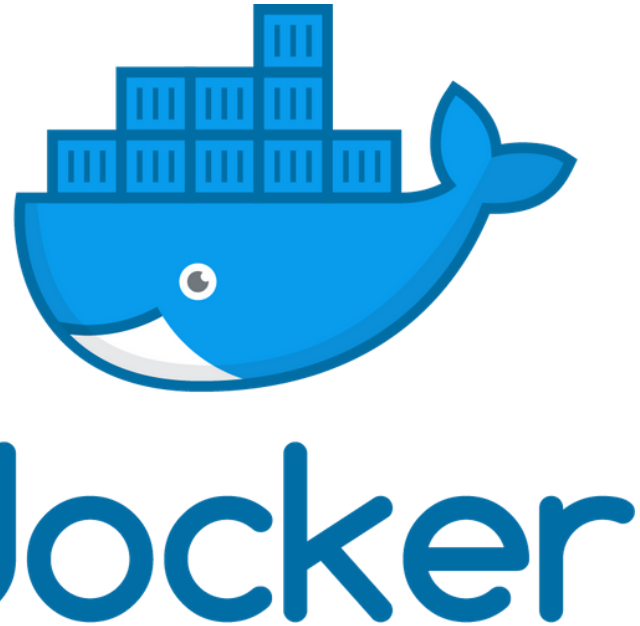
Password Management

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

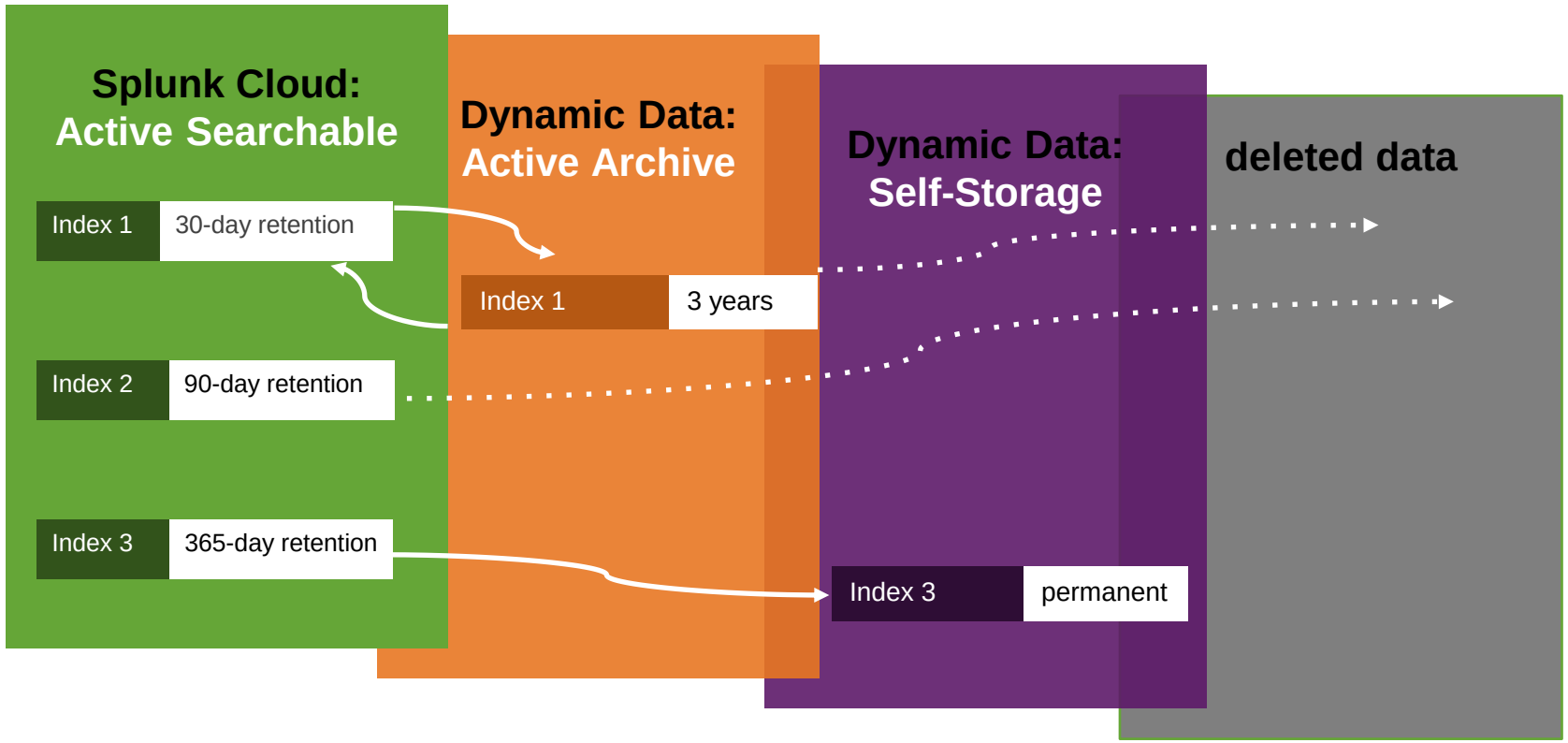
Retain *infrequently accessed* data to meet compliance requirements.
Easily resurrect to *search when required*.

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

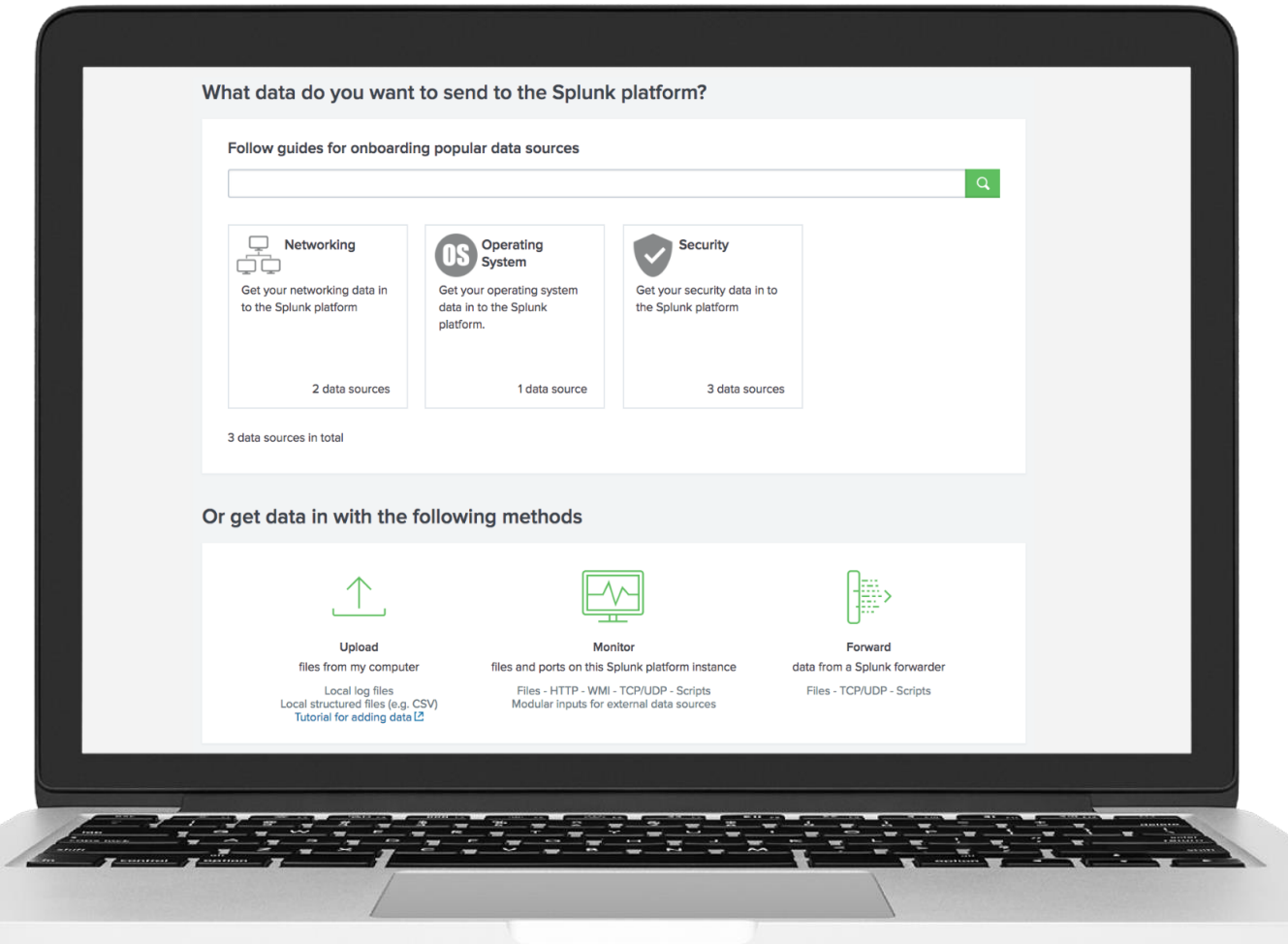
Leverage more data

splunk> .conf18

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

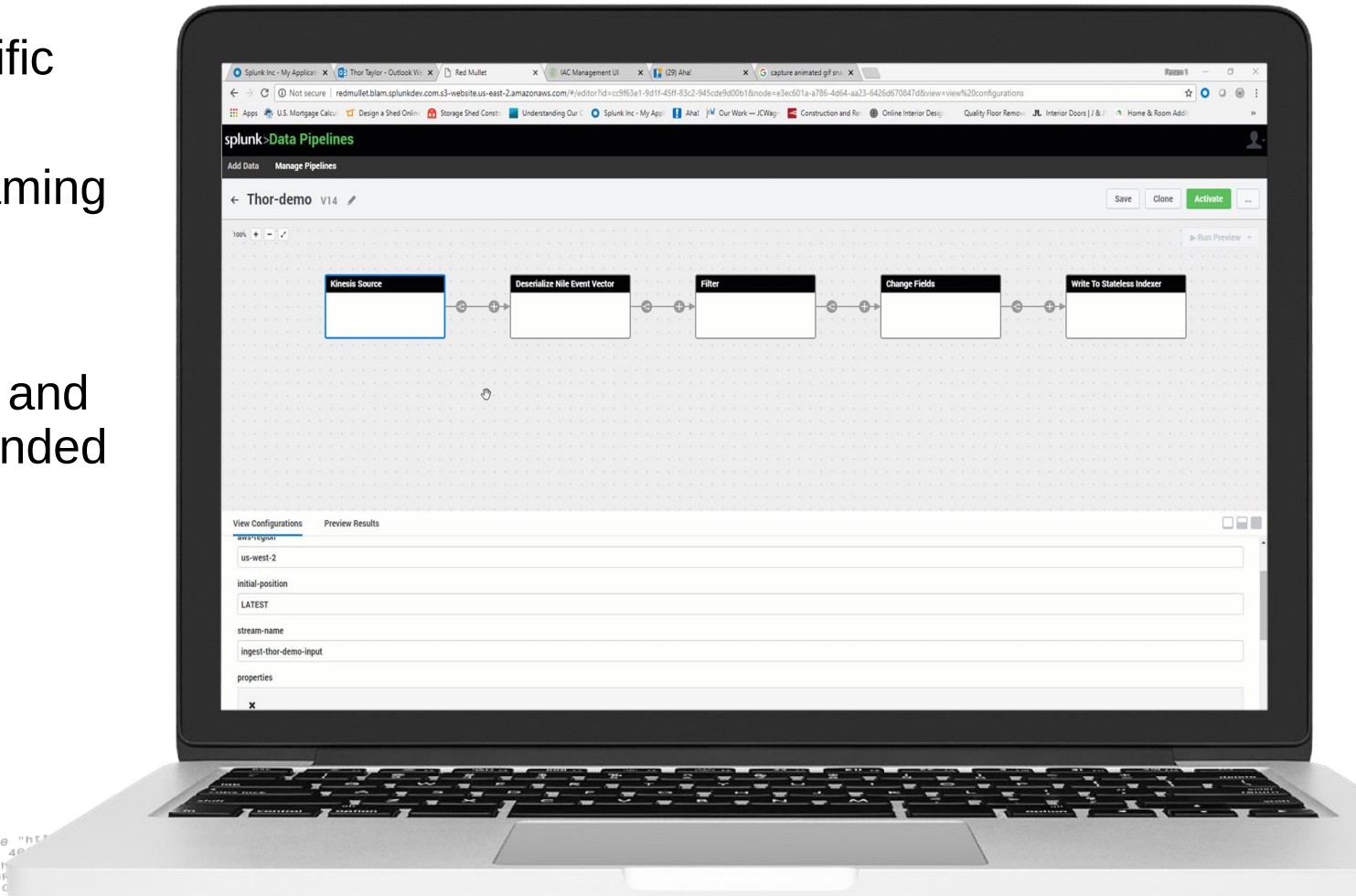


BETA

Data Stream Processor

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

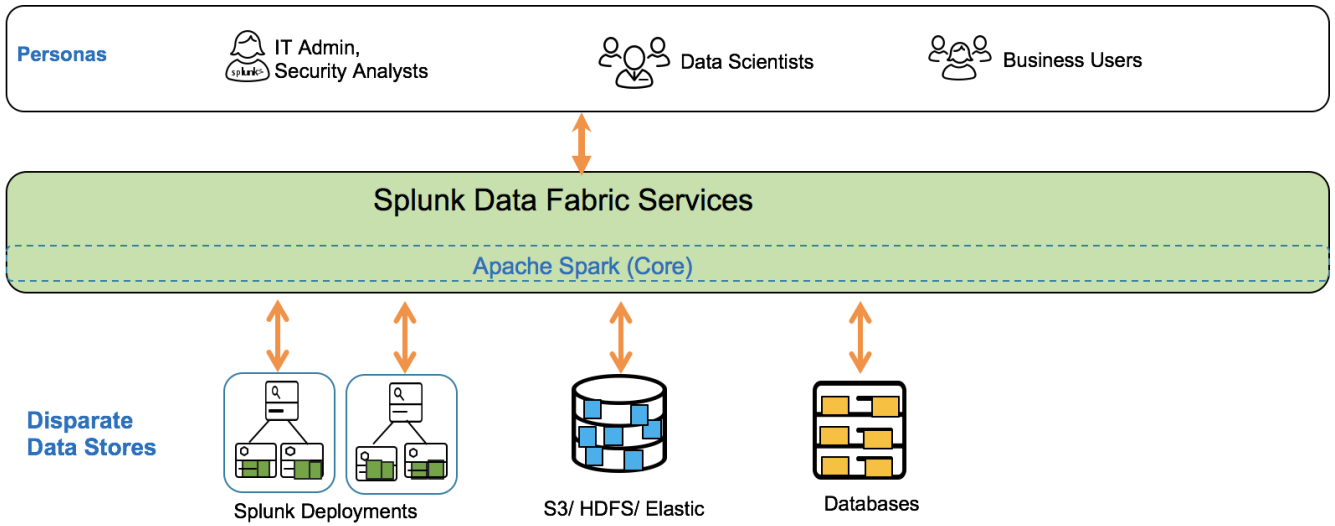
- Customize capabilities and meet specific use cases using our open APIs
- Connect to any data — at rest or streaming
- Refine, modify or adjust data before it reaches its destination
- Track data through the entire pipeline, and ensure it successfully reaches the intended destination



Data Fabric Search

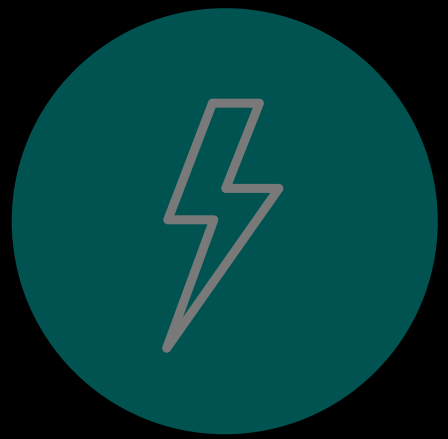
Search trillions of events at ease — single instance or Splunk 2 Splunk

- 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

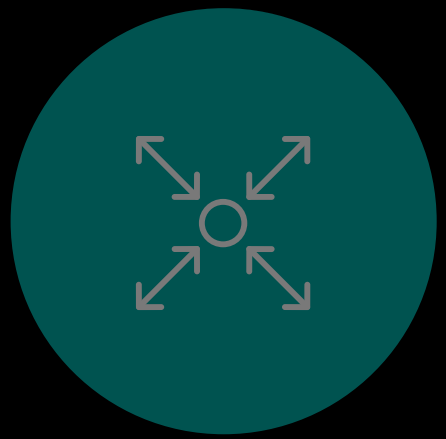


Artificial intelligence and machine learning integrated throughout platform

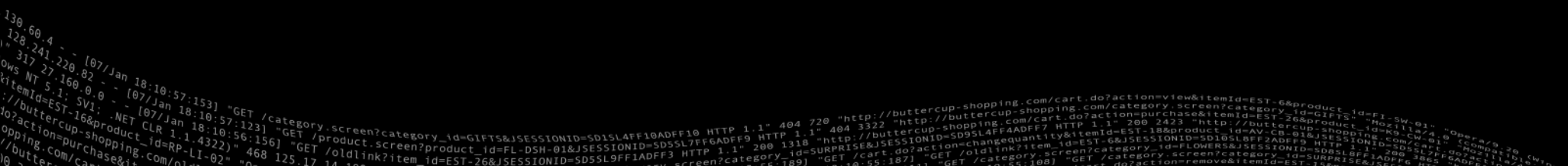
Limitless exploration and investigation



Leadership in performance, scale and manageability



Splunk *and* expansive ecosystem



splunk> .conf18

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

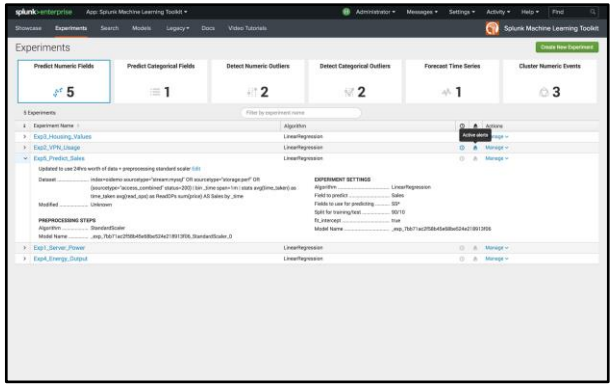
Splunk Platform
Customizable AI and ML for all use cases

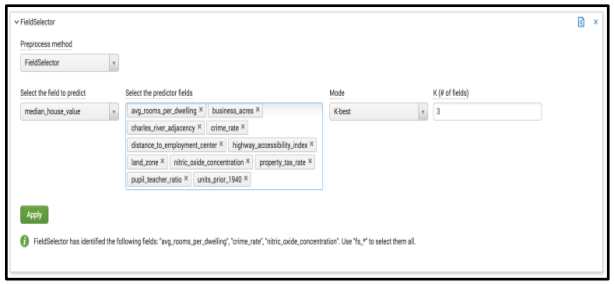
New with MLTK 4.0

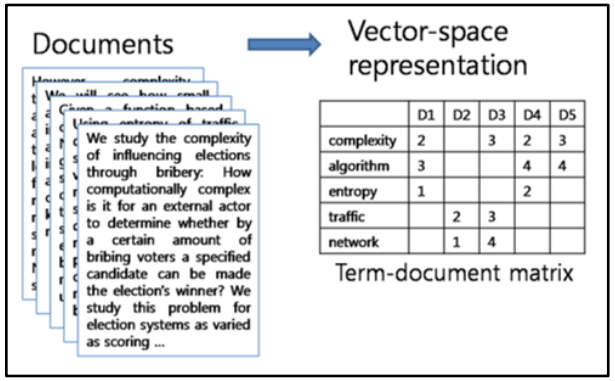
1. **Splunk Community for MLTK Algorithms on GitHub**
   Enables Splunk MLTK users to share code and custom algorithms, get feedback and tips from fellow Splunk MLTK users, as well as the Splunk team and other GitHub community members.

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.







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

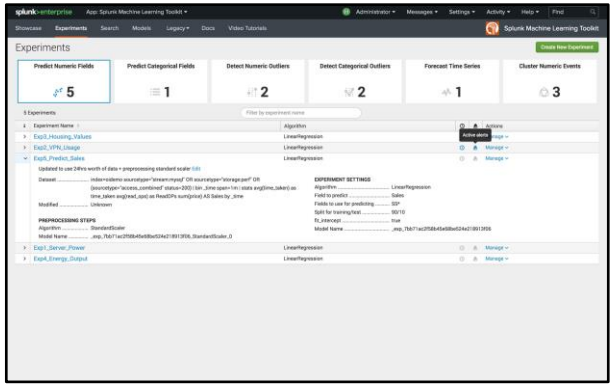
splunk> .conf18

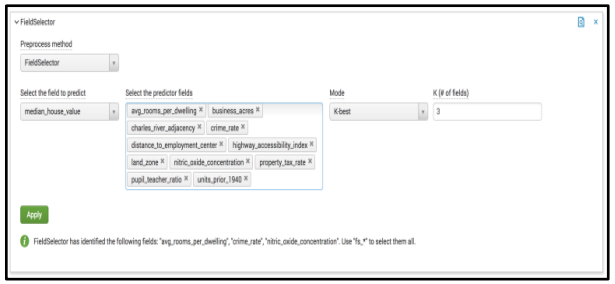
New with MLTK 3.2

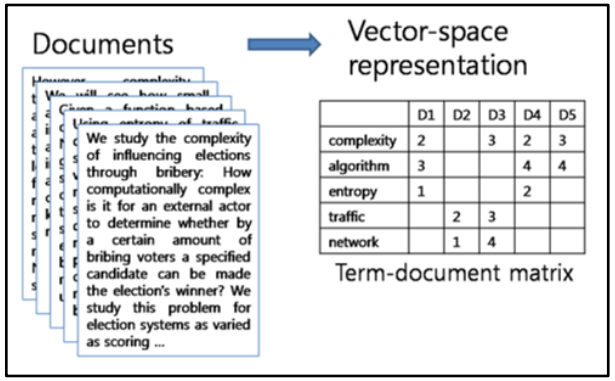
1. **Experiment management framework**
   This new, intuitive interface gives you the ability to view, control, share and monitor the status of your machine learning experiments.

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.







splunk> .conf18

Thank You

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