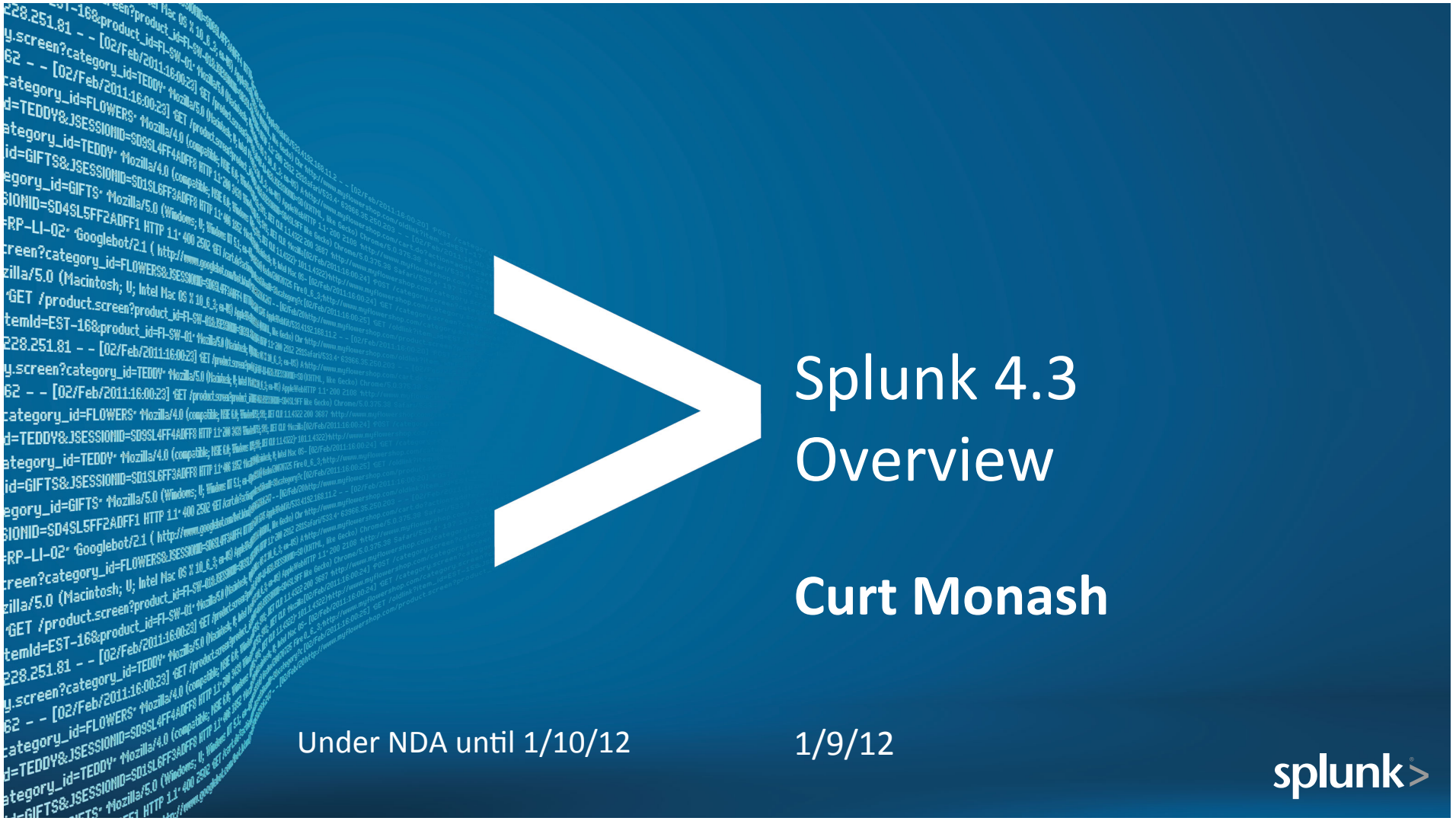


Splunk 4.3 Overview

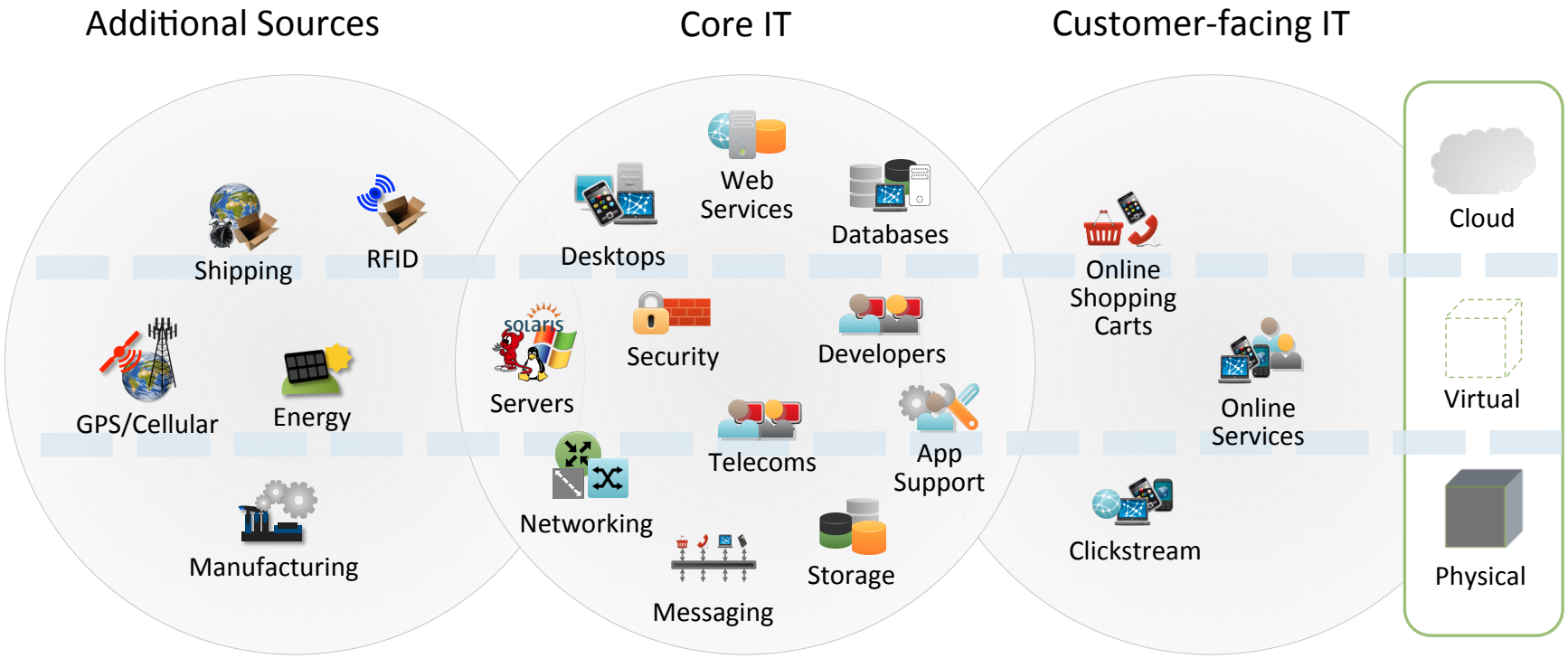
Curt Monash

Under NDA until 1/10/12

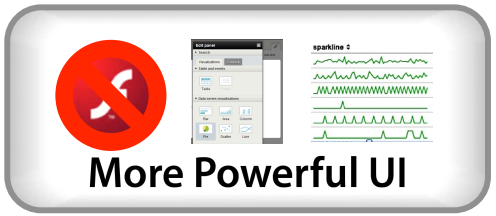
1/9/12

splunk>

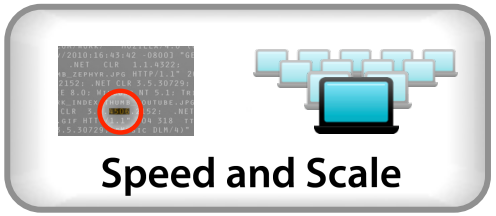
Most Enterprise Data is Machine-generated



Splunk Product Priorities



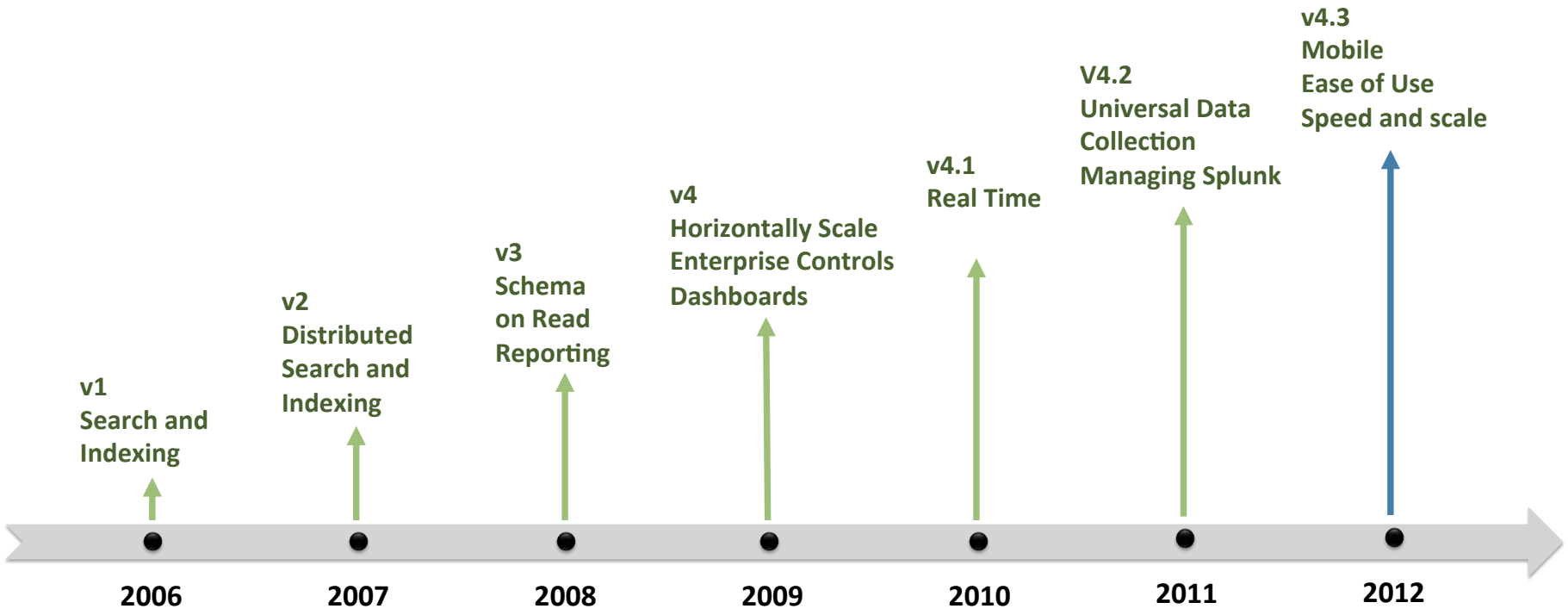
Make Splunk UI easier, more usable for IT users and business users



Drive enterprise-class performance and scalability for mission critical use

Make Spunk easier to administer for complex enterprise deployments

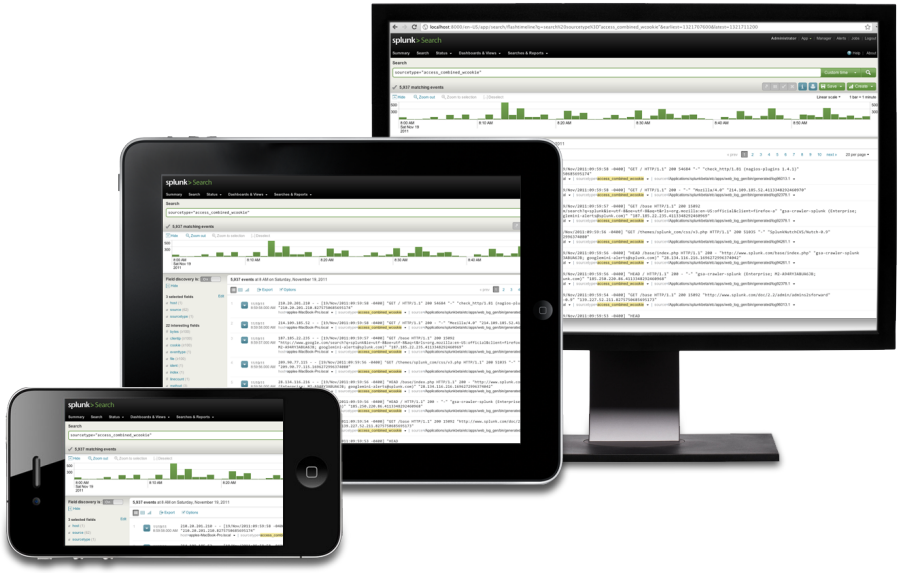
Continuous Development for Over 8 Years



Non-Flash User Interface

Operational Intelligence is now Mobile

- Same UI now offers Flash free charts and timelines
- Supports iOS and other mobile devices
- Support browsers that do not have Flash installed
- Use Splunk anywhere



"We have 2700 users of Splunk and being able to provide dashboards on iPads means we can get more data to more people when they want it."

Eddie Satterly, Sr. Director, Infrastructure Architecture and Emerging Technologies, Expedia

Non-Flash UI: A Big Hit

"Splunk is already fast and agile for turning around ad hoc requests from the business. Typically about a day, compared to 6 months for the BI team. With 4.3 we're ahead of the pack in supporting non-flash UI."

Systems Engineer
Top 5 Financial
Services Company

"We use Splunk to rapidly identify errors and the business impact of problems in our environment. Enabling our management to view Splunk dashboards and reports on mobile platforms will help us more effectively remediate issues."

Michael Otremba
Senior Manager of
CRM Software Development,
Otto Group

"Splunk 4.3 is wicked. Having Splunk reports available on our mobile devices is amazing since there has been an explosion of iPads within our office."

Derek Mock
Director of
Software Development,
Ceryx

Live Demonstration

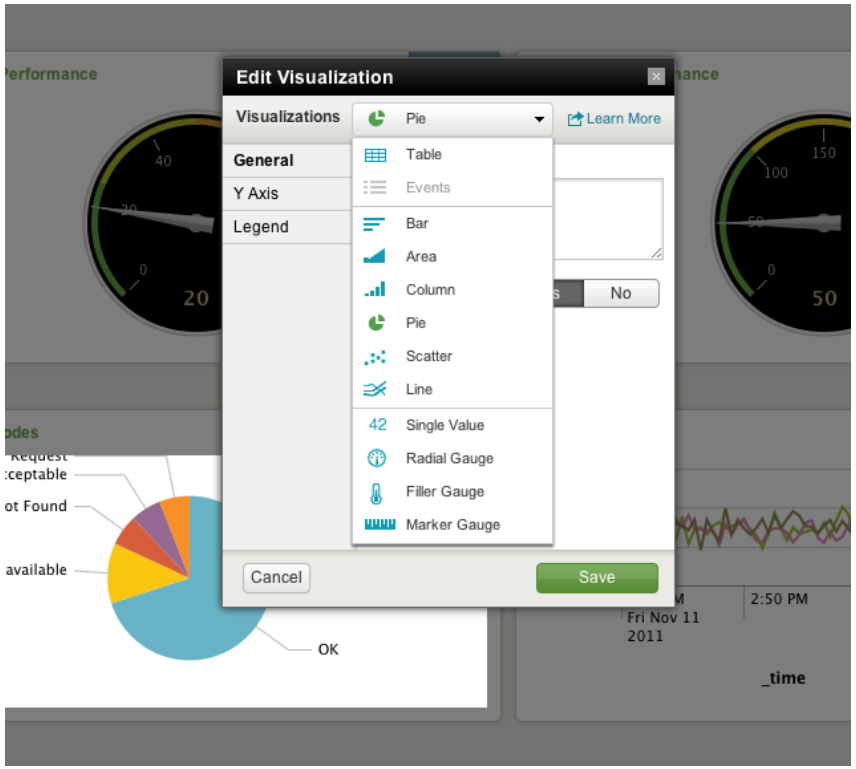
splunk>

>

Visual Dashboard Editor

Easier for Business Users

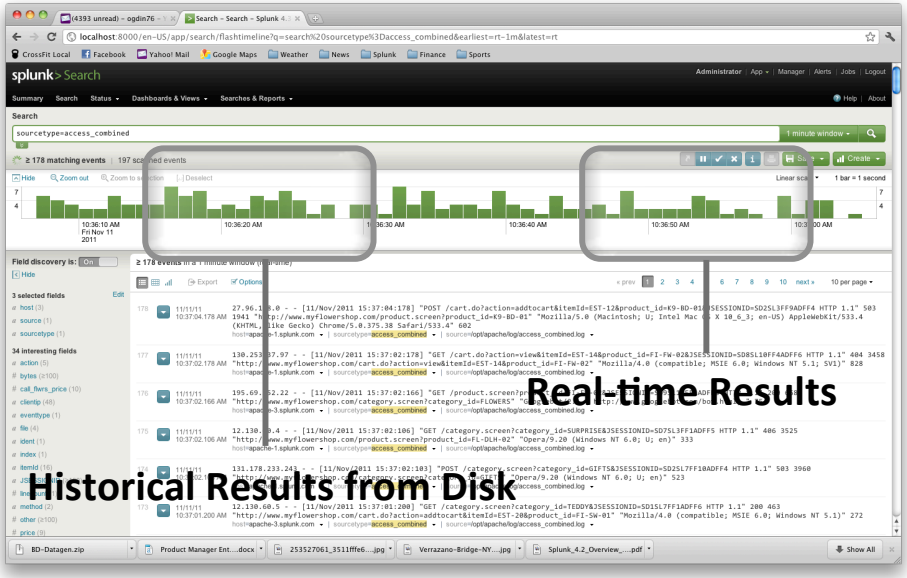
- Define and edit dashboards through a simple UI
- Change chart types with integrated chartings controls
- Drag-and-drop dashboard editing
- Enables self-service



Real-time Backfill

Simplified real-time and historical analysis

- Combines real-time and historical data in a single chart
- Monitor real-time events over longer windows of time
- Ensure greater accuracy



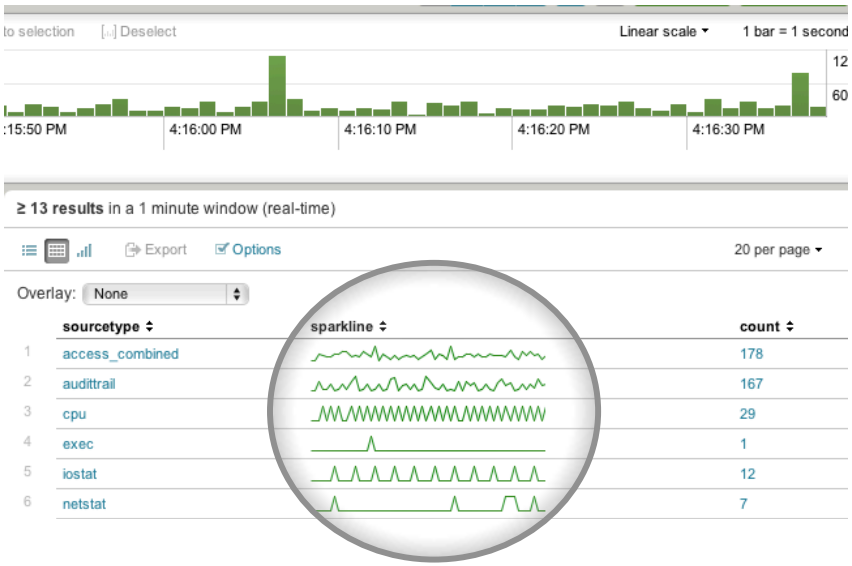
"Real-time back-fill enables me to quickly identify issues on our web proxies. I can visualize everything at one time and capture the historical errors and new errors as the client is seeing it."

Network Administrator, Top 5 Energy Company

Sparklines

Vital granular trend data at-a-glance

- Show time series trends for multiple events together
- New search command adds sparklines to results table
- Add to a dashboard and run in real time for up to the second visibility into trends



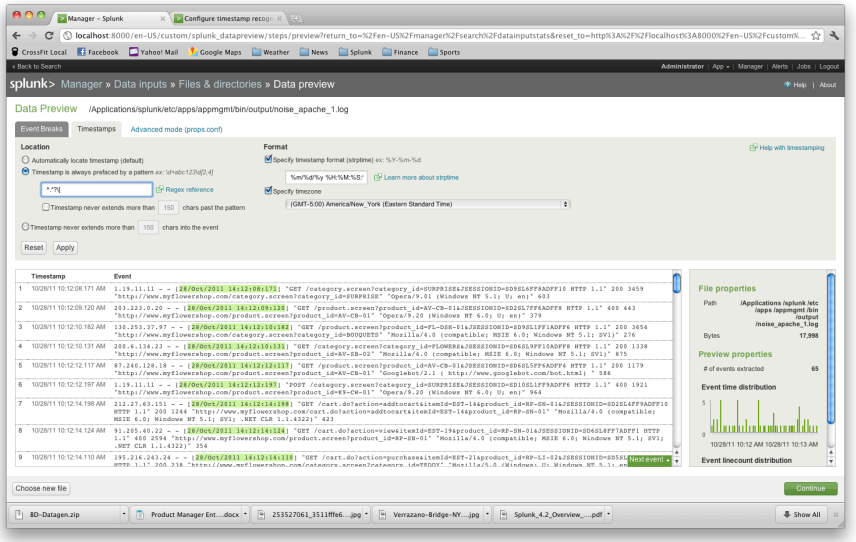
"With 2000 stores we have a lot going on. Sparklines means that we can now very quickly spot trends and quickly spot when something is going to happen."

Large nationwide home improvement retailer

Data Input Preview

Preview new data sources before indexing

- See what data sources are about to be indexed
- Test new data sources and troubleshoot
- Preview how event extractions will be handled
- Speeds time-to-deploy



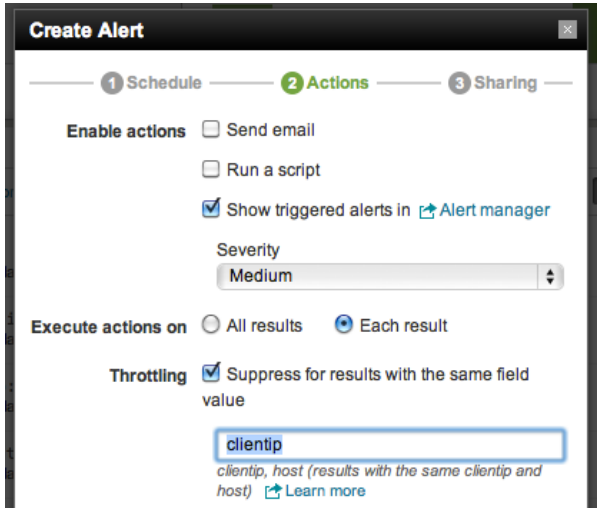
"The data preview feature speeds up the administration of Splunk and saves time so I can deliver services faster to customers and clients."

Thomas Paulsen, Systems Administrator, Otto Group

Per-result Alerting

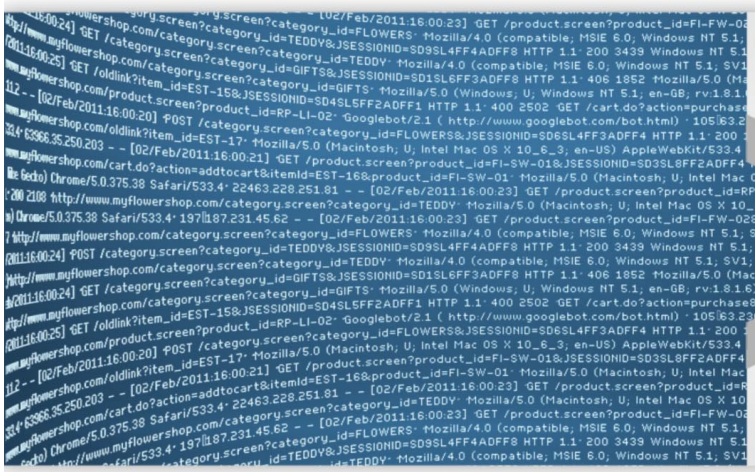
Expanded controls for operational monitoring

- Improved alerting granularity
- Define alerts that trigger based on single events rather than a group of events
- New "digest" field for grouping alert notifications



"Per-result Alerting allows us more granular control over the notifications we receive when using Splunk to monitor our messaging infrastructure for abuse."

Mika Borner, Head of Internet Messaging, Swisscom



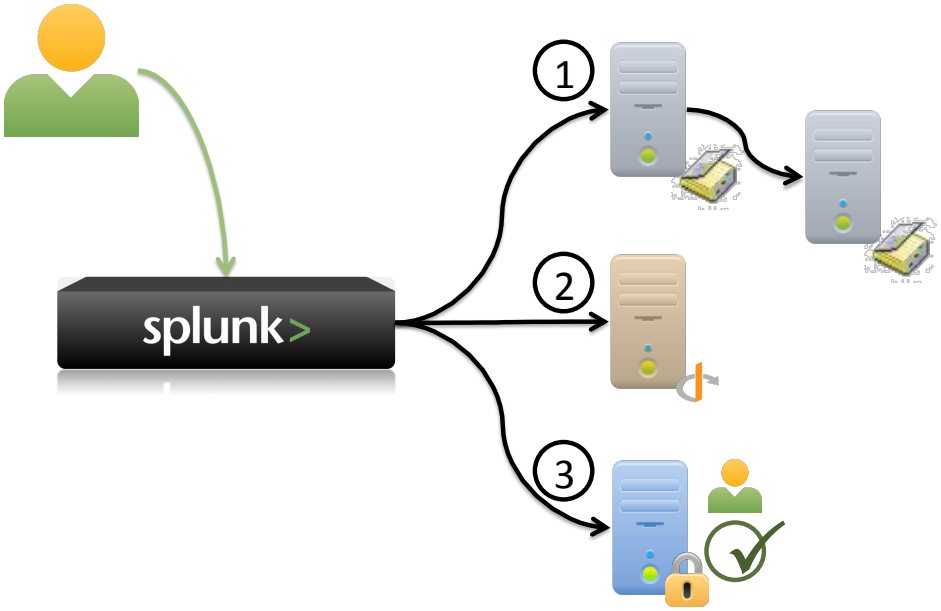
Other New Features in 4.3

splunk>

Multi-domain LDAP

Easier to extend Splunk to more of the organization

- Expand Splunk across departments where different AAA systems are in use
- Easier alignment to more complex enterprise security policies



"Almost everything I do using Splunk's UI takes half the time in 4.3. New features mean that I am able to do so much more in a more intuitive way."

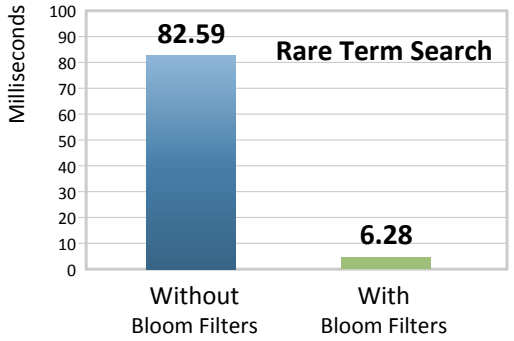
Expedia

Eddie Satterly
Sr. Director, Infrastructure Architecture
and Emerging Technologies

Faster, More Scalable

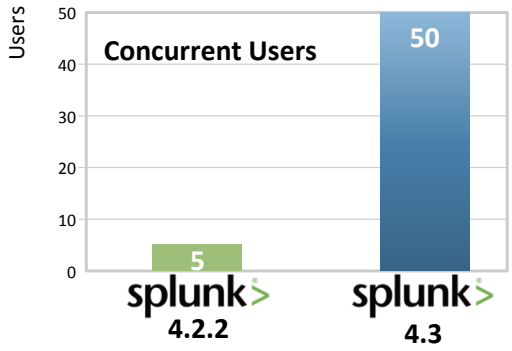
Up to 10x Faster "Needle in a Haystack" Search

- New Search bloom filters
- Rule out where not to search before incurring overhead of searching
- Easy to configure and use



10x More Concurrent Users

- Splunk server now allows many more active users per search head
- Enables more concurrent users on same Splunk deployment
- Scales to thousands of Splunk users



Additional Capabilities

Structured Data Field Extraction

- Easily extract data from structured data formats (XML, JSON)

IPv6 Support

- Splunk now supports using IPv6 addresses for all network activity
- Use Splunk transparently while migrating the network to IPv6

Per-user Time zones

- Enable setting a time zone for each user
- Users can now see the data in the time zone they're in

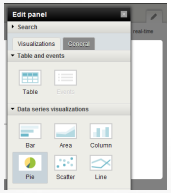
"Per-user time zones enables seamless collaboration with team members in other locations."
Top 5 Media, Entertainment and Communications Company

Splunk 4.3 Recap

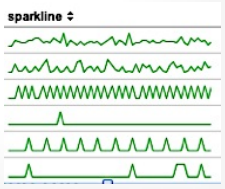
More Powerful UI

**Mobile –
Non-Flash UI**

**Integrated Real-time
and Historical Search**



**Visual
Dashboard Editor**



**Sparklines
Visualizations**

Speed & Scale

**10X More
Scalable UI**

**10X Faster
"Rare" Search**

Manageability

**Data Input
Preview**

**Multi-domain
LDAP**

Splunk 4.3: The Best Splunk Yet

- **Mobile** – new no-Flash user interface delivers the power of Splunk anywhere
- **More powerful** – new visualizations, up to 10x more concurrent users, up to 10x faster search
- **Easier to use** – easier exec-editable dashboards, easier manageability


splunk>