

Introducing Splunk 6



Safe Harbor Statement

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 Company Update

Company (NASDAQ: SPLK)

2004 founded

2006 first software
release

HQ San Francisco

Business Model / Products

On-premise

In the **cloud**

SaaS

Customers

6000+

60+ of the
Fortune 100

Largest license:

100 Terabytes/day

Industry Recognition

FAST COMPANY

#1 Big Data
Innovator

#4 Most
Innovative

Gartner

2013 SIEM Magic Quadrant
LEADER

2012 Security Market Growth
#1 Worldwide

2012 IT Operations Market Growth
#3 Worldwide



Best SIEM North America

**Best Enterprise
Security Solution EMEA**

The Accelerating Pace of Data

Volume | Velocity | Variety | Variability

Machine data is the fastest growing, most complex, most valuable area of big data



GPS,
RFID,
Hypervisor,
Web Servers,
Email, Messaging,
Clickstreams, Mobile,
Telephony, IVR, Databases,
Sensors, Telematics, Storage,
Servers, Security Devices, Desktops

What Does Machine Data Look Like?

Sources



ORDER,2013-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

Order Processing



May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213. Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException: weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port: ACMEDB-01:1521. Reason: Connection refused

Middleware Error

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type 0:19:9, App 0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-13ae51a6d092, Trunk T451.16



Care IVR

05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092 CUSTID 10098213
05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092



Twitter

```
{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:"http://dallascowboys.com/",location:{displayName:"Dallas, TX",objectType:"place"},objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if you hate @ACME!!",objectType:"activity",postedTime:"2013-05-21T16:39:40.647-0600"}
```

Machine Data Contains Critical Insights

Sources



Customer ID

Order ID

Product ID

ORDER,2013-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

Order Processing



May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213.

Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException:
weblogic.common.resourcepool.ResourceDeadException: Could not create pool. The
DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port:
ACMEDB-01:1521. Reason: Connection refused

Order ID

Customer ID

Middleware Error

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type
98#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-
13ae51a6d092, trunk 1451.16

05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092
CUSTID 10098213

05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

```
{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:
"http://dallascowboys.com/",location:{dis
Twitter ID "Dallas, TX",objectType
Customer's Tweet
objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought
this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if
you hate @ACME!!",objectType:"activity",postedTime:"2013-05-21T16:39:40.647-0600"}
```

Company's Twitter ID

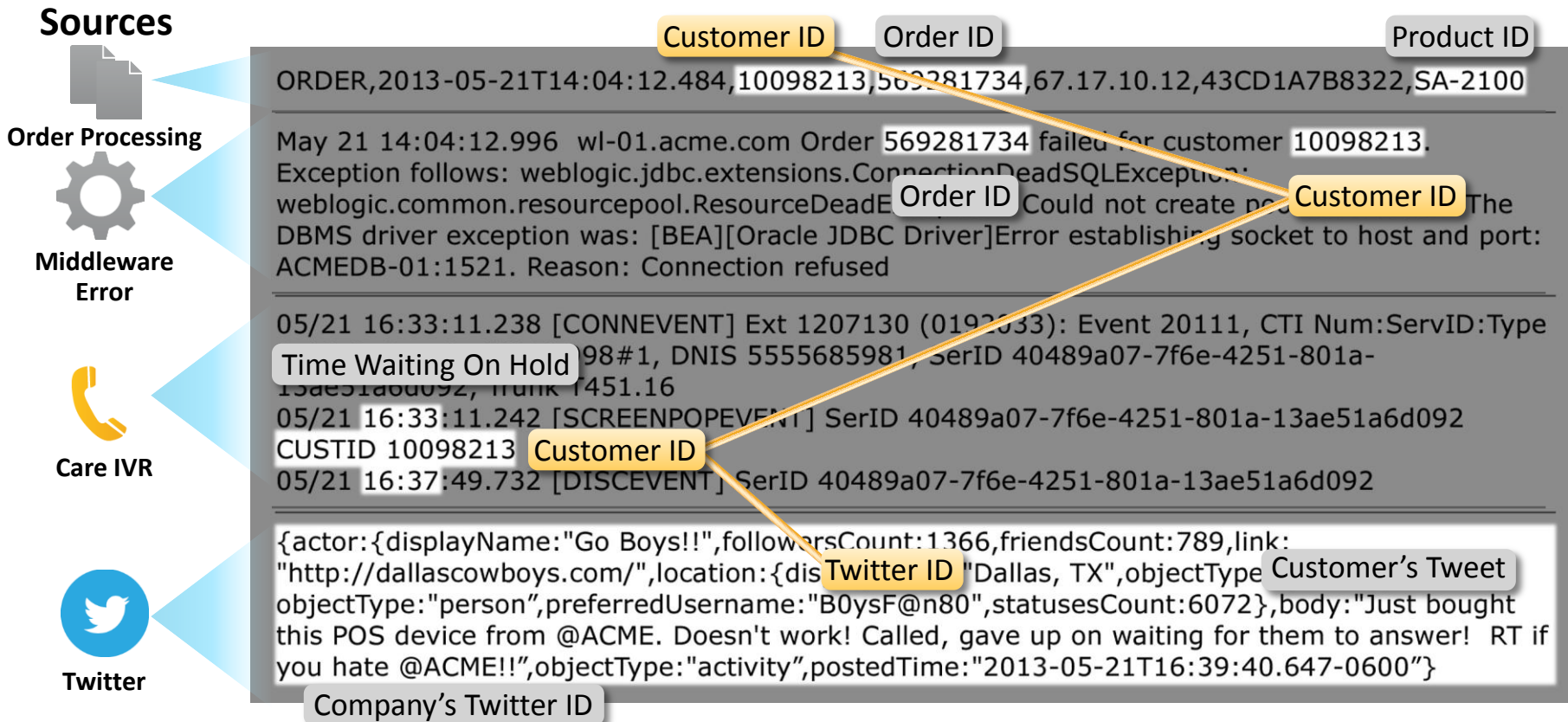


Care IVR



Twitter

Machine Data Contains Critical Insights



splunk

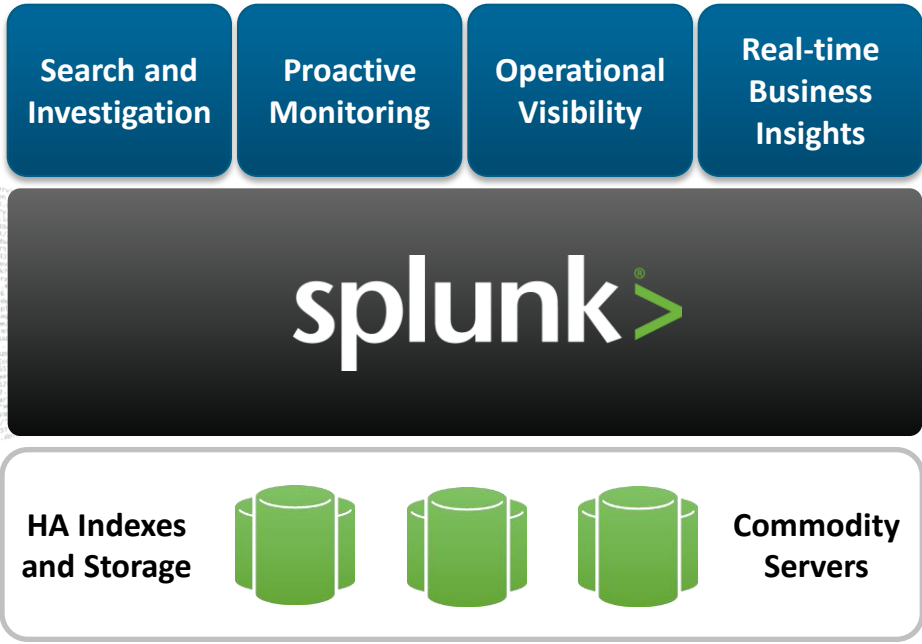
Make machine data accessible, usable
and valuable to everyone.

Industry Leading Platform for Machine Data

Any Machine Data



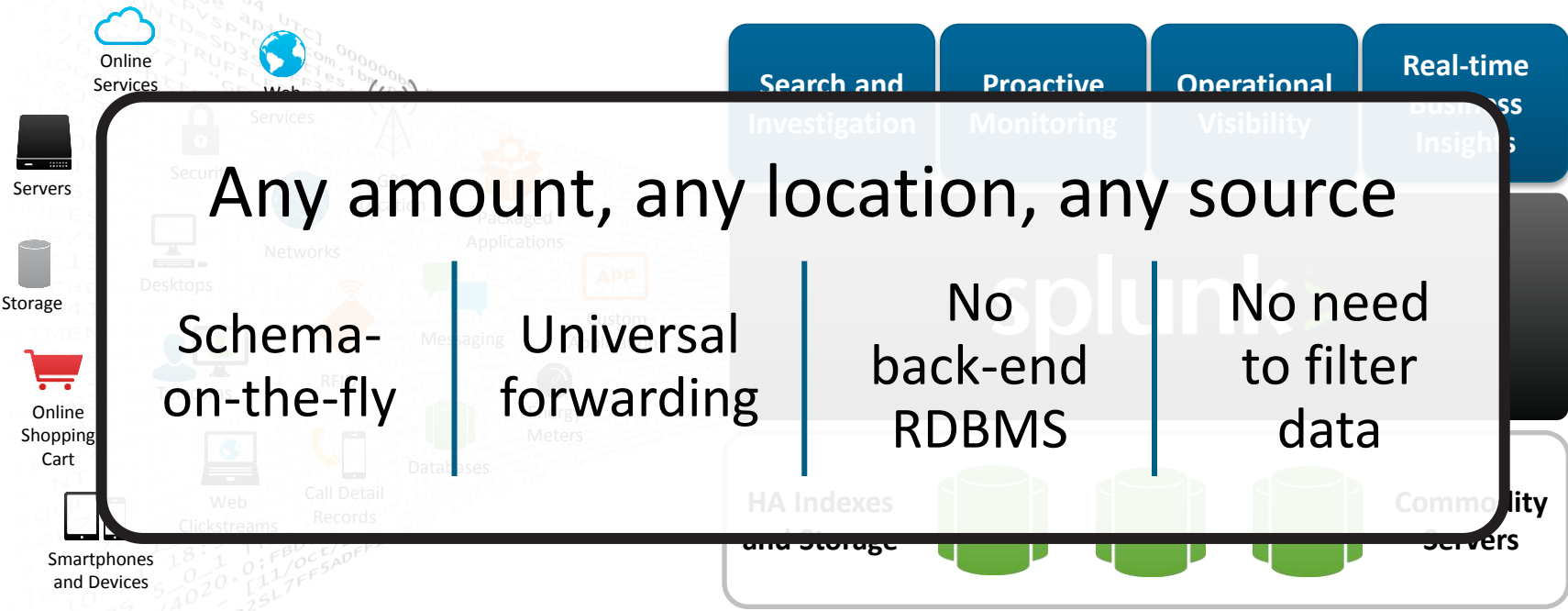
Operational Intelligence



Industry Leading Platform for Machine Data

Any Machine Data

Operational Intelligence

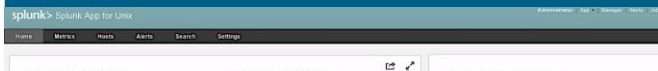


Turning Machine Data Into Operational Intelligence



Operational Intelligence for IT and Business Users

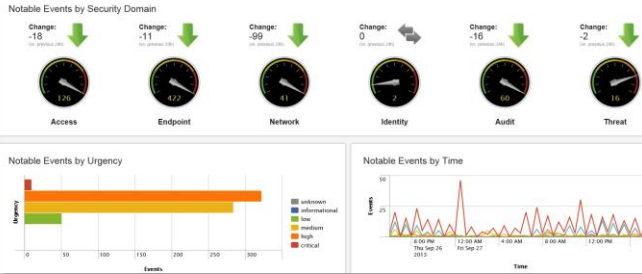
IT Operations Management



Application Management



Security and Compliance



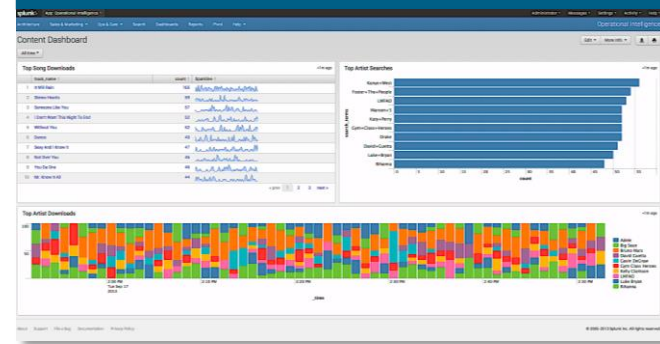
Industrial Data / Internet of Things



Digital Intelligence



Business Analytics



Customer Support

Operations Teams

System Administrator

Application Developers

Security Analysts

Auditors

IT Executives

Website/Business Analysts

LOB Owners/ Executives

Setting the Standard for Operational Intelligence

VERSIONS
1 2 3

Tool

“Google for the datacenter”

2006-2008

VERSIONS
4 4.1 4.2 4.3

Engine

“Engine for machine-generated data”

2009-2011

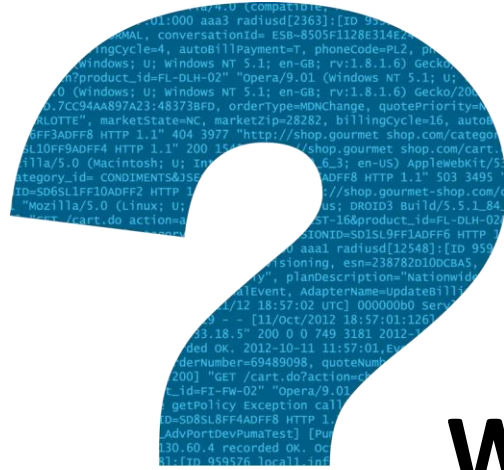
VERSIONS
5

Platform

“Platform for operational intelligence”

2012

What's Next



What do organizations need

Drive Value Across the Enterprise

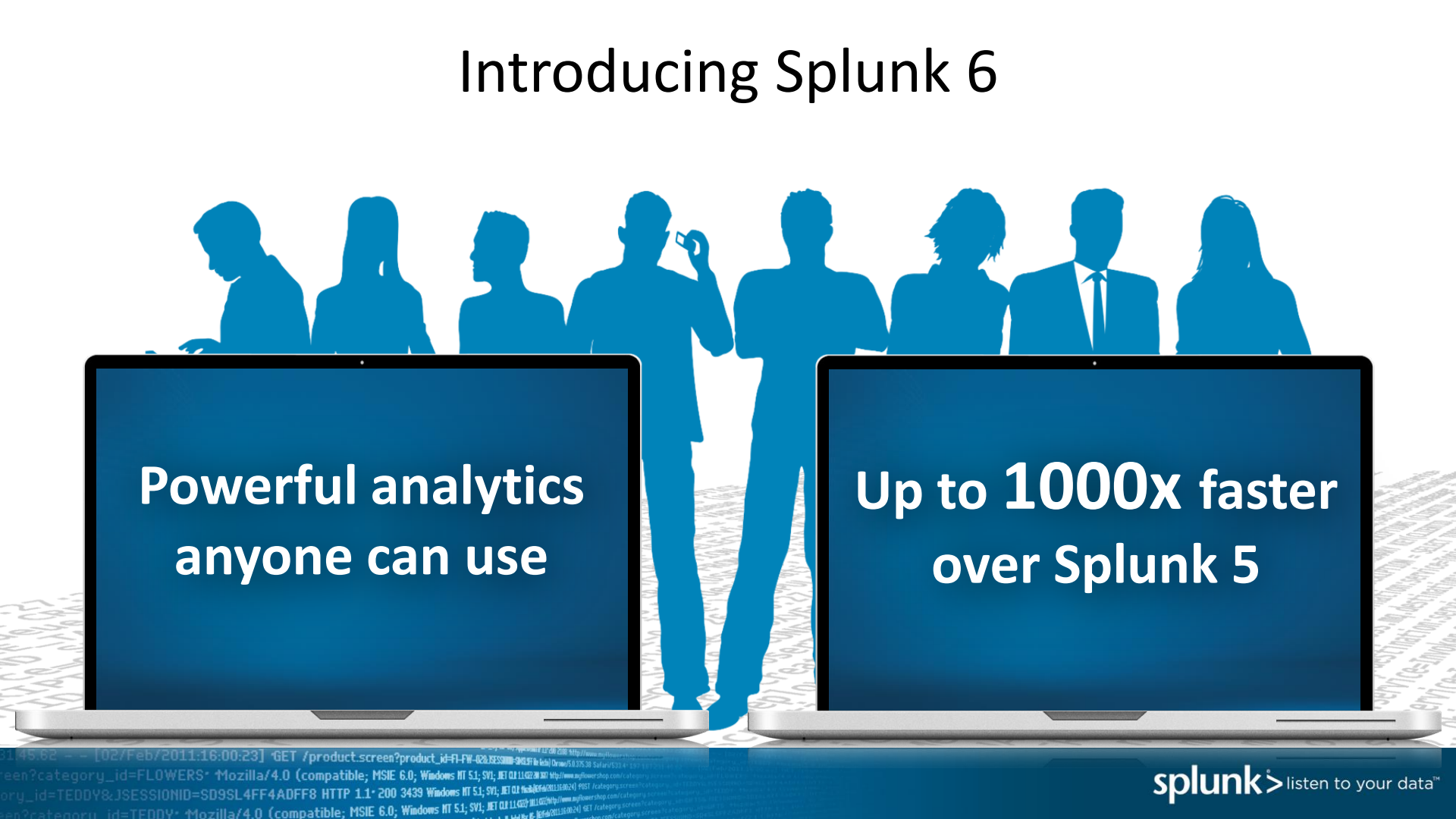
Deliver Operational Intelligence for Everyone

Enable faster and
easier analytics for
broader set of users

Simplify management
of enterprise Splunk
deployments

Accelerate development
of enterprise apps
using Splunk

Introducing Splunk 6



Powerful analytics
anyone can use

Up to **1000x** faster
over Splunk 5

Powerful Analytics Anyone Can Use



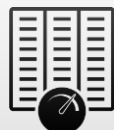
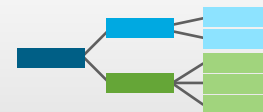
Pivot

Enables non-technical users to build complex reports without learning the search language



Data Model

Provides more meaningful representation of underlying raw machine data



Analytics Store

Acceleration technology delivers up to 1000x faster analytics over Splunk 5



```
1.45.62 -- [02/Feb/2011:16:00:23] GET /product.screen?product_id=FI-FW-4020-3E530000-540E5F161e1e3d http://www.splunk.com/...  
...?category_id=FLOWERS* Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322.2032) http://www.splunk.com/...  
...?category_id=TEDDY&JSESSIONID=3D9SL4FF4ADFF8 HTTP/1.1 200 3439 Windows NT 5.1; SV1; .NET CLR 1.1.4322.2032 http://www.splunk.com/...  
...?category_id=TEDDY* Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322.2032) http://www.splunk.com/...
```

Easy-to-use Analytics Interface



POWERFUL
ANALYTICS

Pivot

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

The screenshot shows the 'New Pivot' interface in Splunk. It displays a table of data with columns for 'Account Number', 'Count of Orders', and 'Count of is_Sales'. The interface includes a 'Filter' section with a 'Time Window' dropdown set to 'All time'. A 'Split Columns' section is visible, and a 'Save Report to share' button is located in the top right corner. A 'Chart Toolbox' is also present, indicating that all chart types are available.

All chart types available in the chart toolbox

Save Report to share

Time Window

Select fields from data model

Account Number	Count of Orders	Count of is_Sales
900000000	51	20
900000001	56	16
900000002		13
900000003		21
900000004		14
900000005	04	24
900000006	56	16
900000007	48	16
900000008	47	13

Deliver Analytics Up to 1000x Faster



POWERFUL
ANALYTICS

High Performance Analytics Store

- Transparent acceleration technology
- Retrieval speeds up to 1000x faster than previous Splunk versions
- Used to accelerate data models - created at the click of a button

Edit Acceleration

Data Model: Operational Intelligence Demo

Accelerate: Check to enable acceleration of data model

Acceleration may increase storage and processing costs.

Summary Range: 1 Day

Time window of data that is accelerated

Cancel Save

Data Models

Data models enable users to easily create reports in the Pivot tool.

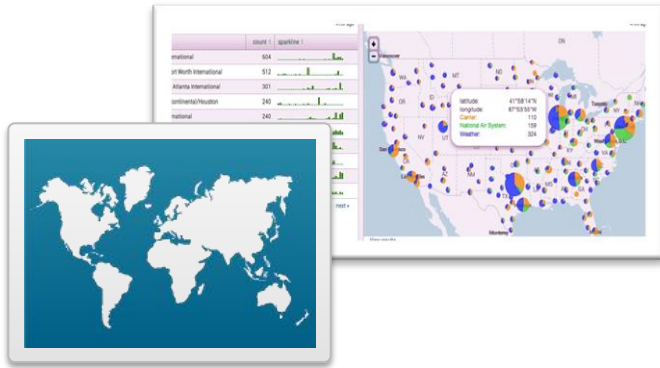
App: Operational Intelligence (oldemo) Created in the App

Title
Operational Intelligence Demo
A data model to support the Operational Intelligence Demo
MODEL
Objects 15 Events Edit
Permissions Shared in App. Owned by nobody. Edit
ACCELERATION
Model is not accelerated. Add

Additional Analytics Features

Maps

- Integrated GeoIP map that display geographic data and summaries



Predictive Analysis

- Find patterns in data to predict system capacity and resource utilization



Powering Security Intelligence



POWERFUL
ANALYTICS

Splunk Enterprise 6

- Normalization without data reduction
- Customized for different data types
- Supports converged IT Security and IT Operations data ontologies
- Support for fast reporting

Data Models

Data models enable users to easily create reports in the Pivot tool. [Learn More](#)

App: Home (launcher) Visible in the App Owner: Any filter

i	Title ^	Actions	App	Owner	Sharing
▶	Alerts	Edit Pivot	SA-CommonInformationModel	nobody	Global
▶	Application State	Edit Pivot	SA-CommonInformationModel	nobody	Global
▶	Assets And Identities	Edit Pivot	SA-IdentityManagement	nobody	Global
▶	Authentication	Edit Pivot	SA-CommonInformationModel	nobody	Global
▶	Change Analysis	Edit Pivot	SA-CommonInformationModel	nobody	Global
▶	Compute_Inventory	Edit Pivot	SA-CommonInformationModel	nobody	Global
▶	Incident Management		SA-ThreatIntelligence	nobody	Global
▶	Intrusion Detection		SA-CommonInformationModel	nobody	Global
▶	Malware		SA-CommonInformationModel	nobody	Global
▶	Network Traffic		SA-CommonInformationModel	nobody	Global
▶	Performance	Edit Pivot	SA-CommonInformationModel	nobody	Global
▶	Splunk Audit Logs	Edit Pivot	SA-CommonInformationModel	nobody	Global
▶	Threat Lists	Edit Pivot	SA-ThreatIntelligence	nobody	Global
▶	Updates	Edit Pivot	SA-CommonInformationModel	nobody	Global
▶	Vulnerabilities	Edit Pivot	SA-CommonInformationModel	nobody	Global
▶	Web	Edit Pivot	SA-CommonInformationModel	nobody	Global

Example of security data models

01:45:52 -- [02/Feb/2011:16:00:23] GET /product.screen?product_id=FI-FW-4020.83533000-540251 (Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322.5060; Safari/523.4))

...?category_id=FLOWERS: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322.5060; Safari/523.4)

...?category_id=TEDDY&JSESSIONID=3D9SL4FF4ADFF8 HTTP 1.1 200 3439 Windows NT 5.1; SV1; .NET CLR 1.1.4322.5060; Safari/523.4

...?category_id=TEDDY: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322.5060; Safari/523.4)

Other New Features in Splunk 6



INTUITIVE USER EXPERIENCE

Improve users' productivity enabling instant access to relevant apps and content



SIMPLIFIED MANAGEMENT

Deliver simplified and scalable management for enterprise Splunk deployments



RICH DEVELOPER ENVIRONMENT

Rapidly build Splunk apps using standards-based web technologies

Increased User Productivity



INTUITIVE USER
EXPERIENCE

New Home Screen

- New menu system enables rapid navigation to apps, data and content relevant to user
- Removes need to open apps in order to explore content
- Customizable to different users and roles

The screenshot shows the Splunk Home interface. At the top, there is a navigation bar with 'splunk> Apps', 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below this is a 'Home' section with a search bar labeled 'Search Bar' and a dropdown menu for 'App: Search & Reporting' and 'Last 15 minutes'. The main content area is divided into several sections: 'Apps' (Operational Intelligence, Simple XML Tests, Bubbles Beta, CloudPassage), 'Search & Reporting', and 'Data' (Add Data, Events Indexed: 12,801,200, Earliest Event: a month ago, Latest Event: a few seconds ago, Manage Inputs). A callout box labeled 'Splunk Apps' points to the 'Operational Intelligence' app card. Another callout box labeled 'Add Data Source' points to the 'Add Data' button in the 'Data' section.

Redesigned Search and Reporting



INTUITIVE USER
EXPERIENCE

Enhanced Search Experience

- Search and analyze data from a unified interface
- Simplified authoring and editing of reports
- Instantly navigate to create new visualizations, tables and dashboard panels

Access Reports and Dashboards Search & Reporting >

Search Bar

Search Results

Search & Reporting >

New Search

33,638 Events INDEXED 1 year, 2 months ago EARLIEST EVENT 1 month, 19 days ago LATEST EVENT

Data Summary

33,638 events (9/26/12 8:28:41 AM to 6/12/13 9:03:42 AM PM)

Events (33,638) Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Direct

Time	Source	Event Type
04/24/2013 00:01:50 AM	LogName=Security	LogName=Security
04/24/2013 00:01:46 AM	LogName=Security	LogName=Security

Centralized Cluster Management



SIMPLIFIED
MANAGEMENT

Simplified Cluster Management

- Monitor Splunk high availability services for business critical deployments at scale
- Automatic search workload and data rebalancing when clusters change
- Easier and more transparent app deployment to indexers
- Faster recovery from failures

The screenshot displays the Splunk Cluster Health dashboard for a Master Node. At the top, it shows three green checkmarks indicating that all data is searchable, the search factor is met, and the replication factor is met. Below these, it shows 20 searchable peers and 0 not searchable peers, and 12 searchable indexes and 0 not searchable indexes. A table below lists various indexes with their status, searchable data copies, replicated data copies, buckets, and cumulative raw data size. The table is titled 'Splunk Indexes'.

Index name	Searchable	Searchable Data Copies	Replicated Data Copies	Buckets	Cumulative Raw Data Size
_audit	✓ Yes	2	3	40	< 0.01Gb
_internal	✓ Yes	2	3	44	< 0.01Gb
index01	✓ Yes	2	3	20	< 0.01Gb
index02	✓ Yes	2	3	20	< 0.01Gb
index03	✓ Yes	2	3	20	< 0.01Gb
index04	✓ Yes	2	3	20	< 0.01Gb
index05	✓ Yes	2	3	20	< 0.01Gb
index06	✓ Yes	2	3	20	< 0.01Gb
index07	✓ Yes	2	3	20	< 0.01Gb
index08	✓ Yes	2	3	20	< 0.01Gb

Easier Deployment, Configuration



SIMPLIFIED
MANAGEMENT

Forwarder Management

- New visual management interface to deploy and monitor thousands of configurations
- Track status of roll out and easily track down errors
- Monitor deployment activity
- Enables management of forwarder configuration

Number of forwarders being monitored

Number with errors

Number that have downloaded a config

Information about forwarder

i	Host Name	IP Address				
▶	soln-perf21.sv.splunk.com	10.160.26.192	Delete Record	linux-x86_64	15 deployed	a few seconds ago
▶	soln-perf17.sv.splunk.com	10.160.26.125	Delete Record	linux-x86_64	15 deployed	a few seconds ago
▶	soln-perf16.sv.splunk.com	10.160.26.123	Delete Record	linux-x86_64	15 deployed	a minute ago
▶	soln-perf22.sv.splunk.com	10.160.26.193	Delete Record	linux-x86_64	15 deployed	a few seconds ago
▶	soln-perf24.sv.splunk.com				15 deployed	a few seconds ago
▶	soln-perf18.sv.splunk.com				15 deployed	a few seconds ago
▶	soln-perf22.sv.splunk.com				15 deployed	a few seconds ago
▶	soln-perf22.sv.splunk.com	10.160.26.193	Delete Record	linux-x86_64	15 deployed	a minute ago
▶	soln-perf22.sv.splunk.com	10.160.26.193	Delete Record	linux-x86_64	15 deployed	a minute ago
▶	soln-perf23.sv.splunk.com	10.160.26.206	Delete Record	linux-x86_64	15 deployed	a minute ago

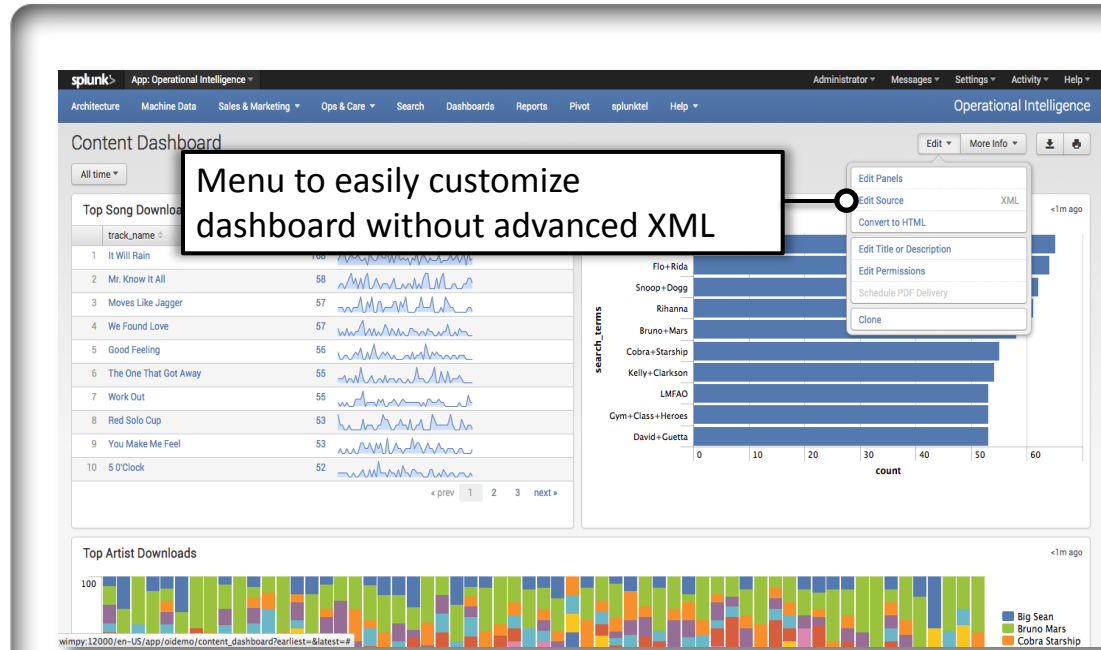
Powerful Dashboard Customization



**RICH
DEVELOPER
ENVIRONMENT**

Enhanced Dashboard Editor

- Build interactive dashboards and user workflows without writing Advanced XML code
- Easily add custom styling, behavior and visualizations
- One-click access to develop in the Splunk web framework



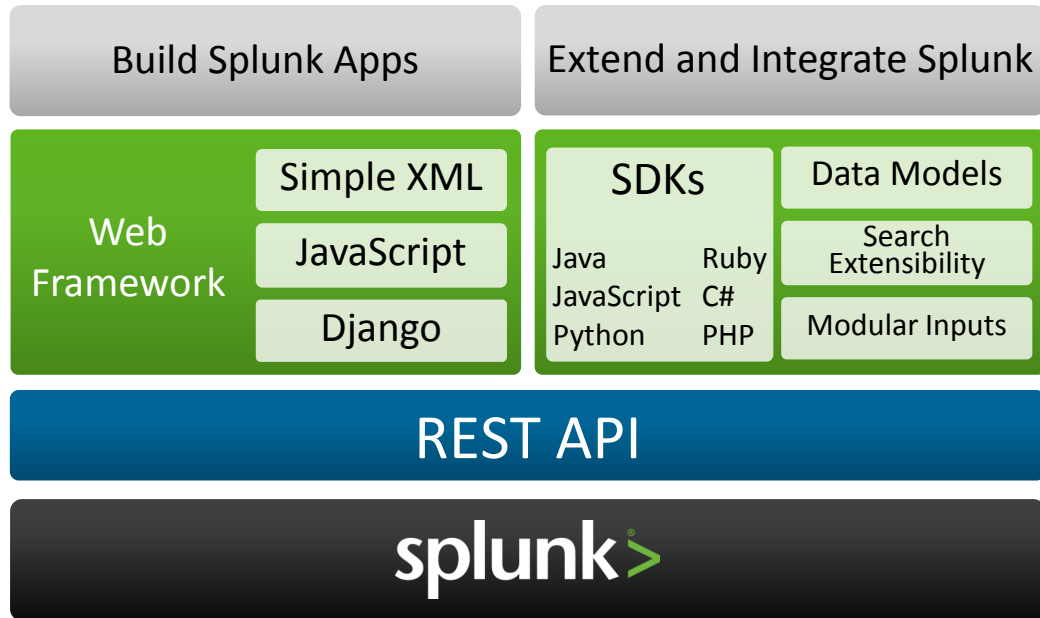
Familiar Developer Environment



RICH
DEVELOPER
ENVIRONMENT

Web Framework

- Quickly and efficiently build Splunk apps using familiar web technologies
- Client-side development with Splunk JavaScript components and JavaScript libraries
- Server-side development support with Python and the Django framework

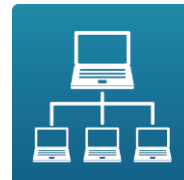


Summary



POWERFUL ANALYTICS

Faster and easier analysis and visualizations for business users



SIMPLIFIED MANAGEMENT

Easier management of enterprise-scale Splunk deployments



INTUITIVE USER EXPERIENCE

Powerful productivity features for end users



RICH DEVELOPER ENVIRONMENT

Rapidly build Splunk apps using standard web languages and frameworks

