Introducing Splunk Enterprise 6.2

Stefano Radaelli
Senior Sales Engineer

splunk>

Splunk Company Overview

Company

- Global HQs:
  - San Francisco
  - London
  - Hong Kong
- 1,300 employees globally
- Annual Revenue: $302.6M (YoY +52%)
- NASDAQ: SPLK

Products

- Free trial to massive scale
- Splunk products:
  - Splunk Enterprise
  - Splunk Cloud
  - Hunk
  - Splunk MINT
  - Premium Apps

Customers

- 7,900+ customers
- Across 100 countries
- Small to large organizations
- 70+ of the Fortune 100
- Largest license:
  - 300+ Terabytes/day


Big Data Comes from Machines
Volume | Velocity | Variety | Variability
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 Processing

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

Middleware Error

```
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
```

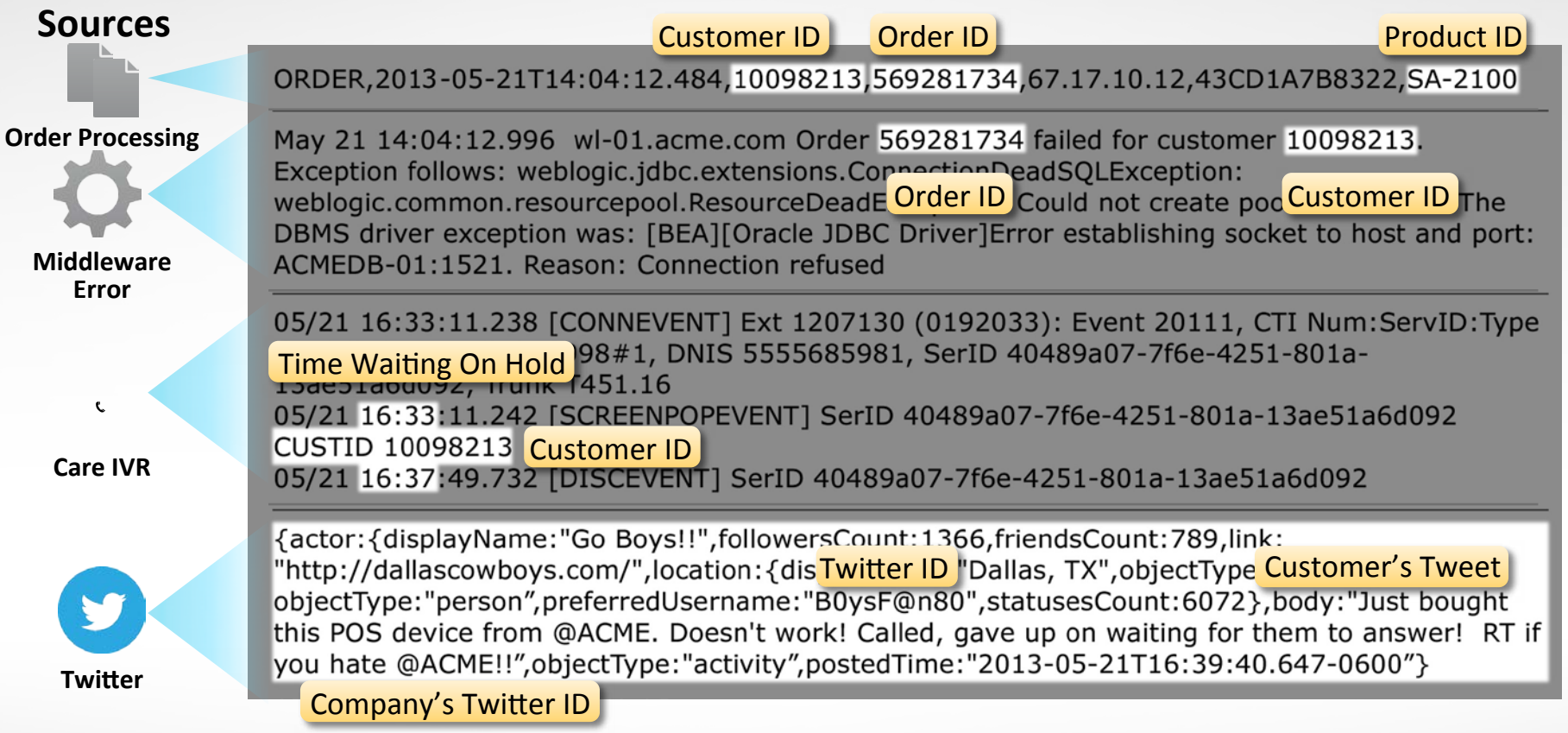

Care IVR

```
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
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
```

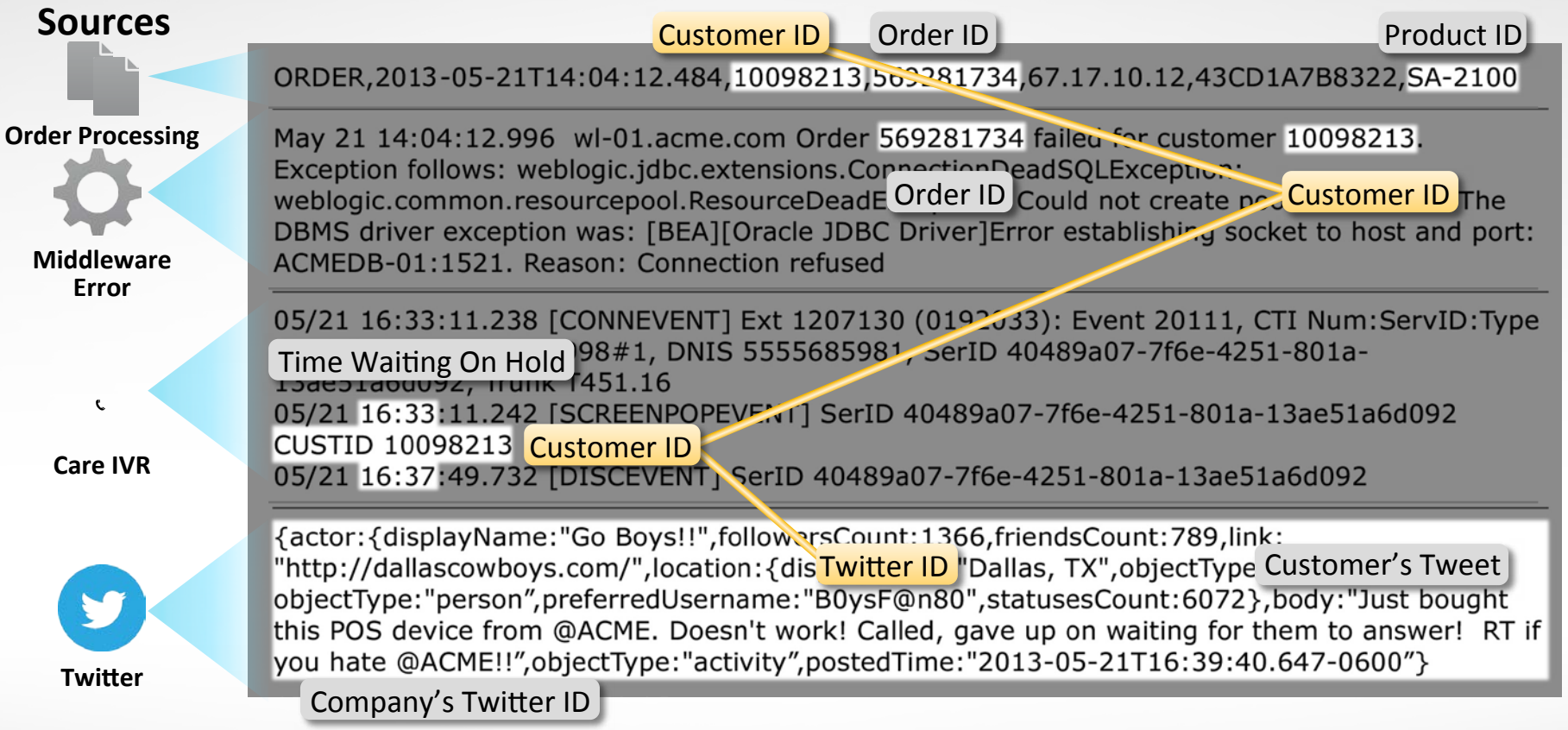
Twitter

```
{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

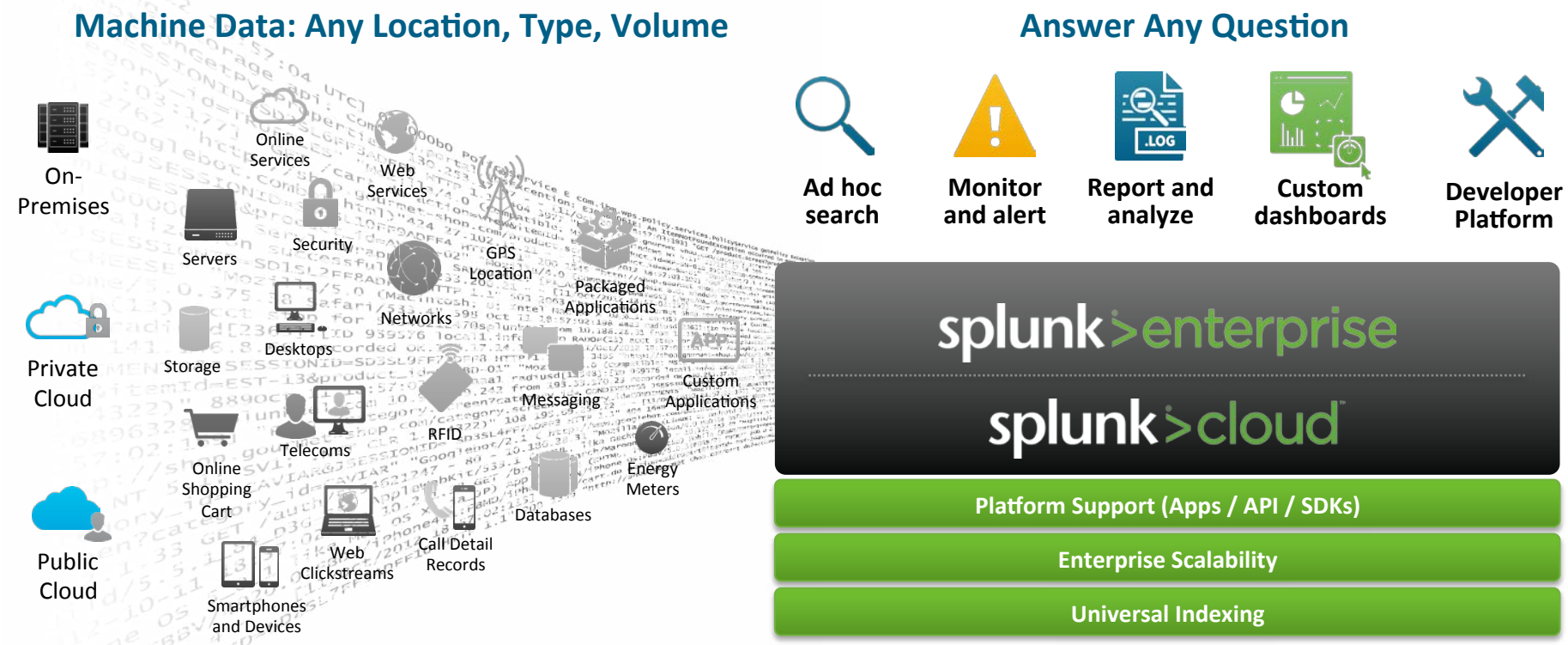


Machine Data Contains Critical Insights

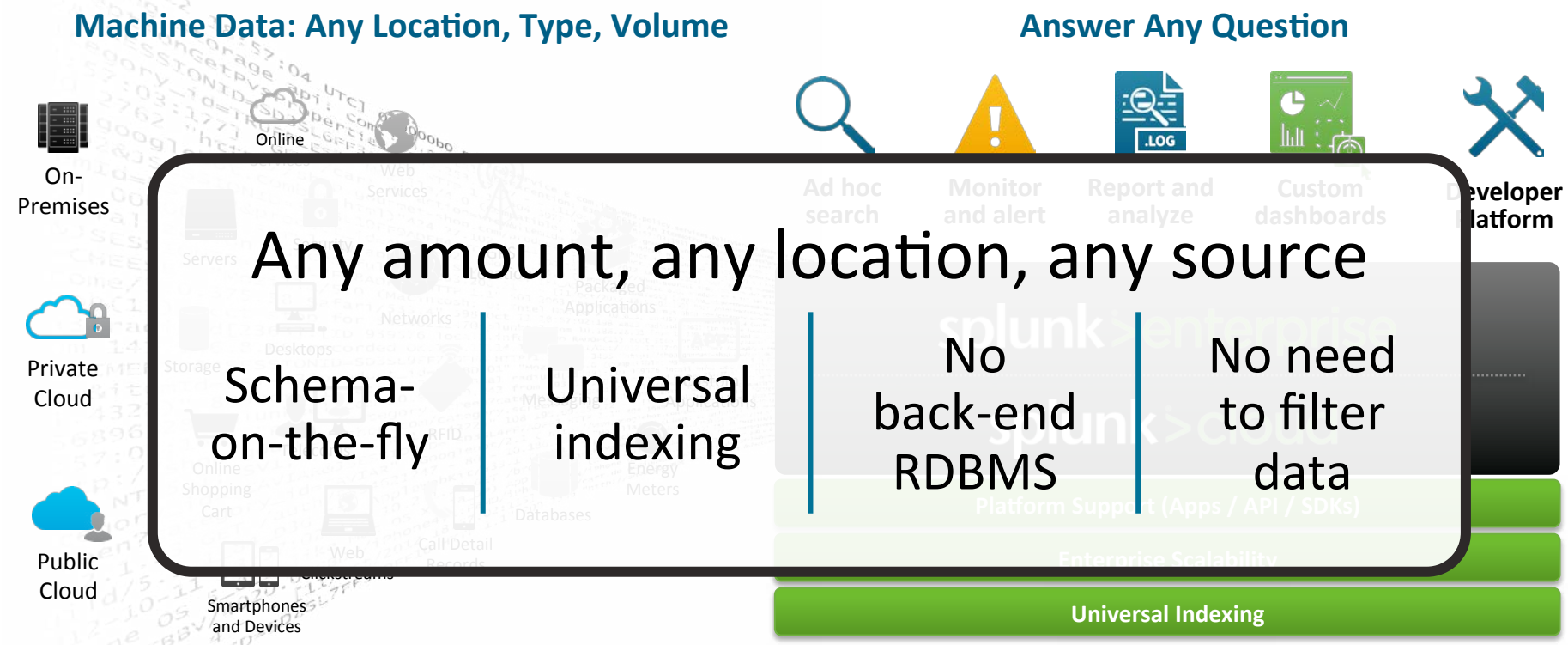


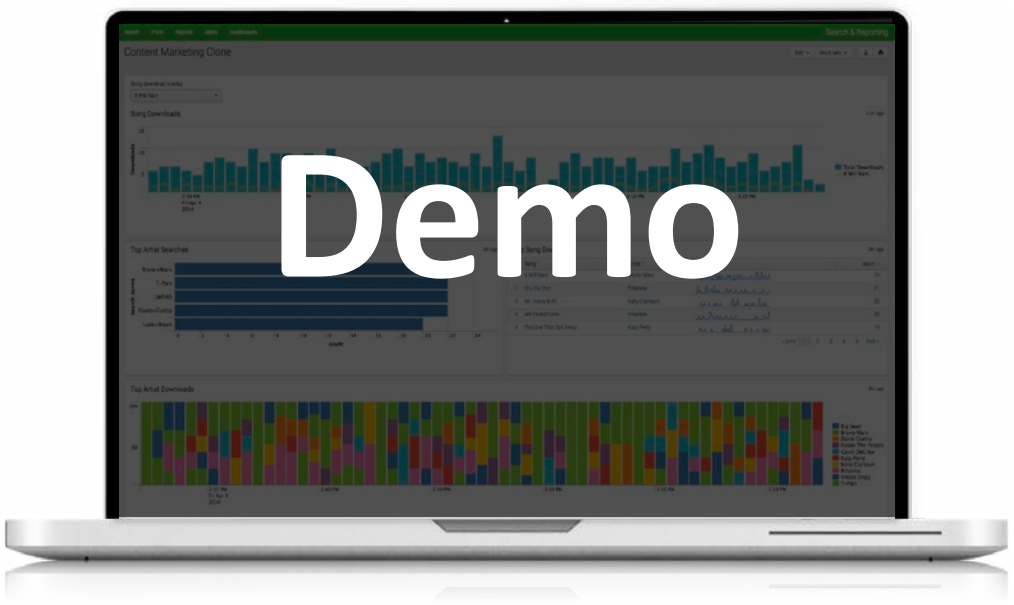

splunk>
Make machine data accessible,
usable and valuable to everyone.

Industry Leading Platform For Machine Data



Industry Leading Platform For Machine Data

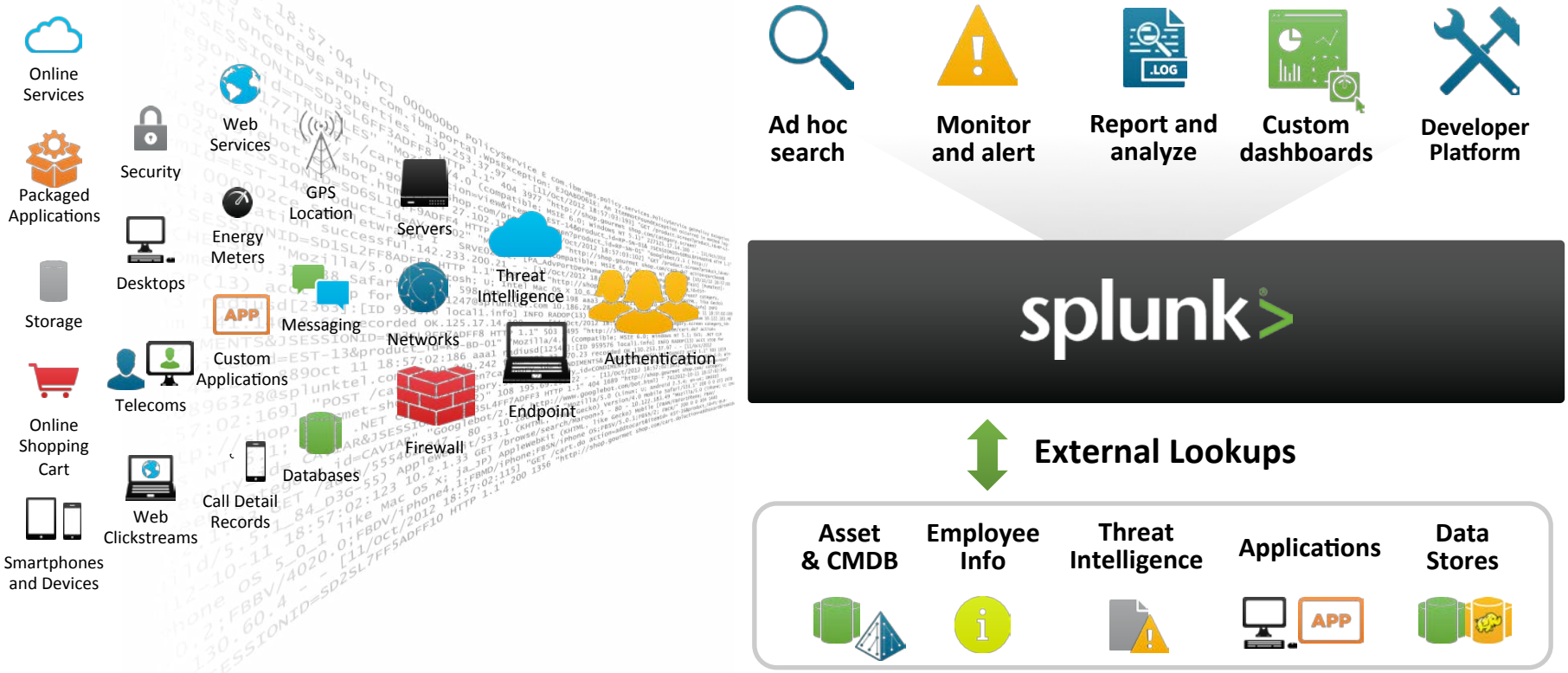




Demo

Security Use Case

Security Intelligence

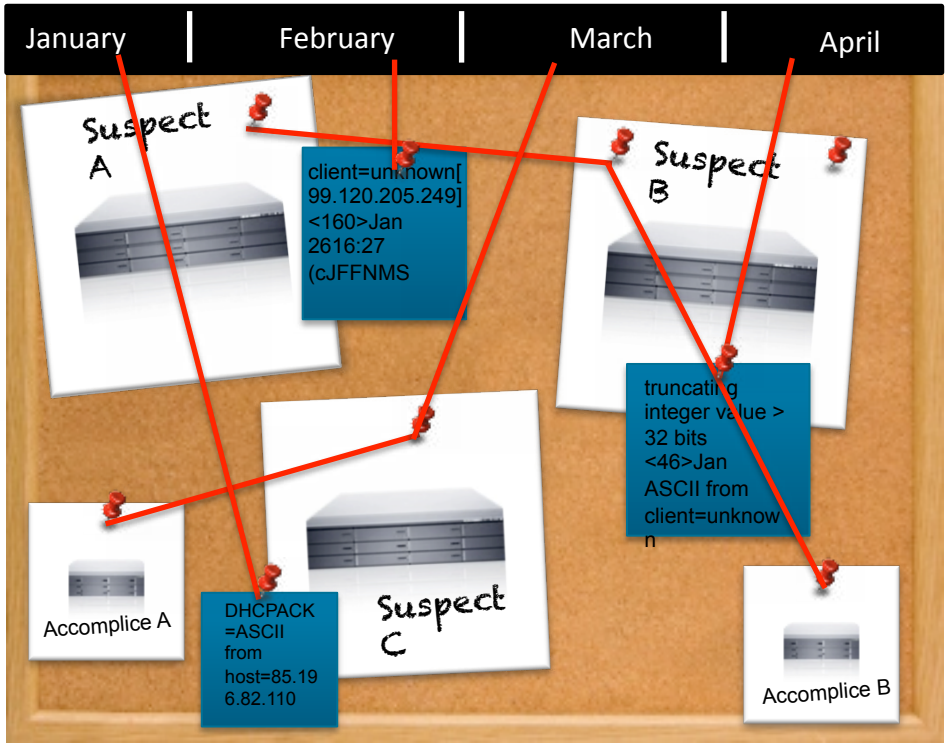


Big Data Platform: Insight for Business Risk

Business Risk and Security

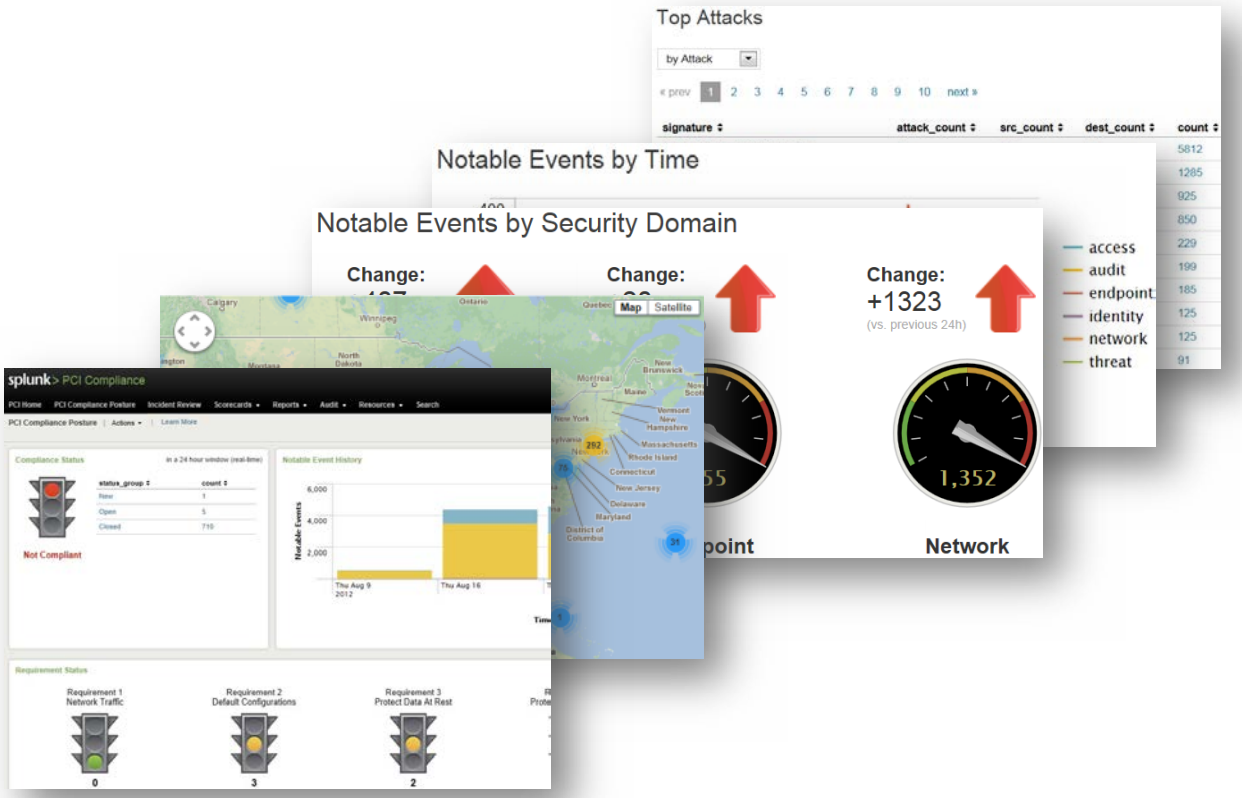
Case #1 - Incident Investigation/Forensics

- Often initiated by alert in another product
- May be a “cold case” investigation requiring machine data going back months
- Need all the original data in one place and a fast way to search it to answer:
  - What happened and was it a false positive?
  - How did the threat get in, where have they gone, and did they steal any data?
  - Has this occurred elsewhere in the past?
- Take results and turn them into a real-time search/alert if needed



Case #2 – Security/Compliance Reporting

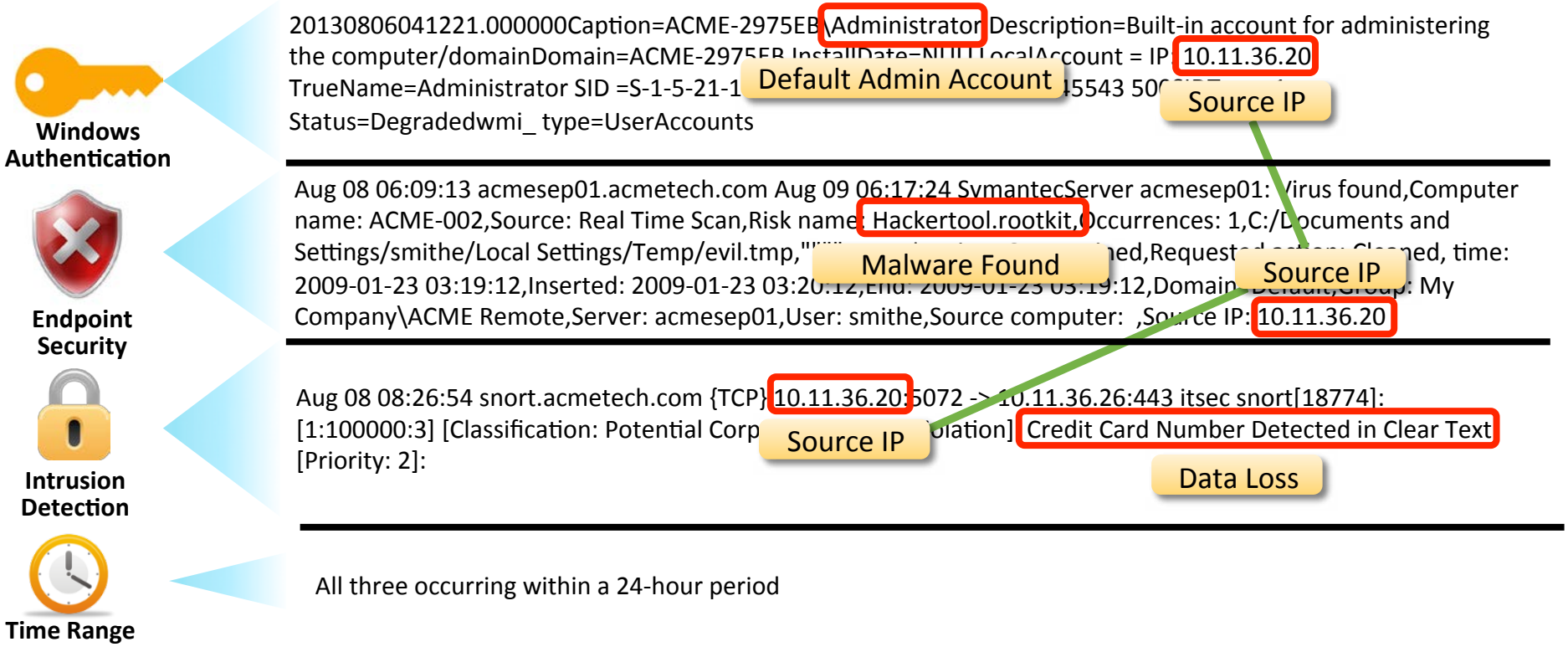
- Many types of visualizations
- Easy to create in Splunk
  - Ad-hoc auditor reports
  - New incident list
  - Historical reports
  - SOC/NOC dashboards
  - Executive/auditor dashboards



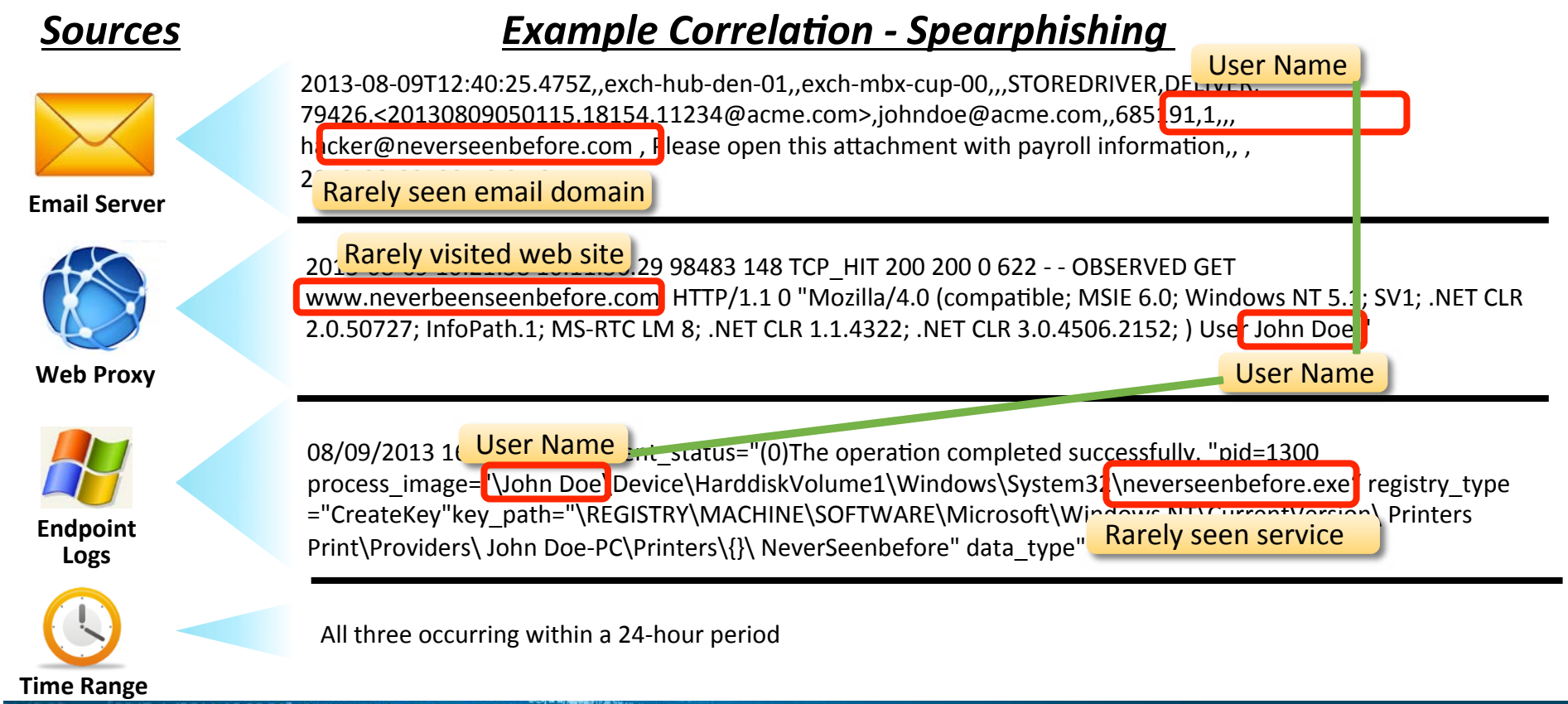
Case #3 – Real-time Monitoring of *Known* Threats

Sources

Example Correlation – Data Loss



Case #4 – Real-time Monitoring of Un*known* Threats



Case #4 – More Examples

Attack Phase	What Threat is Doing	What to Look For	Data Source
Lateral movement	Creating new admin accounts	Account creation without corresponding IT service desk ticket	AD/ Service Desk logs
Data gathering	Stealing credentials	For single employee: Badges in at one location, then logs in countries away	Badge/ VPN/ Auth
Data gathering	Gathering confidential data for theft	Employee makes standard deviations more data requests from file server with confidential data than normal	OS
Exfiltration	Exfiltration of info	Standard deviations larger traffic flows (incl DNS) from a host to a given IP	NetFlow

Case #5 – Insider Threat

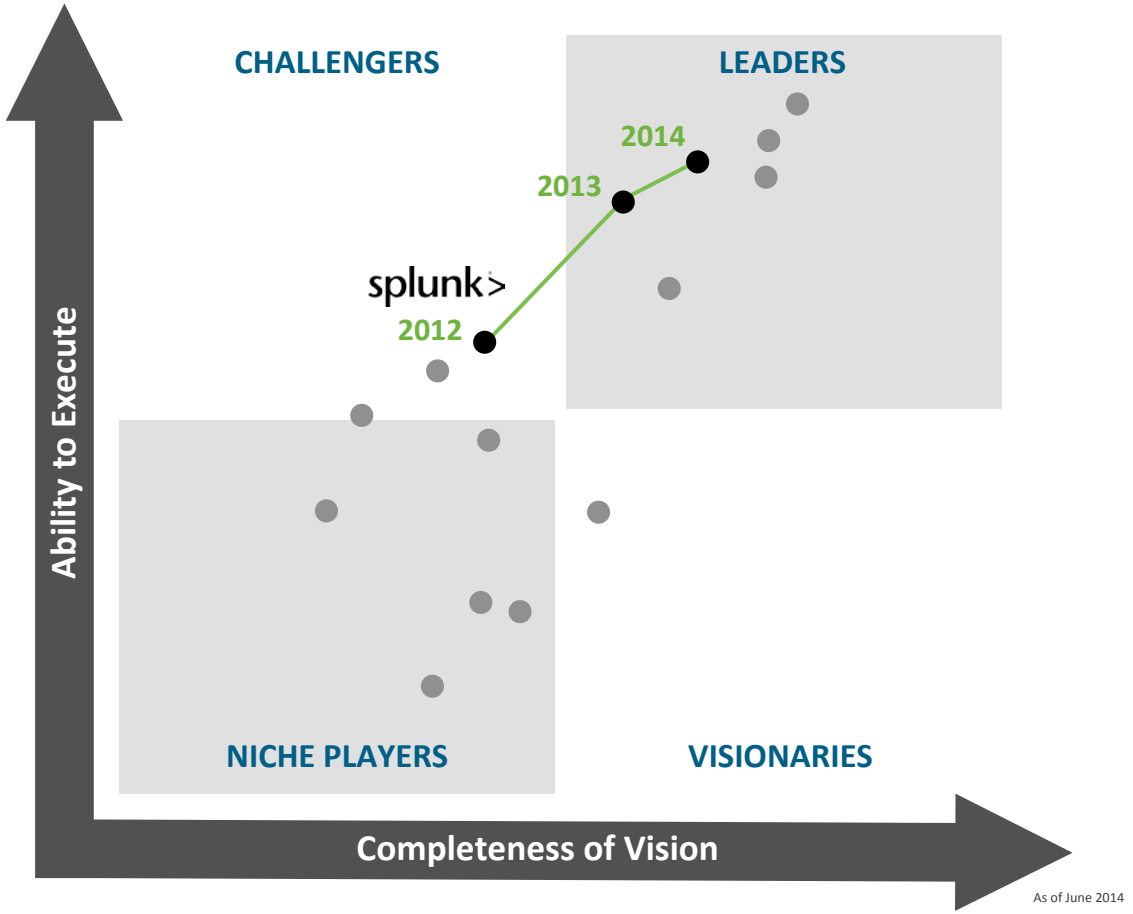
What To Look For	Data Source
Abnormally high number of file transfers to USB or CD/DVD	OS
Abnormally large amount of data going to personal webmail account or uploaded to external file hosting site	Email / web server
Unusual physical access attempts (after hours, accessing unauthorized area, etc)	Physical badge records / AD
Above actions + employee is on an internal watchlist as result of transfer / demotion / poor review / impending layoff	HR systems / above
User name of terminated employee accessing internal system	AD / HR systems

Case #6 – Fraud Detection

Sample Patterns of Fraud in Machine Data:

Vertical	Type of Fraud	Pattern of fraud
Financial Services	Account takeover	Many transactions between $9-10k
Healthcare	Physician billing	Physician billing for drugs outside their expertise area
E-tailing	Account takeover	Many accounts accessed from one IP
Telecom	Roaming abuse	Excessive roaming on partner network by unlimited use customers
Online education	Student loan fraud	Student IP in “high-risk” country and student absent from classes & assignments

A 3-YEAR JOURNEY



As of June 2014

Industry Accolades

BEST SIEM SOLUTION
SC Magazine Awards, 2013

BEST ENTERPRISE SECURITY SOLUTION
SC Magazine Awards, Europe 2013 & US 2014

BEST SIEM
Information Security Magazine Readers' Choice Awards, 2013

Enterprise Security v3.2.1

“Defense-in-depth” Requires a New Strategy

Two types of analysis to fight today’s threats

Traditional Monitoring for Known Events

- In the ‘wild’ but prevalent
- Uses vendor supplied signatures
- Generally caught by IDS/IPS, AV or firewall
- Reported to traditional SIEM

Statistical Analysis for Unknown Events

- Hidden in terabytes of ‘normal’ user activity
- Circumvents perimeter defenses
- Often uses HTTP to communicate
- Much harder to find without advanced analytics

Enterprise Security Content Focus

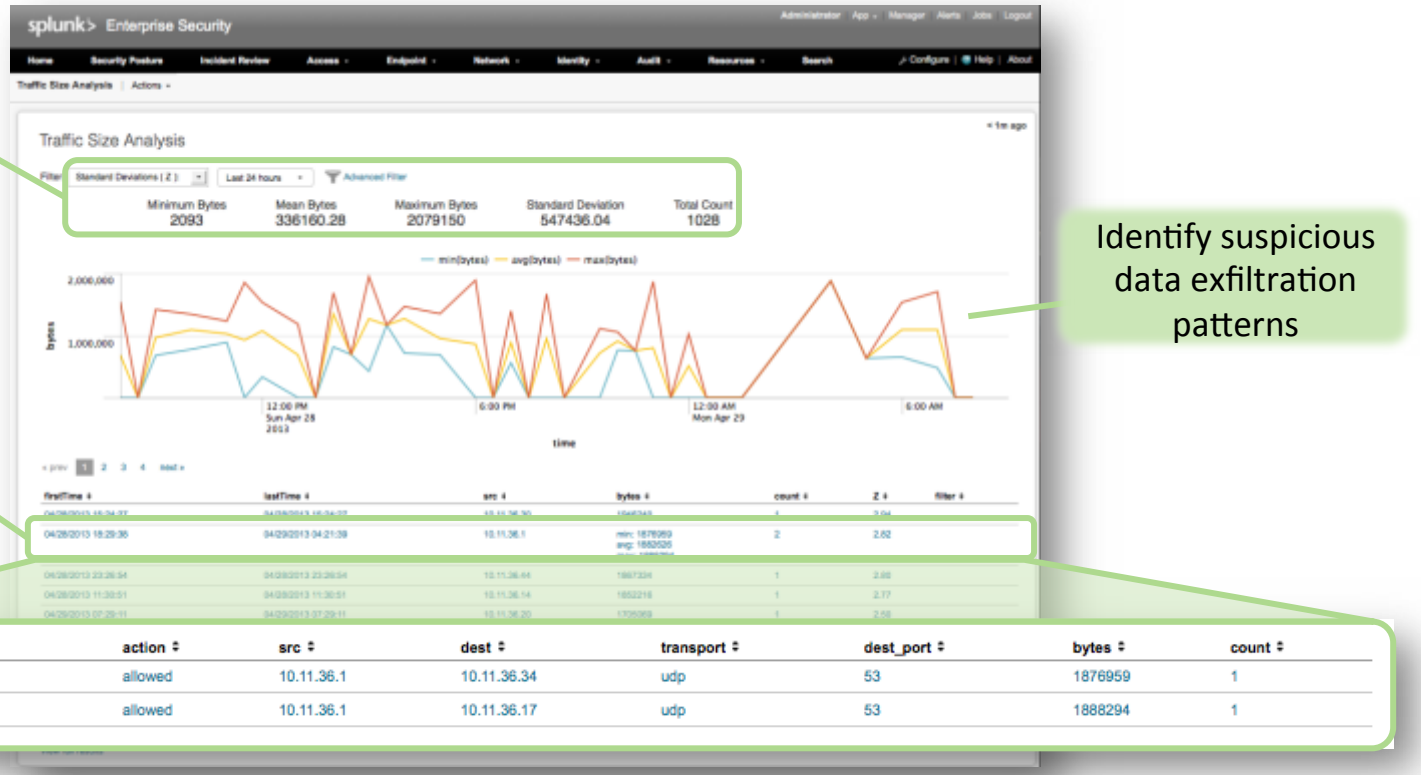
Analysis of real-time and historical data using Splunk statistical analytics to better understand, detect and address unknown threats.

Dashboard: Traffic Size Analysis

Compare traffic data with statistical data to find outliers

Drill-down to look for anomalous source/ dest traffic

Identify suspicious data exfiltration patterns



lastTime	action	src	dest	transport	dest_port	bytes	count
04/29/2013 04:21:39	allowed	10.11.36.1	10.11.36.34	udp	53	1876959	1
04/28/2013 18:29:38	allowed	10.11.36.1	10.11.36.17	udp	53	1888294	1

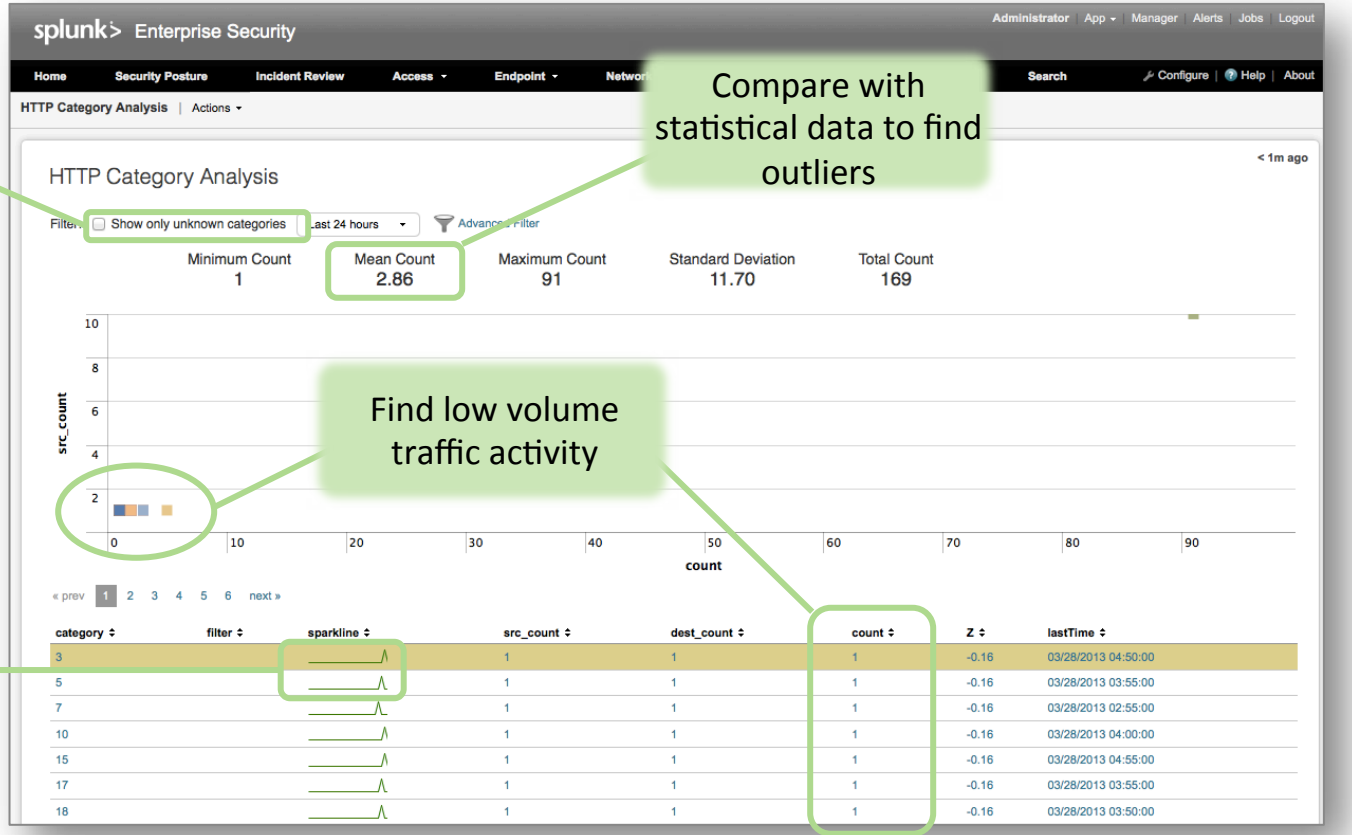
Dashboard: HTTP Category Analysis

Investigate 'unknown' HTTP traffic

Compare with statistical data to find outliers

Find low volume traffic activity

Look for suspicious patterns of activity by category



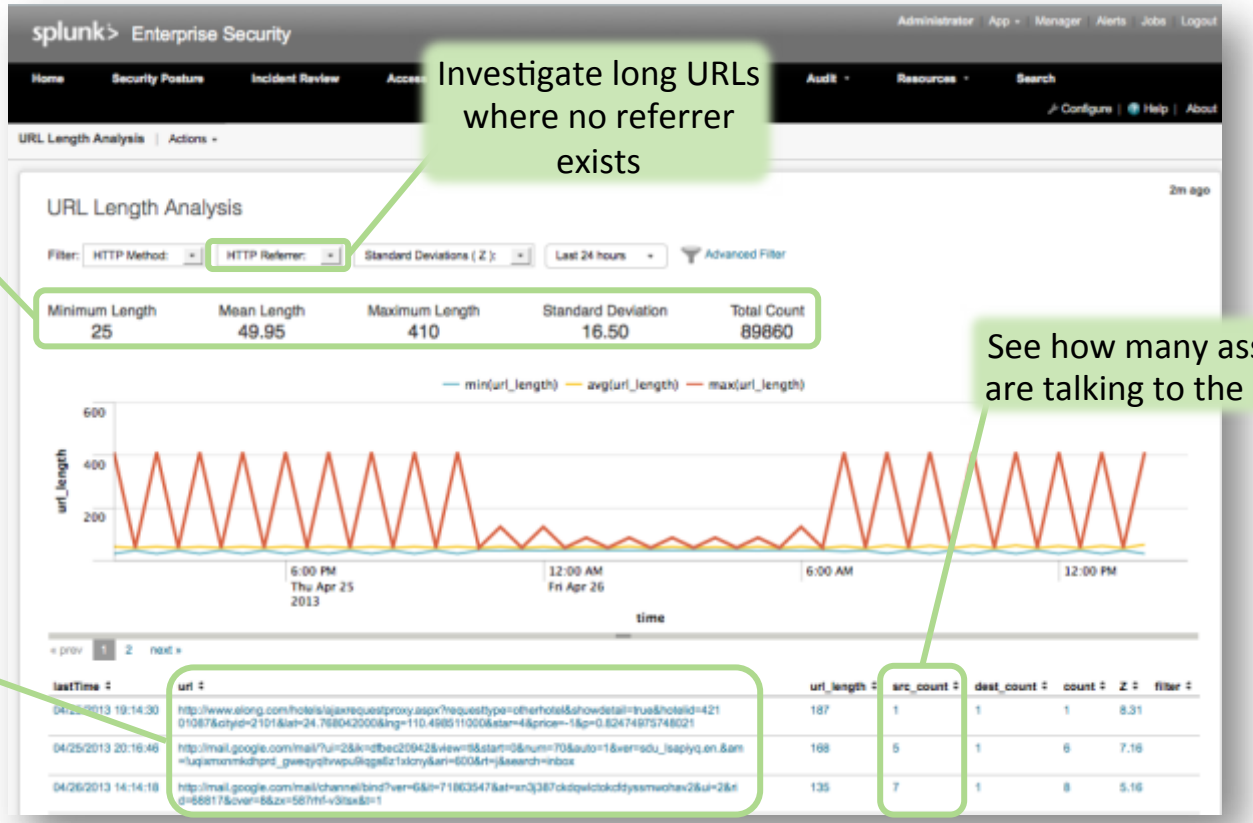
Dashboard: URL Length Analysis

Compare each URL statistically to identify outliers

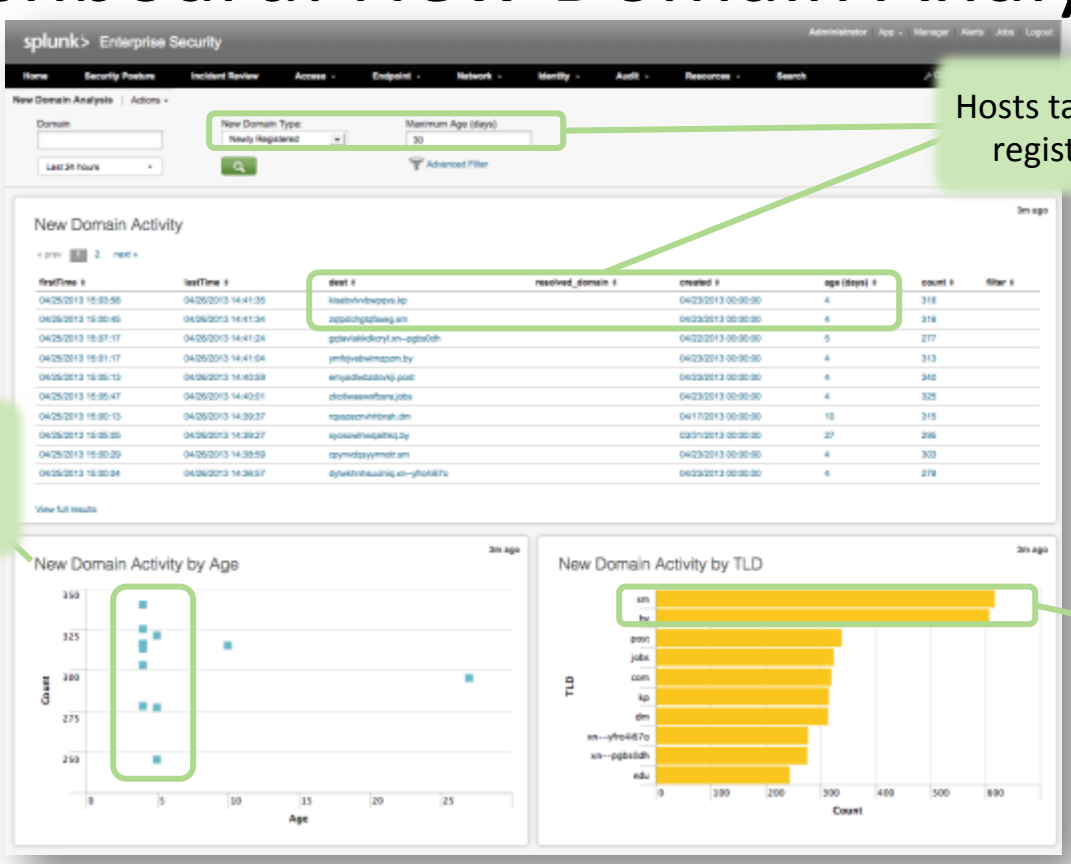
Investigate long URLs where no referrer exists

See how many assets are talking to the URL

Look for long URLs that may include embedded C&C instructions



Dashboard: New Domain Analysis

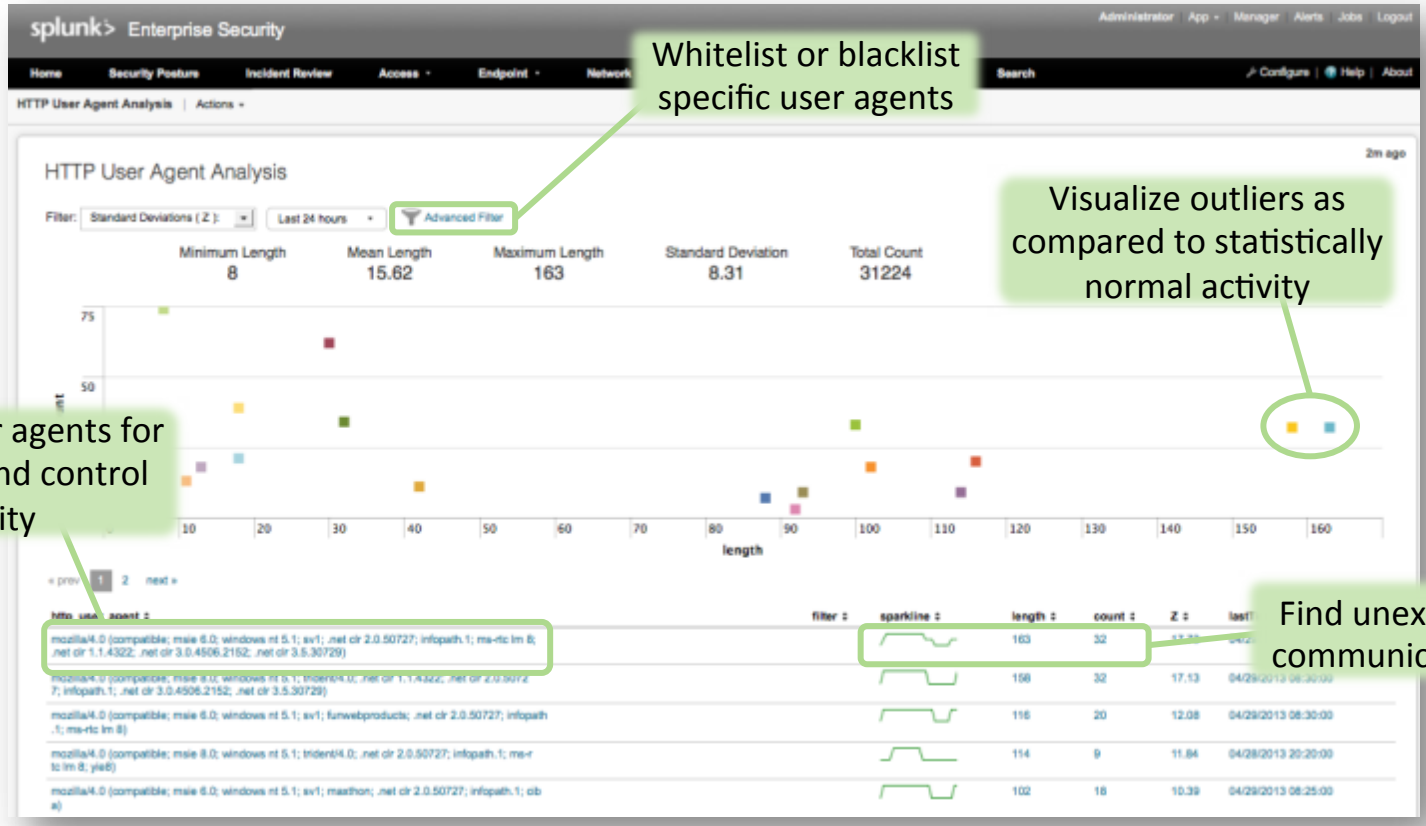


Hosts talking to recently registered domains

Discover outlier activity to newly registered domains

Identify unexpected top level domain activity

Dashboard: HTTP User Agent Analysis



Asset and User Identities Lookup Editor

Edit Lookup File

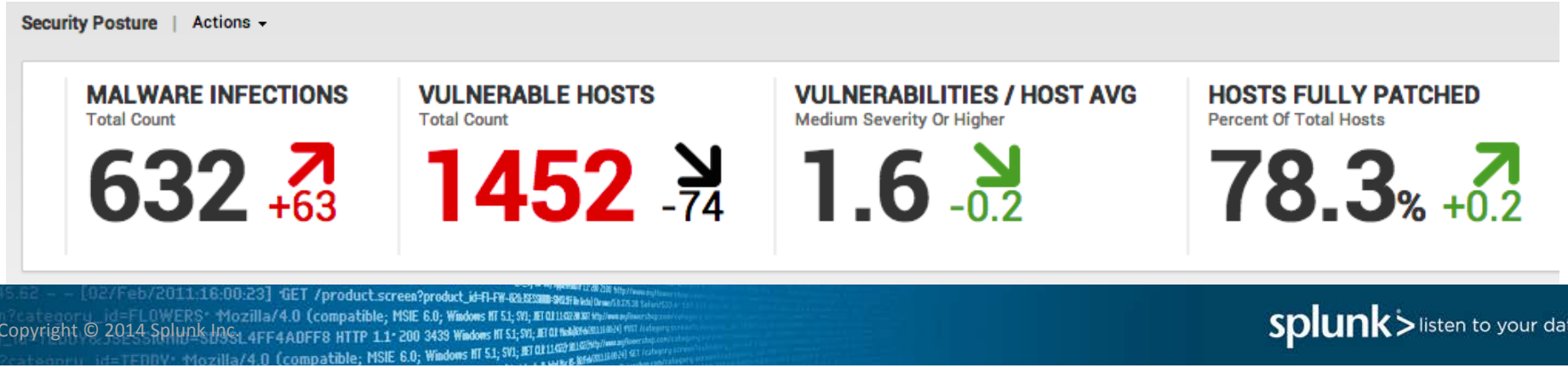
assets.csv

	ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pc
2	6.0.0.1-9.0.0.0					low	41.040855	28.986183	Istanbul	TR	apac		
3	1.2.3.4	00:15:70:91:df:6c				medium	38.959405	-77.04	Washington D.C.	USA	americas		
4				CORP1.acmetech.com		high	37.694452	-121.894461	Pleasanton	USA	americas	pci|cardholder	tn
5	192.168.12.9-192.168.12.9		storefront			critical	32.931277	-96.818167	Dallas	USA	americas	pci	tn
6	2.0.0.0/8					low	50.84436	-0.98451	Havant	UK	emea	pci|sox	dr

- More easily edit values in each of the columns
- Color coding for specialized fields for added visual clarity
- Add new rows of data with a single right-click action

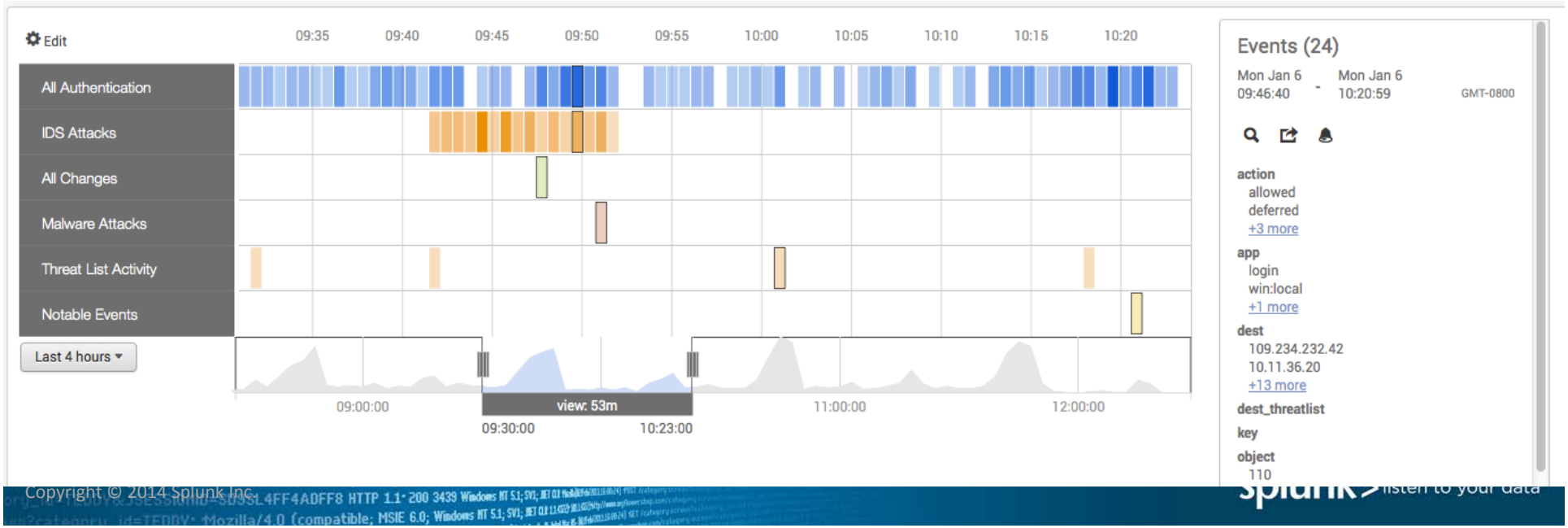
Security Threat Indicator Library

- Key Security Indicators (over 100 available)
- The ability to set a threshold for each metric that indicates if the value is acceptable or not
- Change in color (good or bad) based on customer defined threshold
- A description of the trend (increasing or decreasing) depending on whether the an increase or a decrease ought to be interpreted as good or bad)
- Drill-down from the metric to a dashboard that provides more information



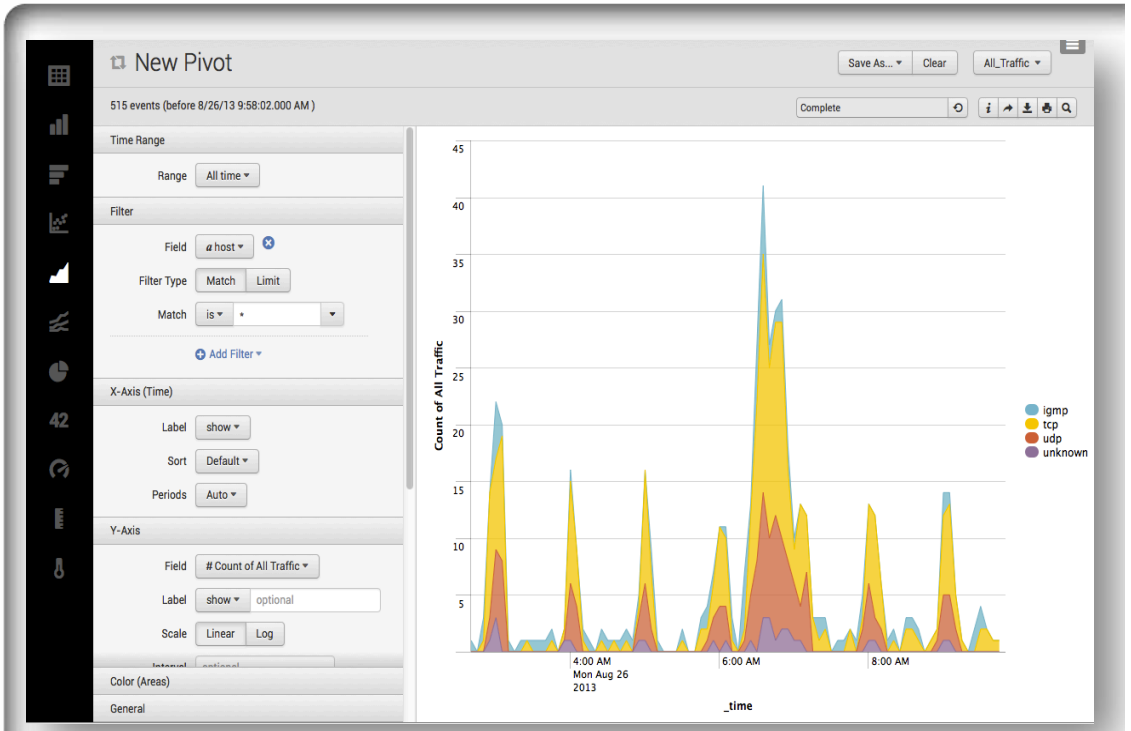
Threat Visualizer

- Search for unusual behavior patterns based on Asset and/or Identity
- Pre-determined (by the customer) events in time-synchronized swim lanes
- Select specific events to create visual correlations across known assets or identities in a single view
- The selections create a “story board” (shown on the right) for investigation

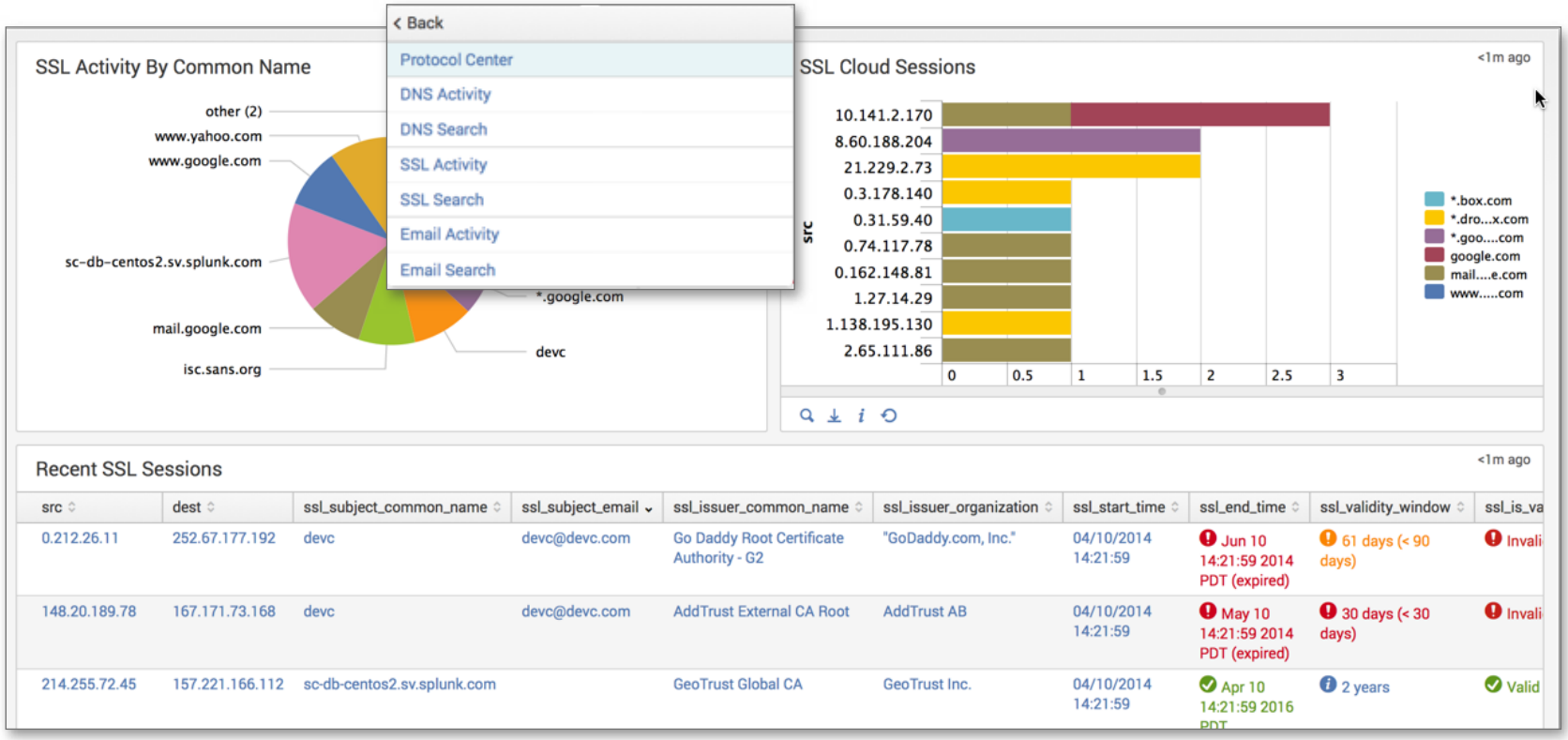


Pivot Tables for Security Reporting

- Driving down report creation complexity
- Create Pivot-based reports
- Customize as needed graph type, color, detail, etc.
- Create and circulate as a report
- Add to or create a dashboard



Protocol Intelligence Reports

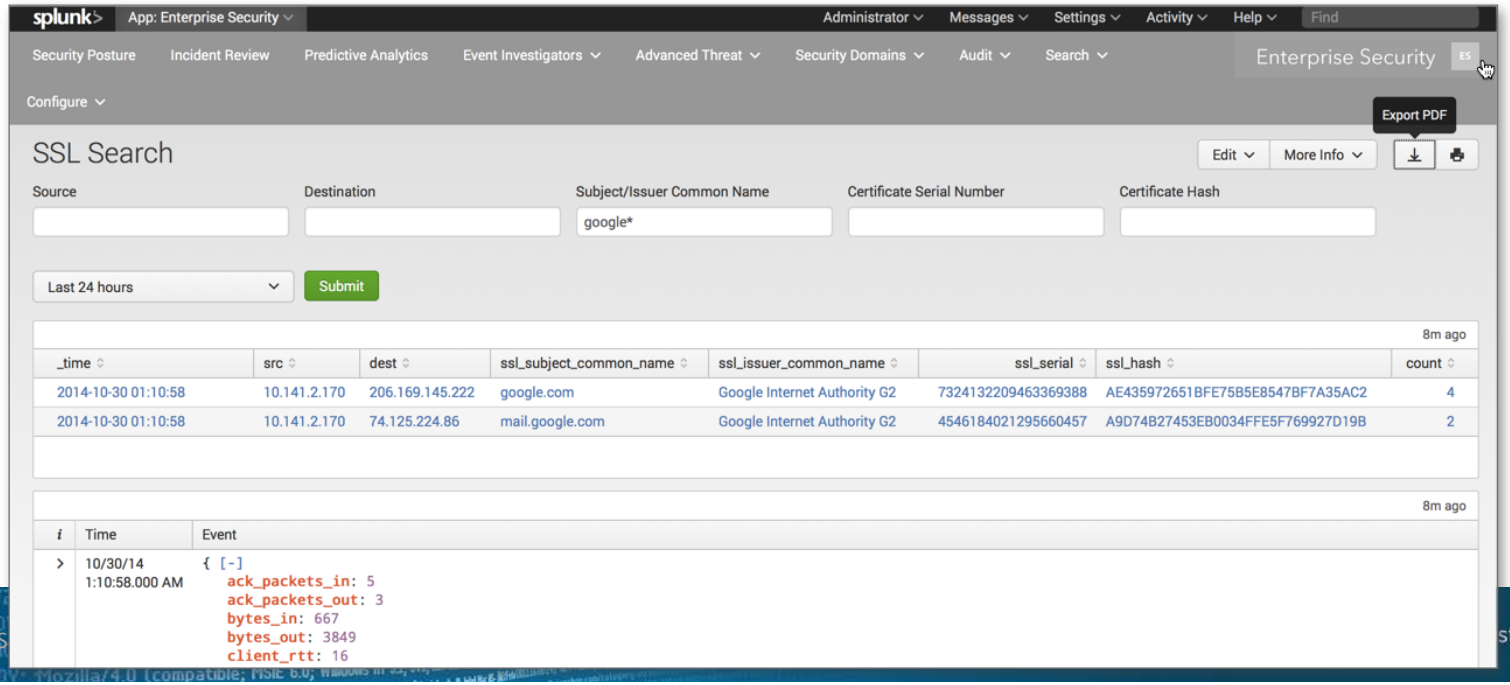


Faster Protocol Investigations

Important protocol fields are exposed for fast access

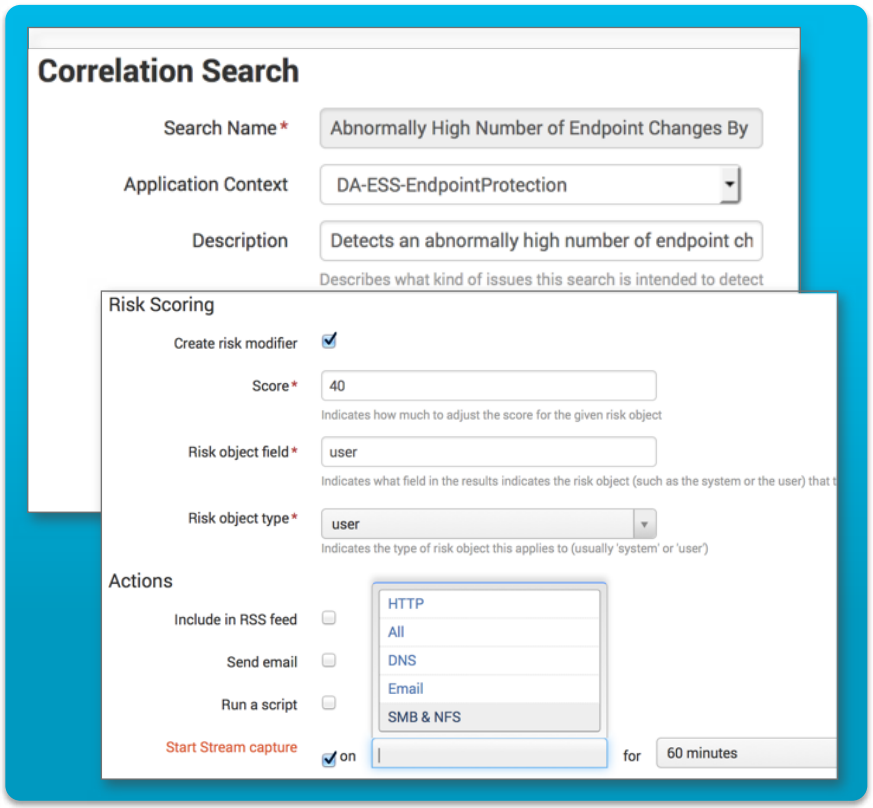
Enter into workflows for investigation

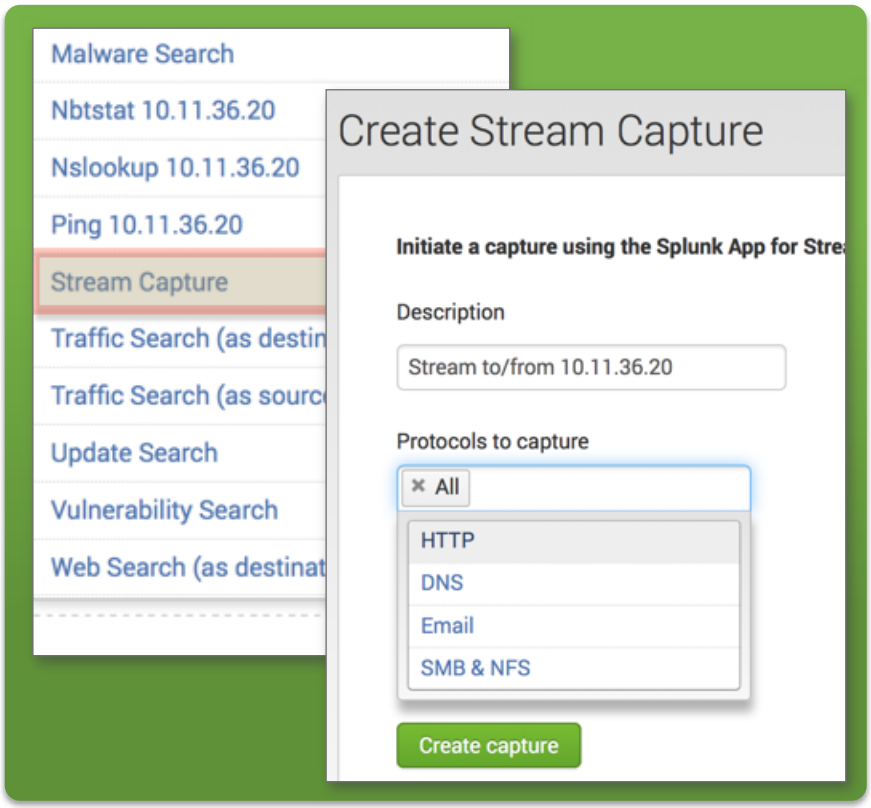
Create new reports or export investigation results



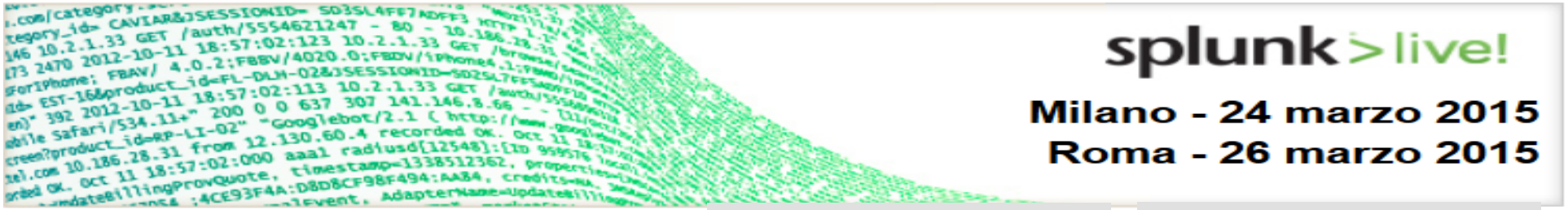
sten to your data™

Acquire Wire Data – On Alert or On-The-Fly





Over 2800 Global Security Customers



Oltre 8.400 aziende di tutto il mondo, incluse 70 tra le Fortune 100 usano Splunk® Enterprise per trasformare i dati macchina in preziose informazioni in grado di garantire un rapido ROI e un valore reale per il reparto IT e il business in generale.

Partecipando a SplunkLive! Italia potrai :

- Scoprire la straordinaria rapidità e semplicità delle funzioni di analisi di Splunk Enterprise 6.2
- Imparare come ottenere in modo eficiente, informazioni da data store tipo Hadoop e NoSQL
- Ascoltare casi di successo direttamente dai clienti e capire come hanno ricavto valore dai loro dati grazie a Splunk.
- Assistere a nuovi training che insegnano come massimizzare l'investimento fatto e risolvere nuovi problem di business.

Qualunque sia la tua attività, dallo sviluppo di applicazioni o generazione di analisi a fini aziendali, alla gestione, protezione e verifica in ambito IT, Splunk può aiutarti ad acquisire rapidamente valore dai tuoi dati..

Iscriviti oggi stesso : http://live.splunk.com/italia_2015

A presto,
Il team Splunk
Any question? gmary@splunk.com

Dettagli evento

Milano: 24 marzo 2015, ore 9.30-16.30 presso **NHOW Milano -** Via Tortona 35

Roma: 26 marzo 2015, ore 9.30-16.30 presso **Westin Excelsior -** Via Vittorio Veneto 125

Testimonianze clienti Milano

- Cerved Group S.P.A
- Alma Mater Studiorum – Università di Bologna
- Fastweb S.P.A.

Testimonianze clienti Roma

- HBG Connex S.P.A.
- Università La Sapienza
- Poste Italiane


Thank You
Stefano Radaelli
sradaelli@splunk.com
splunk>