

Splunk 介绍

崔玥 | cyue@splunk.com



Splunk 公司

公司
(NASDAQ: SPLK)

2004 成立

2006 发布第一个软件版本

总部 美国旧金山

业务模式 /
产品

企业软件

In the **cloud**

SaaS

客户
8,400+

60+ 财富100强

最大的license用量:

400+ TB/天

业内认可

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**

超过2/3 财富100企业



Financial Services and Insurance



Media

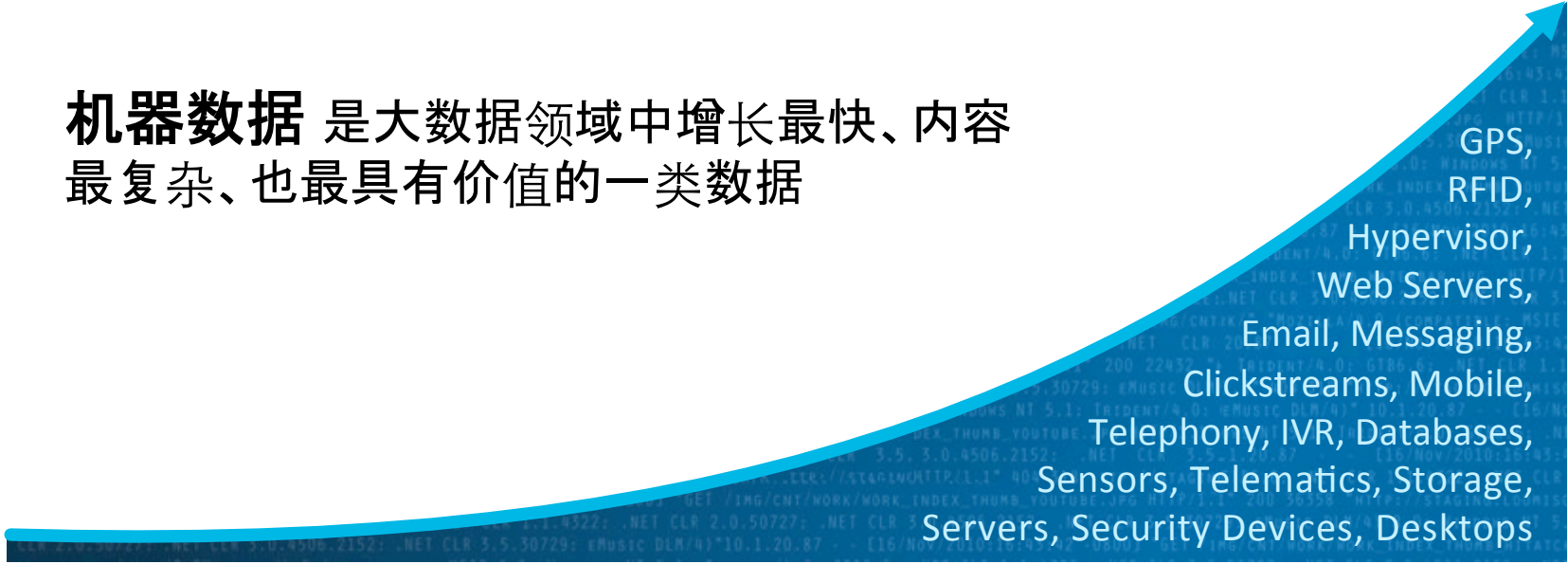


Travel and Leisure

数据在高速增长

Volume | Velocity | Variety | Variability

机器数据 是大数据领域中增长最快、内容最复杂、也最具有价值的一类数据



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

机器数据是什么样的？

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
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

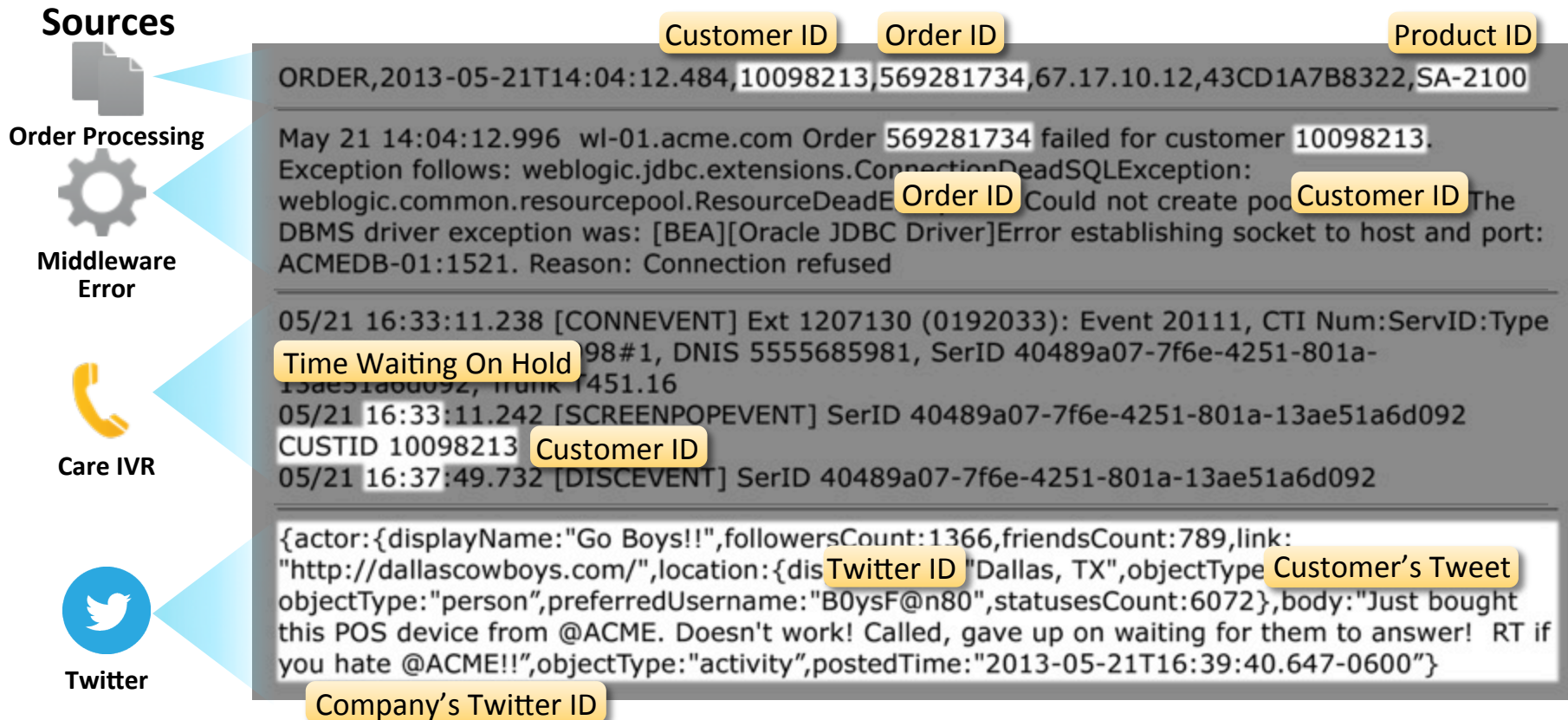
Care IVR



{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"}

Twitter

机器数据包含有大量有价值的信息



机器数据包含有大量有价值的信息

Sources



Order Processing



Middleware
Error



Care IVR



Twitter

Customer ID

Order ID

Product ID

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

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

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

Customer ID

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

splunk®

让机器数据对所有人都可以访问、
使用并带来价值

业内领先的机器数据分析平台

任何机器数据

运维智能



搜索与调查

主动监控

运维可视化

实时业务洞察

splunk>

HA Indexes
and Storage



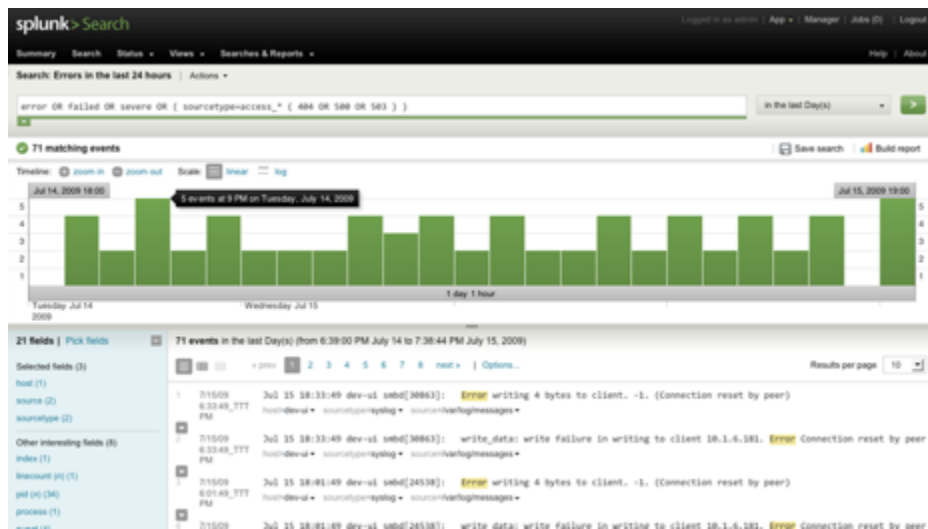
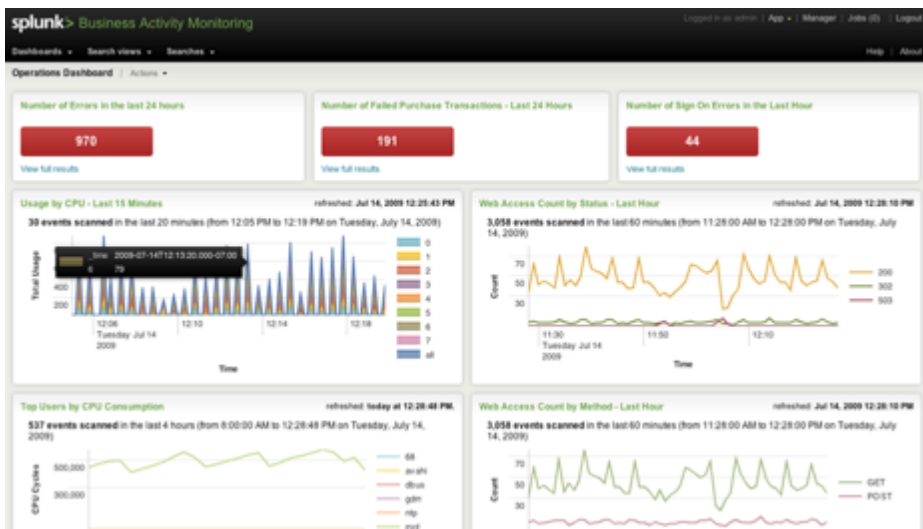
Commodity
Servers

splunk>live!

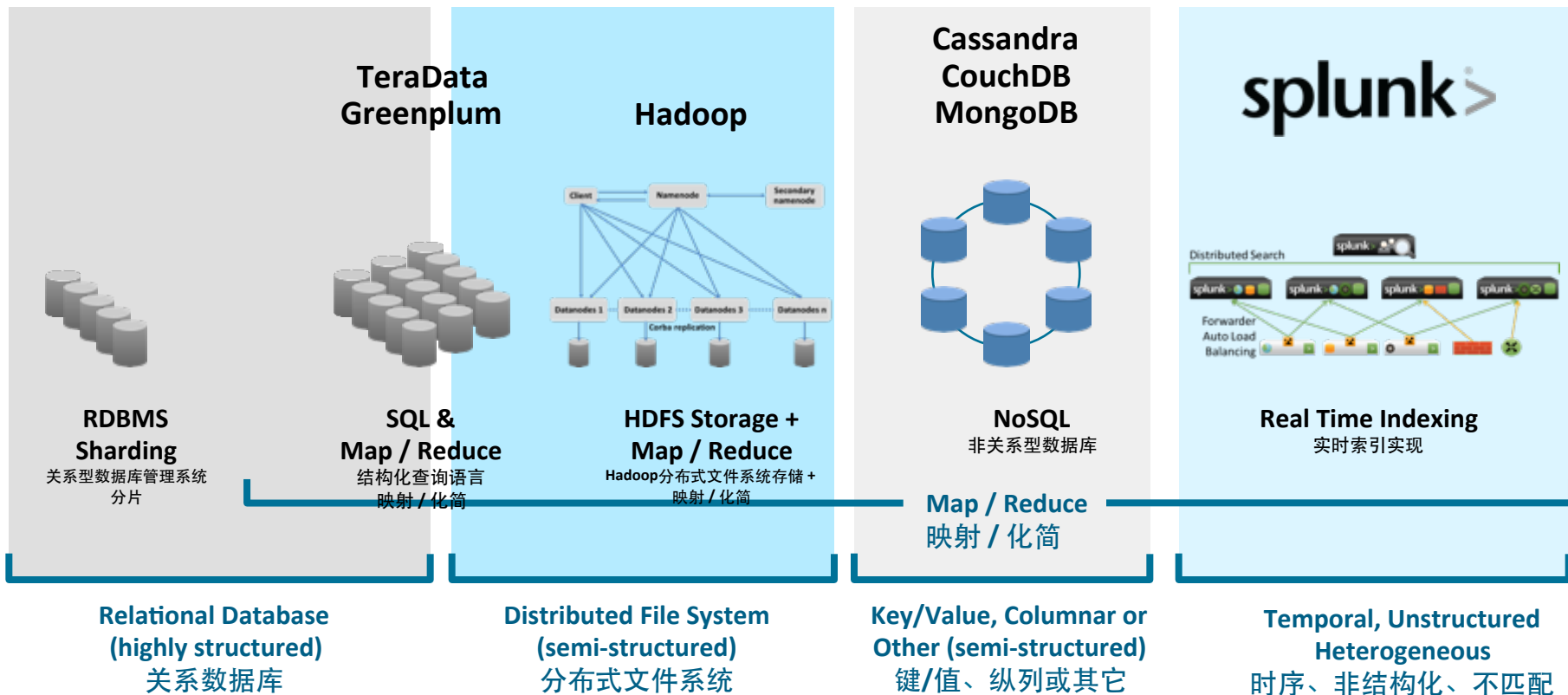
splunk>listen to your data™

Splunk 是什么？

- Splunk 是一个针对机器数据的数据平台
- 针对所有 IT 系统和基础设施数据，提供数据搜索、报表和可视化展现
- Splunk 是软件 – 几分钟就可以完成下载和安装
- 可以运行在各种主流的操作平台



Big Data Technologies 大数据技术

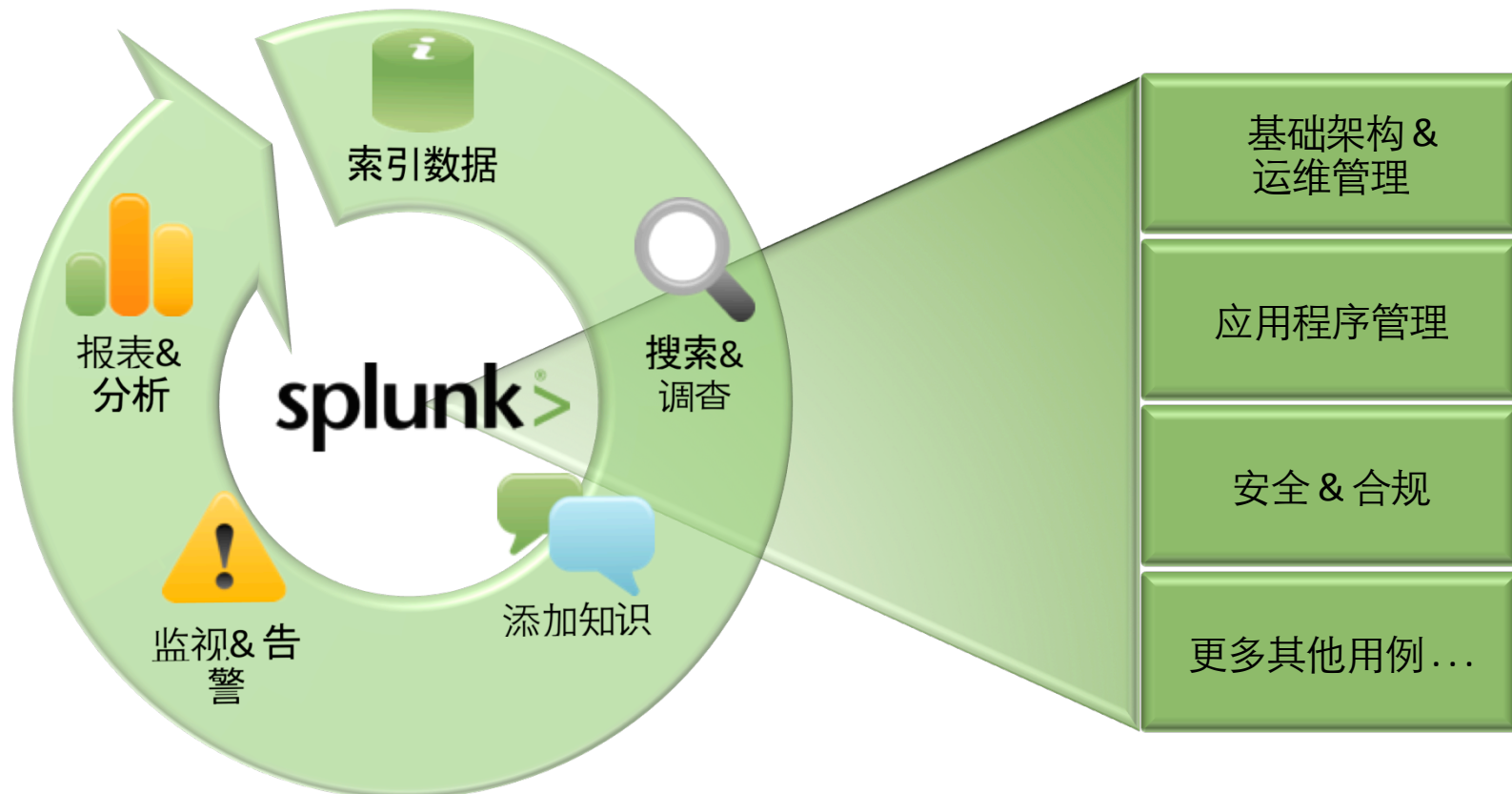


索引任何的机器数据

- 实时从日志文件获取事件
- 运行脚本获取系统参数, 连接到 API 和数据库
- 监听 syslog 或获取 Windows 事件
- 通用方式索引任何内容格式的数据, 不需要连接器



一个 Splunk 多种应用场景



Splunk Approach to Machine Data

Traditional

Schema at Write

SQL

ETL

Structured
RDBMS

Splunk

Schema at Read

Search

Universal Indexing

Unstructured

Volume Velocity Variety

Splunk 平台

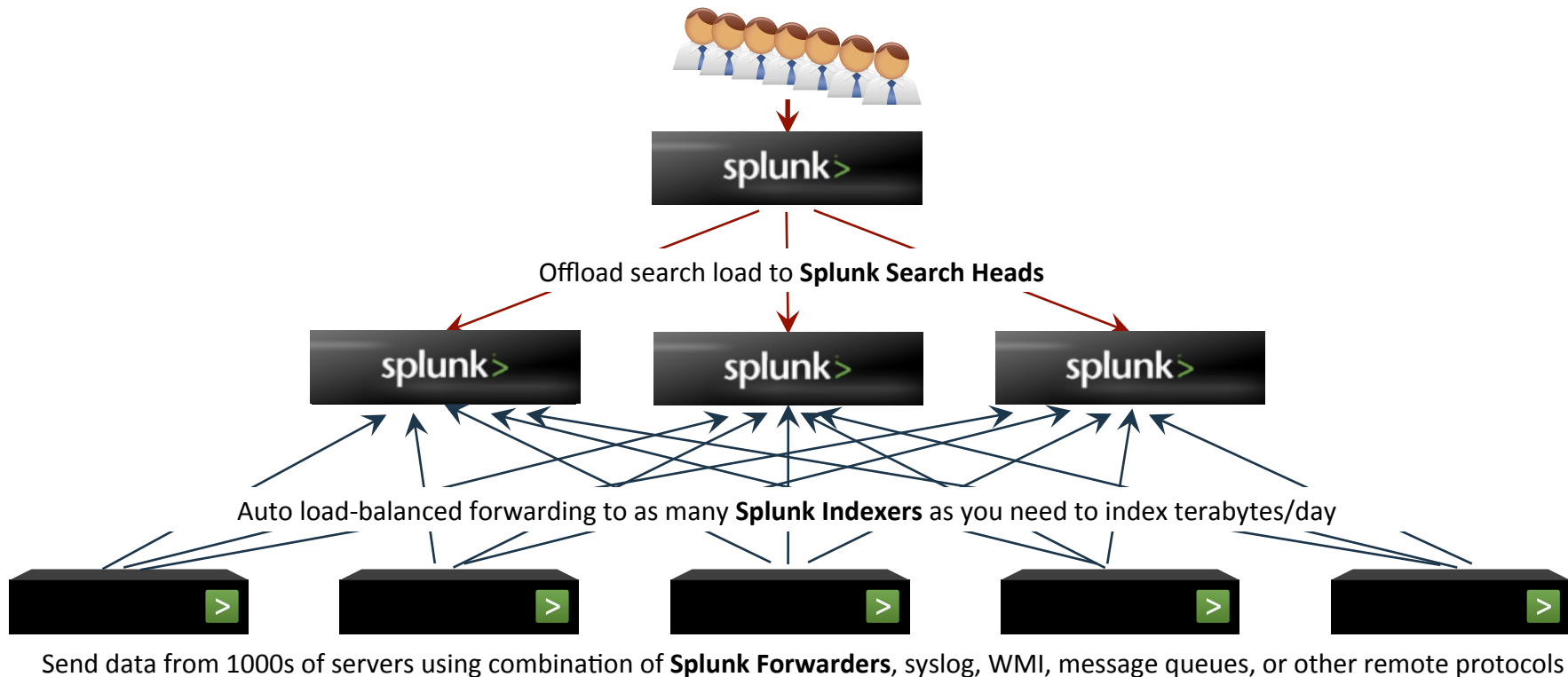


丰富的 Splunk 应用

在 Splunk app 网站有超过500个 apps

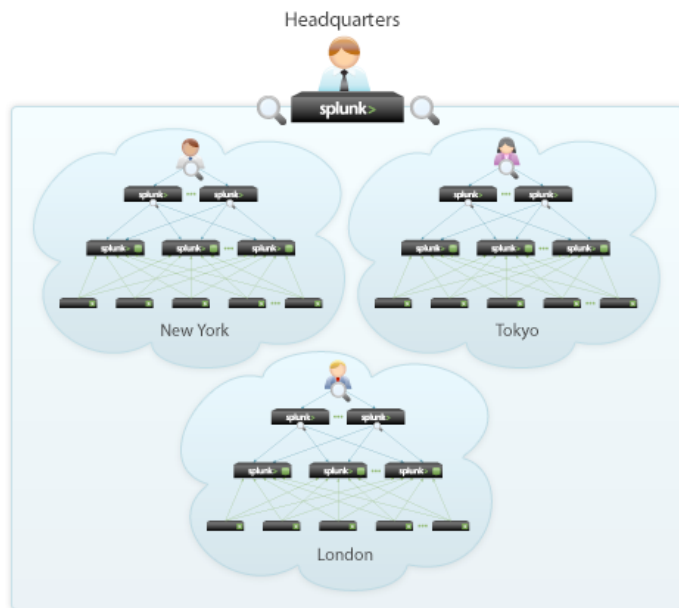


灵活的扩展能力



跨多个数据中心运行

分布式搜索提供跨多个位置的统一视图



A group of goldfish swimming in a white space. The fish are orange and yellow, with some showing darker spots. They are positioned at various angles, suggesting movement. The background is plain white.

- ```
1145.62 - - [02/Feb/2011:16:00:23] GET /product/screen?product_id=FW-G3-2300-043790 http://www.splunk.com/
screen?category_id=FW-G3-2300-043790 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GT.U2.145610M) http://www.splunk.com/
ory_id=splunk>live! ADFF8 HTTP/1.1 200 3439 Windows NT 5.1; SV1; GT.U2.145610M POST /adff8/ HTTP/1.1 200 3439
screen?category_id=TEDDY Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GT.U2.145610M) http://www.splunk.com/
```

# Splunk 在IT和业务领域都可以使用





问题?