opping.com/as

een?category ic

do?action=re-

"Mozilla/4.036

EDDY&JSESI?

een?category

SHOPPINT

200

"Mozītīd, Tio 200 1901 "ht to 3Catesory ich

Splunk and IT Service Intelligence

SIG-NOC, 27th November 2017

Graham Parsons, Operations Specialist



Splunk turns machine data into answers

Splunk's trusted analytics platform empowers people to dive into their machine data so they can find answers quickly and see opportunities in real-time.





What is Machine Data?



Flight and airport data

American Airlines operates 6,700 flights daily to 350 destinations

Customer generated data

Airlines can get more than 15,000 tweets a day

Back office data

The support systems used to run the business ie HR software

Baggage data

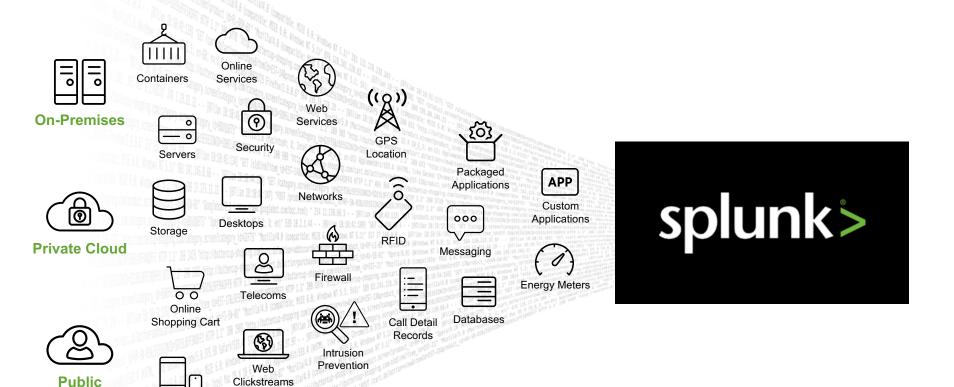
Airlines check >150M bags per year, many with RFID sensors

Device data

A Boeing 737 produces 20 TB of data per hour

splunk>live!

Nearly All the Answers You Need Are In Your Machine Data



Cloud

Smartphones and Devices Application Delivery

IT Operations

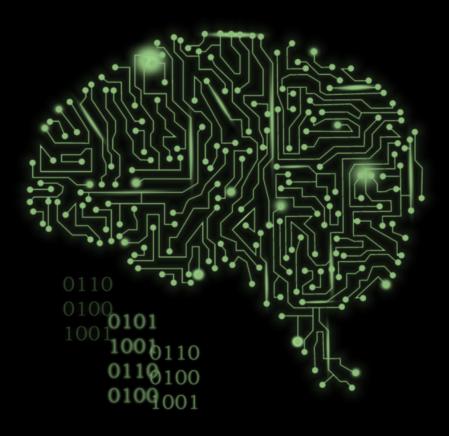
Security, Compliance & Fraud

Business Analytics

Network & Internet of Things

S&JSESSIONID=SDIV. - [07/Jan 18:10:53:118] "GET - [07/Jan 18:10: /Jan 10. //category.screen. efssionID=S08SL2FF5ADFF2 HITT 223 "http://buttercup-shopping.com/category. h20ping.com/product. Screen?product.screen.screen. TONID=SD8SL2FF5ADFT AD 223 "http://buttercup-shoping.com/product.screen?product.screen?product.id=shoping.com/pro Making machine data (compatible installed in the control of the co valuable to everyone.

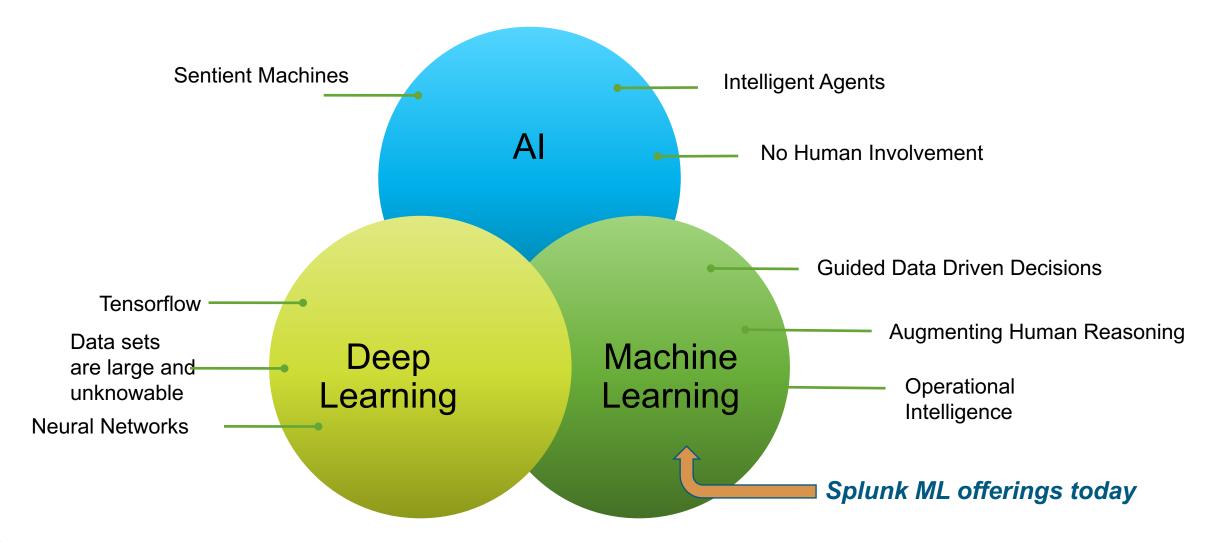
Machine Learning with Machine Data Unlocks Even More Value



Security | IT Ops | Network Ops | IoT



AI, Deep Learning, And Machine Learning

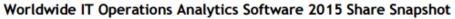


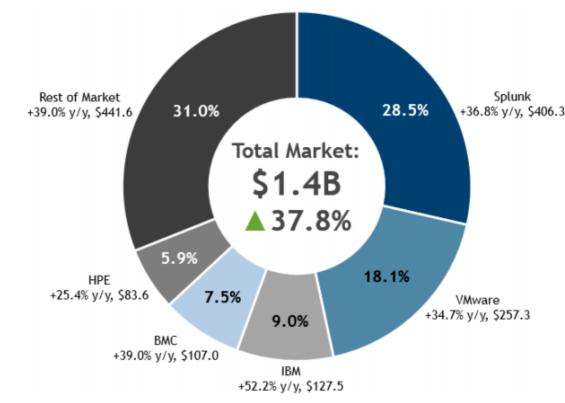
Splunk Positioned as a Leader

IDC Worldwide IT Operations Analytics Software*

- Market share leader in first IDC ITOA report
- Predictive analytics, anomaly detection, business impact analysis
- Recommended for variety & volume of data, use case breadth, pre-packaged content, visualizations and data management.

*IDC, Worldwide IT Operations Analytics Software Market Shares, 2015: Special Report (doc #US41663816 August 2016)





Note: 2015 Share (%), Growth (%), and Revenue (\$M)

Source: IDC, 2016



Splunk Positioned as a Leader

Gartner 2016 Magic Quadrant for Security Information and Event Management*

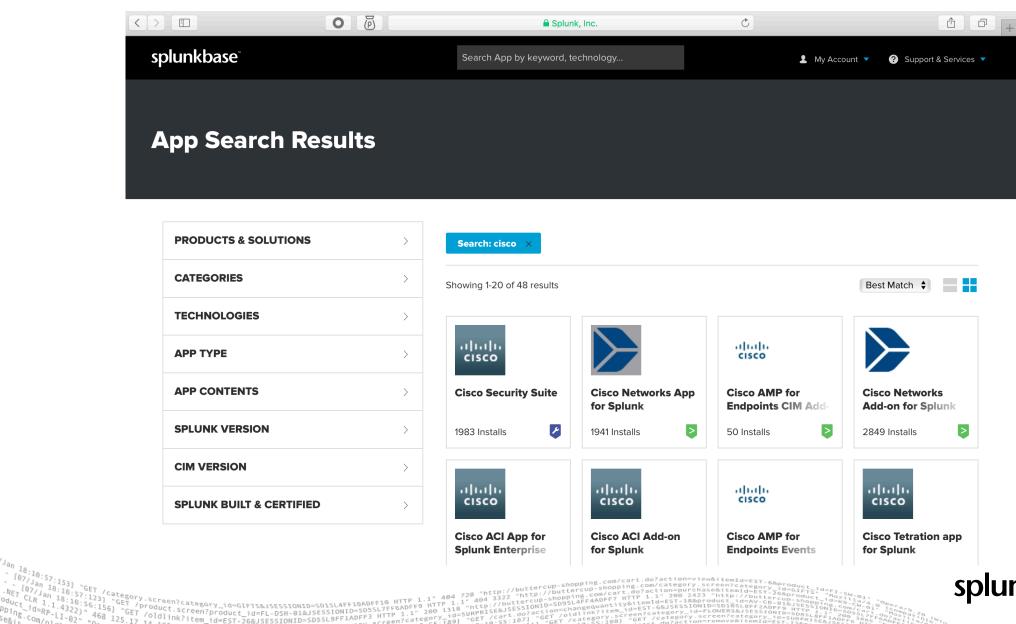
- ► Four Years in a Row as a Leader
- ► Furthest overall in Completeness of Vision
- Splunk also scores highest in 2016 Critical Capabilities for SIEM report in all three Use Cases

Figure 1. Magic Quadrant for Security Information and Event Management



^{*}Gartner, Inc., 2016 Magic Quadrant for Security Information and Event Management, and Critical Capabilities for Security Information and Event Management, Oliver Rochford, Kelly M. Kavanagh, Toby Bussa. 10 August 2016 This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Splunk. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a

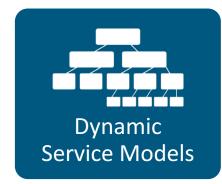
Splunk is a Platform



Splunk IT Service Intelligence

Splunk IT Service Intelligence

Data-driven service monitoring and analytics





At-a-Glance Problem Analysis



Early Warning on Deviations



Simplified Incident Workflows

SPLUNK IT SERVICE INTELLIGENCE



Time-Series Index

Schema-on-Read

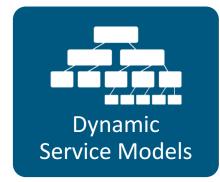
Data Model

Common Information Model



Splunk Service Intelligence

Data-driven service monitoring and analytics





At-a-Glance Problem Analysis



Early Warning on Deviations





SPLUNK IT SERVICE INTELLIGENCE



Time-Series Index

Schema-on-Read

Data Model

Common Information Model

Delivering Consistent Outcomes

Improve Customer Experience

Provide End-to-End Visibility Decrease Incidents and MTTR

Redeploy IT Effort to Proactive Tasks

Common IT Operational Analytics Outcomes (2000+ Customers Analysed, 300+ with ITSI)













SPLUNK IT SERVICE INTELLIGENCE

splunk>



Windows

















Changes

Outside the Datacenter

Log files

Linux/Unix

Configs

Messages
Virtualization
& Cloud

Traps Alerts

aps erts

Metrics

Applications

Scripts

Databases

Tickets

Networking

splunk isten to your data

ITSI Terminology

Logical grouping of operations

Set of actions performed with specific business goals

Component required to deliver a service

Metrics used to evaluate success

EXAMPLES

- Online banking
- Authentication
- Virtualization

EXAMPLES

- Sell products
- Fulfill orders
- Process payroll

EXAMPLES

- Hosts
- Users
- OS Processes

EXAMPLES

- Service health
- Order revenue
- Latency

SERVICES

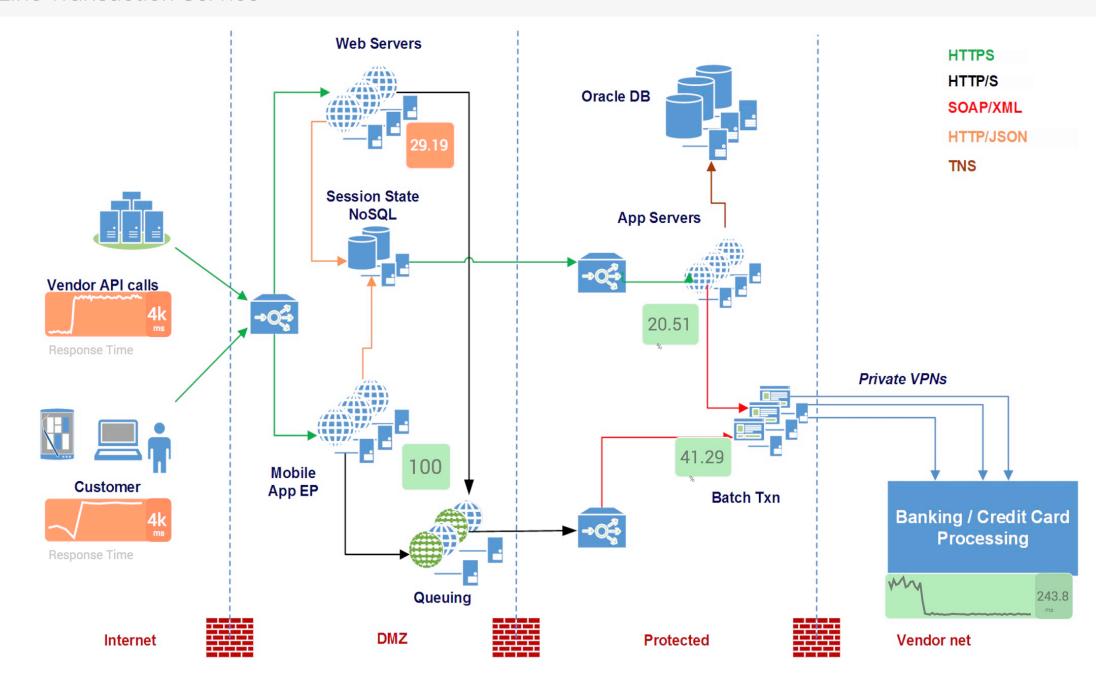
BUSINESS PROCESSES **ENTITIES**

KEY PERFORMANCE INDICATORS

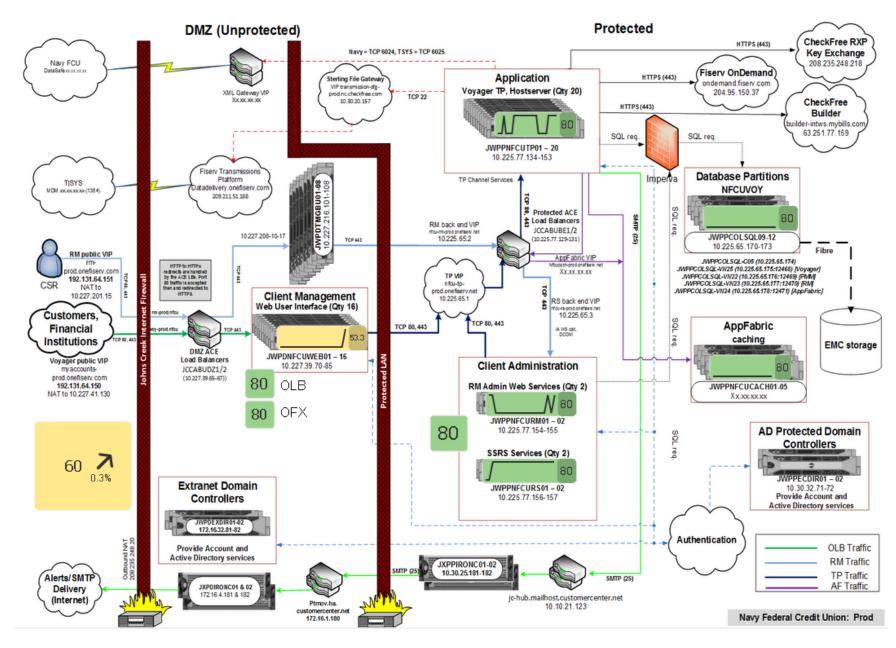
```
The Possibilities:

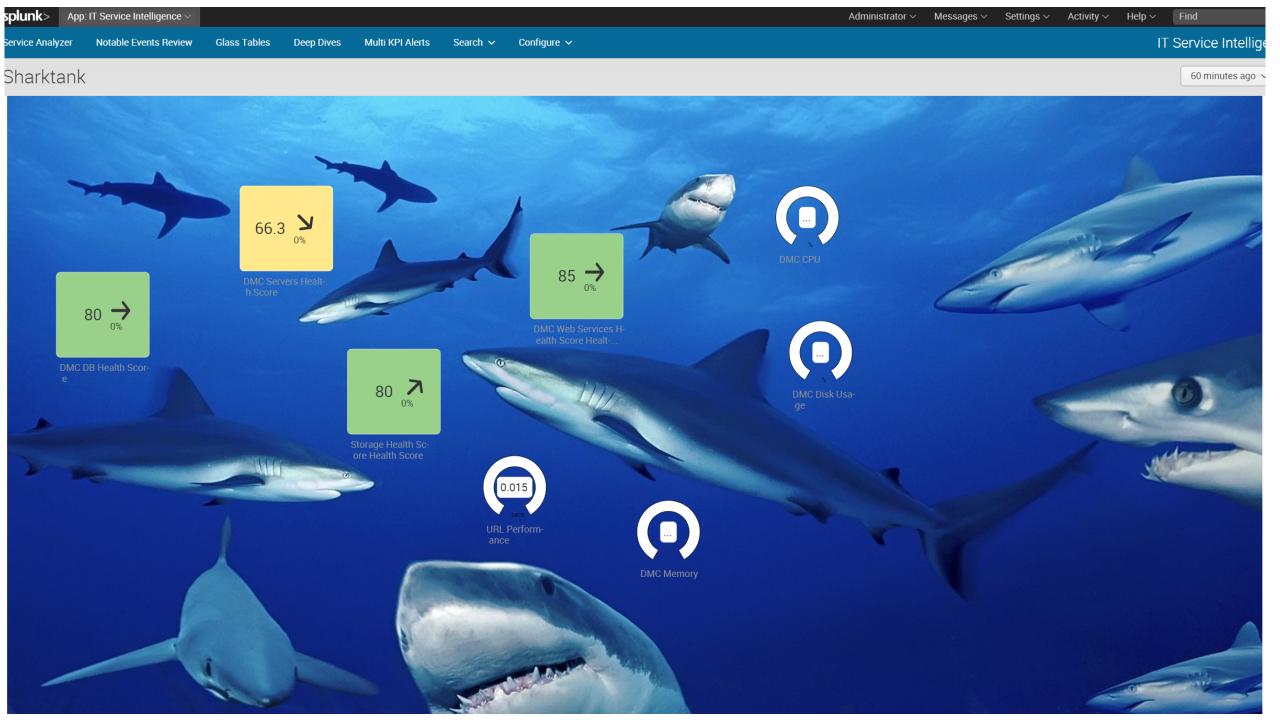
| The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Possibilities: | The Poss
```

splunk > listen to your data



Federal Credit Union- Glass table







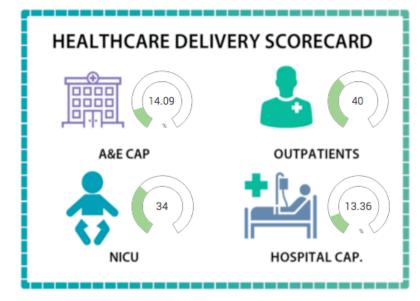
The Possibilities: **Business Glass Tables**

splunk > listen to your data

Healthcare Service Delivery Overview



http://convergingdata.com



OVERALL STATUS



CARE PATHWAYS



TERTIARY SERVICES

SERVICE / ICONS	STATUS	TREND
Pathology	7	16.5
Pharmacy	3	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
Patient Transport	1k	100
Facilities	7	100

SPECIALIST SERVICES

SERVICE / ICONS	STATUS	TREND
Medical imaging	16	my 2
ICU	16	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
NICU	16	my 5
Maternity	100	100
Theater	170	100

SPECIALIST SERVICES



TERTIARY SERVICES



HOSPITAL STATUS LAST 7 DAYS

PATIENTS LAST 7 DAYS				40			
ICU	17	Theater	88	•	ALS/PACE CALL		
A&E	7	Emergency	16	AL			
NICU	16	General	388		0	X	
		Out Patient	172	BIO/DISEASE OUT BREAK-<7D			

Edit

Now ~

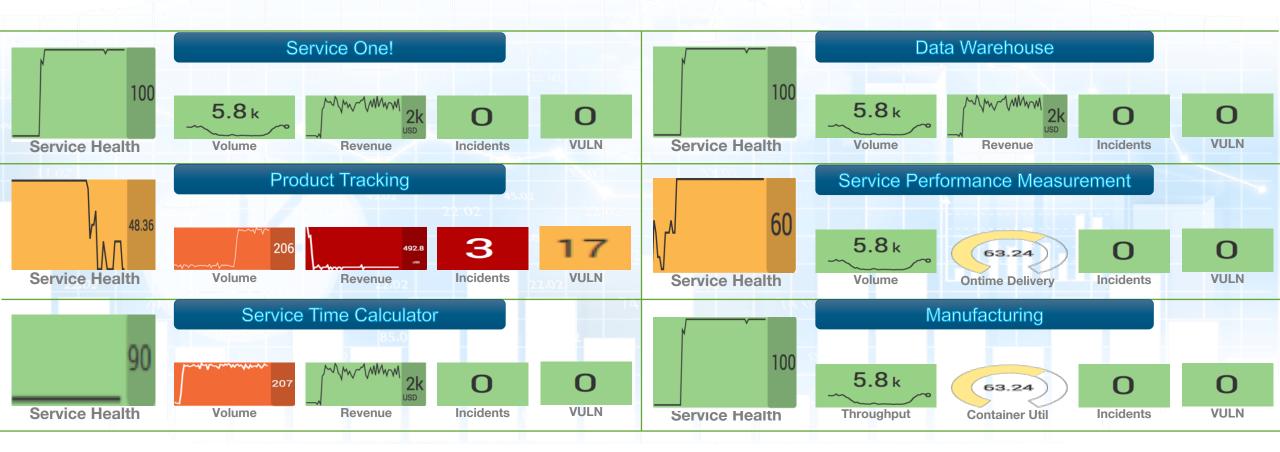
CIO Scorecard











```
Demo
     splunk > listen to your data
```

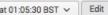
Messages V Settings V Activity V

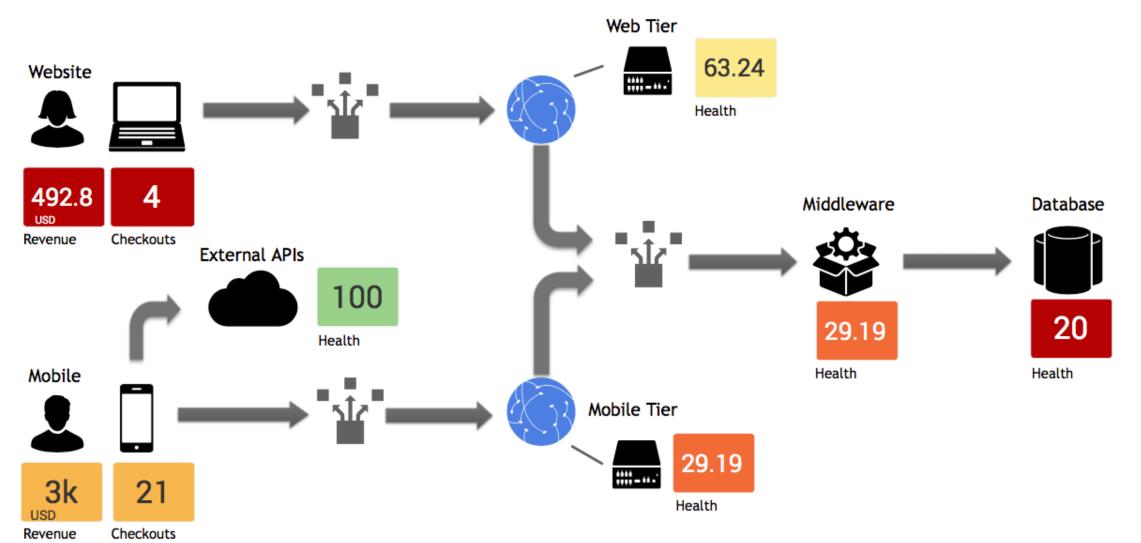
IT Service Intelligence

End to End Health

"7'133] "GET /Category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-lan 18:10:56:123] "GET /product.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-sh. 1.1" 405 322 "http://buttercup-sh. 1.1" 405 322 "http://buttercup-sh. 1.1" 405 322 "http://buttercup-sh. 1.1" 406 322 "http://buttercup-sh. 1.1" 406 322 "http://buttercup-sh. 1.1" 407 322 "http://buttercup-sh. 1.1" 408 322 "http://bu

30 June 2016 at 01:05:30 BST V Edit





All values are per minute



63.24

Healthscore



. 48:10:57:153] "GET / Gategory.screen?category_id=GIFTS&ISESSIONID=SDISLAFF10ADF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-Sep.
- MEF 07/10 18:10:57:123] "GET / Category.screen?category_id=GIFTS&ISESSIONID=SDISLAFF10ADF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-Sep.
- Oduct_id=1.1.4322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-Sep.
- Oduct_id=1.4222 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-Sep.
- Oduct_id=1.4222 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-Sep.
- Oduct_id=1.4222 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-Sep.
- Oduct_id=1.1.4322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-Sep.
- Oduct_id=1.4222 "http://buttercup-shopping.com/cart.do?action=purchas

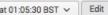
Messages V Settings V Activity V

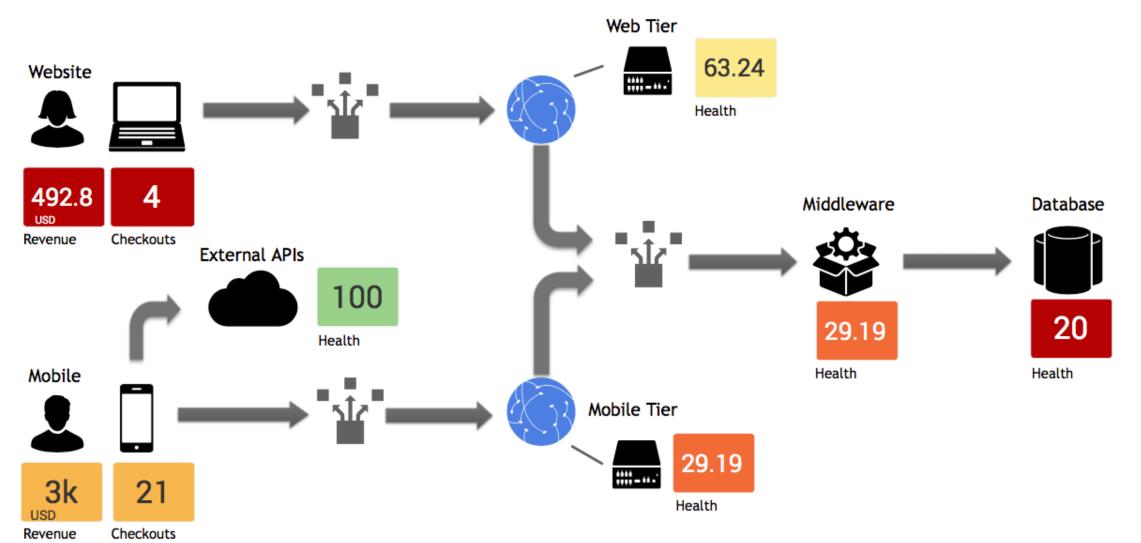
IT Service Intelligence

End to End Health

"7'133] "GET /Category.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-lan 18:10:56:123] "GET /product.screen?category_id=GIFTS&JSESSIONID=SDISL4FF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-sh. 1.1" 405 322 "http://buttercup-sh. 1.1" 405 322 "http://buttercup-sh. 1.1" 405 322 "http://buttercup-sh. 1.1" 406 322 "http://buttercup-sh. 1.1" 406 322 "http://buttercup-sh. 1.1" 407 322 "http://buttercup-sh. 1.1" 408 322 "http://bu

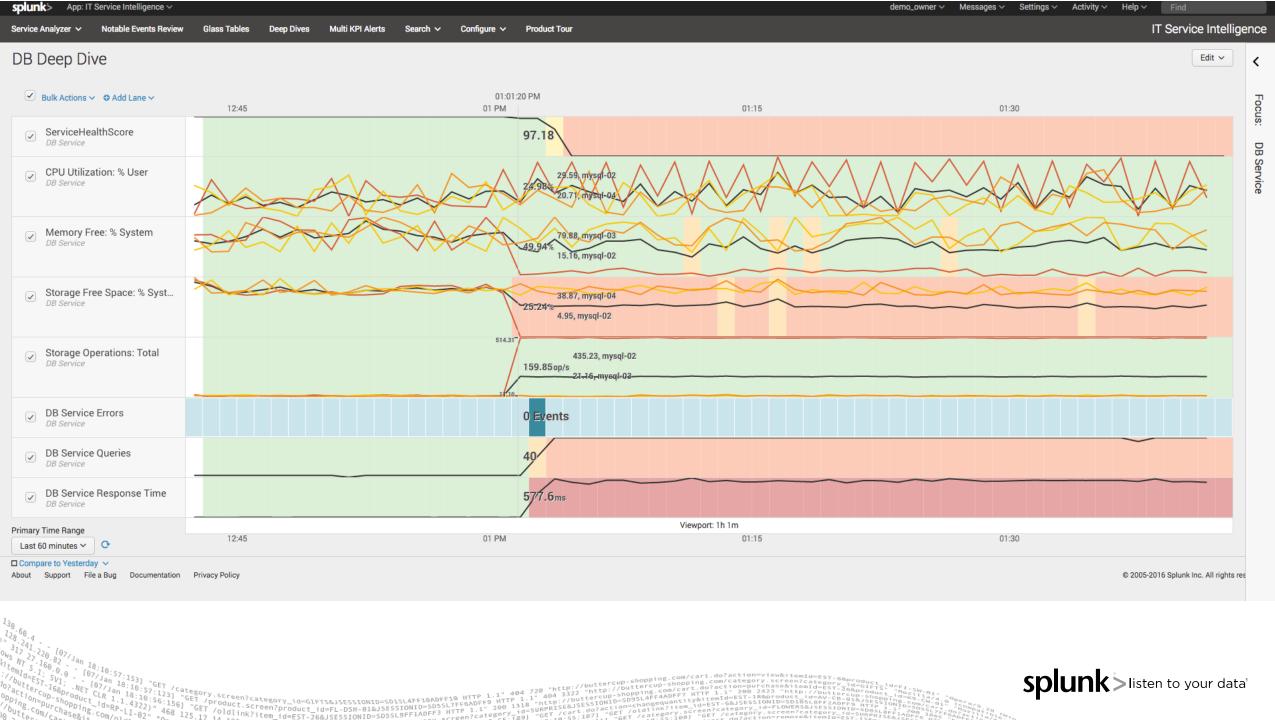
30 June 2016 at 01:05:30 BST V Edit





All values are per minute







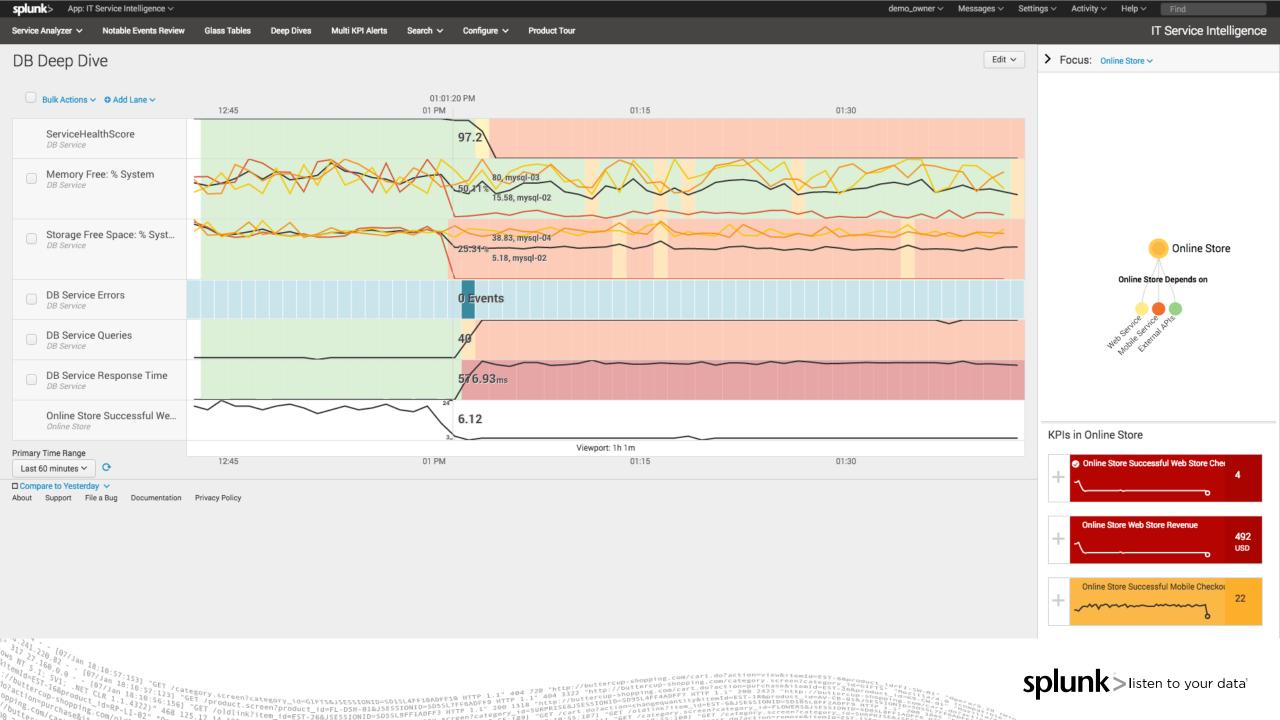


splunk'> App: IT Service Intelligence >



Settings V Activity V Help V





A lot of companies are using their machine data...











Web

Music

Retail

Hotel

Telecom



Travel



Auto



Banking



Healthcare



Government



defi-3. degory.screen?cer egopping.com/ gory shopping.com/as een?category een?category ic

(Windows NT 6; 0;

tegory | d | Book i

do?action=re-404 474 1.1 oduct_id=AV-233.243 - SB-; 1.uct_/G; 1.v-5B, c; 78.233.243 \(\text{intosh}; \quad \text{U}; \quad \text{Intell} \)

6117 189 82.245.228 189 82.245.36

een.
en-US) ABELEWEDK
en-US) ABELEWEDK
tercup-shoppedkebk
ADFF2 HTTP DINECK
ADFE2 HTTP DINECK
ADFE2 HTTP DINECK

FF2 HTTP =TEDDY&JSES17 "POSTESS"

reen?category

en-us) POST

82.243. "Mozilla/4.036 200 1901 ".0 "6 200 1901 "httb

Thank You!

Any questions?

gparsons@splunk.com

splunk>