Splunk and IT Service Intelligence

SIG-NOC, 27th November 2017

Graham Parsons, Operations Specialist

splunk>

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.

splunk> listen to your data

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

splunk>

- Application Delivery
- IT Operations
- Security, Compliance & Fraud
- Business Analytics
- Network & Internet of Things

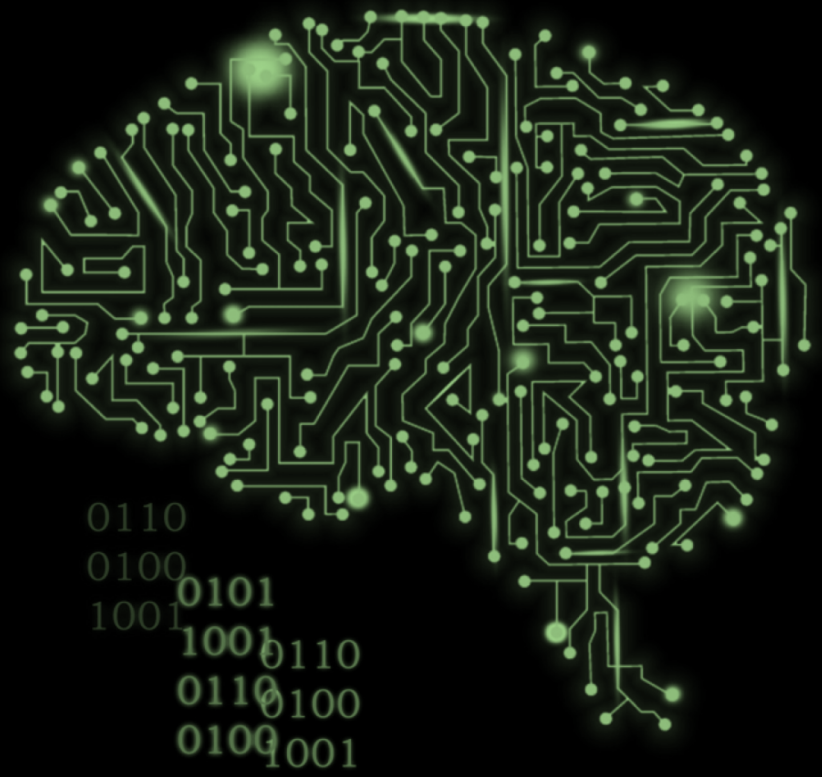
splunk>live!

OUR MISSION

Making machine data accessible, usable and valuable to everyone.

splunk> listen to your data®

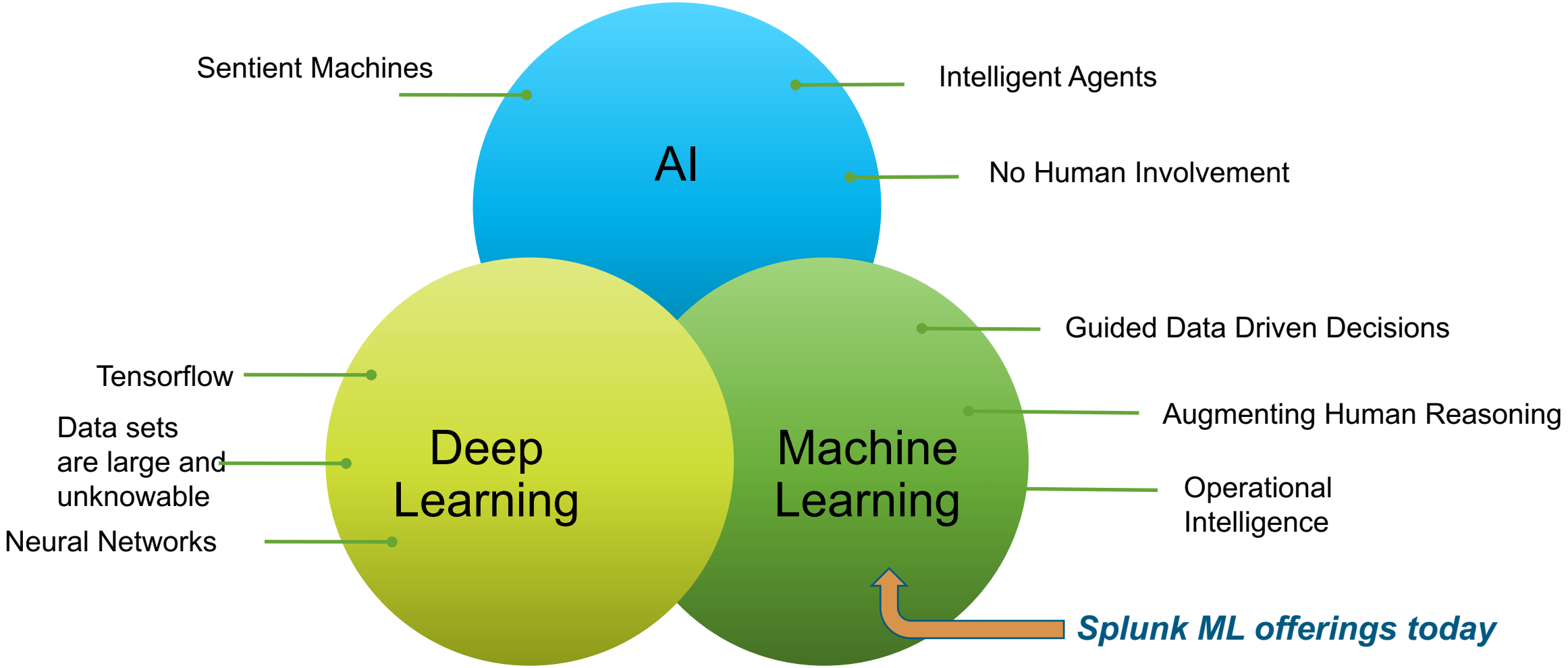
Machine Learning with Machine Data Unlocks Even More Value



Security | IT Ops | Network Ops | IoT

splunk> listen to your data®

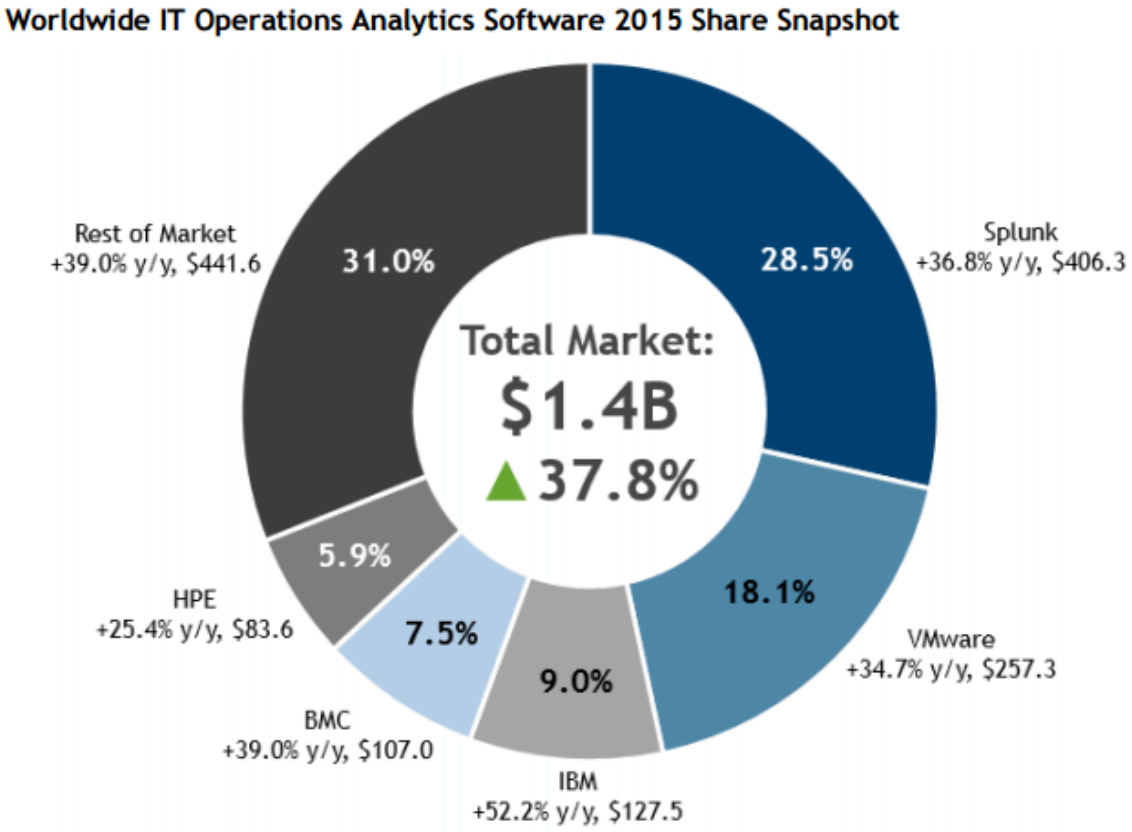
AI, Deep Learning, And Machine Learning



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)

splunk> listen to your data

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

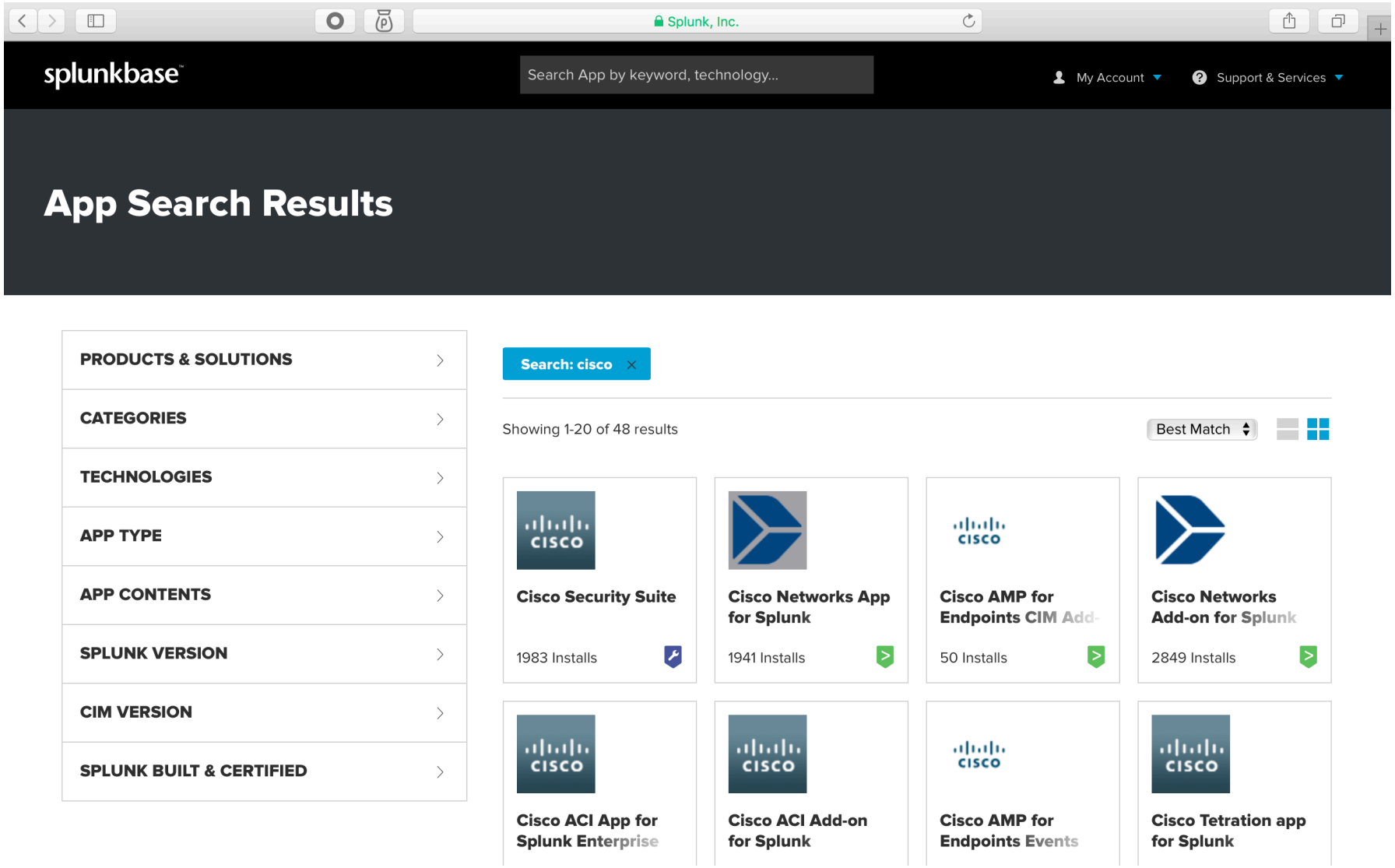
Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (August 2016)

*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 particular purpose.

splunk> listen to your data®

Splunk is a Platform



Splunk IT Service Intelligence

Splunk IT Service Intelligence

Data-driven service monitoring and analytics

Splunk ~~IT~~ Service Intelligence

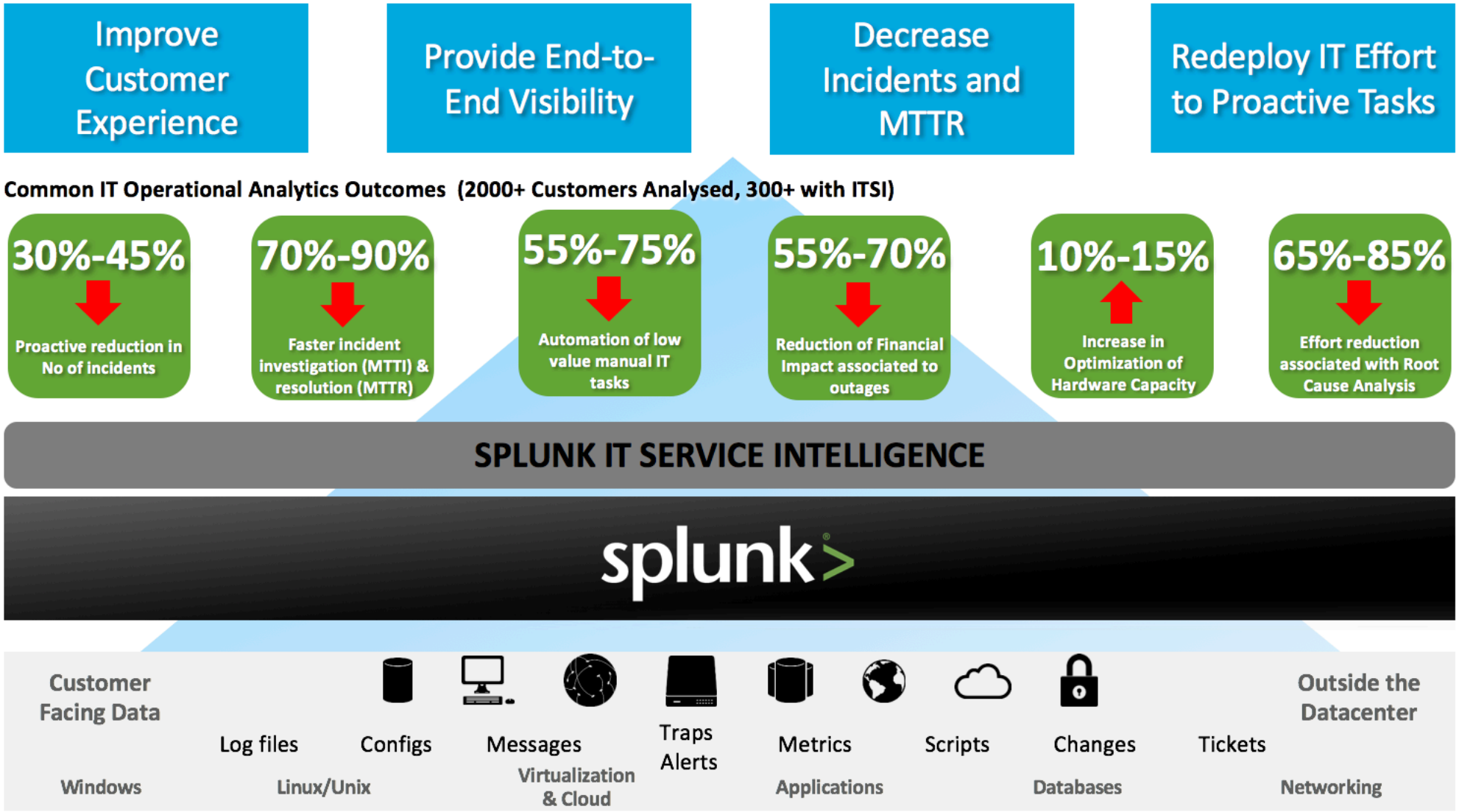
Data-driven service monitoring and analytics

SPLUNK IT SERVICE INTELLIGENCE

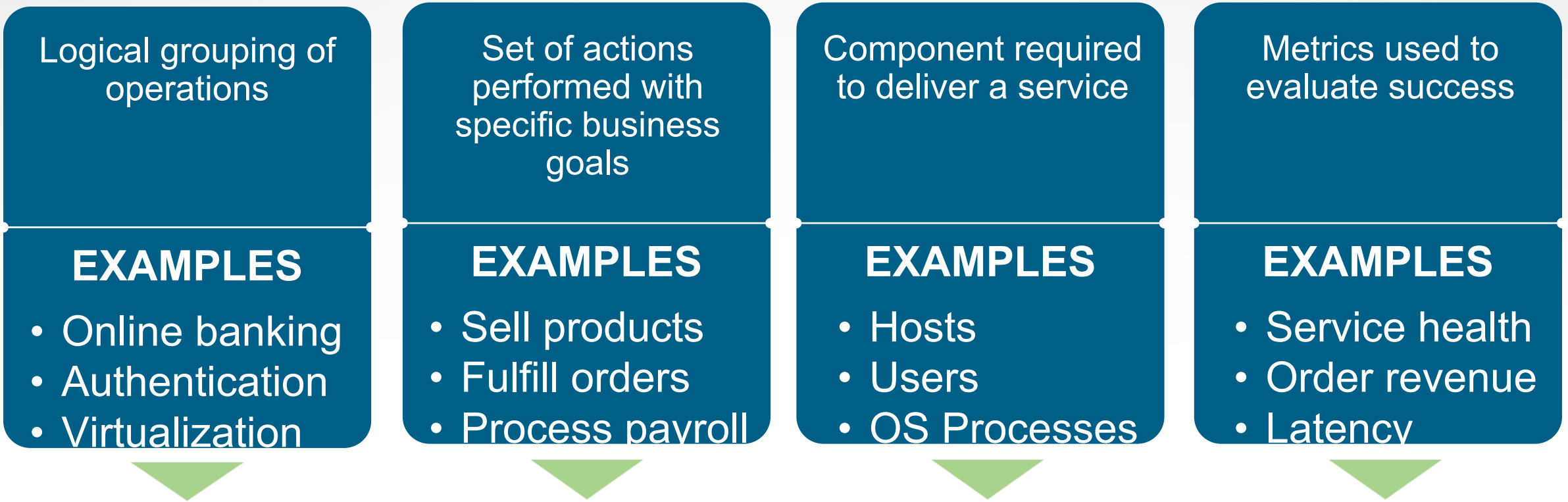
splunk> Platform for Machine Data

Time-Series Index	Schema-on-Read	Data Model	Common Information Model

Delivering Consistent Outcomes

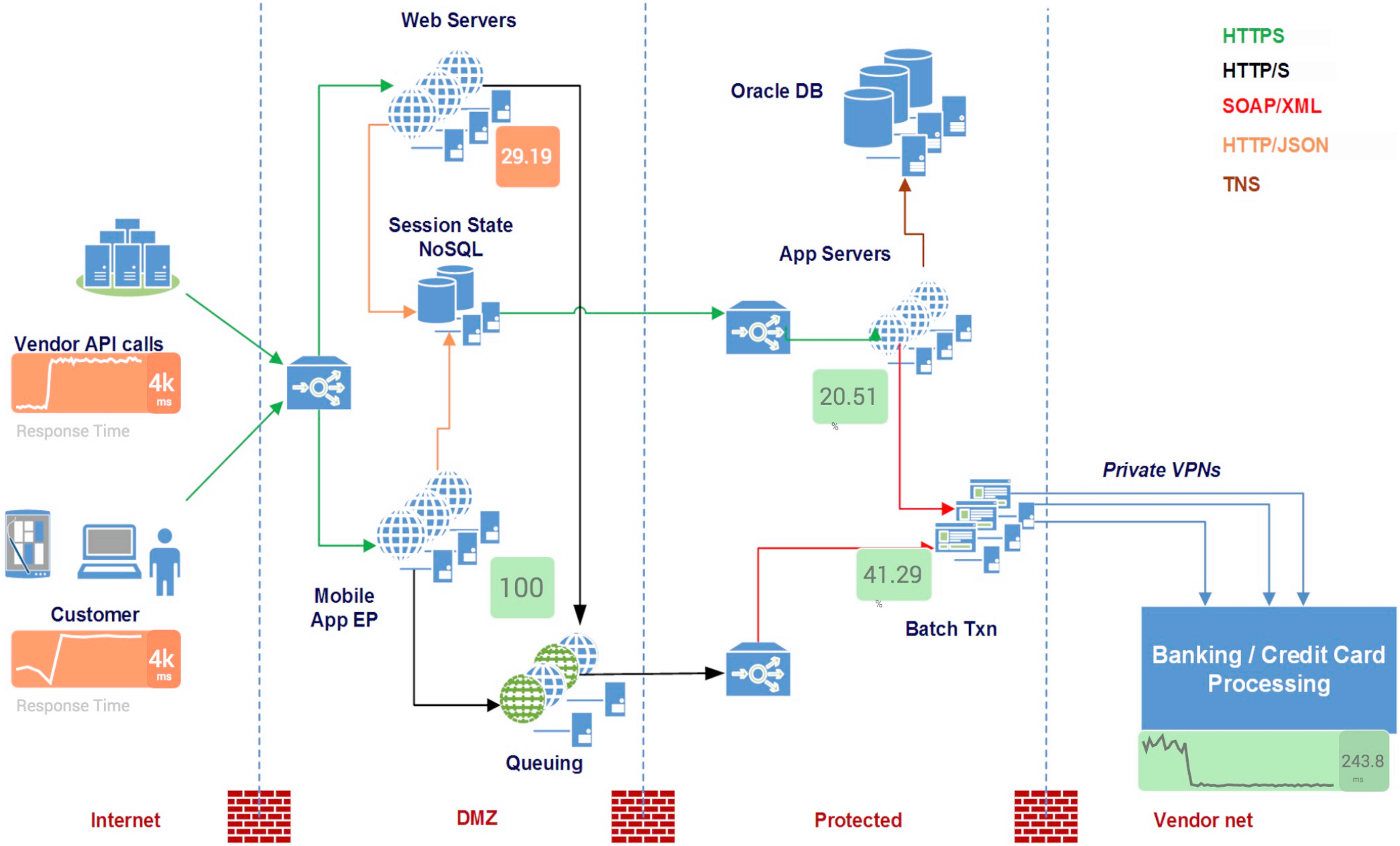


ITSI Terminology

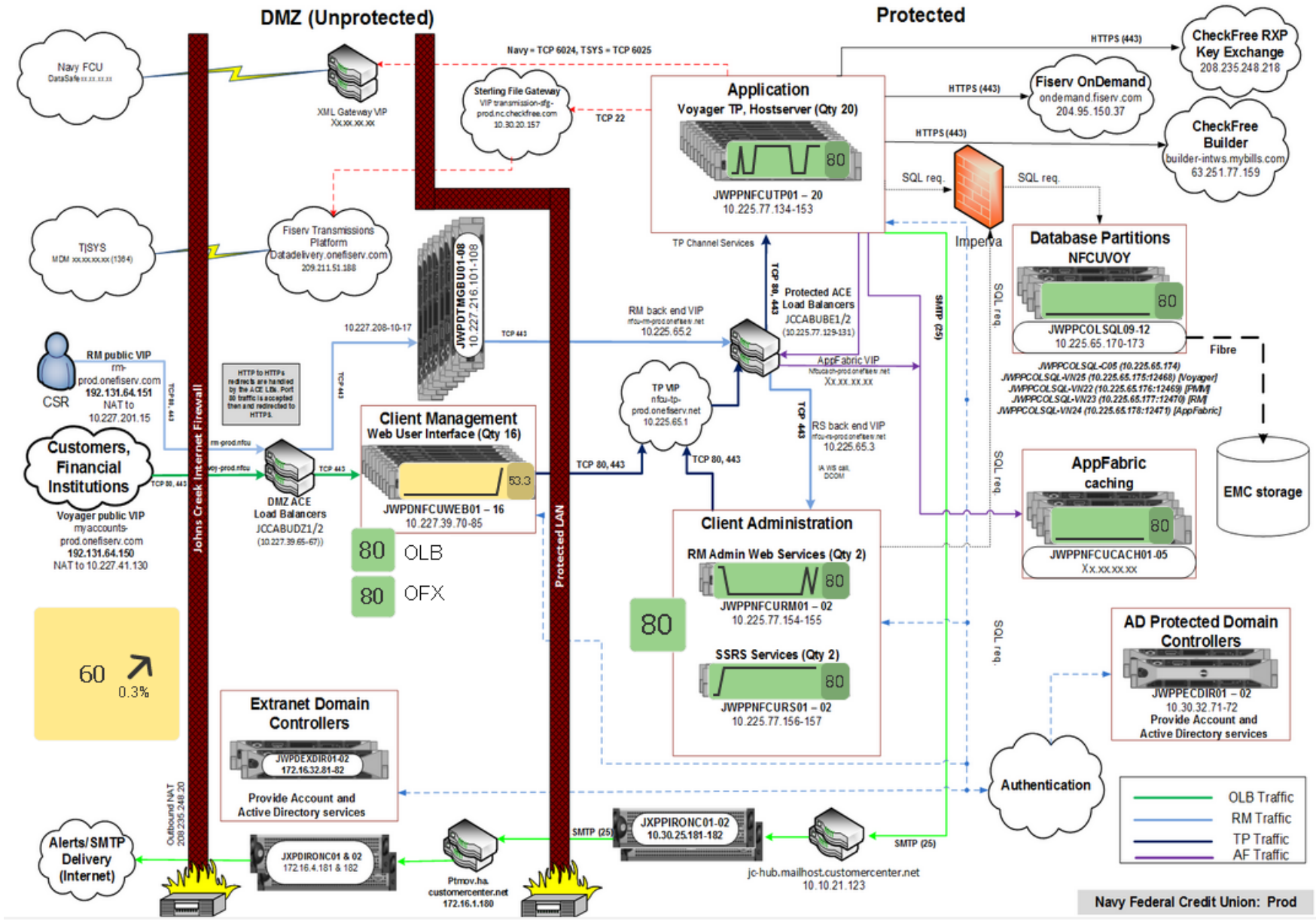


The Possibilities: IT Glass Tables

On Line Transaction Service



Federal Credit Union- Glass table



Sharktank

60 minutes ago

Sterling Metrics

The Possibilities: Business Glass Tables

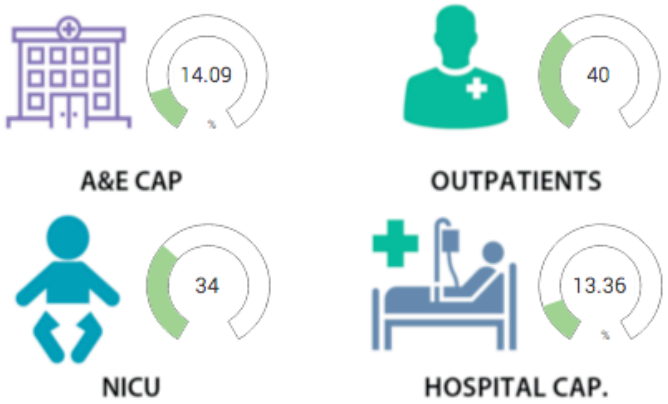
HEALTHCARE
SERVICE INTELLIGENCE

Healthcare Service Delivery Overview

CONVERGING DATA

http://convergingdata.com

HEALTHCARE DELIVERY SCORECARD



OVERALL STATUS

CARE PATHWAYS

TERTIARY SERVICES

SERVICE / ICONS	STATUS	TREND
Pathology	7	16.5
Pharmacy	3	69.6
Patient Transport	1k	100
Facilities	7	100

SPECIALIST SERVICES

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

SPECIALIST SERVICES

TERTIARY SERVICES

HOSPITAL STATUS LAST 7 DAYS

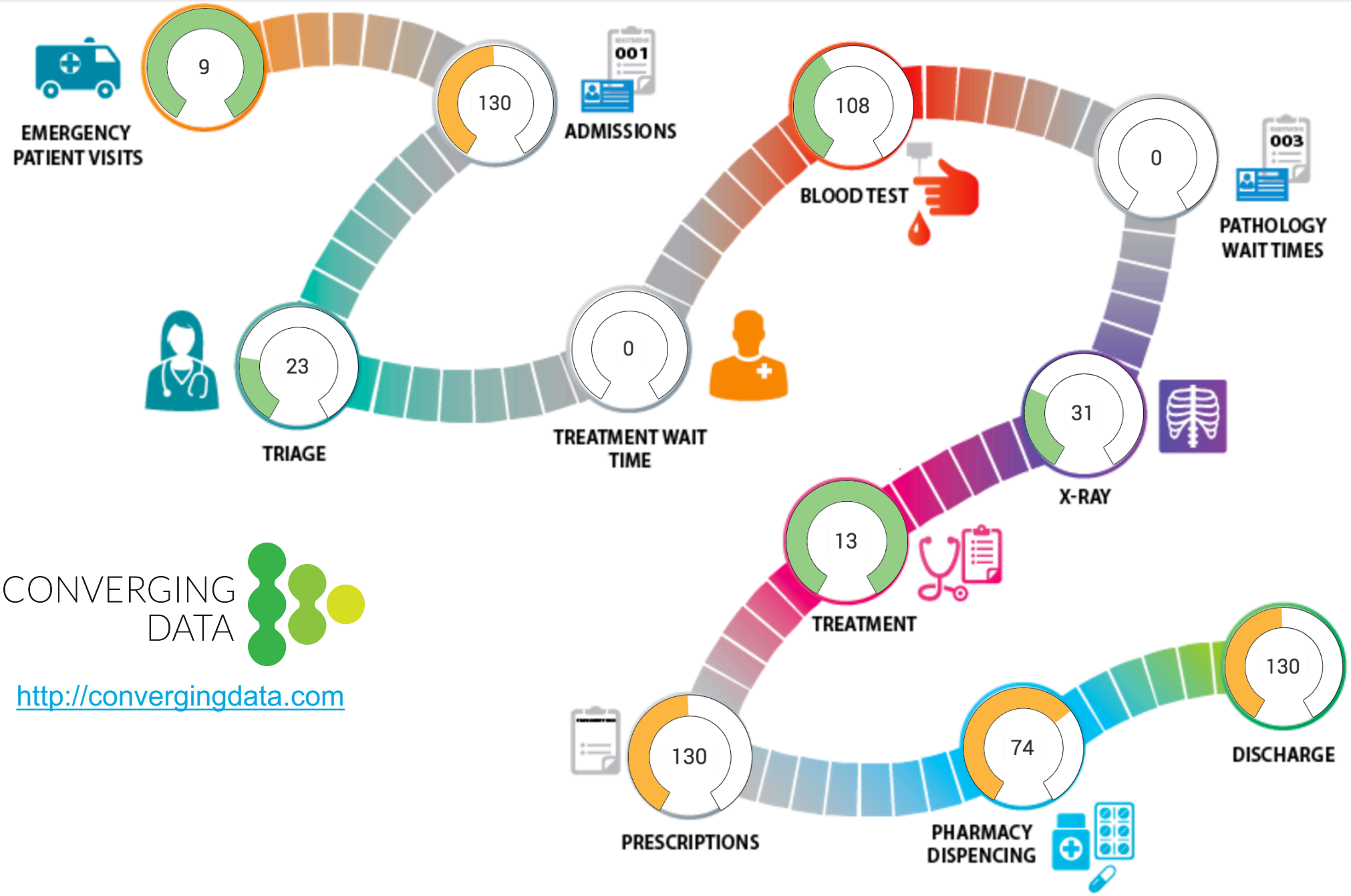
PATIENTS LAST 7 DAYS			
ICU	17	Theater	88
A&E	7	Emergency	16
NICU	16	General	388
		Out Patient	172

40

ALS/PACE CALL

0

BIO/DISEASE OUT BREAK-<7D



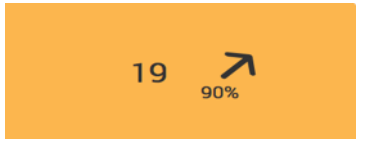
CONVERGING DATA

http://convergingdata.com

CIO Scorecard

Enterprise Service Status

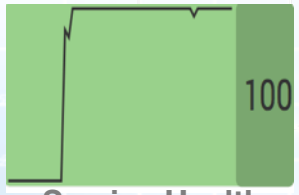
Major Incidents



Major Changes

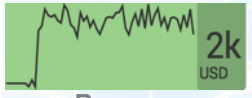
Sec Posture

Service One!



Service Health

Volume

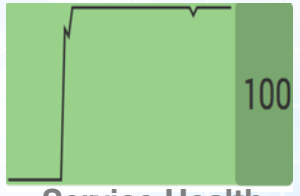


Revenue

Incidents

VULN

Data Warehouse



Service Health

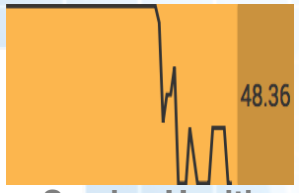
Volume

Revenue

Incidents

VULN

Product Tracking



Service Health

Volume

Revenue

Incidents

VULN

Service Performance Measurement

Service Health

Volume

Ontime Delivery

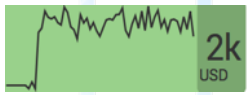
Incidents

VULN

Service Time Calculator

Service Health

Volume

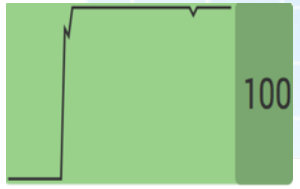


Revenue

Incidents

VULN

Manufacturing



Service Health

Throughput

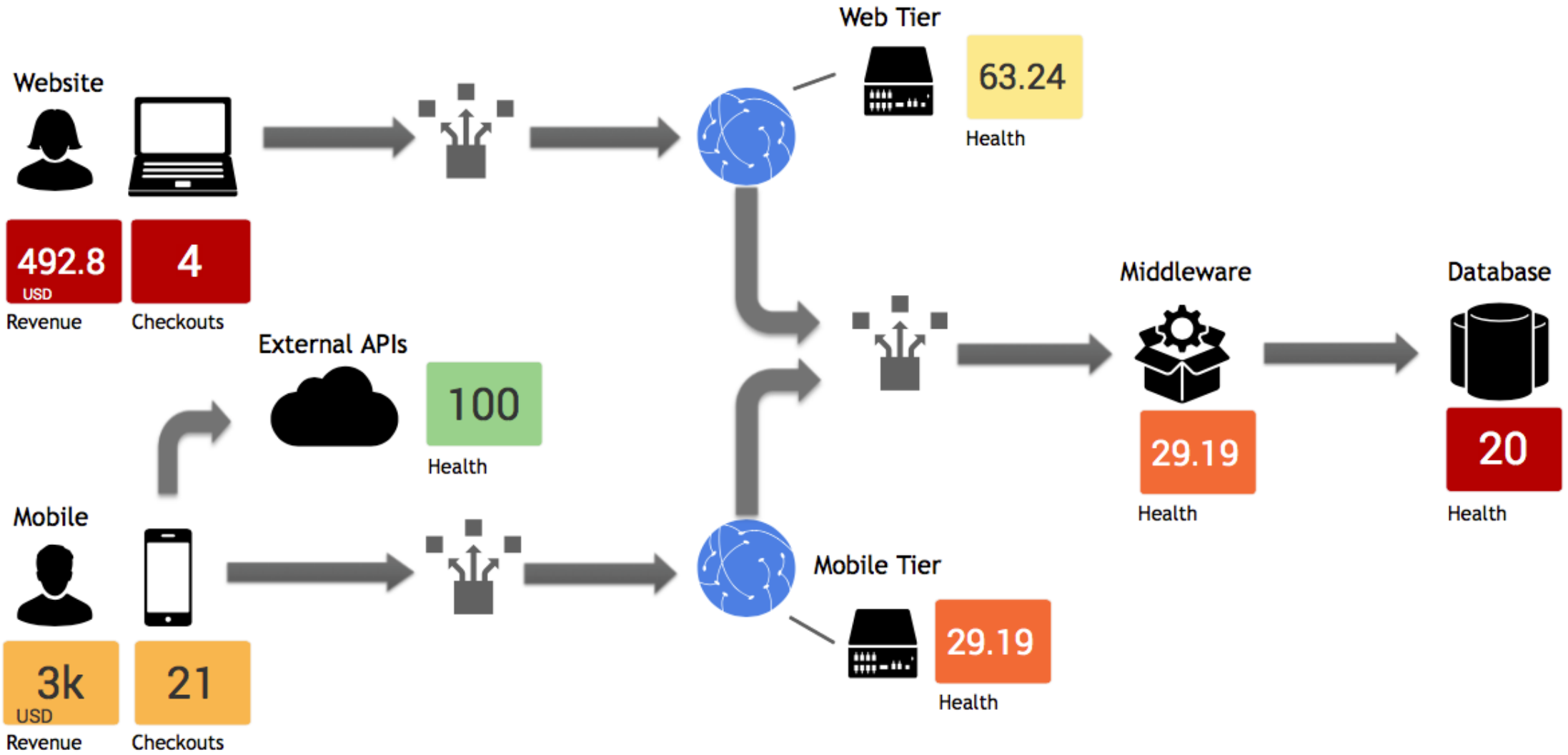
Container Util

Incidents

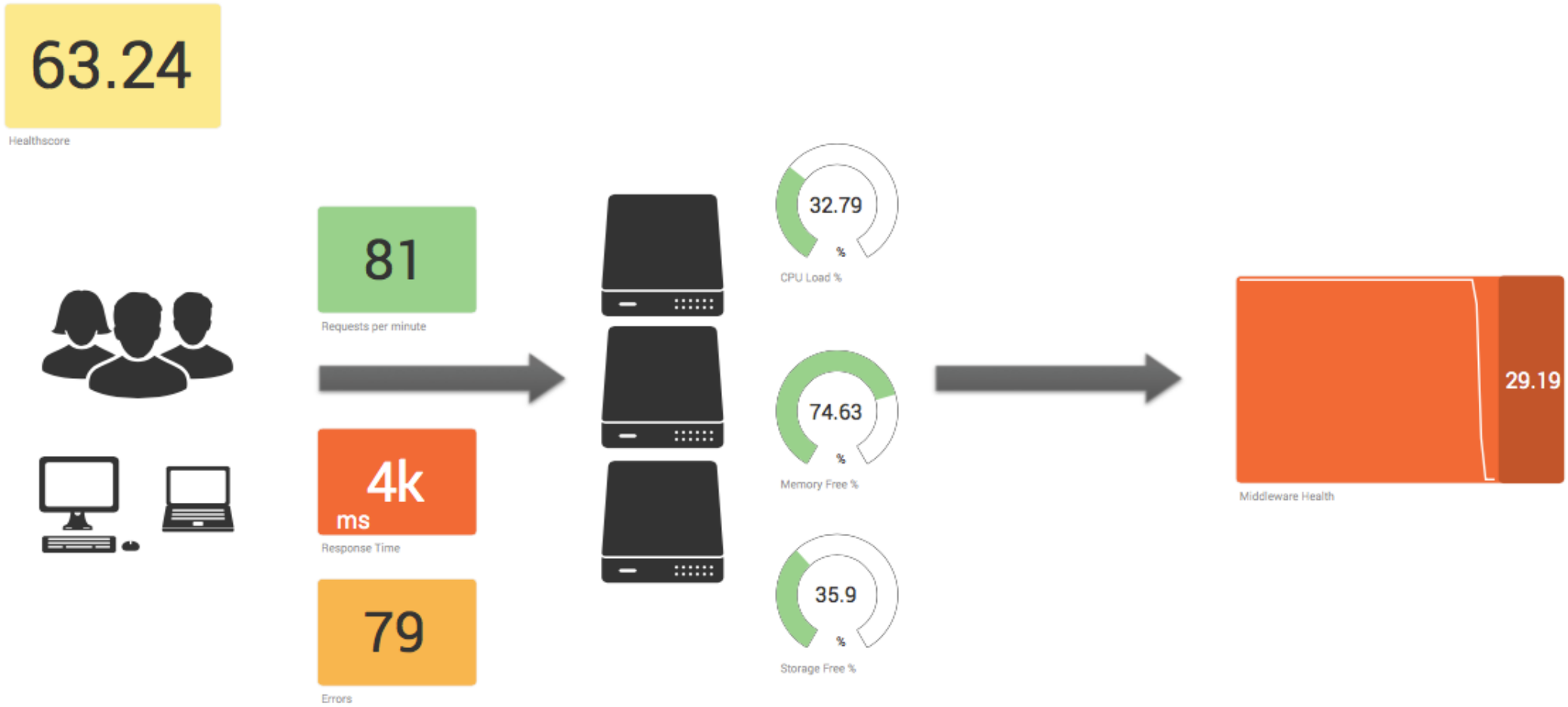
VULN

Demo

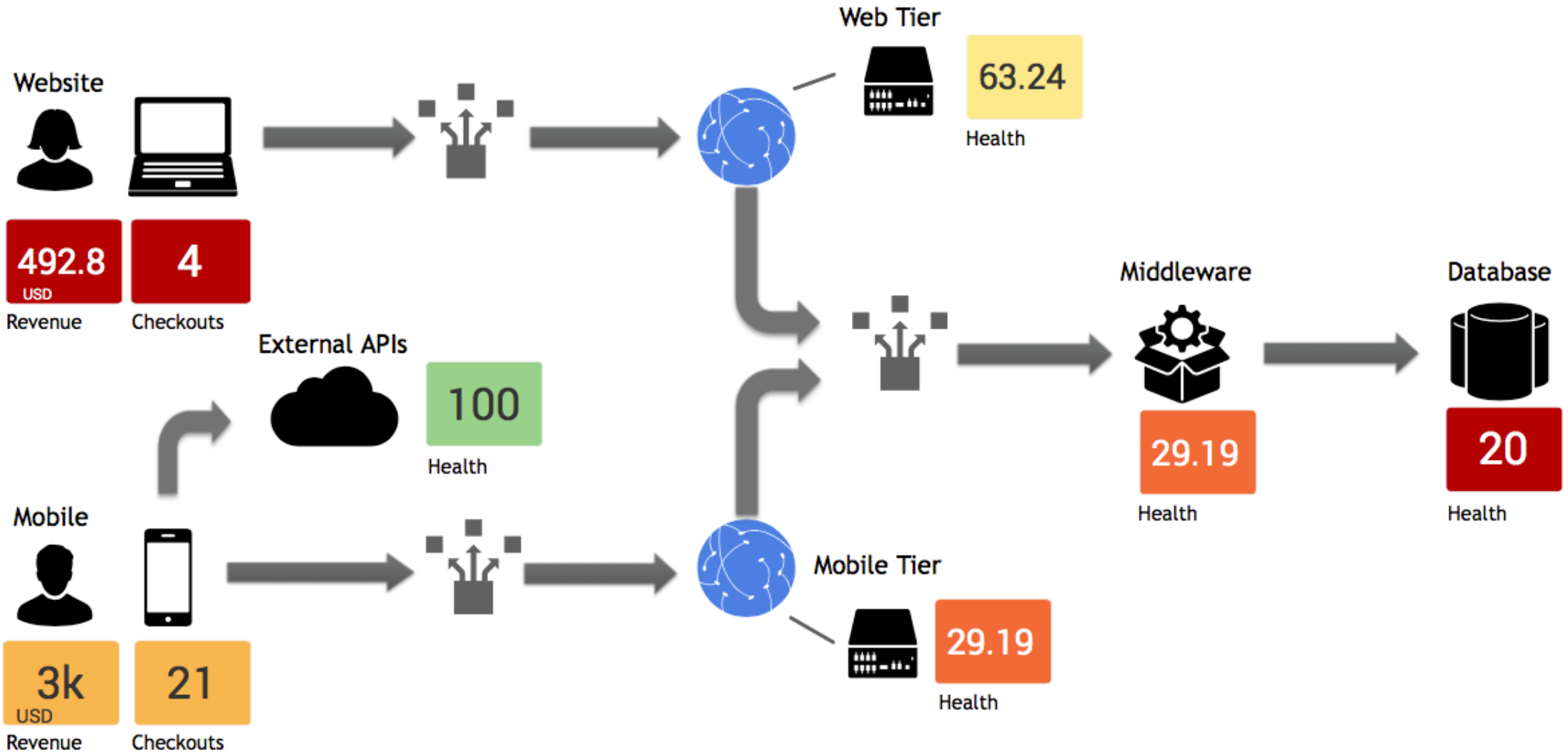
End to End Health



All values are per minute



End to End Health

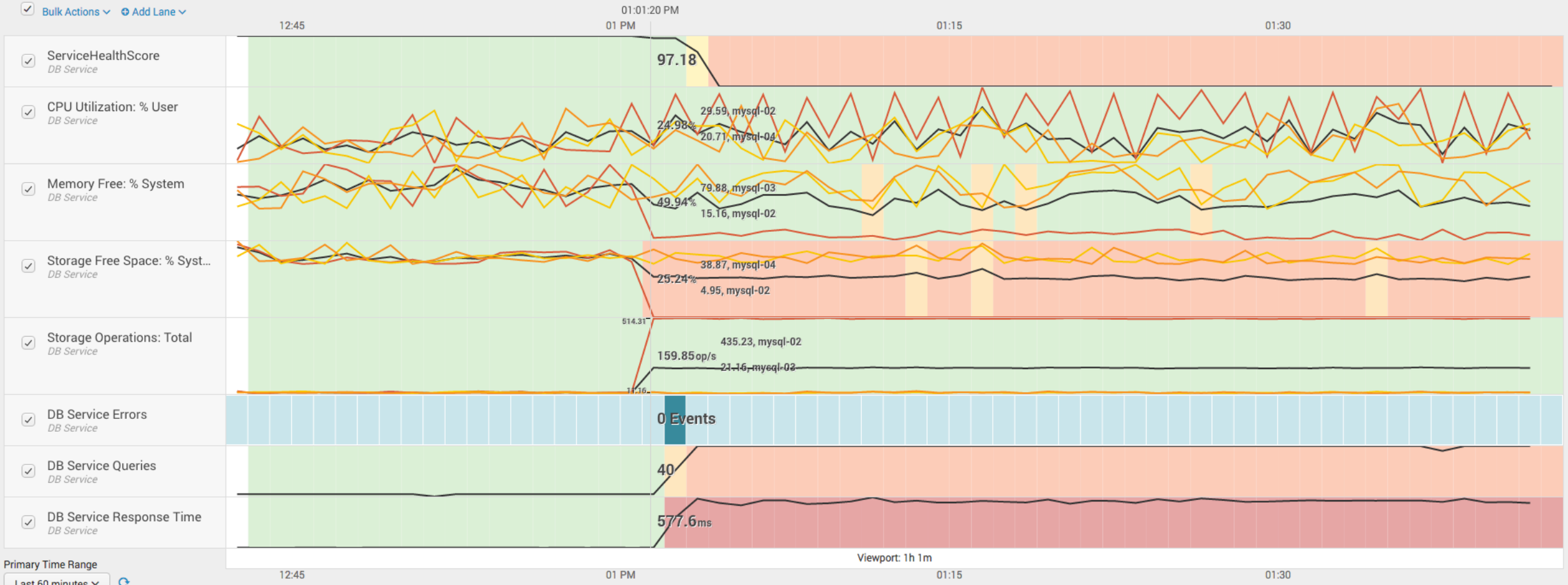


All values are per minute

DB Deep Dive

Edit

Bulk Actions | Add Lane



Primary Time Range

Last 60 minutes

Compare to Yesterday

Focus: DB Service

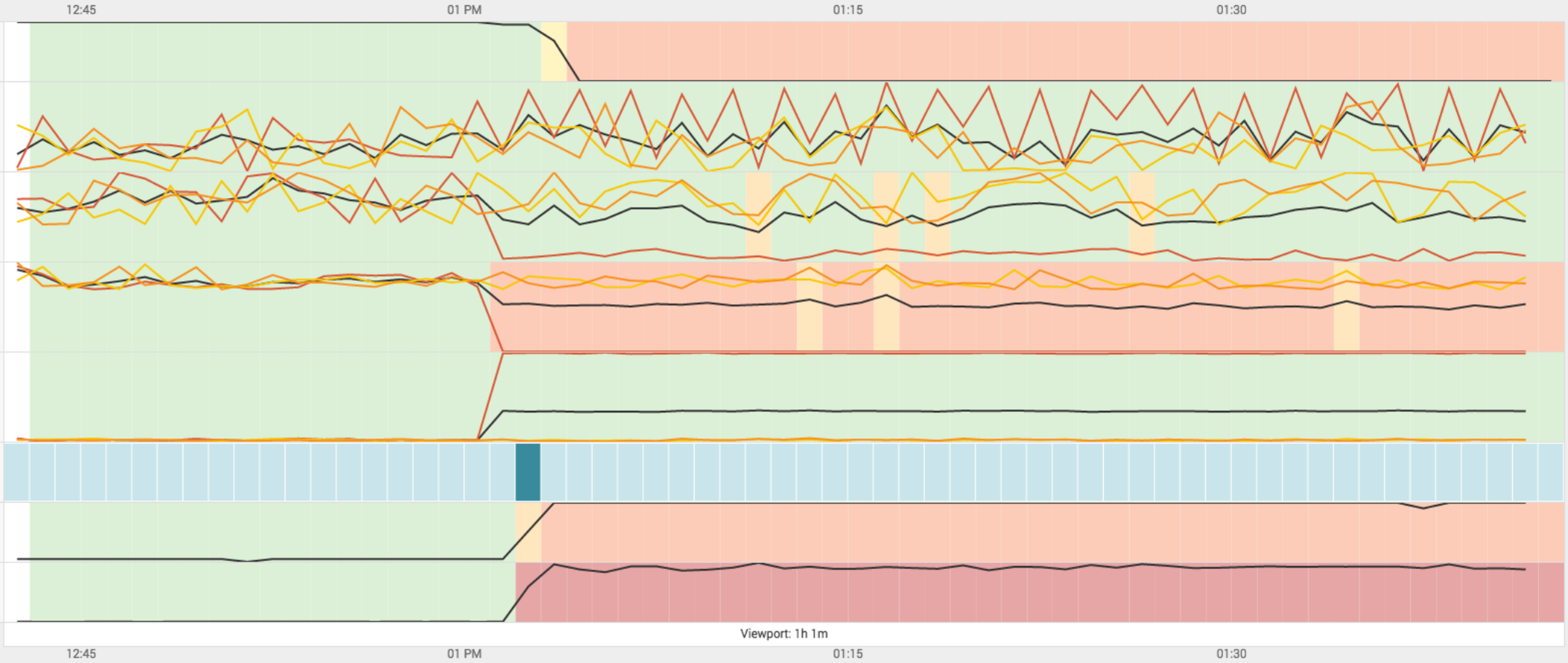
DB Deep Dive

Edit

Focus: DB Service

Bulk Actions Add Lane

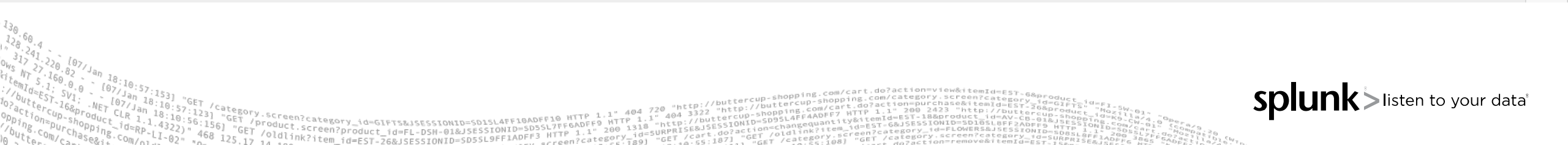
- Create Multi KPI Alert
- Show State Thresholds
- Show Level Thresholds
- Hide Thresholds
- Show Entity Overlays
- Hide Entity Overlays
- Delete



Primary Time Range

Last 60 minutes

Compare to Yesterday

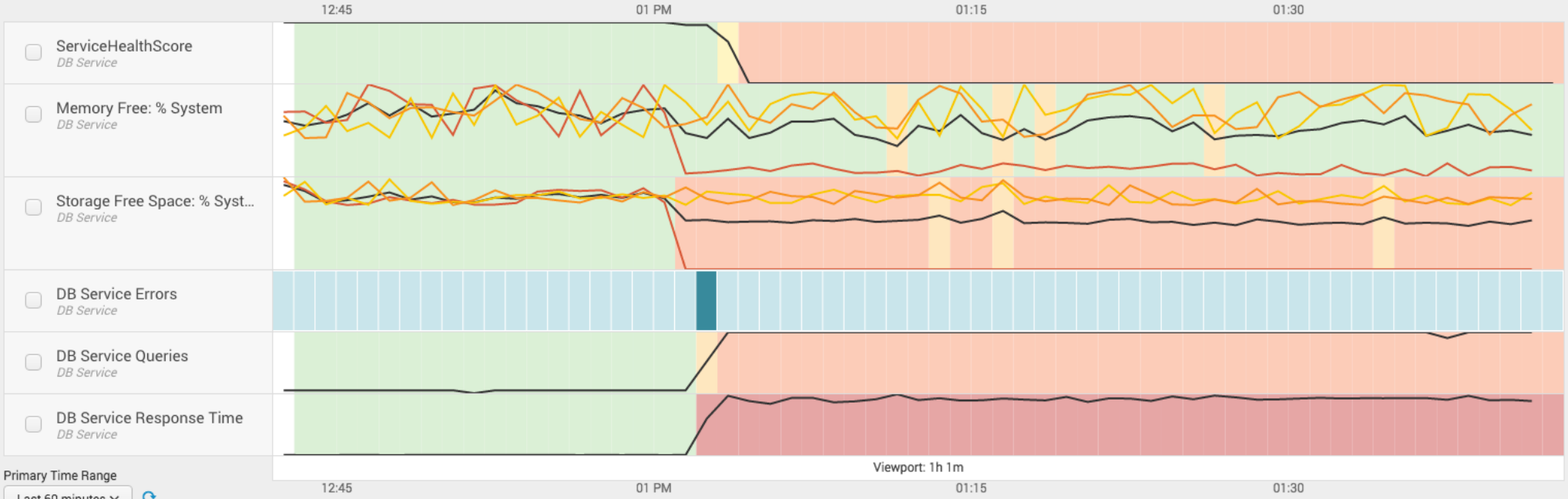


splunk> listen to your data

DB Deep Dive

Edit

Bulk Actions | Add Lane



Primary Time Range

Last 60 minutes

Compare to Yesterday

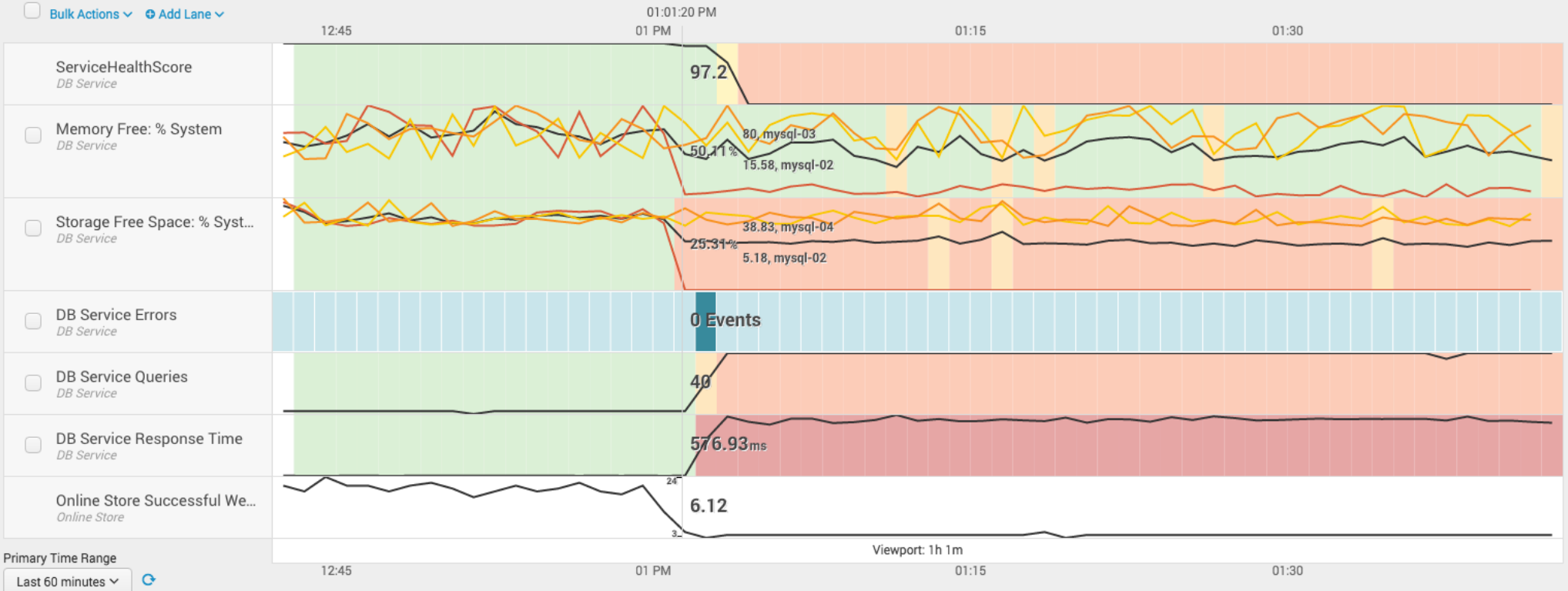
Focus: Online Store

KPIs in Online Store

DB Deep Dive

Edit

Bulk Actions Add Lane



Primary Time Range

Last 60 minutes

Compare to Yesterday

Focus: Online Store

KPIs in Online Store

A lot of companies are using their machine data…

YAHOO! — Web

SHAZAM — Music

TESCO — Retail

Expedia — Hotel

vodafone — Telecom

Gatwick — Travel

Auto

UniCredit — Banking

NHS — Healthcare

Ministry of Defence — Government

Thank You!

Any questions?

gparsons@splunk.com

splunk>