

.conf2015

Splunk ITSI Creating Business Value

Scott Barnhill

VP of IT and Security,
AdvancedMD

splunk>

Disclaimer

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 the 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.

Referenced customers for ITSI product participated in a limited release software program that included items at no charge.



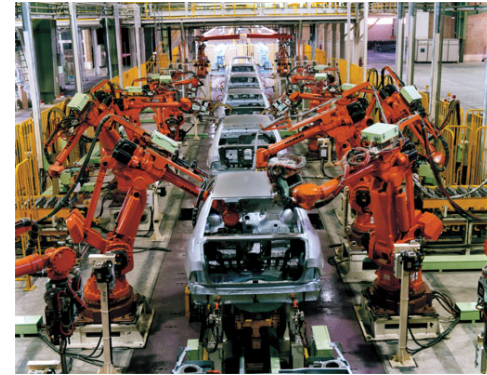
AdvancedMD is a leading provider of cloud-based practice management (PM), electronic health records (EHR) and revenue cycle management (RCM) solutions focused on the independent physician practice market.

AdvancedMD: By the Numbers

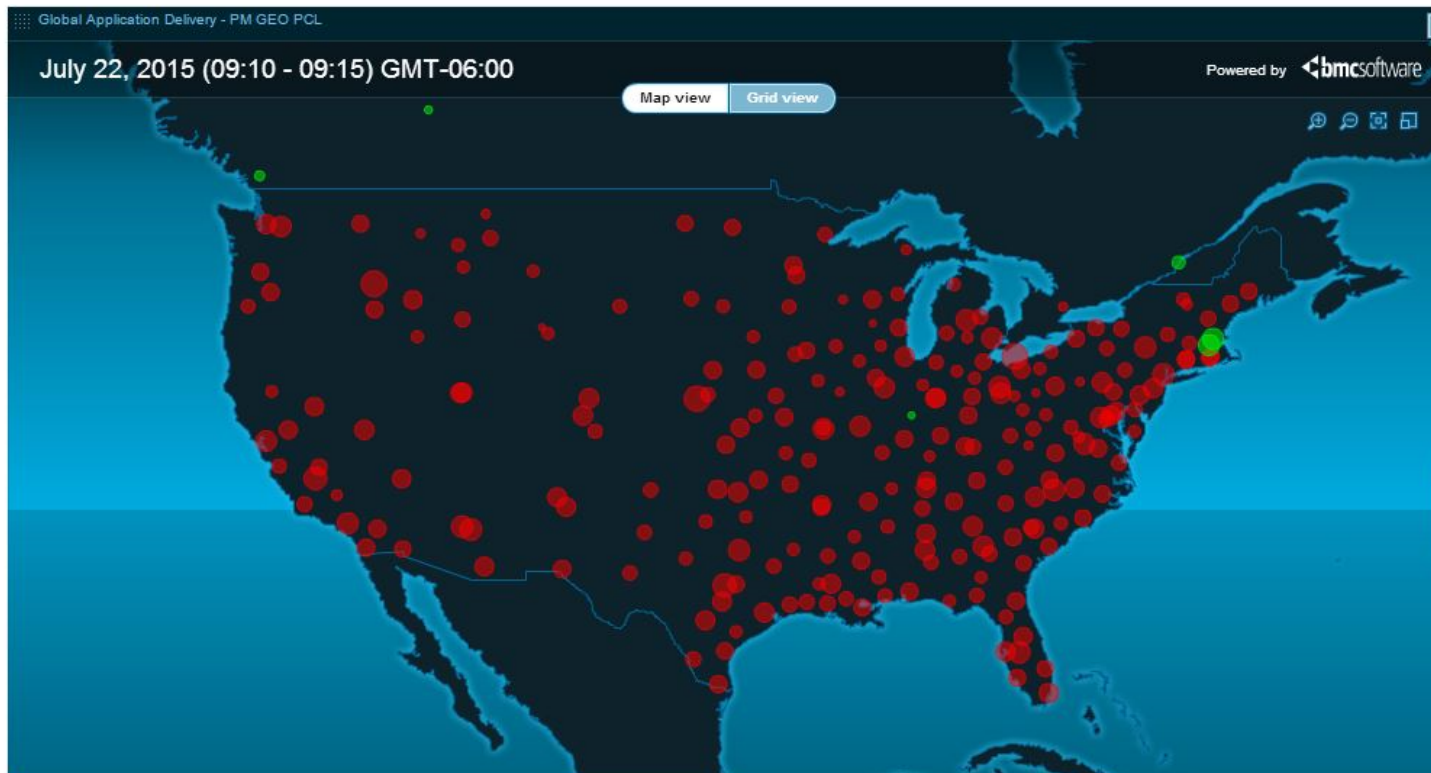
User Base	~ 79,000 Monthly, peak 15,000 daily concurrent
Patient Records	~ 75 Million HIPAA protected records
Servers	~ 625 Physical/virtual servers
Data Storage	~ 450 TB NetApp Storage
Databases	~ 1200 SQL databases, backed up hourly
Transactions/sec	~ 775/Second peak
Total transactions	~ 1 Billion PM/EHR transactions/month
Round Trip Response Time	~ 0.384 Seconds on average
Processing Time (server time)	~ 0.173 seconds on average
Claims Value	~ \$30 Billion/year

Complex Data flows

- Highly distributed architecture – built on a private cloud infrastructure
- Hand off between subsystems, interfaces, databases, 3rd party integrations
- Represent the primary purpose our clients use our products
- Assembly line processes



Monitoring



Kicking Tires

- Traditional I/T monitoring and triage
- Kick the tires on your sub-systems until you find the “flat”
- Process of elimination
- Typically driven by technology – look at servers, network, storage, etc...
- Until you find what is broken



Splunk ITSI

- Allows modeling of business process into I/T monitoring
- You can see what processes are “most important”
- Not just technology
- Common language across the business to assess impacts
- Watch an entire complex data flow and it’s assembly line in one screen
- AdvancedMD claims flow process – represents ~ \$30B/yr to our clients... it’s a pretty important process

.conf2015

Managing IT Ops with Splunk ITSI

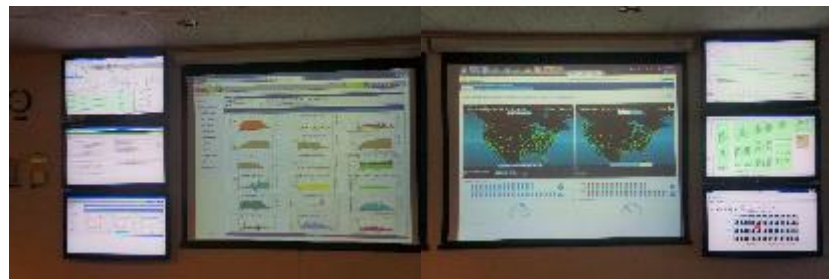
Tyler Germer

Director – Info. Technology,
AdvancedMD

splunk>

Operations Team Charter

- Managing our data center, production server, infrastructure
- Patching our online medical applications
- Reduce client impacting incidents
- Ensure application uptime
- Work with support teams on customer issues



AdvancedMD Splunk EcoSystem



The Problem: The Data Trail ...

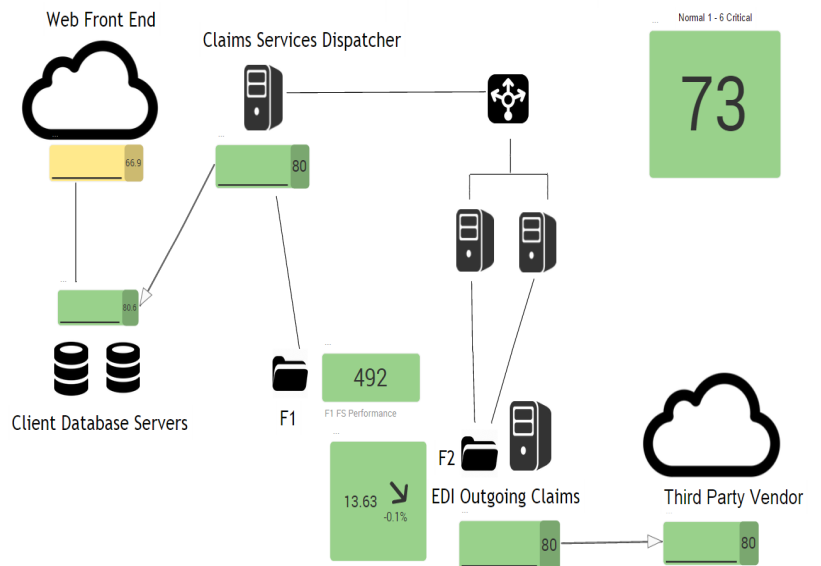
- Native Splunk Enterprise – data at your fingertips
- Which data/what questions/what thresholds?
- It's all about the 'flow'
- Splunk ITSI takes care of the guess work

Simplify

From

To

>	9/4/15 12:23:44.000 PM	{ [-] bytes: 201 dest_ip: 169.254.255.255 endtime: 2015-09-04T19:20:51.535247Z time_taken: 0 timestamp: 2015-09-04T19:20:51.535247Z user_id: 0 } Show as raw text host = WJ-EDIO2 source = stream:smb sourcetype = stream:smb
>	9/4/15 12:23:44.000 PM	{ [-] bytes: 220 dest_ip: 172.31.10.204 endtime: 2015-09-04T19:25:04.022844Z time_taken: 222 timestamp: 2015-09-04T19:25:04.022622Z } Show as raw text host = C-SVC03 source = stream:smb sourcetype = stream:smb
>	9/4/15 12:23:44.000 PM	09/04/2015 12:23:44 PM LogName=Application SourceName=AdvancedMD.Shared EventCode=0 EventType=2 Show all 14 lines host = CB-PM32 source = WinEventLog:Application sourcetype = WinEventLog:Application
>	9/4/15 12:23:44.000 PM	09/04/2015 12:23:44 PM LogName=Application SourceName=AdvancedMD.Report.Web.DLL EventCode=0 EventType=2 Show all 13 lines host = WJ-RS11 source = WinEventLog:Application sourcetype = WinEventLog:Application



Operations Made Easy

- Better high level visibility of ALL data flows
- Quicker TTR
- Better client experience
- Bigger client retention

.conf2015

Implementing Splunk ITSI

Coby Nielsen

Manager – Platform Applications,
AdvancedMD

splunk>

splunk> a_Coby Nielsen Messages Settings Activity Help Find

Apps >

>

Search & Reporting

ITSI


IT Service Intelligence

&

Sideview Utils


+

Explore Splunk Enterprise




Add Data

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.




Splunk Apps [↗](#)

Apps and add-ons extend the capabilities of Splunk Enterprise.



Splunk Docs [↗](#)

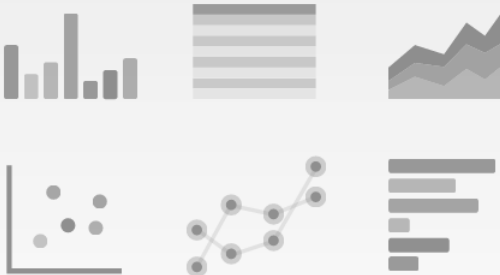
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.



Splunk Answers [↗](#)

Have questions about how to do something with Splunk products? Get answers fast.

Close



Opening page

Contains a view of
services and KPIs that
have been created

Quick overview of
any issues within IT
Service intelligence

Top 30 KPIs ⚙

1 2 27

30 Total



splunk> App: IT Service Intelligence ▾ a_Coby Nielsen ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Service Analyzer Notable Events Review Glass Tables Deep Dives Multi KPI Alerts Search ▾ **Configure ▾** IT Service Intelligence

Services
Viewer for all Services

Create New Service ▾

10 Services Bulk Action ▾ filter

i	<input type="checkbox"/>	Title ^	Entity Rules	KPIs	Actions
>	<input type="checkbox"/>	Claims Service	0	0	Edit ▾
>	<input type="checkbox"/>	Claims Services Dispatcher	0	4	Edit ▾
>	<input type="checkbox"/>	Client Database Servers	0	7	Edit ▾
>	<input type="checkbox"/>	EDI Outgoing Claims	0	5	Edit ▾
>	<input type="checkbox"/>	Eligibility Services	0	2	Edit ▾
>	<input type="checkbox"/>	F1 remote CIFS access	0	1	Edit ▾
>	<input type="checkbox"/>	F2 Local file access	0	1	Edit ▾
>	<input type="checkbox"/>	Relay Health	0	0	Edit ▾
>	<input type="checkbox"/>	Splunk Service	0	8	Edit ▾
>	<input type="checkbox"/>	Web Front End	0	8	Edit ▾

About Support File a Bug Documentation Privacy Policy

© 2005-2015 Splunk Inc. All rights reserved.

Key Performance Indicators

KPIs

Import

New ▾

PM Servers Used Memory

PM Servers Idle Time

PM Servers Disk Pct Free

PM Servers Disk GB Free

Web Response Successes

Web Response Time

Web Response Errors

SVC07 Used Memory

Name

Name PM Servers Used Memory

Description

Percent (%)

Search

Search Type

Data Model

Ad hoc

Search

index=prod_perfmon tag::host=pm-wfe
sourcetype="Perfmon:Memory"
counter="% Committed Bytes In Use"

Threshold Field

Value

Unit

Specify the unit of measurement to display in KPI visualizations. (For example "GB," "Mbps," "secs", etc.).

Generated Search

index=prod_perfmon
tag::host=pm-wfe
sourcetype="Perfmon:Memory"
counter="% Committed Bytes In Use"

[Run Search](#)

Monitoring

Importance

1 2 3 4 5 6 7 8 9 10 11

Calculation

Maximum ▾

Last 5 Minutes ▾

KPI Search Schedule

Every 5 Minute ▾

Take advantage of
using tags

Monitoring

Importance 1 2 3 4 5 6 7 8 9 10 11

Calculation Maximum ▾ Last 5 Minutes ▾

KPI Search Schedule Every 5 Minute ▾

Threshold

Threshold Type Aggregate Per Entity Both

Aggregate Threshold Values

■ Critical ▾ ×

■ Medium ▾ ×

■ Normal ▾ ×

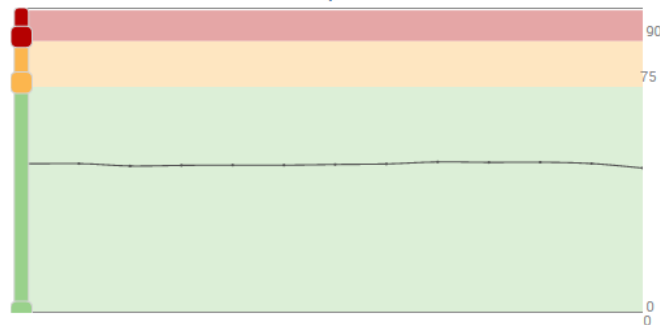
■ Normal ▾

[+ Add Threshold](#)

Generate Suggestions

Treat Gaps in Data as ■ Unknown ▾

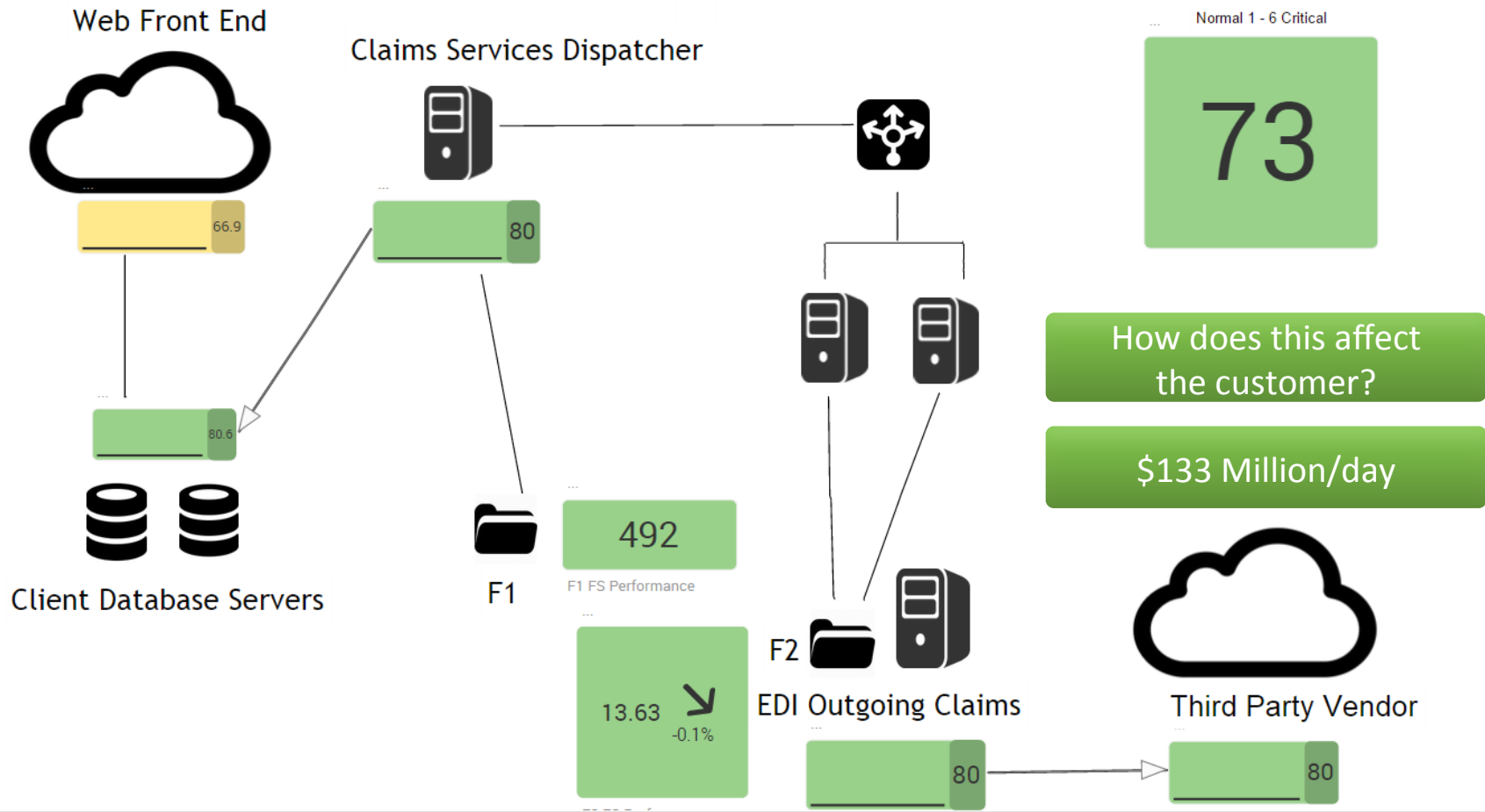
View data from the last 60 minutes ▾ ⚙



Done

Delete

Cancel





.conf2015

THANK YOU

splunk>