



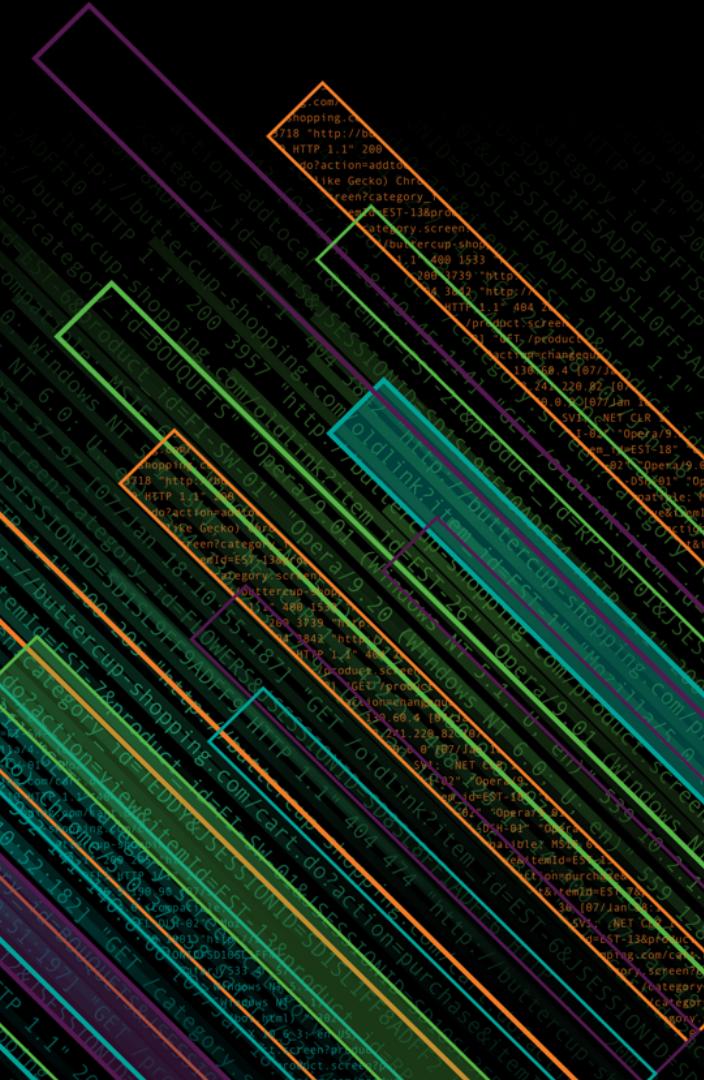
splunk>

Automate Your IT! Moving Faster with Puppet and Splunk

Domnick Eger | Global DevOps Practitioner

Chris Barker | Partner Engineering

October 2018 | Version 1.0



Today's Precentors



DOMNICK EGER

**Global DevOps Practitioner
from Splunk**



CHRIS BARKER

**Senior Principal Integration Engineer
from Puppet**

Forward-Looking Statements

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 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.

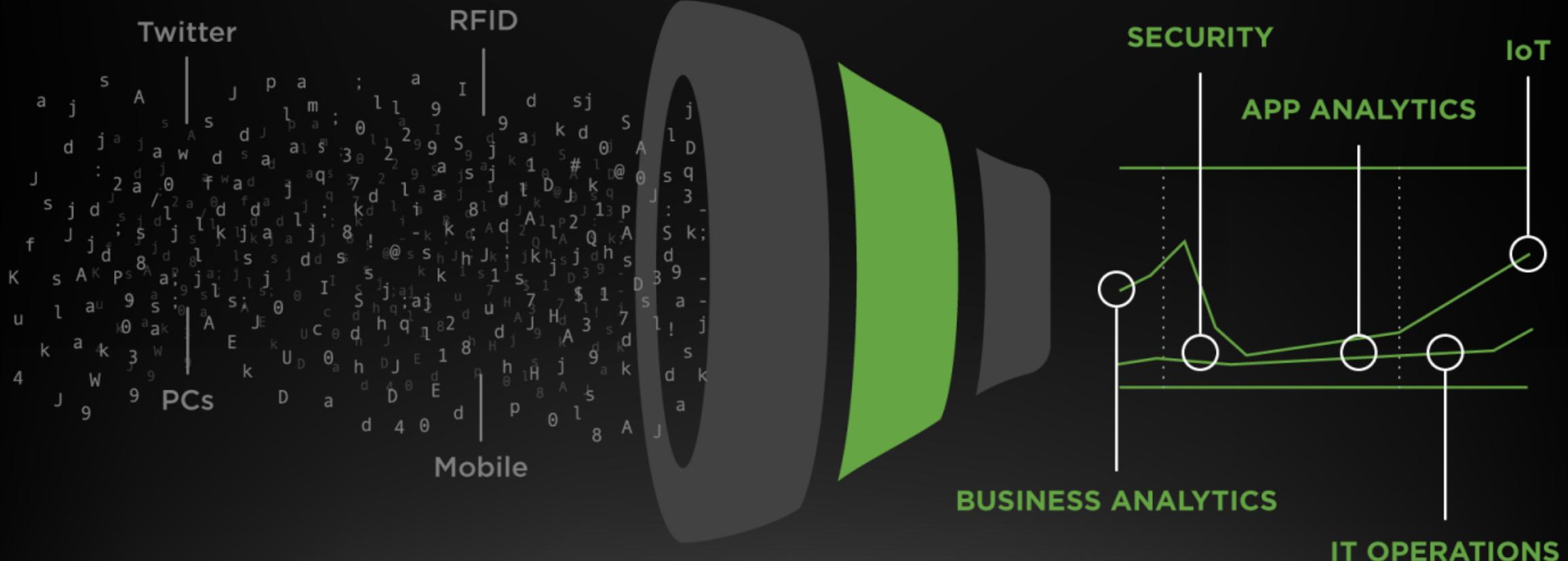
Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

What is Splunk ?

Quick Intro Into the Machine Data Fabric



Splunk Turns Machine Data Into Answers.



Why Splunk ?



FAST TIME-TO-VALUE



VISIBILITY ACROSS STACK--NO SILOS

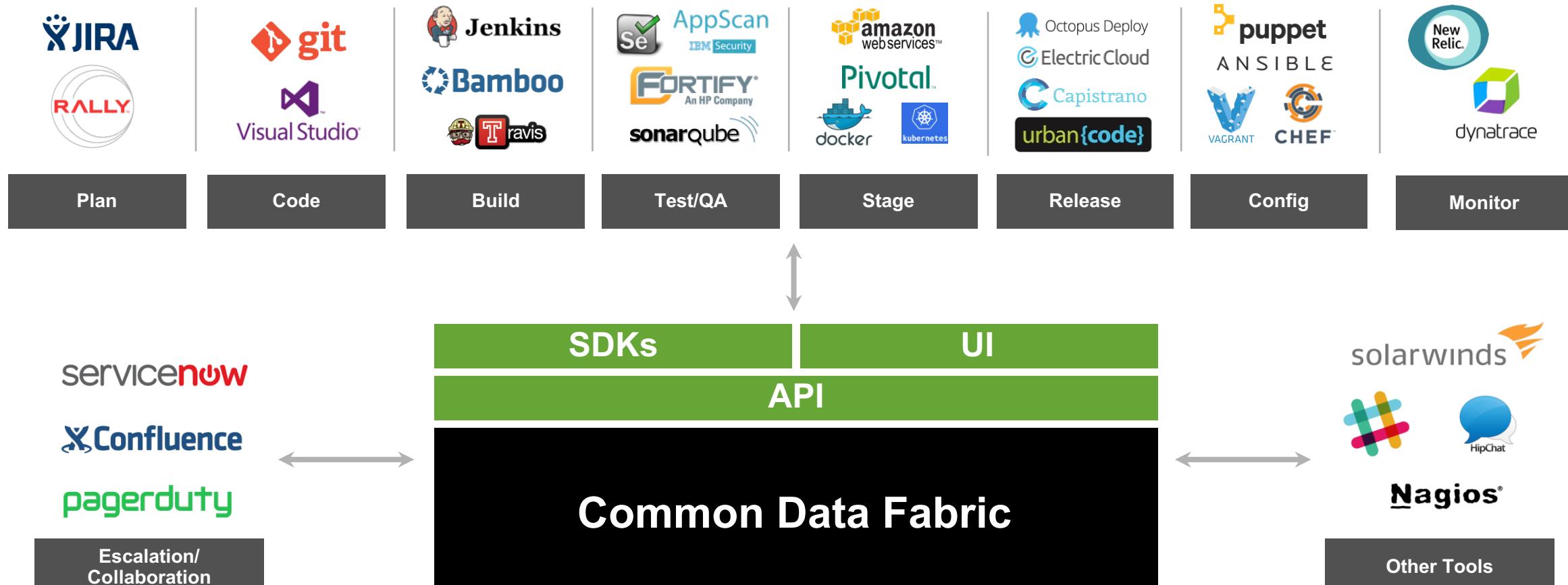
ASK ANY QUESTION OF DATA

ANY DATA, ANY SOURCE



138.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-0&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317.27.160.0.0 - - [07/Jan 18:10:57:156] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 332@ "http://buttercup-shopping.com/cart.do?action=putInCart&itemId=EST-26&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468.125.17.14.10.27.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15LAFF10ADFF10 HTTP 1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-0&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 4318@ "http://buttercup-shopping.com/cart.do?action=changeQuantity&itemId=EST-18&product_id=AFC-CB18-SESSION-ID-SD55L9FF1ADFF3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.142 Safari/537.36" 1891.19.55.1871 "GET /oldlink?item_id=EST-6&JSESSIONID=SD15L8BF2ADFF4 HTTP 1.1" 200 3865@ "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.142 Safari/537.36" 10.27.241.220.82 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 4318@ "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-26&product_id=F1-SW-01" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"

The Dev Lifecycle is Complex



Splunk Solutions

Splunk Premium Solutions



Splunk IT Service
Intelligence™



Splunk Enterprise
Security™



Splunk User Behavior
Analytics™

1,000+ Apps and Add-Ons



splunk>enterprise

splunk>cloud™

splunk> Platform for Operational Intelligence

splunk>.conf18

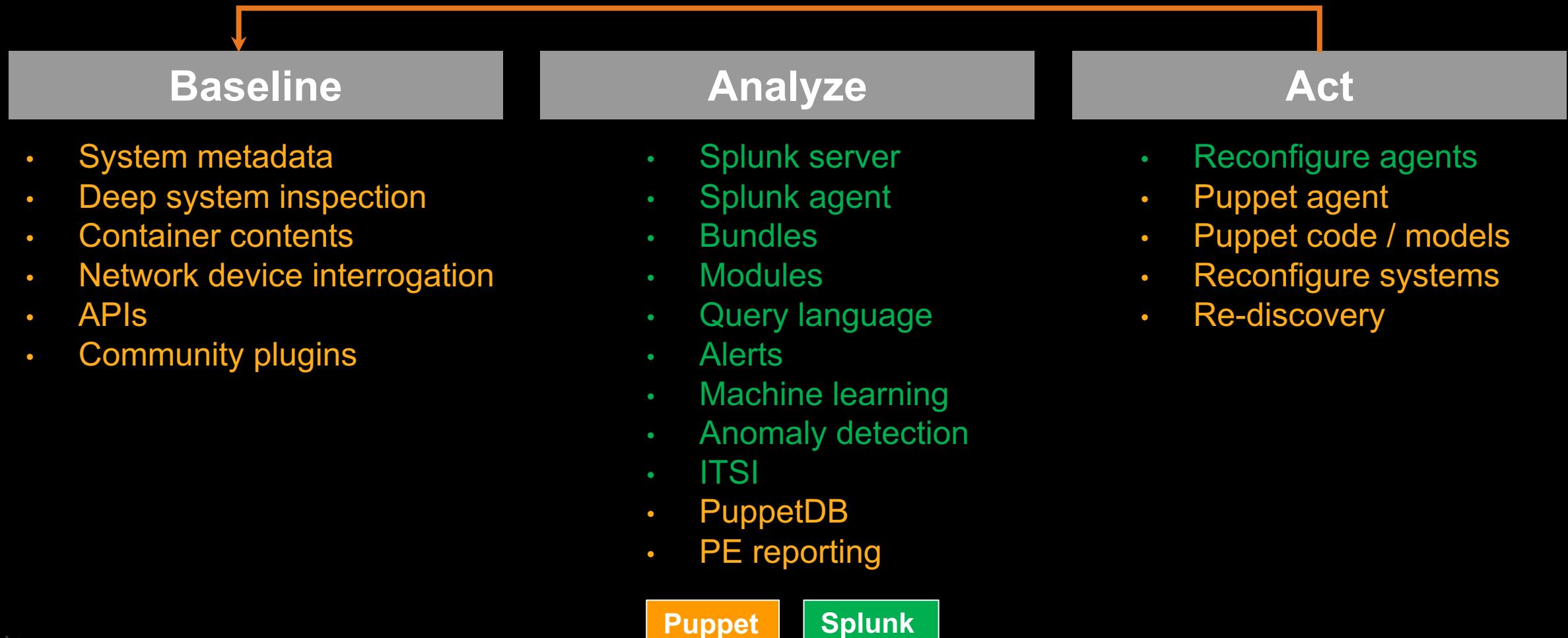
Baseline → Analyze → Act

(if you remember only one **thing** from this talk, this is that **thing**)

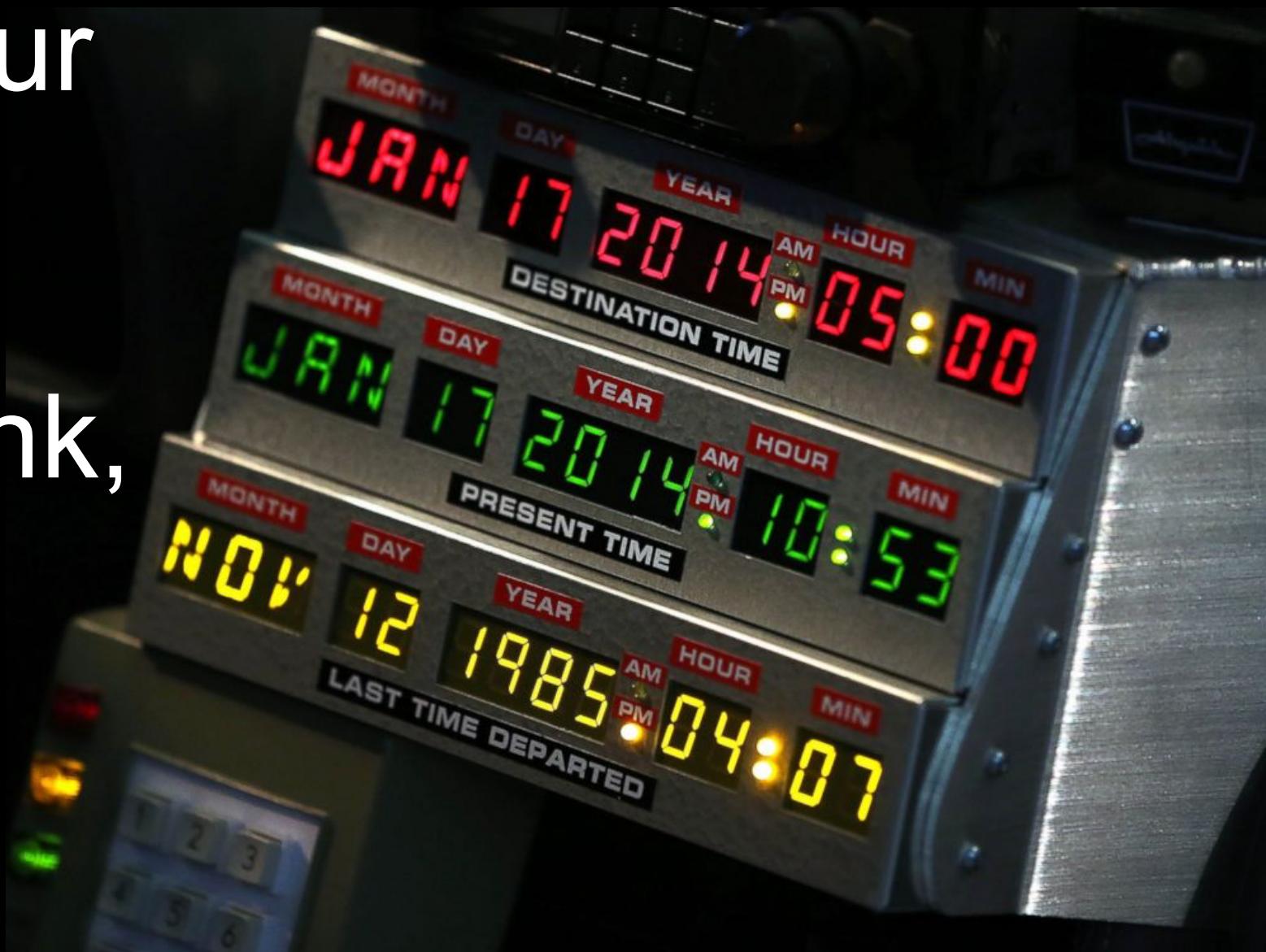


Using Puppet and Splunk
independently is good.
But using them together
is great!

Splunk + Puppet Complementary Capabilities



Connect all your systems, past, present, and future, to Splunk, automatically!



But that's just the beginning
of a long list of possibilities!

Demo

Integrations and Technology Preview

splunk> .conf18

Splunk App and Add-On for Puppet Enterprise

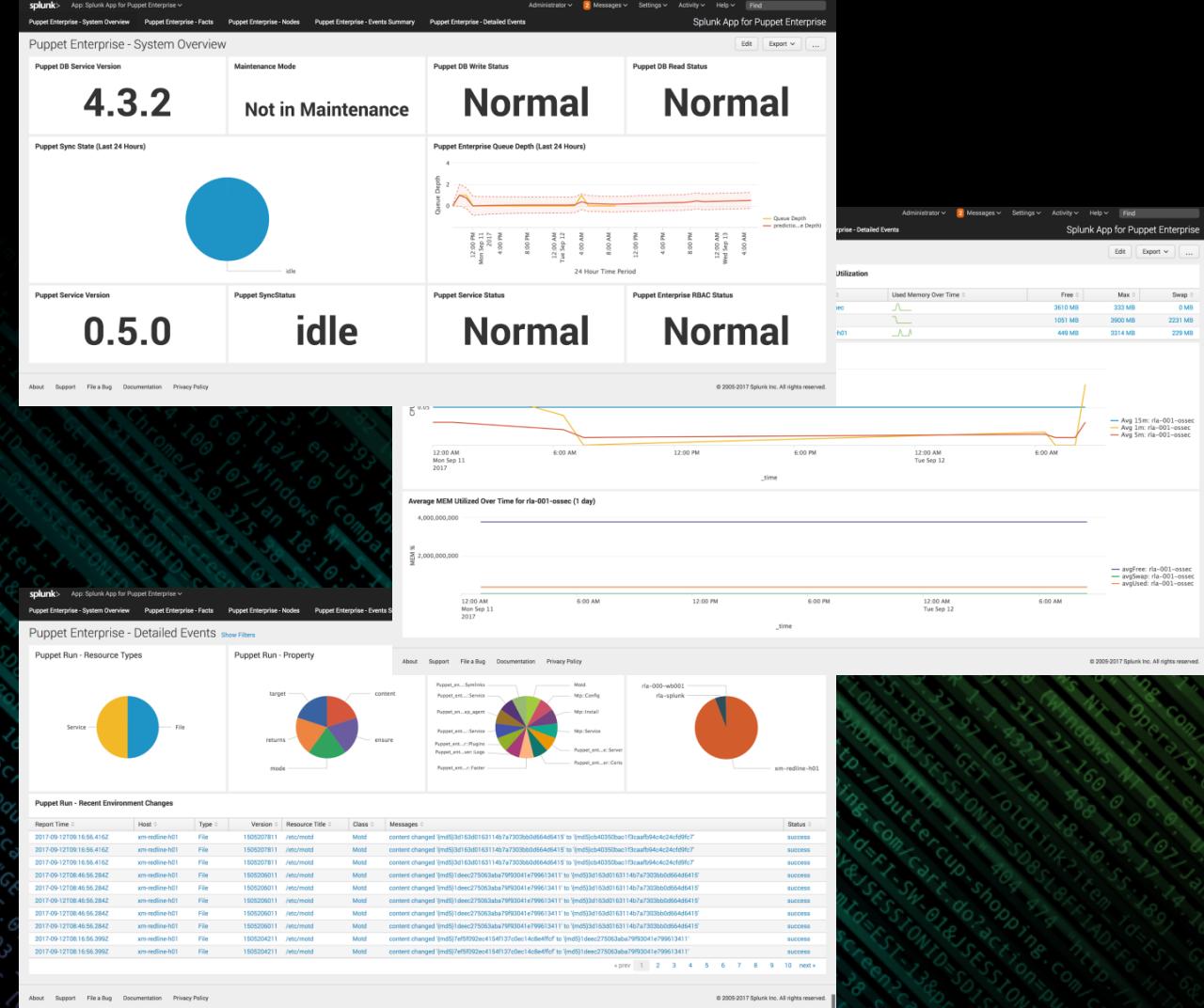
Overview and Demo

Splunk App for Puppet Enterprise

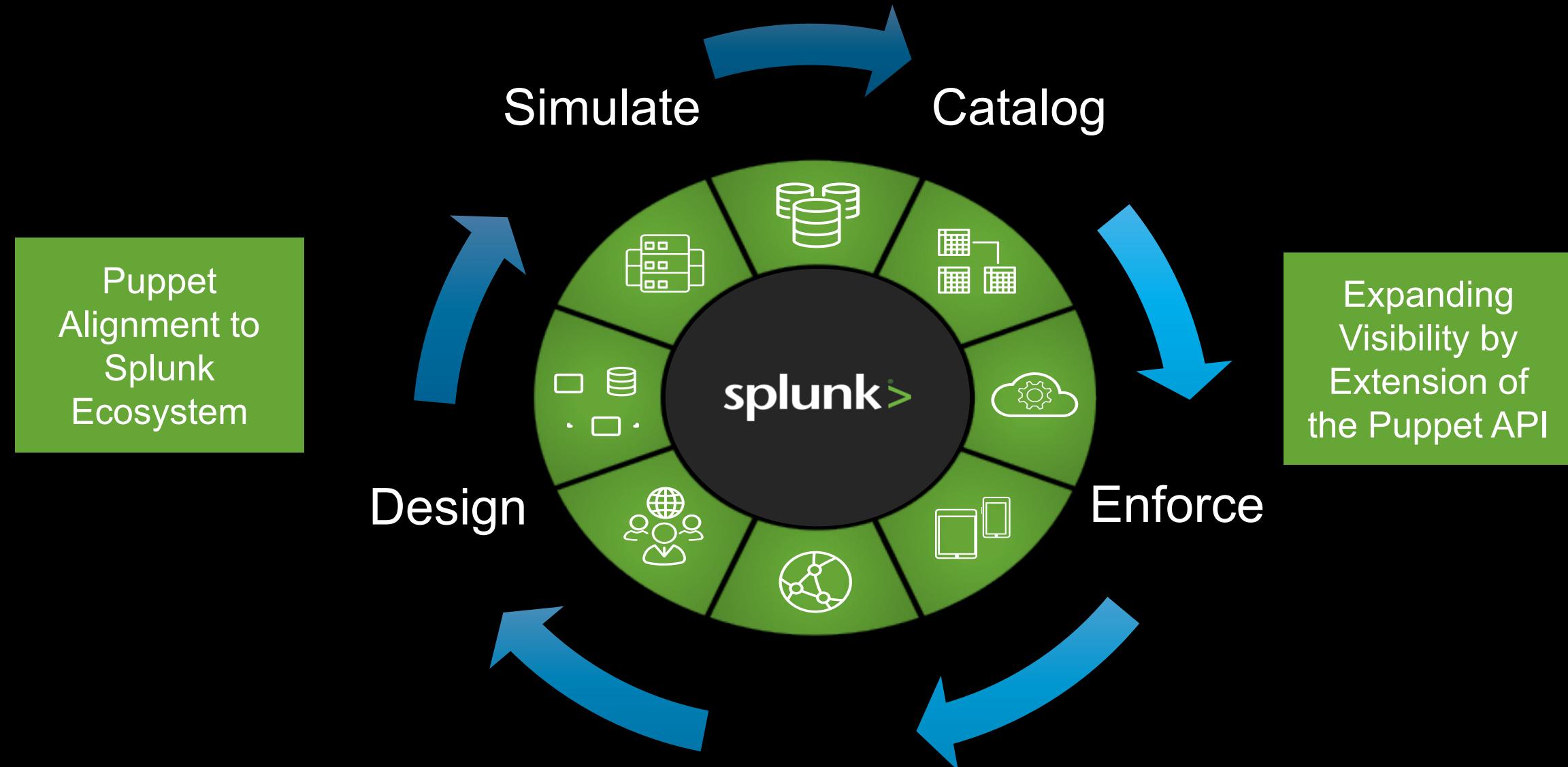
Discover and monitor the health of all resources under management

Ingest all data from Puppet Enterprise and correlate that data across your entire tech stack

Visualize your Puppet data with out of the box dashboards for easy troubleshooting



Current Discussion and Integration



Puppet Tasks for Splunk

Integration Guide

Puppet Task via Bolt: Commands

Basic Use Case: Disk space on Linux server exceeds 90%. Instead of logging into the server to clear disk space, let chain a few commands together to clear the space on a specific servers when Splunk registers 90% utilization.

Splunk Search for Alerts: sourcetype=df | multikv | dedup host,Filesystem | search MountedOn="/mnt/sansmount" | rex field=UsePct "(?<usage>\d+)" | where usage>90 | eval _raw="Filesystem "+Filesystem+" (mount point "+MountedOn+) on host "+host+ " is "+UsePct+" full!" | fields - *

When triggered	 Puppet Tasks - Command	<input type="button" value="Remove"/>
	Type of <input checked="" type="radio"/> Command Operating System <input type="radio"/> Windows <input checked="" type="radio"/> Linux Runtime <input checked="" type="radio"/> Run Node Names * <input type="text"/> Command * <input type="text"/> 'echo " > /var/log/message'	Puppet Execution Method for Puppet Bolt. Select your operating system to run Puppet bolt on the host machine. Pick your execution method for Puppet Bolt. Nodes to run Tasks on Puppet Bolt. Example: web01, web02, web03, web04 Type in your task execution. Example: 'echo " > /var/log/message'

Puppet Tasks Command:

Splunk triggers Puppet Bolt through Puppet Tasks for Splunk. Admin sets command, operating system and runtime. Types out nodes and command.

Execution:

'echo " > /var/log/message && echo " > /var/log/nginx/access.log'

Puppet Task via Bolt: Plans

Basic Use Case: Disk space on Linux server exceeds 90%. Instead of logging into the server to clear disk space, let chain a few commands together to clear the space on a specific servers when Splunk registers 90% utilization.

Splunk Search for Alerts: sourcetype=df | multikv | dedup host,Filesystem | search MountedOn="/mnt/sansmount" | rex field=UsePct "(?\d+)" | where usage>90 | eval _raw="Filesystem "+Filesystem+" (mount point "+MountedOn+) on host "+host+ " is "+UsePct+" full!" | fields - *

When triggered

▼

 Puppet Tasks - Plans Remove

Type of	<input checked="" type="radio"/> Plan	Puppet Execution Method for Puppet Bolt. Select your operating system to run Puppet bolt on the host machine.
Operating System	<input type="radio"/> Windows <input checked="" type="radio"/> Linux	
Runtime	<input checked="" type="radio"/> Run	Pick your execution method for Puppet Bolt.
Node Name *	<input type="text"/>	
Execution *	<input type="text"/>	

Puppet Tasks Command:

Splunk triggers Puppet Bolt through Puppet Tasks for Splunk. Admin sets command, operating system and runtime. Types out nodes and plan name.

Execution:

"webserver::cleanupmess"

Puppet Task via Bolt: Tasks

Basic Use Case: Disk space on Linux server exceeds 90%. Instead of logging into the server to clear disk space, let chain a few commands together to clear the space on a specific servers when Splunk registers 90% utilization.

Splunk Search for Alerts: sourcetype=df | multikv | dedup host,Filesystem | search MountedOn="/mnt/sansmount" | rex field=UsePct "(?\d+)" | where usage>90 | eval _raw="Filesystem "+Filesystem+" (mount point "+MountedOn+) on host "+host+ " is "+UsePct+" full!" | fields - *

When triggered

Puppet Tasks - Task

Type of Tasks

Operating System Windows Linux

Runtime Run

Noop

Node Names *

Task Execution *

Puppet Execution Method for Puppet Bolt.
Select your operating system to run Puppet bolt on the host machine.

Pick your execution method for Puppet Bolt.
Noop run of Puppet Tasks on Bolt.

Nodes to run Tasks on Puppet Bolt. Example: web01, web02, web03, web04
Type in your task execution.
Example: package name=vim action=install

Remove

Puppet Tasks Command:

Splunk triggers Puppet Bolt through Puppet Tasks for Splunk. Admin sets command, operating system and runtime. Types out nodes and plan name.

Execution:
webserver::logs::cleanup

Puppet Discovery for Splunk

Technology Preview

Puppet Discovery for Splunk

splunk>enterprise App: Puppet Discovery for Splunk ▾

Puppet Discovery Topology Mapping Search

Puppet Discovery for Splunk

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Puppet Discovery Topology Mapping

All time

Search by ID or name.

Virtual Network (2) ✓
 Instance (7) ✓
 Subnet (2) ✓
 Volume (0)
 Security Group (0)
 Network Interface (4)

```

graph TD
    DN[default-us-central1-a] --- GKE1[gke-gke-cluster...]
    DN --- GKE2[gke-gke-cluster...]
    DN --- GKE3[gke-gke-cluster...]
    DN --- GKE4[gke-gke-cluster...]
    DN --- GKE5[gke-gke-cluster...]
    GKE1 --- GKE2
    GKE1 --- GKE3
    GKE1 --- GKE4
    GKE1 --- GKE5
    GKE2 --- GKE3
    GKE2 --- GKE4
    GKE2 --- GKE5
    GKE3 --- GKE4
    GKE3 --- GKE5
    GKE4 --- GKE5
    GKE4 --- CLOUD[default]
    GKE5 --- CLOUD
  
```

Edit Export ...

splunk>enterprise App: Puppet Discovery for Splunk ▾

H Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Search

Puppet Discovery Topology Mapping Search

Puppet Discovery Topology Mapping

All time

Search by ID or name.

- > Virtual Network (2)
- > Instance (7)
- > Subnet (2)
- Volume (0)
- Security Group (0)
- Network Interface (4)

gke-gke-cluster-01-default-pool-2006b73e-f7xm

Brief

Relationship

Subnet :

- subnet-default-us-central1-a (default-us-central1-a)

Usage

gke-gke-cluster... subnet-default-us-central1-a

default-us-centr...

splunk> .conf18

Taking you from zero to hero with Baseline, Analyze and Act

“Q&A”

Thank You

Don't forget to rate this session
in the .conf18 mobile app

