How to Build a Secure DevOps Environment for the Government

@Normalfaults
#Dockercon

GSA Booz | Allen | Hamilton
100 YEARS

dockercon 15

SF JUNE 22-23

Using Docker to Drive Transformation for General Services Administration (GSA) - Integrated Award Environment (IAE)

- The current application development cycle is very long and cumbersome due to large monolithic application stacks

- The new IAE Common Service Platform (CSP) focuses on building business specific applications that is abstracted from the platform

- Booz Allen is using docker to drive abstraction between business specific applications and the platform

- Specific numbers of repeated VMs in each current application

- The solution eliminates configuration drift, and reduces attack surface area from developers

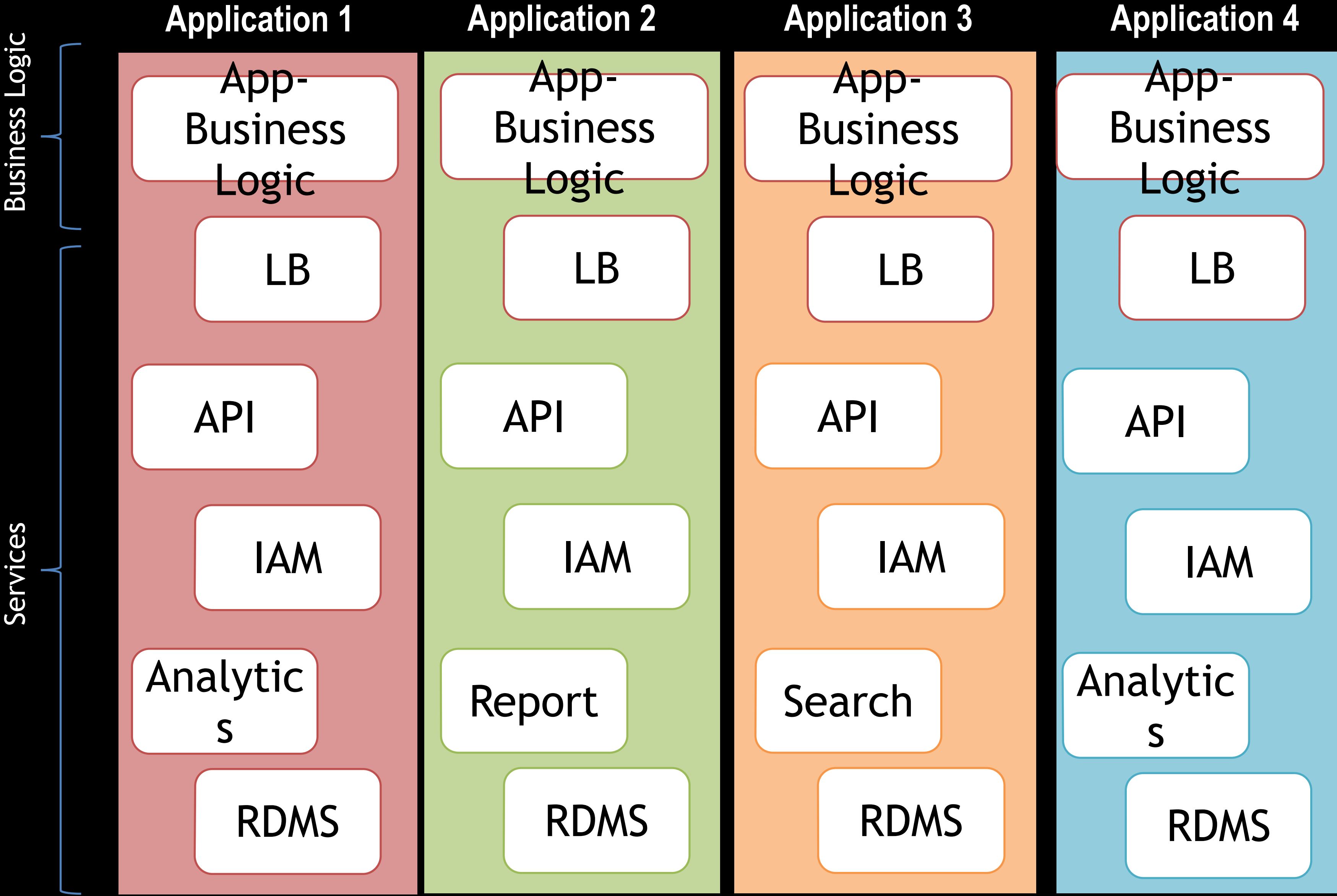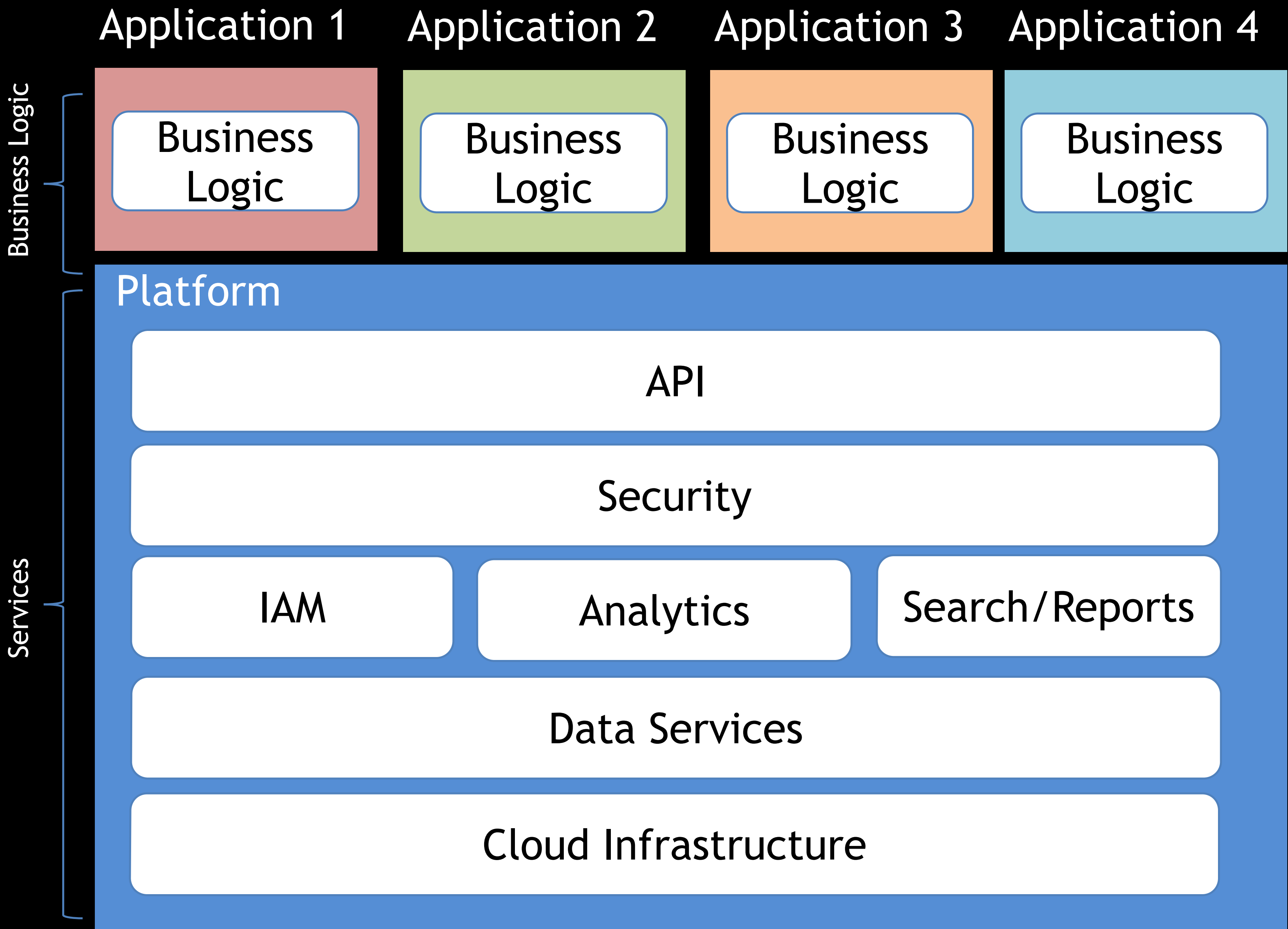**Navin Vembar
Director of the GSA
IAE**

Current State – Monolithic, Stand alone application

The current IAE environment has 10 Free-standing web-based systems Running in silos and different environments

Business Logic

Application 1
- App-Business Logic

Application 2
- App-Business Logic

Application 3
- App-Business Logic

Application 4
- App-Business Logic

Services

Application 1
- LB
- API
- IAM
- Analytics
- RDMS

Application 2
- LB
- API
- IAM
- Report
- RDMS

Application 3
- LB
- API
- IAM
- Search
- RDMS

Application 4
- LB
- API
- IAM
- Analytics
- RDMS

Target State – Business focused abstracted from the common platform

The CSP will provide the foundational capability upon which the future IAE Core Applications will be developed
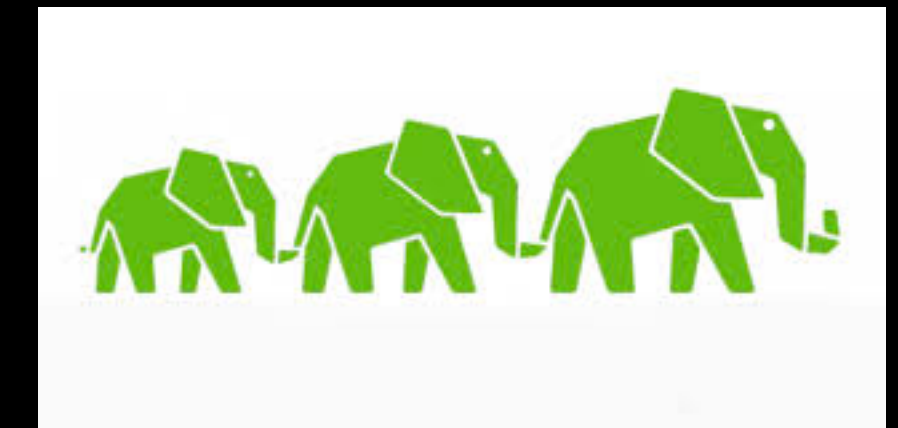
Application 1   Application 2   Application 3   Application 4

Business Logic

| Business Logic | Business Logic | Business Logic | Business Logic |

Platform

Services

API

Security

| IAM | Analytics | Search/Reports |

Data Services

Cloud Infrastructure

Partners and Technologies

Together driving innovation forward

Booz | Allen | Hamilton

docker

amazon web services™

CHEF

redhat LINUX

GitHub

mongoDB

hadoop

tableau SOFTWARE

sensu

HIVE

Demo Flow
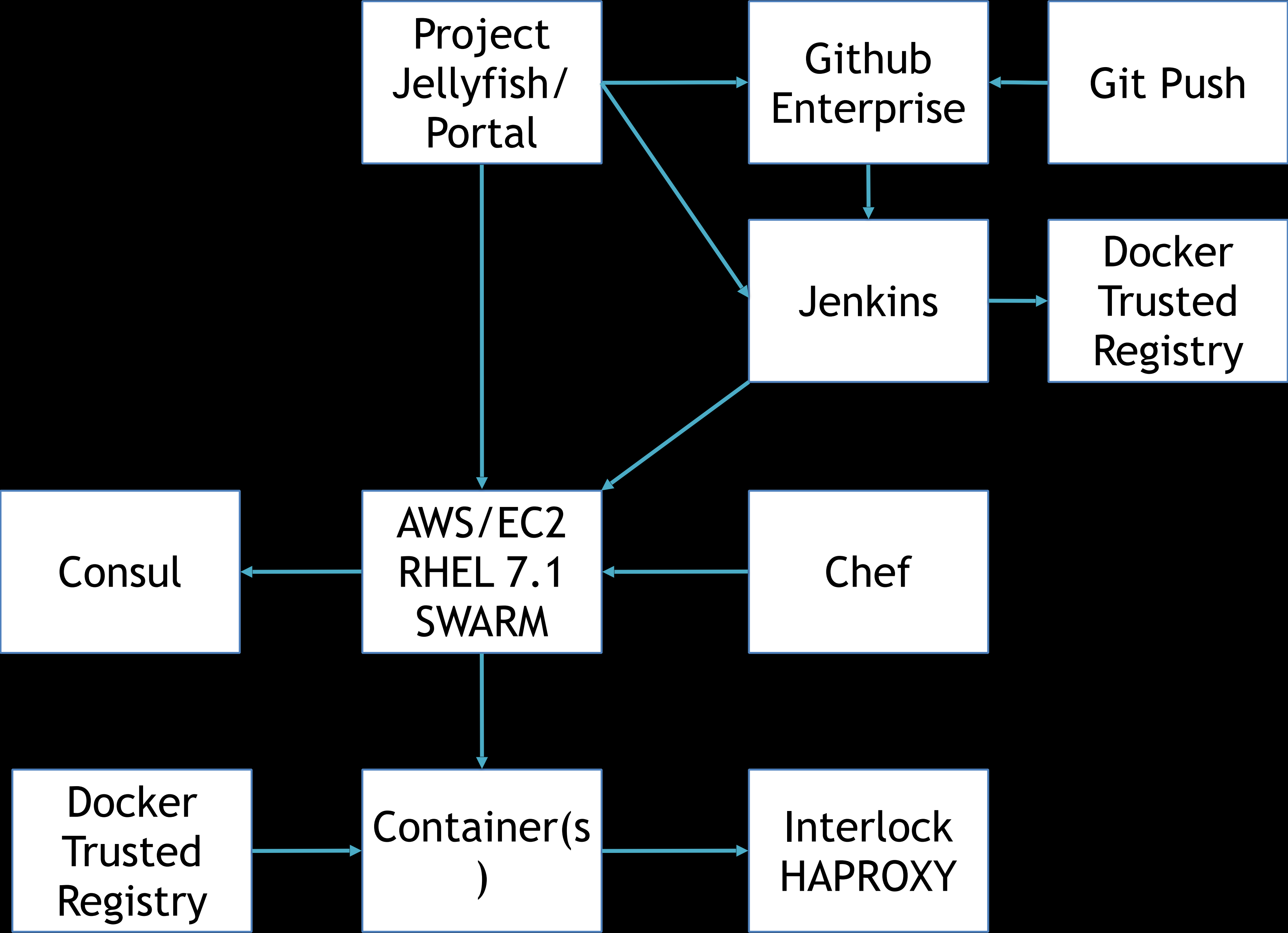
Benefits

- Improved customer-centric services
- Increased time-to-market
- Reduced cost
- Creates opportunities for new business
- Target state of 2 week production sprints for platform and new applications
- Decrease time for security review

Lessons Learned

- Docker Bench CIS to ensure secure dockerhost baseline
- Keep environment simple and build up with ingredients (Swarm, Machine, Compose)
- Simplifying Security Process by focus on building small base images
- Automated Certificate management for TLS is still a challenge (machine)
- Rolling container updates on hosts

Open Source

http://gsa.github.io/openIAE/

Next Steps

- Image Governance through provenance
- Inserting secrets in containers with Keywhiz - https://square.github.io/keywhiz/
- Check out DIOGO MÓNICA and NATHAN MCCAULEY Dockercon talks
- Container Networking

Links

- GSA IAE http://gsa.github.io/openIAE/
- Interlock - https://github.com/ehazlett/interlock
- Conduit - https://github.com/ehazlett/conduit
- Consul.io - https://www.consul.io/
- Project Jellyfish – https://projectjellyfish.org
- Umbrella API – http://apiumbrella.io
- Bot.io – Booz Allen Open Tech

Thanks!

Nirmal Mehta
mehta_nirmal@bah.com
Github/Twitter: @normalfaults
projectjellyfish.org
bot.io
#Dockercon

dockercon 15