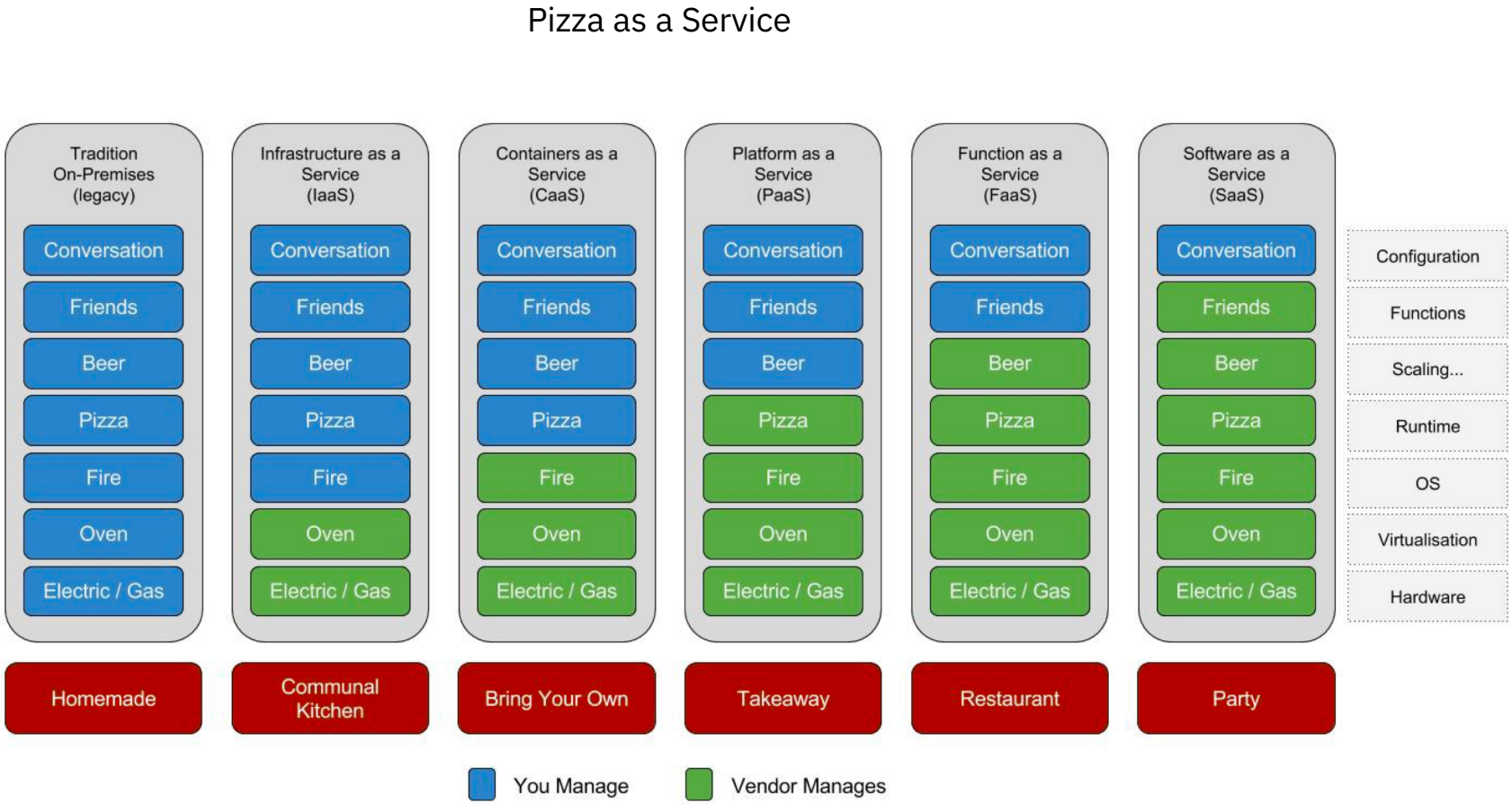
IBM Cloud Private and Secure Service Containers

Elton de Souza
Chief Architect,
LinuxONE Innovation Lab
z Cloud Innovation Lab

Topics

Linux on z Ecosystem
IBM Cloud Private (ICP)
- Building a cross-platform private cloud + demo
- Cross-platform DevOps + demo
- Automated Monolith -> Microservice conversion + demo
- Secure Service Containers
- zOS Cloud Broker + demo

Cloud Models



A Rich Open Ecosystem Offering Greater Flexibility & Choice

Canonical unveils 6th LTS release of Ubuntu with 16.04

For the latest view of packages, see URL

THE LINUX FOUNDATION

OPEN MAINFRAME PROJECT

https://hub.docker.com/search/?isAutomated=0&isOfficial=0&page=1&pullCount=0&q=s390x&starCount=0

https://store.docker.com/search?architecture=s390x&source=verified&type=image

Solution Overview – IBM Cloud Private
… to enable enterprises to both innovate & optimize

A platform located **behind your firewall**.

Enterprise Content Catalog
Open Source and IBM Middleware, Data, Analytics, and AI Software

Core Operational Services
Log Management, Monitoring, Security, Alerting

Kubernetes Container Orchestration Platform

kubernetes

docker

Choose your infrastructure:

vmware · intel · openstack · IBM Spectrum · IBM LinuxONE · IBM Z · Power Systems

Strategic Value:

Self-service catalog

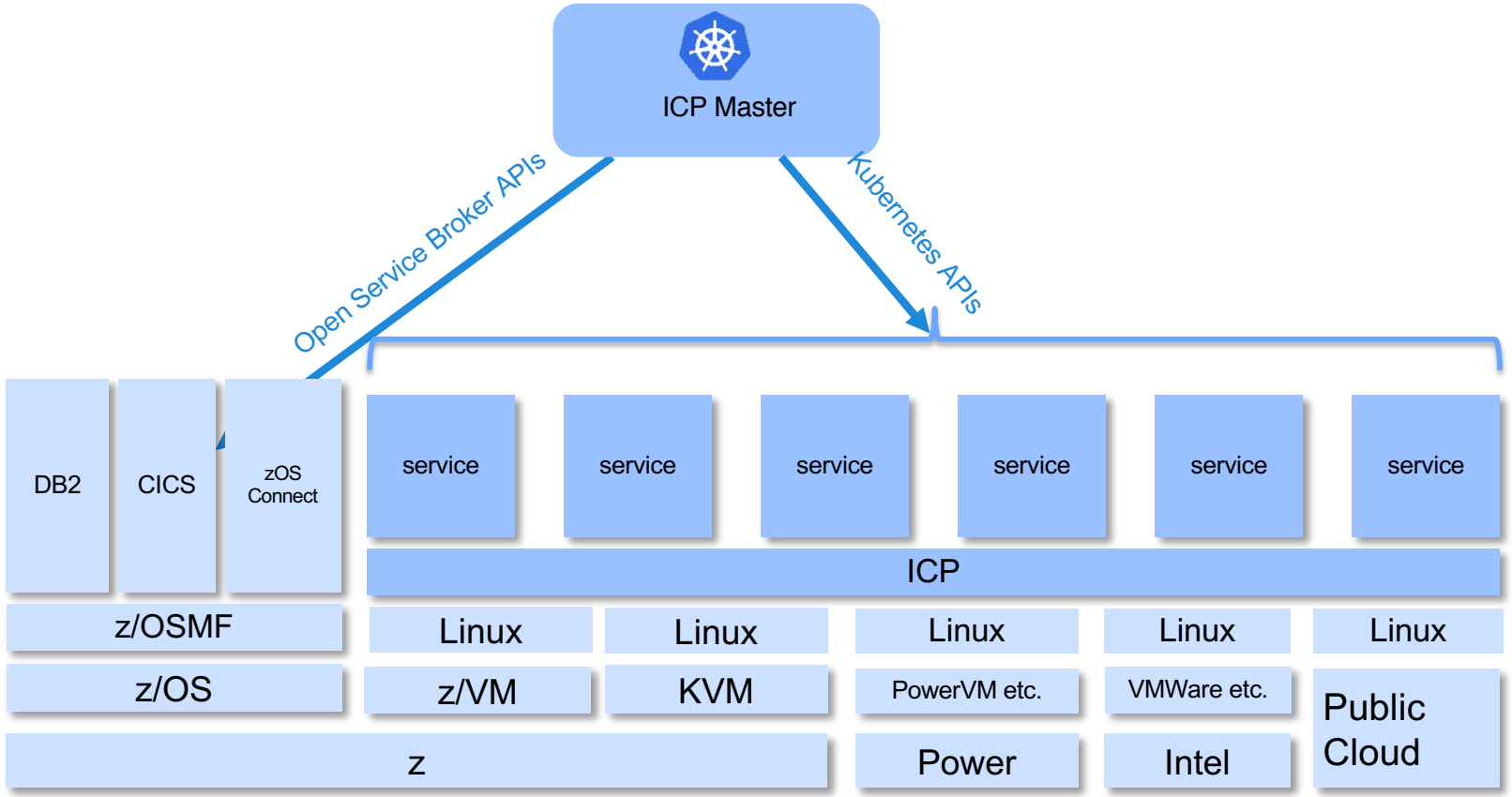
Agility, scalability, and elasticity

Self-healing

Enterprise security

No vendor lock-in

A heterogeneous environment across Intel, Power, z and public cloud



Content on ICP on Z (container based)

ICP Components

Transformation Advisor
Microclimate (2H)
Cloud Automation Mgr
Vulnerability Advisor
Mutation Advisor
MCM: manage-to-Z (2Q)
Spectrum Connect
Spectrum Scale
IBM Istio

Open Source

Jenkins (NA for OSS)?
Open Liberty
Node.js
Swift Runtime
Nginx
RabbitMQ
Kibana (non-logging)
Kafka

Data Services for Apps:
MongoDB CE
MongoDB EE (tbc)
Postgres CE
Postgres EE (tbc)
Redis CE
Maria DB CE

Data Serving for Apps:

Db2 OLTP
Db2 with data server mgr (DSM)
DB2 Warehouse (SMT, MMT)

Integration / AppMod Solution:

MQ Advanced
WebSphere Liberty
IBM IIB V10 (for PoC only)
App Connect Enterprise (2H'19)
Mobile First ()
Urban Code Deploy

Automation:

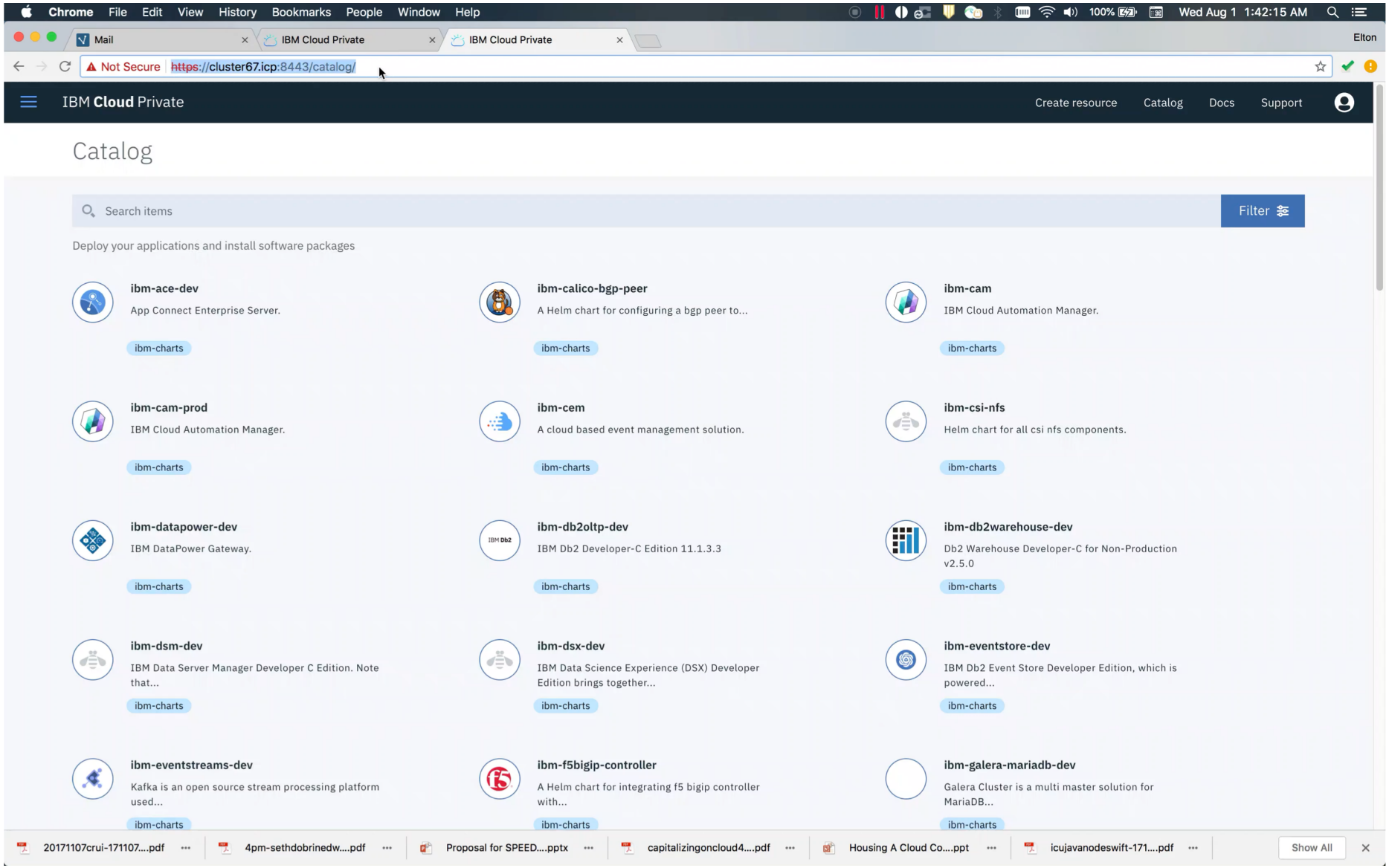
Digital Bus. Automation (tbc)
(workflow + BPM)
IBM Op. Decision Manager (ODM)
Event Stream Dev / Prod

Cloud Automation Manager allows *ANY* VM based workload on ICP

Color Key:
Green: Available
Blue: On the Roadmap

Roadmap includes Commercial Editions available for purchase unless otherwise noted as (i.e. open source)
Catalog content is not distributed with IBM Cloud Private. Content is distributed separately, licensed under separate terms and conditions.

IBM Cloud Private **Demo**


Chrome File Edit View History Bookmarks People Window Help
Wed Aug 1 1:42:15 AM
Mail
IBM Cloud Private
IBM Cloud Private
Elton
Not Secure
https://cluster67.icp:8443/catalog/
IBM Cloud Private
Create resource
Catalog
Docs
Support
Catalog
Search items
Filter
Deploy your applications and install software packages
ibm-ace-dev
App Connect Enterprise Server.
ibm-charts
ibm-calico-bgp-peer
A Helm chart for configuring a bgp peer to...
ibm-charts
ibm-cam
IBM Cloud Automation Manager.
ibm-charts
ibm-cam-prod
IBM Cloud Automation Manager.
ibm-charts
ibm-cem
A cloud based event management solution.
ibm-charts
ibm-csi-nfs
Helm chart for all csi nfs components.
ibm-charts
ibm-datapower-dev
IBM DataPower Gateway.
ibm-charts
ibm-db2oltp-dev
IBM Db2 Developer-C Edition 11.1.3.3
ibm-charts
ibm-db2warehouse-dev
Db2 Warehouse Developer-C for Non-Production v2.5.0
ibm-charts
ibm-dsm-dev
IBM Data Server Manager Developer C Edition. Note that...
ibm-charts
ibm-dsx-dev
IBM Data Science Experience (DSX) Developer Edition brings together...
ibm-charts
ibm-eventstore-dev
IBM Db2 Event Store Developer Edition, which is powered...
ibm-charts
ibm-eventstreams-dev
Kafka is an open source stream processing platform used...
ibm-charts
ibm-f5bigip-controller
A Helm chart for integrating f5 bigip controller with...
ibm-charts
ibm-galera-mariadb-dev
Galera Cluster is a multi master solution for MariaDB...
ibm-charts
20171107crui-171107....pdf
4pm-sethdobrinedw....pdf
Proposal for SPEED....pptx
capitalizingoncloud4....pdf
Housing A Cloud Co....ppt
icujavanodeswift-171....pdf
Show All

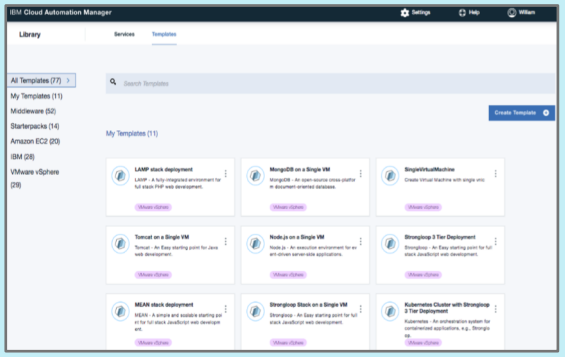
Tools for App Modernization

Transformation Advisor

Assess & Manage traditional apps; **Expose**, **Refactor**, Shift, Extend

Microclimate

Closed loop **CI/CD pipeline** with ability to hook to existing tools



Cloud Automation Manager

Multi-Cloud Provisioning
Deploy **VM based workloads**

IBM Transformation Advisor

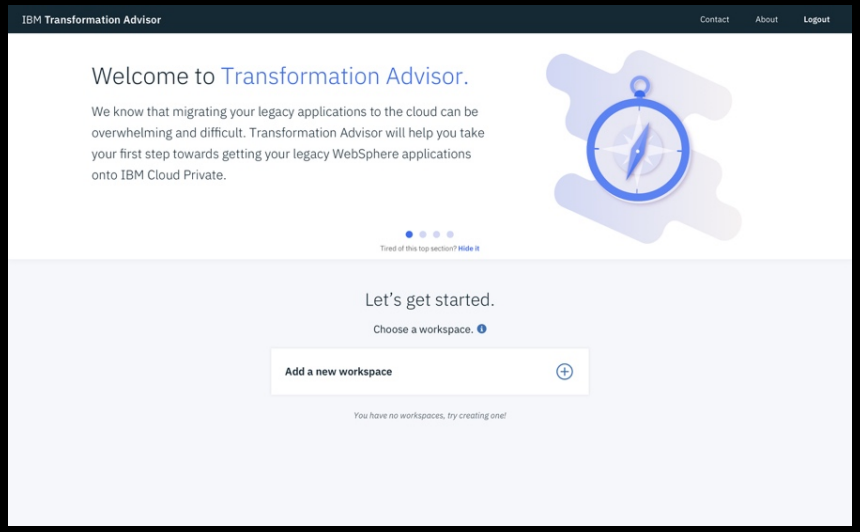
Transformation Advisor is a tool that **consumes information about your WebSphere Environment and Applications.** These inputs are combined with rules and insights gained from years of working with WebSphere and WebSphere applications to provide recommendations for your cloud journey.

CHALLENGES

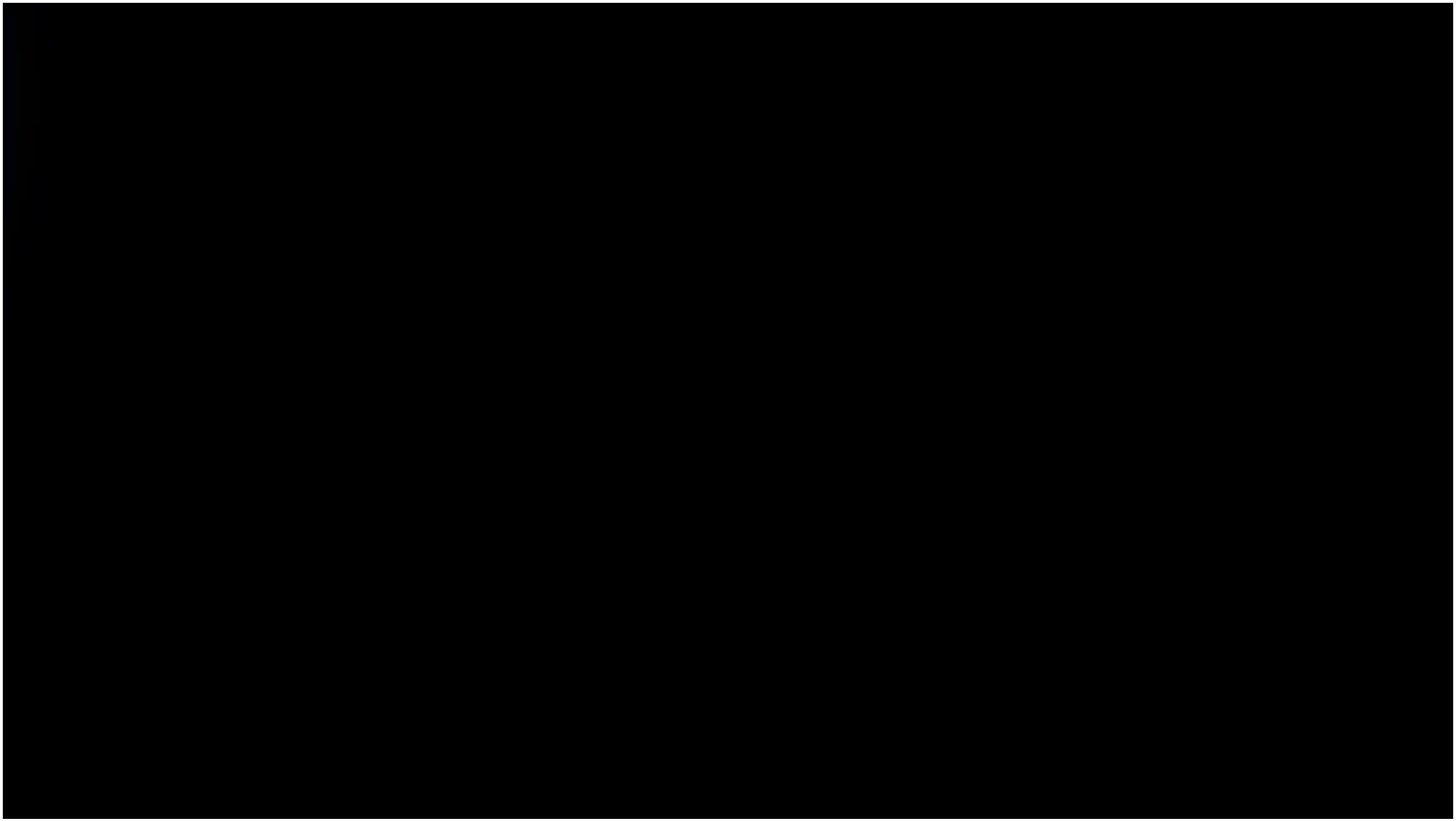
Leverage existing application logic
Need to accelerate application development and maintenance
Monolithic applications that are complex and brittle

BENEFITS

Included and deployed on IBM Cloud Private
Introspects existing WebSphere Deployments
THE source of truth
Provides recommendations for Application Modernization



Transformation Advisor **Demo**



Cloud Automation Manager

- Brings Oracle and other **non-containerizable workloads** (WAS-ND, in house monoliths etc.) to hybrid cloud
- Deploy/manage your existing VM workloads (ami, vmdk etc)
- Based on Terraform so supports all Terraform providers
  - **VMWare**
  - **zVM CMA** or alternative OpenStack implementation APIs on z
  - Azure, GCE, AWS are first class ICP citizens
  - + 75 other integration options (including all Public Cloud IaaS)

IBM Cloud
Automation Manager

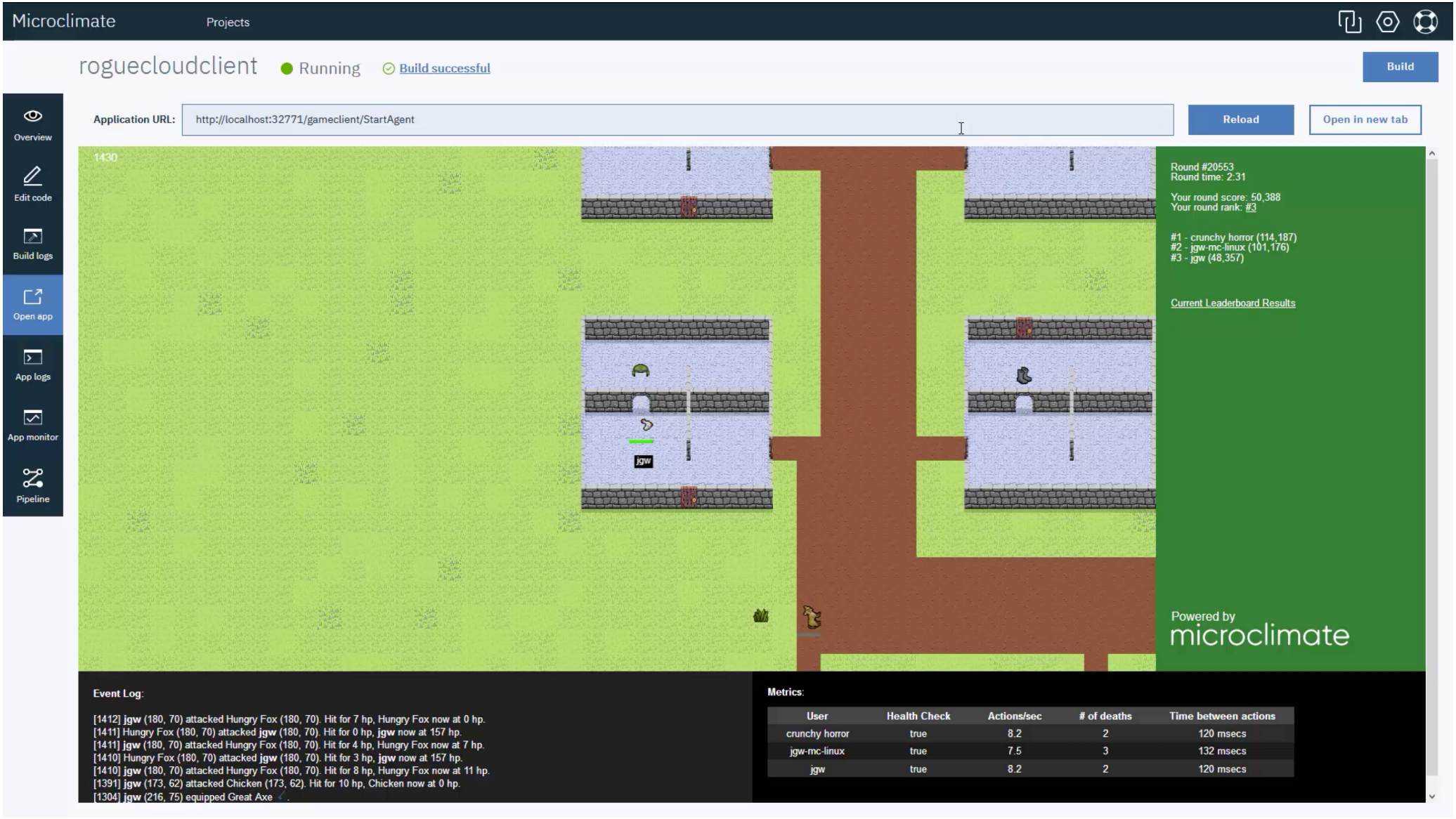
IBM Cloud Automation Manager **Demo**

Deploy MEAN with IBM Cloud Automation to AWS and IBM Cloud
- app in AWS
- mongodb in IBM Cloud

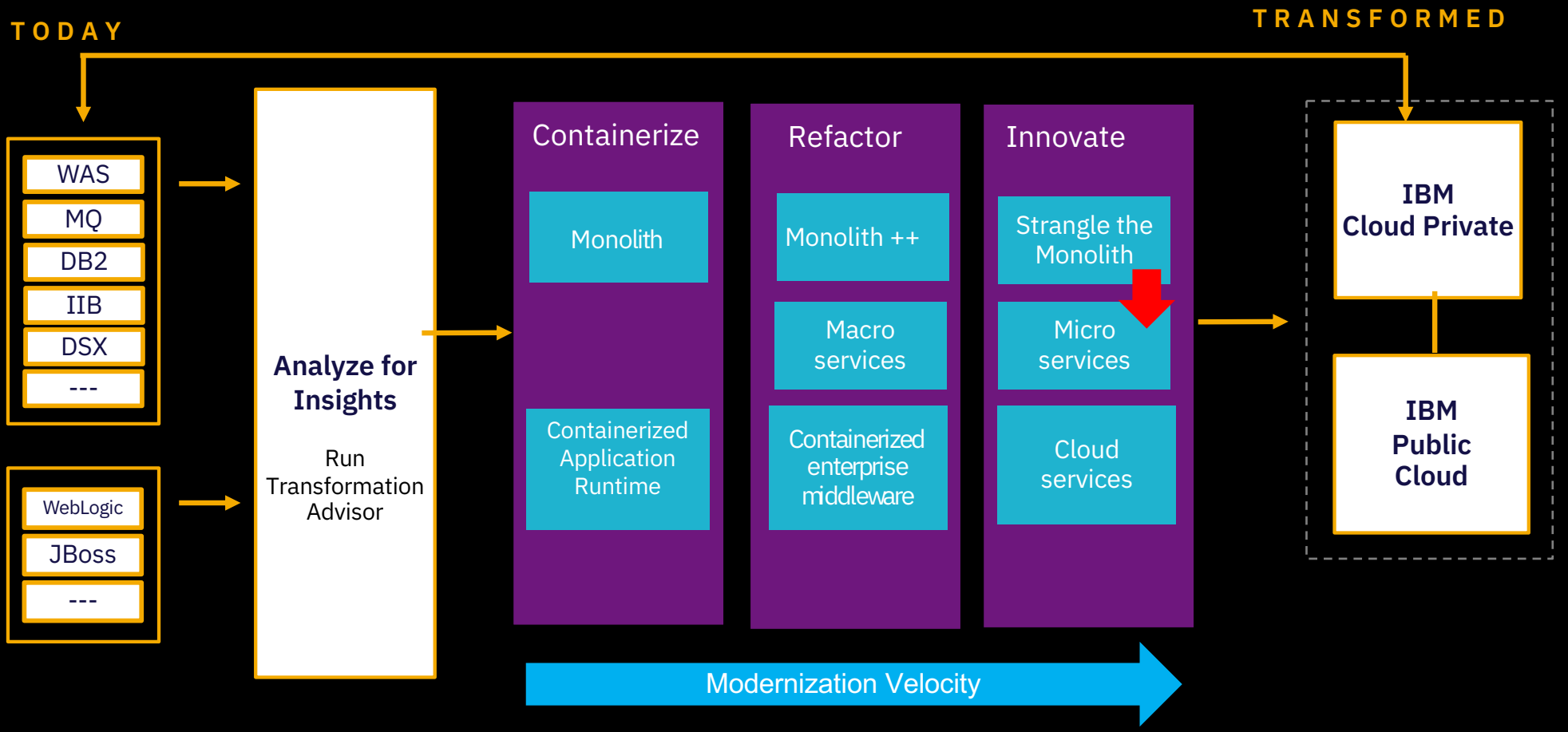
IBM Microclimate

Microclimate is an **end to end development environment that lets you rapidly create, edit, and deploy applications.** Applications are run in **containers** from day one and can be delivered into production on **Kubernetes** through an automated DevOps pipeline using **Jenkins**. Microclimate can be installed locally or on **IBM Cloud Private.**

Microclimate **Demo**

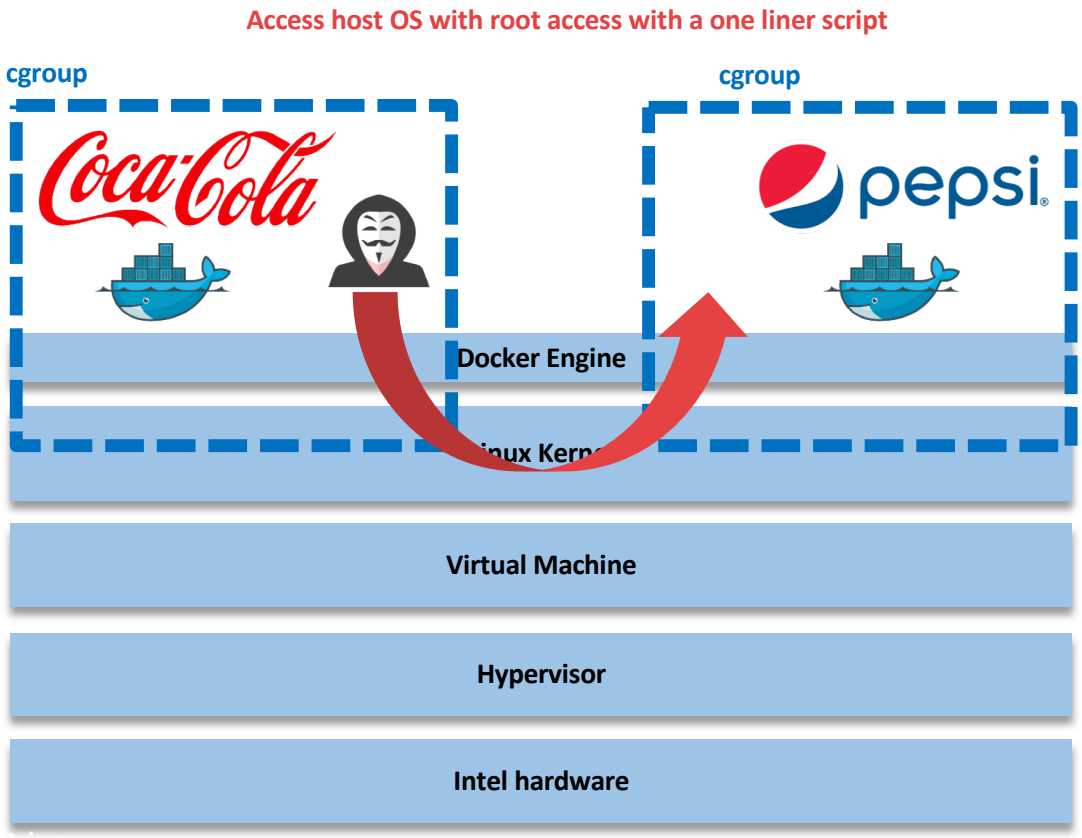

Microclimate
Projects
roguecloudclient
Running
Build successful
Build
Overview
Edit code
Build logs
Open app
App logs
App monitor
Pipeline
Application URL:
http://localhost:32771/gameclient/StartAgent
Reload
Open in new tab
1430
jgw
Round #20553
Round time: 2:31
Your round score: 50,388
Your round rank: #3
#1 - crunchy horror (114,187)
#2 - jgw-mc-linux (101,176)
#3 - jgw (48,357)
Current Leaderboard Results
Powered by
microclimate
Event Log:
[1412] jgw (180, 70) attacked Hungry Fox (180, 70). Hit for 7 hp, Hungry Fox now at 0 hp.
[1411] Hungry Fox (180, 70) attacked jgw (180, 70). Hit for 0 hp, jgw now at 157 hp.
[1411] jgw (180, 70) attacked Hungry Fox (180, 70). Hit for 4 hp, Hungry Fox now at 7 hp.
[1410] Hungry Fox (180, 70) attacked jgw (180, 70). Hit for 3 hp, jgw now at 157 hp.
[1410] jgw (180, 70) attacked Hungry Fox (180, 70). Hit for 8 hp, Hungry Fox now at 11 hp.
[1391] jgw (173, 62) attacked Chicken (173, 62). Hit for 10 hp, Chicken now at 0 hp.
[1304] jgw (216, 75) equipped Great Axe .
Metrics:
User
Health Check
Actions/sec
# of deaths
Time between actions
crunchy horror
true
8.2
2
120 msecs
jgw-mc-linux
true
7.5
3
132 msecs
jgw
true
8.2
2
120 msecs

Application Modernization Journey



Security in the Container world

Docker Isolation Model…..no isolation



These are either intentionally or unintentionally shared between containers:

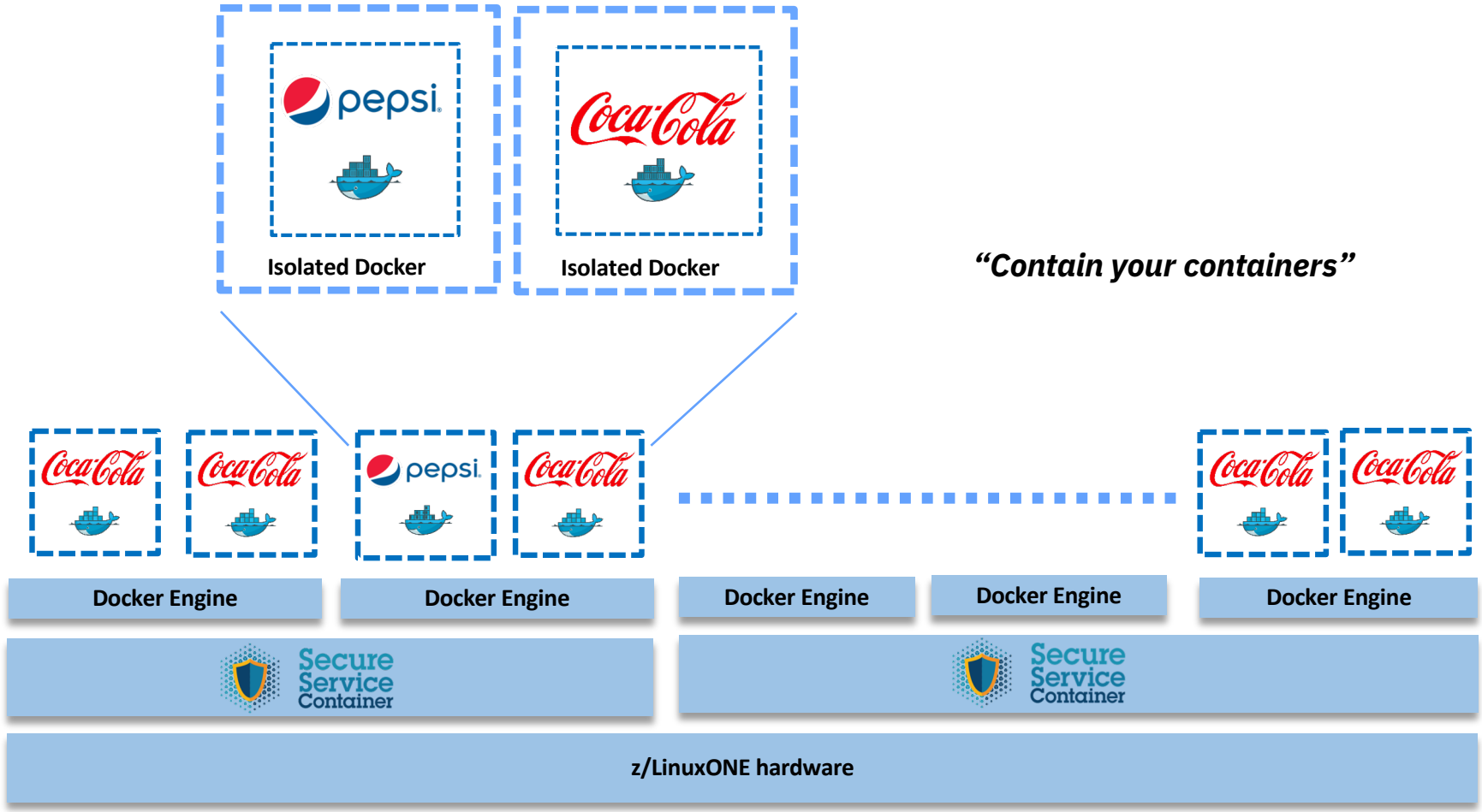
- Network
- Storage
- File System
- Sockets

….everything

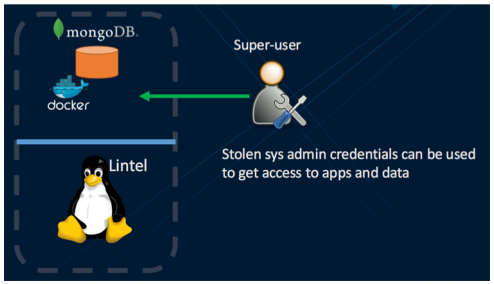
Does not provide VM level isolation

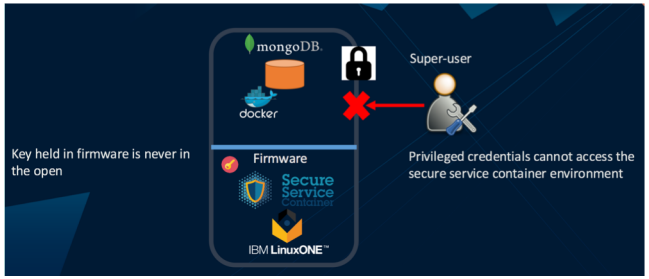
```
$ docker run -v /home/${USER}:/h_docs ubuntu bash -c "cp /bin/bash /h_docs/rootshell && chmod 4777 /h_docs/rootshell;" && ~/rootshell -p
```

Isolated Docker Technology provides VM level isolation between containers



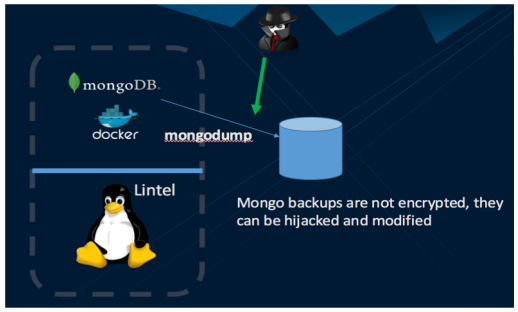
Scenario 1: Privileged Users

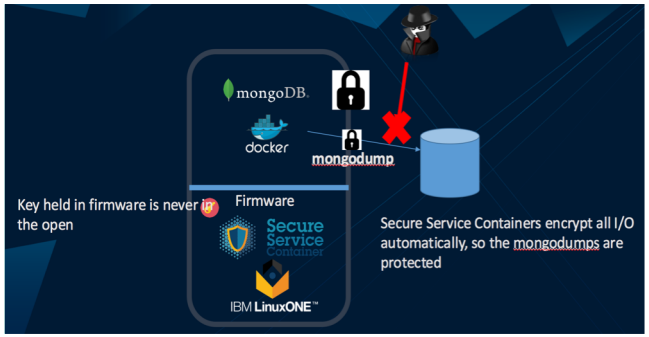




http://uk.businessinsider.com/yahoo-hack-by-state-sponsored-actor-biggest-of-all-time-2016-9?r=US&IR=T

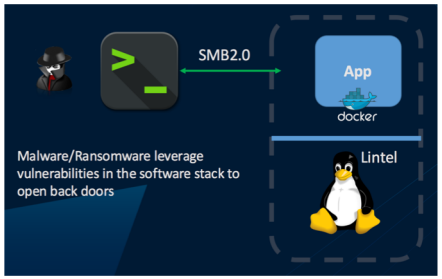
Scenario 2: Pervasive Encryption

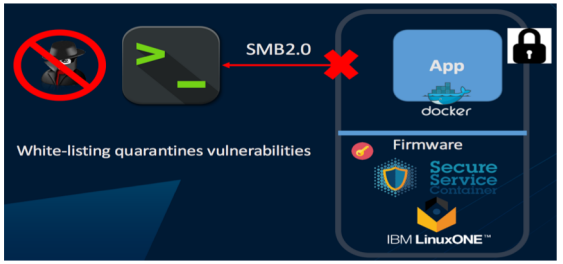




https://www.theguardian.com/technology/2017/aug/30/spambot-leaks-700m-email-addresses-huge-data-breach-passwords

Scenario 3: Malware/Ransomware



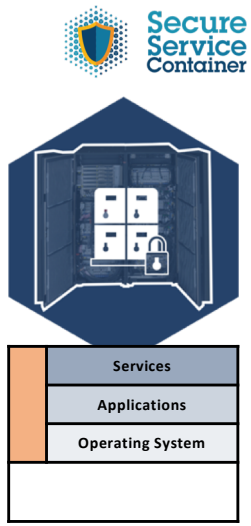


Box folder Demo link

Secure Service Containers

In production with 400+ IBM Blockchain clients!

- **SSC: Protection against misuse of privileged user credentials**
  - Docker execution environment where the infrastructure and data are protected against access and abuse by root users, system administrator credentials and other privileged user access
  - Eliminates any back doors for an internal threat (malicious or accidental) as SSH is disabled
  - Malware (e.g. ransomware) is prevented from being installed or spread
  - Security is whitelist or opt-in based at appliance creation time
- **Key safety**
  - Value further extended by safeguarding all communications & data in SSC
  - Encryption with highest US government computer security standard **(FIPS 140-2 level 4)**
  - All keys held in a tamper resistant HW security module (HSM) certified to same security standard
  - Data is only as safe as the keys: Keys are never in the clear
  - x86 systems do not offer the level of integration with FIPS validated HSM
- **LPAR: Protection of peers in cloud environments**
  - Multi tenancy peers run in protected isolated environments to prevent deliberate or unintentional leakage of information
  - EAL 5+ certification



Application, storage, memory and network is protected with no changes to application code needed !

**** Kubernetes in SSC currently available today in IBM's public cloud http://ibm.biz/HyperPCons***
ICP in SSC in plan for 4Q18, subject to change

Pervasive Encryption *for all workloads*

Protection from Misuse of Privileged Hardware & Operating System Credentials

Infrastructure management organizations can manage the physical IT infrastructure without having visibility to their end users' applications and customer data

Storage Admin

Automatic File System Encryption (LUKS) – Data at Rest

- Encryption keys stored within appliance, not accessible
- Key Management via appliance life cycle export/import
- Docker container data connected to disk also encrypted

Network Admin

Automatic Network Encryption (TLS) – Data in Flight

- Encrypted management REST API interfaces (i.e. storage, network configuration data, dumps, etc.)

System / Hardware Admin

Encrypted Diagnostic Data (ex: Debug Dump Logs)

- First Failure Data Capture – data required to fix problem
- Dump targets host kernel data (log message buffers, etc.)
- Dump data encrypted – only accessible by service teams
- Alternative to memory display alter – minimal access to customer data

Operating System Admin

No Operating System Access

- No direct Host or OS level interaction - SSH Disabled
- Prevent user traditionally with host OS access from having visibility to application or customer data

Software Appliance Form Factor for Simplified Deployment and Management

Appliance

Avoid management of low level execution environment

- Appliance encapsulates operating system, virtualization layer, management UI, REST API interface components
- Agile CI/CD update flow of SSC4ICP platform for feature enhancements, security fixes (CVEs), etc.
- Avoid lifecycle management of individual components

Hybrid & Private Cloud Administrators

- Focus on deployment of k8s cluster to ICP worker / proxy nodes as infrastructure for containerized workloads

Solution Developers

- Focus on building containerized applications

User Feedback

Industries

- Banking
- Retail
- U.S. State and Federal Government
- CSI
- Insurance
- Healthcare

"By not having the OS layer, that's one less layer to manage from a security perspective …"

GERMAN BANK

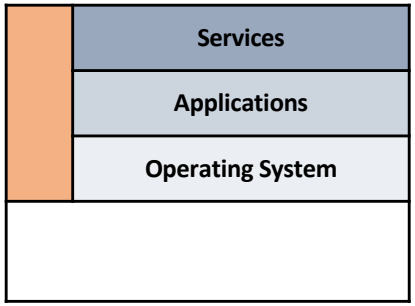
"As a long time z sys programmer - this type of technology you just can't get fast enough … Concept is very usable -- like forward thinking to exploit the HW … love the idea of multiple tenants … fantastic"

US STATE GOV'T

"A real game changer in the marketplace -- being able to say that you can't get to the data will have immense value"

UK MSP

Secure Service Container



FIPS 140-2 Level 2 vs Level 3 vs Level 4

	Level 2	**Level 3**	**Level 4**
Probability of tampering detection	Moderate	Higher	Highest
Requirement for detection	Physical	Physical	Physical, Environmental, Electrical
Action	Evidence of tampering	Zeroization of keys and CSPs	Zeroization of keys and CSPs
Impact to data security	Keys and CSPs can be leaked	Lower potential for keys/CSPs to be leaked	Least potential for keys/CSPs to be leaked
Commercially Availability	Most	Cloud providers are slowly adopting	Only IBM

zOS Cloud Broker

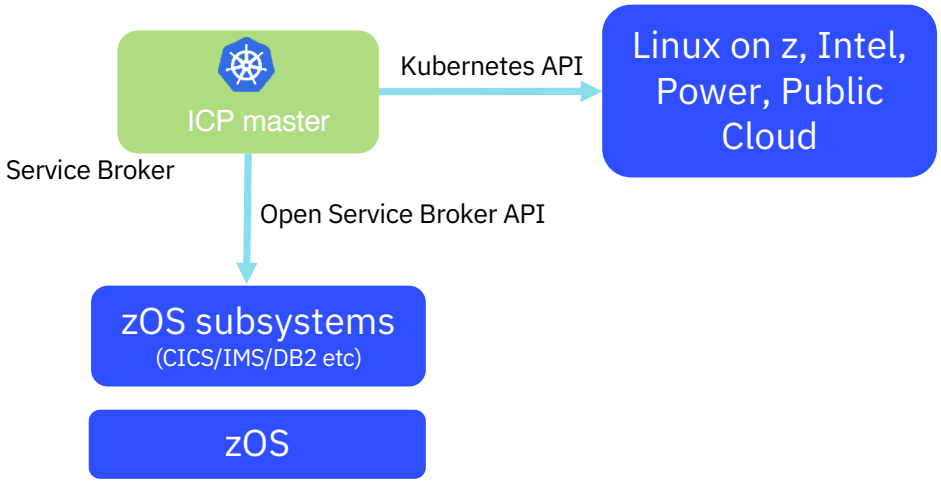
Integrate zOS Environment to Central Enterprise Control Plane

Challenge

Business critical applications running on zOS are isolated, and installation of any Cloud platform will not integrate my zOS subsystem within same control planes. Will require multiple control planes and integration tools

Client Value

- zOS subsystem can be deployed leveraging zOSMF and standardized Service Broker implementation and Open Service Broker APIs
- Single control plane across zOS, Linux on Z, x86, Power, and public cloud
- Protect existing investment, optimize management efficiencies, and achieve speed for innovation



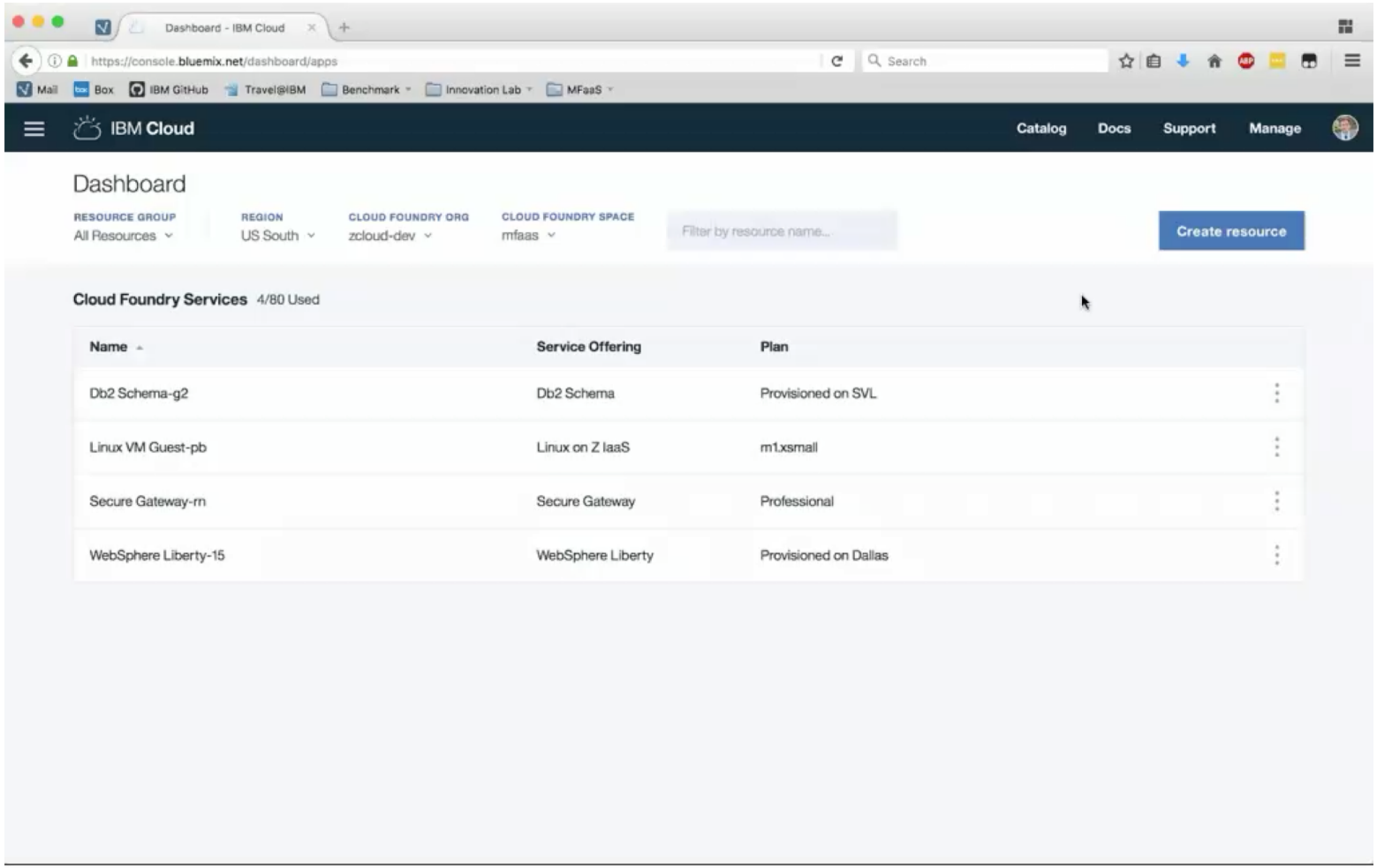
zOS Cloud Bundle for ICP

**** 2Q GA , Beta open now***

Potential Subsystem Support

Services	Description
DB2	Services to provision/de-provision DB2 subsystems, schemas, and databases + snapshot / restore (new)
CICS	Services to provision/de-provision CICS regions
IMS	Services to provision/de-provision IMS TM/DB systems and IMS FastPath databases
MQ	Services to provision/de--provision MQ Queue Manager subsystem and load messages
WAS	WLP server provisioning (with option to connect to Db2 data source with type 2 or type 4 connectivity)
z/OS Connect	Services to provision/de-provision z/OS Connect (new)

zOS Cloud Broker **Demo**


Dashboard - IBM Cloud
https://console.bluemix.net/dashboard/apps
Search
Mail
Box
IBM GitHub
Travel@IBM
Benchmark
Innovation Lab
MFaaS
IBM Cloud
Catalog
Docs
Support
Manage
Dashboard
RESOURCE GROUP
All Resources
REGION
US South
CLOUD FOUNDRY ORG
zcloud-dev
CLOUD FOUNDRY SPACE
mfaas
Filter by resource name...
Create resource
Cloud Foundry Services 4/80 Used
Name
Service Offering
Plan
Db2 Schema-g2
Db2 Schema
Provisioned on SVL
Linux VM Guest-pb
Linux on Z IaaS
m1.xsmall
Secure Gateway-rn
Secure Gateway
Professional
WebSphere Liberty-15
WebSphere Liberty
Provisioned on Dallas

Thank You!

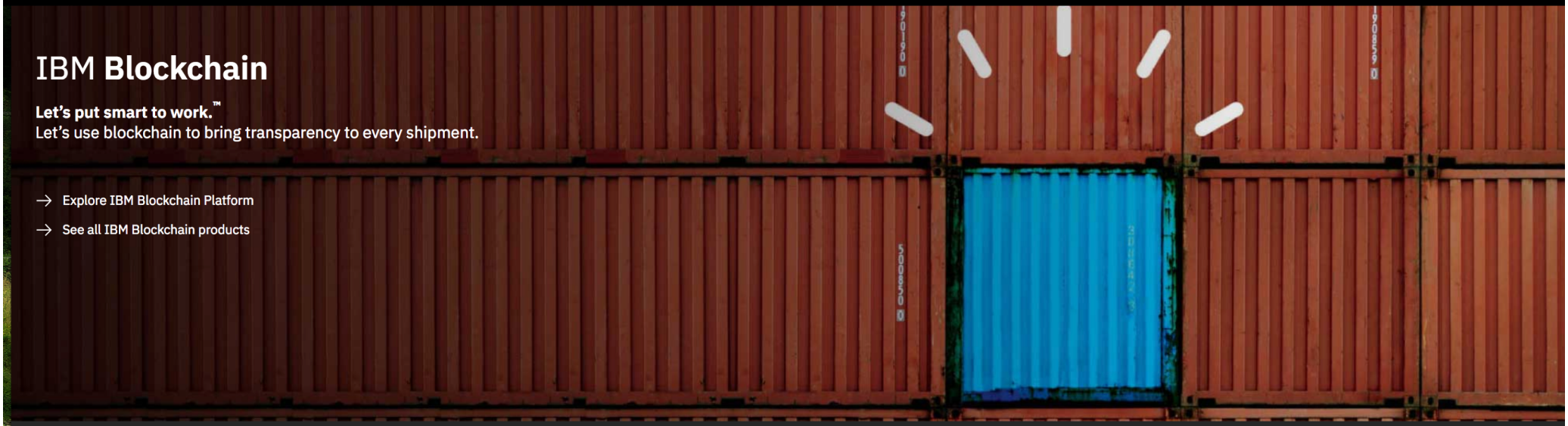
IBM Z in IBM Cloud – Hyper Protect Family

IBM **Blockchain**

Let's put smart to work.™
Let's use blockchain to bring transparency to every shipment.

→ Explore IBM Blockchain Platform

→ See all IBM Blockchain products



Blockchain revolutionizing advertising media buying

→ New solution to help solve pressing problems facing advertisers and publishers

Social and environmental tokens

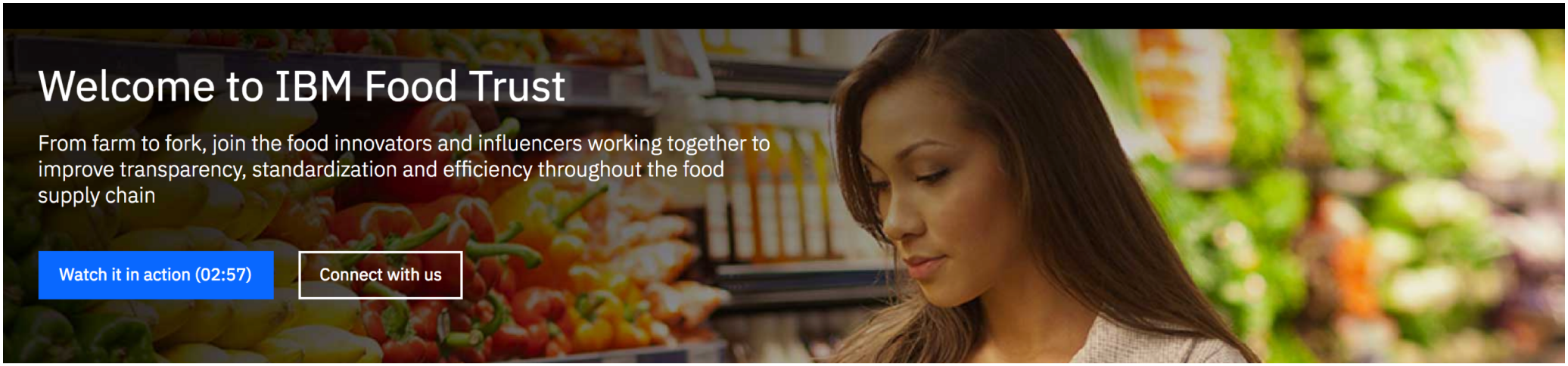
→ Veridium, IBM Blockchain to create carbon credit tokens

Start developing now

→ Get $500 in credits with our starter plan

Blockchain best practices

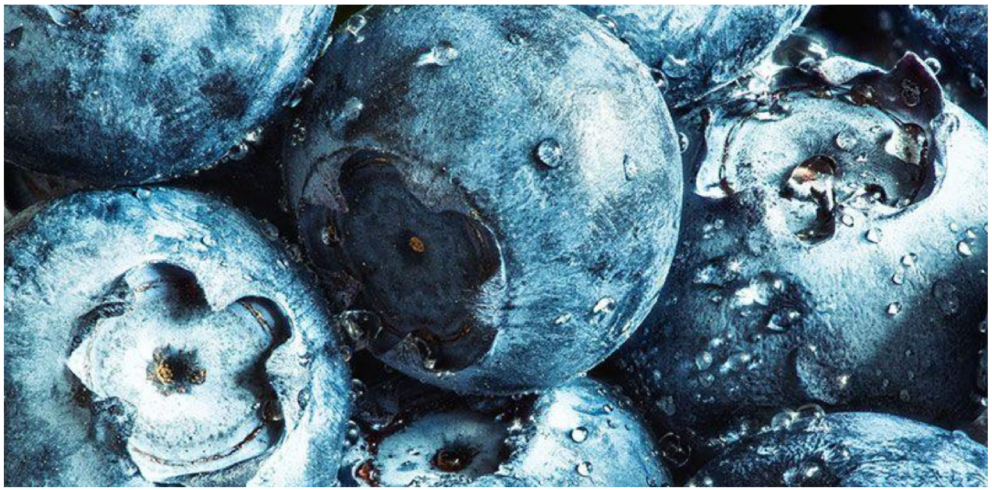
→ From 100s of client projects — The Founder's Handbook

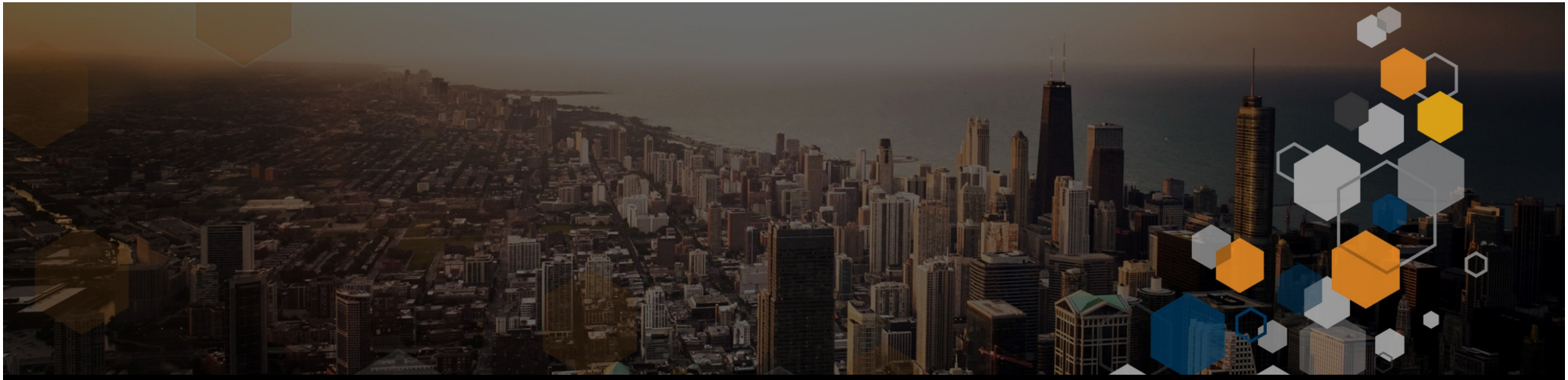


What is IBM Food Trust?

IBM Food Trust™ is a collaborative network of growers, processors, wholesalers, distributors, manufacturers, retailers and others enhancing visibility and accountability in each step of the food supply. Powered by the IBM Blockchain Platform, IBM Food Trust directly connects participants through a permissioned, permanent and shared record of food origin details, processing data, shipping details and more.

→ See the solution overview

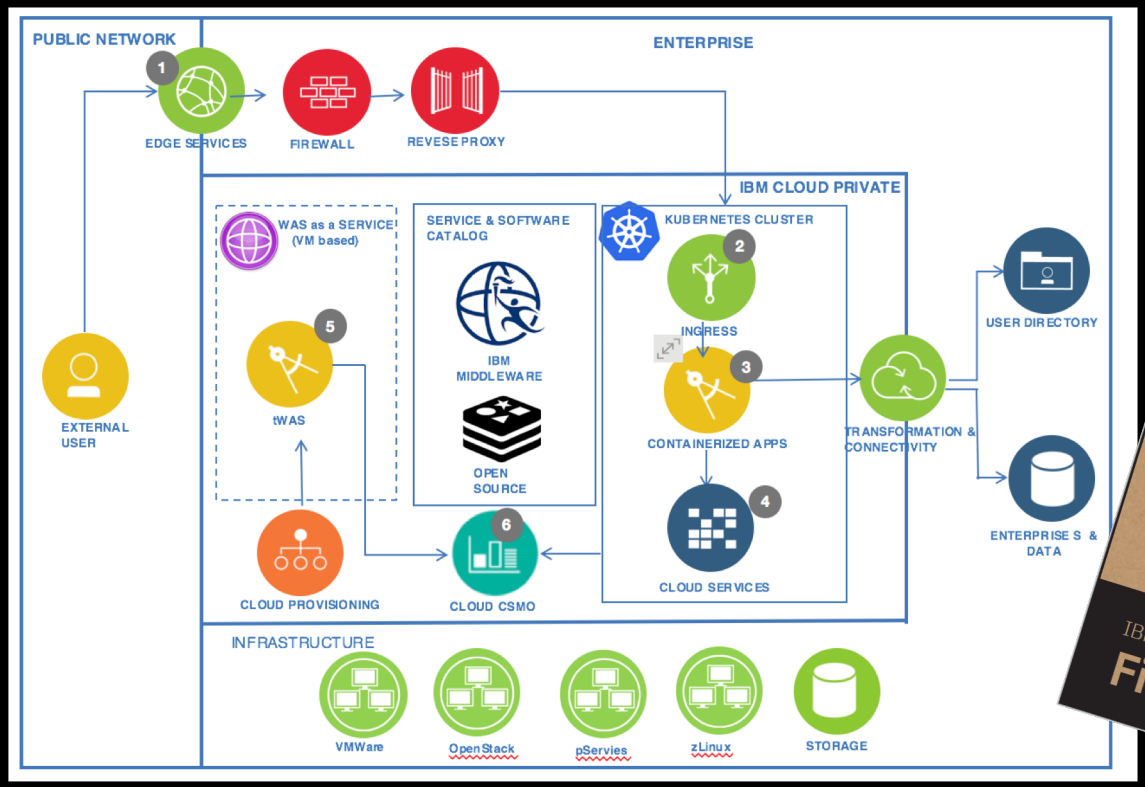


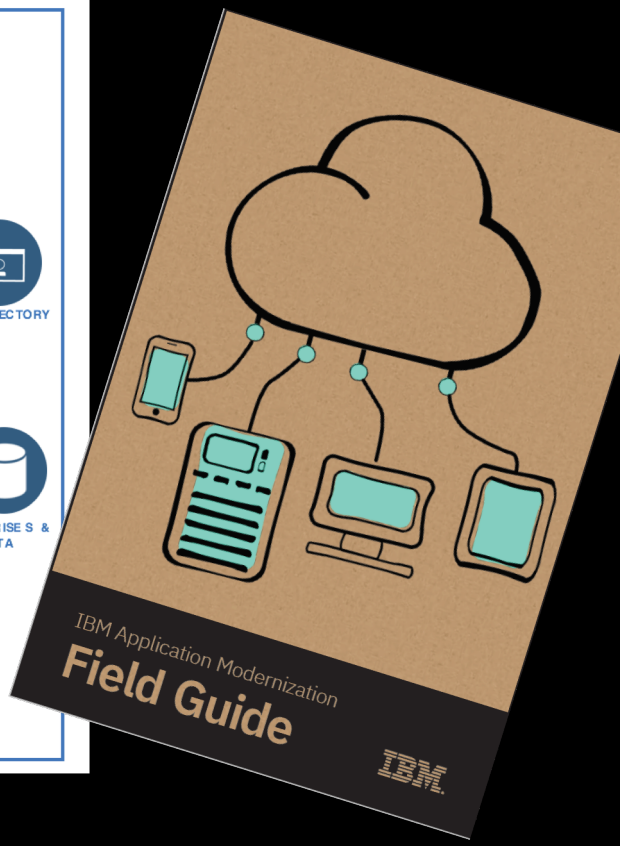


Build, deploy and host applications in IBM Public Cloud with "***Hyper data protection***"

- **Hyper Protect Crypto Services**
- **Hyper Protect Containers**
- **Hyper Protect DBaaS**
- **Hyper Protect VMs**

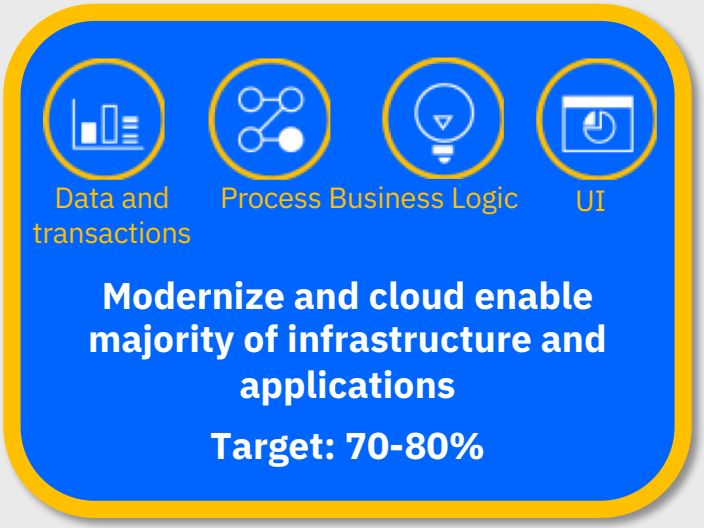
Application Modernization domain at Architecture Center



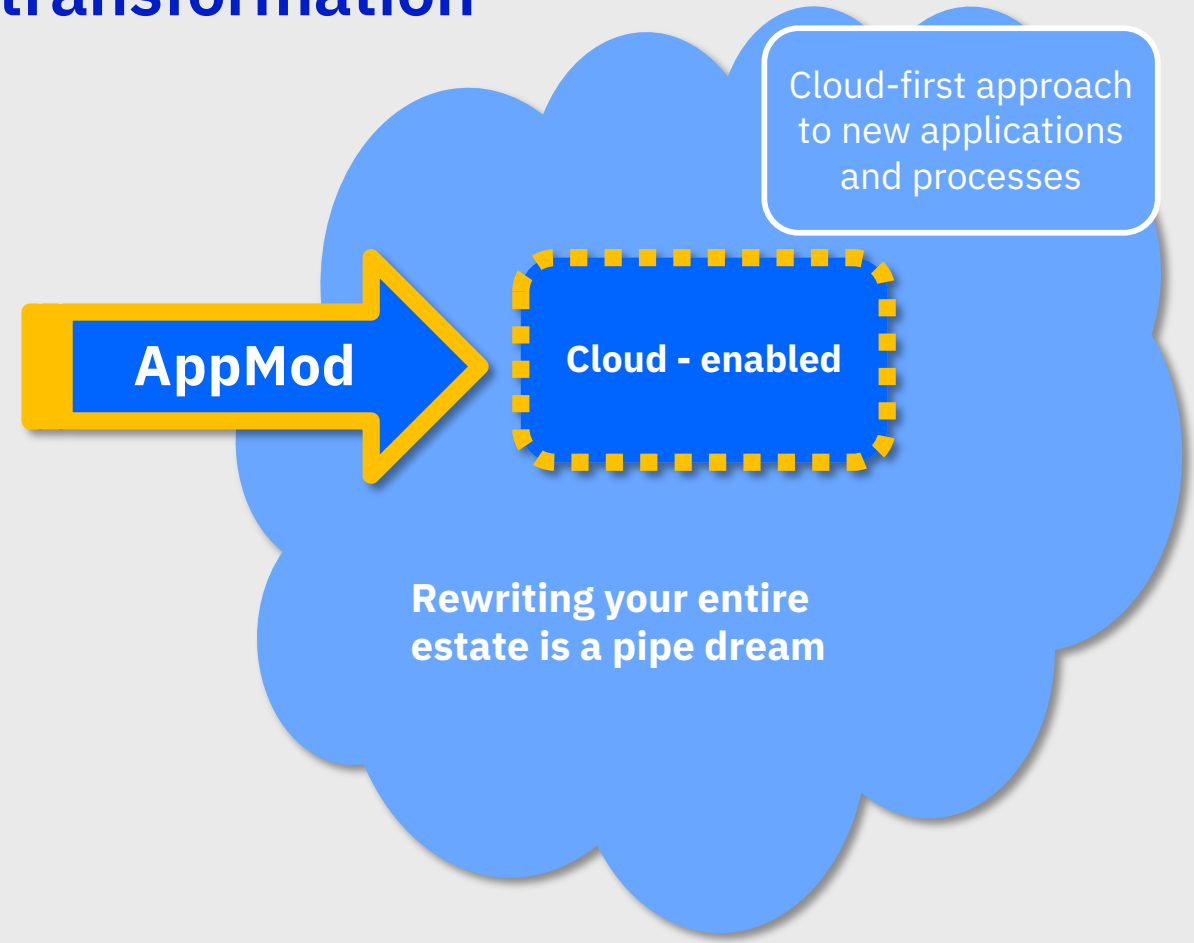


https://www.ibm.com/cloud/garage/architectures

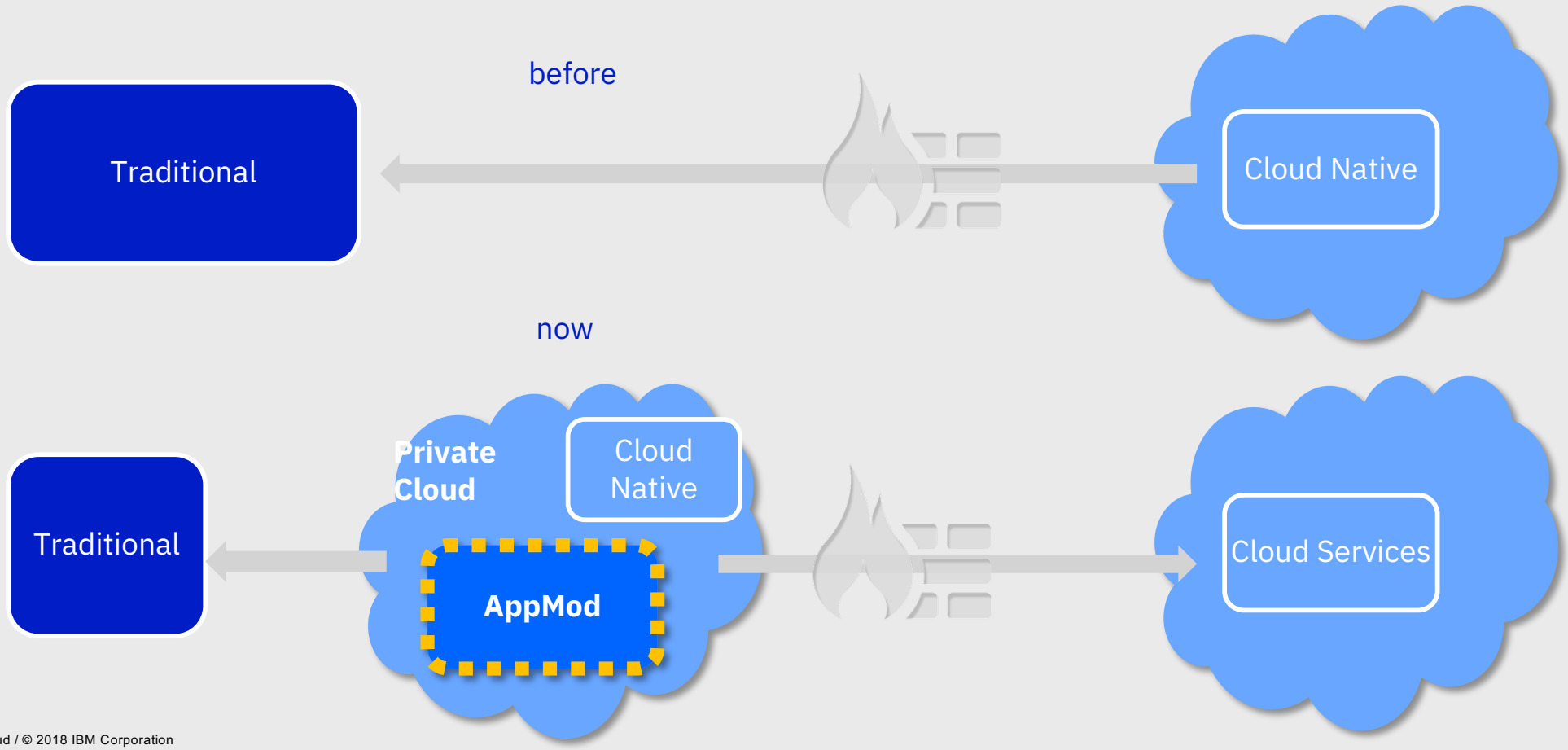
Application modernization is an inevitable part of Cloud transformation



Preserve, standardize and automate subset of existing applications
Target: 20-30% full automation



AppMod use case “unlocked” by Private Cloud



IBM's Approach to Application Modernization

IBM has developed innovative solutions, tools and service to help organizations modernize their existing application portfolio.

1

Built-in Technology

Automated with ***Transformation Advisor***

Rich set of ***containerized Middleware***

Manage ***VMs and Containers***

Built-in ***DevOps*** *with* ***Microclimate***

2

Proven Approaches

Prescriptive guidance*, online demos and tutorials*
IBM Garage Architecture for ***best practices***

3

Acceleration Services

Turnkey modernization
Acceleration services aligned with proven approaches

4

Investment Protection

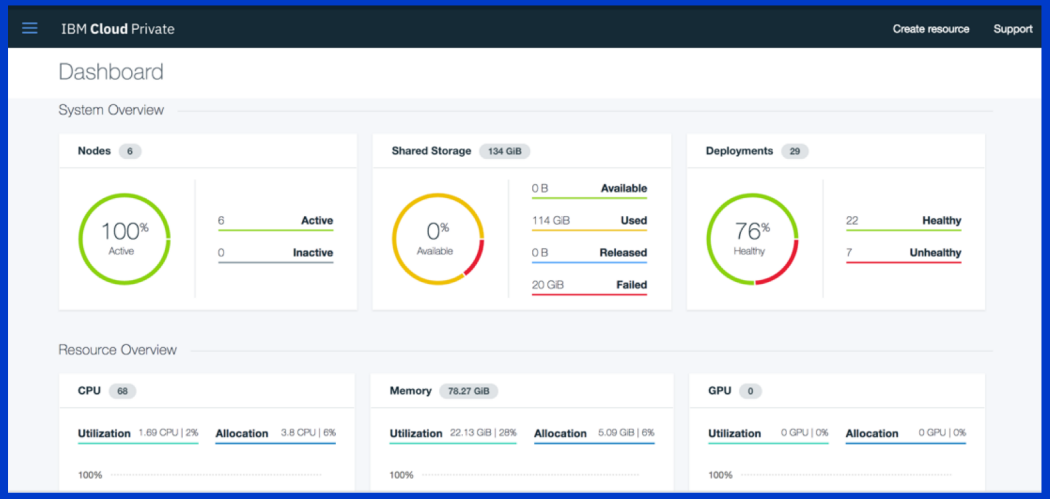
Leverage your existing investments to adopt new technology ***at your pace***

Let IBM simplify and transform your Application modernization journey!

Try IBM Cloud Private today!

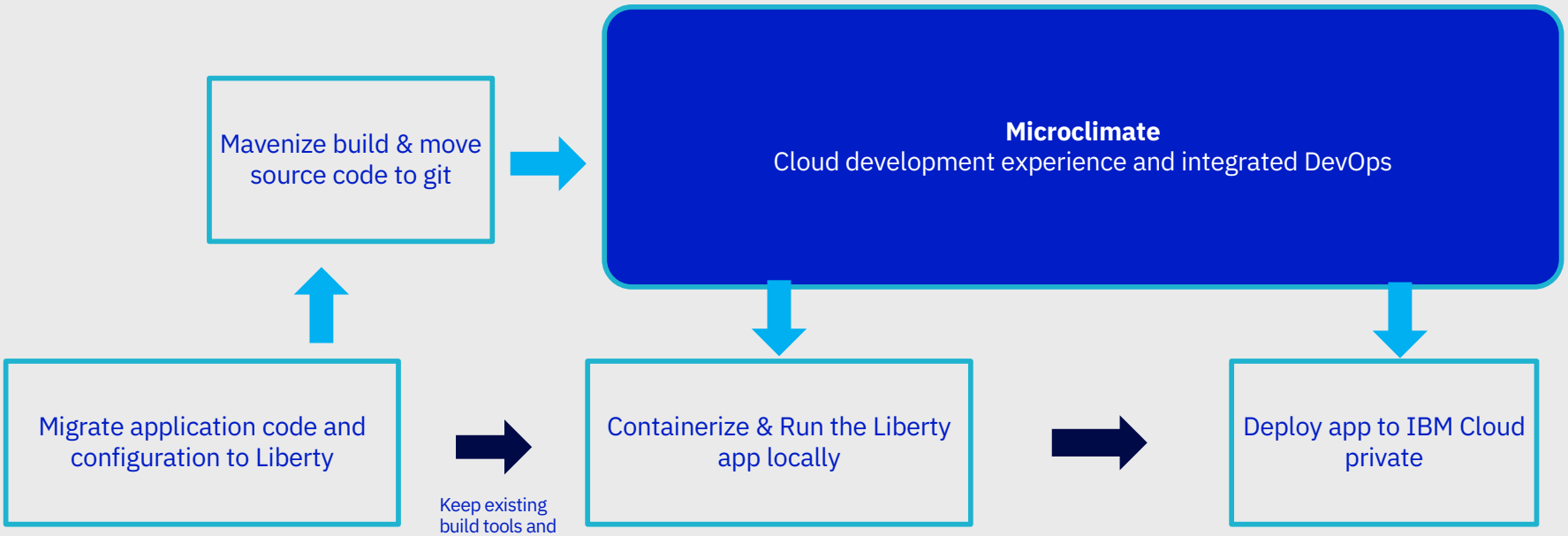
Guided and Proof of Technology demos

Free Community Edition!



http://ibm.biz/ICP-DTE

Developer Experience of Application Modernization



Source code migration (if required)

- Eclipse IDE
- WebSphere Developer Tools for Eclipse
- WebSphere Application Migration Toolkit
- WebSphere Configuration Migration Tool

Create Docker image

- Docker
- Liberty Docker image

Run on Cloud

- Private Docker registry
- ICP admin UI
- Kubernetes CLI
- Helm charts

https://github.com/ibm-cloud-architecture/refarch-jee-customerorder/blob/liberty/tutorial/tutorial.md