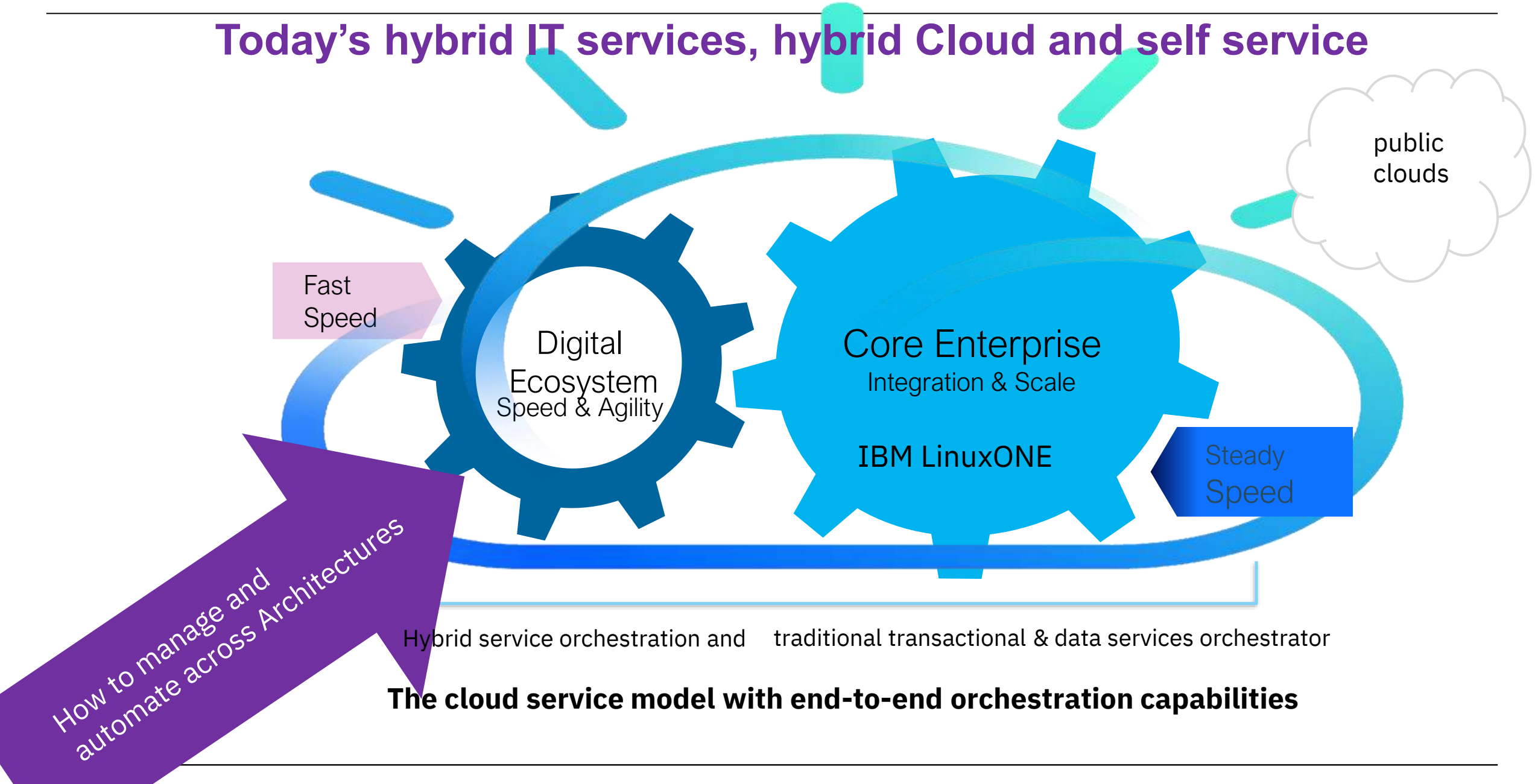
Build a secure, Quantum safe Hub for Automation, Management and Operation on IBM Z & IBM LinuxONE

session 202

Wilhelm Mild
IBM Executive IT Architect
IBM R & D Lab Germany
wilhelm.mild@de.ibm.com

Today's hybrid IT services, hybrid Cloud and self service

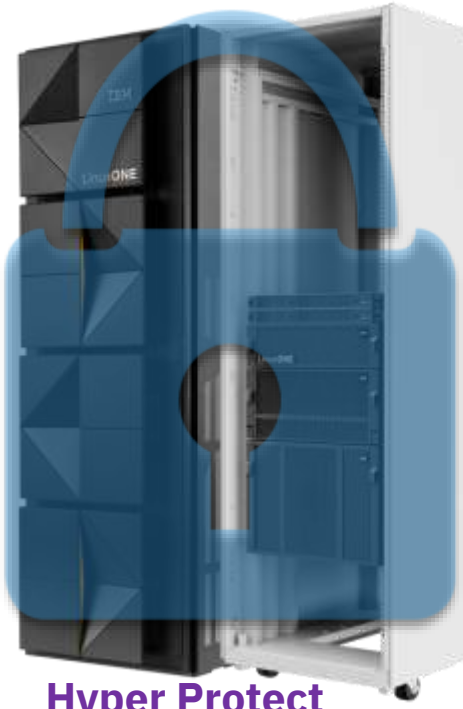


The cloud service model with end-to-end orchestration capabilities

IBM LinuxONE as a secure Hub for the entire enterprise

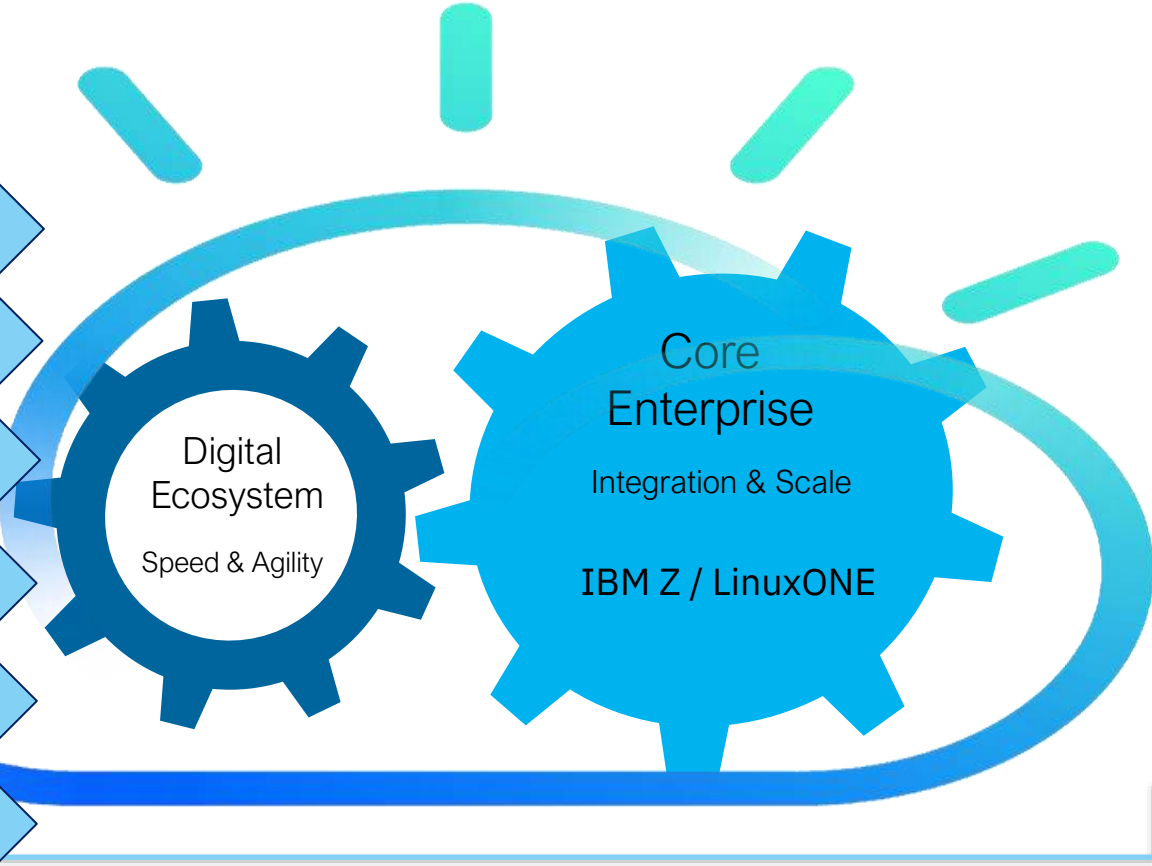
➢ **Why: Most Secure, Role based, Zero Trust environment**

IBM LinuxONE



Hyper Protect & Secure Execution

- ➢ **Enterprise Management & Operation Hub**
- ➢ **Automation Hub**
- ➢ **Data Resiliency Hub, Backup, HA/DR**
- ➢ **Integration Hub**
- ➢ **Security Hub**
- ➢ **Observability Hub, Open Telemetry**

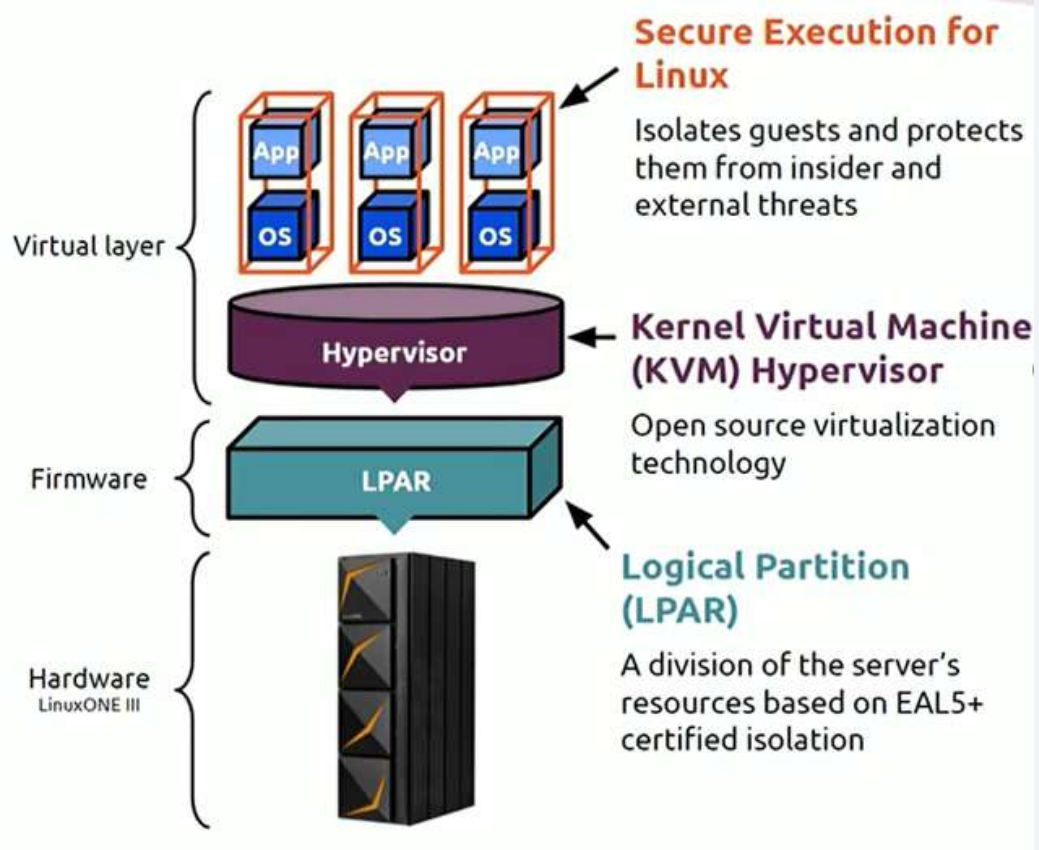


This Management Hub – is a secured centralized service model with end-to-end orchestration capabilities !

Confidential Computing enabled by hardware & Secure Execution for Linux

What is it:

Trusted Execution Environment built into the IBM Z & LinuxONE server



What does it do

Provides scalable isolation for individual workloads to help protect them from not only external attacks, but also insider threats

How does it help

Current approaches only address data at rest and data in transit, Secure Execution Linux protects data in-use.

Trusted Execution Environment (TEE) allows for Hardware enabled protections to realize a Zero Trust environment with workload isolation and hardened access restrictions of data.

IBM Z Security

Full stack provides differentiation

IBM Z® Security Services

- Expert Labs
- X-Force Red
- IBM Consulting
- Crypto Competency Center

IBM Z Security Software

- Confidential Computing
- Data Protection
- Identity & Access Management
- Key & Secrets Management
- Threat Management
- Compliance

Virtualization, Middleware, and OS

- Robust security and privacy capabilities implemented by design

IBM Z Hardware

- Hardware Security Modules
- Quantum Safe Secure Boot & Crypto APIs
- Dual HW Accelerated Cryptography
- IBM Secure Execution for Linux
- Hardware Protected Keys
- Security certifications (FIPS Level 4, EAL5+)

We are entering a new cryptographic era

Quantum computers can, in principle, perform certain mathematical computations exponentially faster than a classical computer

There will be a time when the power of quantum computing may crack public key cryptographic security protection …

Your data and security is already at risk for quantum-attacks

Harvest now, decrypt later
schemes are underway to collect data now for decryption when quantum computers are powerful enough (Data can be exfiltrated)

Replacing most of the public-key systems
currently in use will take 5 to 15 years

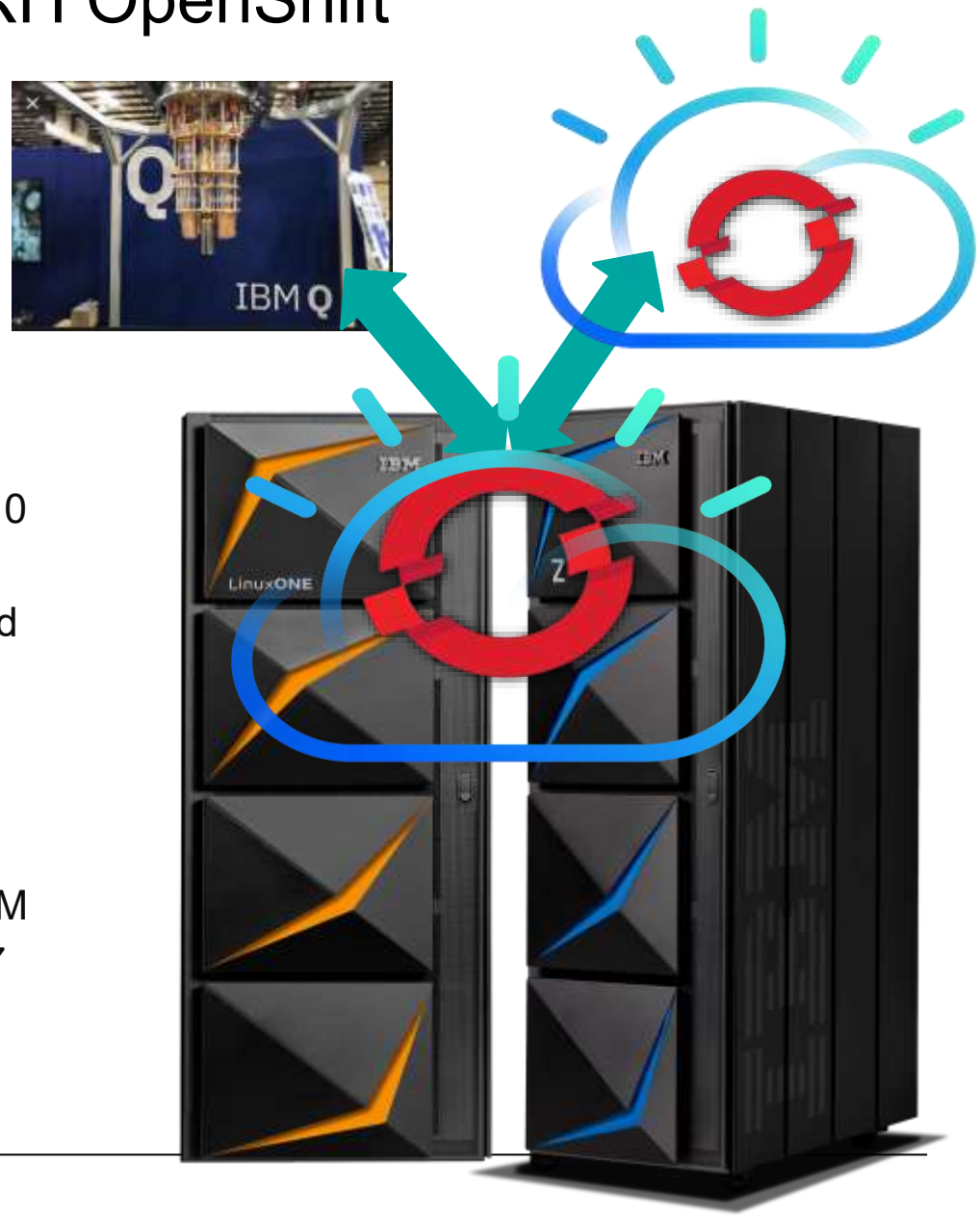
Lifetime of data
means that sensitive data generated today that is not protected with quantum-safe algorithms is at risk now

Start your quantum safe journey now!

Extension to Quantum safe algorithms with RH OpenShift

- Quantum safe security integration

  - **digital signatures** validation like mortgage/credit card approvals
  - **document signing** for Financial Institutions that require decades of retention and validity (e.g mortgages could be 30+ years)
  - **algorithms used for digital signatures** will be invalid (in approx 5-10 years) due to quantum computing. The goal is to dual sign electronic documents so that existing mechanisms can continue to be used, and PQC (**post-quantum cryptography**) can be used where available.
  - **IBM Z algorithms** like Dilithium & Kyber (key encapsulation) can be used for this and signing can be done on existing systems using p12 certs with PKCS11 (via IBM's Enterprise PKCS11 driver) with the HSM backend on a z16 with a CEX8 card. It can be done with z15 & CEX7 too but that only supports 1 Dilithium algorythm, there's newer ones out there only supported on CEX8



LinuxONE as the enterprise Hub for your Hybrid Multi-Cloud

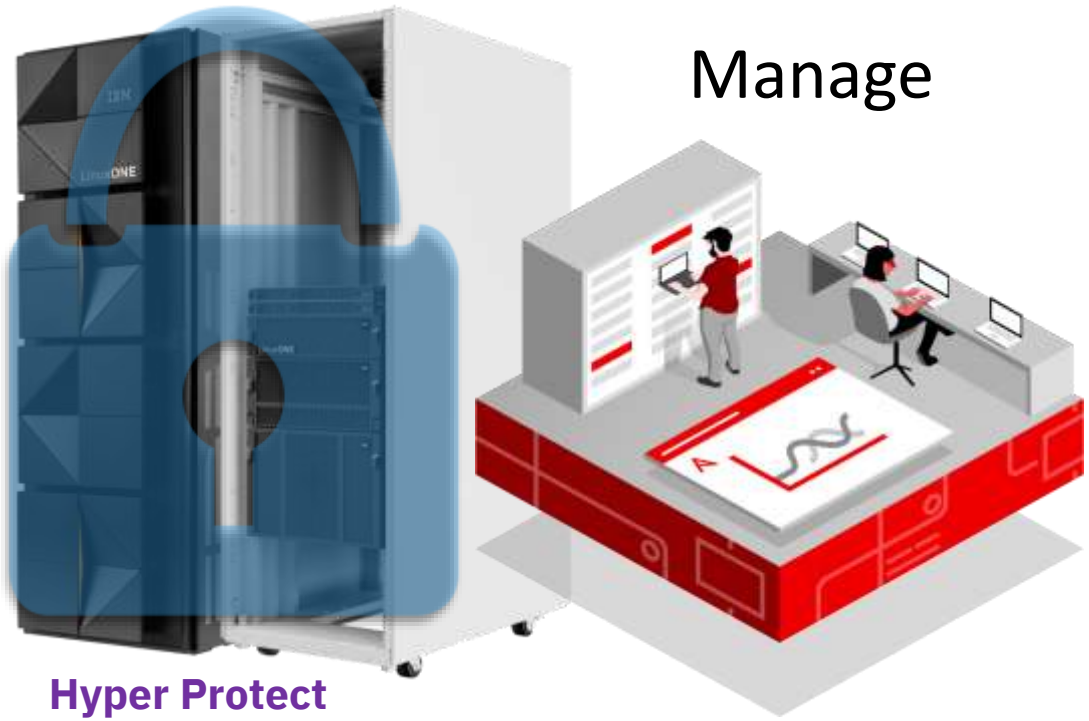
Bundles IBM LinuxONE and Software to build the Hub Options – start today:

1. **Enterprise Management & Operation Hub**
   (SW: Hashicorp Teraform, ICIC, ACM)
2. **Enterprise Automation Hub**
   (SW: Hashicorp Teraform, RH Ansible Automation Platform, ICIC)
3. **Data Resiliency Hub, Backup, HA/DR**
   (SW: Storage Protect+, GDPS Appliance, ACM)
4. **Enterprise Security Hub**
   (SW: IBM Vault, ACS, Security Gateway, Confid. Computing & Secure Execution (SE) enabled SW, Hyper Protect Encrypt Serv)
5. **Enterprise Integration Hub for Hybrid Cloud**
   (SW: CP4I, ACE, AMQ, CP4BA, Data Gate, Nooba GW)
6. **Observability Hub**
   (SW: Instana, Turbonomics, Open Telemetry)

IBM LinuxONE
or Rack Mount

Hyper Protect
& Secure Execution

(1) LinuxONE as Management Hub



Hyper Protect
& Secure Execution

High benefit with inheritance of LinuxONE characteristics:

- Security
- Scalability
- Resiliency

Goal: Centralized Common toolset

- **Infrastructure management**

with Hashicorp Terraform and IBM Cloud Infrastructure Center (ICIC)

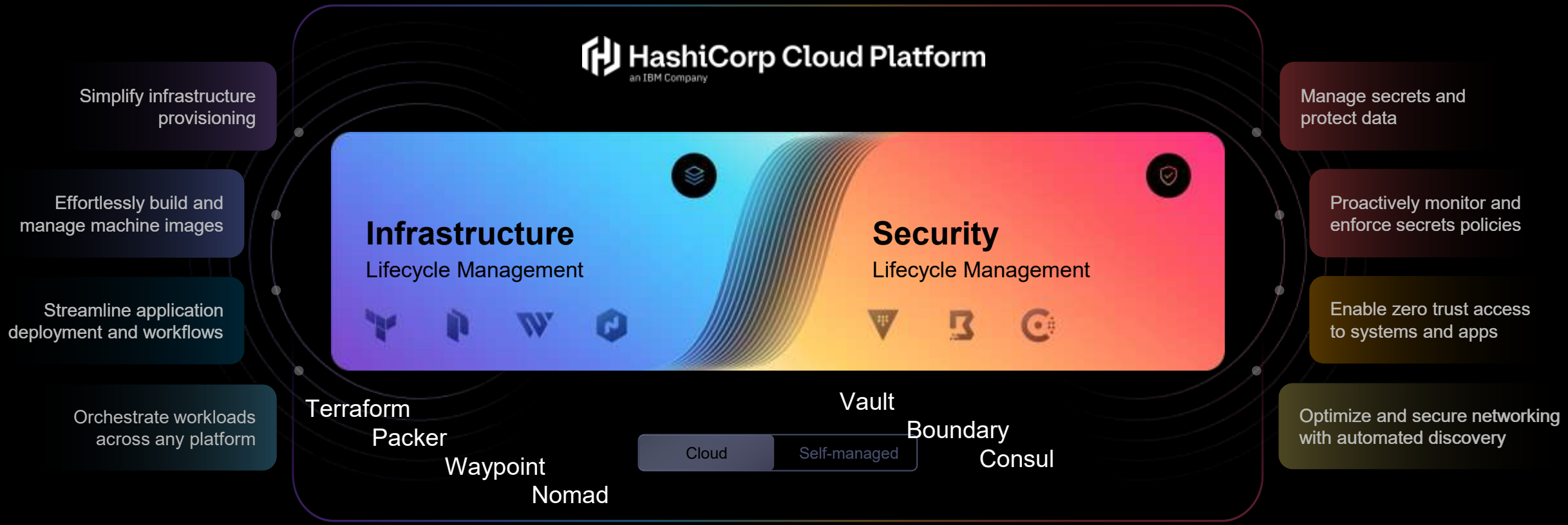
- Virtual environment management (VMs)
- Infrastructure management
- External tools enablement for LinuxONE management

- **Hybrid Multi-Architecture Multi Cloud management**

- **using RH Advanced Cluster Management for Kubernetes**
- single Pane of Glas
- on-premise
- heterogeneous Kubernetes Container environments
- Multi Cloud & Multi-Architecture
- including Kubernetes in public clouds

THE INFRASTRUCTURE CLOUD

Delivering a portfolio of hybrid solutions



Terraform, Packer, Waypoint, and Nomad standardize provisioning, orchestration, and automation, ensuring consistency in how infrastructure is deployed and managed.

Vault, Boundary, and Consul unify access management, secrets governance, and network security, enforcing centralized policies and eliminating security gaps.

HashiCorp product suite

Infrastructure Lifecycle Management

Provisioning and Management

Use infrastructure as code to build, deploy, and manage the infrastructure that underpins cloud applications

Terraform
Infrastructure provisioning

Packer
Image management

Nomad
Workload orchestration

Security Lifecycle Management

Identity and Access

Use identity-based access controls to manage the security of your secrets, users, and services

Vault
Secrets management

Boundary
Secure access

Consul
Service networking

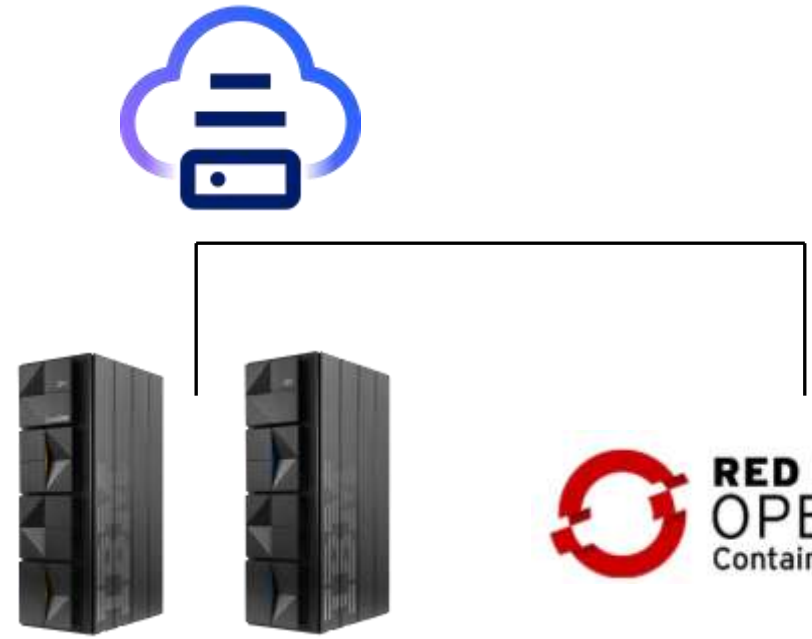
IBM Terraform Self-Managed for Z and LinuxONE

- The capabilities, enable users to support a variety of networking and storage use cases:
  - Generate Terraform resources representing the networking configuration of an existing LPAR
  - Define new physical networks with PNETIDs
  - Define new IO devices and associated LPARs
- Storage
  - Generate and edit a Terraform for Z representation of LPARs.
  - Add new IO devices to a logical sub-system
  - Synchronize storage resources with Terraform state

Statement of direction

IBM intends to deliver IBM Terraform Self-Managed for Z and LinuxONE supported on s390x architecture to include IBM z/OS Container Extensions (zCX). This enhancement will be designed to deepen Terraform integration with IBM infrastructure and provide a more comprehensive automation experience.

➢ **IBM Cloud Infrastructure Center** for Infrastructure-as-a-Service for IBM LinuxONE



Guest provisioning for traditional workloads

RED HAT® OPENSHIFT Container Platform

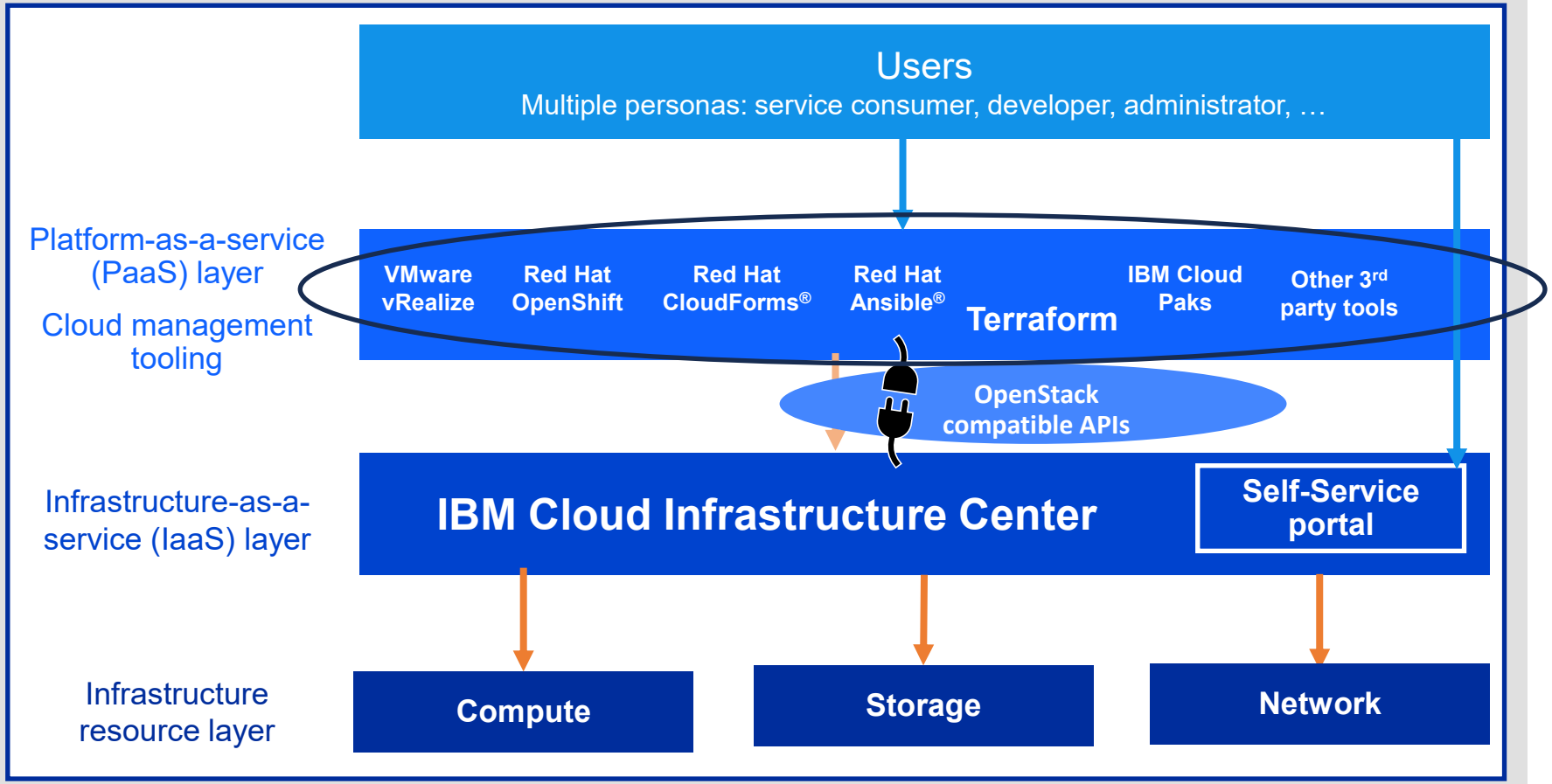
IaaS layer for Red Hat OpenShift deployments (hybrid cloud stack)

- Foundation for scalable Infrastructure-as-a-Service (IaaS) management of traditional and cloud workloads across the enterprise and hybrid cloud

IBM’s hybrid cloud management approach

IBM Cloud integration via cloud tools

- Connecting the layers enables to integrate the IBM LinuxONE infrastructure across the enterprise.



Capabilities

Modernize for hybrid cloud and traditional workloads – empower how you manage, automate, and integrate infrastructure as a service

Infrastructure management

Instantiate, define, capture, and manage the full lifecycle of the virtual machines based on IBM z/VM® and Red Hat KVM on IBM Z and IBM® LinuxONE.

Service automation

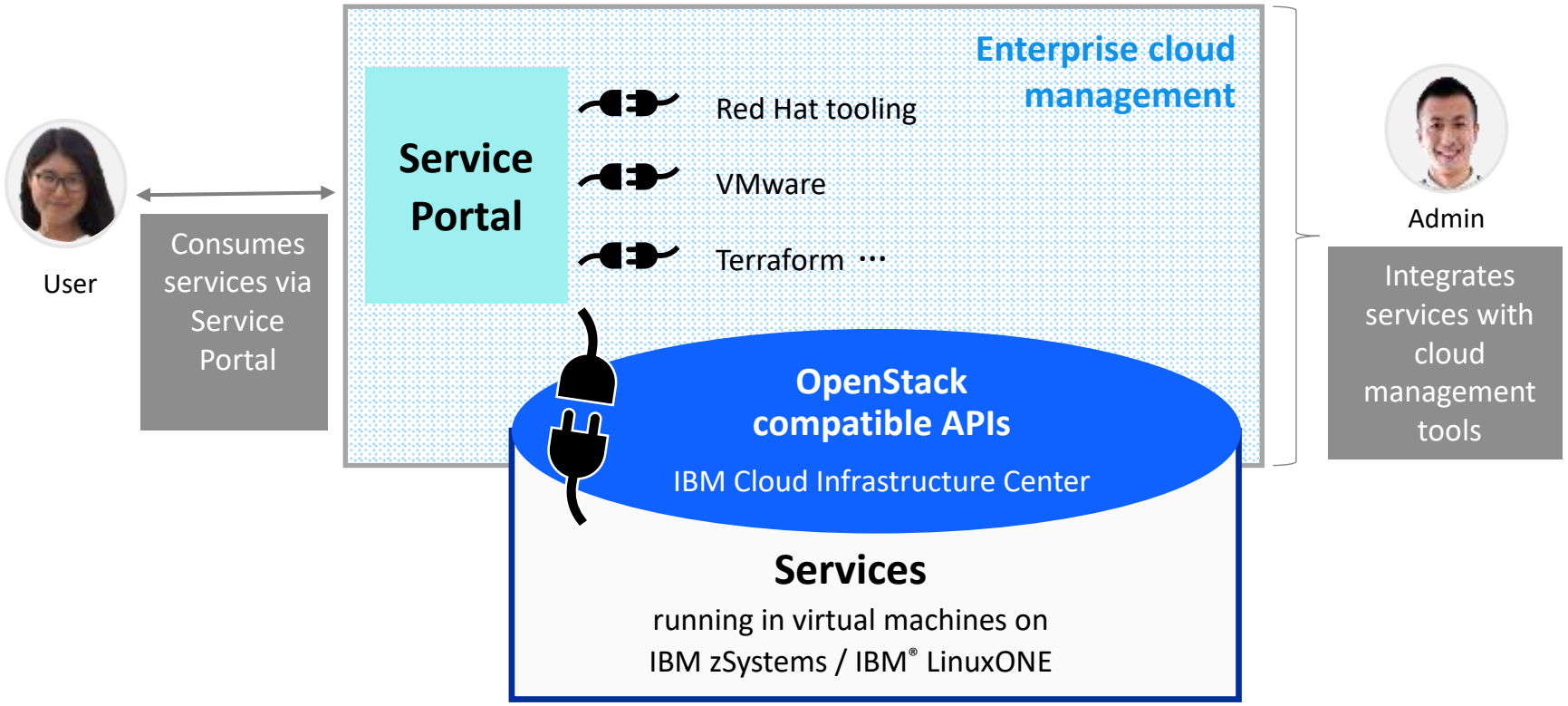
Automate infrastructure management services for users via the Cloud Infrastructure Center self-service portal, while leveraging IBM Z and IBM® LinuxONE investments.

Cloud integration

Integrate the IBM Z and IBM® LinuxONE infrastructure across the enterprise and hybrid cloud by connecting the layers of cloud computing via OpenStack compatible APIs.

Enterprise cloud management

- Via OpenStack compatible APIs, Cloud Infrastructure Center allows for easy integration with cloud management tools to provide an out-of-the-box experience
- to users



Use cases

- **Simplified experience with virtualization**
- *“Simplify”*
- Industry standard based and vendor-agnostic technology for simplified IaaS management

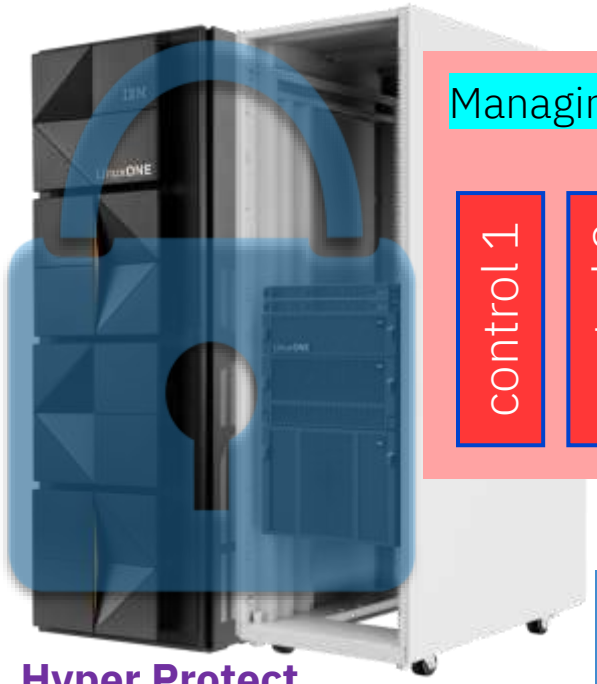
- **Deployment support of Red Hat OpenShift clusters**
- *“User Provisioned Infrastructure”*
- Support to help simplify and automate Red Hat OpenShift cluster deployments

- **IaaS management for service providers**
- *“Tenant-safe services”*
- Service providers can offer tenant-safe IaaS, in a virtual environment

- **Deployment of on-premises database-as-a-service**
- *“Data Gravity”*
- Select a database and automate deployments in an as-a-service model at scale.

➢ Hybrid Multi-Architecture Multi Cloud management

- traditional RH OpenShift landscape managed from a single pane of glass using Red Hat Advanced Cluster Management for Kubernetes (RHACM)



Hyper Protect & Secure Execution

Managing OCP Cluster

control 1 | control 2 | control 3 | RHACM comp1 | RHACM comp2

OCP on x86 (amd64)

control 1 | control 2 | control 3 | compute 1 | compute 2

OCP on IBM LinuxONE (s390x)

control 1 | control 2 | control 3 | compute 1 | compute 2 | compute 3

z/VM or KVM

public/managed clouds

OCP on x86 (amd64)

control 1 | control 2 | control 3 | compute 1 | compute 2

OCP on IBM Z (s390x)

control 1 | control 2 | control 3 | compute 1 | compute 2 | compute 3

Plain Kubernetes

control 1 | control 2 | control 3 | compute 1 | compute 2

OCP on IBM Z (s390x)

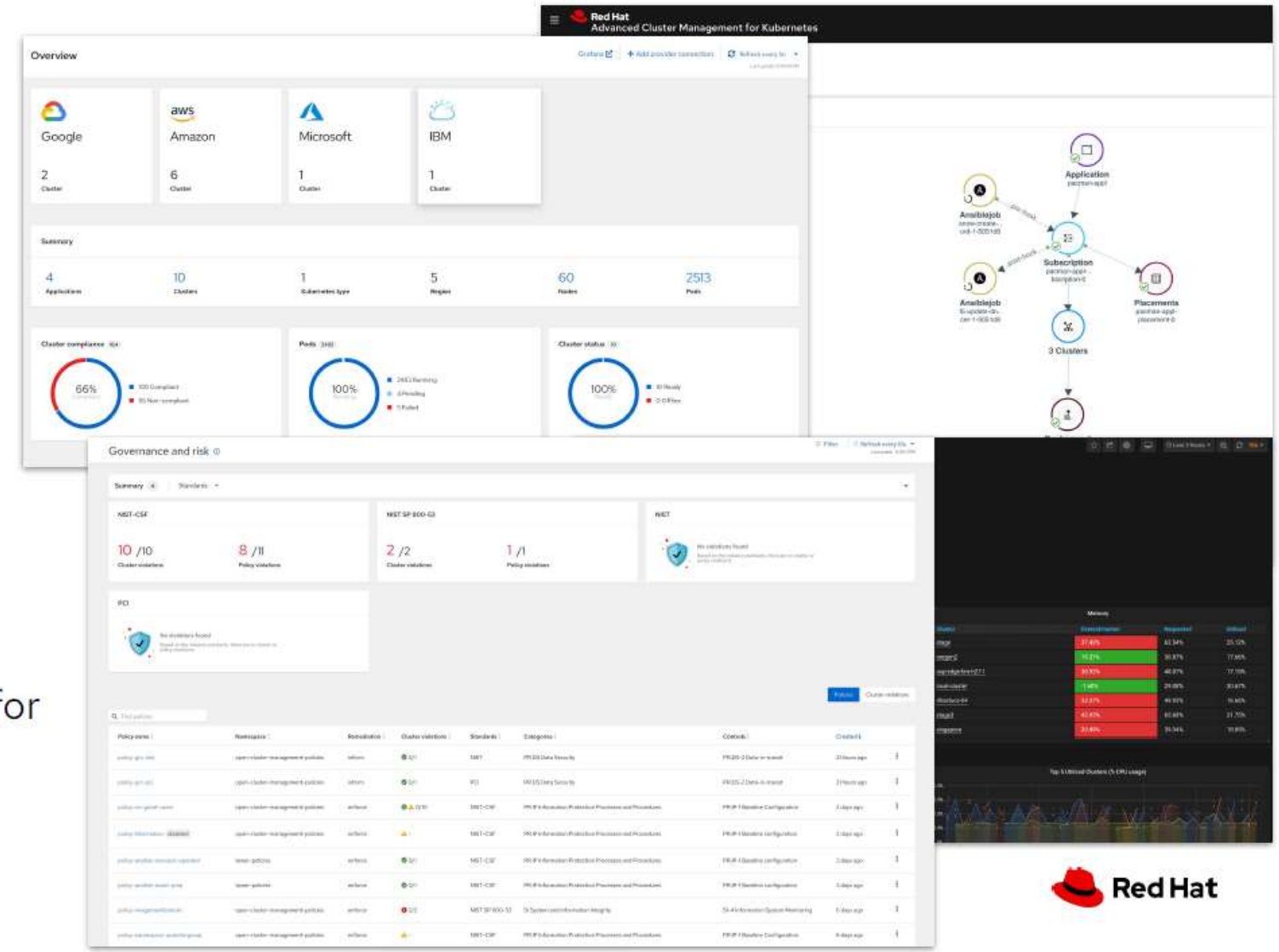
control 1 | control 2 | control 3 | compute 1 | compute 2 | compute 3

z/VM or KVM

Red Hat Advance Cluster manager (RHACM) pillars

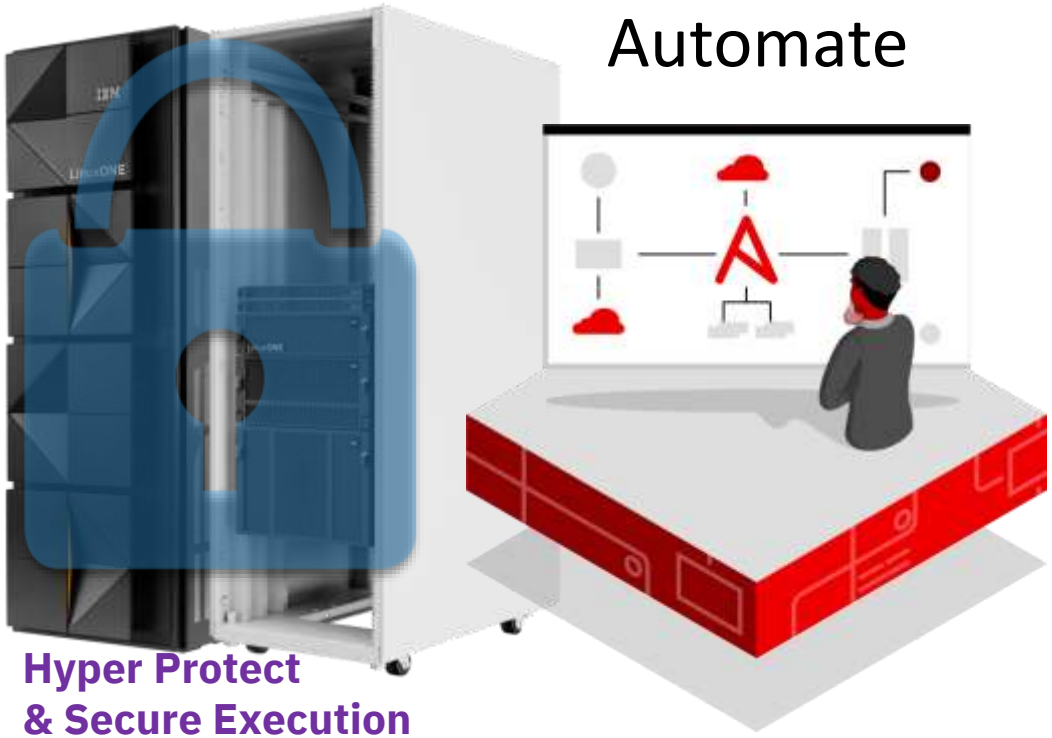
Red Hat Advanced Cluster Management Overview (RHACM)

- Multicluster lifecycle management
- Policy driven governance, risk, and compliance
- Advanced application lifecycle management
- Multicluster observability for health and optimization



Red Hat

(2) LinuxONE as Automation Hub



High benefit with inheritance of LinuxONE capabilities:

- Security
- Scalability
- Resiliency

Goal: Common enterprise toolset

- **Centralized Enterprise Automation management using RH Ansible Automation Platform**
  - on IBM LinuxONE

- Integrate RH Ansible with Infrastructure tooling
- Integrate RH Ansible with Linux on Z
- Make use of Content Collections for IBM LinuxONE
- Automate heterogeneous CI/CD and Container environments
- single Pane of Glas for Automation control
- on-premise
- multi-Architecture
- including public clouds

- **Centralized integrated RH OpenShift Automation**

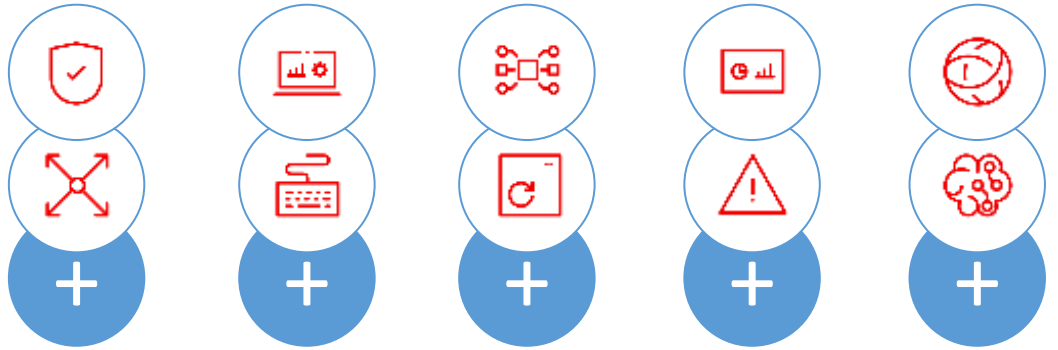
- **using OpenShift Pipelines**
- across RH OpenShift environments

Challenges that require Automation

Many organizations share the same challenge

Differing skills, roles, and responsibilities

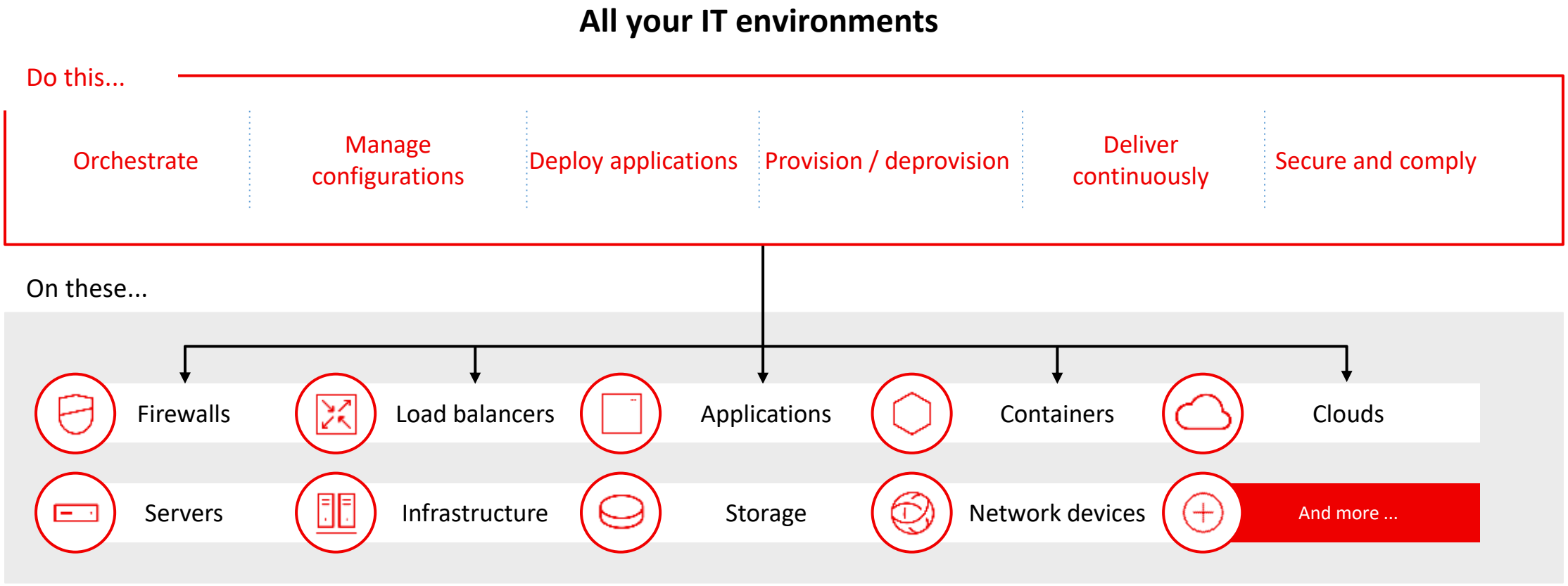
Growing number of use cases



Multiple platforms and locations

Across multiple domains

Red Hat Ansible Automation Platform



Red Hat Ansible usage with IBM Z and IBM LinuxONE

Ansible can be helpful to work with/automate the following IBM Z / IBM LinuxONE environments as well:

- Linux on IBM Z / IBM LinuxONE
- IBM z/VM
- KVM on IBM Z / IBM LinuxONE
- Red Hat OpenShift
- IBM Cloud Infrastructure Center

Developers, administrators, and operators can benefit from **pre-existing certified content** to build from, for both building and testing.

Ansible Content Collections

Ansible content can be created and managed internally for your organizations to use. However, curated content is also available from Red Hat through Ansible Content Collections. These collections provide developers with the option of building on curated automation content, which includes more than 100 certified collections and more than 40,000 modules.

- Ansible Content Collections
- Getting Started With Ansible Content Collections

Ansible automation hub

This hosted service is the place for users to find and use supported Ansible Content Collections, which contains modules, roles, and plug-ins, along with the documentation needed to get started.

- Ansible automation hub

Red Hat Ansible Certified Content for IBM z/OS environment

IBM CICS® TS Operator collection provides automation for provisioning CICS TS on one or more z/OS endpoints and managing its lifecycle in a hybrid cloud environment.

IBM z/OS IMS collection supports tasks such as generating IMS Database Descriptors (DBD), Program Specification Blocks (PSB), Application Control Blocks (ACB), and running IMS type-1 & type-2 commands.

IBM Operator Collection SDK provides the automation to deploy an operator in your namespace that contains your latest Ansible collection modifications, quickly redeploy your local modifications in seconds, and delete the operator once development is complete.

IBM Z Open Automation Utilities Operator collection provides automation for installing the ZOAU language on one or more z/OS endpoints and managing its lifecycle in a hybrid cloud environment. It uses the z/OS Package Manager to install the software on to z/OS and manage its lifecycle.

IBM z/OS core collection supports automation tasks submitting / querying jobs, creating / fetching / copying data sets, executing operator / TSO commands, ping, querying operator actions, backing up and restoring data sets / volumes, APF authorizing libraries, mounting file systems, running z/OS programs without JCL, initializing volumes, archiving / unarchiving / templating with Jinja, etc.

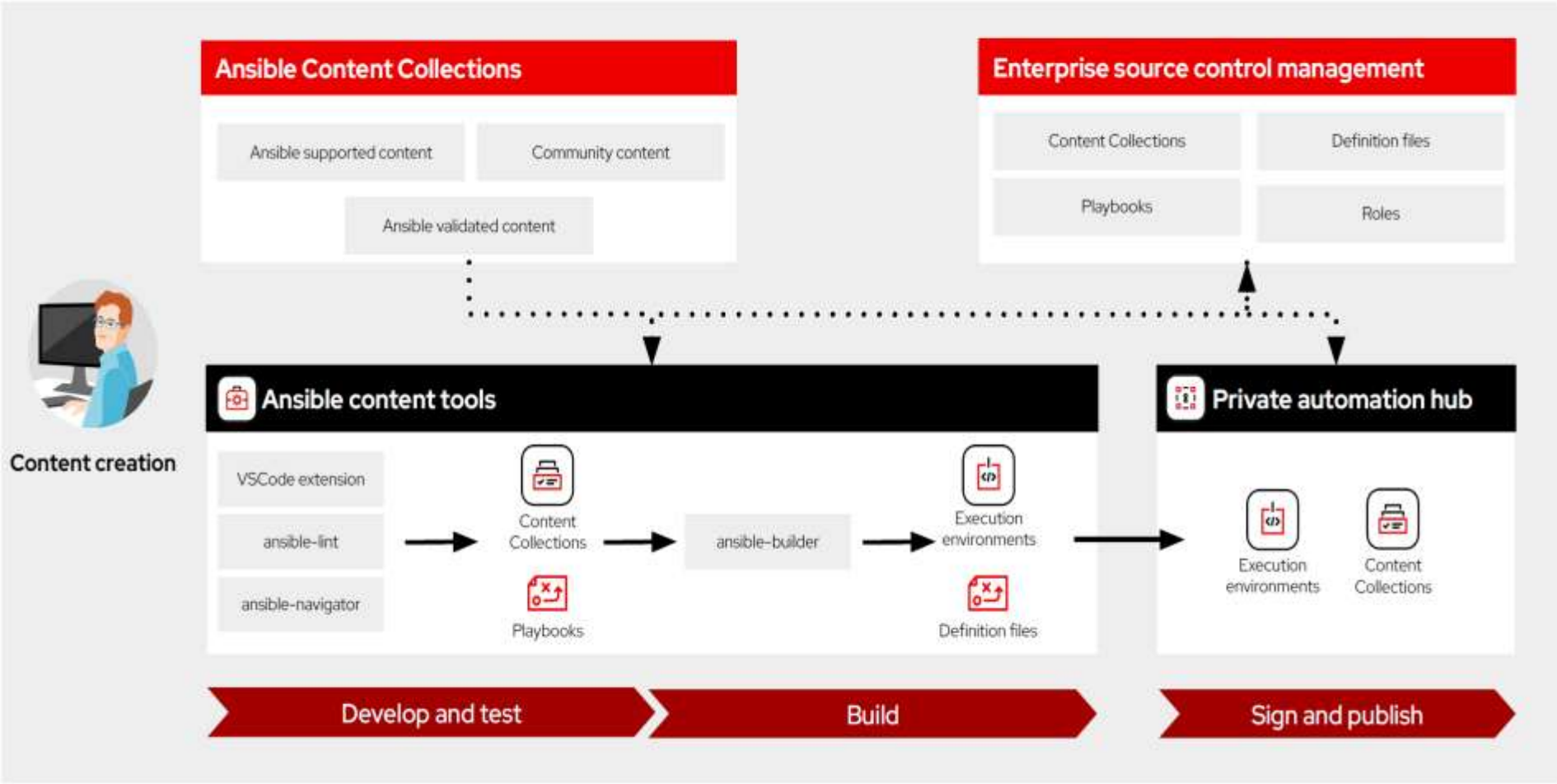
IBM Z System Automation collection supports operational tasks using the IBM Z System Automation Operations API such as creating and deleting dynamic resources from a template defined in the current active policy of an IBM Z System Automation environment. It interacts with IBM Z System Automation using the SA Operations API provided by the SA Operations REST Server.

IBM z/OS Package Manager collection provides automation for installing z/OS Package Manager and the z/OS products on one or more z/OS endpoints and managing their lifecycle in a hybrid cloud environment. IBM z/OS Package Manager is a utility that can install any z/OS software that is packaged as an OCI artifact on z/OS.

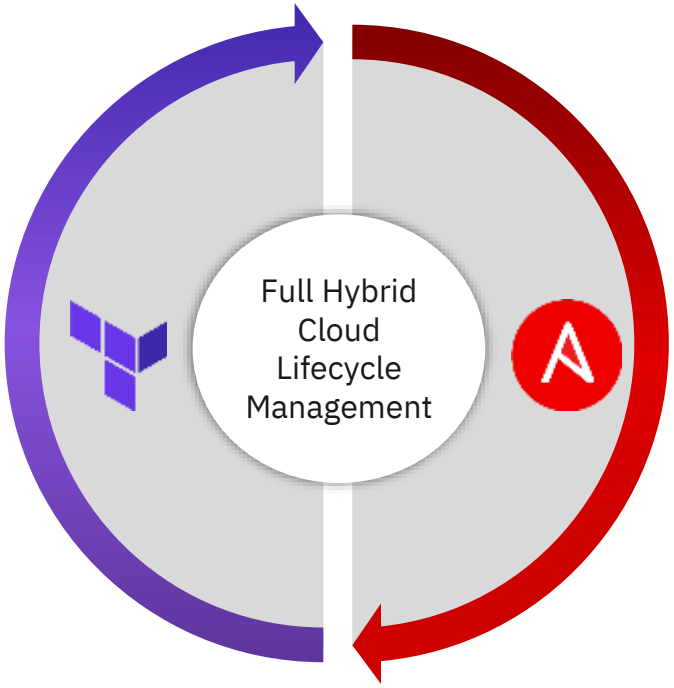
IBM z/OSMF collection supports automation tasks such as operating z/OS workflows, provisioning and managing z/OS middleware / software, via z/OSMF RESTful services.

Red Hat Ansible Automation Platform

The automation content life cycle.



Build and manage infrastructure as code with Teraform and use Ansible in conjunction, for a global automation

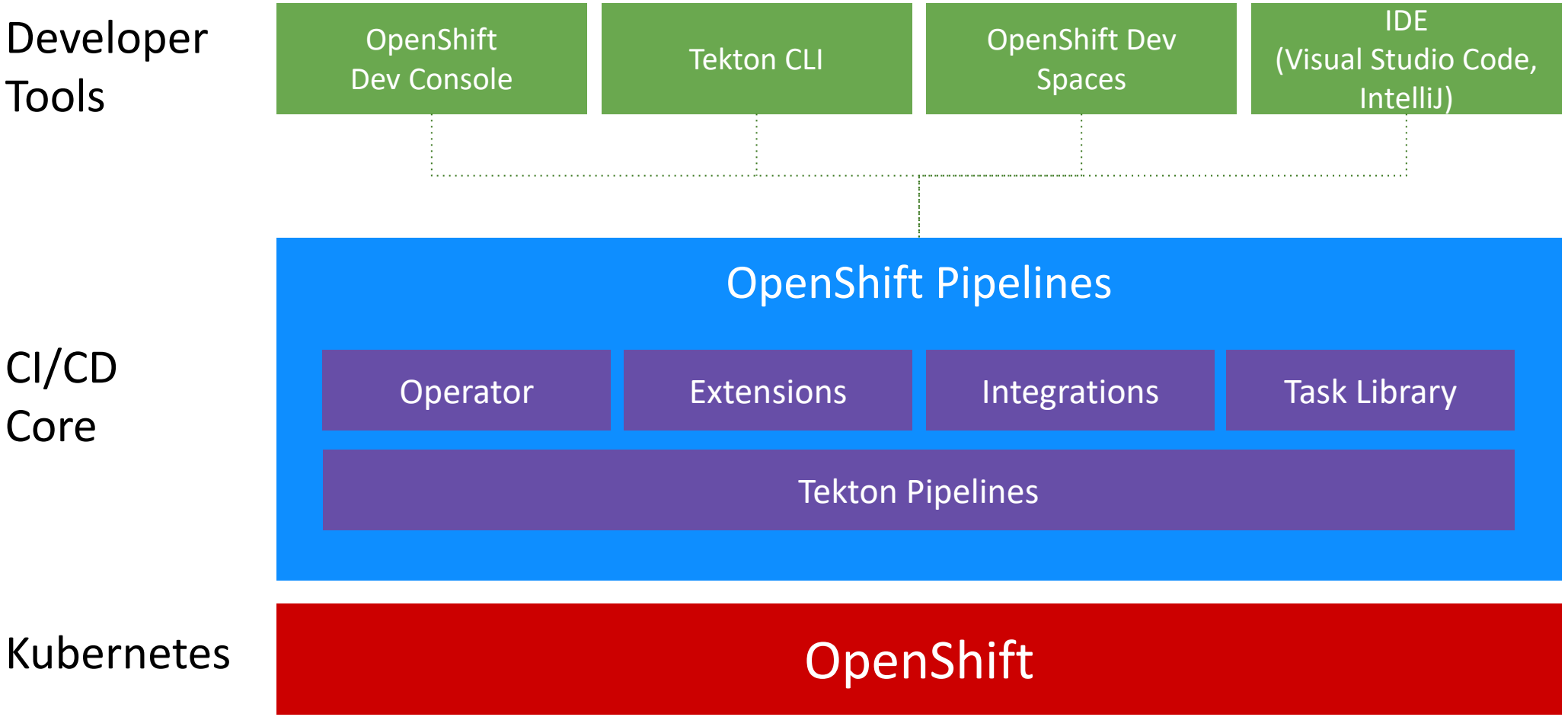


IBM Terraform and Red Hat Ansible provide full Hybrid Cloud lifecycle management to build and manage applications and the supporting infrastructure

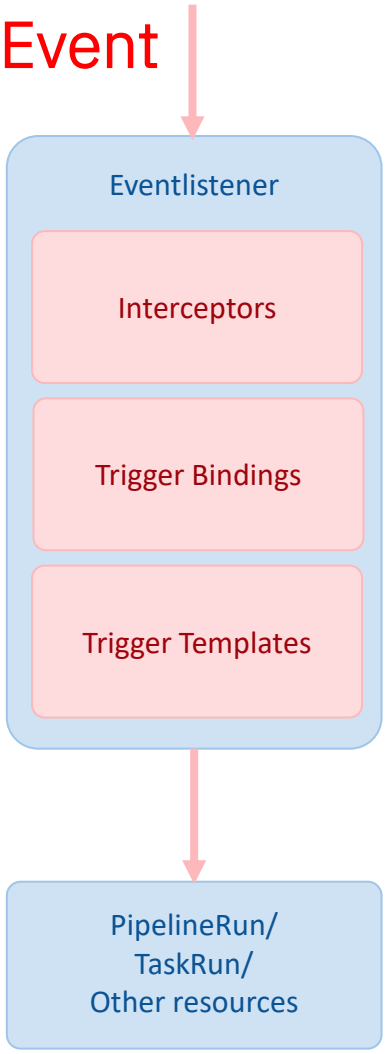
This combination of best of breed tooling provides a consistent, reliable, and scalable path to automation, accelerating ROI, while decreasing costs, complexity and risk

Centralized integrated RH OpenShift Automation

- using **OpenShift Pipelines (Tekton)**



Main Concepts of OpenShift Pipeline Triggers



Trigger

Start pipelines based on events: GitHub Webhooks Gitlab events, Cron jobs Custom event

Event Listener

A listener for events, which transforms them into some actions

Interceptor

An event processor for filtering, verification and transformation

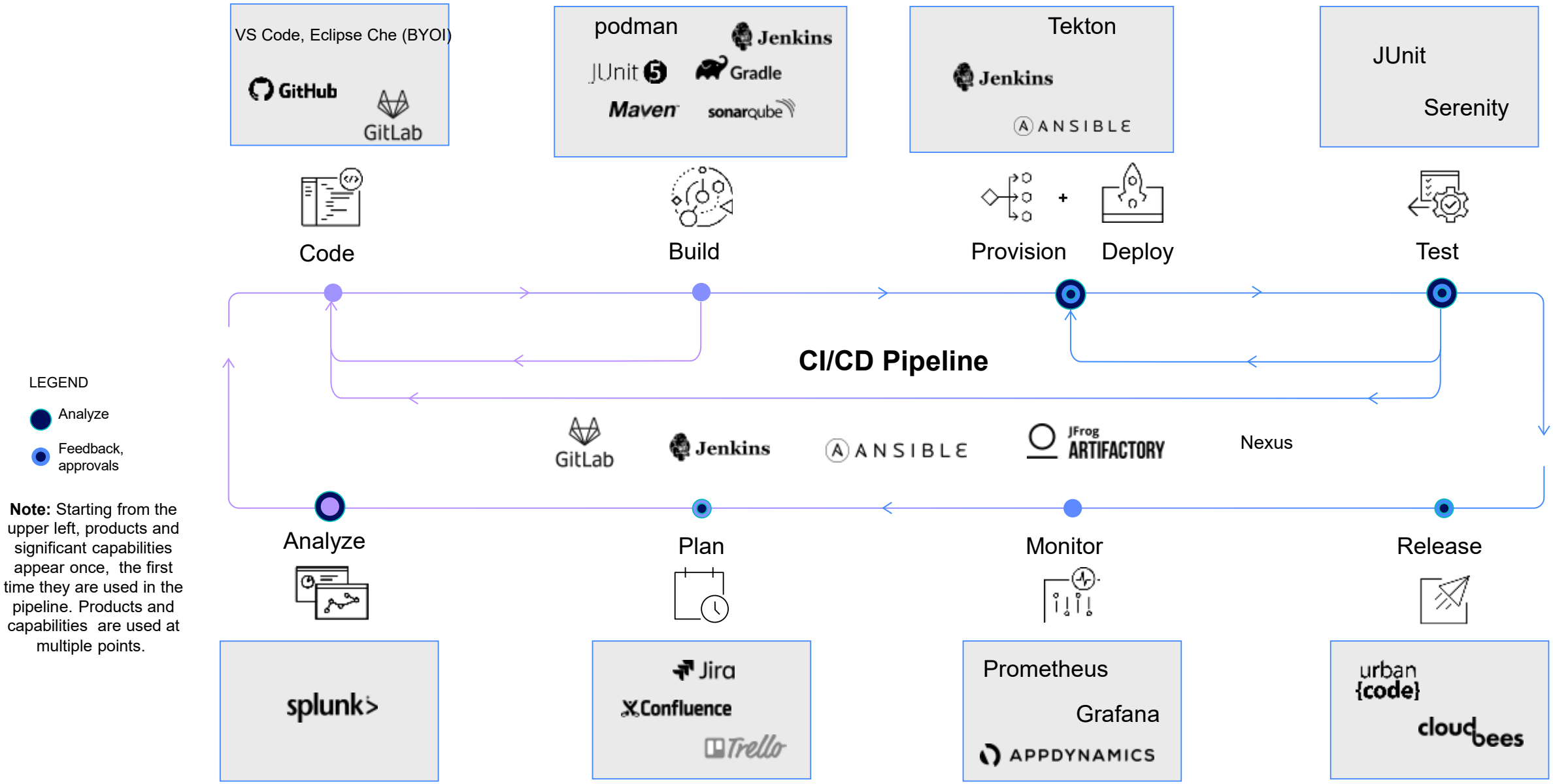
Trigger Binding

A mapping between event payload and Trigger Template parameters

Trigger Template

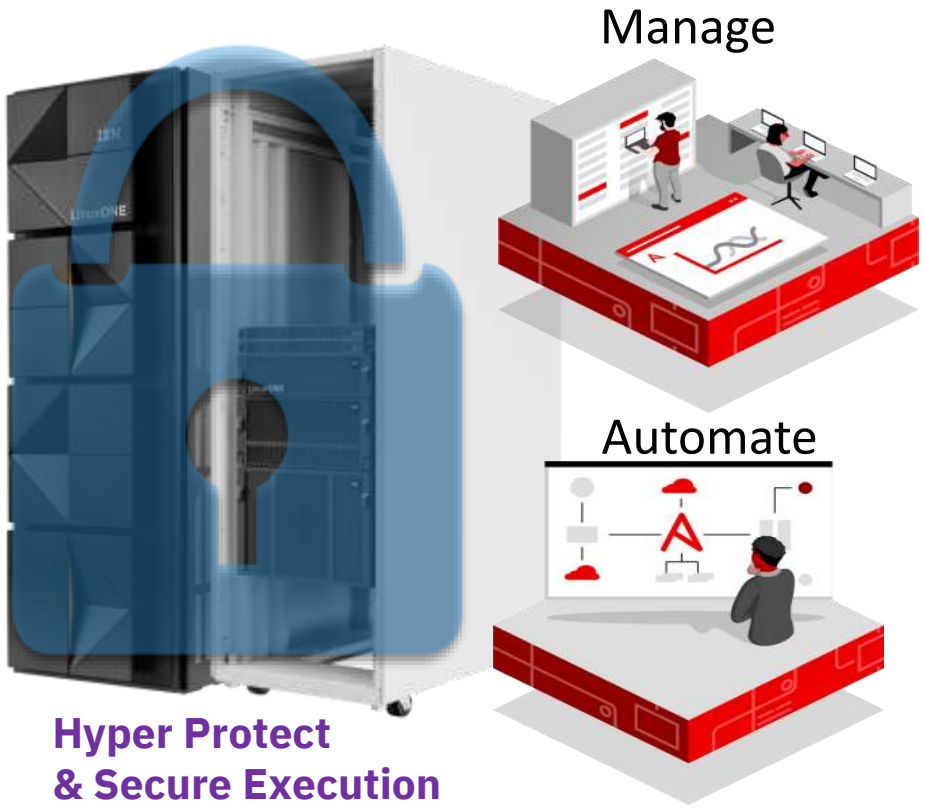
A template for resource to create based on event info

DevOps and CI/CD integrate well with Ansible



Note: Starting from the upper left, products and significant capabilities appear once, the first time they are used in the pipeline. Products and capabilities are used at multiple points.

Conclusion: Exploit IBM LinuxONE as Management and Automation Hub



High benefit with inheritance of LinuxONE characteristics:

- Security
- Scalability
- Resiliency

Goal: Centralized Common toolset

- Infrastructure management for IBM Z & LinuxONE with **Teraform & IBM Cloud Infrastructure Center (ICIC)**
- Hybrid Multi-Architecture Multi Cloud management using **RH Advanced Cluster Management for Kubernetes**
- Centralized Enterprise Automation management using **Teraform or RH Ansible Automation Platform on IBM Z & LinuxONE**
- Centralized integrated RH OpenShift Automation using **OpenShift Pipelines**

Experience more with IBM

Visit us at SHARE IBM Booth #113

After a full day of technical sessions, take a break with us!

Connect with our experts, snap a photo with the z17 Plexi or the latest Telum II, and get an up-close look at our Spyre Accelerator.

Come back each day for fresh topics and demos at our expert stations.

Think 2026

Join 5000+ senior business and technology leaders who are seizing the AI revolution to unlock unprecedented growth and productivity at Think 2026.

Find out more information using the QR code below.

IBM Digital Asset Haven

IBM Digital Asset Haven is the operational backbone for financial institutions and regulated enterprises entering the digital asset economy.

Find out more information using the QR code below.

Your feedback is important!

SHARE
EDUCATE • NETWORK • INFLUENCE

Submit a session evaluation for each session you attend:

www.share.org/evaluation

Questions?

Wilhelm Mild

IBM Executive IT Architect

The Open Group Open Certified Distinguished Architect — IT Architecture Chief/Lead IT Architect

IBM

IBM Deutschland Research & Development GmbH
IBM Campus 1
71139 Ehningen
Germany

wilhelm.mild@de.ibm.com

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

BLU Acceleration*	IBM Z*	MQ*	WebSphere*	Z14	z/VM*
CICS*	InfoSphere	Spectrum Scale	XIV*	z/OS*	z/VSE*
Db2*	LinuxONE	Storwize*	z13*	z Systems*	
IBM*	Maximo*	System Storage*	z13s*		
IBM (logo)*	MobileFirst	Tivoli*			

* Registered trademarks of IBM Corporation

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.
ITIL is a Registered Trade Mark of AXELOS Limited.
Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
UNIX is a registered trademark of The Open Group in the United States and other countries.
VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.
Other product and service names might be trademarks of IBM or other companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.
This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g, zIIPs, zAAPs, and IFLs) ("SEs"). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the “Authorized Use Table for IBM Machines” provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html (“AUT”). No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

Notices and disclaimers

- © 2019 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.
- **U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**
- Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.
- IBM products are manufactured from new parts or new and used parts.
  In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."
- **Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**
- Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those
- customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
- References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.
- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
- It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers continued

- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**
- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.
- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml