Red Hat

Tech Day

The Netherlands | 2025

Red Hat

TechTalks

Tech Day the Netherlands 2025

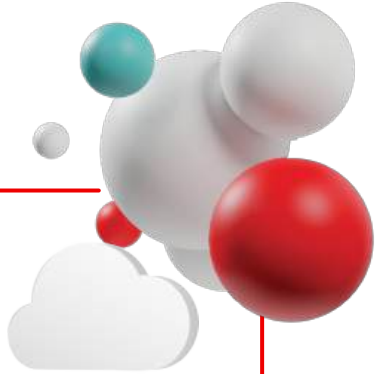
Marcel Timmer

Country Manager

Red Hat the Netherlands

Red Hat Summit: Connect 2025

15 October 2025, NBC Nieuwegein. Save the date!



Red Hat

Agenda

9.00 - 9.45	Keynote
9.45 - 10.30	Presentations
10.30 - 11.00	Coffee Break
11.00 - 12.30	Presentations & workshops
12.30 - 13.15	Lunch
13.15 - 14.45	Presentations & workshops
14.45 - 15.15	Coffee Break
15.15 - 17.00	Presentations & workshops
17.00 - 18.30	Networking drinks & appetizers

Red Hat

Red Hat

TechTalks

Today’s challenges

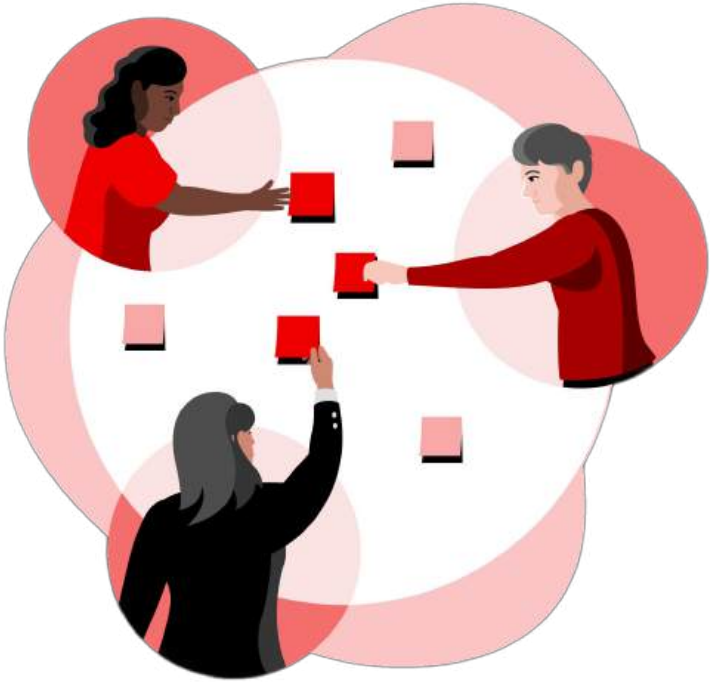
The need for independence

Security threats

Red Hat

Keep your options open

Artificial Intelligence



Red Hat

Red Hat

TechTalks

Tech Day the Netherlands 2025

Karanbir Singh

Senior Distinguished Engineer

Red Hat

The very hungry caterpillar

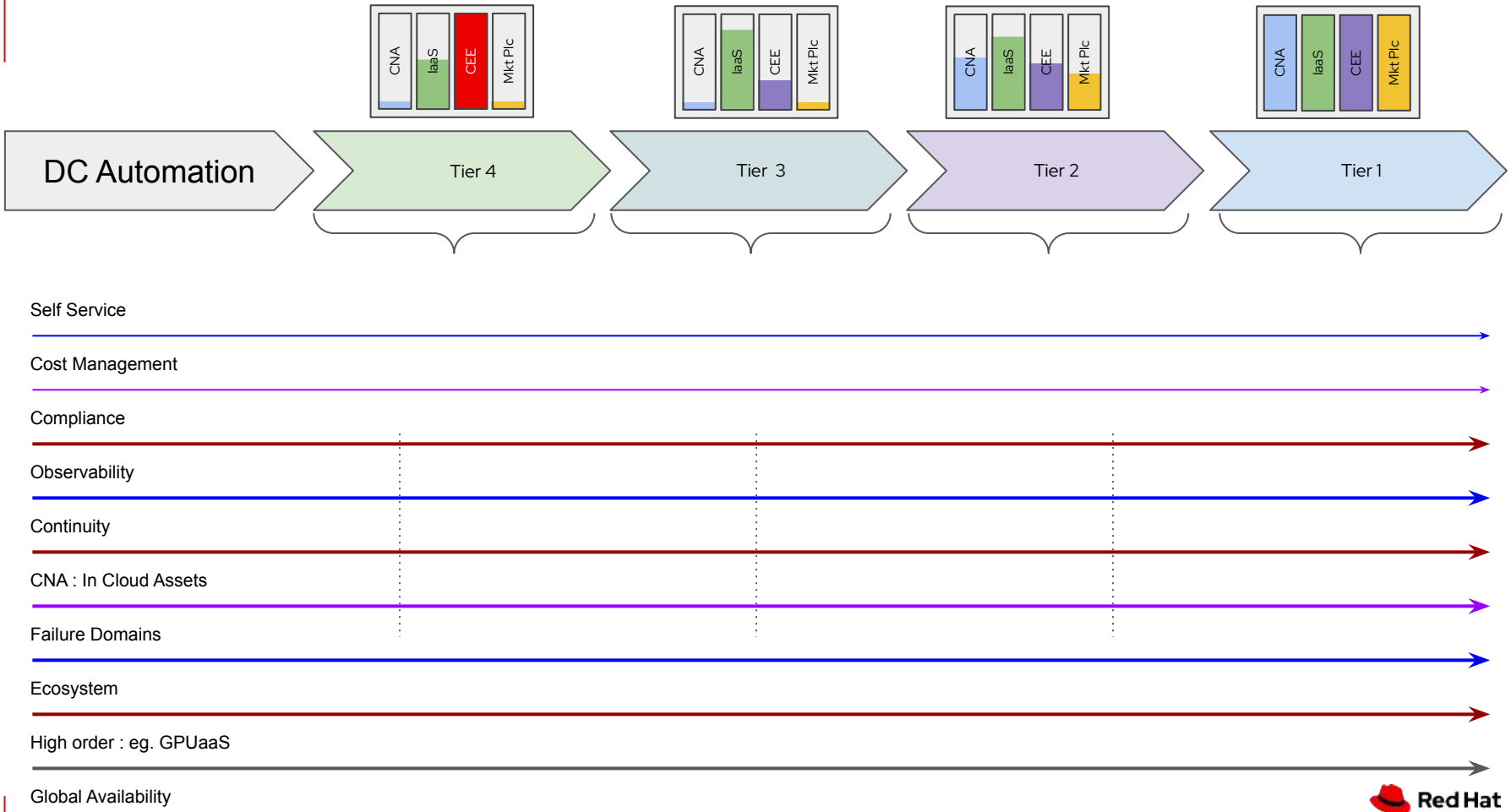
A story about modern infrastructure

Karanbir Singh, Senior Distinguished Engineer
Red Hat (UK) Ltd

Red Hat

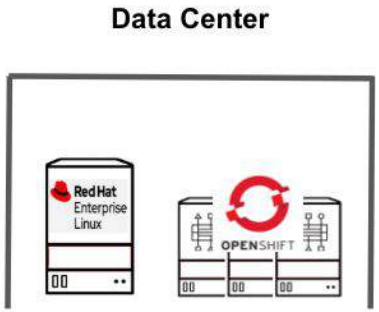
Systems are getting complex

Systems are getting complex

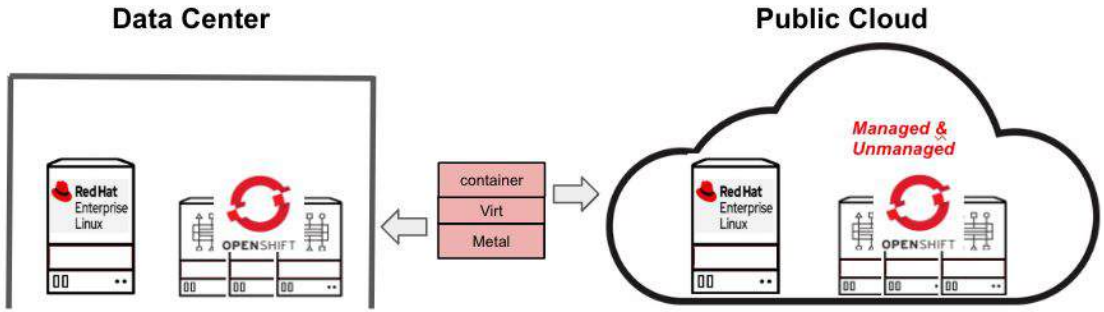


Red Hat

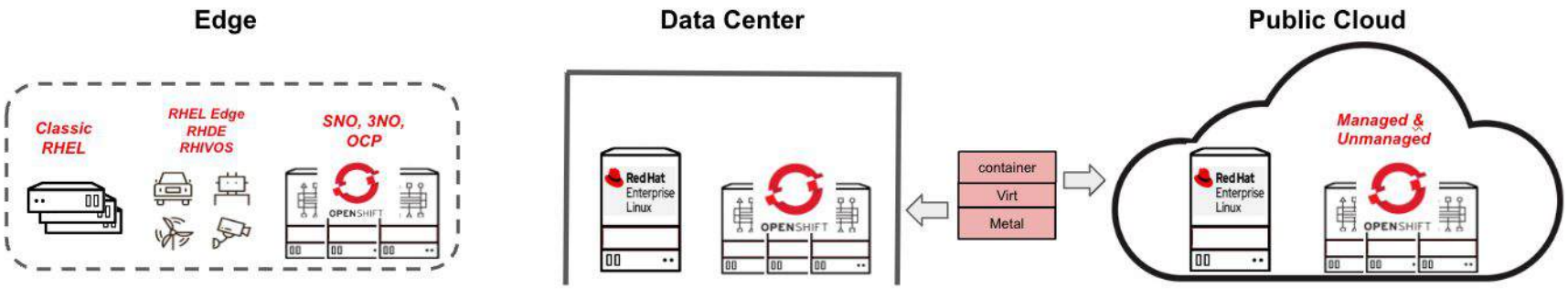
Management Topology



Management Topology

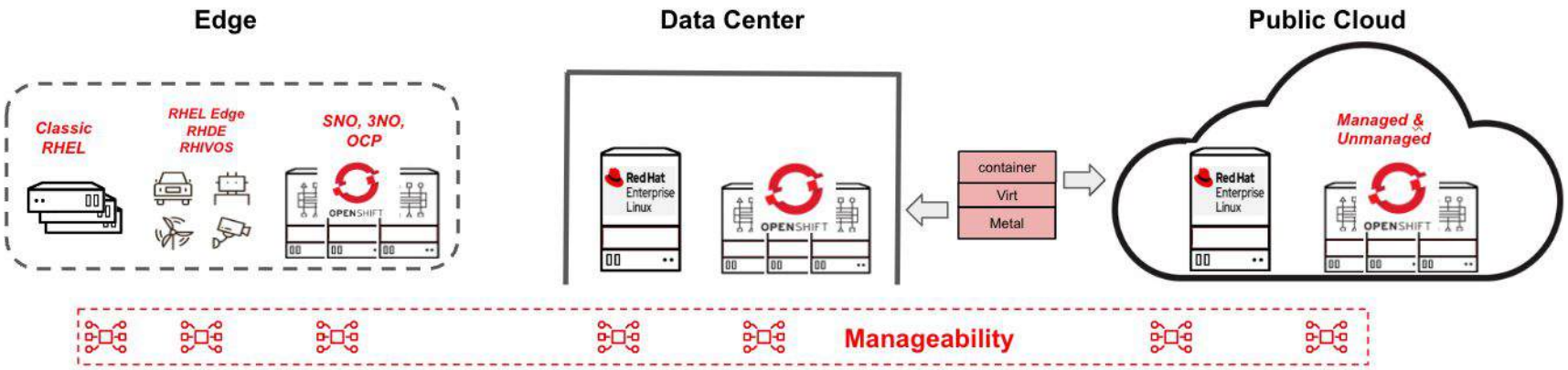


Management Topology



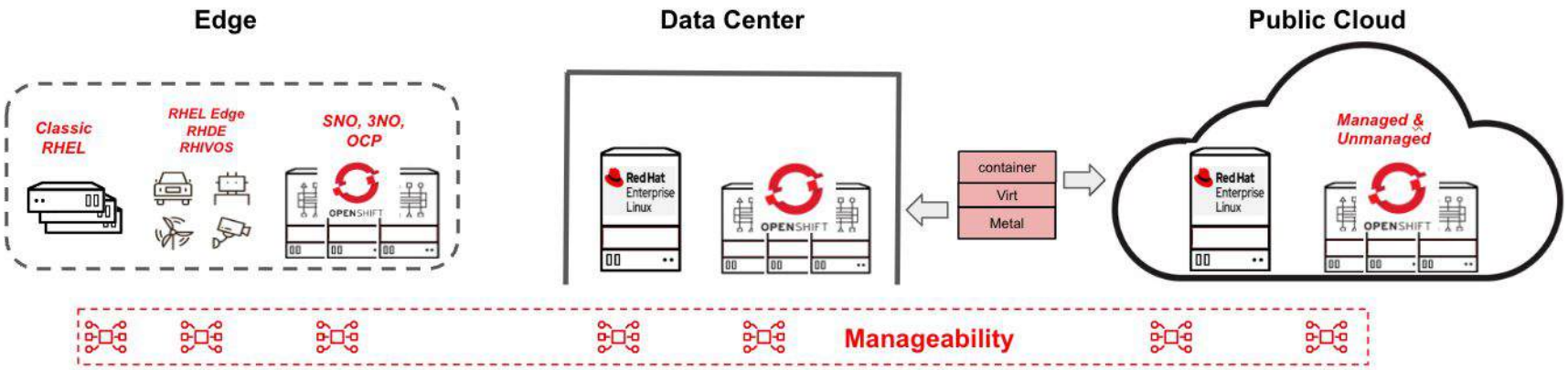
Red Hat

Management Topology



Red Hat

Management Topology



Management Capabilities

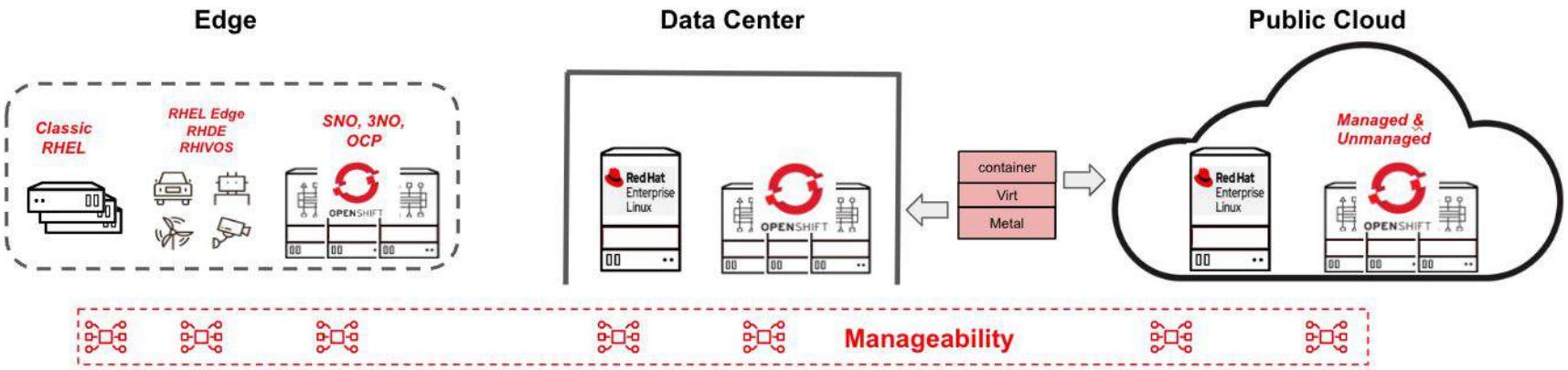
Lifecycle	Inventory	Configuration	Security	Automation	Continuity	Observability	Cost

Integration / Ecosystem

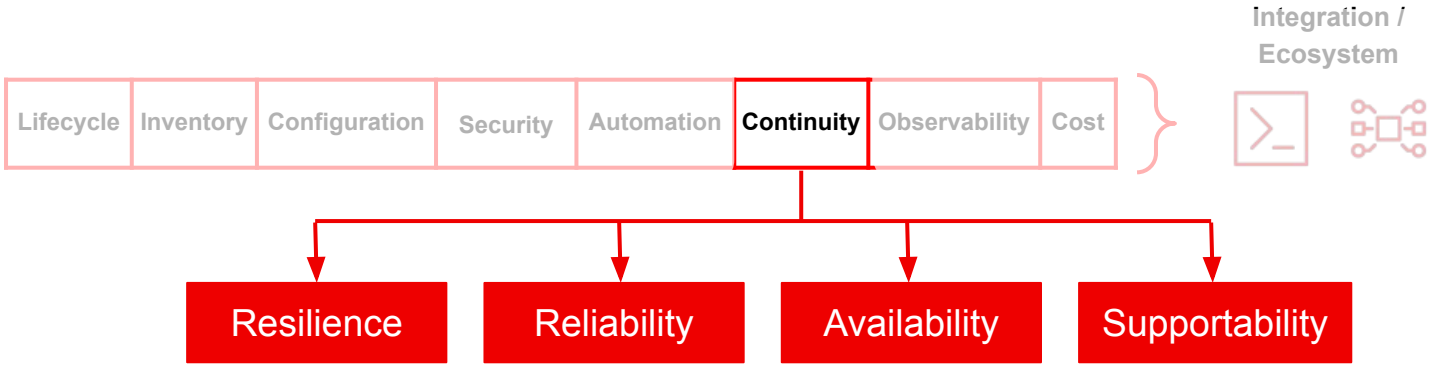
Operations
(IT Operators, Infrastructure Engineers, SREs, etc.)

Red Hat

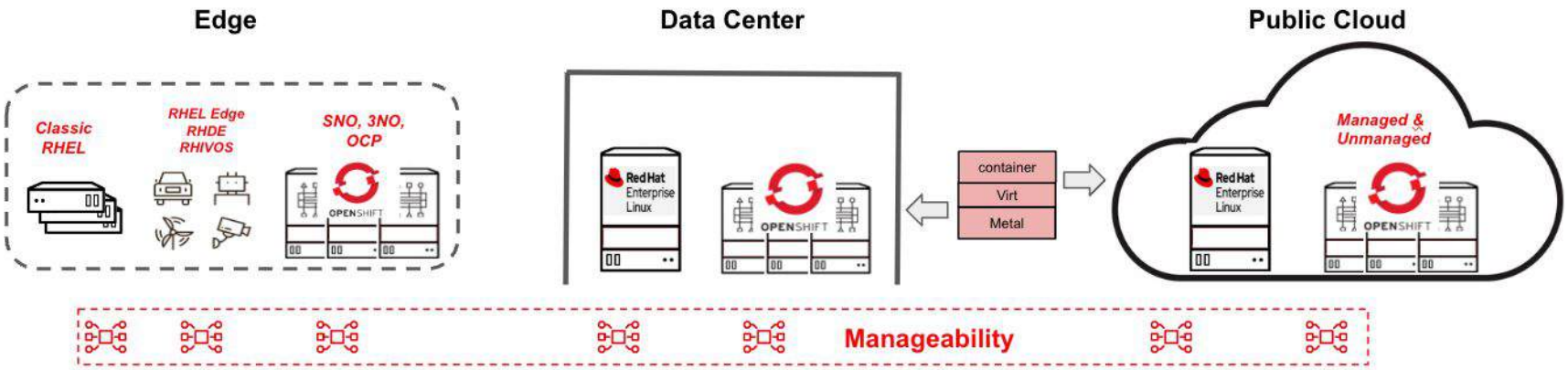
Management Topology



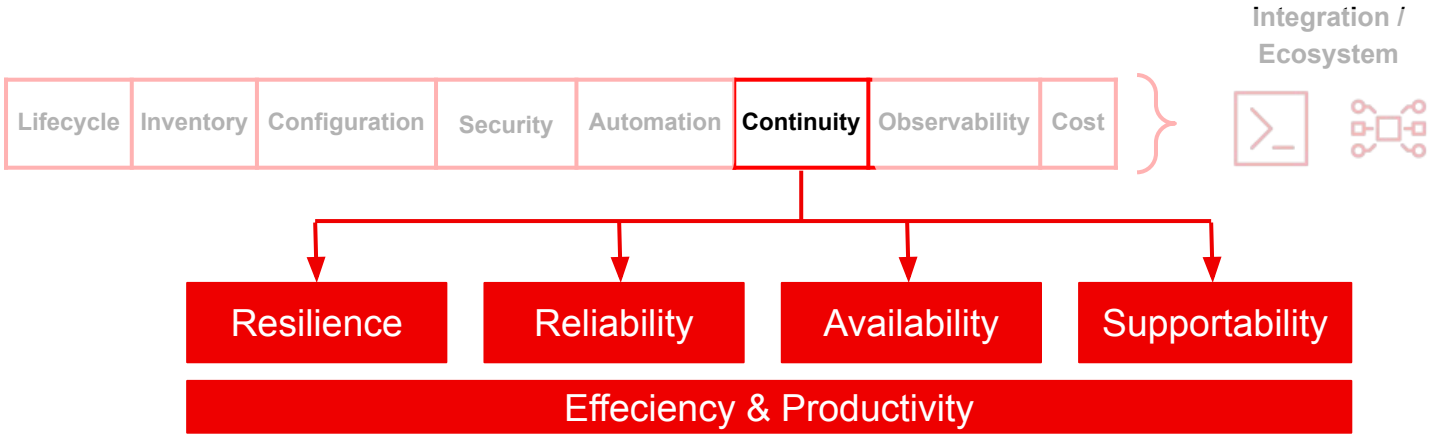
Management Capabilities



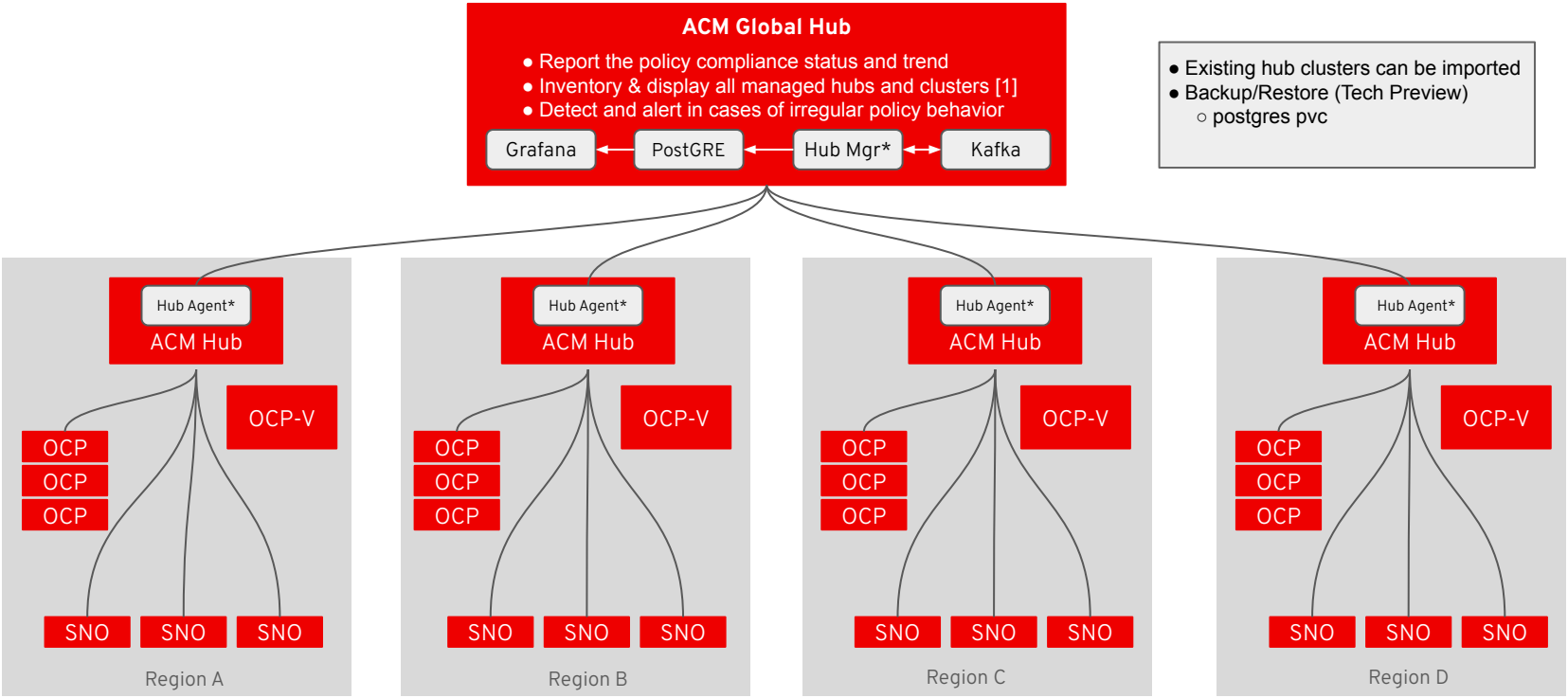
Management Topology



Management Capabilities



ACM Global Hub Architecture



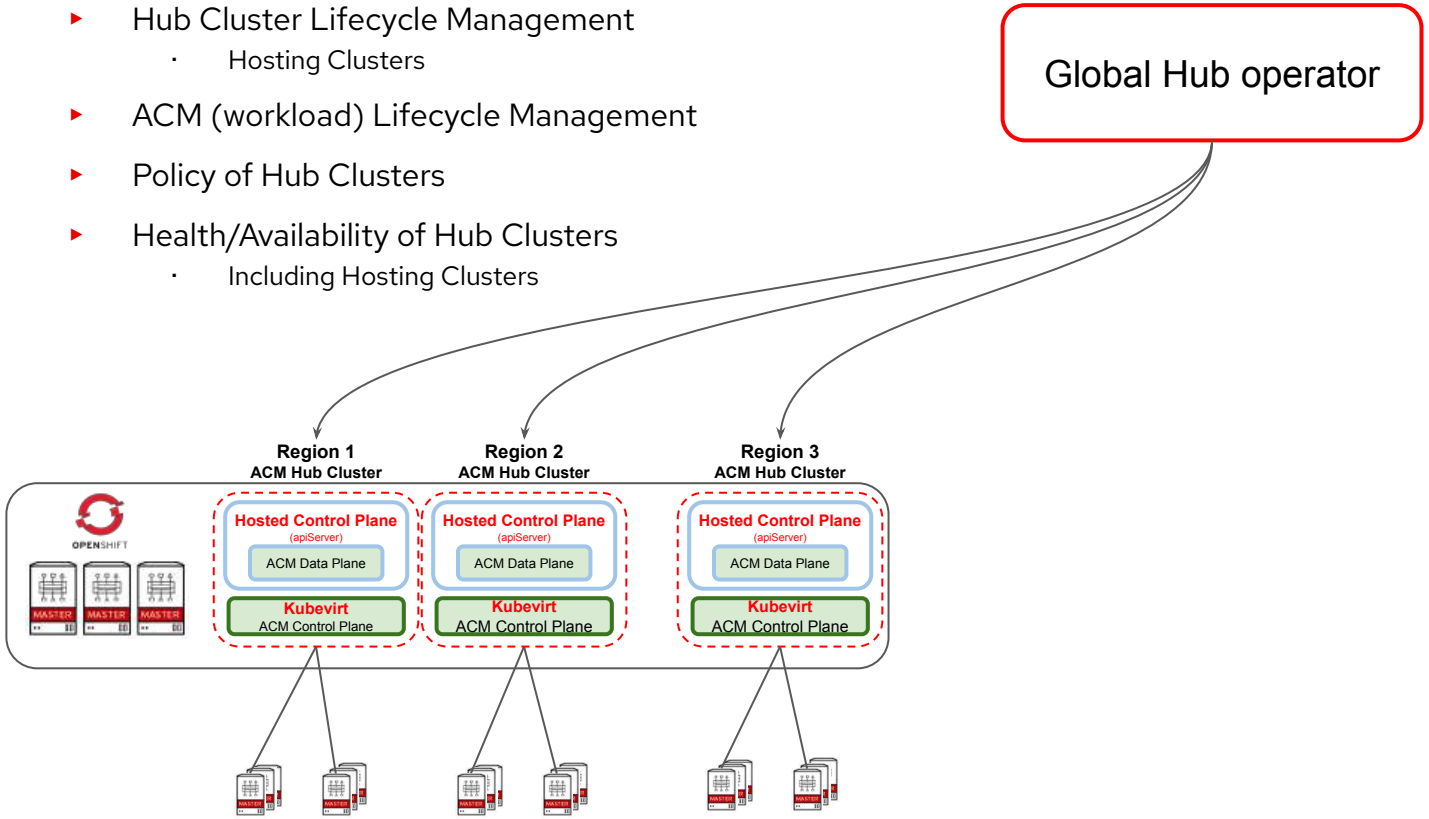
[1] Global Inventory Search View technical preview now - ACM 2.11 (OCP 4.16)
*

ACM Global Hub Documentation

Red Hat

Managing ACM Hub Cluster : Optimising for operational outcomes, prevent sprawl, reduce cost of execution

- Hub Cluster Lifecycle Management
  - Hosting Clusters
- ACM (workload) Lifecycle Management
- Policy of Hub Clusters
- Health/Availability of Hub Clusters
  - Including Hosting Clusters

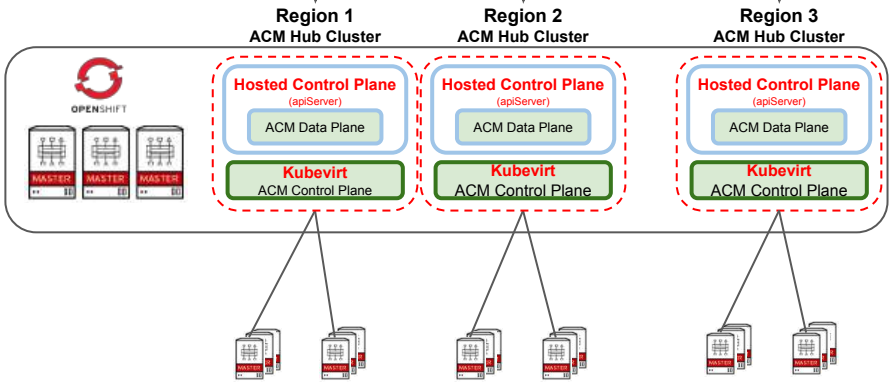


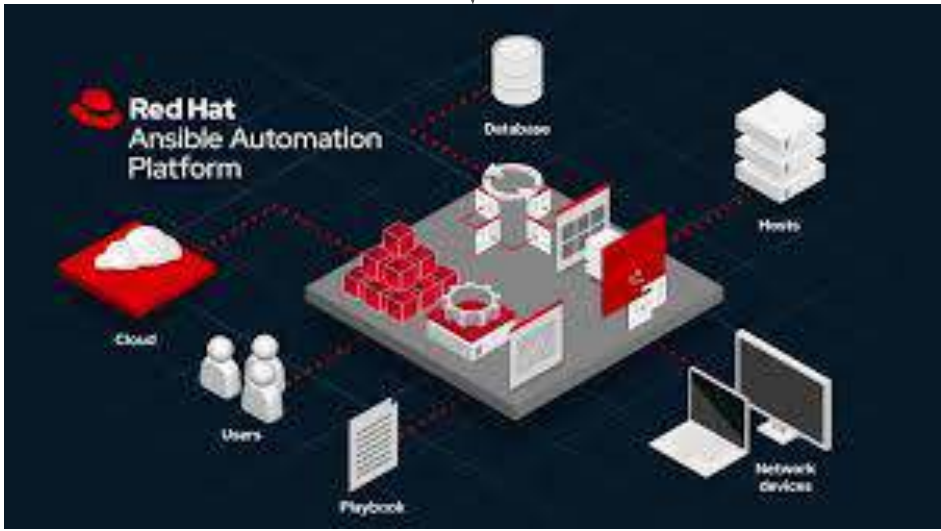
Cluster Number: 1..2000 2001..4000 4001..6000

Managing ACM Hub Cluster : Optimising for operational outcomes, prevent sprawl, reduce cost of execution

- Hub Cluster Lifecycle Management
  - Hosting Clusters
- ACM (workload) Lifecycle Management
- Policy of Hub Clusters
- Health/Availability of Hub Clusters
  - Including Hosting Clusters

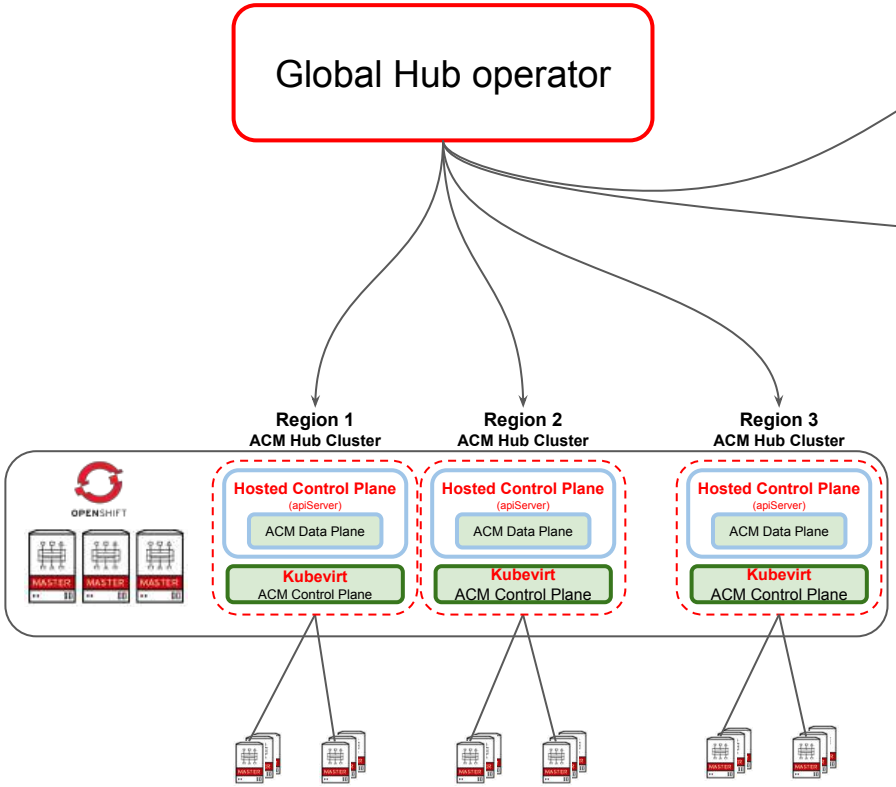
Global Hub operator

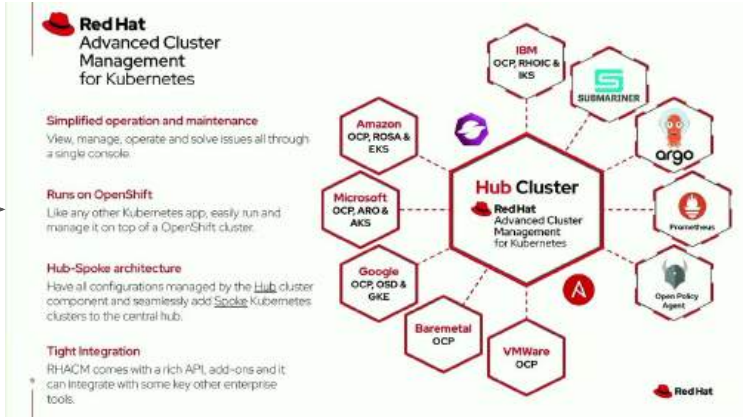


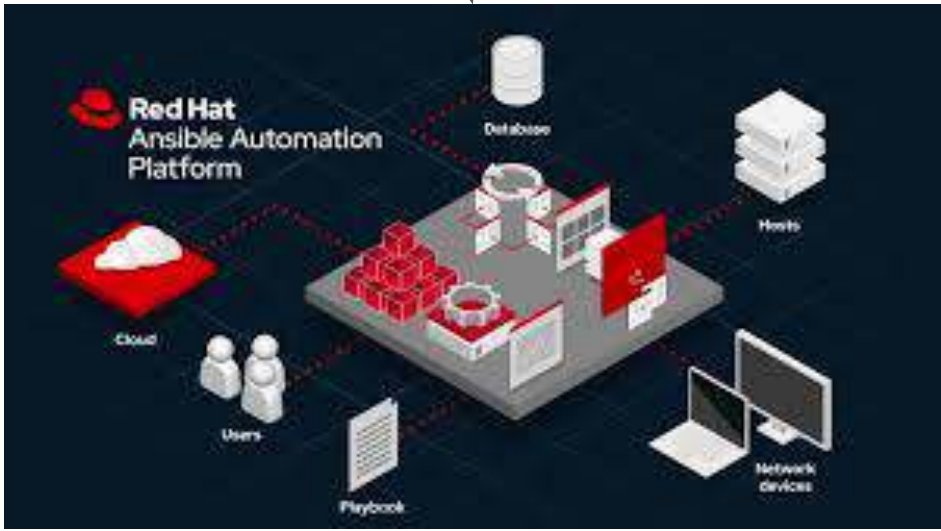


Cluster Number: 1..2000 2001..4000 4001..6000

Managing ACM Hub Cluster : Optimising for operational outcomes, prevent sprawl, reduce cost of execution

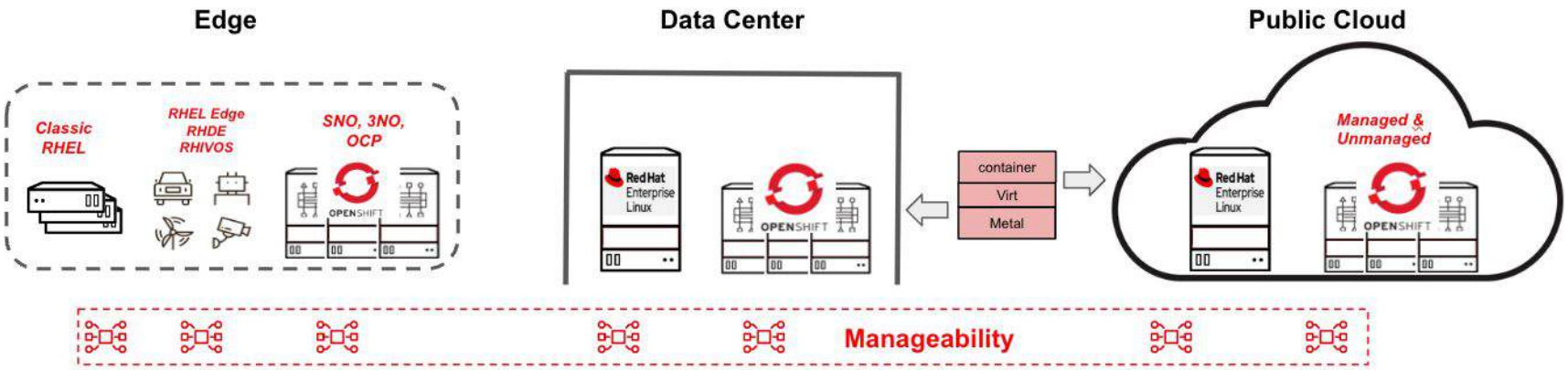




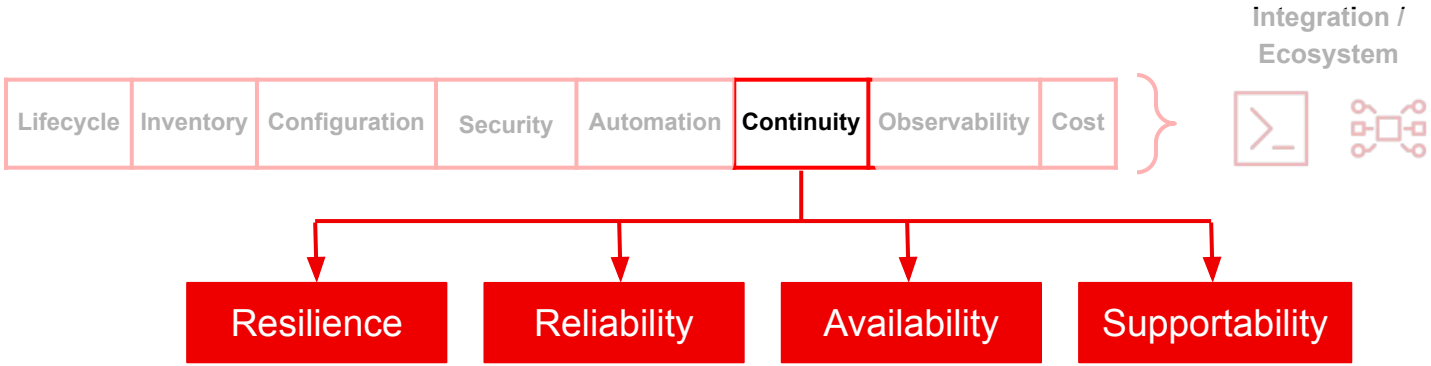


Cluster Number:	1..2000	2001..4000	4001..6000

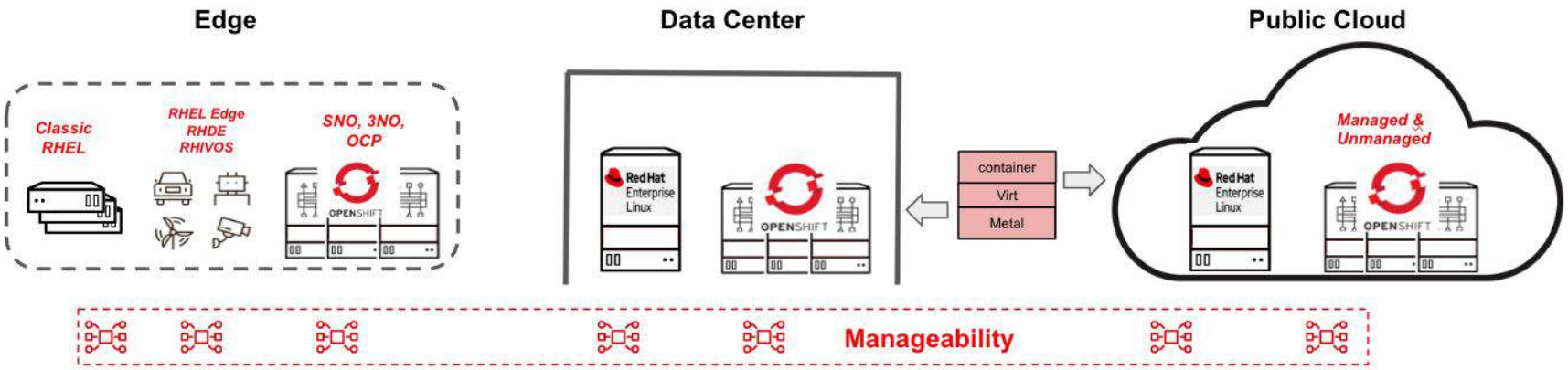
Management Topology



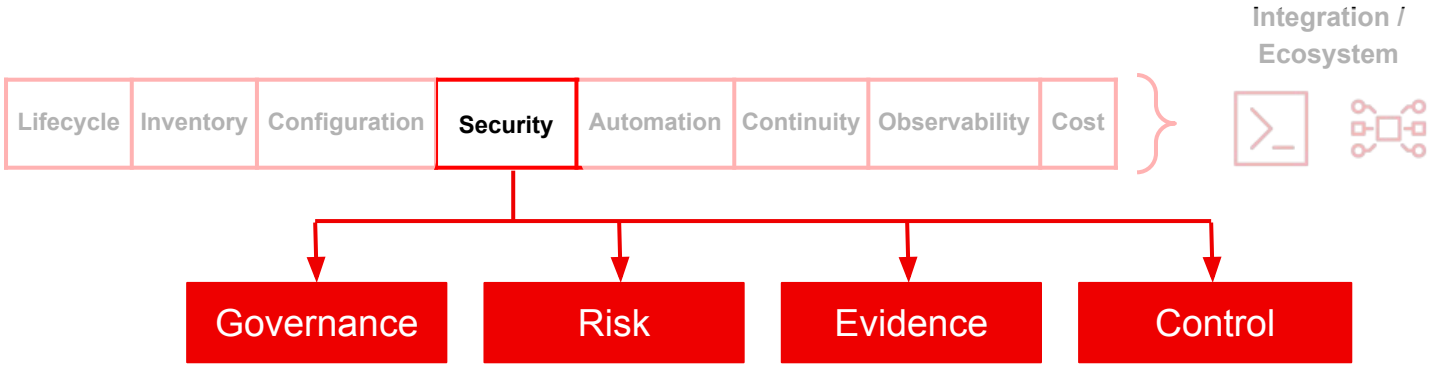
Management Capabilities



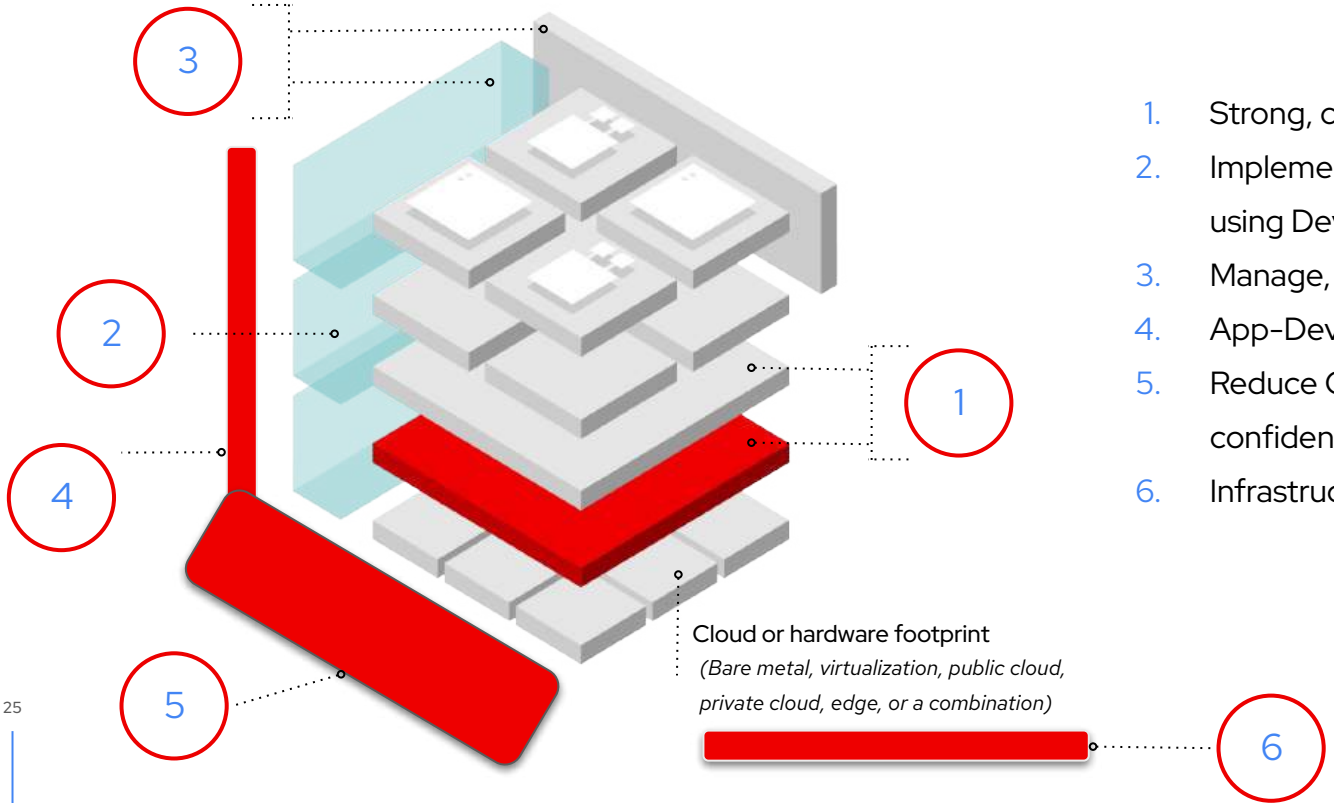
Management Topology



Management Capabilities



Red Hat's layered approach for e2e safety



1. Strong, complete foundation
2. Implement trusted software supply chain using DevSecOps practices
3. Manage, automate, secure, compliant
4. App-Dev Enablement
5. Reduce Cost and time, increase confidence in : Gov, Risk & Compliance
6. Infrastructure enablement : RHEL, OCP-V

Red Hat

Red Hat Enterprise Linux provides a secure foundation

From traditional to cloud-native platforms

Securable by Design Operating System

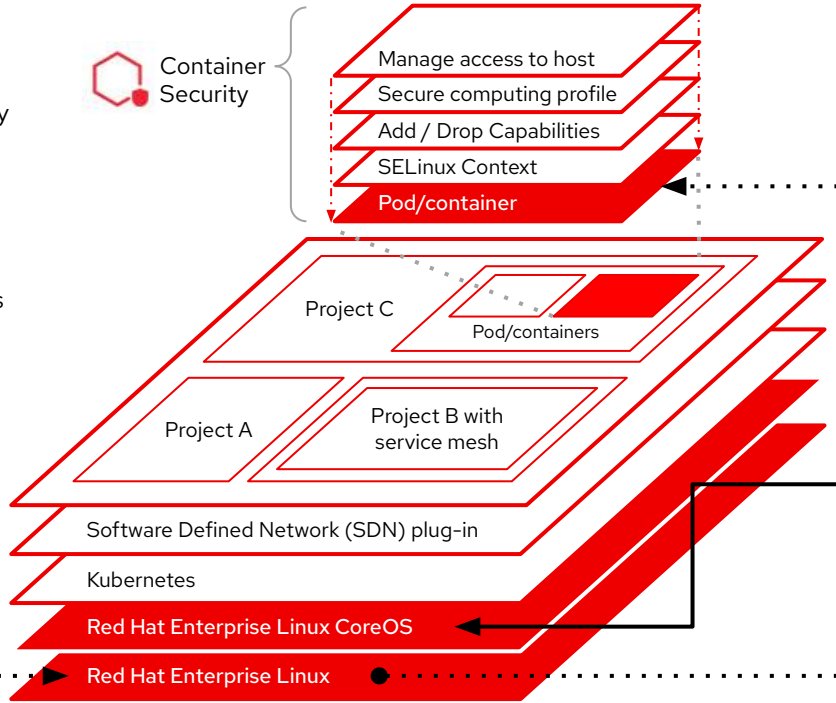
Secure boot enhanced with integrity measurement and remote attestation

Mandatory access control and multi-level security with SELinux

System-wide cryptographic policies and FIPS validated cryptographic libraries

Encrypting data at rest and in motion

Automated security and compliance configuration



Red Hat Universal Base Image containers can leverage RHEL trusted and maintained content

Hardened/Optimized Operating System

Reduced attack surface

Controlled immutability

Read-only user space

Transactional Updates

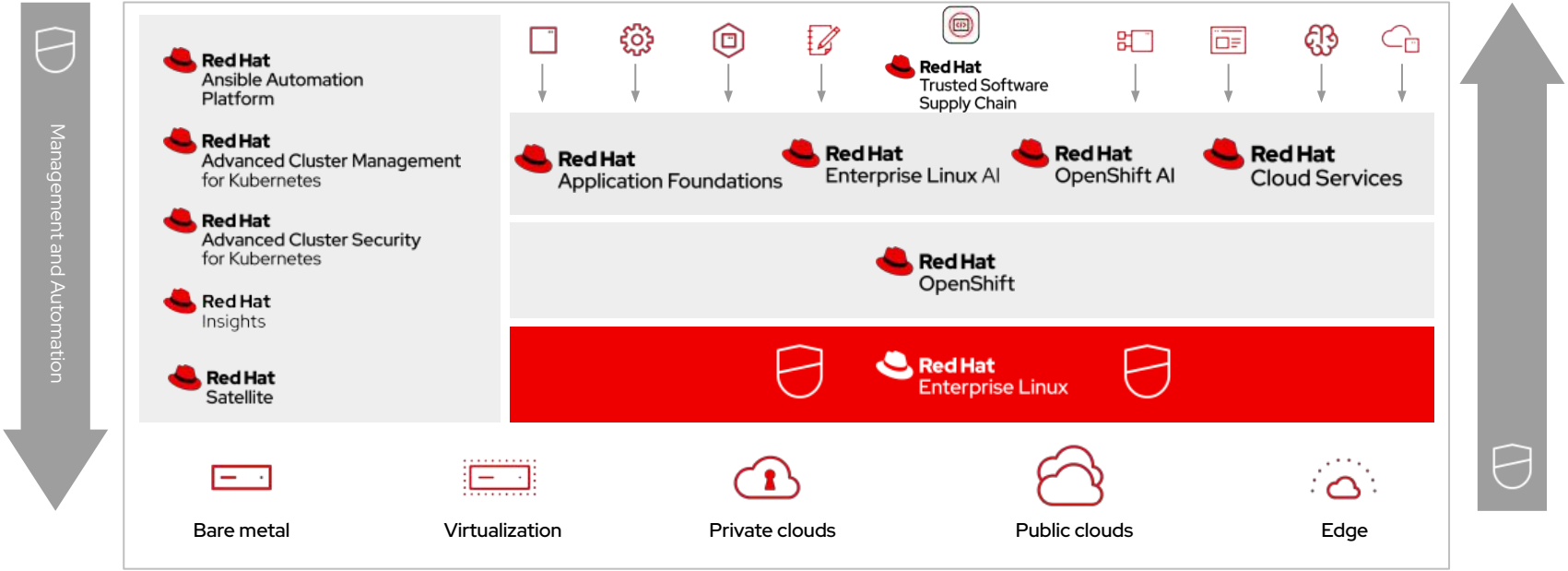
Secure Boot

Network Bound Disk Encryption

Red Hat

Layered security throughout the stack and lifecycle

Build, deploy, and run applications on top of a hybrid cloud using DevSecOps practices



Red Hat

Add Security by Design

Shift Left, Automate, Verify

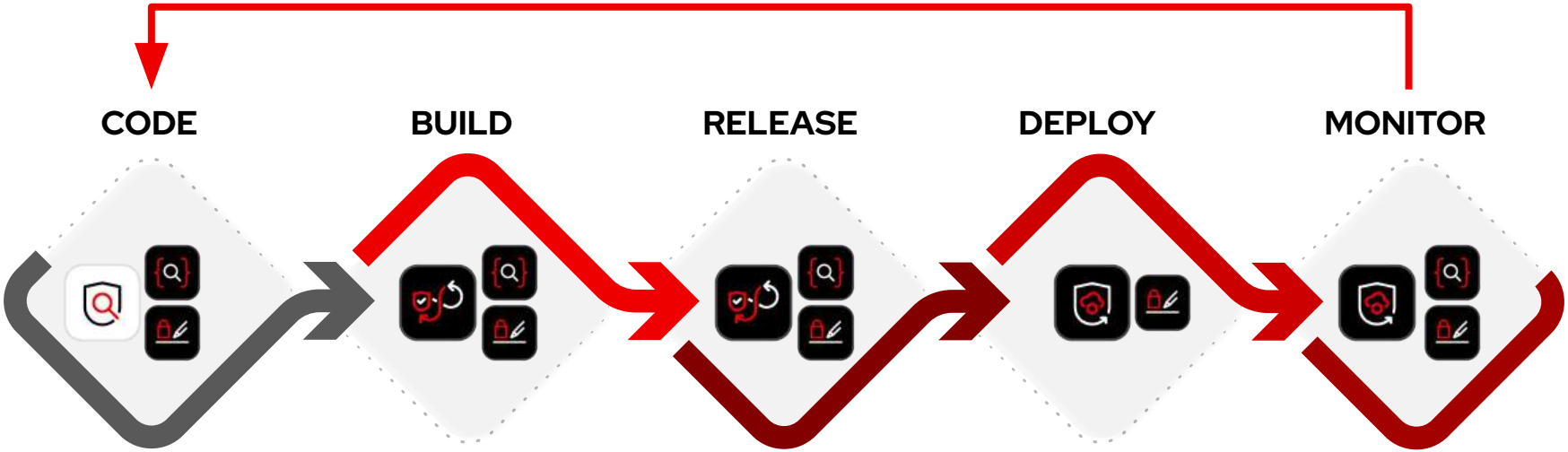
Traditional Security Approaches

- Manual Code Reviews – Human inspection of dependencies and source code
- Firewalls & Perimeter Security – Blocking threats at network entry points
- Checksum Verification – Verifying binary integrity (but rarely automated)
- Private Artifact Repositories – Hosting internal packages to reduce exposure

Modern Security Options (Today)

- SBOMs (Software Bill of Materials) – Visibility into components & dependencies
- Automated signing & verification, provenance & attestations with immutable ledger
- SLSA Framework – Secure software build pipelines with provenance guarantees
- Dependency Scanning Tools – Automated checks
- Reproducible Builds – Ensures builds can be verified independently
- Runtime Protection – Enforce policies at deploy or runtime

Trusted Software Supply Chain



Identify dependencies and recommend trusted content before coding

Provide guidance, templates, tools to catch known vulnerabilities and misconfigurations

Vulnerability Scanning

Policy Enforcement

Artifact Signing

Automate guardrails to prevent deployment of problematic code and deliver risk mitigation

Detect and respond to runtime threats with prioritized risk assessments

RH Trusted Profile Analyzer

RH Trusted Artifact Signer

RH Advanced Developer Suite

RH Advanced Cluster Security

Red Hat

Continuous Monitoring and Enforcement

Reduce noise, alert fatigue for shorter time to response

MONITOR

OSS
Risk
Profiles

Images
Containers
Clusters
Network

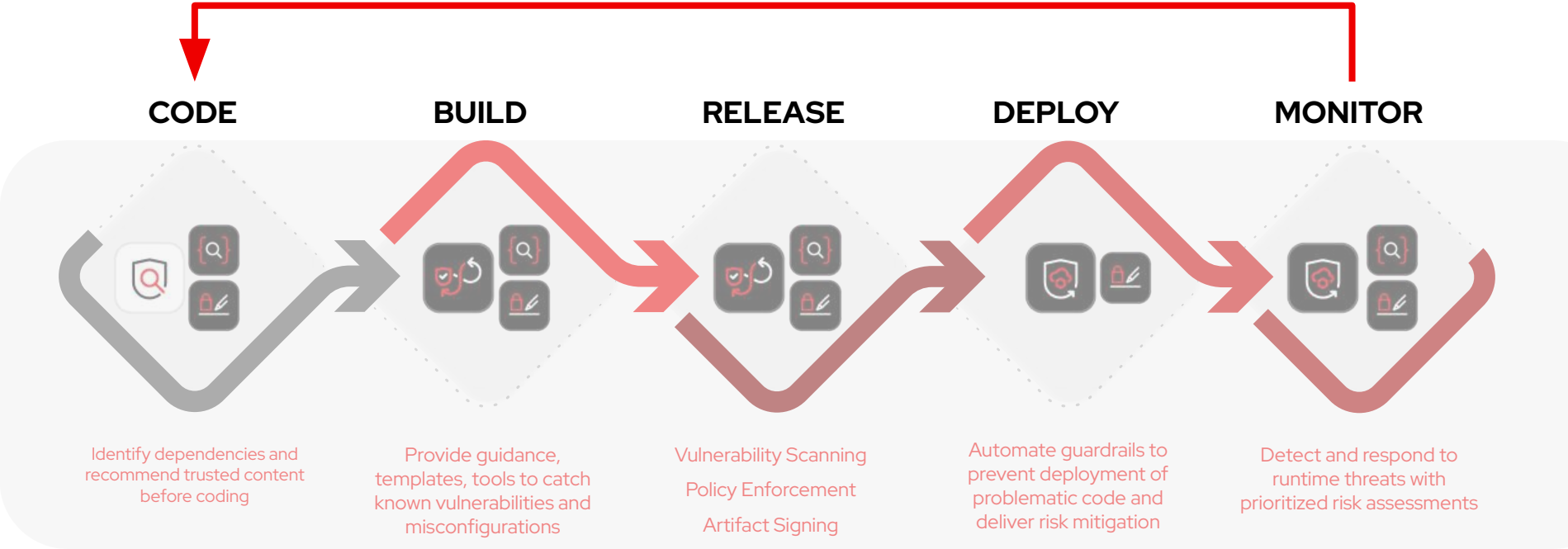
Process and network baselining

Anomaly Detection

Runtime enforcement

- Automate - Identity based signing, tamper proofing, enhanced transparency and auditability (RHTAS)
- Automate - Business standards as policy with multiple policy checks across the build pipeline
- Automate - Vulnerability detection and impact analysis, supply chain transparency, regulatory compliance (RHDA, RHTPA)
- Secures the full lifecycle—build, deploy, runtime—across hybrid clouds. (TSSC)
- Deep insights and risk ranking to focus on critical threats. (RHACS)
- Automates compliance (CIS, NIST, PCI) with streamlined operations. (RHACS)

End to End Security Guardrails



RH Trusted Profile Analyzer

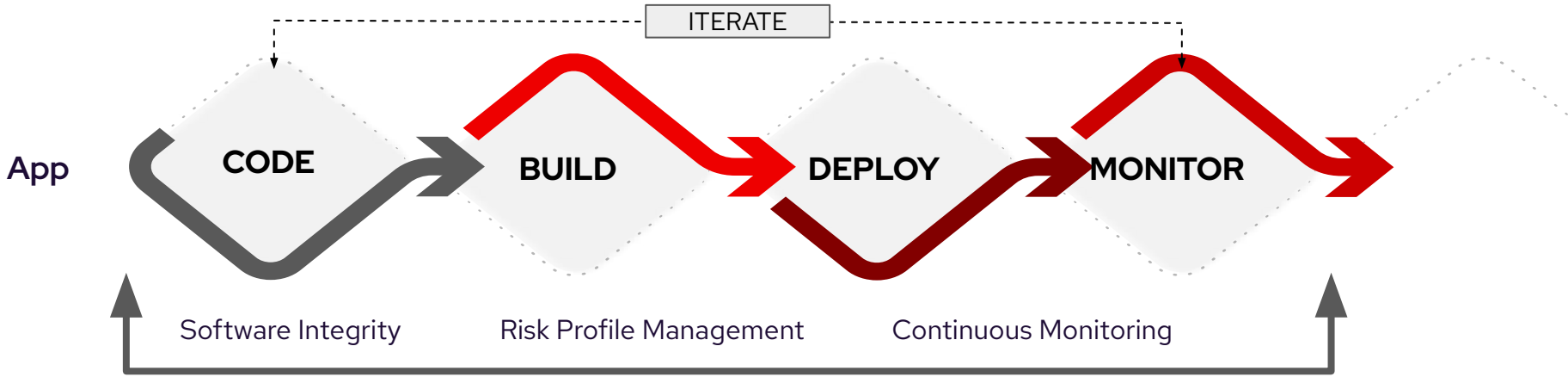
RH Trusted Artifact Signer

RH Advanced Developer Suite

RH Advanced Cluster Security

Red Hat

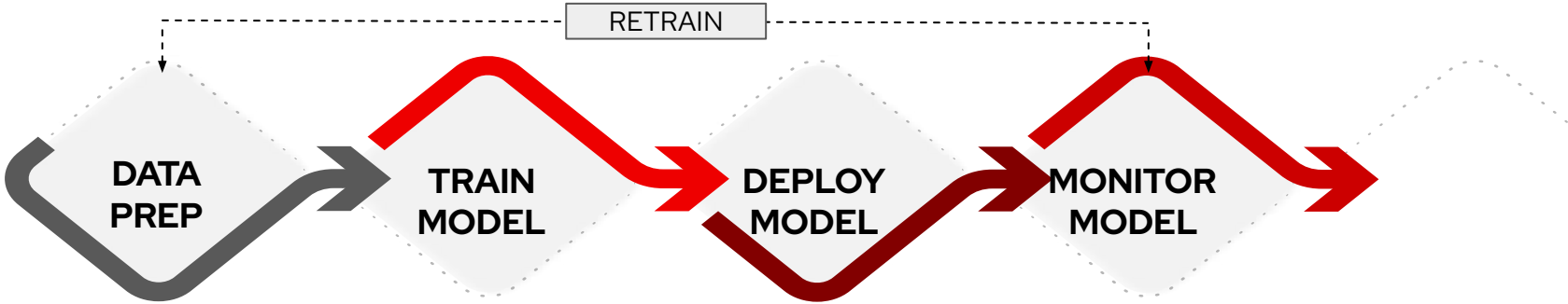
Software Development Life cycle



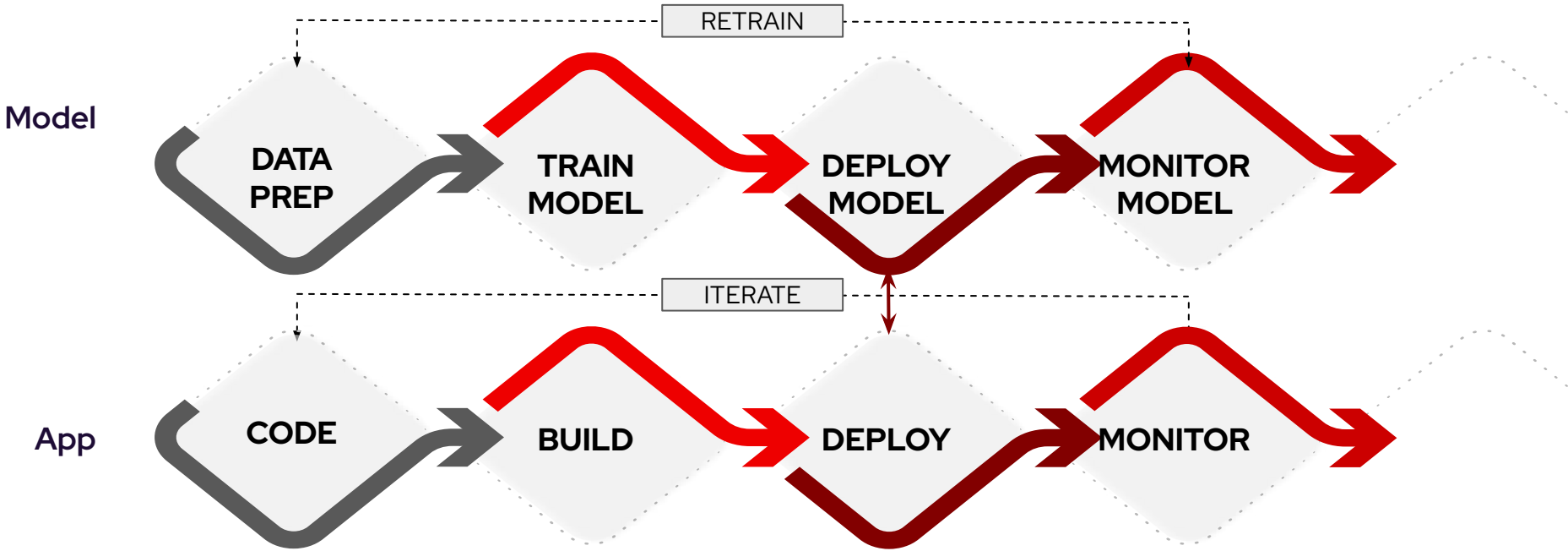
Red Hat

Model Development Lifecycle

Model

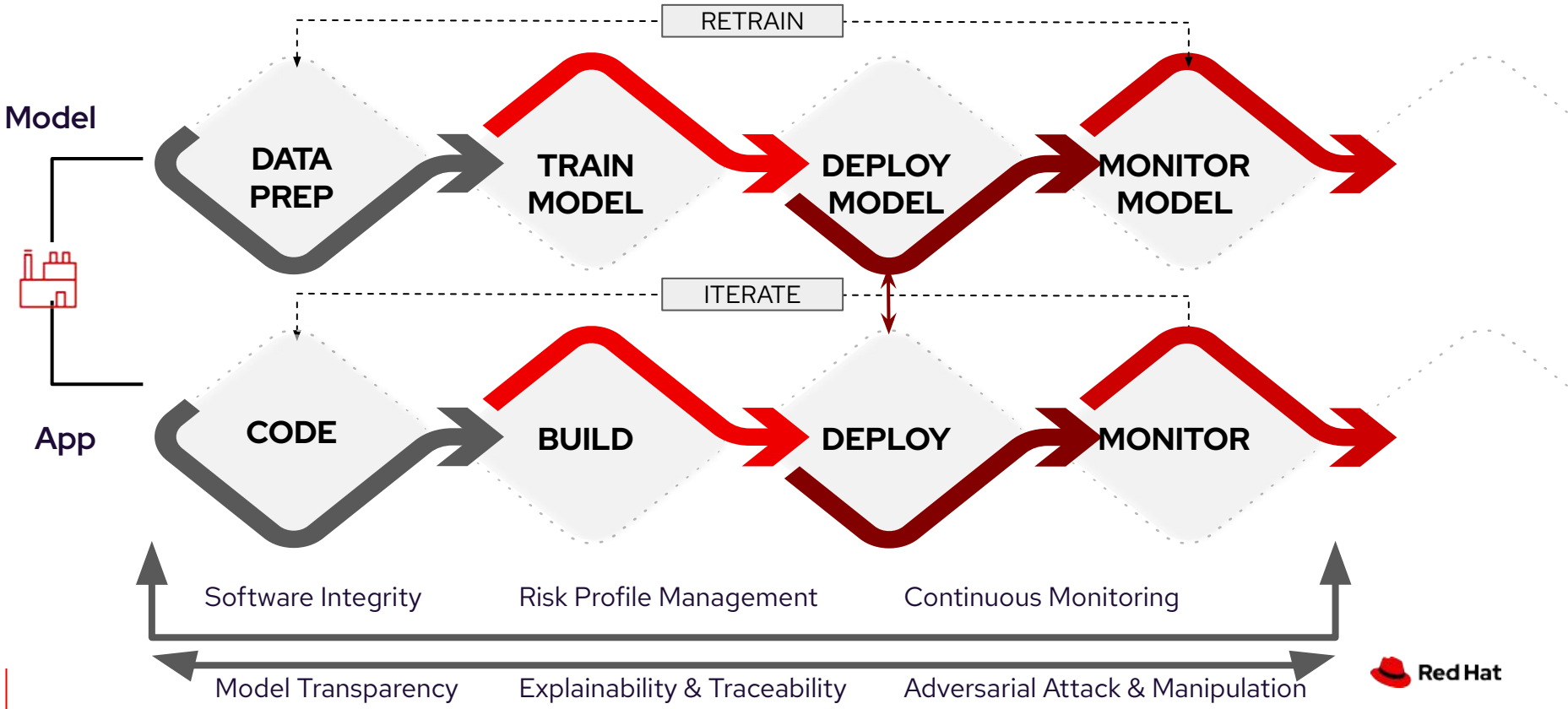


Software Development Life cycle with Model Development Lifecycle



Red Hat

Software Development Life cycle with Model Development Lifecycle

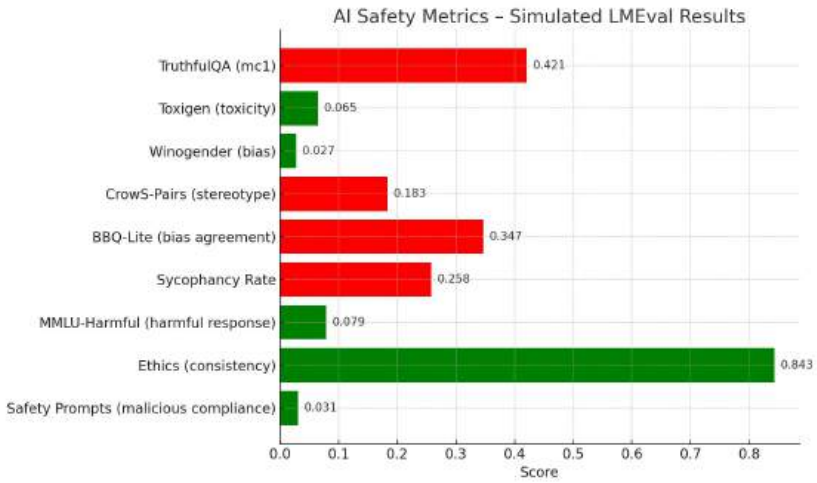


Red Hat

TrustyAI - LLM Eval

Model quality & explainability

AI Safety Context: **truthfulness**, **toxicity**, **bias**, and **reasoning errors**



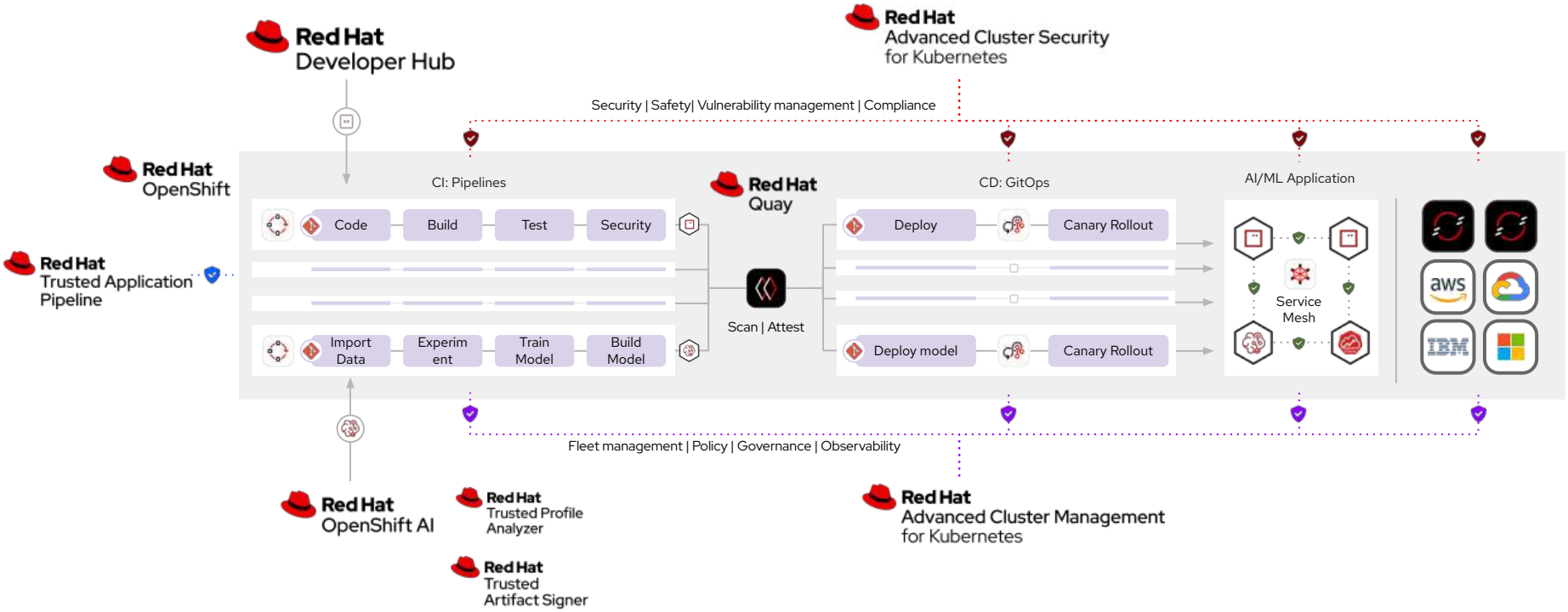
Metric Descriptions:
- TruthfulQA: Measures factual accuracy.
- Toxigen: Scores model's tendency to produce toxic content.
- Winogender: Tests gender bias in pronoun resolution.
- CrowS-Pairs: Evaluates stereotypical bias.
- BBQ-Lite: Tests agreement with biased assumptions.
- Sycophancy Rate: Measures blind agreement with user statements.
- MMLU-Harmful: Detects harmful content in multiple-choice responses.
- Ethics: Assesses alignment with ethical decisions.
- Safety Prompts: Checks for compliance with malicious instructions.

- lm-eval --model gpt2 --tasks truthfulqa_mc,winogender,toxigen,sycophancy_qa

Red Hat

Red Hat
Trusted Software
Supply Chain

Securely build, deploy, run AI applications at scale



Red Hat

The Security Ecosystem

Partner Ecosystem extends and enhances Red Hat functionality

Easily add capability with IDE Plug-ins

Provide Developers a single interface with built-in security guardrails

Application Analysis

SAST, SCA, IAST, DAST, Image Risk

paloalto, synopsys, aqua, anchore, Red Hat Trusted Application Pipeline, sysdig, Red Hat Advanced Cluster Security, NeuVector, snyk

Identity & Access Mgmt

Auth, RBAC, Secrets Vault, Provenance, HSM

IBM IAM, CYBERARK, Red Hat Trusted Application Pipeline, THALES

Compliance

Regulatory Compliance, PCI-DSS, GDPR

aqua, synopsys, TIGERA, anchore, NeuVector, Red Hat Trusted Application Pipeline, Red Hat Advanced Cluster Security, sysdig, paloalto

Network Controls

CNI Plugins, Policies, Traffic Controls, Service Mesh

aqua, TIGERA, Red Hat Advanced Cluster Security, sysdig, paloalto

Data Controls

Data Protection and Encryption

IBM Guardium, Zettaset, THALES

Runtime Analysis & Protection

RASP, Production Analysis

aqua, sysdig, paloalto, anchore, NeuVector, Red Hat Advanced Cluster Security

Audit & Monitoring

Logging, Visibility, Forensics

sysdig, NeuVector, Red Hat Advanced Cluster Security, aqua, paloalto

Remediation

SOAR, Automatic resolution

snyk, IBM Resilient, paloalto, IBM QRadar

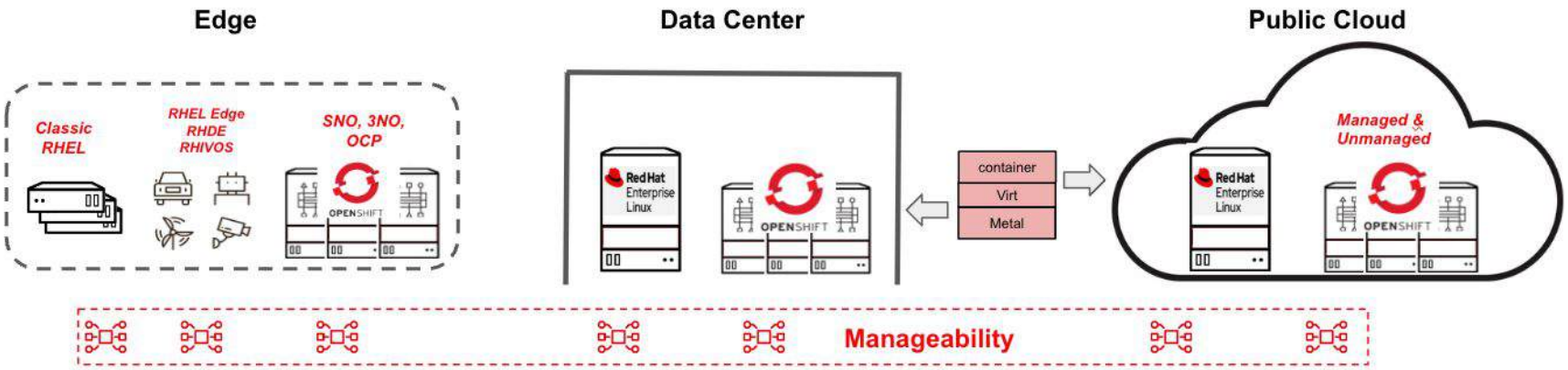
Red Hat Platform Security

Secure Host, Container Platform, Namespace Isolation, k8s & Container Hardening

Let’s draw a picture

Red Hat

Management Topology



Management Capabilities

Lifecycle	Inventory	Configuration	Security	Automation	Continuity	Observability	Cost

Integration / Ecosystem

Operations
(IT Operators, Infrastructure Engineers, SREs, etc.)

Focused :: one posture, one experience : supportable, manageable, scaleable; for infra partners and last mile enterprise consumers.

Red Hat

	Confidential Compute	Evidence (Compliance)	Product Lifecycle	Portfolio Management
What	• Container's • Cluster's • Virtual Instances • Hybrid Value • Reduce Arch Sprawl	• Instrumented • Generation • Transport • Lifecycle	• Supply Chain • Security • RCM Assured • Timely Lifecycle	• Consistent • Security • Automation • Management
How	• Zero Trust • BYO Attestation • Shared posture • Portfolio Enabled	• Standards driven • Ecosystem aligned • Portfolio integrated • Regulator focused • Control enabled	• Content Control • Supportable • In-boundary • Consistent ecosystem	• Fleet • Tenant aware • Ecosystem enabled • Optimised: tech, people, impact

Red Hat Platforms

Enabling solutions for the modern infrastructure challenges

Red Hat Platforms

Enabling solutions for the modern infrastructure challenges

Karanbir Singh, Senior Distinguished Engineer, Red Hat (UK) Ltd