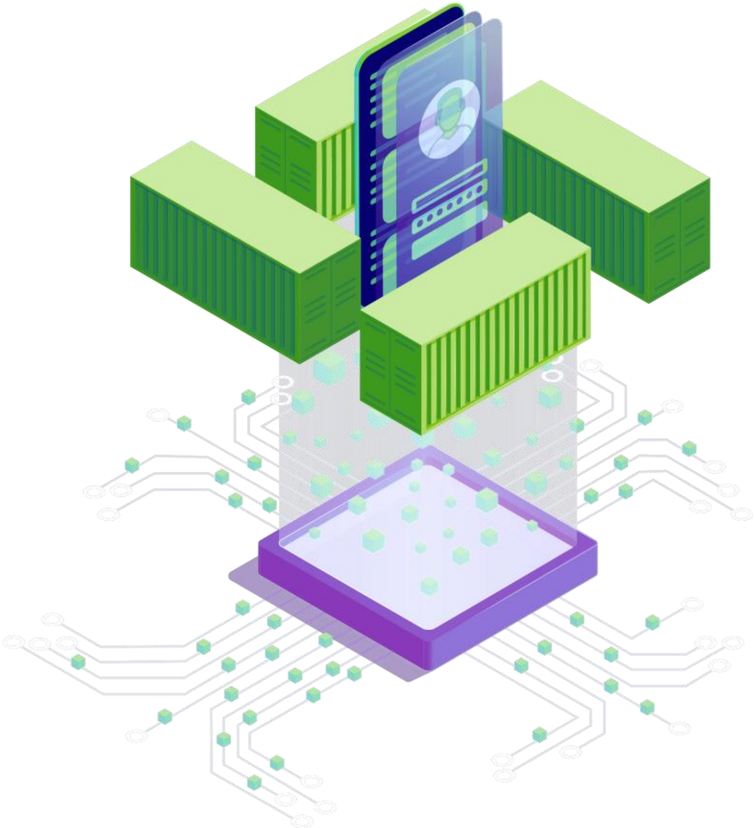
MORO

Moro Container Service

NEXT GENERATION APPLICATION MODERNIZATION PLATFORM

Why Do We Need Containers?

- Customers are under pressure **to modernize applications to reduce risk, stay competitive, and increase market agility**
- Businesses' ability to win, serve and retain customers depends on delivering new capabilities through **secure software applications rapidly and continuously.**
- Some core business applications are architected in a way **that cannot evolve or change quickly** to meet rapidly changing market requirements.
- IT needs to provide their developers the flexibility to **securely build, deploy, run and scale applications across the hybrid cloud.**



"**80%** of legacy applications will be modernized within the next 2 years"

Source: IDC

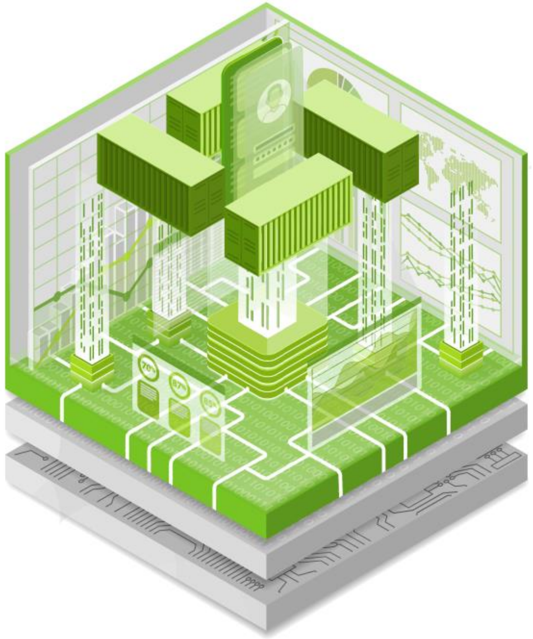
"More than half of all applications worldwide are legacy applications"

Source: IDC

How Containers Can Help?

Modern Platforms Can Solve Business Challenges

- Cost reduction for operating infrastructure
- Innovate at speed
- Scalability
- Security Focused
- Integrated development tools



"By 2025

95% of new digital workloads will be deployed on cloud-native platforms"

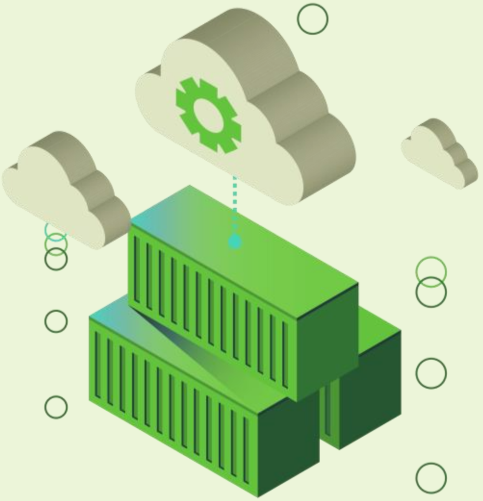
Source: Gartner

Moro Container Service

"A managed cloud service, powered by Red Hat OpenShift, used to deploy modern (containerized) applications with ease and securely on a multi-tenant Kubernetes cluster"

Red Hat OpenShift

MORO CONTAINER SERVICE



Hosted in Moro Hub Data Centers AZ1 & AZ2

- Locally Hosted in UAE
- Industry Standards
- Scalability
- Developer Friendly
- Enterprise Grade
- Secure
- Automation
- Collaboration
- Multi - tenant

Benefits of the Service:

- **Accelerating Value** | Focus on building and scaling applications that provide value to the business.
- **Innovation First** | Simplifying operations so the customers' teams can focus on innovation, not managing the infrastructure.
- **Investment Optimization** | Take advantage of the multi-tenant k8s cluster to optimize overall cost.
- **Cloud Freedom** | Run applications across disparate cloud environments, consistently.

Moro Container Service Offering

Managed Kubernetes Cluster | Kubernetes cluster that is managed by Moro Hub, from monitoring, patching, platform updates and security

Multi-tenant | Dedicated and logically isolated environments ("Namespaces") for individual tenants that includes compute, storage and network resources on a multi-tenant Kubernetes cluster

Monitoring | Comprehensive view of customer environment that includes container images, deployments and configurations

Cloud Portal | Feature rich cloud portal with built-in CI/CD, monitoring, and developer friendly interface/tools

Secure | Securely build, deploy and run applications, scan images for vulnerabilities and securely publish applications using managed web application firewall

Container Registry | Dedicated private registry to store container images, including team-based access control

Network Services | Define network policies to restrict network traffic within customer environment

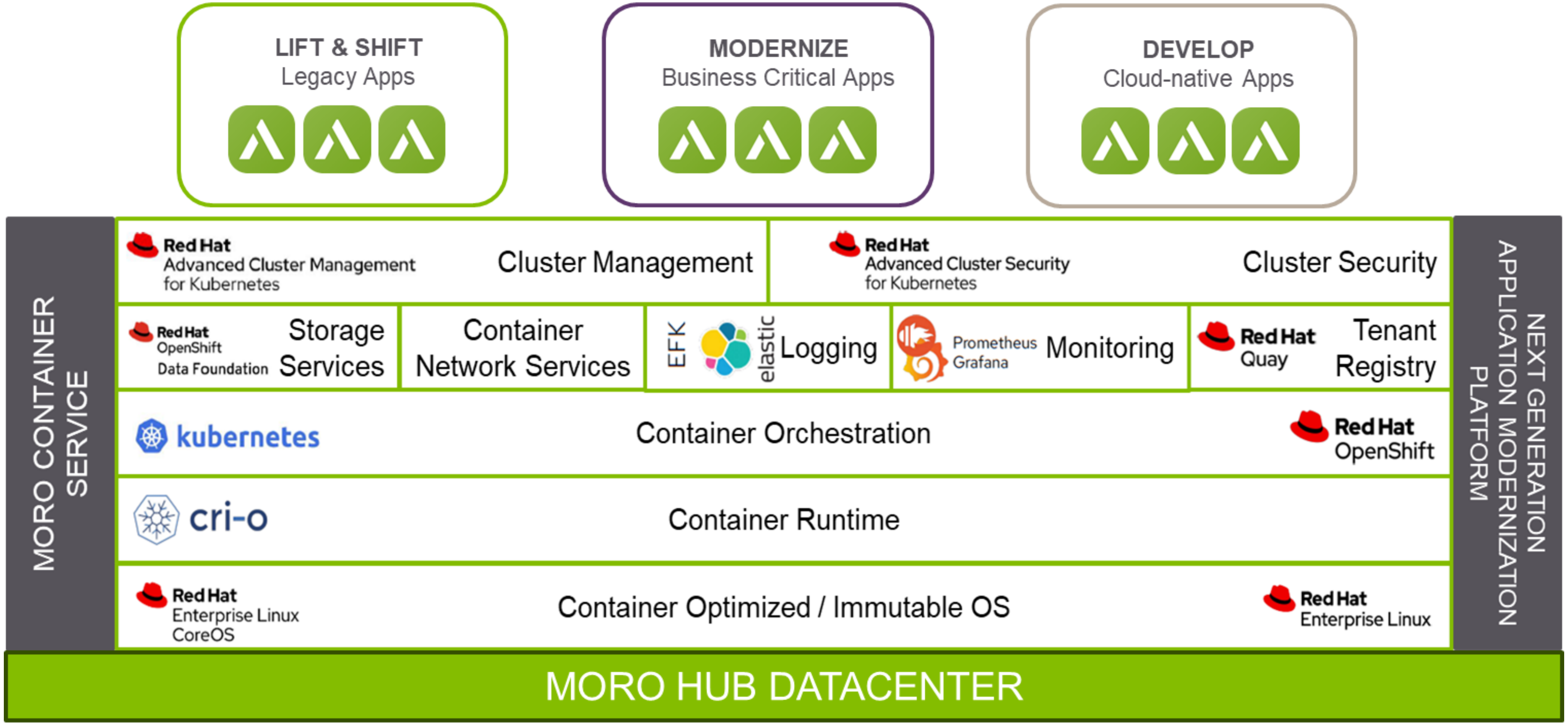
Connectivity | Choice of connectivity to customer premise either through Internet, MPLS, Site to Site VPN

Automate | Automate the creation, configuration and management of community or certified Kubernetes applications

Multi Availability Zones | Deploy identical environments such as Production and DR in geographically separated Moro Hub datacenters

24x7 Customer Support | Access to 24x7 service desk for any issues or support required

Moro Container Service Technology Stack



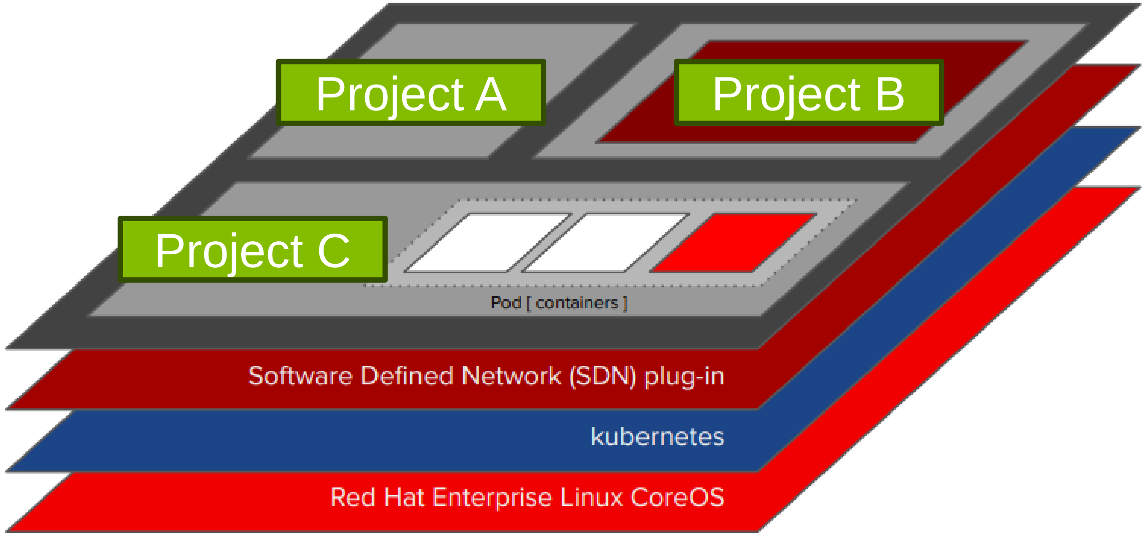
Moro Container Service Security

RHEL Core OS

- Lightweight and purpose built operating system (OS)
- Secure OS for running k8s, OpenShift services, containerized workloads

Container Security

- Project or Namespaces forms the logical boundaries and multi-tenancy
- Define network policies
- Scan container images for known vulnerabilities
- Container registry for secure access to container images, team-based access control


Project A
Project B
Project C
Pod [containers]
Software Defined Network (SDN) plug-in
kubernetes
Red Hat Enterprise Linux CoreOS

Kubernetes Security

- Manage resources such as network and storage policies
- Enable containers to discover or prevent from seeing each other
- Regular cluster upgrades with latest fixes and patches
- Automated cluster heath checks to repair worker nodes
- Cluster monitored 24x7 for any issues or problems

Network Security

- Ingress and egress rules for services
- Network policies for POD isolation
- Firewall to define access rules and NAT

Identity and Access Management

- Role based access control for tenant users

Encryption, Secrets Management

- Data-at-rest and Data-in-transit encryption
- Secrets management service (External Vault) for application security