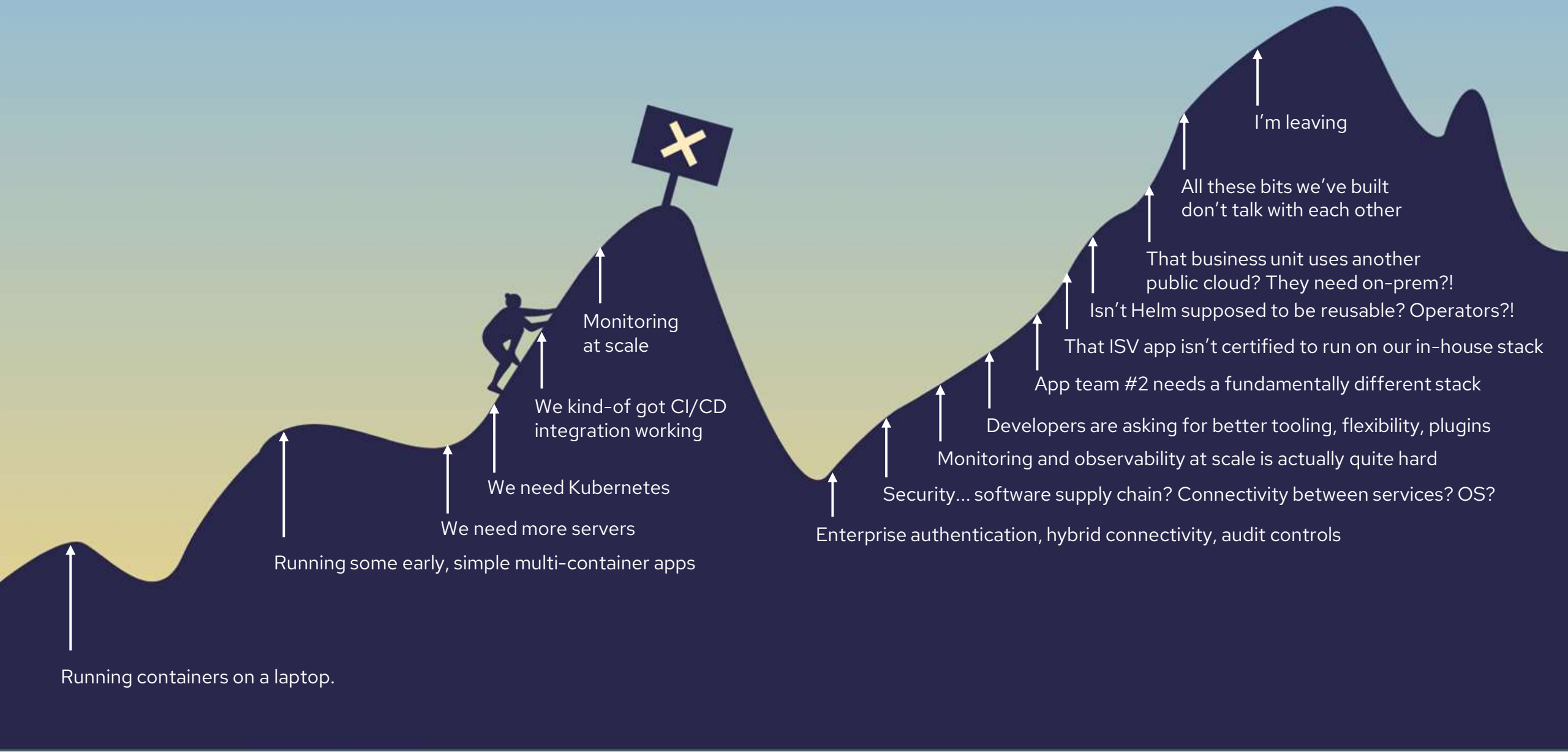
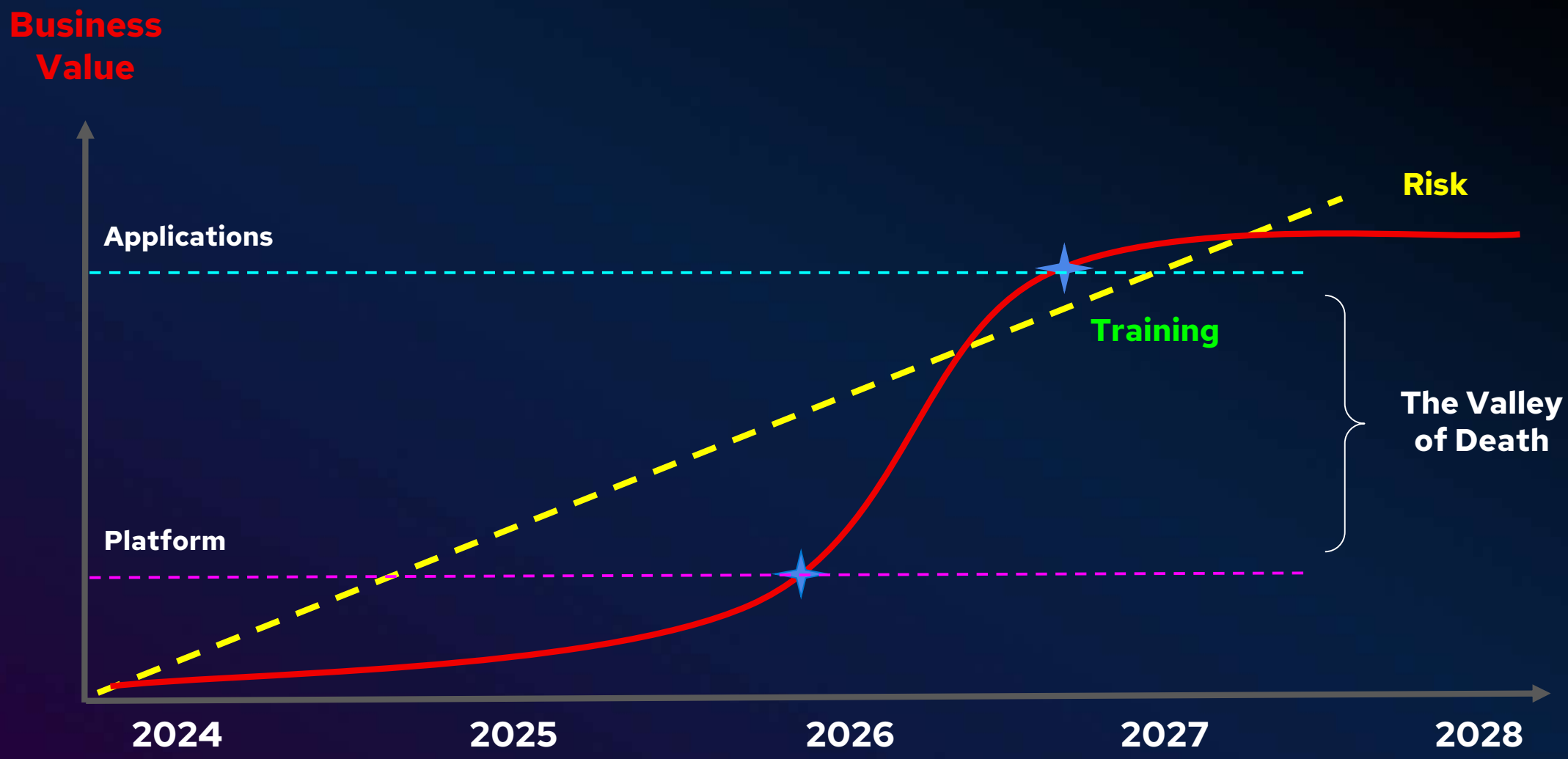
A Secured Hybrid Cloud Experience

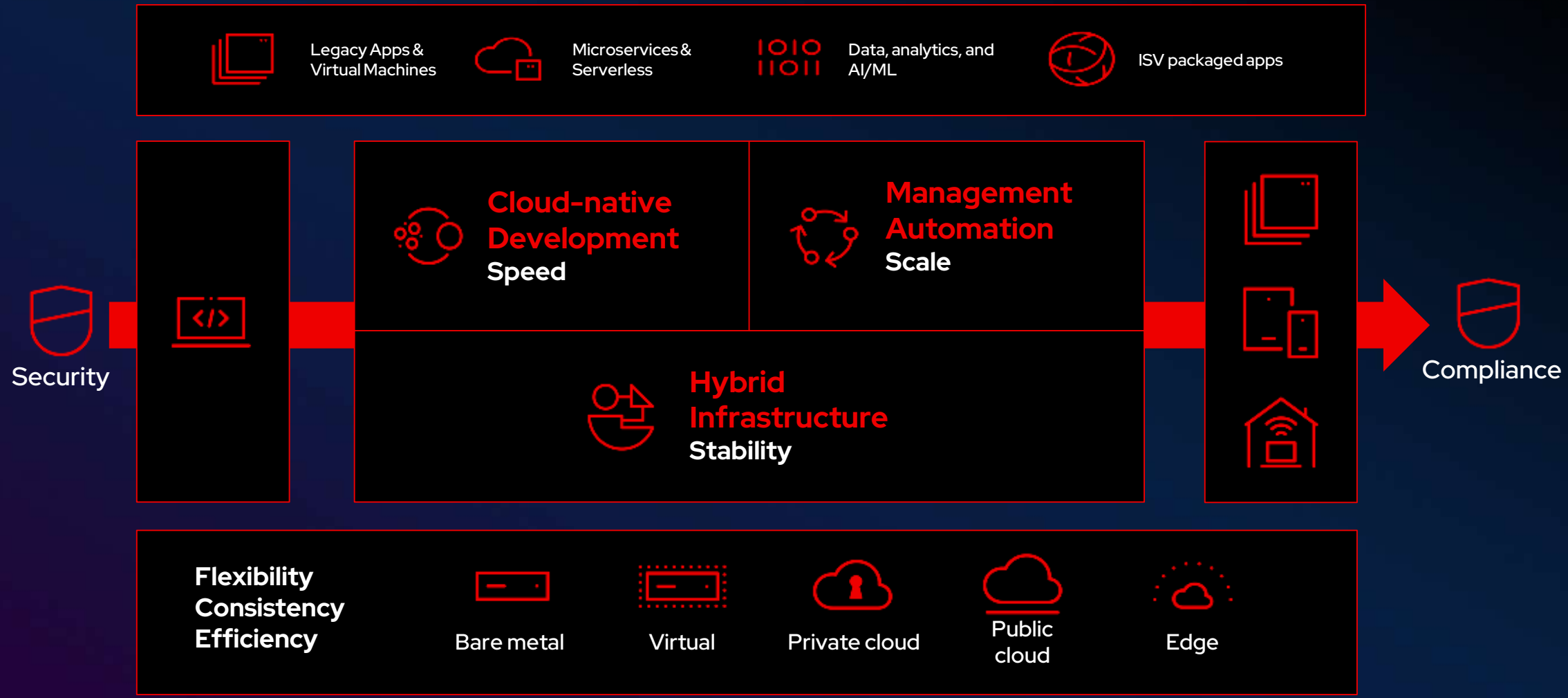
The Platform Trail



The Platform Trail



Red Hat Open Hybrid Cloud with OpenShift



Red Hat OpenShift on AWS (ROSA)

Turnkey application platform with integrated services, tools, and supported by AWS and Red Hat.

Managed Kubernetes & components to reduce complexity while improving Security by AWS and Red Hat.

Consistent hybrid cloud experience and cloud choice

Build, Test, Deploy

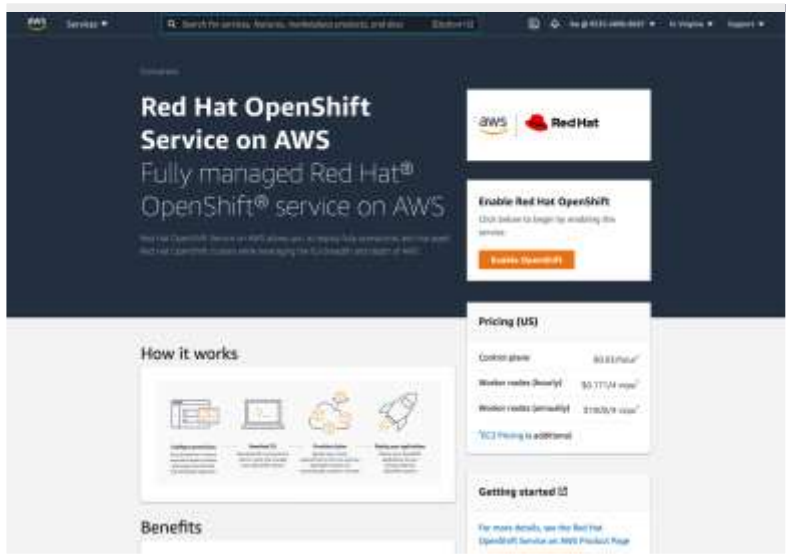
Apply the heart of DevSecOps policy & procedure on a consistent infrastructure foundation.

Run and Manage

with consistency and unified security.

Design & Code

using cloud-native dev tools & application technology while benefiting from DevSecOps right at the start.



Most customers choose to run OpenShift on AWS because they want to keep existing tools and practices while leveraging investments in the vast AWS services portfolio

ROSA is the easiest and most convenient way to pay for and deploy fully supported and managed OpenShift clusters on AWS

Accelerate Migration to Cloud with Integrated AWS Services

ROSA

Application Development and Monitoring

- AWS **DynamoDB**
- AWS **RDS**
- **Amazon Aurora**
- **Amazon API Gateway**
- **AWS CodeCommit**
- **AWS EventBridge**
- CloudWatch
- Amazon Managed Service for Prometheus
- Amazon Managed Service for Grafana

Ongoing updates to integrations available via AWS Controllers for Kubernetes on Operator Hub

Infrastructure and Operations

- Amazon **EC2**
- Amazon **EBS**
- Amazon **EFS**
- Amazon **FSx**
- Amazon **ELB**
- Amazon **VPC**
- Route 53
- **AWS Private Link**
- Amazon ECR

AWS security, identity, and compliance solutions

Identity and access management

AWS Identity and Access Management (IAM)

AWS IAM Identity Center

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager

Amazon Verified Permissions

Detective controls

AWS Security Hub

Amazon GuardDuty

Amazon Security Lake

Amazon Inspector

Amazon CloudWatch

AWS Config

AWS CloudTrail

VPC Flow Logs

AWS IoT Device Defender

Infrastructure protection

AWS Firewall Manager

AWS Network Firewall

AWS Shield

AWS WAF

Amazon VPC

AWS PrivateLink

AWS Systems Manager

AWS Verified Access

Data protection

Amazon Macie

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Private CA

AWS Secrets Manager

AWS VPN

Server-Side Encryption

Incident response

Amazon Detective

Amazon EventBridge

AWS Backup

AWS Security Hub

AWS Elastic Disaster Recovery

Compliance

AWS Artifact

AWS Audit Manager

Large community of security partners & solutions

Network and Infrastructure security

Identity and Access Control

Vulnerability and configuration analysis

Logging, Monitoring, SIEM, Threat Detection und Analytics

Host and Endpoint Security

Application Security

Data protection and data encryption

Consulting and “Technology Competency” partner

Security Engineering

Governance, Risk- and Compliance-Management

Security Operations and Automation

AWS extends the cloud to where customers need it

REGIONS

AWS global infrastructure

AWS European Sovereign Cloud (announced)

METRO AREAS & TELCO NETWORKS

Amazon CloudFront

AWS Local Zones

AWS Wavelength

ON PREMISES

AWS Outposts

AWS Dedicated Local Zones

Amazon ECS Anywhere

Amazon EKS Anywhere

FAR EDGE

AWS Snow Family

Integrated Private Wireless

AWS Private 5G

AWS IoT

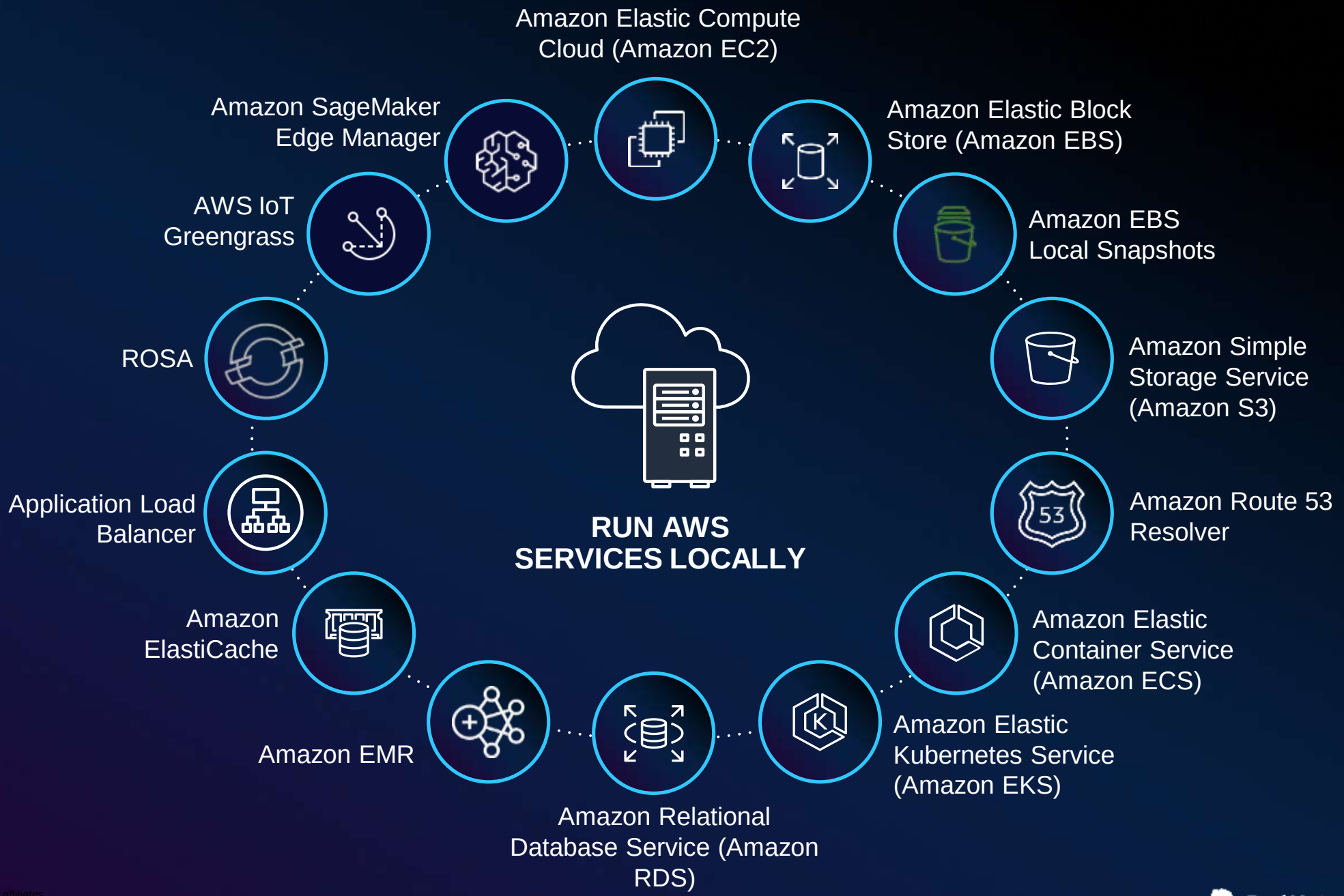
Same services, architecture, APIs, and tools for a consistent experience

AWS Dedicated Local Zones

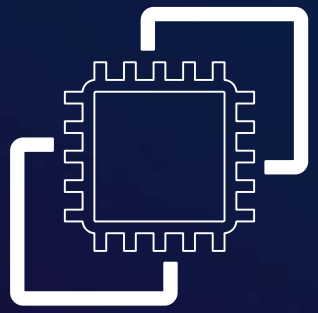
**AWS INFRASTRUCTURE FULLY MANAGED BY AWS,
BUILT FOR EXCLUSIVE USE BY A CUSTOMER OR COMMUNITY**

- AWS infrastructure placed in a customer-specified location or data center to help comply with regulatory requirements
- Offer the same benefits of Local Zones, such as elasticity, scalability, and pay-as-you-go pricing, and the ability to establish further security and governance features
- Can be operated by local AWS personnel

AWS Outposts services today



AWS Nitro System – Confidential compute



AWS Nitro System

All interactions with the AWS Nitro System are through narrow, authorized, and authenticated APIs

There is no mechanism for any system or person to log in to the underlying Amazon EC2 host (no operational access)

There is no interactive access (no SSH, no general-purpose access of any kind)

Debugging features can’t disclose customer data

Nitro Systems run in an isolated network

More options to control the key: AWS KMS External Key Store (XKS)

- Full removal of root of trust from AWS KMS
- Transparent to AWS services and client applications
- Flexibility on which keys you choose to store in external key manager
- Customer owns the key in meaningful ways (e.g., turn off XKS and AWS data becomes unreadable)

AWS Data Privacy & Security Differentiation

Storage: Customers choose the AWS Region(s) in which their content is stored and the type of storage to comply with data sovereignty regulations.

Security: Customers choose how their content is secured. AWS uses FIPS 140 validated HSMs for storing cryptographic key material and NIST standardized cryptographic primitives, algorithms and schemes.

Access: AWS prohibits, and our systems are designed to prevent, remote access by AWS personnel to customer data for any purpose, including service maintenance, unless access is requested by the customer, is required to prevent fraud and abuse, or to comply with law.

Disclosure of Customer Content: We will not disclose customer content unless we're required to do so to comply with the law or a binding order of a government body.

Security Assurance: AWS security protections and control processes are independently validated by multiple third-party independent assessments. 2,500 security controls audited each year.

Third-party validation

Customer Stories

Fachklinikum Mainschleife

Using the cloud to safeguard its patient and medical data and comply with regulatory requirements

30+ applications and workflows
built on AWS

10+ TB of patient and medical data
migrated to the cloud

Cost savings
on encryption and storage

100% cloud infrastructure
as the first German hospital

Safeguarding Ukraine’s data to preserve its present and build its future

42
Government authorities

10PB+
of Ukrainian citizen data migrated to AWS

24
Ukrainian universities

“From the day I began working with the AWS team, I have been impressed by their singular focus on helping the Ukrainian people and ensuring that our government can continue working despite external disruption. What is also amazing is that, in responding to our immediate needs, we have never lost sight of the future, of building a better Ukraine augmented by new, cutting-edge cloud technologies."

Vadym Prystaiko
Ukraine’s Ambassador to the United Kingdom

Singapore Government's Smart Nation and Digital Government Group (SNDGG) collaborated with AWS to define and build Dedicated Local Zones to help us meet our stringent data isolation and security requirements, enabling Singapore to run more sensitive workloads in the cloud securely.

Chan Cheow Hoe

Government Chief Digital Technology Officer of Singapore

Amazon SageMaker & OpenShift for data science

Combing AI with app modernization
SageMaker/ROSA fingerprint model training

Data scientist
Data engineers

MLOps engineer

Clients

IDE | Ingest data | Label data | Train/ Tune model | Evaluate model | Save models

Model server | Ingest model | User interface | Metrics | Dashboard

Starburst, Label Studio, Snorkel | **SageMaker notebook instance** | **ODH/RHODS notebook Amazon SageMaker SDK**

OPENSHIFT

aws

SageMaker endpoints | **SageMaker containers for Docker images** | **Amazon SageMaker Model Monitor** | **Amazon SageMaker Clarify**

IT/Admin

Resource integration & mgmt.

Argo

GitHub

Amazon S3

SageMaker

Amazon EC2

Learn about AWS Digital Sovereignty

https://aws.amazon.com/compliance/digital-sovereignty/