UNICORN project

UNICORN

Manos Papoutsakis

FORTH

11th SummerSOC
June 26, 2017, Crete

UNICORN project

Horizon 2020

Call: H2020-ICT-2016-2017

Topic: ICT-06-2016

Type of action: IA
(Innovation action)

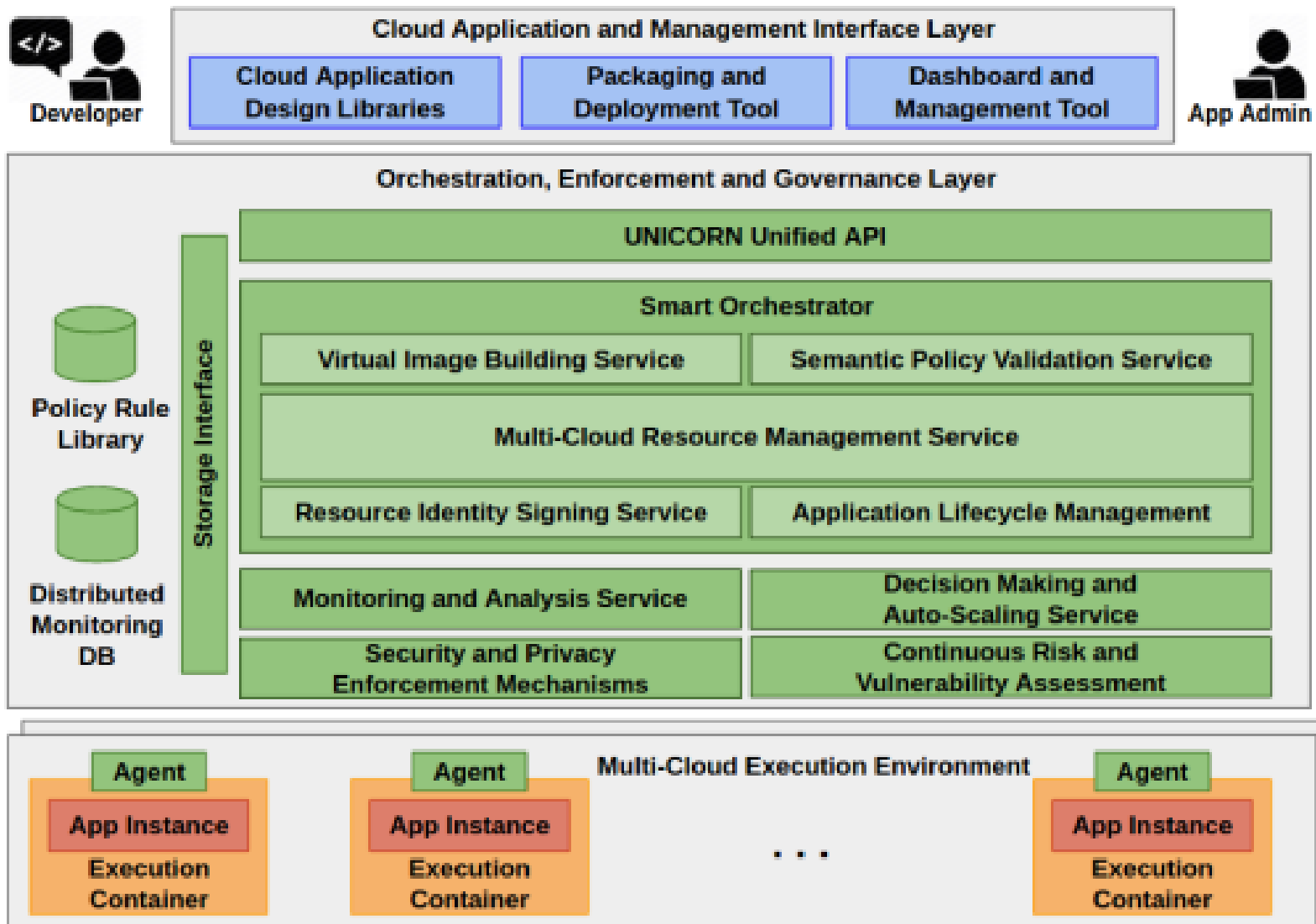**Proposal number**: 731846

Proposal acronym: UNICORN

Motivation for UNICORN

- ■ **Challenges for multi-cloud adoption**
    - ■ security, compliance and software vulnerabilities
    - ■ monitoring and management
    - ■ resource scaling (elasticity)

- ■ **Existing multi-cloud solutions (e.g. AWS CloudFormation, Oracle Exalogic, CAMF, Juju, ServiceMesh) do not fully**
    - ■ tackle data protection privacy constraints and restrictions
    - ■ manage the entire application lifecycle
    - ■ support elasticity techniques comprehensively
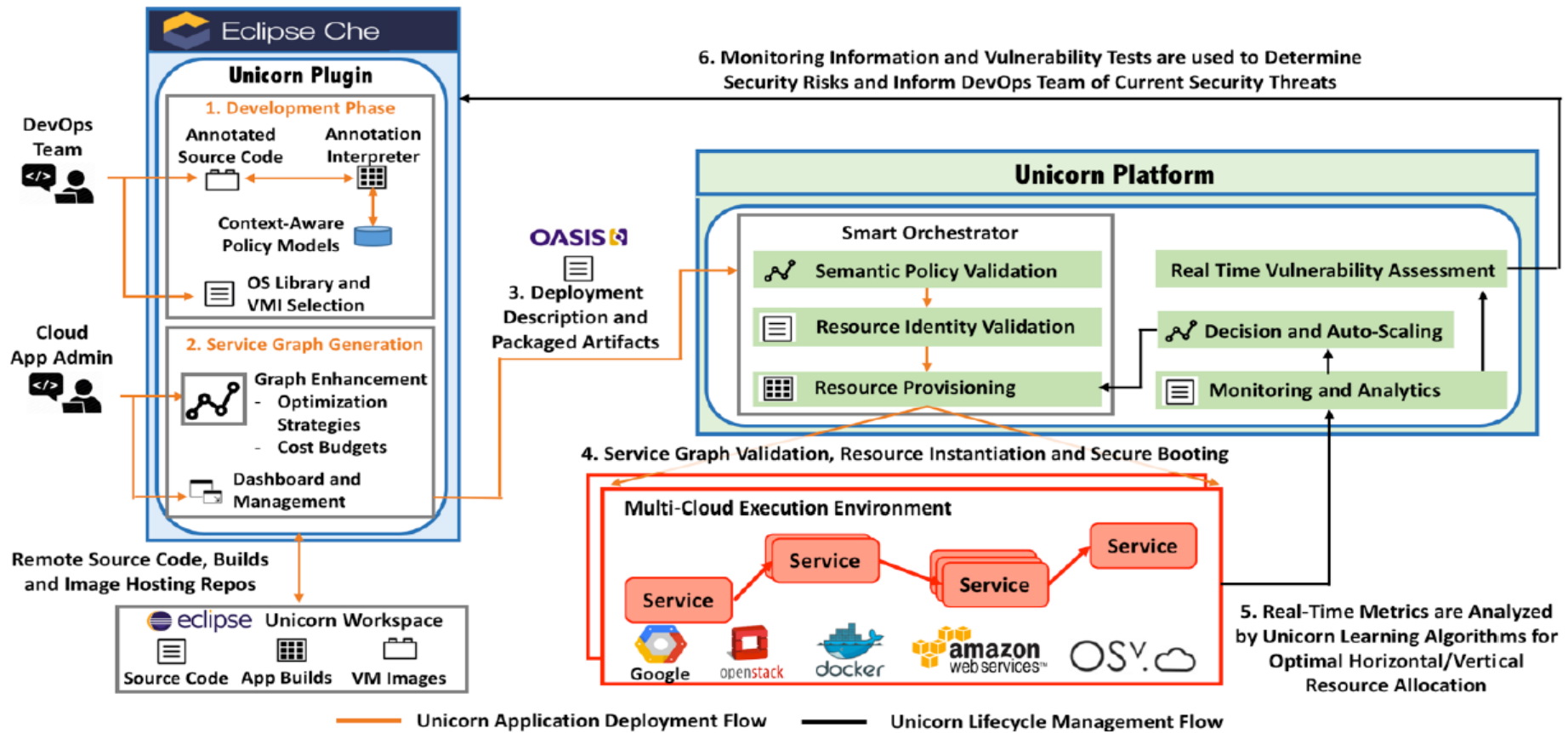
What UNICORN platform offers?

- **UNICORN platform will allow software developers to:**
    - include privacy-by-design and elasticity-by-design features
    - define application characteristics including constraints and policies
    - deploy without manually performing resource mappings and bindings

- **Based upon existing solutions and developments**
    - CELAR
    - PaaSport
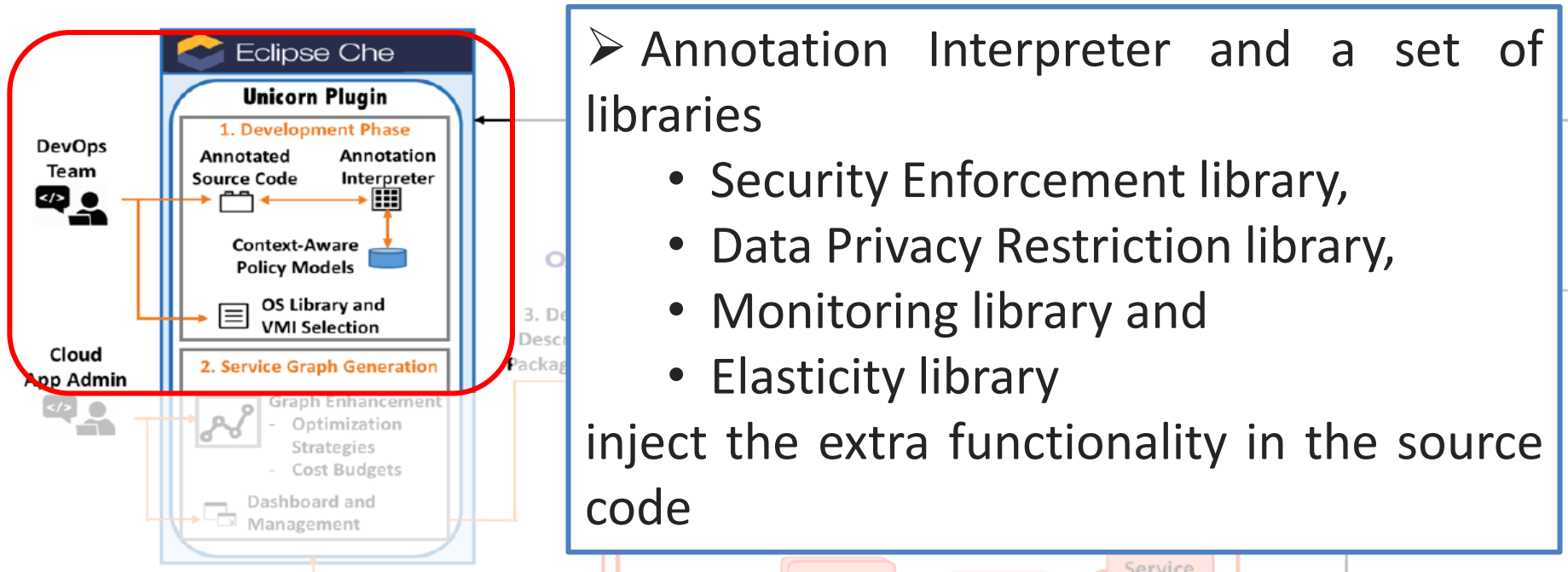   - PaaSword
    - ARCADIA
    - PaaSage

Design, deploy and manage steps

UNICORN

Eclipse Che

Unicorn Plugin

DevOps Team

1. Development Phase
- Annotated Source Code
- Annotation Interpreter
- Context-Aware Policy Models
- OS Library and VMI Selection

Cloud App Admin

2. Service Graph Generation
- Graph Enhancement
  - Optimization Strategies
  - Cost Budgets
- Dashboard and Management

Remote Source Code, Builds and Image Hosting Repos

eclipse Unicorn Workspace
- Source Code
- App Builds
- VM Images

OASIS

3. Deployment Description and Packaged Artifacts

6. Monitoring Information and Vulnerability Tests are used to Determine Security Risks and Inform DevOps Team of Current Security Threats

Unicorn Platform

Smart Orchestrator
- Semantic Policy Validation
- Resource Identity Validation
- Resource Provisioning

- Real Time Vulnerability Assessment
- Decision and Auto-Scaling
- Monitoring and Analytics

4. Service Graph Validation, Resource Instantiation and Secure Booting

Multi-Cloud Execution Environment

Service · Service · Service · Service

Google · openstack · docker · amazon web services · OSv.

5. Real-Time Metrics are Analyzed by Unicorn Learning Algorithms for Optimal Horizontal/Vertical Resource Allocation

Unicorn Application Deployment Flow   Unicorn Lifecycle Management Flow

Development phase

➤ Annotation Interpreter and a set of libraries
- Security Enforcement library,
- Data Privacy Restriction library,
- Monitoring library and
- Elasticity library

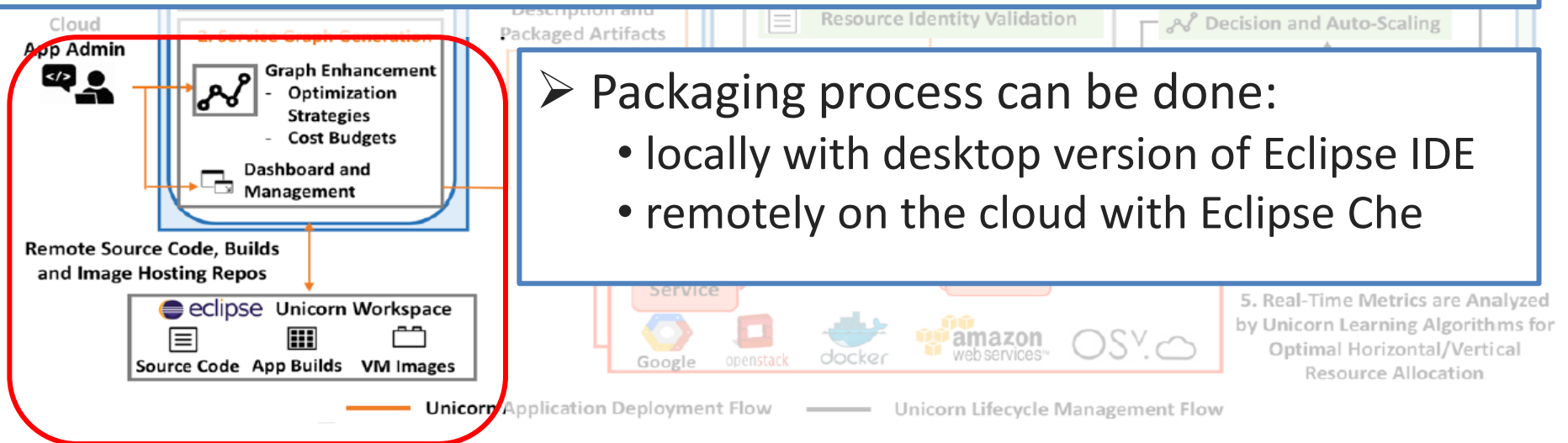inject the extra functionality in the source code

➤ User is prompted to select:
- OS images public or custom
- specific OS libraries with no extra bulks of software

# Service graph generation and deployment description

UNICORN

➢ The application topology description is a direct graph where:
- nodes == services
- edges == relationships
- node/edges attributes == security enforcement mechanisms, data privacy restrictions, monitoring metric collection and elastic scaling

➢ Packaging process can be done:
- locally with desktop version of Eclipse IDE
- remotely on the cloud with Eclipse Che

Service graph validation, resource instantiation and secure booting

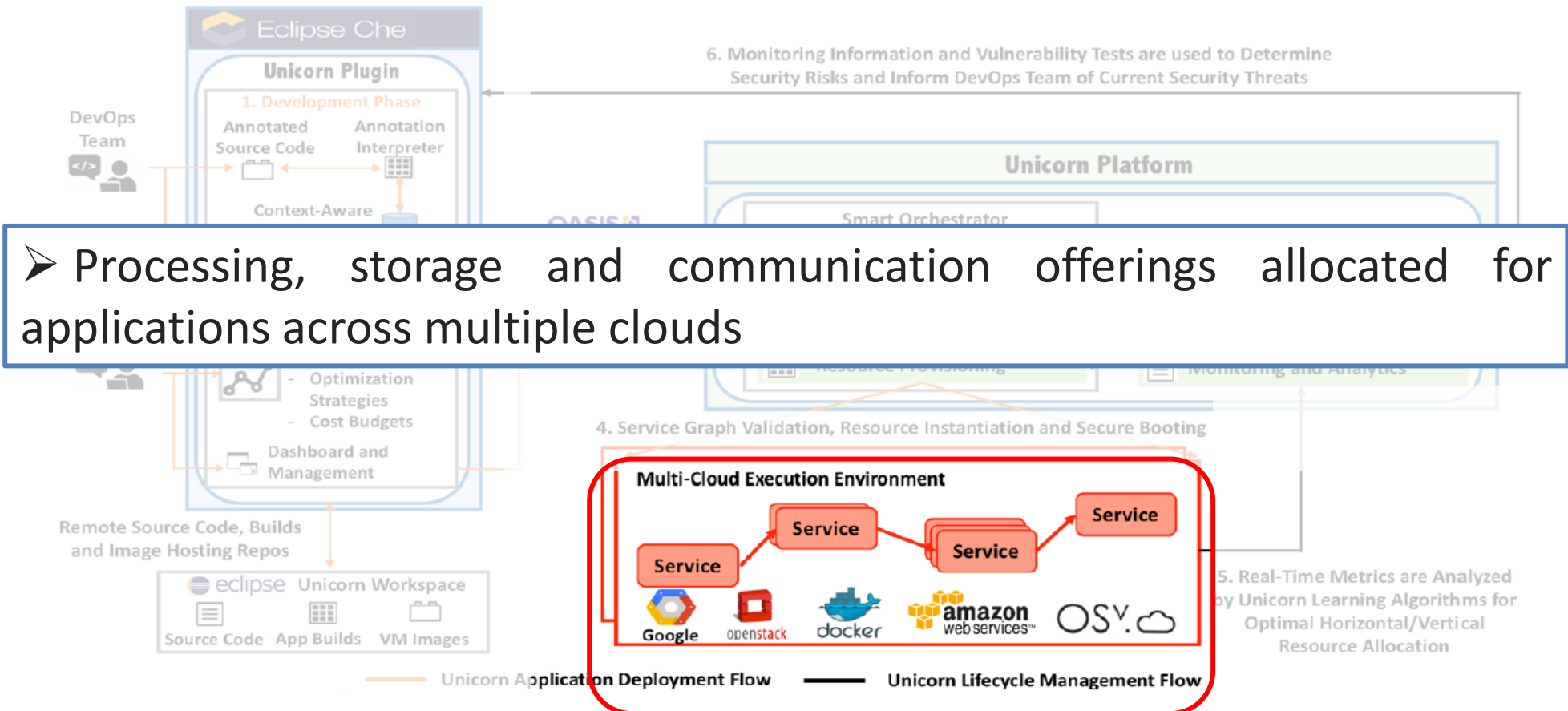> ➤ Deployment description adherers to the Topology and Orchestration Specification for Cloud Applications (TOSCA)
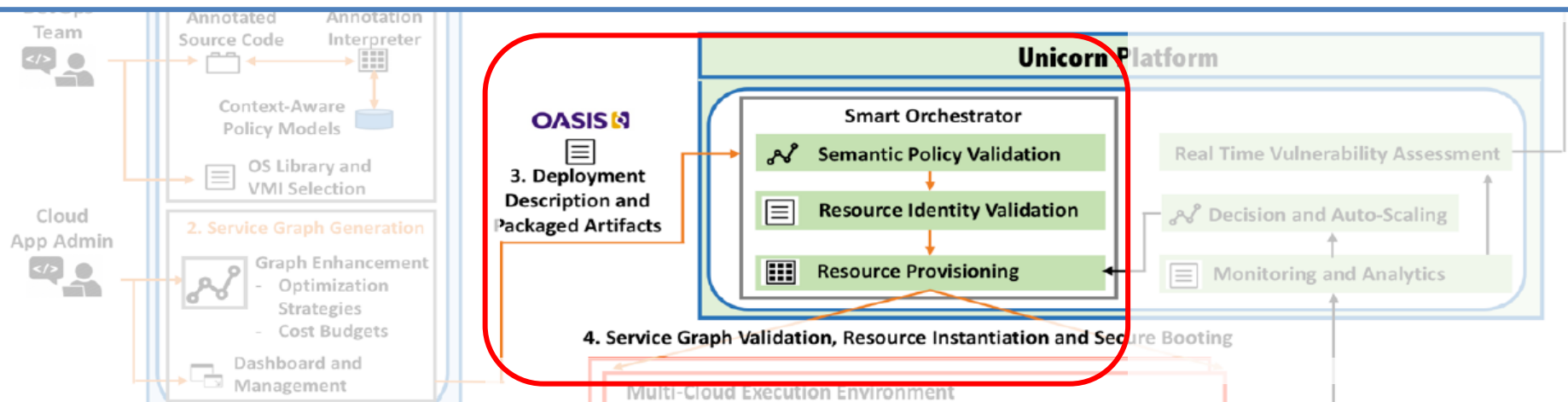
> ➤ Smart Orchestrator (Arcadia Orchestrator) will:
> - semantically validate annotated policy rules
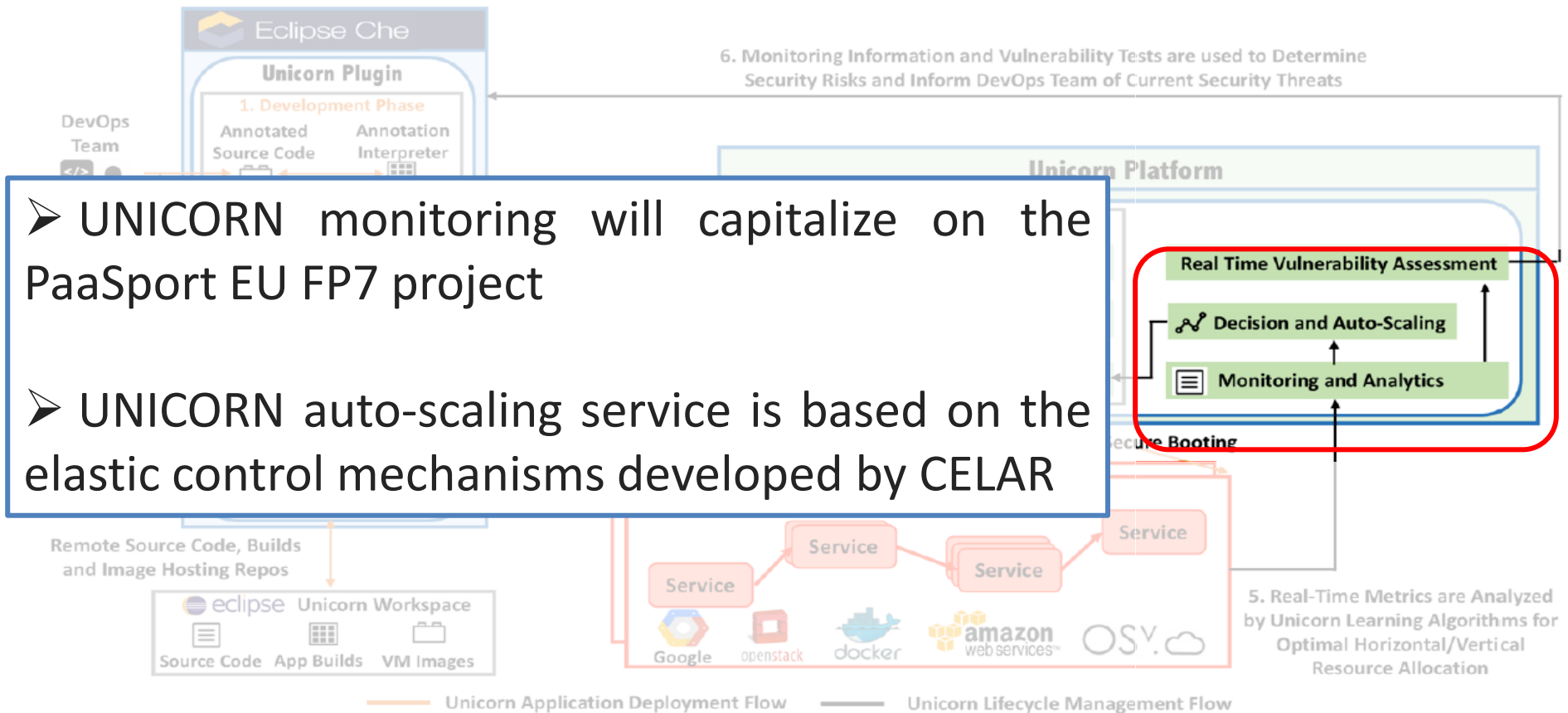> - verify the validity of the hosted images

Multi-Cloud execution environment

> ➤ Processing, storage and communication offerings allocated for applications across multiple clouds

Monitoring and auto-scaling

> UNICORN monitoring will capitalize on the PaaSport EU FP7 project

> UNICORN auto-scaling service is based on the elastic control mechanisms developed by CELAR

Beyond the state of the art

UNICORN

- Cloud application development and management
  - design and enforce security, data privacy and elastic scaling
  - package cloud applications with OS libraries and deploy on unikernel environments
  - extensions to Eclipse CAMF

Beyond the state of the art

- Cloud and resource orchestration over programmable infrastructure
  - TOSCA extensions to cover UNICORN concepts of security, data protection and privacy, monitoring and elasticity by design
  - support for unikernels in Smart Orchestrator
  - resource identity and validation signing mechanism

UNICORN

UNICORN

- Cloud, application and unikernel monitoring
    - VM and unikernel monitoring leveraging OSv kernel metrics
    - automatic monitoring instantiation and configuration
    - secure metric dissemination over a secure channel
    - low-cost adaptive monitoring techniques

Beyond the state of the art

- Cloud security and privacy enforcement, risk and vulnerability assessment
  - code-annotated mechanisms for implementing the core functionality of security and data privacy policy specification and enforcement
  - monitoring and vulnerability assessment

- Cloud-Based personal activity tracking for the Internet of Things
  - SUITE 5
- Encrypted voice communication service over programmable infrastructure
  - UBITECH
- Prosocial learning digital game
  - REDIKOD
- Cyber-Forum cloud platform for startups and SMEs
  - CAS/CyberForum IT environment

Questions?

UNICORN

Acknowledgements:

Visit us:

www.unicorn-project.eu