RHUG
Sécurité des conteneurs

Martin Ouimet
Architecte de solutions
infonuagiques

Red Hat

Sécurité

Conformité

Portabilité

- Les enjeux de sécurité en conteneur
- Les bonnes pratiques
- Les solutions
- Démonstrations

Red Hat

Sécurité

Conformité

Portabilité

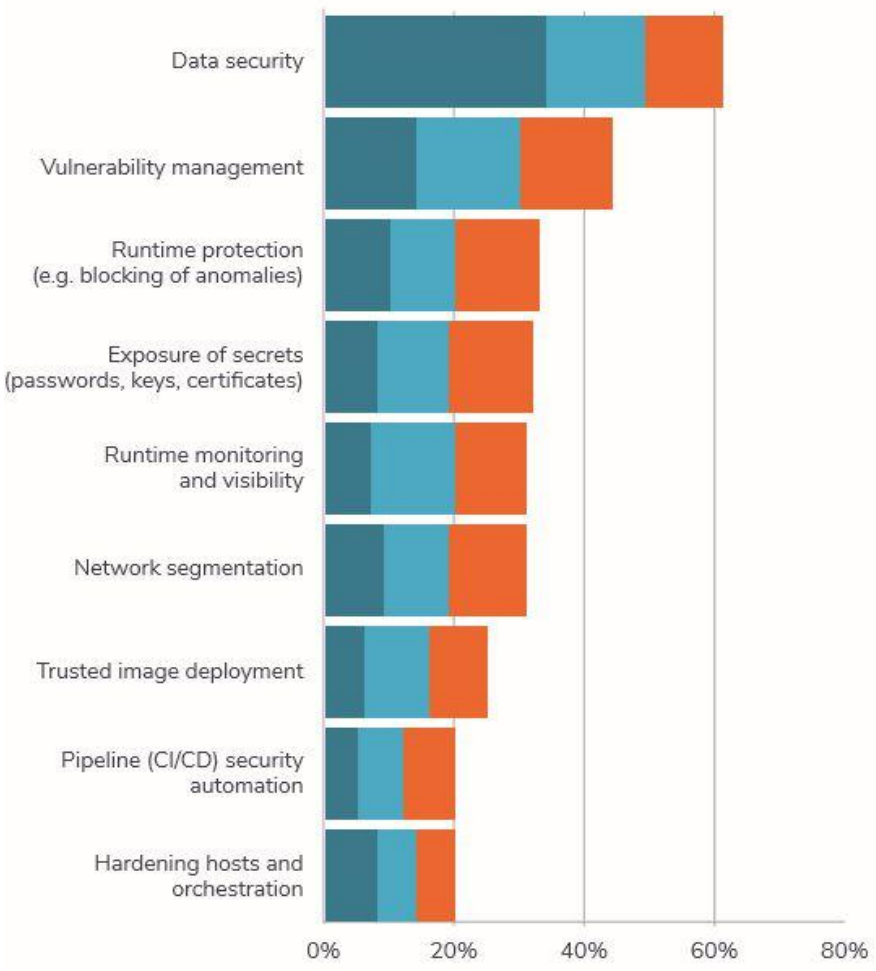
- **Les enjeux de sécurité en conteneur**
- Les bonnes pratiques
- Les solutions
- Démonstrations

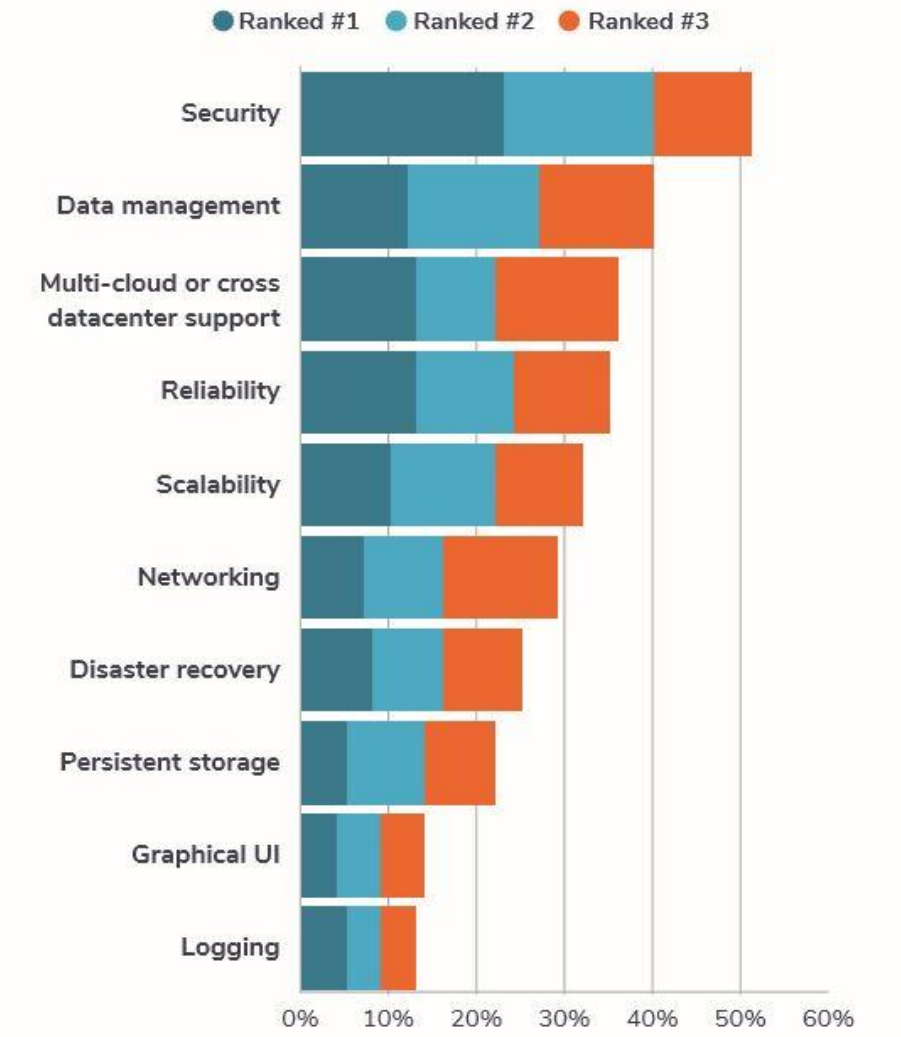
Red Hat

Les clients disent...

Data from The State of Container and Kubernetes Security 2020

La sécurité est **l'enjeu no.1** à l'adoption des conteneurs



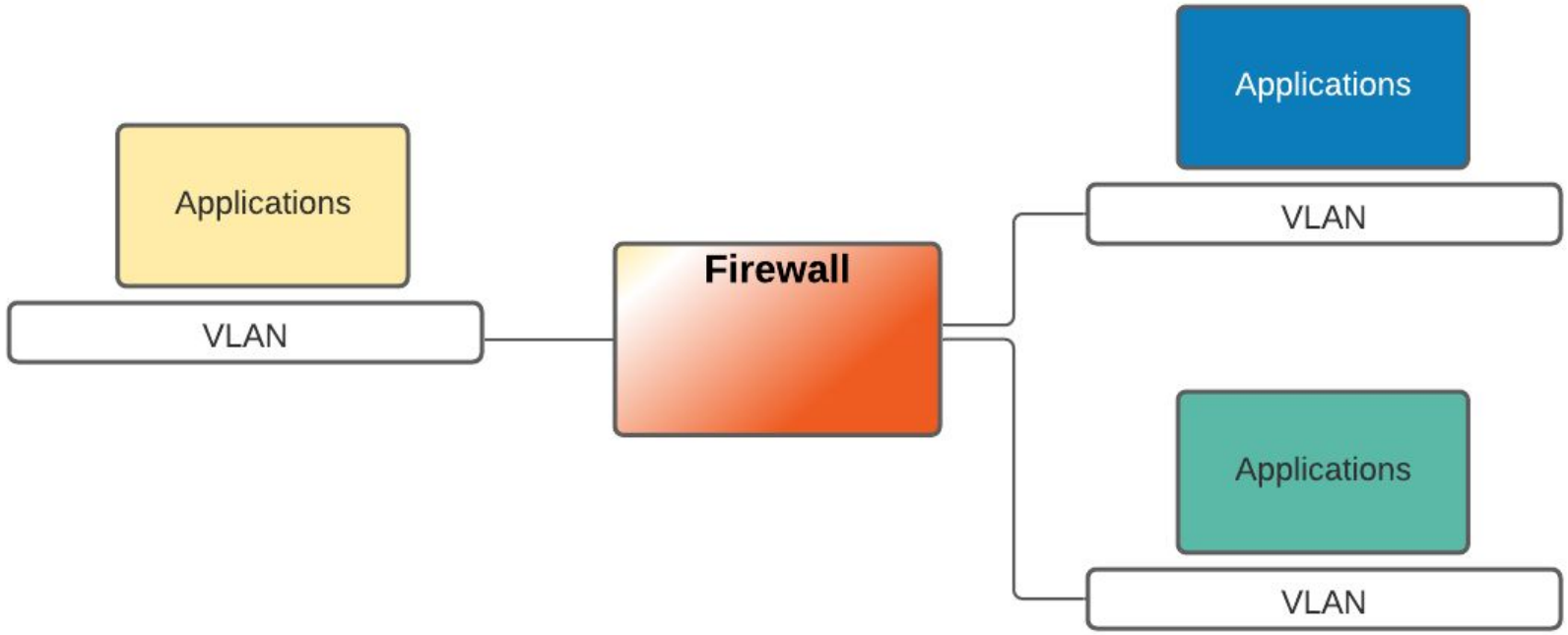


This State of Container and Kubernetes Security Report, Winter 2020, is our third edition of the report, this time compiling survey results from more than 540 IT professionals

Red Hat

Le bon vieux temps !

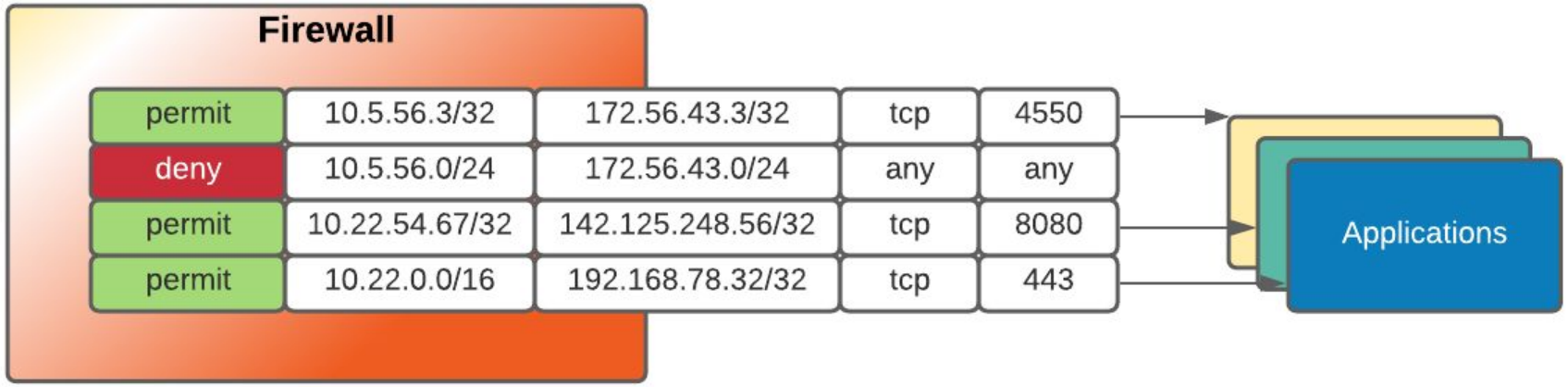
L'élément de sécurité principal est le coupe-feu



Red Hat

Le bon vieux temps !

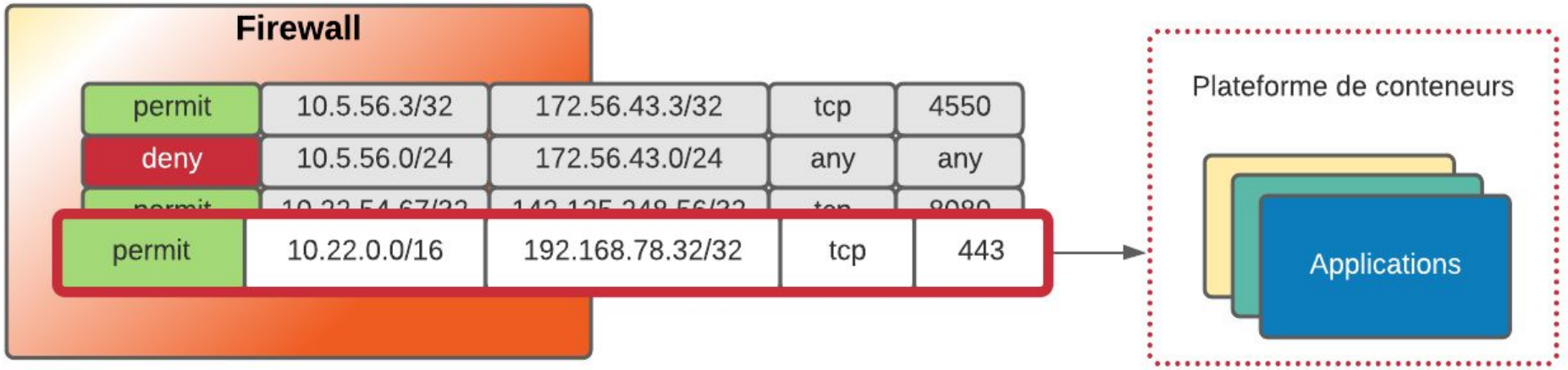
Faux sentiment de sécurité basé sur des configurations statiques



Red Hat

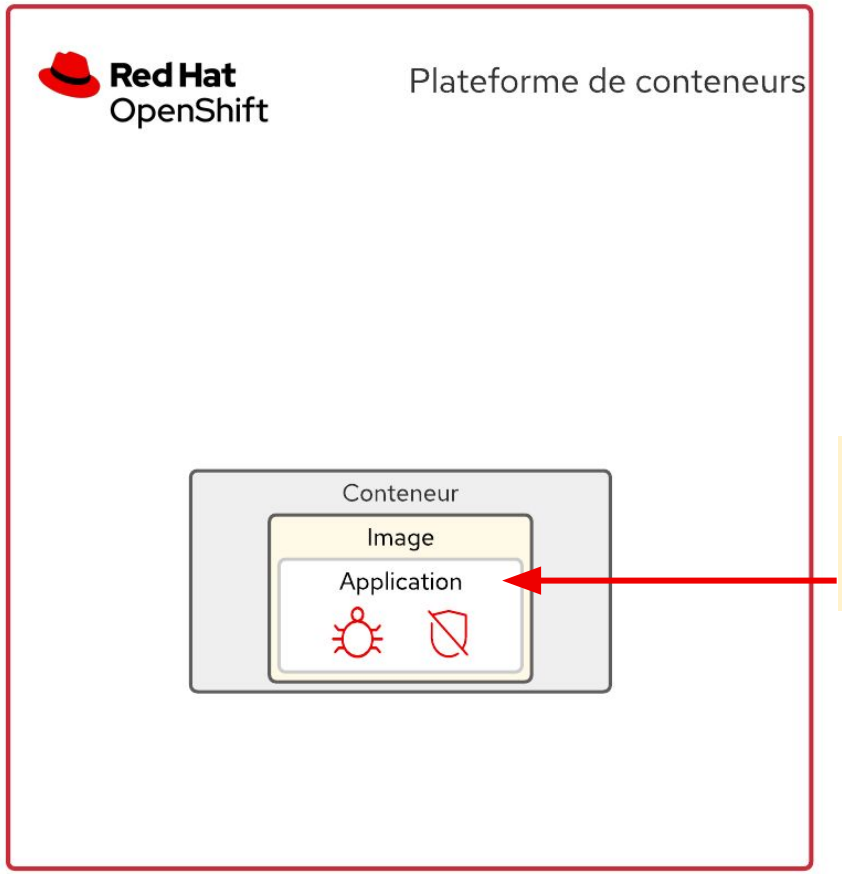
Applications modernes

Applications Web et serveurs API



Red Hat

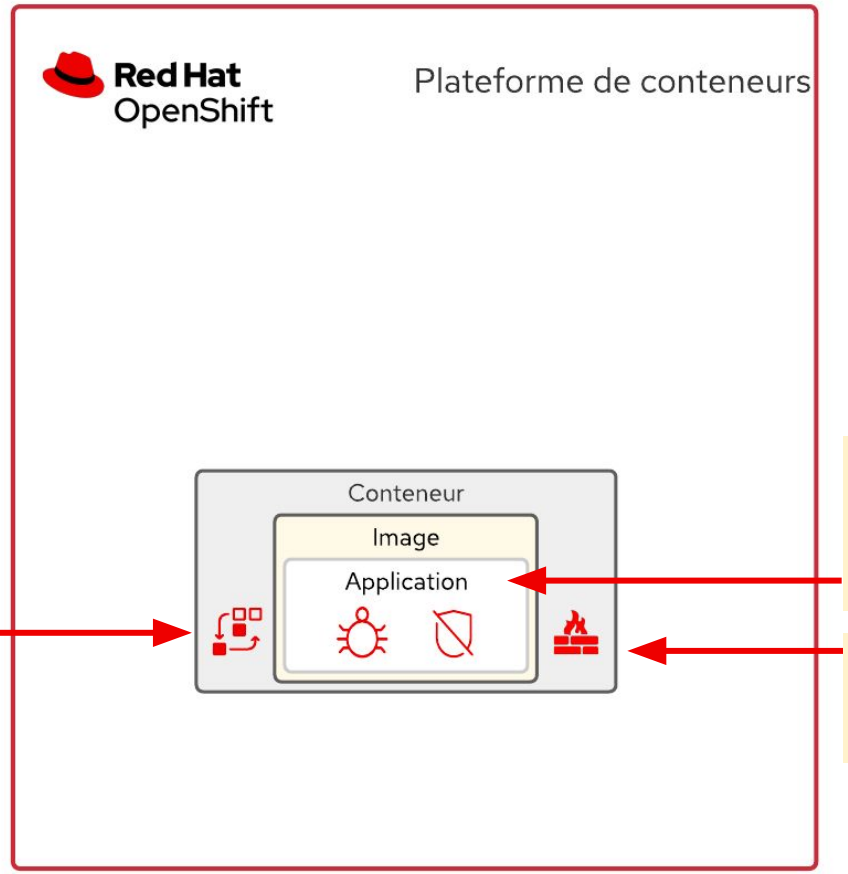
Détecter les vulnérabilités et restreindre l'exécution



Détecter et éviter l'exécution de conteneurs contenant des vulnérabilités

Red Hat

Appliquer des contrôles au niveau des déploiements



Les définitions des ressources Kubernetes doivent respecter des standards de sécurité

Détecter et éviter l'exécution de conteneurs contenant des vulnérabilités

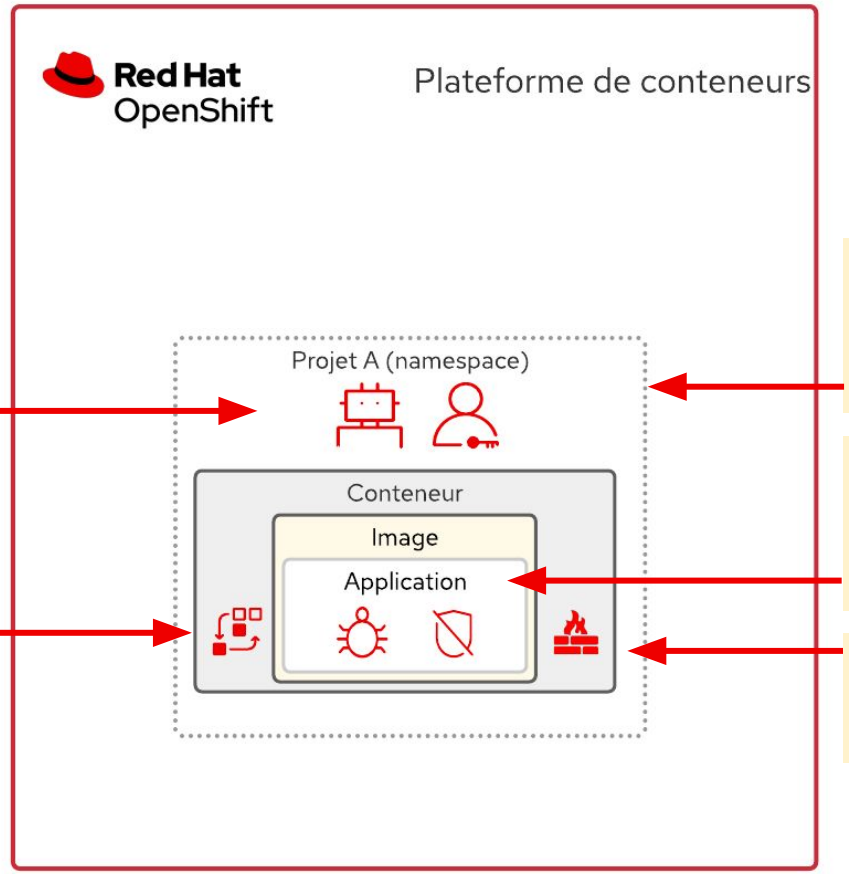
Règles d'isolation contrôle l'accès aux conteneurs

Red Hat

Segmenter les applications et contrôler l'accès

Contrôle des accès moderne basé sur la notion de jetons

Les définitions des ressources Kubernetes doivent respecter des standards de sécurité



Segmenter les applications dans des compartiments étanches (Projets, Namespaces)

Détecter et éviter l'exécution de conteneurs contenant des vulnérabilités

Règles d'isolation contrôle l'accès aux conteneurs

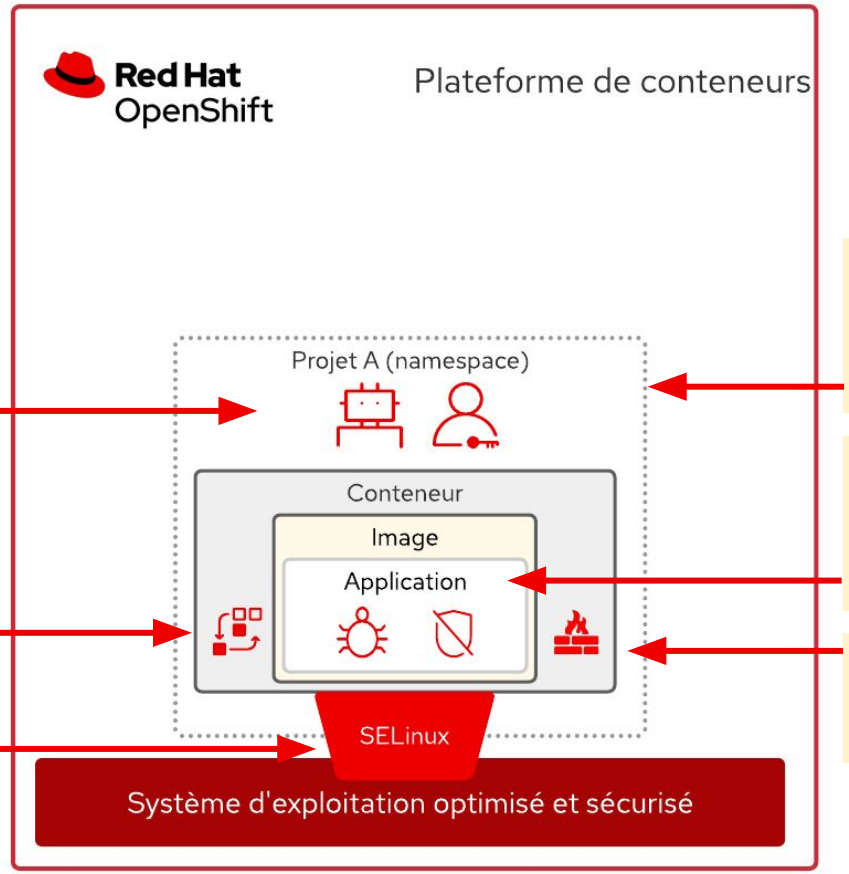
Red Hat

Utiliser un système d'exploitation sécuritaire et optimisé

Contrôle des accès moderne basé sur la notion de jetons

Les définitions des ressources Kubernetes doivent respecter des standards de sécurité

Système d'exploitation sous-jacent fournie l'isolation des processus



Segmenter les applications dans des compartiments étanches (Projets, Namespaces)

Détecter et éviter l'exécution de conteneurs contenant des vulnérabilités

Règles d'isolation contrôle l'accès aux conteneurs

Red Hat

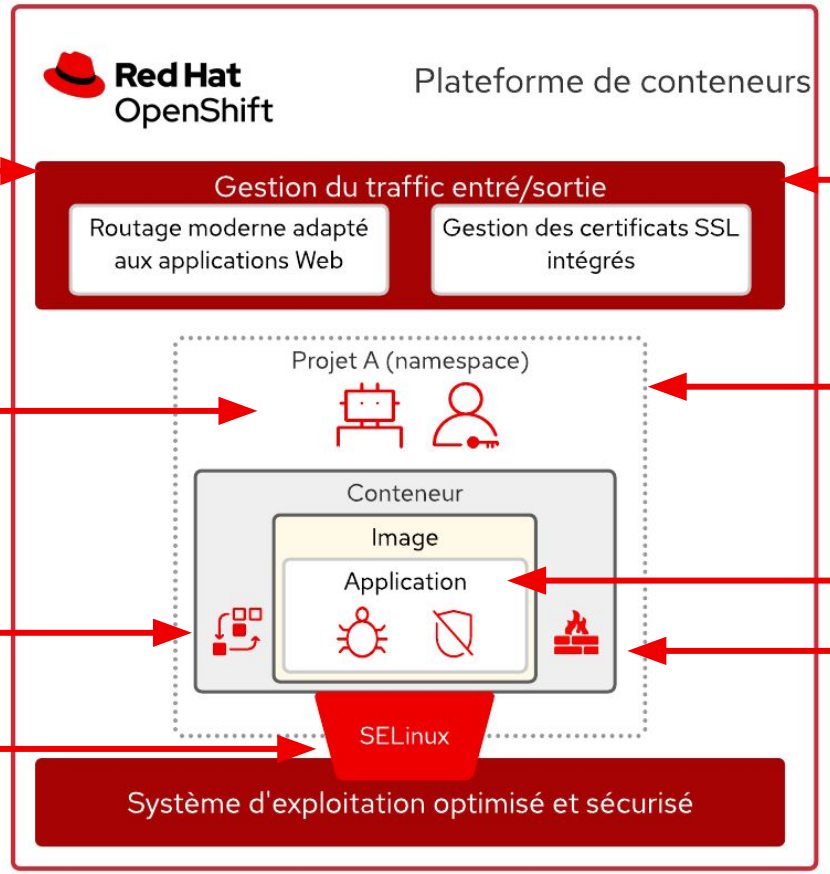
Contrôler et sécuriser le trafic applicatif

Contrôler l'accès réseau des applications

Contrôle des accès moderne basé sur la notion de jetons

Les définitions des ressources Kubernetes doivent respecter des standards de sécurité

Système d'exploitation sous-jacent fournie l'isolation des processus



Gestion des certificats centralisée. **Toutes** les applications mérites d'avoir un **certificat valide**

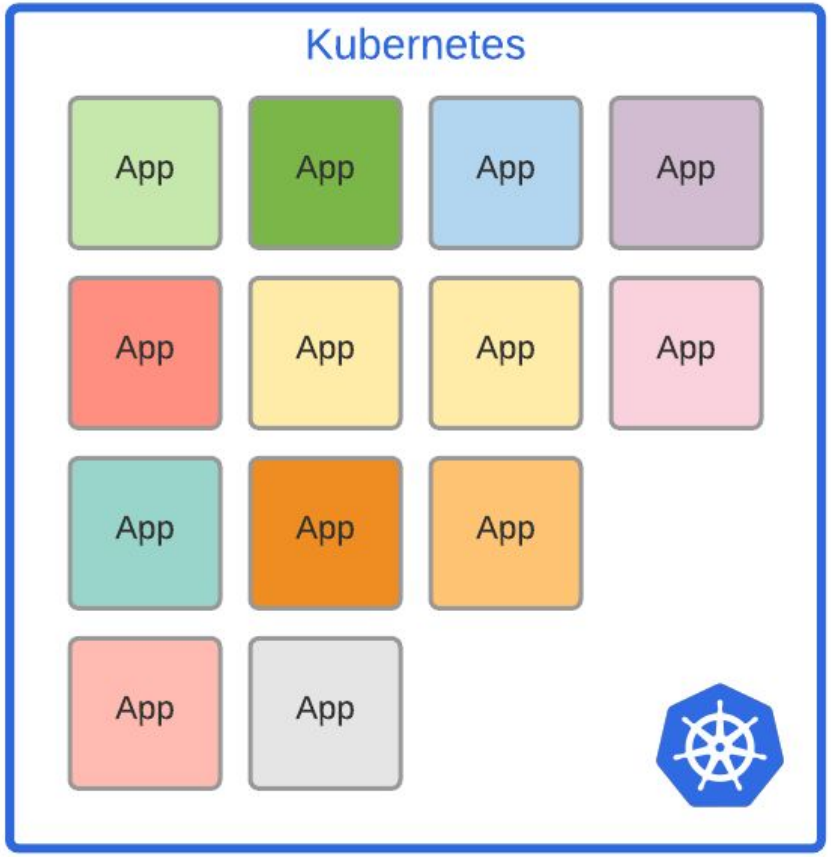
Segmenter les applications dans des compartiments étanches (Projets, Namespaces)

Détecter et éviter l'exécution de conteneurs contenant des vulnérabilités

Règles d'isolation contrôle l'accès aux conteneurs

Red Hat

Mais… on m’a dit que ça allait être facile, rapide… et Agile !



Red Hat

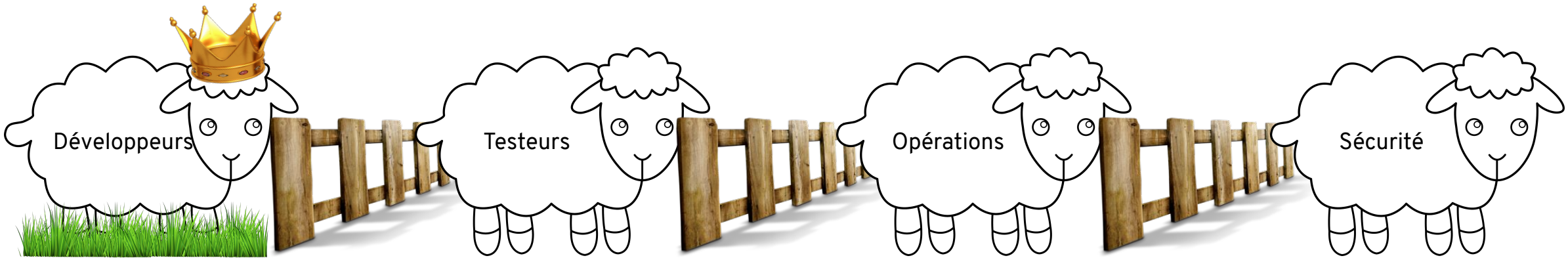
Sécurité

Conformité

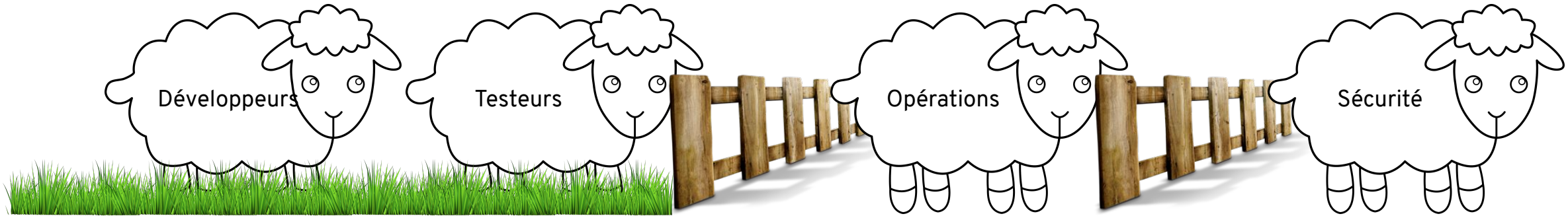
Portabilité

- Les enjeux de sécurité en conteneur
- **Les bonnes pratiques**
- Les solutions
- Démonstrations

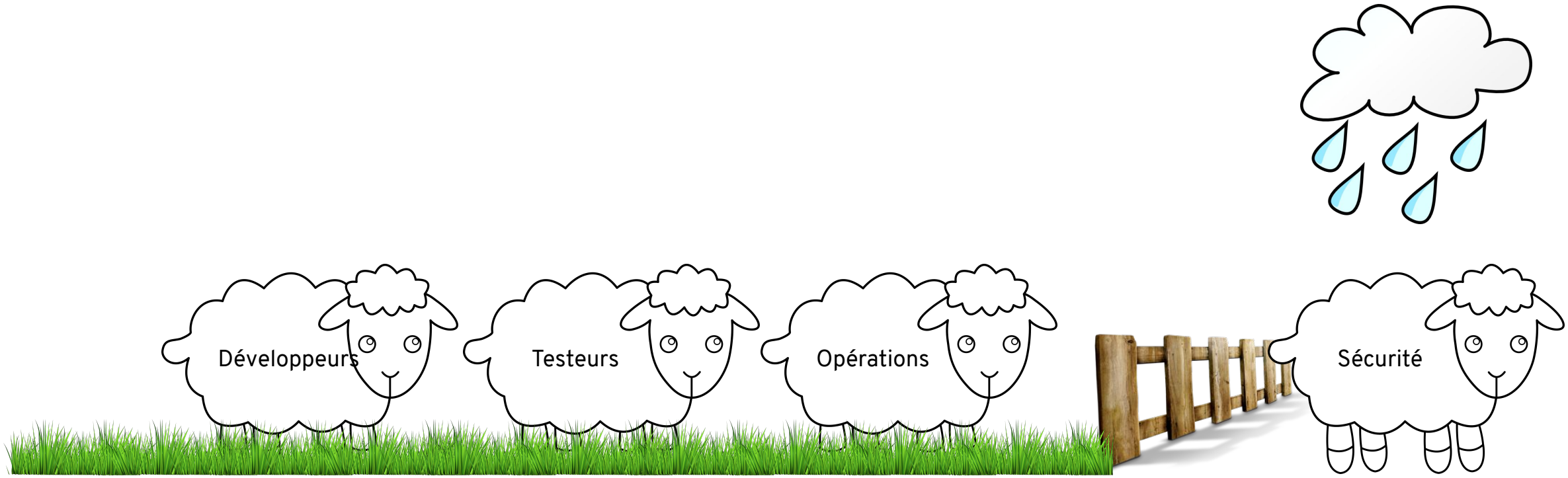
Red Hat


Développeurs
Testeurs
Opérations
Sécurité

Agile



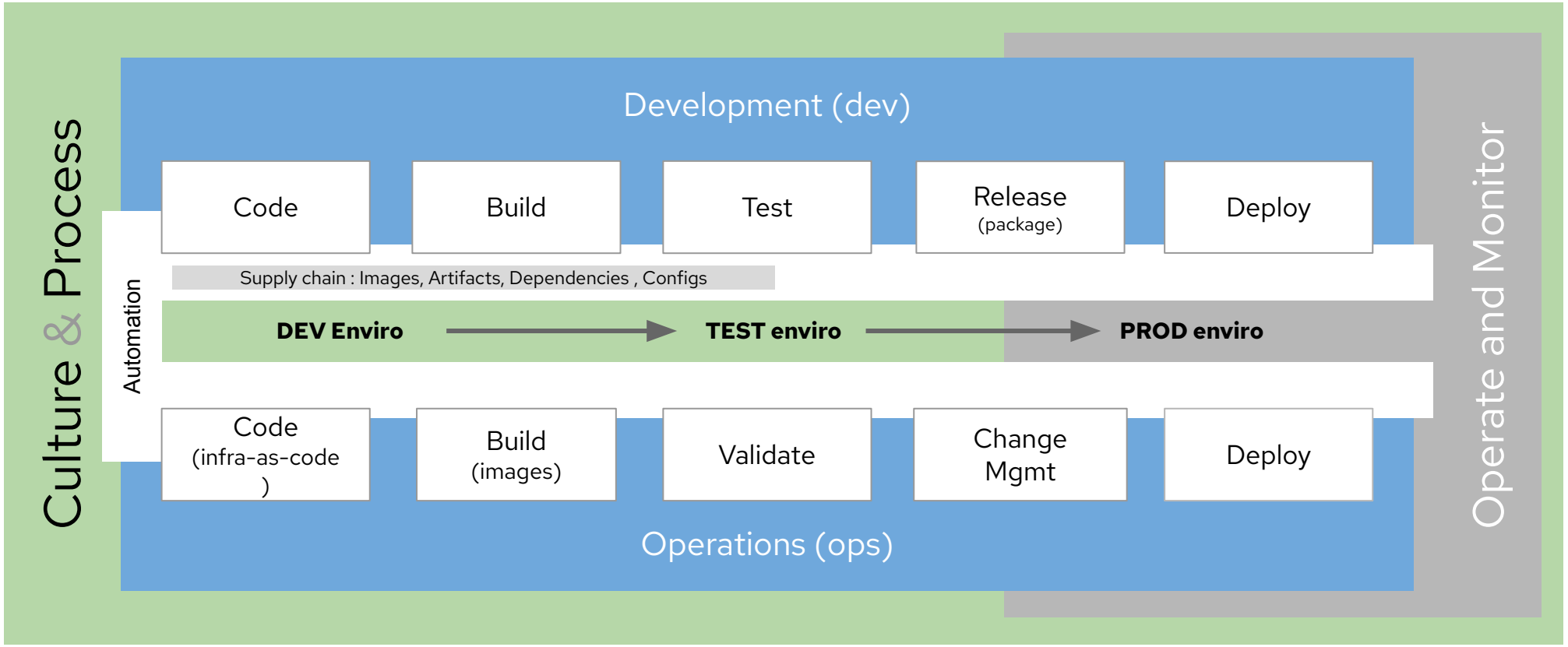
DevOps


Développeurs
Testeurs
Opérations
Sécurité

DevSecOps

Sécuriser le cycle de vie complet des applications avec DevSecOps

Sécurité omniprésente - Rendez-la ... Invisible



Red Hat

Sécurité

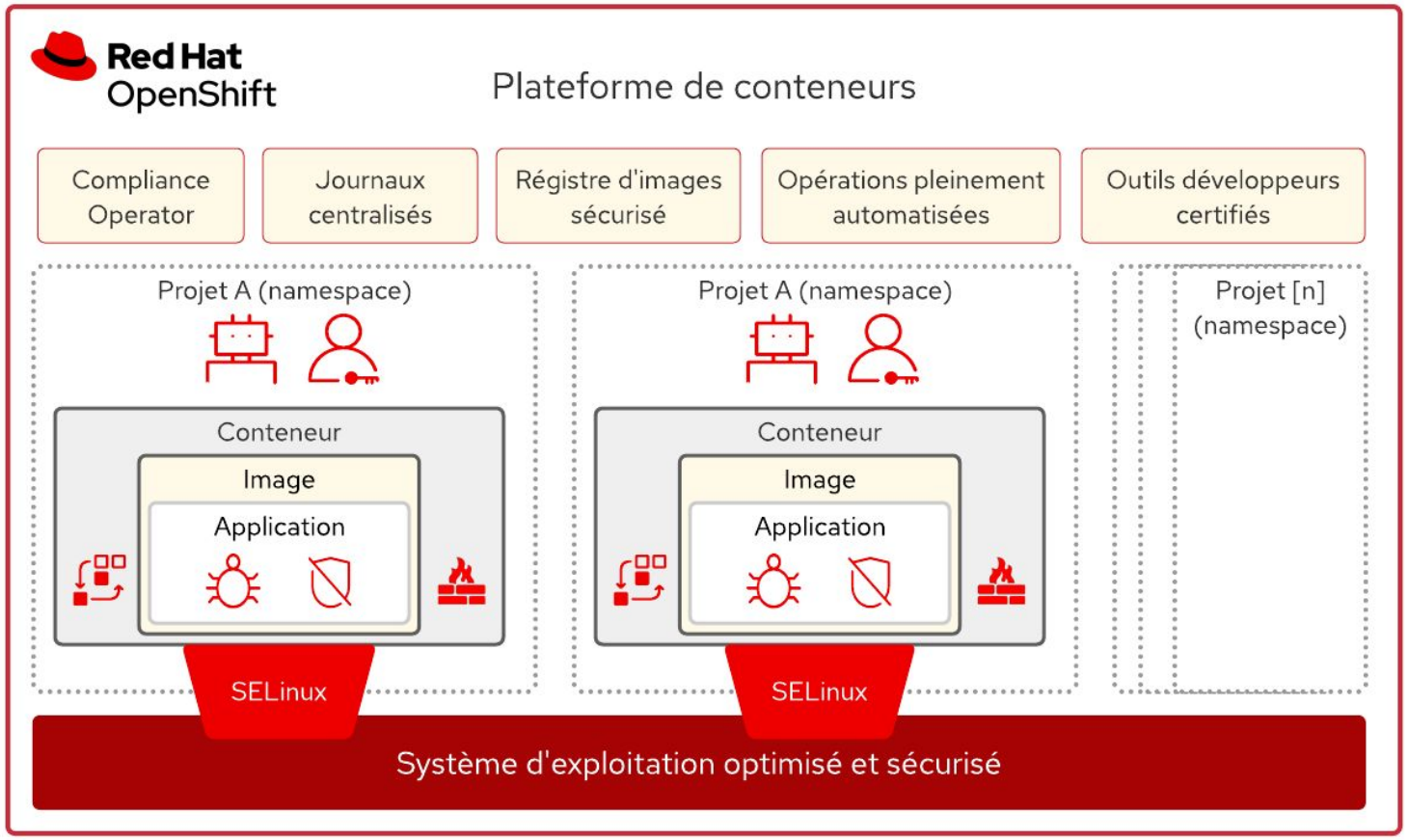
Conformité

Portabilité

- Les enjeux de sécurité en conteneur
- Les bonnes pratiques
- **Les solutions**
- Démonstrations

Red Hat

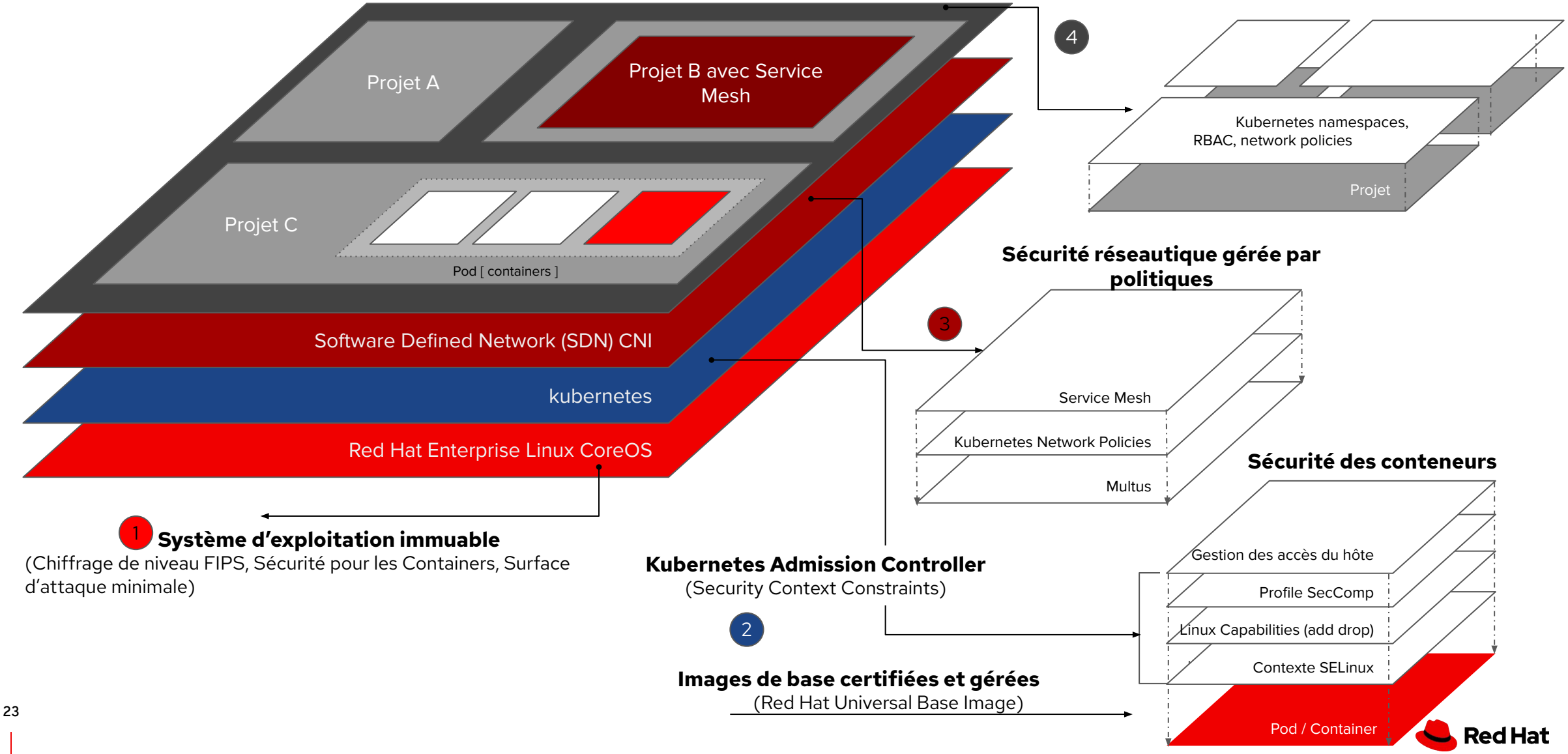
Importance d’une plateforme de conteneurs pour Entreprises



Red Hat

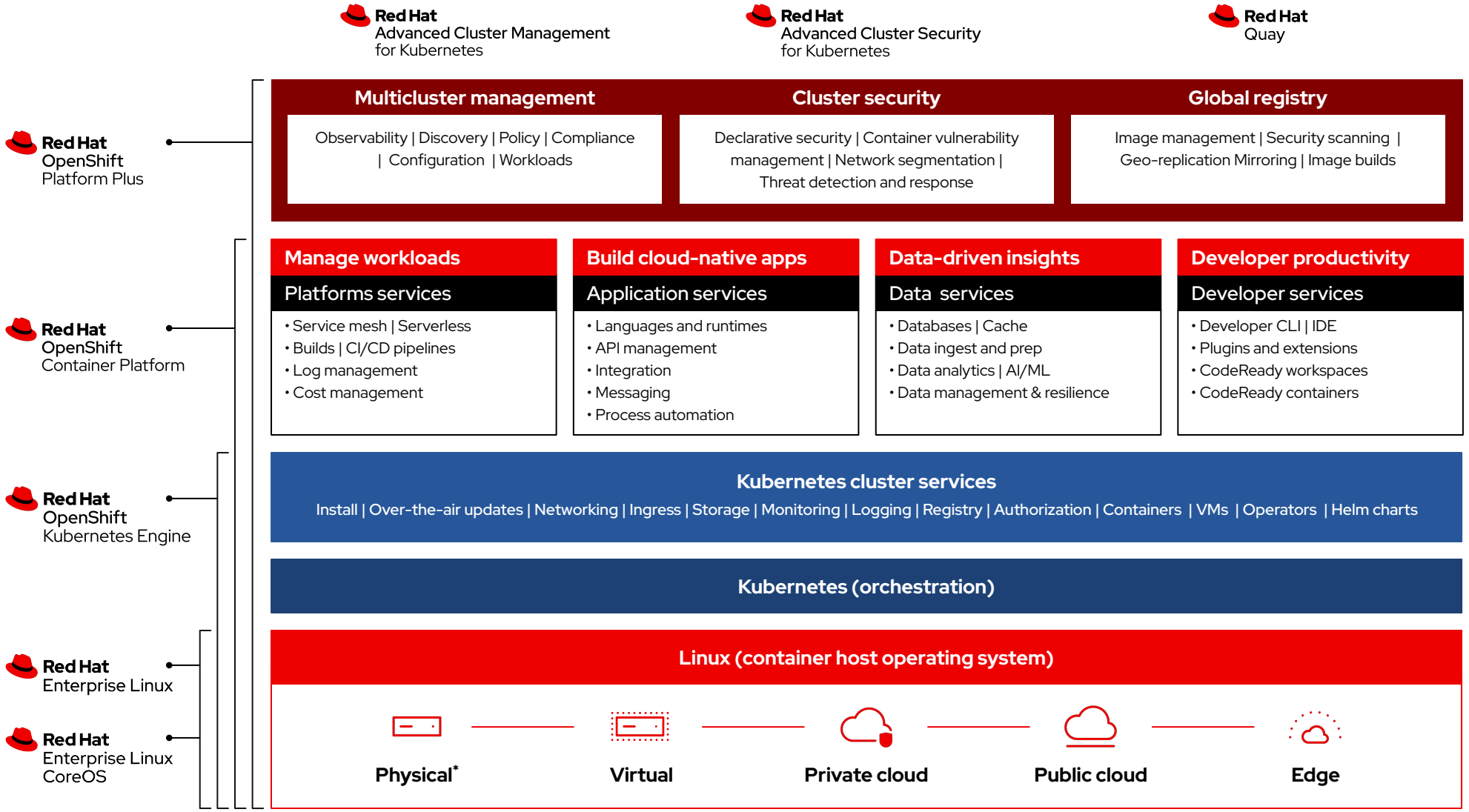
OpenShift Container Platform

Sécurité automatisée



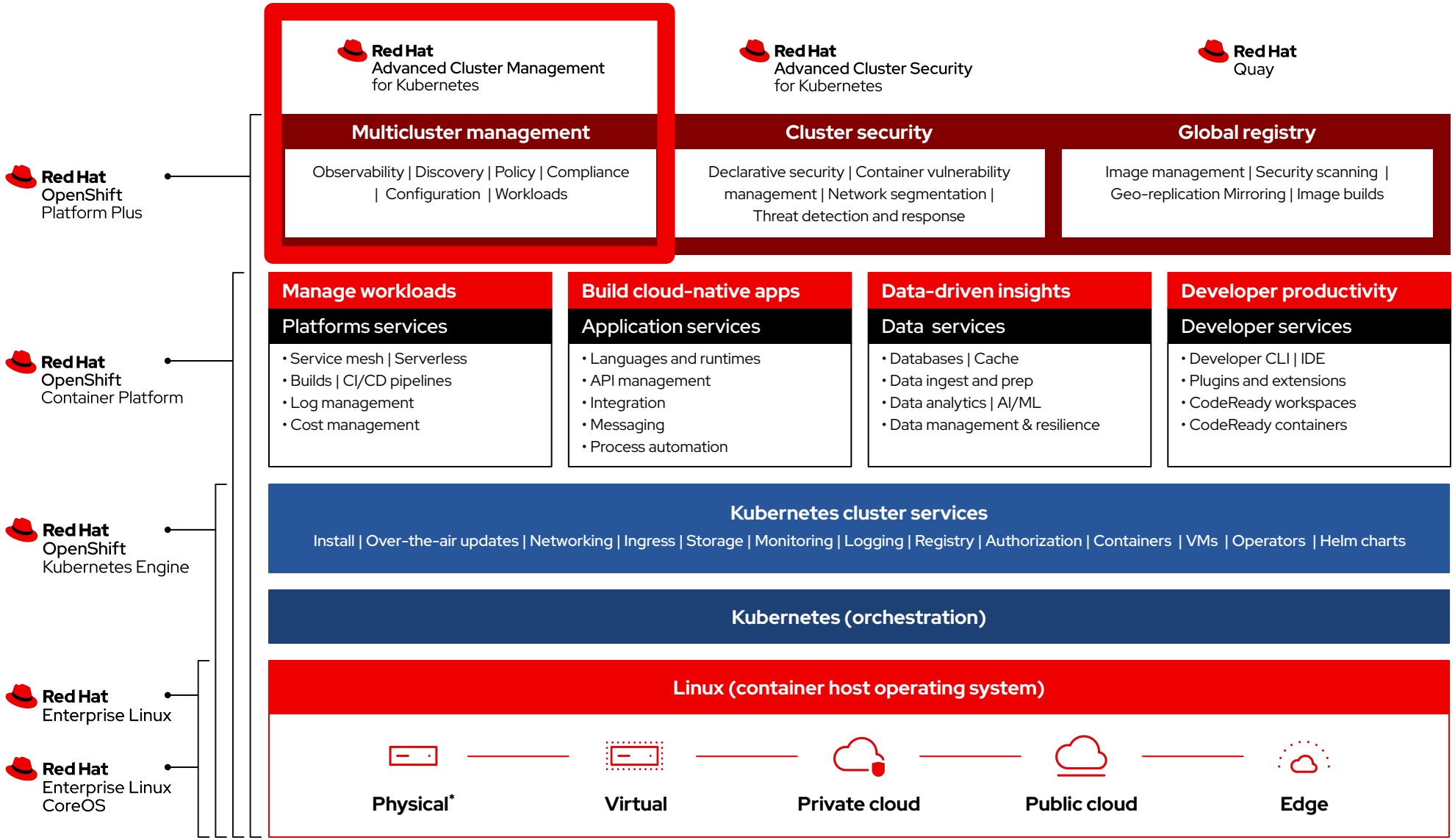
Red Hat

Red Hat open hybrid cloud platform



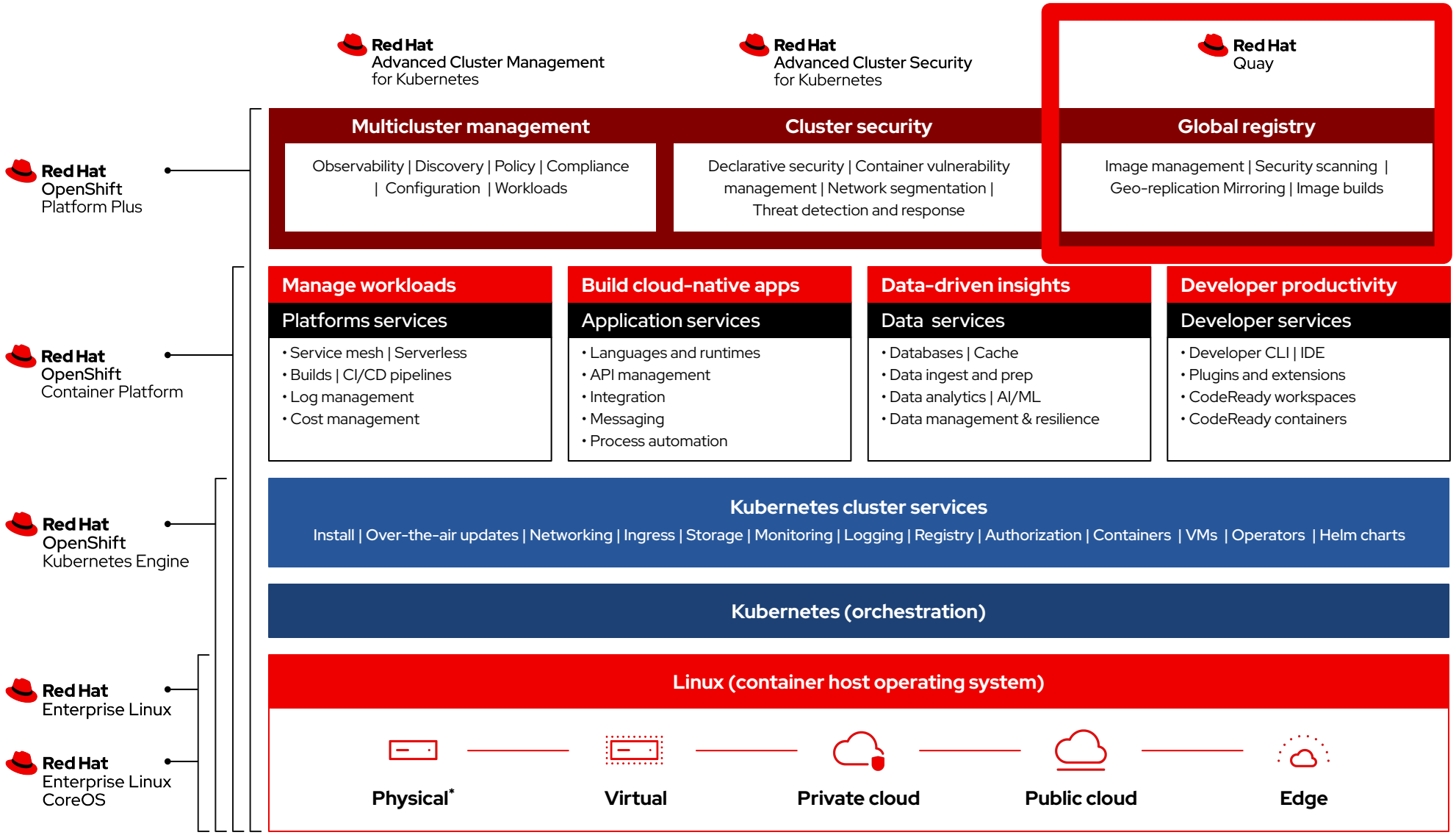
* Red Hat OpenShift® includes supported runtimes for popular languages/frameworks/databases. Additional capabilities listed are from the Red Hat Application and Data Services portfolio.

Red Hat open hybrid cloud platform



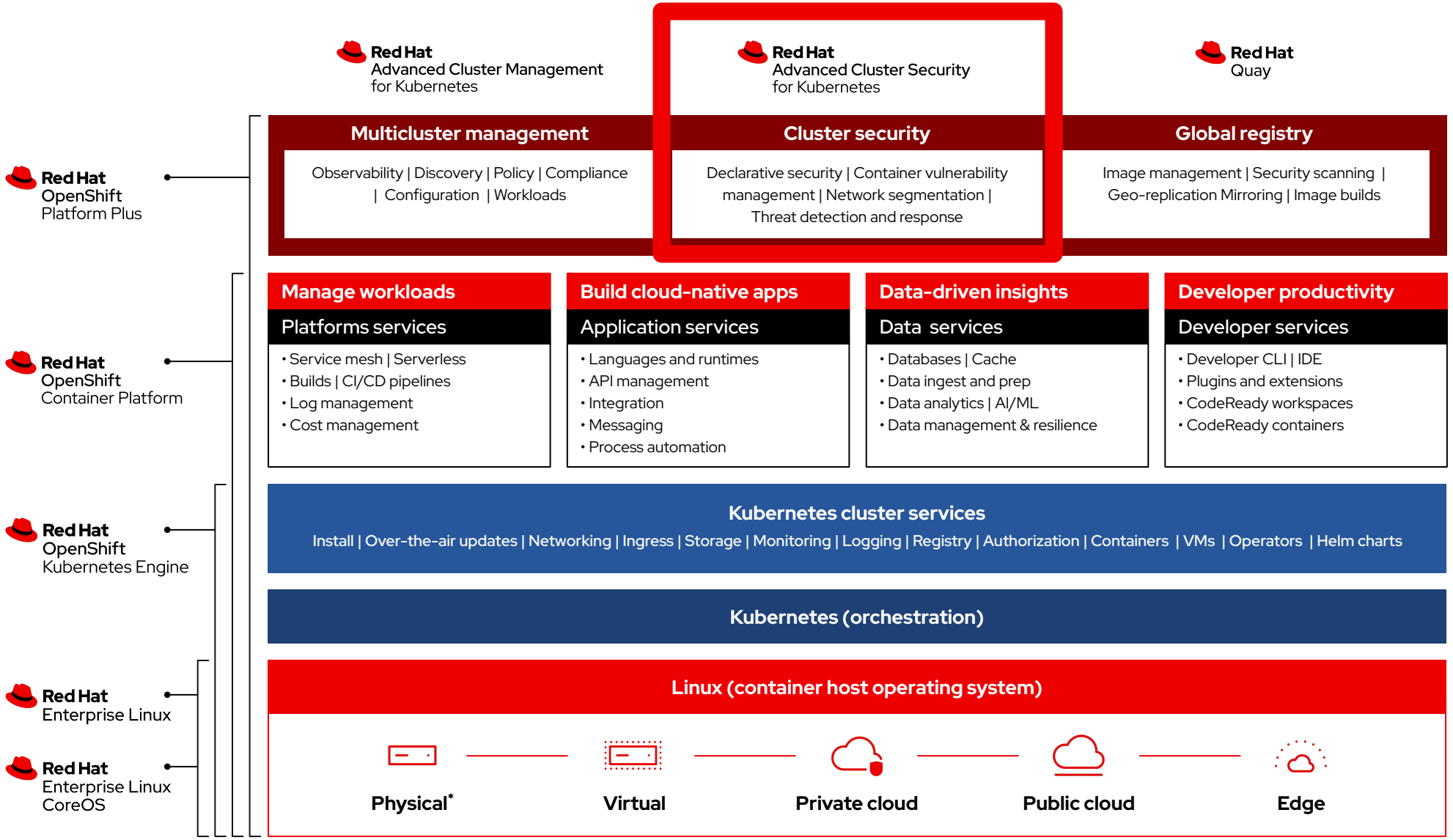
* Red Hat OpenShift® includes supported runtimes for popular languages/frameworks/databases. Additional capabilities listed are from the Red Hat Application and Data Services portfolio.

Red Hat open hybrid cloud platform

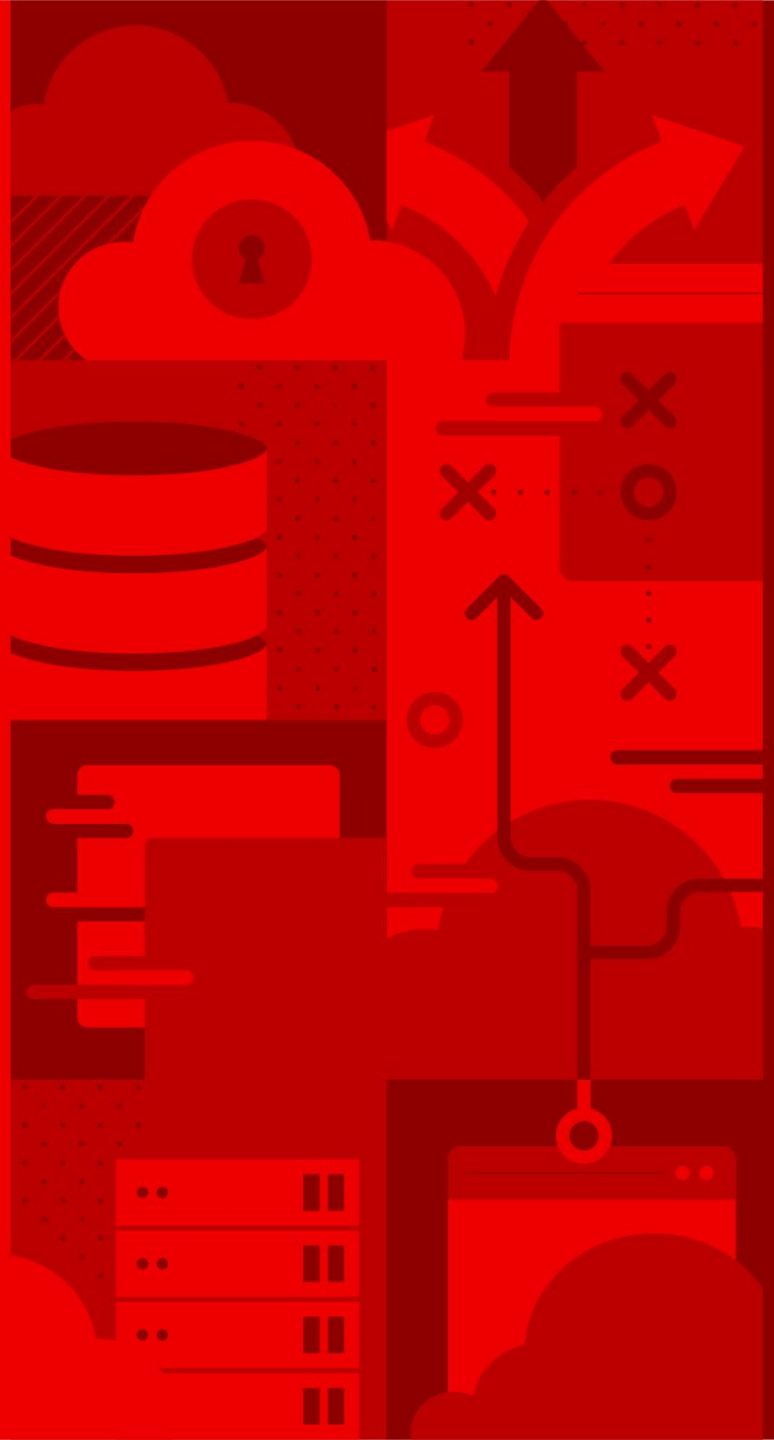


* Red Hat OpenShift® includes supported runtimes for popular languages/frameworks/databases. Additional capabilities listed are from the Red Hat Application and Data Services portfolio.

Red Hat open hybrid cloud platform



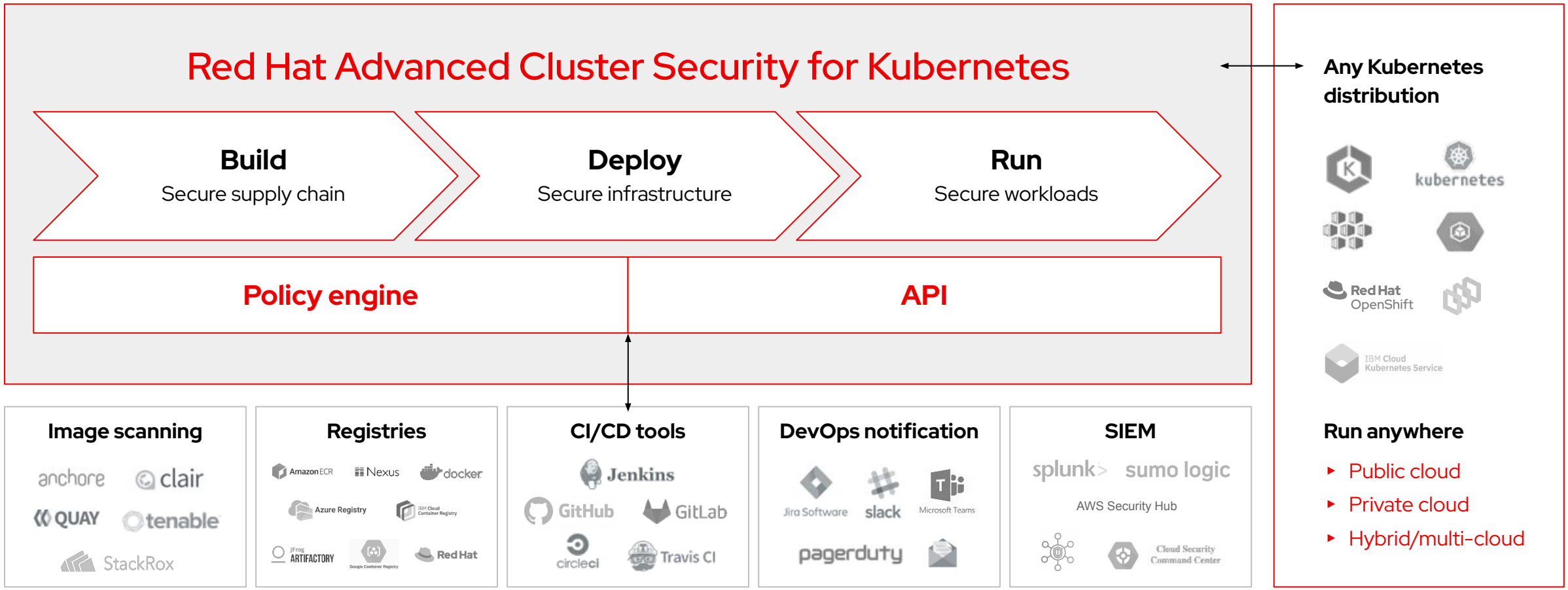
* Red Hat OpenShift® includes supported runtimes for popular languages/frameworks/databases. Additional capabilities listed are from the Red Hat Application and Data Services portfolio.



Advanced Cluster Security

Red Hat

La première plateforme de sécurité Kubernetes-native



Red Hat

Red Hat OpenShift provides a secure foundation

Detect

- Trusted content
- Container registry
- Build management
- CI/CD pipeline

Protect

- Kubernetes platform lifecycle
- Identity and access management
- Platform data
- Deployment policies

Respond

- Container isolation
- Network isolation
- Application access and data
- Observability

Build — **Deploy** — **Run**

DevSecOps

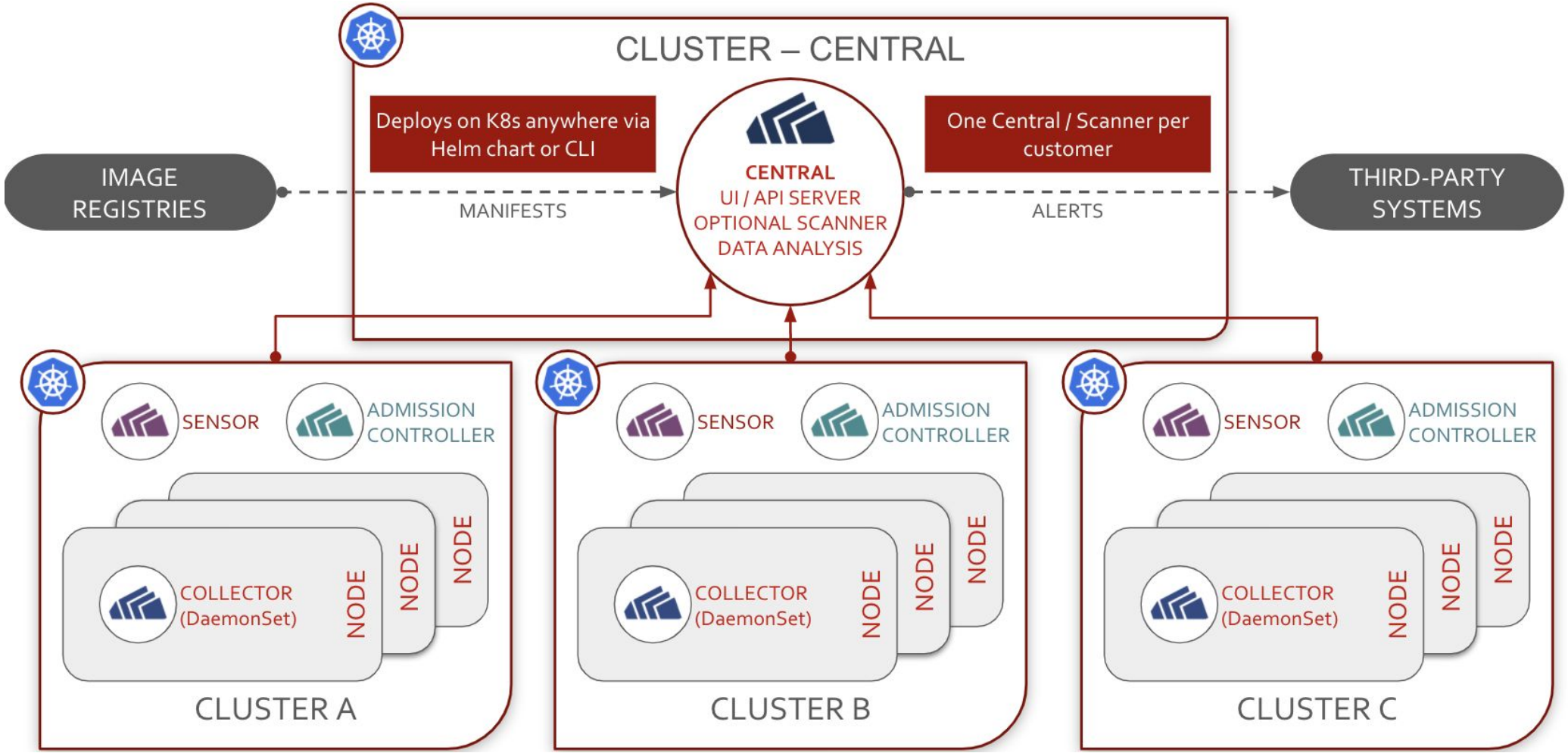
RHACS delivers security depth to entire application lifecycle

Detect	Protect	Respond
Trusted content	Kubernetes platform lifecycle	Container isolation
Container registry	Identity and access management	Network isolation
Build management	Platform data	Application access and data
CI/CD pipeline	Deployment policies	Observability
Vulnerability analysis	Image assurance and policy admission controller	Runtime behavioral analysis
App config analysis	Compliance assessments	Auto-suggest network policies
APIs for CI/CD integrations	Risk profiling	Threat detection / incident response

Build — **Deploy** — **Run**

DevSecOps

Architecture



Red Hat

8 sujets essentiels

Visibilité

Visibilité complète de votre infrastructure cloud native, y compris toutes les images, les registres de conteneurs, les configurations de déploiement Kubernetes, le comportement d'exécution des conteneurs, etc.

Gestion des vulnérabilités

Recherchez les vulnérabilités connues dans le cadre de votre pipeline CI / CD ou analysez les images déjà déployées. Recherchez les erreurs de configuration des applications ou encore des privilèges trop élevés.

Concepts DevSecOps

Appliquez des règles de sécurité au moment de la construction et du déploiement avant de déployer des images et des charges de travail. Intégrez l'analyse de vulnérabilité et de configuration dans le pipeline CI / CD.

Gestion des configurations

Utilisez la sécurité déclarative pour augmenter l'utilisation de la plate-forme, tout en diminuant les frictions et les risques.

8 sujets essentiels

Profilage du risque

Priorisation heuristique des résultats relatifs à la sécurité en fonction de l'impact et de la probabilité d'un compromis

Conformité et audits automatisés

Fournit des contrôles de sécurité spécifiques aux normes CIS, NIST, PCI et HIPAA, avec plus de 300 contrôles et des évaluations de conformité continues.

Segmentation du réseau

Découvrez et affichez les informations de stratégie et de flux réseau pour les clusters, les projets et les charges de travail. Générez automatiquement des stratégies réseau et prévisualisez ou simulez les chemins de connectivité avant d'appliquer de nouvelles stratégies.

Runtime detection and response

L'analyse comportementale d'exécution détermine le comportement de base et alerte en cas de comportement anormal. Tirez parti de la collecte et de la corrélation de données approfondies pour identifier les menaces et permettre une analyse en profondeur..

Red Hat

Sécurité

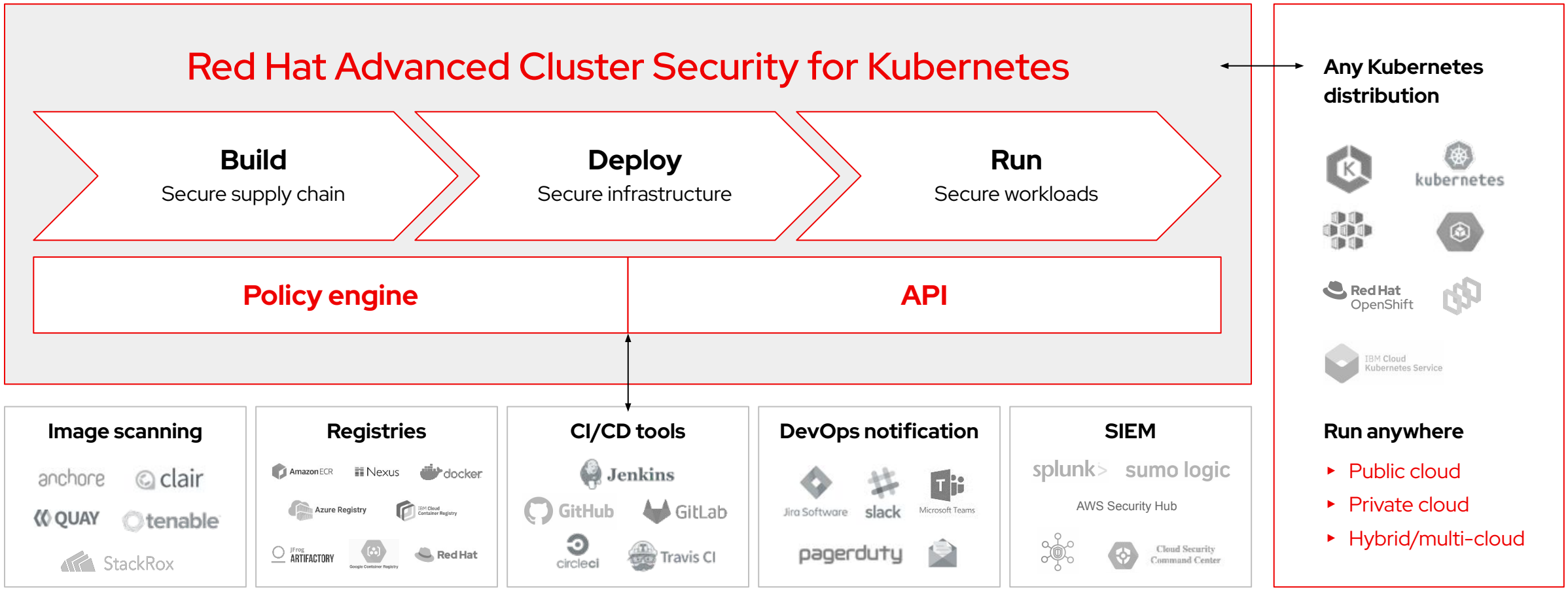
Conformité

Portabilité

- Les enjeux de sécurité en conteneur
- Les bonnes pratiques
- Les solutions
- **Démonstrations**

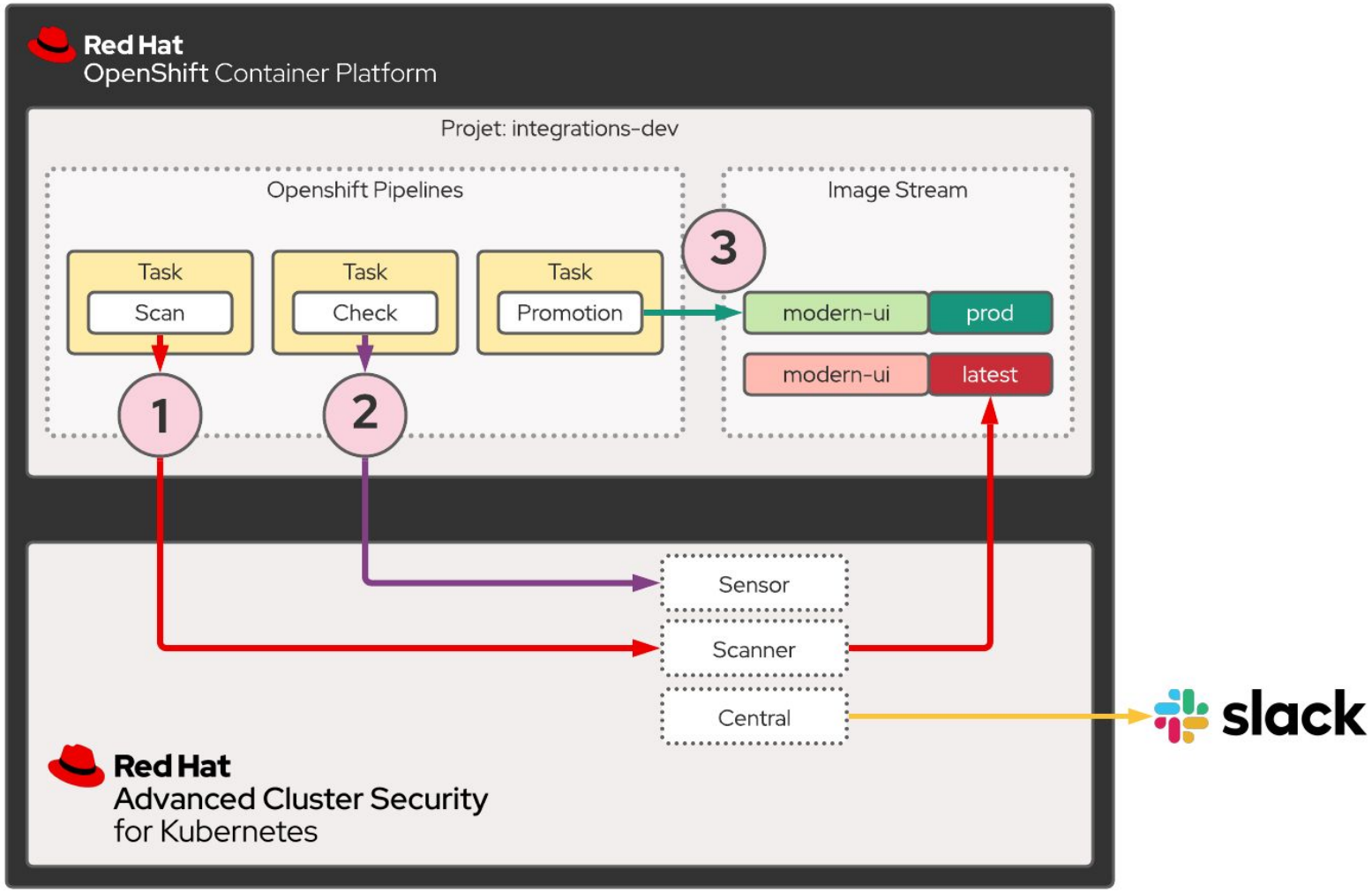
Red Hat

La première plateforme de sécurité Kubernetes-native



Red Hat

Démo 1



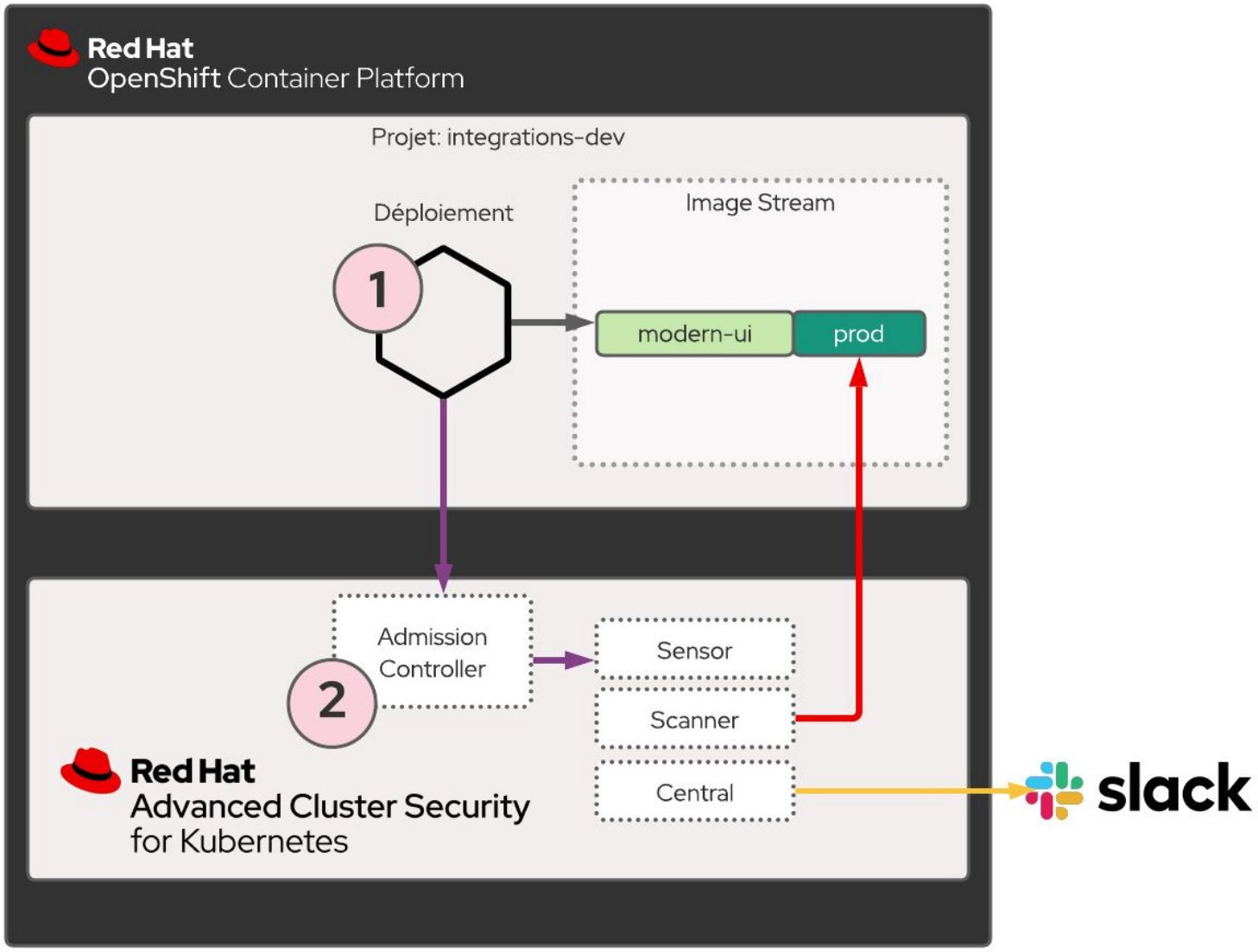
Build

Empêcher la promotion d'une image contenant des vulnérabilités catégorisées Importantes

Améliorer la collaboration de la sécurité et des développeurs

Red Hat

Démo 2



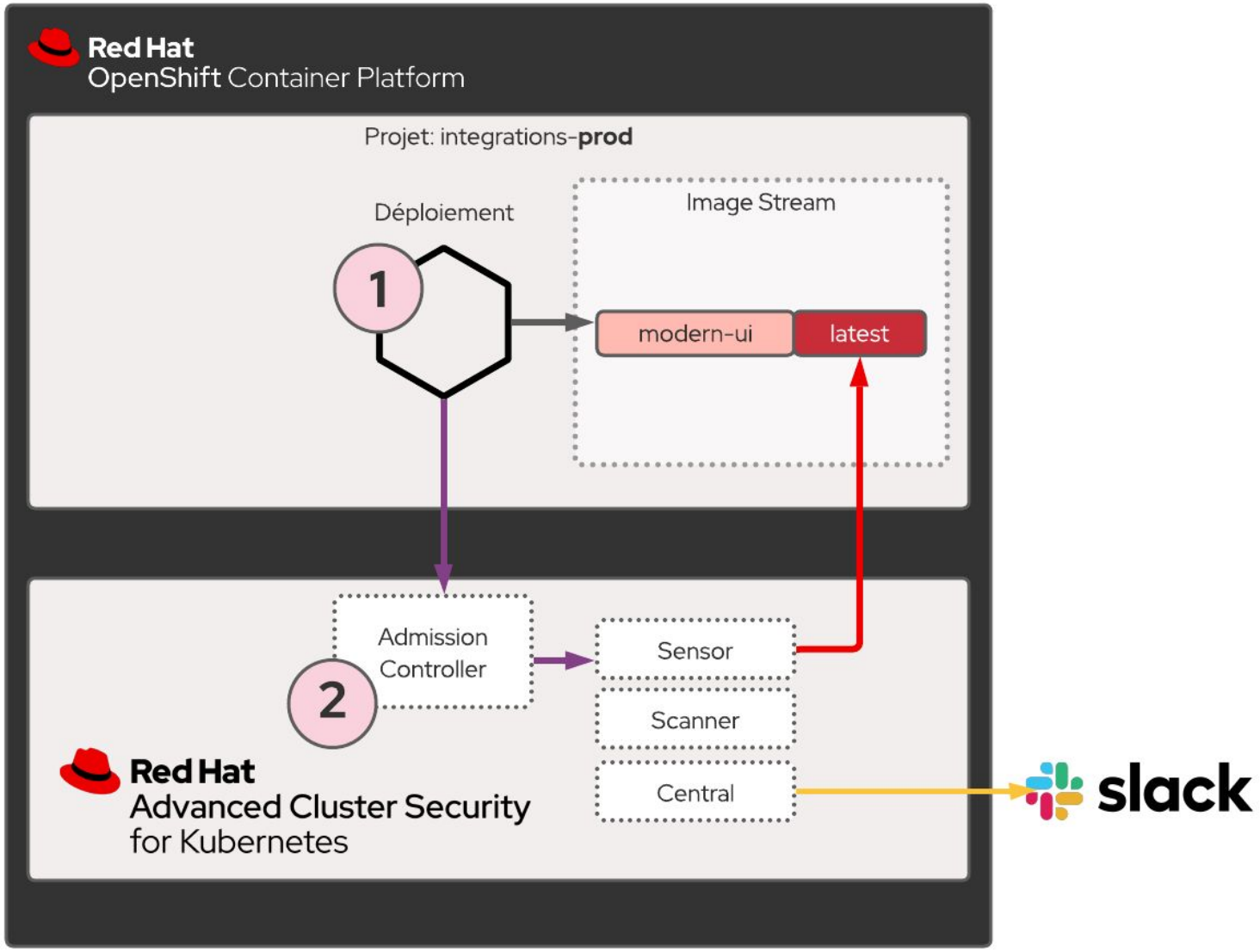
Deploy

Empêcher un déploiement d'une image contenant des vulnérabilités catégorisées Importantes

Assurer la sécurité des déploiements applicatifs

Red Hat

Démo 3



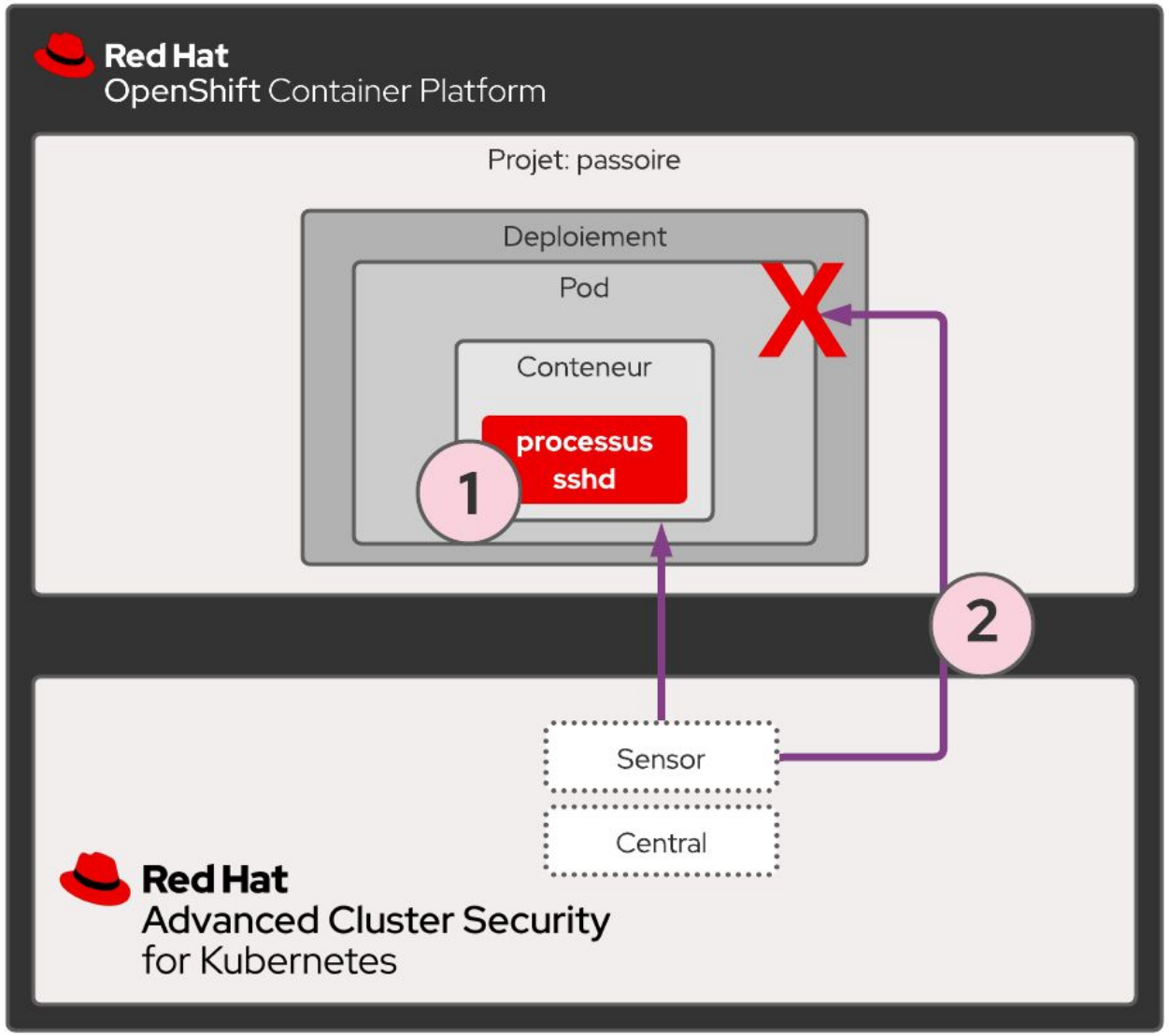
Deploy

Empêcher un déploiement en production avec le tag latest

Assurer la conformité des environnements

Red Hat

Démo 4



Run

Empêcher l'exécution de processus malicieux

Améliorer le contrôle et la sécurité des infrastructures

Red Hat

Merci !


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat