HCLTech | Red Hat

HCLTech container security service

Leverage the power of unified coherent container security in the face of growing global concerns

HCL

Application container technologies have gained high acceptance and usage in the past two years. According to the 2021 Annual Survey by Cloud Native Computing Foundation (CNCF), 96% of organizations worldwide are either using or evaluating Kubernetes – establishing it as a mainstream technology for container orchestration. Very few virtualization environments provide the kind of portable, flexible, reusable and automatable features that containers offer.

However, the growing adoption of containerization has placed it in plain sight of cyber attackers. Security is, therefore, one of the biggest challenges slowing container adoption. So much so that security concerns have delayed application rollouts in 55% of surveyed organizations in the last year alone. The fact that orchestration-led containerization is far more challenging to secure compared to other computer platforms further complicate matters. And often, the implementation of Kubernetes security solutions are marked by sluggish development and failure to protect the entire application development lifecycle.

Red Hat Advanced Cluster Security (ACS): A way forward

Implementing security measures in Kubernetes-based environments are hampered by complex traffic flow. Extracting and identifying risk indicators, in runtime, across thousands of running pods in a standard environment is often a Herculean task.

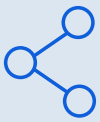
Red Hat ACS provides a set of cutting-edge runtime tools to monitor microservices, enforce compliance policies and detect and thwart attack attempts across a multitude of clusters in an easy, unified manner.

Deployment-centric visibility

ACS delivers visibility around deployments across namespaces and clusters

Multi-factor risk profiling

ACS uses risk ranking tied to common vulnerabilities and contextual Kubernetes data for prioritizing remediation



Network segmentation

ACS leverages Kubernetes network policies for network segmentation visualization and is designed for scale

Compliance

ACS provides built-in checks for CIS, NIST, PCI DSS, HIPAA and one-click audit checks

Configuration management

ACS provides several out-of-the-box policies designed to prevent misconfigurations in the Kubernetes environment

Designed for Kubernetes

ACS' architecture is designed to secure Kubernetes environments through declarative definitions and an immutable infrastructure inherent to Kubernetes

Coherent network security

ACS leverages the built-in network policy capabilities in Kubernetes to enforce network segmentation at scale automatically. This approach ensures that security works with, not against, how developers and operators build and operate clusters

Unified security

ACS can be a standalone security solution for Kubernetes clusters running anywhere, including on managed services via cloud and self-managed clusters

Integration

ACS is fully integrated with the OpenShift platform and combined with Advanced Cluster Management (ACM) and Red Hat Quay

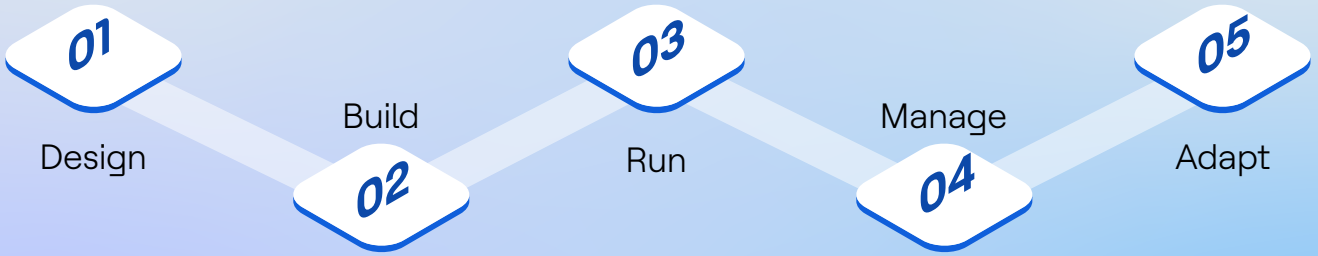
Annual Survey 2021: https://www.cncf.io/wp-content/uploads/2022/02/CNCF-AR_FINAL-edits-15.2.21.pdf
State of Kubernetes security report: https://www.redhat.com/rhdc/managed-files/cl-state-of-kubernetes-security-report-2022-ebook-f31209-202205-en.pdf

HCLTech's Container security services:A one-stop container resilience offering

As a long-standing global SI partner for Red Hat, HCLTech has developed comprehensive container security offering built on Red Hat's Advanced Cluster Security platform. The solution leverages a Kubernetes-native approach to bake in security across the entire software development lifecycle while securely building, deploying and running cloud-native applications anywhere.

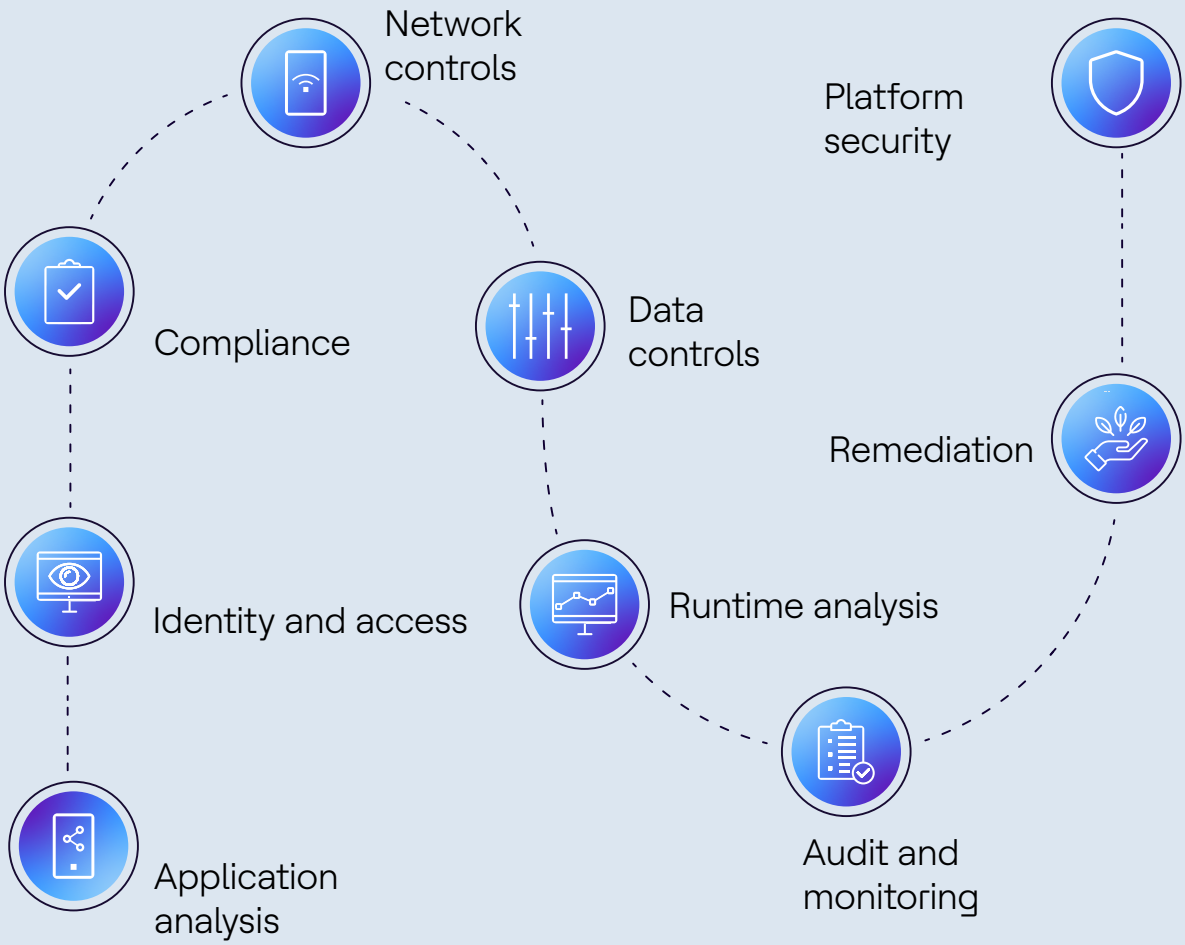
HCLTech's container security service is based on a philosophy of integrating security with development/DevOps. This solution ensures continuous security measures integrated throughout the entire software development lifecycle. It does this early in the development process by identifying security requirements and governance models and building in security at the very start. This is in complete variance with the standard practice of implementing pre-defined security policies bolted on at a later stage. The HCLTech solution then deploys applications to trusted platforms with multiple enhanced security capabilities. These include automated security and compliance systems and a continuous process of revising, updating and remediating issues mapped to a changing threat landscape.

Security policy, process & procedures



Integrated security approach

Security categories covered:



Why HCLTech container security service?

Benefits

1. Increase developer velocity and productivity by automating DevSecOps
2. Harden Kubernetes for more resilient and compliant clusters
3. Reduces costs by addressing security and compliance issues throughout the application development lifecycle
4. Mitigate threats using Kubernetes-native controls to enforce security policies
5. Leverage integrated governance guardrails through Kubernetes and the existing CI/CD pipeline to increase development speed without compromising on the security posture

For more information: https://www.hcltech.com/

HCLTech | Supercharging Progress™

hcltech.com

HCLTech is a global technology company, home to 211,000+ people across 52 countries, delivering industry-leading capabilities centered around Digital, Engineering and Cloud powered by a broad portfolio of technology services and software. The company generated consolidated revenues of $11.79 billion over the 12 months ended June 30, 2022. To learn how we can supercharge progress for you, visit hcltech.com.