COMPANY DESCRIPTION
In an environment where application development must be fast and flexible, containers are here to stay. Adoption is accelerating, but with it comes risk.

Anchore makes it possible to ensure security and compliance throughout the software development lifecycle. Without sacrificing speed. Through policy definition and in-depth image analysis, it delivers a way to make container development and deployment secure from the start. All designed for the fluid nature of containers.

Anchore sets a trusted standard for containers. It empowers you to analyze and certify your containers, making them predictable and protectable, so you can deploy containers with confidence.

PRODUCT PROFILE
Anchore is an open platform for container security and compliance that allows developers, operations and security teams to discover, analyze, and certify container images. Anchore lets ops and developer teams to perform detailed analysis, run queries, produce reports and define policies on container images that can be used in CI/CD pipelines to ensure that only containers that meet an organization’s requirements are deployed into production.

OVERVIEW
Anchore is an open platform that provides security and compliance for container native applications.

EXECUTIVE SUMMARY
As organizations develop and deploy an increasing number of critical container-native applications, they are challenged with ensuring the ongoing security and policy compliance of these applications without undermining the benefits that continuous integration and deployment practices bring to software delivery.

Anchore has partnered with RedHat to ensure security and compliance enforcement for RedHat container deployments through the open source Anchore Engine and Anchore Enterprise platforms.

STATEMENT FROM PARTNER
“Security and compliance are top of mind for enterprises deploying container into production environments. As RedHat solutions like OpenShift continue to grow in popularity, Anchore’s best-in-class deep analysis and policy management platform helps to ensure that users can certify the contents of container deployments and ultimately enterprises can deploy their containers with confidence.”

STATEMENT FROM RED HAT CONNECT
“Developers and architects looking to build new applications in, and for the cloud, or migrate existing applications to a cloud-based infrastructure, partner with Red Hat to develop and deliver more supportable solutions sooner.” said Mike Werner, Sr. Director, Global Technology Partners, Red Hat. “Red Hat certification assures a supportable platform for all types of customer deployment models. Red Hat is thrilled to work with software partners like Anchore resulting in the world’s largest open, and commercially supportable application ecosystem.”
Anchore is a Red Hat certified container and is available for customer download from the Red Hat certified container registry.

https://access.redhat.com/containers/#/vendor/anchore

**Product Benefits**

Anchore is a leading provider of container security and compliance enforcement solutions designed for open-source users and enterprises.

- **Anchore Deep Image Inspection**: Anchore performs comprehensive inspection and analysis of container image contents to uncover packages, third-party libraries, secrets, credentials, misconfigurations, vulnerabilities. Thus, providing users with a deep insight into the entire contents of their container images.

- **Anchore Policy and Compliance Enforcement Engine**: Anchore provides a flexible and robust policy enforcement engine and language capable of regulating an organization's security, compliance, and best-practice requirements.

With Anchore, Red Hat technology users get:

- **Vulnerability Management**: Anchore conducts an in-depth analysis of the container image contents identifying vulnerabilities. Users can generate vulnerability reports, or create vulnerability specific checks using Anchore Policy Engine.

- **Policy Management**: Anchore’s Policy Engine provides users the ability to enforce security and compliance standards to which all developers must build their container images. Additionally, policies can easily be transferred between teams or altered as security standards, and policy requirements change with the dynamic nature of containers.

- **Flexible Integration**: Anchore ease-of-integrates directly into CI systems, or container registries, incorporating policy enforcement at the build and ship phases of the container lifecycle, allowing developers to identify and remediate any security vulnerabilities before images make their way to production environments.

**Use Cases**

- **Container CI/CD Security**: Anchore has been designed to plug seamlessly into your container based CI/CD pipeline to add security, compliance, and governance to your workflow.

- **Container Security Auditing**: Anchore provides dynamic security and best practice enforcement reporting against your container image registry.

- **Container Compliance**: Anchore helps you achieve and enforce your organizations container compliance standards to ensure non-compliant images do not make it into trusted container registries and production environments.