Runecast

Optimize Your Kubernetes Security Posture Management

with Runecast

High Performer SPRING 2023

Best Support SPRING 2023

Gartner COOL VENDOR 2020

Optimize your KSPM with Runecast

Kubernetes Security Posture Management (KSPM) utilizes automated checks for security and compliance across clusters, assisting organizations with detecting misconfigurations, evaluating and classifying threats and specifying security policies.

A lack of Kubernetes security expertise and knowledge means that most production environments are running containers with vulnerabilities. Without the right solution to check container images in the development stage, DevOps and DevSecOps teams struggle to ensure that containers released into production are secure. The solution is to automate checks against vulnerabilities within Kubernetes workloads from the CI/CD pipeline to the runtime.

Runecast is a Cloud Native Application Protection Platform (CNAPP) enabling CISOs, CIOs, DevOps and DevSecOps teams with proactive KSPM, providing visibility of security vulnerabilities and potential issues in their Kubernetes workloads. Thus, both cluster administrators and operators know where to focus their attention to secure their infrastructures by using a unified single platform.

Full Visibility of Your Kubernetes Infrastructure

Runecast enables simpler, proactive Security Configuration Assessment (SCA) and Cloud Security Posture Management (CSPM) within a single platform. It scans your Kubernetes runtime against best practices, vulnerabilities, and security compliance, revealing configuration drift, generating remediation scripts, and requiring practically no learning curve.

Consistent and Secure Workloads

Runecast scans your Kubernetes infrastructure and keeps track of any changes to your configurations. Using a combination of historical scans and consistency analysis, you can easily troubleshoot configuration drift across your workloads, ensuring consistency across your production deployments.

Runecast provides comprehensive historical reporting for internal and external audits, ensuring your internal posture management can be proven, and therefore, providing peace of mind for admins and managers since your data is secured against latest vulnerability and security compliance including checks for CISA Kubernetes Hardening Guide.

Runecast provides support for:

- Bare Metal Kubernetes
- VMware Tanzu
- Amazon EKS
- Google GKE
- Microsoft AKS
- OpenShift
- HPE Ezmeral Container Platform

Shift Security Left with Runecast

For years, security testing was implemented at the end of the development cycle which implied security risks and delays when releasing software. To shift security left means to execute security testing and best practices along the entire development cycle detecting and remediating potential security issues and vulnerabilities before moving to production. This approach is easier, more cost-effective and boosts DevOps and DevSecOps teams performance.

To perform checks for vulnerabilities in all container images deployed across your environments, Runecast provides image scanning as a part of the DevOps deployment process (CI/CD pipeline) and for staging, prod and pre-prod deployments.

The ability to scan container images before they are released into test or production environments enables the shift left approach whereby you can ensure your containers are secured against the Runecast admissions policies; evaluation is also available through the K8s admission controller webhook API.

By utilizing the API endpoint, you can trigger image scanning and get the results via our public API. The response from the API endpoint will either allow or deny deployments based on the selected policy, ensuring all container images meet your required level of security before they are released into test or production. This way, when containers are deployed, they are fully secure.

Key benefits of integrating Runecast into your CI/CD pipeline

- Cluster level:
  - Automatically scan the Kubernetes runtime for security, availability, performance and manageability best practices
  - Monitor and detect changes in the runtime configurations
  - Scan for appropriate best practices based on whether its bare metal, EKS or other Kubernetes flavor where applicable

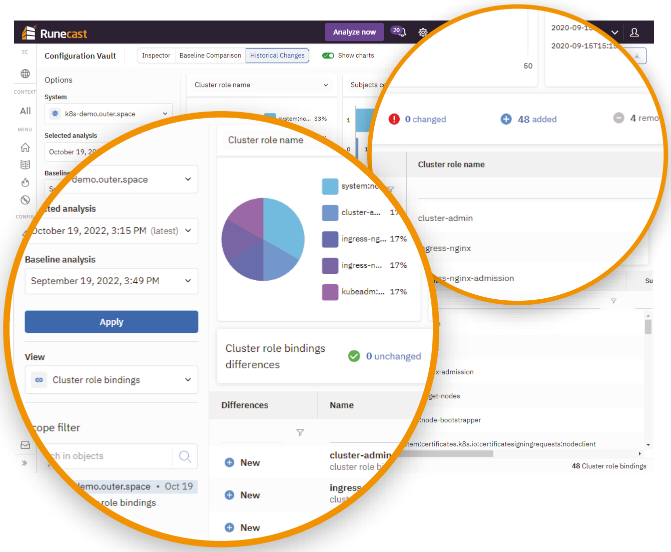
- Container image scanning:
  - One or multiple images can be scanned in a single API call.
  - Get all vulnerability info straight into a convenient form, no individual command line scanning required
  - See all versions, CVEs and fix versions
  - Integrate with K8s admission controller to make image scanning part of your deployment process
  - Container security allows image scanning through the CI/CD process ensuring deployment of secure workloads.

Support for Configuration Drift Management in Production Environments

Configuration drift can be caused by hardware and software upgrades, or through simple administration errors. Without a properly documented environment, configuration drift becomes unmanageable.

Runecast provides current configuration visualization for your Kubernetes deployments and supports you creating a baseline to ensure consistent OS image, Kernel versions, etc.

Once your environment has been configured to your required specifications, historical changes can be tracked over time, illustrating where you have configuration drift in your environment and therefore what you need to change to bring you back to your baseline requirements.



Runecast makes your Kubernetes platform stable and secure, helping to accomplish industry standard best practices, vulnerability and security compliance, configuration drift management tailored to your environments.

Highlights

- Easy deployment – agentless, up and running in minutes
- Monitor, secure, and troubleshoot your hybrid cloud for proactive CSPM and KSPM
- Gain real-time security compliance insights
- Mitigate risk of data breaches
- Maintain audit-readiness for security compliance
- Proactively discover previously unknown issues

Runecast helps DevOps and DevSecOps teams to visualize and implement best practices, vulnerability assessment and security compliance checks throughout the entire workload lifecycle from the build pipeline through to runtime. Complemented by the Configuration Vault to manage configuration drift, Runecast delivers unrivaled Container Security wherever workloads reside.

Runecast is a CNAPP solution combining deep insights into VMware, AWS, Azure, GCP, Kubernetes and OS infrastructures with Vulnerability and Compliance Management across on-prem, hybrid and multi cloud, providing a true single platform.