



RUNECAST FOR KUBERNETES
An Ideal Partnership

Runecast for Kubernetes, an ideal partnership

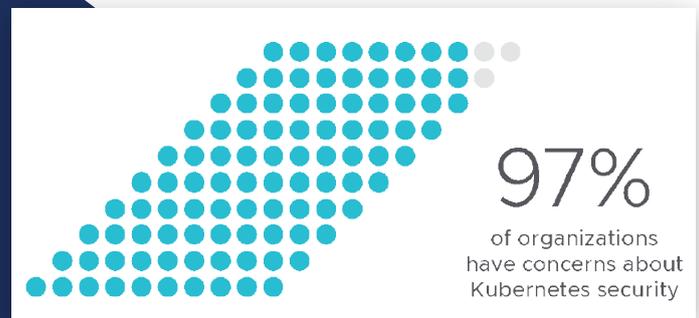
Runecast is an IT Security and Operations platform designed to enable CISOs, CIOs, Security and Operations teams with proactive Kubernetes Security Posture Management (KSPM), making sure they know where to focus their attention first.

Running securely on your own infrastructure – whether on-prem, hybrid or public cloud – Runecast automates security and compliance checks for your Kubernetes containers, with insights into what is happening both in the cloud and on-premises. No sensitive company, employee, or customer data ever needs to leave your control.

Are you one of the 97% who have concerns about K8s security?

Runecast provides proactive security, compliance, vulnerability assessment, configuration drift management, remediation and reporting for your Kubernetes deployments.

Kubernetes is no longer an up and coming technology, it's a well established container orchestration platform running mission critical workloads and needs to be treated seriously when it comes to security and compliance.



Source: State of Kubernetes 2022, VMware

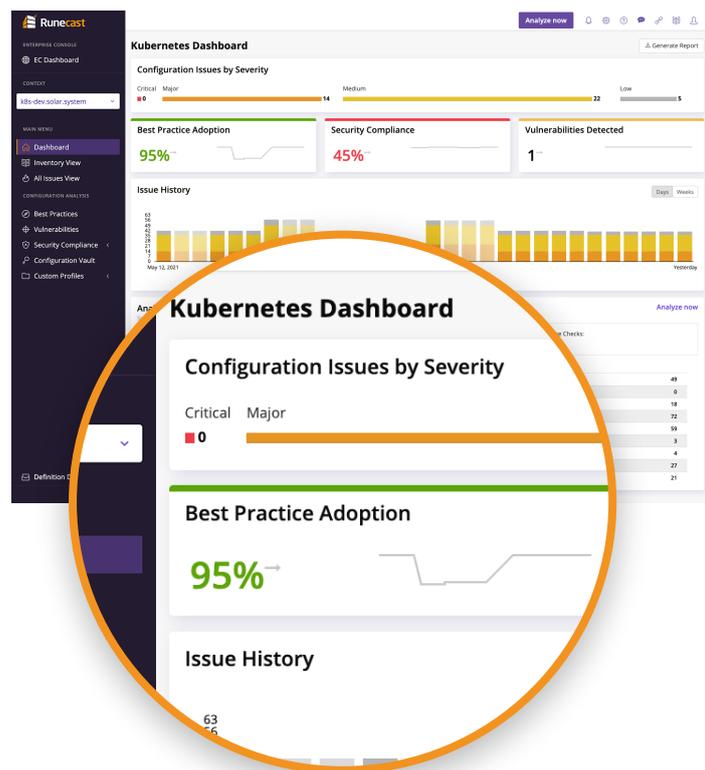
Simplify security, speed up operations

There's been an increase in organizations deploying Kubernetes in hybrid and multi-cloud environments, but there are still a large number of organizations that deploy to private cloud or infrastructure. Runecast caters to all, because we secure your K8s workloads and the underlying infrastructure it runs on. Using Runecast you can scan other areas of your infrastructure with 10+ security standards out of the box.

Runecast automates Kubernetes configuration analysis by auditing common cluster operational and security best practices for KSPM, including CIS Benchmarks for Kubernetes security. It also provides vulnerability mapping.

Runecast supports:

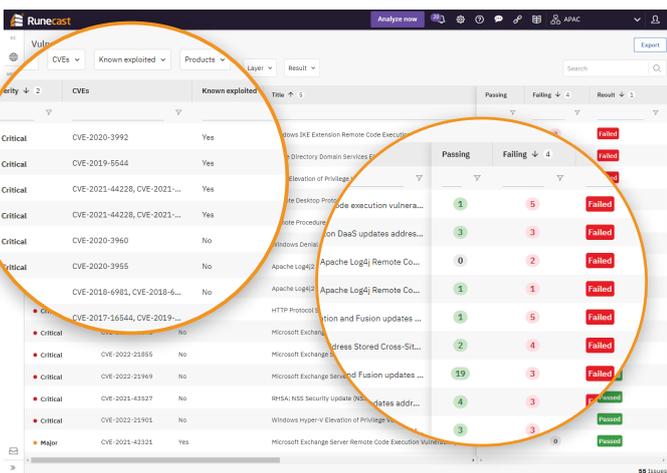
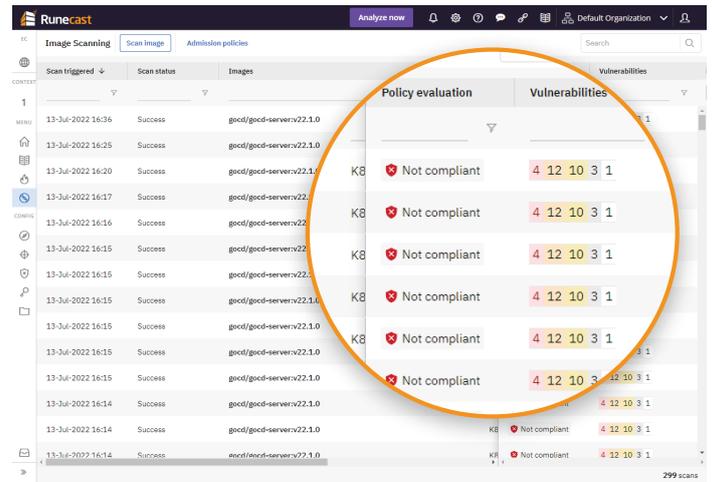
- Bare Metal Kubernetes
- Amazon EKS
- Google GKE
- HPE Ezmeral Container Platform
- OpenShift
- Microsoft AKS
- VMware Tanzu
- And more...



Shift Left with Runecast

To ensure no images are deployed with vulnerabilities, you can configure the Kubernetes admission controller to use bearer token authentication for the webhook. The response from the API endpoint will either allow or deny deployments based on the selected admission policy.

Through admission policies, development teams can control container image releases, ensuring images are free of vulnerabilities before they are released to the test environment. This ensures that when containers are deployed into production, they are fully secure and need only to be checked for the latest vulnerabilities found in the wild, which are constantly updated in the Runecast knowledge definitions.



We aim to make things easy

Ensure consistency and end configuration drift with Configuration Vault. Reduce your manual remediation effort and generate custom remediation scripts from within Runecast. Maintain historical data for audit evidence and historical trending.

You can deploy Runecast directly to Kubernetes in a matter of minutes (using our Helm chart) and have immediate automated Kubernetes configuration analysis at the node-level, cluster-level, and workload level. You will see a list of critical issues according to Kubernetes Best Practices or Security and Compliance Standards. For hybrid environments Runecast has you covered. You can see the

same level of detail for AWS, Azure, VMware, Windows and Linux deployments all in one platform.

Runecast makes focusing on the most critical vulnerabilities easy, by not only showing you the severity of any given vulnerability, but also whether this vulnerability is known to have been exploited in the wild according to CISA's KEV catalog.

Runecast is here to make your Kubernetes platform as stable and secure as possible, with industry standard best practices, configuration drift management and continuous compliance tailored to your environments.

Highlights

- Easy deployment – up and running in minutes
- Monitor, secure and troubleshoot your hybrid cloud for proactive CSPM and KSPM
- Gain real-time ITOM and security compliance insights
- Mitigate risk of data breaches
- Maintain audit-readiness for security compliance
- Proactively discover previously unknown issues
- Have performance analysis, vulnerability assessment, and patch management – all in one place