RUNECAST FOR KUBERNETES

AN IDEAL PARTNERSHIP

www.runecast.com

Runecast for Kubernetes, an ideal partnership

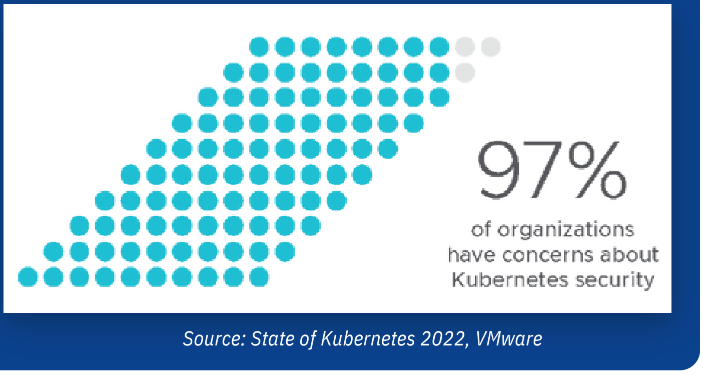
Runecast is an IT Security and Operations platform designed to enable CISOs, CIOs, Security and Operations teams with proactive Kubernetes Security Posture Management (KSPM), making sure they know where to focus their attention first.

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.

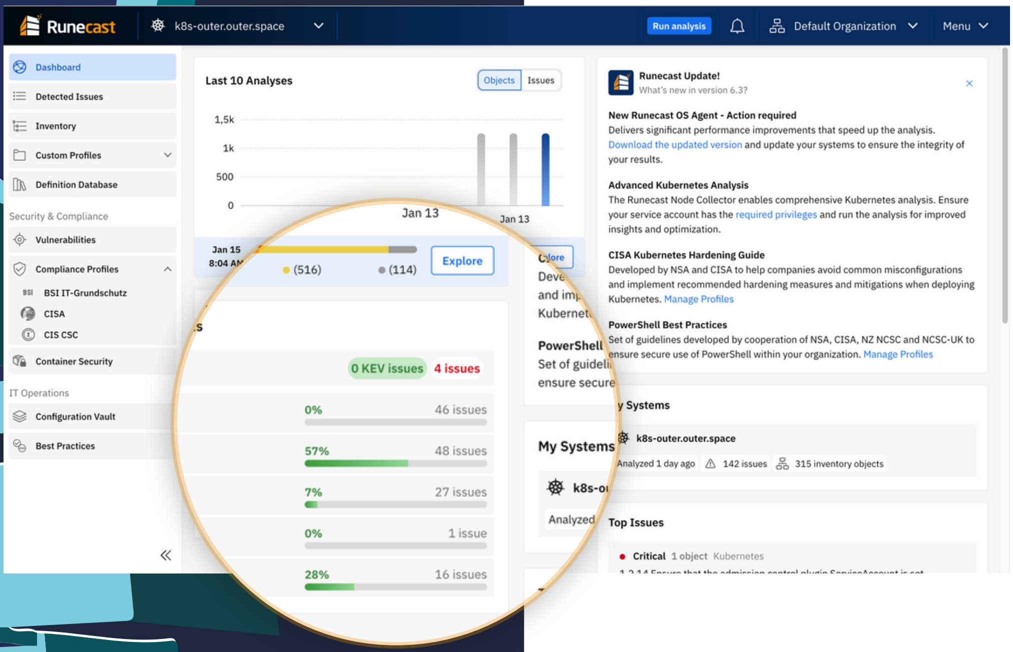


Source: State of Kubernetes 2022, VMware

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 and CISA Kubernetes Hardening Guide. It also provides vulnerability mapping.



Runecast Update!
What's new in version 6.3?

New Runecast OS Agent - Action required
Delivers significant performance improvements that speed up the analysis. Download the updated version and update your systems to ensure the integrity of your results.

Advanced Kubernetes Analysis
The Runecast Node Collector enables comprehensive Kubernetes analysis. Ensure your service account has the required privileges and run the analysis for improved insights and optimization.

CISA Kubernetes Hardening Guide
Developed by NSA and CISA to help companies avoid common misconfigurations and implement recommended hardening measures and mitigations when deploying Kubernetes. Manage Profiles

PowerShell Best Practices
Set of guidelines developed by cooperation of NSA, CISA, NZ NCSC and NCSC-UK to ensure secure use of PowerShell within your organization. Manage Profiles

My Systems
k8s-outer.outer.space
Analyzed 1 day ago | 142 issues | 315 inventory objects

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.

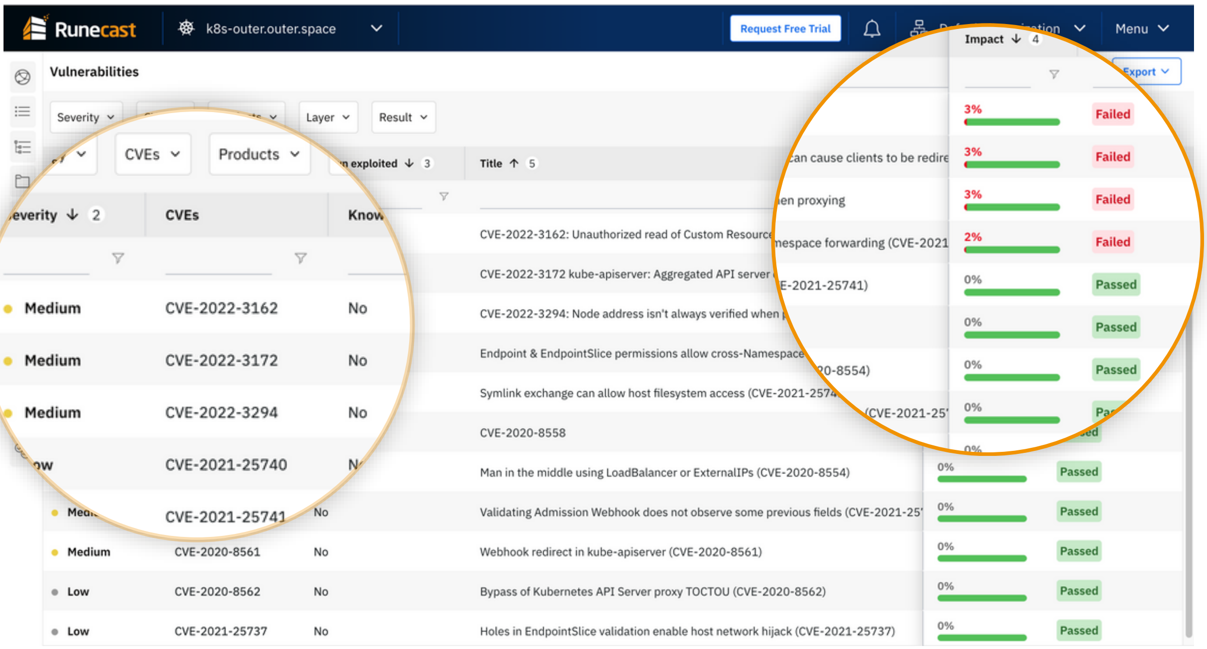
Through admission policies, development teams can control container image releases, ensuring images are free of vulnerabilities before they are released to the test environment. This ensures that when containers are deployed into production, they are fully secure and need only to be checked for the latest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



everity ↓ 2	CVEs	Know
Medium	CVE-2022-3162	No
Medium	CVE-2022-3172	No
Medium	CVE-2022-3294	No
ow	CVE-2021-25740	N
Med	CVE-2021-25741	No
Medium	CVE-2020-8561	No
Low	CVE-2020-8562	No
Low	CVE-2021-25737	No

Title ↑ 5	Impact ↓ 4	
CVE-2022-3162: Unauthorized read of Custom Resourc	3%	Failed
CVE-2022-3172 kube-apiserver: Aggregated API server can cause clients to be redire	3%	Failed
CVE-2022-3294: Node address isn't always verified when proxying	3%	Failed
Endpoint & EndpointSlice permissions allow cross-Namespace forwarding (CVE-2021	2%	Failed
Symlink exchange can allow host filesystem access (CVE-2021-2574	0%	Passed
CVE-2020-8558	0%	Passed
Man in the middle using LoadBalancer or ExternalIPs (CVE-2020-8554)	0%	Passed
Validating Admission Webhook does not observe some previous fields (CVE-2021-25'	0%	Passed
Webhook redirect in kube-apiserver (CVE-2020-8561)	0%	Passed
Bypass of Kubernetes API Server proxy TOCTOU (CVE-2020-8562)	0%	Passed
Holes in EndpointSlice validation enable host network hijack (CVE-2021-25737)	0%	Passed

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