Runecast

FROST & SULLIVAN
BEST PRACTICES
AWARDS

RUNECAST PLATFORM
Datasheet

www.runecast.com

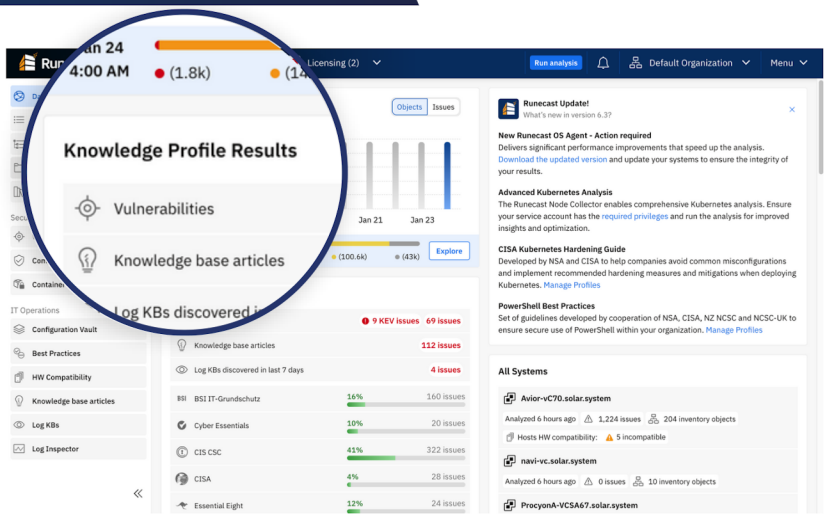
FROST & SULLIVAN BEST PRACTICES AWARDS

computing Cloud Excellence Awards 2020 Winner Cloud Security Product of the Year - SMEs

Gartner COOL VENDOR 2020

The Runecast platform helps you to proactively avoid outages, mitigate risks, and ensure compliance with your necessary security standards. Its patented rules engine converts industry sources of information into machine-readable data. This data is processed on the Runecast platform, which then scans your environments for hidden problems, deviations from best practices, and noncompliance with the security frameworks that you select.

The appliance can be deployed as an industry-standard OVA, to Kubernetes, via Azure and AWS marketplaces or as SaaS, and you can be up and running with actionable insights in minutes.



SUPPORTED TECHNOLOGIES:

- **AWS** – AWS Config, AWS Health, AWS Inspector, Cloudfront, Cloudtrail, Cloudwatch, EC2, ECS, EFS, EKS, IAM, Kinesis, Lambda, RDS, Redshift, S3, VPC
- **Azure** – AAKS, Azure AD, Azure App Services, Disks, Key Vault, MySQL Server, Network Security Group, Network Watcher, PostgreSQL Server, SQL Server, Storage Accounts, Subscription, Virtual Machines
- **GCP** – Cloud Functions, Storage Buckets, DNS Policies, Firewall Rules, VPC Networks, SQL Instances, Compute Instances, Service Accounts, Metrics & Alerts, IAM Policies.
- **Kubernetes** – Amazon EKS, Microsoft AKS, Google GKE, VMware Tanzu, HPE Ezmeral Container Platform
- **VMware** – vSphere, Horizon, vSAN, NSX-T, NSX-V, VMware Cloud Director, SAP HANA (on vSphere), PureStorage (on vSphere), vSphere on Nutanix
- **OS analysis** – Vulnerabilities for any Windows and Linux versions, including BSI-IT Grundschutz, CIS CSC, DISA STIG, DORA, ISO 27001, NIST & TISAX compliance for Windows and Linux.
- **Plugins** - available for integration with the vSphere Client, vRealize Orchestrator, Jira, and ServiceNow

VMware System Requirements

Network communications between Runecast all take place over a secure HTTPS connection (TCP 443). ESXi communication to Runecast for Syslog communication runs over the standard Syslog port (UDP 514).

Full port requirements are detailed in the Runecast User Guide, which can be found at docs.runecast.com

Size	CPU	RAM (GB)	Disk (GB)	Network (Mbps)
Small (up to 50 hosts)	2	12	120	100 (1GB rec.)
Medium (up to 150 hosts)	4	16	120	100 (1GB rec.)
Large (up to 1200 hosts)	8	32	120	100 (1GB rec.)

Full system requirements are documented in the Runecast User Guide | docs.runecast.com

Required Privileges

The majority of Runecast's reporting capabilities can be achieved using an account with Read-Only permissions, however, within vCenter, in order to utilize some features, extra privileges may be required. These are detailed in the Runecast User Guide. A PowerCLI script is provided on our Github page to automate the creation of this role if required.

runecast.com | roi@runecast.com

Key Features

ISSUE PREVENTION

Continuously checks your environment for configuration problems against known issues, best practices, vulnerabilities & security compliance standards – for AWS, Azure, GCP, Kubernetes, OS and VMware infrastructures.

ORGANIZATIONS

Separate team views by departments and regions, enabling global and team management and reporting through one unified platform.

KNOWN EXPLOITED VULNERABILITIES (KEVs)

Focus on vulnerabilities that are known to have been actively exploited in the wild, as per the CISA KEV catalog.

RUNS FULLY ON-PREM OR IN THE CLOUD

All analysis is run either in the cloud or locally on the Runecast Analyzer appliance. No data is sent outside your data center, ensuring data protection. It can also operate entirely disconnected from the internet, with updates applied out-of-band. If you are connected to the internet, you can pull updates automati cally from our online repository.

LOG ANALYTICS

Monitors ESXi host & VM log files for problems, showing you how to resolve issues quickly.

UPGRADE SIMULATIONS

Validates your hardware, drivers, and firmware against current and upstream releases of ESXi for faster upgrade planning.

SECURITY COMPLIANCE

Proactively audits your compliance against BSIC5, BSI IT-Grundschutz, CIS CSC, CISA, Cyber Essentials, DISA STIG, DORA, Essential 8, GDPR, HIPAA, ISO 27001, KVKK, NIST, PCI-DSS, TISAX, VMware Security Configuration Guide, Kubernetes Hardening Guide, PowerShell best practices, Common Vulnerabilities and Exposures (CVEs) and customized checks for your internal audit needs. Runecast Analyzer is CIS Certified for both vSphere and AWS.

CONFIGURATION VAULT

Reports on configurations for AWS, Azure, GCP, Kubernetes, OS and VMware. Create baselines to ensure hosts and OS are consistent, and then track configuration drift over time for a compliant environment with full accountability for actions taken by administrators.

CAPACITY MANAGEMENT

Reports resource use for every VMware cluster's CPU/memory including overcommitment ratios and predictive trends providing insights into likely future utilization changes. In-depth data on each cluster enables further assessment of capacity metrics and by simulating potential host failures, you can strategize upcoming workload placements to determine the most suitable cluster for your upcoming projects.

ON-PREMISES AND SaaS OPTIONS

All analysis can be run locally on the Runecast platform appliance, meaning no data is sent outside of your control. It can operate entirely disconnected from the internet, with updates applied out-of-band. If you can connect to the internet then you can pull updates automatically from our online repository.

Alternatively Runecast SaaS provides a solution which does not need to be hosted in your environment, while still providing the same security measures as an on-premises deployment, saving your IT resources and automatically providing the latest upgrades and updates to knowledge definitions. Runecast SaaS also provides agentless monitoring for Linux EC2 instances, removing the burden of deploying and maintaining agents in the environment.

AGENTLESS SCANNING

Runecast provides monitoring of your AWS, Azure, Google Cloud, Kubernetes, OS and VMware, all completely agentless, ensuring swift deployment and automatic asset detection from the initial scan of the environment.

REMEDIATION SCRIPTS

A growing number of findings in Runecast offer remediation actions – allowing you to download the customized script to perform the reconfiguration. Some rules offer more than one remediation option, for example PowerCLI and Ansible.

runecast.com | roi@runecast.com