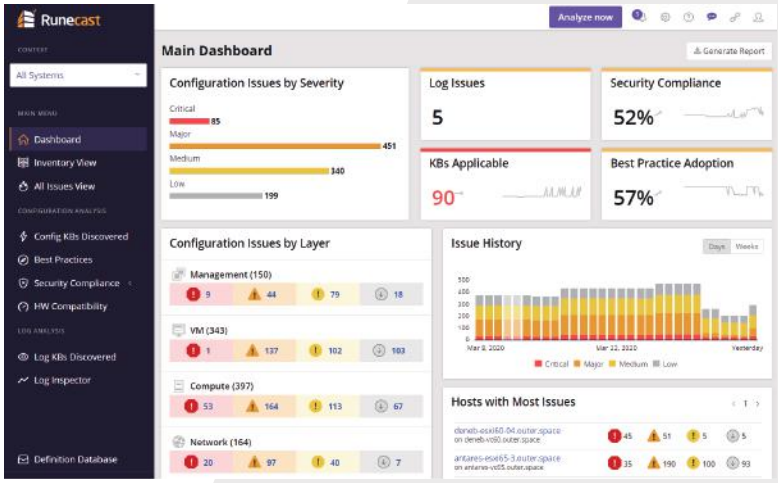
Runecast | RUNECAST ANALYZER **DATASHEET**

Gartner COOL VENDOR 2020

Runecast Analyzer helps you to avoid outages, mitigate risks, and ensure compliance with your necessary security standards. You get a patented AI engine that converts industry sources of information into machine-readable data. This data is processed on the Runecast Analyzer appliance, which then scans your VMware and AWS environments for hidden problems, deviations from best practices, and non-compliance with the security frameworks that you select.

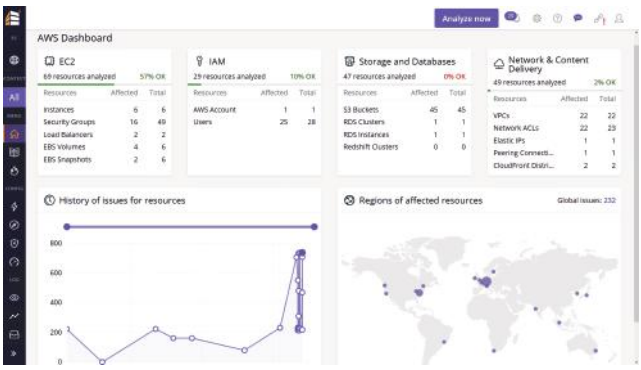
The appliance is provided as an industry-standard OVA, and you can be up and running with actionable insights in minutes.



SUPPORTED PRODUCTS:

- **AWS** – AWS Config, AWS Health, AWS Inspector, Cloudfront, Cloudtrail,Cloudwatch, EC2, ECS, EFS, EKS, IAM, Kinesis, Lambda, RDS, Redshift, S3, VPC
- **Azure** – AKS, App Services, Azure AD, Disk, Key Vault, MySQL Server, Network Security Group, Network Watcher, Postgres Server, SQL Server, Storage Account, Subscription, Virtual Machine
- **Kubernetes**
- **VMware** – NSX-T, NSX-V, VMware Cloud Director, vSAN, vSphere
- Plugins available for integration with the vSphere Client, vRealize Orchestrator and ServiceNow

Key Features



ISSUE PREVENTION

continuously check your environment for configuration problems against known issues, best practices & security compliance standards. This provides insights that help you to stabilize and secure both your VMware and also native AWS infrastructure.

LOG ANALYTICS

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

RUNS FULLY ON-PREMISES

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

SECURITY COMPLIANCE

Continuously evaluate your compliance against BSI IT-Grundschutz, CIS CSC, Cyber Essentials, DISA STIG, Essential 8, GDPR, HIPAA, ISO 27001, NIST, PCI-DSS, VMware Security Configuration Guide and also customized checks for your internal audit needs. Runecast Analyzer is CISCertified for both vSphere and AWS.

UPGRADE SIMULATIONS

validate your hardware, drivers, and firmware against current and upstream releases of ESXi.

System Requirements

Full system requirements are documented in the Runecast User Guide, however, Runecast Analyzer is deployed as a virtual appliance to your VMware SDDC, and resource requirements are as follows.

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

Network communications between Runecast Analyzer, vCenter Server, ESXi, NSX Manager, Horizon Connection Servers, and the AWS APIs all take place over a secure HTTPS connection (TCP 443). ESXi communication to Runecast Analyzer for Syslog communication runs over the standard Syslog port (UDP 514).

When Runecast Analyser is allowed to perform online updates these are also pulled over HTTPS from https://updates.runecast.com

Full port requirements are detailed in the Runecast User Guide, which can be found at https://runecast.com/RunecastUserGuide.pdf

Required Privileges

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

Want to learn more?

For further information, to download a demo or to set up a call to further discuss Runecast Analyzer with our team of experts please visit www.runecast.com or email us at innovate@runecast.com. We look forward to speaking with you!