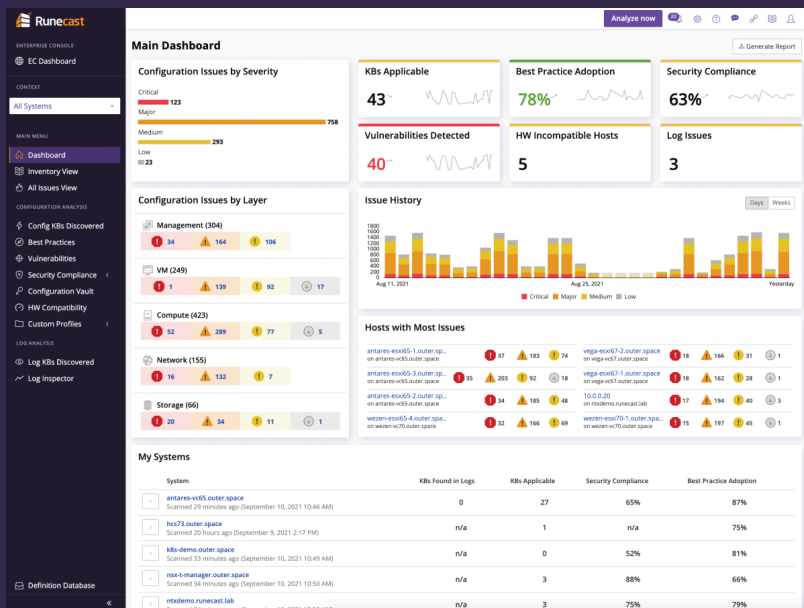


Optimize and Secure your Hybrid Cloud

Proactively detect and mitigate configuration issues and security risks with a patented solution for real-time, actionable insights.



INCLUDES ENTERPRISE CONSOLE

ENDORSED BY OUR CUSTOMERS

"It took away a lot of the pressure from firefighting mode. It shows you how you should have done things in the first place, so it's also training people and giving them the confidence to do something they may not have known how to do before. With Runecast, we can now look at one screen and have the visibility and transparency to know what we are working on and why."

Henderson Alleyne

Head of IT & Telecoms, DHU Health Care



"A vital tool for maintaining uptime for your virtual environment"

Cloud Services Manager

"Runecast gives you the information you need to prevent potential and dangerous issues saving lot of time and keeping the environment healthy"

System Engineer



Stanimir Markov

Runecast CEO, Co-Founder,
VCDX #74

"We designed this platform so sysadmins never have to waste valuable time identifying, diagnosing or searching for error codes ever again"

FULL VISIBILITY OF ISSUES IN YOUR HYBRID CLOUD AND OPERATING SYSTEMS

With one platform, Runecast enables simpler, proactive IT Operations Management (ITOM), including Security Configuration Assessment (SCA) and Cloud Security Posture Management (CSPM). It continuously scans your configurations and logs against many 1000s of known issues, more than 10 common security standards, VMware HCL, vendor best practices and vulnerabilities (including VMASs/CVEs). It reveals configuration drift, generates remediation scripts and requires no learning curve. Take proactive control over AWS, Azure, Kubernetes, Linux Red Hat, Microsoft Operating Systems, and VMware.

SECURITY COMPLIANCE AUDIT READINESS

Automated security standards audits map and report your compliance with the following:

BSI IT-Grundschutz, CIS Benchmarks, Cyber Essentials, DISA STIG, Essential 8, GDPR, HIPAA, ISO 27001, NIST, PCI-DSS, VMware Security Configuration Guide, and Custom profiles (for internal standards), with more checks regularly added.

REGARDLESS WHERE YOU RUN IT, YOU MAINTAIN CONTROL OF YOUR DATA

Running securely within the infrastructure, Runecast helps to automate security compliance checks, performance analysis, vulnerability assessment and patch management with insights into what is happening in both hybrid-cloud and on-premises. No sensitive company, employee or customer data need ever leave your control.

BUILT BY ADMINS - FOR ADMINS

Working with infrastructure provides insights into the required information to succeed. Runecast Analyzer was created by sysadmins to provide the insights required to proactively identify this information and gain an understanding of the issues. Remediation information is provided so that admins can be proactive in their work, understand the issues and stay ahead of the game.

Forward-thinking organizations that rely on Runecast Analyzer



By the numbers

90%

Savings in upgrade
compatibility tracing
effort

- FLEXdata

90%

Time savings over
previously troubleshooting
issues reactively

- Near East Bank

75%

Reduction of
outages and issues

- NCC Media

100%

Delivery of uptime to
their cloud customers

- ONI PLC

Definition Database

Severity ▾

Source ▾

Applies to ▾

Affects ▾

Products (3) ▾

Filters Applied: VPC x EC2 x IAM x Clear All

	Severity ▾	Source	Applies to	Affects	Products	Title
⊞	Critical	BP	Compute	Security	EC2	Ensure no security groups allow incoming connections to ALL ports and protocols
⊞	Major	BP	Management	Security	IAM	Password Policy must require at least one uppercase character
⊞	Major	BP	Compute	Recoverability	EC2	Enable termination protection for EC2 instances
⊞	Major	BP	Management	Security	IAM	Password Policy must require at least one lowercase character
⊞	Major	BP	Management	Security	IAM	Password Policy must require at least one number
⊞	Major	BP	Management	Security	IAM	Password Policy must require at least one symbol
⊞	Major	BP	Management	Security	IAM	Password policy must prevent reuse of previously used passwords
⊞	Major	BP	Management	Security	IAM	Password policy must require rotation every 90 days
⊞	Major	BP	Management	Security	IAM	Password Policy must require a minimum length of 14
⊞	Major	BP	Management	Security	IAM	Enable MFA for console login
⊞	Major	BP	Compute	Security	EC2	Ensure no security groups allow incoming connections to SSH (TCP:22)
⊞	Major	BP	Compute	Security	EC2	Ensure no security groups allow incoming connections to RDP (TCP:3389)
⊞	Medium	BP	Management	Security	VPC	Ensure VPC flow logging is enabled in all VPCs
⊞	Medium	BP	Network	Security	VPC	Ensure the default security group of every VPC restricts all traffic
⊞	Medium	BP	Management	Security	IAM	Credentials with password enabled, unused for 90 days should be disabled
⊞	Medium	BP	Management	Manageability	IAM	Use Groups to Assign Permissions to IAM Users
⊞	Medium	BP	Compute	Recoverability	EC2	Consider EBS-backed instances as root-device storage

- Gain real-time IT Operations Management (ITOM) and security compliance insights.
- Monitor, secure and troubleshoot your hybrid and multi-cloud for proactive Cloud Security Posture Management (CSPM).
- Remove downtime through actionable insights for a proactive sysadmin team.
- Proactively discover previously unknown issues and mitigate risk of data breaches.
- Maintain audit-readiness by automating vulnerability management and security compliance audits for over 10 global standards including vendor guidelines.
- Performance analysis, vulnerability assessment and patch management – all in one place.
- See the future with upgrade simulations and the past with detailed history.
- Provide even the most junior admin information which allows responding to incidents like a seasoned pro.
- Detect drift in your infrastructure and close the configuration gap before a major failure can occur.
- Customizable reporting capabilities for complete visibility.

RUNECAST ADDS VALUE TO HYBRID CLOUD & OS

Runecast Analyzer provides IT Security and Operations teams, IT architects, and CIOs/CISOs unparalleled operational transparency, risk mitigation, and cost savings for hybrid and multi cloud investments. Running securely in your infrastructure, it provides insights into what is happening, both in the cloud and on-site. Automated reporting of support tickets can also be achieved with the ServiceNow plugin.

OUR CLIENTS REPORT IMMEDIATE ROI

Since Runecast provides IT Security and Operations teams a proactive approach to stabilising and securing their environment, our clients often report ROI from the very first scan, plus major ongoing time savings that enable more focus on growth drivers.

SUPPORTED SERVICES

- Amazon Web Services (AWS) – AWS Config, AWS Health, AWS Inspector, CloudFront, CloudTrail, CloudWatch, EC2, ECS, EFS, EKS, IAM, Kinesis, Lambda, RDS, Redshift, S3, VPC
- Microsoft 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
- Kubernetes – Amazon EKS, Microsoft AKS, Google GKE, VMware Tanzu, HPE Ezmeral Container Platform
- Operating Systems – Linux Red Hat, Microsoft Windows
- VMware – vSphere, vSAN, NSX-V, NSX-T, Horizon and VMware Cloud Director, SAP HANA (on vSphere), PureStorage (on vSphere), vSphere on Nutanix

