

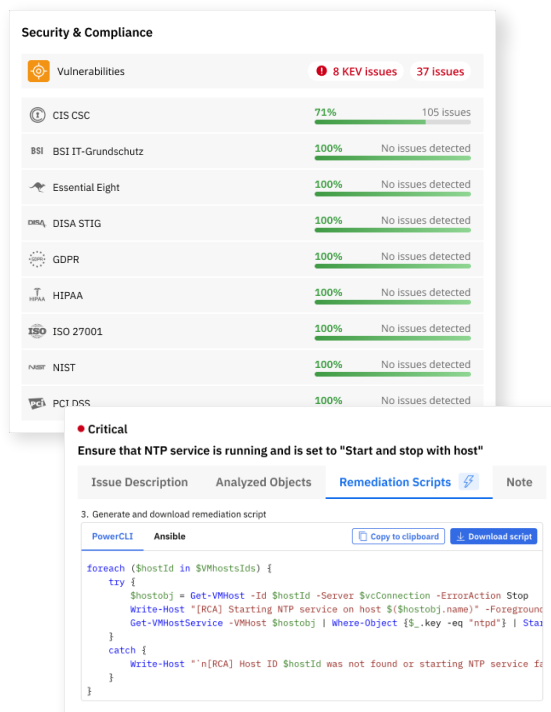
## Security across the Hybrid Cloud

Security and compliance have to be paramount in any modern environment. With potential attacks and intrusions originating from both external and internal threat actors, the ability to quickly and automatically identify existing or new vulnerabilities and changes in configurations is every System Administrators, Security, SecOps and DevSecOps team's highest priority.

Compliance and Vulnerability management should not only rely on manual checks. A platform that continuously and automatically analyzes the environment ensures the highest possible effectiveness.

Compliance, Security and Infrastructure teams are on the front line and require a solution which enables them to visualize security flaws within the environment, to facilitate quick remediation and to ensure the infrastructure is secure.

Runecast provides immediate insights by analyzing the environment against security and compliance standards, highlights misconfigurations and tracks configuration drift, allowing organizations to strengthen their security posture, and ensures appropriate controls are in place from on-prem to the cloud.



**Security & Compliance**

Vulnerabilities 8 KEV issues 37 issues

Standard	Compliance	Issues
CIS CSC	71%	105 issues
BSI IT-Grundschutz	100%	No issues detected
Essential Eight	100%	No issues detected
DISA STIG	100%	No issues detected
GDPR	100%	No issues detected
HIPAA	100%	No issues detected
ISO 27001	100%	No issues detected
NIST	100%	No issues detected
PCI DSS	100%	No issues detected

**Critical**  
Ensure that NTP service is running and is set to "Start and stop with host"

Issue Description	Analyzed Objects	Remediation Scripts	Note
3. Generate and download remediation script			
PowerCLI	Ansible	<a href="#">Copy to clipboard</a>	<a href="#">Download script</a>
<pre> foreach (\$HostId in \$VMHostsIds) {   try {     \$Hostobj = Get-VMHost -Id \$HostId -Server SvcConnection -ErrorAction Stop     Write-Host "[RCA] Starting NTP service on host \$(\$Hostobj.name)" -ForegroundColor Green     Get-VMHostService -VMHost \$Hostobj   Where-Object {\$_.key -eq "ntpd"}   Start-Service   } catch {     Write-Host "`n[RCA] Host ID \$HostId was not found or starting NTP service failed" -ForegroundColor Red   } } </pre>			

### CONTINUOUS COMPLIANCE: NOT A MYTH

Keeping up with ever-changing regulatory, regional and internal requirements can be a daunting, frustrating, and costly task, whether that is in the form of a highly skilled practitioner whose time is spent on repetitive manual tasks, or through post-audit fines. Reducing the pre-audit fire fighting, while improving overall security and compliance across the environment can be achieved.

Organizations need a single platform that allows for automated security, vulnerability management and compliance checks, whether on-premises or in the cloud. Runecast removes silos between Infrastructure, Security and Compliance teams and streamlines reporting, analyzing, remediation and adoption across the entire environment.



#### RUNECAST FOR EVERYTHING

From AWS, Azure and Google Cloud through Kubernetes, Windows and Linux to VMware environments. Runecast helps your teams follow continuous security and compliance practices all from one platform, deployable on-prem, in public or hybrid cloud and even fully air-gapped environments.

#### YOUR ENVIRONMENT – YOUR RULES

Not only is it important to have easy to access and enforce Security and Compliance standards, it is equally important for Organizations to have the ability to create their own. Runecast audits BSI, CIS, Cyber Essentials, DISA STIG, Essential 8, GDPR, HIPAA, ISO 27001, NIST, PCI DSS, and more. Using Runecast, practitioners can create and augment profiles that can be built from thousands of checks to your requirements allowing for broader coverage and greater adoption.

Forward-thinking organizations that rely on Runecast



SCANIA

Swedbank



avast



## Bringing security to your Infrastructure

Runecast provides security, compliance and vulnerability assessment across your on-prem, public and hybrid cloud platforms. Some of the supported technologies are:

### 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
- ✔ **Google Cloud** – 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
- ✔ **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

### WITH RUNECAST YOUR TEAMS WILL:

- ✔ **Gain** insights into performance analysis, vulnerability assessment and patch management – all in one place.
- ✔ **Monitor, secure** and **troubleshoot** your hybrid and multi cloud and containers for proactive Cloud and Kubernetes Security Posture Management (CSPM/KSPM).
- ✔ **Remove** the risk of downtime through actionable insights.
- ✔ **Discover** previously unknown issues and mitigate the risk of data breaches.
- ✔ **Maintain** audit-readiness by automating vulnerability management and security and compliance audits against global standards, including vendor guidelines.
- ✔ **Provide** even the most junior member of the team key information that allows responding to incidents like a seasoned pro.
- ✔ **Detect** drift in your infrastructure and close the configuration gap before a major failure can occur.
- ✔ **Utilize** customizable reporting capabilities for complete visibility.

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



**Stanimir Markov**  
Runecast CEO, Co-Founder