Take control of your VMware SDDC & AWS Cloud. Avoid outages, mitigate risks, be security compliant.

Mitigate configuration issues and security risks with a single platform for real-time, automated VMware and AWS insights: Runecast Analyzer.

**ISSUE PREVENTION**
Continuously checks your environment configuration and logs against known issues, security standards, Hardware Compatibility Lists, Best Practices (e.g. VMware, AWS, and SAP HANA) to provide you insights to stabilize and secure your VMware + AWS infrastructure. Provides upgrade simulations and keeps historical data for all scans.

**SECURITY COMPLIANCE**
Evaluates your VMware and AWS security compliance for PCI-DSS, DISA-STIG, HIPAA, BSI, CIS and NIST. Provides mapping of technical checks vs security controls and requirements, detailed historical data and option for automated remediation.

**FULLY ON-PREM SECURE**
Operates fully on-prem to analyze your hybrid-cloud environment, so that your data remains safely on-site.

"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, VCDX #74

"We found out that there were a few ongoing issues in the environment that eventually brought our systems down. The troubleshooting took too long because we had to call VMware Support Center in many cases. Runecast Analyzer changed all that."

-Henderson Alleyne
Director of Network Operations, NCC Media

"Best 3rd party software for your vSphere environments"
IT Services Engineer

"A vital tool for maintaining uptime for your virtual environment"
Cloud Services Manager

**ENDORSED BY OUR CUSTOMERS**

©2020 Runecast Solutions Ltd. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws.
**HOW IT WORKS**

- Connect all your vCenters and AWS API to a single, lightweight Runecast Analyzer virtual appliance and take control from a single dashboard.

- Runecast Analyzer engine has fully offline capabilities and can even be upgraded in offline mode.

- Its patent-pending rules engine uses Artificial Intelligence (AI) and Natural Language Processing (NLP) to automatically discover misconfigurations in your environment that can cause failed security audits or trigger outages.

**RUNECAST ADDS VALUE & STABILITY TO VMWARE & AWS HYBRID CLOUD**

**IMMEDIATE VALUE**

As Runecast Analyzer helps teams to stabilize availability and ensure security compliance, its ROI contributes also to greater ROI for both existing and future VMware and AWS investments.

**FULL VISIBILITY OVER YOUR HYBRID CLOUD**

Runecast helps teams with a simpler transition to AWS, enabling admins to fully understand their hybrid environments. Running securely on-prem, it provides insights into what is happening both in the cloud and on-site.

**SUPPORTED SERVICES**

- VMware vSphere, vSAN, NSX, Horizon
- VMware Cloud on AWS
- AWS IAM, EC2, VPC, S3

---

**By the numbers**

- **99%** Mitigate 99% of known issues, proactively
- **85%** Reduce outage downtime by 85%
- **98%** Find problems in 98% less time (3x productivity)
- **95%** Automate 95% of security compliance checks

---

**Definition Database**

<table>
<thead>
<tr>
<th>Severity</th>
<th>Source</th>
<th>Applies to</th>
<th>Affects</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Compute</td>
<td>Security</td>
<td>EC2</td>
<td>Ensure no security groups allow incoming connections to EC2 ports and protocols</td>
</tr>
<tr>
<td>Major</td>
<td>Compute</td>
<td>Security</td>
<td>VMware</td>
<td>Password Policy must require at least one uppercase char</td>
</tr>
<tr>
<td>Major</td>
<td>Compute</td>
<td>Security</td>
<td>EC2</td>
<td>Enable two-factor authentication for EC2 instances</td>
</tr>
<tr>
<td>Major</td>
<td>Management</td>
<td>Security</td>
<td>VMware</td>
<td>Password Policy must require at least one lowercase char</td>
</tr>
<tr>
<td>Major</td>
<td>Management</td>
<td>Security</td>
<td>VMware</td>
<td>Password Policy must require at least one number</td>
</tr>
<tr>
<td>Major</td>
<td>Management</td>
<td>Security</td>
<td>VMware</td>
<td>Password Policy must require at least one symbol</td>
</tr>
<tr>
<td>Major</td>
<td>Management</td>
<td>Security</td>
<td>VMware</td>
<td>Password policy must prevent reuse of previously used password</td>
</tr>
<tr>
<td>Major</td>
<td>Management</td>
<td>Security</td>
<td>VMware</td>
<td>Password policy must rotate every 90 days</td>
</tr>
<tr>
<td>Major</td>
<td>Management</td>
<td>Security</td>
<td>VMware</td>
<td>Password Policy must rotate a minimum length of 14 characters</td>
</tr>
<tr>
<td>Major</td>
<td>Management</td>
<td>Security</td>
<td>VMware</td>
<td>Enable 2FA for console login</td>
</tr>
<tr>
<td>Major</td>
<td>Compute</td>
<td>Security</td>
<td>EC2</td>
<td>Ensure no security groups allow incoming connections to EC2 (TCP/22)</td>
</tr>
<tr>
<td>Major</td>
<td>Compute</td>
<td>Security</td>
<td>EC2</td>
<td>Ensure no security groups allow incoming connections to EC2 (TCP/443)</td>
</tr>
<tr>
<td>Medium</td>
<td>Management</td>
<td>Security</td>
<td>VPC</td>
<td>Ensure VPC User logging is enabled in all VPCs</td>
</tr>
<tr>
<td>Medium</td>
<td>Network</td>
<td>Security</td>
<td>VPC</td>
<td>Ensure the default security group of every VPC has EC2 access</td>
</tr>
<tr>
<td>Medium</td>
<td>Management</td>
<td>Security</td>
<td>VMware</td>
<td>Ensure private IP addresses of all VPC’s should be isolated</td>
</tr>
<tr>
<td>Medium</td>
<td>Management</td>
<td>Management</td>
<td>VMware</td>
<td>Ensure Groups for Azure Permissions in VPC Users</td>
</tr>
<tr>
<td>Medium</td>
<td>Compute</td>
<td>Security</td>
<td>EC2</td>
<td>Ensure Azure Virtual Network virtual machines have access to EC2 services</td>
</tr>
</tbody>
</table>

---

- Gain **real-time** operational and security insights
- Monitor, **secure and troubleshoot** your VMware and AWS infrastructures
- See the **future** with upgrade simulations and the past with detailed history
- **Easy OVA deployment** – up and running in minutes
- **Offline repository** limits exposing the internal network to the internet
- **Routinely updates** as soon as new issues or standards are released