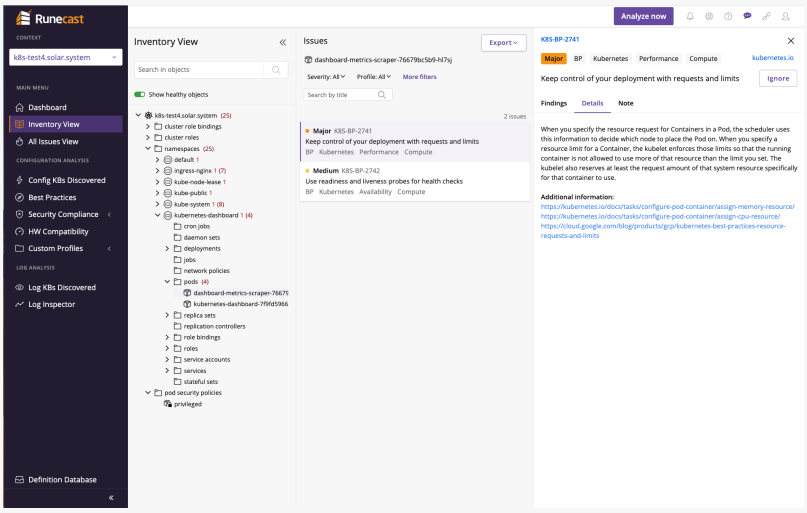
Runecast introduces Kubernetes support to tackle complexity and security compliance challenges with containers adoption

Runecast Analyzer's automated, proactive issues analysis now includes checks for Kubernetes, GDPR compliance on AWS, and offers Custom Profiles.

Runecast Analyzer automates proactive checks of your Kubernetes infrastructure against best practices and security compliance standards.



Dashboard - Kubernetes Best Practices & Security

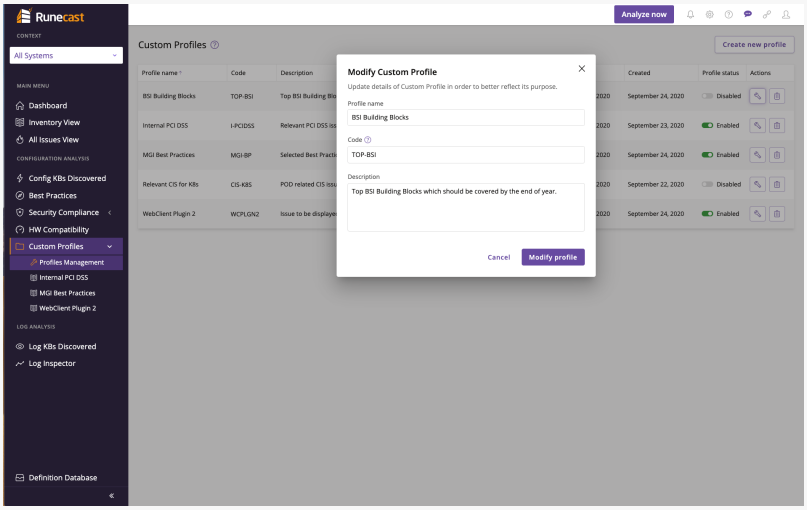
LONDON, UNITED KINGDOM, October 1, 2020 /EINPresswire.com/ -- Runecast Solutions Ltd., a leading provider of patented, predictive analytics for VMware and AWS environments, today announced that its Runecast Analyzer version 4.5 combines new automated best practices and security standards compliance checks for Kubernetes, GDPR compliance checks for AWS, and the ability to set up Custom Profiles.

Built by Admins, for Admins, Runecast Analyzer is a disruptive solution that proactively scans IT infrastructures to identify and report on all known issues that can be prevented within that system. Runecast technology was granted a US patent this year and the company was named a 2020 Cool Vendor by Gartner.

Despite providing IT administrators with hybrid-cloud configuration analysis, Runecast Analyzer runs securely on-premises, with offline capabilities, so that no data leaves the customer organization. Weekly updates are available both through the online, automatic update feature, as well as the download for offline, out-of-band

application.

“Our mission is to help customers automate security compliance and improve business continuity while saving time in IT Operations,,” said Stanimir Markov, CEO and Co-Founder of Runecast. “As organizations start adopting Kubernetes within their hybrid cloud strategy, they face challenges like complexity, skill gaps and ensuring security compliance. Extending Runecast Analyzer's functionality to Kubernetes can now help them tackle these challenges through a single platform.”



Custom Profiles in Runecast Analyzer

Kubernetes best practices & security compliance via automated, proactive checks:

As a natural evolution within the virtualization industry, Kubernetes out-of-the-box is insecure and requires careful tuning to secure the cluster resources and workloads. Even after successfully hardening a Kubernetes environment for production use, the bigger challenge is in maintaining a secure environment over time. It has already proven simple for hackers to identify and make use of Kubernetes clusters by watching specific ports and encountering an insecure Kubernetes API service.

The vast number of security best practices combined with an ever-evolving environment make vulnerabilities a default status without the help of proactive automation. Therefore, it was a natural development to add automated checks for Kubernetes best practices and CIS security compliance standards to Runecast Analyzer.

Runecast Analyzer now offers automated Kubernetes configuration analysis at the node-level, cluster-level, and workload level by covering common cluster operational and security best practices for Kubernetes, as well as the CIS Benchmarks for Kubernetes security standard.

GDPR compliance on Amazon Web Services (AWS) via automated, proactive checks:

As with any security standards that carry a risk for non-compliance, it is humanly impossible to manually keep track of all updates and changes to the standard – and to the environment – at the same time. And while AWS complies with GDPR (to a limited extent) under its Shared Responsibility Model and also attempts to segment services by region, it remains quite possible

for AWS-using organizations to accidentally violate GDPR compliance due to some global services spanning sovereign borders.

Runecast Analyzer enables automated compliance checks according to both the AWS guide Navigating GDPR Compliance on AWS (October 2019) and GDPR Chapter 4 (Art. 24-43) Controller and Processor articles.

Runecast's automated GDPR compliance checks for AWS enable a proactive approach to compliance, rather than firefighting only after a breach has been brought to light.

Custom Profiles for a complex mix of internal security policies and industry security standards:

When managing the infrastructure, it's common to have custom baselines, rules and often specific custom names, descriptions, internal IDs, and even orders within the profile that are tied to internal processes. These custom changes can make security compliance checks even more challenging.

Custom Profiles give Runecast Analyzer users the option to create their own security or best practice profiles based on any rules found in existing Runecast profiles, addressing the need to comply with enterprise-specific custom standards based on a mix of common industry standards such as NIST, CIS, VMware Best Practices, and any other internal policies. It's as simple as picking a name for the new profile and copying rules from any list view in Runecast Analyzer over to the new profile.

Full operational transparency, for risk mitigation and cost savings:

"Compliance to various security standards is still crucial for most companies, especially when transitioning to hybrid environments," said Aylin Sali, CTO and Co-Founder of Runecast. "These enhancements to Runecast Analyzer validate our role in enabling IT admins the best solution for dealing with such in the most cost-effective way possible."

Some forward-thinking organizations already using Runecast Analyzer to mitigate service risks and ensure maximum efficiency and security within their IT infrastructure include (among many others) Chevron, Erste Bank, Raiffeisen Bank, de Volksbank, Fujisoft, Scania, Avast Software, the NHS, and the German Aerospace Center (DLR). "Our customers report increased uptime and audit-readiness for security compliance and as much as 80% operational-time savings," said Mr. Sali.

In addition to version 4.5 providing new best practice and security compliance checks for Kubernetes and new GDPR compliance checks for AWS, Runecast Analyzer provides automated log analysis, best practice checks, and security compliance checks for VMware and AWS

environments. Automated security checks include VMware and AWS security hardening guidelines and common security standards such as CIS, NIST, PCI DSS, DISA STIG, HIPAA, or BSI IT-Grundschutz, with more standards added regularly to the analyzer's secure on-premises (and even offline) capabilities.

"We have always done our best to enable IT admins of mission-critical systems to clearly 'see the future' in terms of potential issues and be able to proactively remediate them," said Mr. Sali. "And great feedback from our customers helps validate that we are fulfilling our aims."
IT admins can test Runecast Analyzer in their own environments with a 14-day free trial.

Jason Mashak
Runecast Solutions
+44 20 3318 1991
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
