# Business stability in 2023 depends on proactive IT security measures, says Runecast

**Platforms that integrate and centralize otherwise disparate security functions into a single user interface plays a significant role.**


**New York City, New York Dec 13, 2022 (**Issuewire.com**)** - Runecast Solutions Ltd. announces significant gains in the latest version of its Cloud Native Application Protection Platform (CNAPP). The AI-driven Runecast platform has added new security standards checks and expanded upon existing security capabilities, making proactive cybersecurity approaches available, more efficient, and less expensive for organizations across the globe.

Named a Cool Vendor by Gartner, Runecast provides an AI-driven platform that helps DevOps and SecOps teams to run secure and compliant workloads across hybrid environments. Runecast customers have given the platform's capabilities high ratings on review portals such as Capterra, GetApp, and G2.

According to *Forbes* (The 7 Biggest Business Challenges Every Company Is Facing In 2023, November 2022), data and device security are one of the biggest business challenges every company faces in 2023: "Cyberattacks are on the rise, and ransomware and phishing scams are now a common occurrence…. Companies can take steps to protect themselves by taking proactive measures like evaluating their data backup and recovery processes, conducting penetration testing and vulnerability scanning, and taking proactive steps to protect sensitive data and prevent cyberattacks."

## What's needed for a proactive approach

**Visibility** – A solution that can automate vulnerability management and compliance of an entire IT

environment with best practices and security standards has become a crucial need for IT teams. Having full visibility of misconfigurations, remediation steps, and reporting is essential for proactive cybersecurity and efficient IT operations management – especially in light of ongoing skills shortages in these areas.

**Consolidation** – On top of cyberattacks being on the rise, global economic activity experiences a broad-based and sharper-than-expected slowdown, according to the International Monetary Fund (World Economic Outlook Report, October 2022). As a result, organizations are forced to restructure their budgets and focus on cost savings. For an IT department, that means consolidating various tool sets where possible, while keeping the same or better level of visibility to ensure security and compliance across the estate.

Runecast Head of Product Management Markus Strauss stated, “It is important for organizations to choose a platform that meets specific needs, which in terms of multi and hybrid cloud environments typically means coverage of multiple vendors and locations visible through a single vendor or a single-platform view.” This holistic view enables organizations to effectively secure and protect cloud-native applications and remove silos between the large number of tools that an organization might be used to prevent any security gaps in its infrastructure. “Besides the holistic view, moving from multiple tools to a single platform can streamline the procurement process, improve the quality of business operations, and most importantly, cut costs”, said Mr. Strauss.

“In Runecast, we've had the centralized proactive approach to security and IT operations in mind since day one. Knowing the amount of time, money, and headache this could save – for admins and organizations as a whole – we were determined to embark on this mission,” stated company CEO and Co-Founder, Stanimir Markov. Using AI to find and remediate misconfigurations, vulnerabilities, and security threats before they cause security breaches or outages is now highly valued by forward-thinking enterprises like Avast, DocuSign, and the German Aerospace Center (DLR) – all customers of Runecast, along with others in heavily regulated verticals such as Financial, Healthcare, Government and Defense.

**A proactive solution must evolve with future needs**

With the latest version released in December this year, Runecast announced new additions of security standards and best practices to its automation capabilities. The platform brings Kubernetes users new compliance checks against the CISA Kubernetes Hardening Guide, as well as the German BSI IT-Grundschutz security standard. Runecast already checks workloads for the CISA Known Exploited Vulnerabilities (KEVs) catalog, so that organizations can see which known vulnerabilities apply to their environment and prioritize remediation actions. With this information in the analysis engine – powered by Runecast AI Knowledge Automation (RAIKA) – IT teams can easily automate checks to avoid common misconfigurations, implement the recommended hardening measures and make their environment better protected against cyberattacks.

Turkish customers can look forward to automated checks of VMware environments against KVKK, the Turkish Data Protection Law, and any company that follows the USA’s NIST cybersecurity framework can now analyze their Operating Systems to reduce cybersecurity risks at the OS level to protect their networks and data.

Runecast now also includes best practices for PowerShell based on the Cybersecurity Information Sheet from NSA, CISA, NZ NCSC, and NCSC-UK. Cybersecurity authorities from the United States, New Zealand, and the United Kingdom recommend proper configuration and monitoring of PowerShell,

as opposed to removing or disabling PowerShell entirely. This provides benefits from the security capabilities PowerShell can enable while reducing the likelihood of malicious actors using it undetected after gaining access to victim networks.

Enabling IT Security and Operations teams with a single platform for discovering and resolving IT problems proactively, the Runecast dashboard shows the entire hybrid IT environment, revealing the most critical areas to prioritize – whether they might be misconfigurations, vulnerabilities, or noncompliances – to ensure security and compliance across the estate for every organization, regardless of on-premises, cloud, or hybrid environments.

Get started with 14 days trial.

**Media Contact**

Runecast Solutions Ltd.

team@runecast.com

Source : Runecast Solutions Ltd.

See on IssueWire