Q4 Company

Cado Security Introduces First-Ever Support to Perform Investigations in Distroless Container Environments

5/8/2024

Cado Security Platform now Supports Investigations in Distroless Container Environments, Eliminating Critical Blindspots and Delivering Unprecedented Visibility into Cloud Risk

LONDON--(BUSINESS WIRE)-- **Cado Security** , provider of the first investigation and response automation platform, today announced the world's first solution to perform forensic investigations in distroless container environments. With Cado Security's new offering, security teams can investigate the root cause, scope, and impact of malicious activity detected within distroless container environments to gain greater visibility into cloud risk.

Investigating Distroless Container Environments with Cado (Photo: Business Wire)

Distroless containers are designed for efficiency and security, stripped of standard OS components like shell utilities and package managers. While these containers offer some security benefits by minimizing the attack surface, they actually leave a huge security blindspot when something malicious does indeed occur. Until today, it was impossible to perform an investigation in these environments, resulting in a significant visibility gap.

"The use of distroless containers is on the rise, promising agile deployment and increased security," said Chris Doman, CTO & Co-Founder at Cado Security. "However, their minimalist design introduces complexities when it comes to investigation and response. This is a pressing security challenge as millions of distroless containers are being used by companies worldwide. We are addressing this with the world's first and only solution to perform forensics investigations in these environments in order to provide much-needed visibility for security teams."

Cado Security delivers a first-of-its-kind solution that addresses the unique challenges distroless containers introduce for security teams. Cado's unique patent-pending approach collects data from distroless and private clusters without impacting the target container to enable immediate investigation. The collected data includes running processes, crucial log files, and forensic artifacts. Cado also uses its previously open-sourced "varc" toolset to collect memory from individual processes for forensic analysis. This evidence is then seamlessly presented in the Cado platform for unprecedented visibility into cloud risk.

Join **Cado Security at RSA 2024 :** Visit the team at Booth #4316 or schedule an on-site meeting during the RSA Conference in San Francisco from May 6-9. For more information about Cado Security's Distroless Container Support, please visit **https://www.cadosecurity.com/blog/cado-introduces-first-ever-support-to-perform-investigations-in-distroless-containers**.

About Cado Security

Cado Security is the provider of the first investigation and response automation platform focused on revolutionizing incident response for the hybrid world. Cado significantly reduces response times by automating the capture, processing, and analysis of data residing in cloud, container, serverless, SaaS, and on-premises environments. Only Cado empowers security teams to add critical context to everyday security investigations on any system. Anywhere. Anytime. Backed by Eurazeo, Blossom Capital, and Ten Eleven Ventures, Cado Security has offices in the United States and United Kingdom. For more information, please visit **www.cadosecurity.com** or follow us on Twitter **@cadosecurity**.

Media Contact:

Michelle Yusupov

Hi-Touch PR

443-857-9468

yusupov@hi-touchpr.com

Source: Cado Security