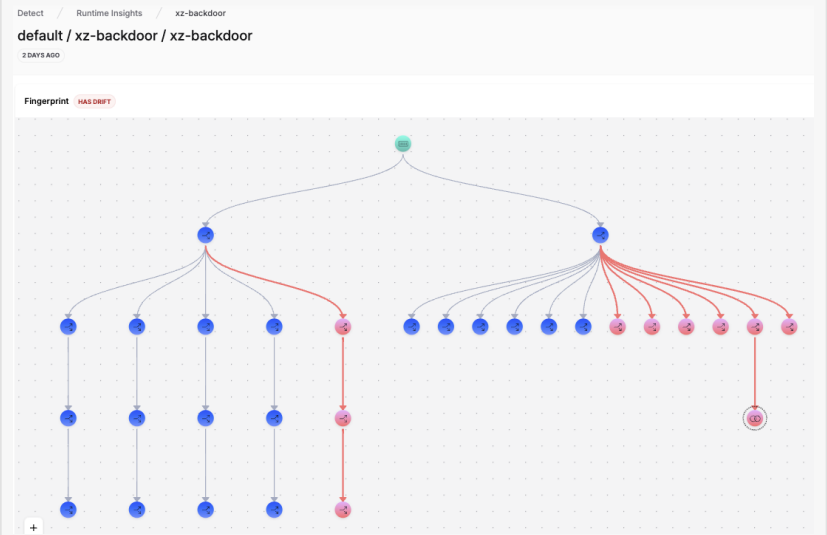
RAD Security launches first behavioral detection and response solution for cloud native environments

Unique behavioral fingerprints allow security teams to detect novel attacks and respond with real-time identity and infrastructure context



Fingerprint of XZ Backdoor Attack in RAD Security

SAN FRANCISCO, CA, USA, May 6, 2024 /EINPresswire.com/ -- Today, RAD Security releases the industry's first behavioral detection and response solution for cloud native environments, as CEO Brooke Motta takes the stage in San Francisco for the RSA Conference Innovation Sandbox. To-date, signature and anomaly-based methods are late and ineffective against cloud native attacks like the recent XZ Backdoor. RAD's detection and response platform is the first to baseline behavior through workload fingerprints, detecting cloud native attacks as they happen, while tying in real-time infrastructure and identity context for response prioritization.

> As the footprint of cloud native environments continues growing, security teams can no longer rely on signature-based detection that only works after the attack"
>
> *Jimmy Mesta, CTO and Co-Founder of Rad Security*

"As the footprint of cloud native environments continues growing, security teams can no longer rely on signature-based detection that only works after the attack, or false promises from AI and machine learning models based on insufficient samples of cloud attacks. Security teams need to respond to cloud native attacks as they happen, with clear prioritization across workloads, infrastructure and identity," explains CTO and Co-Founder, Jimmy Mesta.

Today, 70% of teams are using containers in production, and analysts predict that, by 2025, 95% of new applications will be built using cloud native workloads. A recent survey shows that 90% of teams using containers and Kubernetes had an incident in the last year, and a

full 95% of IT decision makers feel their team has been negatively impacted by the cloud security skills gap.

In the weeks following the zero day XZ Backdoor software supply chain attack, cloud native IDS approaches resulted in signatures days and weeks following the attack, and anomaly detection approaches were blind to the set of attackers' techniques that relied on normal processes. To detect the XZ Backdoor and other zero day attacks, a behavioral profile of the environment would have been required before the attack took place.

RAD's behavioral fingerprints are based on the fact that the majority of cloud native workloads exhibit a consistent set of core processes, programs and files at runtime. Any drift from this core set of behaviors is suspicious. RAD fingerprints get critical context from its ITDR and KSPM capabilities to help reduce noise and allow teams to understand the true impact of detections, compared to leading CSPM and CNAPP vendors that leave teams blind to the real-time changes between cloud native identity, infrastructure, and workloads.

The launch of the behavioral detection and response platform follows the release of the open source fingerprint standard and Cloud Native Identity Threat Detection & Response (ITDR). Over a dozen companies are using RAD to create fingerprints in their environment, and in the last year alone, RAD Security has seen ARR grow by 3 times, with a 219% net retention rate and new logos from highly regulated and digitally mature industries such as insurance, banking and media. At the same time, the current and growing importance of cloud native technologies in the security team's priorities is reflected in 60% growth of customer contract value, with nearly half of new ARR coming from expansion of current customers.

New features in this release include:
- Fingerprints and drift for unique containers:
RAD can now create cloud native behavioral workload fingerprints and detect drift for custom containers (versus just open source) at runtime

- eBPF sensor:
RAD is releasing a newly re-configured, custom eBPF sensor to get around the inflexibility and instability inherent in legacy agents. RAD's agent requires the fewest and most precise permissions, has more flexibility for correlation of data across the environment, and a smaller footprint

- Response actions:
Customers can terminate pods, label pods, and quarantine pods (e.g. prevent network egress from pods) in response to drift detection

- AI/LLM Categorization of Drift Events:
Drift events are classified into different attacks (if known), based on LLM-driven analysis

- Workflow manager:
Set up automated workflows to choose how to respond to detections from RAD, whether that's to notify to one or more channels, label a pod to enable security teams to further investigate, kill a pod, or quarantine, open a pull request, run Terraform, call an AWS API to change a setting, and more

Learn more about behavioral cloud native threat detection and response, meet us in the innovation showcase at the RSA Conference Innovation Sandbox competition, or reach out to get started creating your unique behavioral fingerprints today!

About RAD Security
RAD Security is a cloud native security company that empowers engineering and security teams to push boundaries, build technology and drive innovation so they can focus on growth versus security problems. In sharp contrast to one-size-fits-all, legacy CWPP and container detection and response solutions, RAD takes a custom, behavioral approach to cloud native detection and response that can counter evolving threats while sharpening inputs into shift-left and posture management.

Daniel Delson
Magnitude Growth
+1 917-328-9337
email us here
