



Amiram Shachar
CEO & Cofounder
Upwind

As cloud-native architectures become central to GCC operations, how is Upwind helping GCCs secure their cloud workloads without slowing innovation?

As cloud-native architectures become central to GCC operations, Upwind helps teams secure workloads by grounding every decision in real-time runtime data. GCC teams are building and operating high-velocity environments where services, APIs, and infrastructure are constantly changing. Upwind provides continuous visibility into what is actively running, which vulnerabilities are in use, and how applications communicate in real time. This allows teams to prioritize the risks that have real impact, streamline remediation, and stay aligned with development velocity. Security and engineering teams get a shared, accurate picture of risk, which means faster decisions, fewer false positives, and protection that keeps pace with the speed of modern cloud-native development. The result is security that operates as an enabler of innovation.

Upwind

How do you see runtime cloud security evolving for GCCs that manage global, business-critical applications from India?

For GCCs managing global, business-critical applications from India, runtime cloud security will continue to become a central layer of how decisions are made to protect against AI risks. These teams are running business-critical infrastructure for some of the world's largest enterprises, which makes them a high-value target for increasingly sophisticated attacks. The threat landscape has shifted toward real-time attacks targeting AI pipelines, APIs, and cloud-native services directly. Runtime insights bring together signals across posture, behavior, and live traffic, creating a unified view of risk. This enables teams to continuously validate what matters across the lifecycle, from build to production. As AI models become more deeply embedded in GCC workflows, the ability to monitor and protect those systems at runtime, in real time, will become a baseline requirement for every modern enterprise.

What role will real-time threat intelligence and automation play in shaping the future security posture of cloud-first GCCs?

Real-time threat intelligence and automation will play a key role in shaping the security posture of cloud-first GCCs. Real-time intelligence

provides immediate context into how threats relate to active workloads, including exploitability, exposure, and potential impact. Automation builds on that context to accelerate investigation and response, connecting signals across environments and surfacing clear actions for teams. Together, they support faster decision-making, reduce operational overhead, and allow GCC teams to manage complex global systems with precision and confidence. ■