# CrowdStrike Stops Cloud Attacks in Seconds with Real-Time Cloud Detection and Response Innovations

December 1, 2025

*New real-time detection engine, cloud Indicators of Attack, and automated response actions give SOC teams real-time protection at machine speed*

AUSTIN, Texas & LAS VEGAS--(BUSINESS WIRE)--Dec. 1, 2025-- **AWS re:Invent 2025** -- CrowdStrike (NASDAQ: CRWD) today unveiled new Cloud Detection and Response (CDR) innovations, advancing real-time protection across hybrid and multi-cloud environments. Powered by a new real-time detection engine built on streaming technology pioneered and battle-tested by the world's top threat hunters, the enhanced CDR eliminates detection delays, surfacing high-fidelity alerts in seconds. With expanded cloud Indicators of Attack (IOAs) and new automated response actions, CrowdStrike gives defenders the speed and precision to stop cloud attacks the moment they begin.

"Real-time security is the difference between stopping a breach and needing incident response – every second counts. Today's adversary moves fast and across domains, and defenders can't afford to waste time waiting for cloud logs to process or detections to populate," said Elia Zaitsev, chief technology officer at CrowdStrike. "CrowdStrike's new real-time CDR reduces response time to seconds, stopping cloud threats before they spread."

As adversaries weaponize AI to accelerate cloud attacks and move laterally across systems, traditional CDR relying on log batch processing is too slow to keep up, often taking 15 minutes or more to surface a single detection. CrowdStrike pioneered CDR and continues to innovate to stop modern cloud threats. By processing logs in real time with event streaming technology hardened at scale by Falcon® Adversary OverWatch, CrowdStrike instantly surfaces high-fidelity alerts. Paired with new IOAs and automated response actions, these enhancements eliminate detection delays, alert noise, and manual bottlenecks, detecting stealthy cloud attacks in real time and dramatically reducing mean time to respond.

As part of Falcon® Cloud Security's unified CNAPP securing every layer of hybrid cloud risk, CrowdStrike delivers the next evolution of CDR built on three key innovations:

- **Real-Time Detection Engine:** Built on event streaming technology from the world's top threat hunters, this real-time detection engine analyzes cloud logs as they stream in, applying detections instantly to eliminate latency and false positives.
- **Expanded Cloud Indicators of Attack:** New out-of-the-box real-time detections engineered specifically for cloud adversary behavior leverage AI and machine learning to correlate live activity with cloud asset and identity context to expose advanced attacks – from stealthy privilege escalation to CloudShell abuse – in real time.
- **Automated Cloud Response Actions and Workflows:** Traditional Cloud Workload Protection (CWP) stops at the workload, leaving the cloud control plane exposed, while Cloud Security Posture Management (CSPM) only shows what could go wrong without providing runtime protection. Built on Falcon® Fusion SOAR, new customizable, out-of-the-box workflows close this gap, triggering the instant that threats are detected to automatically disrupt adversaries without waiting for manual SOC intervention.

To learn more about CrowdStrike's latest CDR innovations visit booth #1102 at AWS re:Invent and read our blog.

**About CrowdStrike**

CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/
Follow us: Blog | X | LinkedIn | Instagram
Start a free trial today: https://www.crowdstrike.com/trial

brands of third parties to identify their products and services.

View source version on businesswire.com: https://www.businesswire.com/news/home/20251130325280/en/

**Media Contact**
Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike