

Falcon Cloud Security: Cloud Detection and Response (CDR)

Real-time cloud defense to stop the breach

Cloud is the new SOC battleground

Cloud environments have become one of the most attractive targets for modern adversaries. As AI becomes the new operating model for the enterprise, cloud environments are scaling rapidly to support AI-driven workloads, which expands the attack surface for modern adversaries. Adversaries increasingly exploit cloud control planes, stolen identities, and ephemeral workloads to move at machine speed and evade legacy security approaches.

The CrowdStrike 2026 Global Threat Report reflects this new reality: Cloud-conscious intrusions increased 37% in 2025, with the fastest breakout time recorded at 27 seconds, leaving security teams with virtually no margin for gaps. In many cases, cloud attacks are completed before traditional cloud security tools can surface a detection at all.

SOC teams are facing mounting challenges:

- Discovering and managing a constantly changing cloud attack surface spanning agent-based workloads and agentless cloud services, creating visibility gaps and operational complexity
- Navigating a shortage of cloud-skilled SOC analysts, slowing triage and response
- Separating real cloud threats from noise, as massive volumes of ever-changing identity, workload, and API activity make adversary behavior appear legitimate
- Operating with siloed tools that provide visibility without cloud-native enforcement, leaving teams unable to stop active attacks
- Relying on delayed agentless detections that arrive out of sequence and slow investigations and response

Stopping modern cloud breaches requires real-time detection, unified runtime, and cloud telemetry within a single platform, and immediate cloud-native response.

Key benefits

- **Stop cloud attacks in real time:** Detect and stop active cloud attacks in seconds, before lateral movement, data theft, or ransomware deployment.
- **See the full attack, not isolated alerts:** Unify cloud, identity, and endpoint activity into a single attack timeline to quickly understand scope and impact.
- **Accelerate investigations at adversary speed:** Reduce analyst effort and response time by eliminating manual correlation and alert noise.
- **Turn cloud visibility into immediate action:** Contain active attacks across cloud environments to stop abuse as it happens.

Stop cloud breaches with real-time CDR

Cloud detection and response (CDR), a feature of CrowdStrike Falcon® Cloud Security, delivers the industry's most complete real-time cloud defense for SOC teams by unifying:

- Battle-tested, real-time cloud indicators of attack (IOAs)
- Cloud workload protection (CWP)
- Native identity and endpoint context

Falcon Cloud Security exposes adversary behavior in real time, enabling defenders to disrupt attacks in seconds — not minutes — across cloud infrastructure and control planes.

What makes Falcon Cloud Security CDR different

Real-time IOAs

Falcon Cloud Security CDR detects malicious cloud behavior the moment it happens, using adversary-informed, behavior-based cloud IOAs powered by real-time streaming detection and battle-tested by CrowdStrike Falcon® Adversary OverWatch™ threat hunters — not static rules or delayed logs — to expose stealthy attacks that bypass traditional tools.

Unified cross-domain correlation, built for SOC operations

Falcon Cloud Security CDR natively integrates cloud detections with identity and endpoint signals inside the Falcon platform, delivering cross-domain context directly within existing SOC workflows to enable faster triage, investigation, and response without forcing analysts to pivot between disconnected consoles.

Proven against real adversaries

Falcon Cloud Security CDR is powered by CrowdStrike's industry-leading threat intelligence and validated through real-world adversary campaigns, including identity-driven cloud intrusions like SCATTERED SPIDER.

Key capabilities

Detect

- **Cloud Asset and Attack Surface Visibility:** Gain continuous visibility into cloud accounts, services, identities, and workloads, including ephemeral infrastructure
- **Real-Time Detections:** Detect active cloud attacks across the cloud stack
- **Adversary Intelligence:** Get detections informed by real-world adversary behavior and campaigns

Investigate

- **Unified Cases:** Correlate cloud, identity, and endpoint activity into a single investigation with a complete attack timeline
- **Attack Path Context:** Understand how attackers move from initial access to impact
- **Agentic AI-powered Investigations:** Accelerate analysis from detection to response with AI-guided workflows

Independently validated real-time cloud defense

MITRE ATT&CK® Validated: Falcon Cloud Security achieved 100% detection and 100% protection with zero false positives in the 2025 MITRE ATT&CK Evaluations across cloud, identity, and endpoint scenarios.

The result is a SOC that operates with greater efficiency, higher confidence, and the ability to stop cloud breaches.

Respond

- **Immediate Sensor-Based and Sensorless Containment:** Block malicious identities, terminate compromised workloads, and stop active abuse

Protect

- **Hybrid and Multi-Cloud Coverage:** Protect AWS, Azure, Google Cloud, Kubernetes, and on-premises workloads

Managed cloud defense, 24/7

Extend cloud runtime protection with CrowdStrike Falcon® Adversary OverWatch™ and CrowdStrike Falcon® Complete to deliver 24/7, human intelligence-led cloud threat hunting and response.

With these managed services, elite CrowdStrike analysts monitor cloud activity around the clock, proactively hunting adversaries and executing full-cycle remediation to extend SOC capacity without adding operational overhead.

Proven business outcomes

Organizations using Falcon Cloud Security can achieve:

- Up to 89% faster cloud detection and response – [Mercury Financial](#)¹
- Up to 72% faster ability to monitor the entire cloud estate²
- Up to 83% reduction in cloud security licenses through consolidation²
- Up to \$480K average annual savings²
- Up to 130 hours saved per month per security team²
- Up to 71% improvement in cloud policy consistency²

Why CrowdStrike

CrowdStrike is the only cloud security provider that:

- Delivers battle-tested, real-time cloud IOAs to detect and disrupt attacks in real time
- Natively correlates cloud, identity, and endpoint telemetry to deliver complete cross-domain context
- Unifies CDR, CWP, and adversary intelligence to enable immediate response across cloud workloads and control planes
- Actually stops breaches, doesn't just report on risk after the fact

Next steps

- [Get a deeper look into Falcon Cloud Security CDR](#)
- [Learn how real-time cloud IOAs stop modern cloud adversaries](#)
- [Leverage five best practices to strengthen your cloud detection and response program](#)
- [Explore Falcon Complete for managed cloud defense](#)

¹ Results are from a customer. Individual results may vary. Read more about [Mercury Financial](#).

² The above numbers reflect the median inputs provided by Customers during post-sale motions that compare the value of CrowdStrike with incumbent solutions and are not guaranteed. They are intended to demonstrate potential value compared to incumbent solutions and do not represent promised outcomes. Actual value realized will depend on individual Customer module deployment and environment.

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/>

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>

