

Falcon Adversary OverWatch: Cloud Threat Hunting

Disrupt cloud-based attacks with the industry's most complete threat hunting service powered by AI and industry-leading threat intelligence

Challenges

Modern attacks make the most of today's vast cloud attack surface — serverless computing vulnerabilities, misconfigured services, and container registry dependencies are just a few of the issues ripe for adversary compromise and weaponization. Making matters worse, as adversaries shift their operations to the cloud, security teams struggle to keep pace.

The cloud remains a prime target for adversaries. According to the [CrowdStrike 2025 Global Threat Report](#), cloud intrusions rose 26% from 2023 to 2024, underscoring the growth in adversaries exploiting cloud services. Cloud-focused threat actors are leveraging misconfigurations, stolen credentials, and cloud management tools to infiltrate systems, move laterally, and maintain persistent access for malicious activities like data theft and ransomware deployment. Valid account abuse has become the primary initial access tactic, observed in 35% of cloud incidents in the first half of 2024. Once inside, adversaries quickly move laterally within the network — the fastest observed eCrime breakout time in 2024 was 51 seconds.

Key benefits

- **Hunt adversaries in the cloud:** CrowdStrike Falcon Adversary OverWatch relentlessly hunts 24/7 across your critical cloud infrastructure — including Microsoft Azure, AWS, and Google Cloud — to detect the stealthiest and most sophisticated cloud threats.
- **Protect the cloud control plane:** CrowdStrike Falcon® Cloud Security generates granular data and control plane visibility, enabling CrowdStrike Falcon® Adversary OverWatch™ hunters to detect unauthorized resource provisioning, suspicious configuration changes, and improper access controls.
- **Stop breaches across all domains:** With industry-first unified visibility across cloud, identity, and endpoint, and paired with Falcon Adversary OverWatch Next-Gen SIEM, CrowdStrike threat hunters monitor for compromised users in cloud attacks and track lateral movements everywhere, ensuring no adversary slips through unnoticed.

Solution

To disrupt the stealthiest and most advanced cloud-based attacks, organizations need the specialized and proactive cloud threat hunting provided by CrowdStrike Falcon Adversary OverWatch and its managed 24/7 operations.

Falcon Adversary OverWatch delivers a robust, integrated cloud threat hunting capability to rapidly detect advanced threats that originate, operate, and persist in cloud environments. It leverages the CrowdStrike Falcon® platform's unified visibility — spanning cloud, identity, and endpoint first-party data, along with CrowdStrike Falcon® Next-Gen SIEM third-party data — to accelerate detection and response at every stage of a cloud attack, even as threats move laterally across domains. With expanded visibility into the cloud control planes and runtime environments of critical cloud infrastructures — including Microsoft Azure, AWS, and Google Cloud — Falcon Adversary OverWatch provides a comprehensive cloud threat hunting service to rapidly detect threats and accelerate response.

CrowdStrike delivers best-in-class cloud runtime workload protection (CWP) and cloud detection and response (CDR), allowing SOC teams to detect and respond to active threats across hybrid clouds.

Bolstered by Falcon Adversary OverWatch's AI-powered 24/7 threat hunting and industry-leading threat intelligence, you can stop cloud-based breaches and protect your organization.

Key capabilities

Disrupt cloud-based attacks

- **Unrivaled cloud telemetry:** Falcon Cloud Security protects billions of containers every day. Gain real-time visibility into this massive cloud sensor network through Falcon Adversary OverWatch cloud threat hunting, and view cloud threat activity as it happens.
- **Limitless operations:** Hunt cloud threats everywhere with full visibility into Kubernetes; workloads in production; host incidents (e.g., cryptominers, suspicious ELF headers); and entire running applications, active processes, and system and network calls across all ingoing and outgoing active ports.
- **Native control plane observability:** Falcon Cloud Security generates granular data and control plane visibility — down to the workload operating system — for Falcon Adversary OverWatch to hunt deep within and across cloud containers, workloads, Kubernetes clusters, and other cloud infrastructure.

Gain threat hunting across the attack surface spanning cloud, identity, endpoint, and beyond

- **24/7/365 global coverage:** When a sophisticated intrusion occurs, time is critical. Adversaries are not restricted by time zones or geography — and CrowdStrike's threat hunters are always watching.
- **Protection for cloud environments:** Falcon Adversary OverWatch expert hunters continuously scour hybrid and multi-cloud environments for novel and suspicious cloud threat behaviors, such as control plane and serverless workload vulnerabilities, misconfigurations, application behavior anomalies, container escapes, API privilege escalations, worker node compromise, and more.
- **Expand protection across your environment*:** Enhance threat hunting with additional Falcon Adversary OverWatch modules that cover endpoint, identity, and third-party Falcon Next-Gen SIEM data to uncover stealthy adversaries before they can breach your network.

**For threat hunting across the attack surface, please see the Products and Services chart.*

Speed up decision-making with intelligence

- **Adversary insights:** Falcon Adversary OverWatch tracks 255+ nation-state, eCrime, and hacktivist adversaries. Identify the adversaries targeting your organization, and gain insights into their intent and capabilities.
- **Automated malware sandbox:** Safely detonate suspicious files in a secure environment. Get threat verdicts, severity ratings, and indicators of compromise (IOCs), and understand file behavior and related malware to anticipate and stop future attacks.
- **Context-aware indicators:** Falcon modules are enriched with built-in intelligence and context-aware indicators. Explore the relationship between IOCs, endpoints, and adversaries, and search across millions of real-time threat indicators.

Examples of Falcon Adversary OverWatch cloud threat hunting

- **Cloud control plane attack:** An adversary logged in with legitimate credentials and then downloaded PCUnlocker, likely aiming to reset other credentials. They used AD Explorer for domain reconnaissance, identifying Azure hosts to which they then moved laterally. Once in the control plane, they installed Azure AD PowerShell to conduct further Active Directory reconnaissance, facilitate additional lateral movements, and execute significant data exfiltration. Falcon Adversary OverWatch quickly detected the threat and provided the customer with strategic countermeasures to mitigate the risk.
- **Cloud as a gateway to endpoint:** An adversary used valid credentials to achieve execution on Windows endpoints via a third-party cloud management tool. They proceeded to use PowerShell to download an unknown executable to Windows endpoints. Falcon Adversary OverWatch detected the activity in real time and alerted the customer for immediate response.
- **Identity attack on the cloud:** During an eCrime intrusion, a Falcon Adversary OverWatch threat hunter used data from Falcon Cloud Security to support their analysis. They identified the adversary's attempt to establish persistence in the cloud by adding an additional federated domain. In this instance, the threat hunter provided essential intelligence that enabled the customer's incident response team to quickly contain the incident.

Attend a hands-on workshop →

Request a demo →

CrowdStrike Threat Intelligence and Hunting Products and Services

Feature Categories	Key Features	Falcon Adversary OverWatch	Falcon Adversary OverWatch Identity ¹	Falcon Adversary OverWatch Cloud	Falcon Adversary OverWatch Next-Gen SIEM ²	Falcon Adversary Intelligence	Falcon Adversary Intelligence Premium	Falcon Adversary Operations Elite ³
Threat Hunting	24/7 Managed Threat Hunting	✓	✓	✓	✓			
	- Falcon Insight XDR	✓						
	- Falcon Identity Protection		✓					
	- Falcon Cloud Security			✓				
	- Falcon Next-Gen SIEM				✓			
Threat Intelligence	Adversary Cards	✓	✓	✓	✓			
	In-Depth Adversary Profiles					✓	✓	
	Weekly Threat Summaries					✓	✓	
	Threat Landscape Dashboards					✓	✓	
	Intelligence Reports						✓	
	Quarterly Threat Briefs						✓	
	Threat Hunting Libraries						✓	
	Requests for Information (5 Pack)						Ability to add	✓
	Priority Intelligence Requirements							✓
	Threat Graph Queries (50 per Year)							✓
Digital Risk Protection	Dark Web Monitoring					✓	✓	
	Brand and Domain Monitoring					✓	✓	
	Credential Monitoring					✓	✓	
	Dark Web Activity Reports					✓	✓	
Automation and Tools	Malware Sandbox Quarantined by Falcon Sensor	Unlimited		Unlimited		Unlimited	Unlimited	
	Malware Sandbox Manual Submissions	100/month		100/month		500/month	500/month	
	Indicator of Compromise App	✓			✓	✓	✓	
	Vulnerability Intelligence App	✓				✓	✓	
	QuickScan Pro Analysis					1,000/month	2,500/month	
	Threat Feed (IOCs)					✓	✓	
	APIs and Integrations					✓	✓	
	Human Malware Analysis (50 per Year)						✓	
	Pre-Built Detection Rules (YARA, Snort)						✓	
Assigned Analyst	Access Analyst via Email							✓
	Customer-Directed Threat Hunts							✓
	Threat Hunt Query Optimization							✓
	External Digital Risk Investigations							✓
	Tailored Threat Briefings and Risk Reports							✓

¹ Falcon Adversary OverWatch or Falcon Adversary OverWatch Cloud is a prerequisite for Falcon Adversary OverWatch Identity.

² Falcon Adversary OverWatch Endpoint or Falcon Adversary OverWatch Cloud, and Falcon Next-Gen SIEM are prerequisites for Falcon Adversary OverWatch Next-Gen SIEM.

³ Falcon Adversary Intelligence Premium is a prerequisite for Falcon Counter Adversary Operations Elite.

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/>

