

Falcon Adversary OverWatch

Disrupt attacks everywhere across endpoint, identity, cloud, and beyond with the industry's most complete threat hunting service powered by AI and elite adversary intelligence

Challenges

Adversaries are no longer confined to a single domain — they attack everywhere. From cloud environments and endpoints to firewalls, VPNs, routers, and email gateways, threat actors exploit every available surface to gain entry and move fast. Valid credentials remain their weapon of choice, enabling stealthy access and rapid lateral movement across domains.

According to the [CrowdStrike 2025 Global Threat Report](#), 52% of vulnerabilities exploited in 2024 were tied to initial access, with valid account abuse driving 35% of cloud intrusions. Once inside, adversaries moved fast — the fastest observed eCrime breakout time was just 51 seconds. Cloud intrusions rose 26% year-over-year, driven by misconfigurations, stolen credentials, and abuse of cloud management tools.

The gaps across domains and entry points create significant challenges for security teams, who struggle to correlate signals across siloed tools. This disconnect leads to missed threats and delayed response. Closing these gaps requires effective threat hunting with end-to-end visibility, actionable threat intelligence, and expert threat hunters who can connect the dots and stop breaches in real time.

Solution

CrowdStrike Falcon® Adversary OverWatch™ delivers a complete managed threat hunting solution to rapidly detect advanced threats across the entire attack surface. By leveraging true end-to-end visibility across endpoint, identity, cloud environments, and third-party next-gen SIEM data, CrowdStrike experts effectively hunt threats across all attack surfaces, detecting exploitations of common entry points like firewalls, routers, and email gateways, monitoring for compromised users in cloud attacks, and tracking lateral movement between cloud and endpoint. Falcon Adversary OverWatch breaks down silos to hunt adversaries everywhere, significantly reducing complexity and accelerating response time for customers.

Leveraging the AI-native CrowdStrike Falcon® platform and CrowdStrike's industry-leading threat intelligence, Falcon Adversary OverWatch provides proactive 24/7 threat hunting to stop breaches and protect your organization.

Key benefits

- **Hunt Threats Across the Attack Surface:** CrowdStrike Falcon Adversary OverWatch delivers 24/7 proactive detection of adversaries everywhere across domains and beyond — leveraging first-party endpoint, identity, and cloud data, along with Falcon Next-Gen SIEM third-party data.
- **Detect Threats Early:** With true end-to-end visibility, Falcon Adversary OverWatch detects adversary movement earlier in the attack, disrupting threats before they breach the network.
- **Protection from Day One:** With no downtime or additional action required from customers, Falcon Adversary OverWatch immediately correlates vast amounts of first- and third-party data to detect threats, ensuring no adversary slips through unnoticed.

Falcon Adversary OverWatch solutions

Threat hunting across all attack surfaces

- **Falcon Adversary OverWatch Endpoint:** CrowdStrike threat hunters relentlessly pursue adversaries targeting your endpoints. Fortify your defense against sophisticated identity attacks with real-time protection and accelerated response.
- **Falcon Adversary OverWatch Identity:** Defend against identity threats with Falcon Adversary OverWatch's identity threat hunting and credential monitoring. Threat hunters proactively contain and alert on identity-based attacks, minimizing further damage. Monitor criminal forums for stolen credentials and force multifactor authentication (MFA) challenges.
- **Falcon Adversary OverWatch Cloud:** Stop cloud attacks with the industry's most complete cloud threat hunting service within CrowdStrike Falcon® Cloud Security unified cloud detection and response (CDR). Expand visibility into runtime environments and cloud control planes for Microsoft Azure, AWS, and Google Cloud. Monitor for compromised users and lateral movement between cloud and endpoint.
- **Falcon Adversary OverWatch Next-Gen SIEM:** Falcon Adversary OverWatch expands threat hunting to third-party data ingested by Falcon Next-Gen SIEM — covering network edge devices, SaaS, email, identity access and management, operating systems, and more — to detect stealthy adversaries before they breach the network.

Key capabilities

World-class expertise powered by AI

- **Elite threat hunters:** CrowdStrike's threat hunters are best-in-class at detecting the stealthiest adversaries, including those exploiting legitimate tools for their attacks. These elite threat hunters proactively identify novel threats in real time across the entire CrowdStrike customer base and instantly deploy new detections on your behalf.
- **AI-powered hunting techniques:** CrowdStrike expert threat hunters use state-of-the-art AI, statistical methods, and hypothesis testing to detect stealthy attacks 24/7, finding the most sophisticated threats.
- **Vulnerability intelligence:** Find and prioritize vulnerabilities with real-time National Vulnerability Database updates. Gain additional threat insights, including severity scores, affected products, and related malware, threat actors, and reports.

Native intelligence to speed up decision-making

- **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:** CrowdStrike 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 threat hunting across the attack surface

- **Cloud as a gateway to endpoints:** 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 CrowdStrike Falcon Cloud Security to support the analysis. The adversary was identified while attempting 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.
- **Identity attack on endpoints:** A Falcon Adversary OverWatch threat hunter used both identity and endpoint data to inform their analysis while hunting an eCrime intrusion. The threat hunter was able to understand the adversary's identity reconnaissance efforts, the tools they used on the endpoint, and their credential dump attempts. Due to this comprehensive insight, the customer rapidly disabled the compromised accounts and contained the intrusion.
- **Insider threat detected via third-party SIEM data:** Falcon Adversary OverWatch identified a new employee with a BYOD device logging in from an IP linked to known adversary activity. Using third-party identity data from Falcon Next-Gen SIEM and pivoting to identity provider logs, Falcon Adversary OverWatch confirmed additional overlaps, exposing activity that would've remained hidden without expanded visibility.

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							✓

¹Falcon 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 at www.crowdstrike.com/

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

