

Falcon Adversary OverWatch: Identity Threat Hunting

Disrupt sophisticated adversaries executing identity-based attacks with 24/7 managed threat hunting powered by AI and CrowdStrike expertise

Challenges

Adversaries aren't breaking in, they're logging in. More than half of breaches involve credentials, bypassing traditional endpoint protections to gain access to an organization's network without being detected. According to the [CrowdStrike 2025 Global Threat Report](#), malware-free intrusions represented 79% of detections in 2024.

This trend indicates that adversaries are increasingly employing identity attacks — like phishing and social engineering — and purchasing stolen credentials on criminal forums to gain access. Valid account abuse has become the primary initial access tactic, observed in 35% of cloud incidents in the first half of 2024. Once they log in, they move quickly, breaking out from the initial system to move laterally within the network. The CrowdStrike 2025 Global Threat Report showed that the fastest observed eCrime breakout time in 2024 was just 51 seconds.

Identity is the new security battleground, and the onslaught of identity-related attacks requires constant vigilance. With adversaries' growing proficiency in obtaining legitimate credentials, hunting for users performing unexpected activity has never been more important. Defenders need to stop breaches faster by protecting workforce identities and enforcing multifactor authentication (MFA) when suspicious user activity is detected.

Key benefits

- CrowdStrike Falcon® Adversary OverWatch™ proactively hunts adversaries everywhere across all attack surfaces — leveraging first-party identity, endpoint, and cloud data and third-party CrowdStrike Falcon® Next-Gen SIEM data — stopping stealthy threats before they breach the network.
- CrowdStrike threat hunters detect the stealthiest adversaries, including those that use tactics such as brute force attacks, account takeover, privilege escalation, or suspicious login activities from unfamiliar locations or devices
- Falcon Adversary OverWatch constantly monitors the criminal underground for compromised credentials and mitigates the threat using Falcon Identity Protection

Solution

Identity threat hunting is a complex task requiring expertise and sophisticated tools. CrowdStrike Falcon® Adversary OverWatch™ reduces cost and complexity by delivering a managed service that provides 24/7 protection — all powered by the AI-native CrowdStrike Falcon® platform and CrowdStrike's unrivaled team of threat hunting experts.

The inclusion of identity data in threat hunting activities is a crucial component of a comprehensive investigation. Adversaries often gain access to numerous accounts to maintain persistent access during an intrusion. CrowdStrike Falcon® Identity Protection generates robust identity telemetry, enabling CrowdStrike's threat hunters to identify both managed and unmanaged hosts. This enables them to detect adversaries attempting to gather additional credentials or escalate privileges in preparation for lateral movement.

By continuously monitoring user behaviors, access controls, and authentication mechanisms, Falcon Adversary OverWatch can detect threats that specifically target user credentials, allowing organizations to undertake proactive mitigation and defensive actions.

Key capabilities

Disrupt identity-based attacks

- **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.
- **Identify compromised credentials:** Falcon Adversary OverWatch analyzes user identity data, login patterns, and authentication data to detect early signs of compromised credentials. This data is used to enrich intrusion investigations with endpoint and cloud runtime telemetry. Upon discovery, Falcon Adversary OverWatch hunters promptly alert customers so they can take immediate action to mitigate the impact of unauthorized access in their environments.
- **Discover stolen credentials on the dark web:** Falcon Adversary OverWatch continuously monitors criminal forums for stolen credentials and will force an MFA challenge or password reset through Falcon Identity Protection.

Hunt identity threats across every attack surface

Identity threat hunting is crucial, as adversaries are increasingly exploiting compromised identities to launch attacks across endpoints, cloud, and beyond. With Falcon Adversary OverWatch, you gain comprehensive protection everywhere and peace of mind against sophisticated identity threats.

- **Expand protection across your environment*:** Enhance threat hunting with additional Falcon Adversary OverWatch modules that cover endpoint, cloud, and third-party Falcon Next-Gen SIEM data — uncovering 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:** 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 identity threat hunting

- **Malicious access:** During an eCrime intrusion, a Falcon Adversary OverWatch threat hunter discovered 21 compromised accounts attempting to log in from a malicious VPN. Upon investigating a known compromised user, the hunter detected logins from unknown IP addresses. It was also observed that the other 20 users had logged in or attempted to log in from the same IP. Recognizing the malicious nature of this activity, the analyst quickly notified the customer, enabling them to immediately reset the password and block the malicious IPs.
- **Multi-domain attack:** A Falcon Adversary OverWatch threat hunter used both identity and endpoint data to inform their analysis while hunting an eCrime intrusion. The analyst 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.
- **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 analyst identified the adversary's attempt to establish persistence in the cloud by adding an additional federated domain. Such visibility would not have been possible with cloud data alone. In this instance, the analyst 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/>

