CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Adversary OverWatch: Endpoint Threat Hunting

Disrupt the most sophisticated adversaries with intelligence-led threat hunting powered by AI and elite expertise

Challenges

Adversaries have become faster and more sophisticated, consistently outpacing security teams and leaving organizations exposed to breaches. Being slower than the adversaries poses significant risks to your brand, reputation, and financial standing.

According to the CrowdStrike 2025 Global Threat Report, adversaries are getting faster, moving laterally from initial compromise to other hosts in the victim environment in as fast as 51 seconds. In 79% of detections, threat actors gained initial access using malware-free techniques, showcasing their increased proficiency. Furthermore, adversaries are exploring new attack vectors — CrowdStrike observed a 26% increase in new and unattributed cloud intrusions in 2024 and also saw an uptick in attacks using compromised identities and unmanaged systems.

With adversaries' growing proficiency and speed in executing complex, cross-domain attacks to defeat endpoint, identity, and cloud security solutions, it is imperative for defenders to stay one step ahead to proactively stop breaches.

Key benefits

- Expert threat hunters detect and stop the stealthiest adversaries, including those that exploit legitimate tools to execute their attacks
- These hunters identify novel threats in real time across the entire CrowdStrike customer base and instantly deploy new detections on your behalf
- With industry-first unified visibility from endpoints, expandable to identities, clouds, and third-party data, CrowdStrike threat hunters detect initial access and track lateral movements everywhere across all domains, ensuring no adversary slips through unnoticed.

Solution

Disrupt the most sophisticated adversaries with CrowdStrike Falcon® Adversary OverWatch, powered by the AI-native CrowdStrike Falcon® platform, industry-leading threat intelligence, and unrivaled human expertise, delivering 24/7 protection across all domains, spanning endpoints, identities, cloud workloads, and beyond.

Falcon Adversary OverWatch actively monitors all customer environments to identify novel attacks, misuse of remote access tools, credential compromises, insider threats, and more. These findings are promptly applied to your environment, along with real-time alerts to keep you well-informed about potential threats.

As a managed threat hunting service, Falcon Adversary OverWatch can reduce or completely eliminate the need for in-house threat hunting staff. Organizations can realize up to a 95% reduction in staffing costs. Additionally, the service decreases the time spent researching adversaries and emerging threats by up to 97%, and reduces the effort spent on investigating new alerts by up to 85%.[1]

Key capabilities

24/7 Managed Threat Hunting

Falcon Adversary OverWatch hunts 24/7 for adversaries everywhere across all attack surfaces, leveraging first-party endpoint, identity, and cloud data, along with third-party data from CrowdStrike Falcon® Next-Gen SIEM. CrowdStrike's expert hunters efficiently uncover external threats by monitoring for stolen credentials in the criminal underground, ensuring a robust defense against evolving threats.

- **24/7/365 expert coverage:** When a sophisticated intrusion occurs, time is critical. Adversaries are not restricted by time zones or geography — and your threat hunting team should always be watching.
- **Protection on endpoints:** Falcon Adversary OverWatch threat hunters leverage AI to relentlessly pursue adversaries targeting your endpoints. Fortify your defense against sophisticated attacks with real-time protection and accelerated response.
- **Expand protection across your environment*:** Enhance threat hunting with additional Falcon Adversary OverWatch modules that cover identity, cloud, and third-party Falcon Next-Gen SIEM data — uncovering stealthy adversaries before they can breach your network.

[1] These numbers are projected estimates of average benefits based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on the individual customer's module deployment and environment.

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

World-Class Expertise, Powered by AI

Falcon Adversary OverWatch combines the acumen of security experts with the precision of cutting-edge AI. CrowdStrike's threat hunters are best-in-class at detecting and stopping the stealthiest adversaries, including those that exploit legitimate tools to execute their attacks. Falcon Adversary OverWatch proactively identifies novel threats in real time across the entire CrowdStrike customer base and instantly deploys 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

Falcon Adversary OverWatch delivers industry-leading threat intelligence within the Falcon platform, making other CrowdStrike modules intelligence-aware on Day One. With threat intelligence at your fingertips, you can make quick, confident, and better-informed decisions. This strategic advantage is key to maintaining a strong and responsive security posture in a rapidly changing threat landscape.

- **Adversary profiles:** Access 255+ adversary profiles, including nation-state, eCrime, and hacktivist threat actors. Identify adversaries targeting your organization, and gain insights into intent, capabilities, and predictive behaviors.
- **Advanced malware sandbox:** Safely detonate suspicious files in a secure environment. Get threat verdicts, severity ratings, and 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.

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[2]	Falcon Adversary OverWatch Cloud	Falcon Adversary OverWatch Next-Gen SIEM[3]	Falcon Adversary Intelligence	Falcon Adversary Intelligence Premium	Falcon Adversary Operations Elite[4]
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							✓

[2] Falcon Adversary OverWatch or Falcon Adversary OverWatch Cloud is a prerequisite for Falcon Adversary OverWatch Identity.
[3] Falcon Adversary OverWatch Endpoint or Falcon Adversary OverWatch Cloud, and Falcon Next-Gen SIEM are prerequisites for Falcon Adversary OverWatch Next-Gen SIEM.
[4] 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/