CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Adversary OverWatch

Disrupt the most sophisticated adversaries with intelligence-led threat hunting powered by AI and unrivaled 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 2024 Global Threat Report**, adversaries are getting faster, managing to move laterally from initial compromise to other hosts in the victim environment in less than 3 minutes. In 75% of attacks, threat actors gained initial access using malware-free techniques, showcasing their increased proficiency. Furthermore, adversaries are exploring new attack vectors — CrowdStrike observed a 75% year-over-year increase in cloud intrusions in 2023 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

- Falcon Adversary OverWatch **hunts adversaries targeting your business** across endpoints, identities and cloud environments
- 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**

Solution

Disrupt the most sophisticated adversaries with CrowdStrike Falcon® Adversary OverWatch, powered by AI, threat intelligence, and unrivaled human expertise, to deliver 24/7 protection across endpoints, identities and cloud workloads.

CrowdStrike's expert hunters leverage the world-class intelligence of the unified, AI-native CrowdStrike Falcon® platform. 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

Managed Threat Hunting Across Endpoint, Identity and Cloud

Falcon Adversary OverWatch hunts 24/7 for adversaries targeting your business across endpoints, identities and cloud environments by leveraging the comprehensive visibility of the unified AI-native Falcon platform. CrowdStrike's expert hunters efficiently uncover external threats by monitoring for stolen credentials in the criminal underground, ensuring a robust defense against evolving digital 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.
- **Protection for identities:** Defend against identity threats with Falcon Adversary OverWatch's identity threat hunting and credential monitoring. CrowdStrike's threat hunters proactively contain and neutralize identity-based attacks, minimizing further damage. Monitor criminal forums for stolen credentials and force multifactor authentication (MFA) challenge.
- **Protection for cloud environments (AWS, Azure and GCP):** Leveraging patented cloud-native tooling and tactics, Falcon Adversary OverWatch scours hybrid and multi-cloud environments for threats across cloud containers, workloads and infrastructure.

[1] Based on CrowdStrike Business Value Assessments (BVAs). Expected results and actual outcomes are not guaranteed and may vary for every customer. Calculations are based on aggregated averages from over 100 Business Value Assessment (BVA) and Business Value Realized (BVR) cases conducted with CrowdStrike Enterprise customers and completed by CrowdStrike's Business Value team from 2018 to December 2022. BVAs are a projected ROI analysis based on the value of CrowdStrike compared to the customer's incumbent solution. BVRs are a realized ROI analysis for customers deployed for 6+ months using customer inputs and recorded telemetry.

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. By providing 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 230+ 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 platform 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 →

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.

Request a demo →