CROWDSTRIKE

CrowdStrike Products
Solution Brief

Falcon Adversary OverWatch:

Cross-Domain Threat Hunting

Disrupt attacks across identities, cloud and endpoints with the industry's most complete threat hunting service powered by AI and elite adversary intelligence

Challenges

Cross-domain attacks have become mainstream, with adversaries exploiting valid credentials to breach cloud environments and move laterally to endpoints, thereby increasing the efficiency and success of their operations. Without comprehensive visibility across identity, cloud and endpoint, organizations struggle to detect and respond to these threats effectively.

According to the CrowdStrike 2024 Global Threat Report, cloud environment intrusions surged by 75% from 2022 to 2023. The number of attacks by cloud-conscious adversaries continued to grow in 2023, with 110% more cases than the previous year. Their preference for identity-based techniques in these cloud-focused attacks is evident — 75% of attacks to gain access were malware-free and primarily relied on stolen credentials. Once inside, adversaries can move laterally within the network in just over 2 minutes — the fastest eCrime breakout time observed in 2023.

The fragmentation across domains poses significant challenges, with each requiring different hunting methodologies and tactics. Breaking down these silos requires elite expertise along with integrated telemetry for a unified end-to-end response. Defenders must adopt a robust detection and response strategy with extensive visibility across all domains and rapid response capabilities to effectively stop breaches.

Key benefits

- **Unified visibility:** CrowdStrike Falcon® Adversary OverWatch disrupts advanced attacks through its pioneering 24/7 threat hunting, bolstered by industry-first unified visibility across cloud, identities and endpoints.
- **Cross-domain threat hunting:** Falcon Adversary OverWatch stops breaches everywhere by monitoring for compromised users in cloud attacks and tracking lateral movements between cloud and endpoint for a comprehensive response.
- **Protection from Day One:** With no downtime or additional action from customers, Falcon Adversary OverWatch immediately correlates cross-domain events to detect threats, ensuring no adversary slips through unnoticed.

Solution

CrowdStrike Falcon Adversary OverWatch delivers the world's most complete threat hunting capability to rapidly detect advanced cross-domain threats. By leveraging industry-first unified visibility across cloud environments, identities, and endpoints, CrowdStrike experts effectively hunt threats across domains, 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 world-class threat intelligence, Falcon Adversary OverWatch provides elite 24/7 threat hunting to stop breaches and protect your organization.

Key capabilities

Cross-domain threat hunting across identity, cloud and endpoint

- **Protection for cloud environments:** Stop cloud attacks with the world's most complete cloud threat hunting service within CrowdStrike Falcon® Cloud Security unified cloud detection and response (CDR). Expand visibility into the Microsoft Azure control plane, along with AWS and Google Cloud cloud runtime environments. Monitor for compromised users and lateral movement between cloud and endpoint.
- **Protection for identities:** 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.
- **Protection for endpoints:** Falcon Adversary OverWatch threat hunters relentlessly pursue adversaries targeting your endpoints. Fortify your defense against sophisticated identity attacks with real-time protection and accelerated response.
- **Unrivaled cross-domain telemetry:** Only CrowdStrike offers unparalleled visibility and telemetry across all major domains, enabling effective threat hunting, accelerated response and robust protection against sophisticated adversaries everywhere.

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 230+ 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 cross-domain threat hunting

- **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.

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 →