Falcon Adversary OverWatch:

Cloud Threat Hunting

Disrupt cloud-based attacks with the industry's most complete threat hunting service powered by AI and world-class adversary intelligence

Challenges

Modern attacks make the most of today's vast cloud attack surface — serverless computing vulnerabilities, misconfigured services and container registry dependencies are just a few of the issues ripe for adversary compromise and weaponization. Making matters worse, as adversaries shift their operations to the cloud, security teams struggle to keep pace.

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

Solution

To disrupt the stealthiest and most advanced cloud-based attacks, organizations need the specialized and proactive cloud threat hunting provided by CrowdStrike Falcon® Adversary OverWatch and its managed 24/7 operations.

Falcon Adversary OverWatch delivers the world's most complete cloud threat hunting capability to rapidly detect advanced threats that originate, operate and persist in cloud environments. It leverages the CrowdStrike Falcon® platform's unified visibility across cloud, identity and endpoints to speed detection and response across every stage of a cloud attack, even as threats move laterally from cloud to endpoint.

With expanded visibility into the cloud control planes and runtime environments of critical cloud infrastructures — including Microsoft Azure, AWS and Google Cloud — Falcon Adversary OverWatch provides the industry's most comprehensive cloud threat hunting service to rapidly detect threats and accelerate response.

Key benefits

- **Hunt adversaries in the cloud:** CrowdStrike Falcon Adversary OverWatch relentlessly hunts 24/7 across your critical cloud infrastructure — including Azure, AWS and Google Cloud — to detect the stealthiest and most sophisticated cloud threats.
- **Protect the cloud control plane:** CrowdStrike Falcon® Cloud Security generates granular data and control plane visibility for Microsoft Azure, enabling Falcon Adversary OverWatch hunters to detect unauthorized resource provisioning, suspicious configuration changes and improper access controls.
- **Stop breaches across domains:** With industry-first unified visibility across clouds, identities and endpoints, Falcon Adversary OverWatch monitors for compromised users in cloud attacks and tracks lateral movements between the cloud and endpoints, ensuring no adversary slips through unnoticed.

CrowdStrike leads in cloud detection and response with the industry's most complete cloud-native application protection platform (CNAPP). Bolstered by Falcon Adversary OverWatch's AI-powered 24/7 threat hunting and world-class threat intelligence, you can stop cloud-based breaches and protect your organization.

Key capabilities

Disrupt cloud-based attacks

- **Unrivaled cloud telemetry:** Falcon Cloud Security protects billions of containers every day. Gain real-time visibility into this massive cloud sensor network through Falcon Adversary OverWatch cloud threat hunting and view cloud threat activity as it happens.
- **Limitless operations:** Hunt cloud threats everywhere with full visibility into Kubernetes; workloads in production; host incidents (e.g., cryptominers, suspicious ELF headers); and entire running applications, active processes, and system and network calls across all ingoing and outgoing active ports.
- **Native control plane observability:** Falcon Cloud Security generates granular data and control plane visibility — down to the workload operating system — for Falcon Adversary OverWatch to hunt deep within and across cloud containers, workloads, Kubernetes clusters and other cloud infrastructure.

Gain cross-domain threat hunting coverage across identity, cloud and endpoint

- **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.
- **Protection for cloud environments:** Falcon Adversary OverWatch expert hunters continuously scour hybrid and multi-cloud environments for novel and suspicious cloud threat behaviors, such as control plane and serverless workload vulnerabilities, misconfigurations, application behavior anomalies, container escapes, API privilege escalations, worker node compromise and more.
- **Protection for identities:** Defend against identity threats with Falcon Adversary OverWatch's identity threat hunting and credential monitoring. CrowdStrike 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.

Speed up decision-making with intelligence

- **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:** 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.

Examples of Falcon Adversary OverWatch cloud threat hunting

- **Cloud control plane attack:** An adversary logged in with legitimate credentials and then downloaded PCUnlocker, likely aiming to reset other credentials. They used AD Explorer for domain reconnaissance, identifying Azure hosts to which they then moved laterally. Once in the control plane, they installed Azure AD PowerShell to conduct further Active Directory reconnaissance, facilitate additional lateral movements and execute significant data exfiltration. Falcon Adversary OverWatch quickly detected the threat and provided the customer with strategic countermeasures to mitigate the risk.
- **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 Falcon Cloud Security to support their analysis. They identified the adversary's attempt 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.

Request a demo →

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.

© 2024 CrowdStrike, Inc. All rights reserved.