CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Adversary OverWatch Next-Gen SIEM

Managed threat hunting across the CrowdStrike Falcon® platform and third-party data

Challenges

Adversaries continue to exploit long-standing entry points — like firewalls, routers, VPNs, and email gateways — to bypass defenses. In 2024, 52% of vulnerabilities observed by CrowdStrike were related to initial access, highlighting the persistent risk at common entry points.[1] These attack vectors aren't new — but detecting threats across them remains one of the biggest challenges facing security teams.

Security teams struggle to correlate signals across siloed tools, leading to missed threats, delayed response, and increased dwell time. Despite significant investments in SIEMs and log aggregation, organizations are overwhelmed with data but lack actionable insight. Without proactive threat hunting and unified visibility, adversaries exploit these gaps to gain access, escalate privileges, and move undetected within the network.

Solution

CrowdStrike Falcon® Adversary OverWatch™ Next-Gen SIEM is the industry's first and only managed threat hunting service that delivers proactive, real-time detection of adversary activity across every attack surface. Powered by the AI-native CrowdStrike Falcon® platform, Falcon Adversary OverWatch goes beyond endpoints, correlating first-party endpoint, identity, and cloud telemetry with available third-party data from CrowdStrike Falcon® Next-Gen SIEM for true end-to-end visibility.

Key benefits

- **Hunt threats across all domains:** Falcon Adversary OverWatch delivers 24/7 proactive detection of adversaries everywhere across all attack surfaces — leveraging first-party endpoint, identity, and cloud data, along with available Falcon Next-Gen SIEM third-party data.
- **Detect threats early:** With true end-to-end visibility, Falcon Adversary OverWatch detects adversary movement earlier in the attack, disrupting threats before they breach the network.
- **Maximize the value of Falcon Next-Gen SIEM:** Falcon Adversary OverWatch enriches SIEM data with threat intelligence and expert-driven investigations to cut through the noise and surface high-confidence alerts.

[1] CrowdStrike 2025 Global Threat Report

From network edge devices and identity and access management to SaaS applications, email security, and operating systems, Falcon Adversary OverWatch correlates and analyzes vast amounts of data to uncover stealthy threats where others can't — before a breach occurs.

Unlike other threat hunting solutions that rely on after-the-fact analysis, Falcon Adversary OverWatch continuously hunts for novel and evasive threats to stay ahead of the adversary. CrowdStrike's elite threat hunters operate 24/7, augmenting security teams with high-confidence alerts and rich adversary context, giving security teams the clarity they need to stop real threats without alert fatigue.

Built on industry-leading threat intelligence and telemetry at scale, Falcon Adversary OverWatch delivers the visibility, speed, and expertise organizations need to stay ahead of today's most advanced adversaries.

Key capabilities

Comprehensive Threat Hunting Across the Attack Surface*

- **Extended Visibility Into Blind Spots:** Falcon Adversary OverWatch Next-Gen SIEM extends threat hunting to available third-party telemetry through Falcon Next-Gen SIEM. With support for 275+ pre-built connectors and AI-generated parsers, Falcon Next-Gen SIEM enables Falcon Adversary OverWatch to hunt across virtually any data source — regardless of vendor or format. This empowers Falcon Adversary OverWatch to detect and disrupt adversaries across the full attack surface, including previously siloed systems, enabling earlier detection of activities like initial access, lateral movement, and privilege escalation — before a breach can occur.
- **True End-to-End Hunting:** Falcon Adversary OverWatch breaks down silos by hunting across aggregated first- and third-party data from all domains — from endpoint, identity, and cloud* to network edge devices (firewalls, routers, VPNs), identity and access management (Okta, Entra ID), SaaS applications (Microsoft 365, Google Workspace), email security (Mimecast, Proofpoint), operating systems (Windows, Linux), and more — delivering comprehensive threat detection across all attack surfaces.
- **Power of the Crowd:** Falcon Adversary OverWatch doesn't just hunt across your data — it hunts across the global CrowdStrike customer base. When emerging threats are identified anywhere, Falcon Adversary OverWatch proactively checks your environment for similar activity and alerts your team. Falcon Adversary OverWatch detections strengthen protection for all CrowdStrike customers — delivering faster, smarter threat detection through true collective defense.

"Getting OverWatch is one of the best investments we've made. It's a 24/7 team leveraging AI to monitor our environment, even while we sleep. Many companies struggle to achieve this level of security on their own, but with OverWatch, we're getting the best of the best."

– David Levin
Chief Information Security Officer, American Express Global Travel

*For threat hunting across the attack surface, please see the Products and Services chart on p. 4.

Expert-Led, AI-Driven Threat Hunting

- **Turnkey Threat Hunting:** Falcon Adversary OverWatch delivers fully managed, 24/7 threat hunting with zero effort required from security teams. If you have an in-house threat hunting team, Falcon Adversary OverWatch acts as a force multiplier, augmenting your capabilities with deep expertise and around-the-clock coverage. Hunting across the most targeted data sources, Falcon Adversary OverWatch exposes novel threats and emerging adversary tradecraft, eliminating the need to manage detection content, write rules, or triage noisy alerts.
- **AI-Driven Threat Hunting at Scale:** Built on the AI-native Falcon platform, Falcon Adversary OverWatch regularly processes up to 4.7 trillion events per day across first- and third-party data. This unmatched scale enables faster threat detection, earlier intervention, and comprehensive protection across complex IT environments.
- **Enriched with Threat Intelligence:** With Falcon Adversary OverWatch, your Falcon Next-Gen SIEM just got better. Falcon Adversary OverWatch enriches SIEM events with industry-leading threat intelligence and behavioral analytics, transforming raw logs into meaningful, actionable detections.

Faster Detection, Lower Risk

- **Early Detection of Adversary Movement:** By unifying and analyzing vast amounts of data in real time, Falcon Adversary OverWatch detects threats earlier in the attack, before adversaries can escalate privileges or exfiltrate data, reducing dwell time and preventing breaches.
- **Real-Time Adversary Tracking:** Falcon Adversary OverWatch continuously tracks adversaries across all domains, detecting stealthy movement and surfacing patterns that siloed tools miss.
- **Clarity Without Alert Fatigue:** Expert-driven investigations and behavioral analyses cut through the noise, ensuring security teams receive only high-confidence alerts. Falcon Adversary OverWatch acts as a force multiplier, filtering out false positives and enabling teams to focus on real threats that matter.

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/