CROWDSTRIKE

CrowdStrike Products
Solution Brief

Falcon Adversary Intelligence:

Digital Risk Protection

Expose threats to your brand, employees, and sensitive data across the open, deep, and dark web

Falcon Adversary Intelligence Recon

CrowdStrike Falcon® Adversary Intelligence, an industry-leading solution for uncovering adversary activity, equips organizations to detect and disrupt sophisticated threats. This solution includes Falcon Adversary Intelligence Recon (aka "Recon"), a digital risk protection feature that identifies critical threats across the open, deep, and dark web to protect organizations' brands, employees, and sensitive data.

Recon monitors millions of restricted webpages, criminal forums, and encrypted messaging platforms — the hidden corners of the internet where adversaries operate and underground digital economies thrive. By enabling real-time investigations, Recon empowers security teams to proactively identify fraud, data breaches, phishing campaigns, and other online threats targeting their organization.

Key capabilities

Collect

Recon provides comprehensive visibility into difficult-to-access channels across the open, deep, and dark web. By proactively collecting raw intelligence about fraudulent activity, stolen data, emerging tools, and exploits, Recon enables organizations to stay ahead of evolving external threats.

- **Collect raw intelligence at scale:** Automatically monitor millions of hidden webpages and thousands of restricted forums, marketplaces, paste sites, IRC channels, rogue apps, phishing domains, and open and closed messaging applications like Telegram, QQ, and more.
- **Perform real-time, covert investigations:** With access to real-time raw intelligence, you can disrupt adversaries and limit their opportunities to attack. Gain covert, undetectable access to restricted sites and preserve historical data, ensuring adversaries can't erase their tracks by altering or deleting posts.

Key benefits

- Provides extensive coverage of the open, deep, dark web
- Automates the data extraction from millions of restricted and underground environments
- Reduces investigation time and improves efficiency and response
- Monitors in real time with rules tailored to your organization
- Delivers time-to-value faster than ever — deploys and becomes operational in minutes
- Reduces exposure to threats with automated takedowns and blocklist submissions

- **Track adversarial behavior:** Analyze evolving tradecraft, tools, and attack trends to anticipate and mitigate external threats targeting your organization.

Monitor and protect your digital footprint

- **Brand protection:** Identify adversaries associated with fraudulent interactions with your brand, including fake social media accounts, domains, and mobile apps.
- **Data leak discovery:** Detect compromised credentials and stolen sensitive data — including IP and credit card information — from leaks on underground marketplaces and forums.
- **Supply chain monitoring:** Identify threats to your suppliers by exposing chatter, phishing campaigns, counterfeit websites, and more.
- **Executive protection:** Monitor threats, impersonations, and phishing attempts against VIPs and executives.
- **App store monitoring:** Monitor mobile app stores to detect brand impersonations and fraudulent apps, with detailed insights on app authors, domains, creation dates, and more.
- **Automated takedowns and blocklist submissions:** Proactively reduce exposure to threats by reporting malicious domains and submitting blocklists. CrowdStrike will trigger automated takedowns[1] with registrars, hosting providers, and SSL certificate issuers, removing malicious content such as phishing sites and fake profiles. Blocklist submissions enable CrowdStrike to engage third-party providers — including email services, web browsers, registrars, and industry working groups — to rapidly restrict access to harmful domains.

Investigate

Gain real-time visibility into external threats and accelerate investigations into fraudulent activity targeting your organization. Recon eliminates risky guesswork and enriches traditional incident response by providing broader context to improve the depth and breadth of investigative reporting and analysis.

- **Identify targeted threats:** Continuously monitor underground environments for external threats to the organization without the need to create complex queries. Easy-to-use wizards that include predefined search criteria — such as brand names, executives, domains, vulnerabilities, and email addresses — streamline threat detection. Create and save your own monitoring rules to proactively sift through raw intelligence or share them with your team.
- **Expose the adversary:** Investigate results displayed in customizable dashboards and easy-to-read cards. Access the original threat actor posts enriched with additional context about the actor and the site. View results in their original language, and they can be translated from 18 other languages using augmented translation with hacker slang dictionaries.
- **Enrich investigations:** Gain a complete understanding of the threat. Universal Search enables users to automatically correlate results with additional context provided by other licensed CrowdStrike Falcon® modules. Maximize efficiency and effectiveness of response by revealing the relationships between digital threats and endpoint detections, hosts, threat intelligence reports, vulnerabilities, and much more.

[1] *Takedowns are subject to the policies of registrars and other third parties and may not be guaranteed in all cases.*

Notify

Optimize the investigation and response workflow with real-time notifications when potential threats are identified. Ensure that the users responsible for triage and response have the details they need at their fingertips.

- **Prioritize alerts:** Set the priority of the alert based on the criticality of the external threat. Immediately pivot from the notification to the details of the alert.
- **Gain complete administrative control:** Customize how team members are notified and how often they receive alerts. They can be alerted immediately or on a schedule such as daily or weekly. Toggle notifications on or off without affecting the underlying monitoring rule.
- **Inform the right team:** Go beyond cybersecurity — digital threats affect an organization's brand, reputation, and employee safety. Alert your departments outside of security, such as marketing, legal, human resources, and fraud.

Offerings

All Falcon Adversary Intelligence Recon capabilities are included in Falcon Adversary Intelligence and Falcon Adversary Intelligence Premium modules.

Falcon Adversary Intelligence Recon+ is a fully managed service where CrowdStrike experts handle digital risk monitoring and mitigation with Recon on your behalf.

CrowdStrike Threat Intelligence and Hunting Products and Services

Feature Categories	Key Features	Falcon Adversary OverWatch	Falcon Adversary OverWatch Identity[2]	Falcon Adversary OverWatch	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/