CROWDSTRIKE

CrowdStrike Products

Data Sheet

Falcon Adversary Intelligence Premium

Reduce the risk, cost, and impact of every threat

Challenges

Adversaries are evolving faster than ever, growing more sophisticated and consistently outpacing organizations to breach defenses. Even as organizations harden their environments with advanced capabilities like endpoint detection and response (EDR), identity protection, and cloud security solutions, attackers adapt. They exploit new entry points and employ stealthy evasion techniques that attempt to bypass traditional defenses and complicate detection and response. When adversaries move faster than your ability to respond, the consequences are significant — putting your brand, reputation, and financial standing at serious risk.

Staying ahead requires more than reactive workflows and hardened defenses — it demands the ability to understand adversary behavior, assess business risk, and adapt defenses in real time. For many organizations, this means establishing an advanced threat intelligence practice: a team equipped to track adversaries, monitor threats to the business, and guide proactive defense. But developing that capability is costly, requiring specialized talent, tooling, and continuous access to high-fidelity intelligence. As a result, many teams are left with irrelevant indicators with limited context, siloed tools, and outdated countermeasures — creating exploitable gaps and slowing down response time.

Solution

CrowdStrike Falcon® Adversary Intelligence Premium delivers the analysis, insight, and tools of a world-class threat intelligence team, enhancing your existing team while reducing cost and complexity.

Gain in-depth visibility into the latest eCrime, nation-state, and hacktivist tradecraft by surfacing the tactics, techniques, and infrastructure most relevant to your business. With this intelligence embedded directly into SOC workflows, teams can shape proactive defenses, improve detection, and respond with greater speed and confidence.

Key benefits

- Augment or replace the need for in-house threat research and adversary tracking
- Reduce the time and effort to triage, investigate, and threat hunt
- Quickly analyze threats with the Malware Analysis Agent, using AI to connect malware samples, intelligence context, and response
- Gain external visibility with real-time monitoring across the open, deep, and dark web
- Proactively adapt security controls as adversary tactics evolve, improving protection and team productivity
- Includes all capabilities of CrowdStrike Falcon® Adversary Intelligence

Falcon Adversary Intelligence Premium includes CrowdStrike Threat AI, the industry's first Agentic Threat Intelligence suite of AI-powered agents purposely built to accelerate and amplify analyst workflows. These agents reason across threat data, hunt proactively, and act decisively across the kill chain. Threat AI combines LLM-driven reasoning with operational integrations, giving security teams the speed and clarity they need to stay ahead of sophisticated adversaries.

Threat intelligence teams can cut research time by up to 97%, detection engineers can accelerate rule development by up to 65%, and organizations report up to 80% overall improvement in security posture.[1] Falcon Adversary Intelligence Premium transforms how security teams operationalize intelligence, improving protection, increasing efficiency, and keeping adversaries at a disadvantage.

Key capabilities

Accelerate Detection and Response Across Your SOC

Falcon Adversary Intelligence Premium includes all of the core capabilities of Falcon Adversary Intelligence, delivering personalized threat models, automation, and external visibility that accelerate SOC workflows. These foundational capabilities support triage, detection, and response. Falcon Adversary Intelligence Premium goes further, extending the value of threat intelligence across advanced use cases, empowering threat intel teams, hunters, and detection engineers with deeper insights and broader impact.

Falcon Adversary Intelligence capabilities enable you to:

- **Expose the threats that matter most** through customized threat modeling, indicators of compromise (IOCs), and attack surface visibility tailored to your environment
- **Streamline your SOC** with a built-in advanced malware sandbox and real-time IOC feeds for faster detection and response
- **Protect your brand** with continuous monitoring of the open, deep, and dark web, including automated takedowns and fraud detection
- **Integrate seamlessly across your security stack** with prebuilt playbooks and easy-to-use APIs to simplify response workflows and extend intelligence into your existing tools

Intelligence Reporting and Insights

CrowdStrike tracks 265+ adversaries and produces thousands of intelligence reports annually, delivering timely insights across eCrime, nation-state, and hacktivist threats. Reports are prioritized based on your organization's environment and risk profile, ensuring the most relevant and urgent threats are surfaced first.

- **Real-time threat emails:** Receive instant updates on emerging threats, breaches, and adversary activity, along with actionable recommendations
- **In-depth technical analysis:** Gain a deep understanding of adversary tools, techniques, and infrastructure to support effective hunting, patching, and detection efforts
- **Strategic insights for leadership:** Leverage industry- and region-specific reporting to inform risk decisions, engage stakeholders, and align security investments with business priorities
- **CrowdStrike Threat Intelligence Browser Extension:** Access CrowdStrike's industry-leading intelligence everywhere you work, with instant insights during external research to provide immediate context and speed investigations without disrupting existing workflows

Every team benefits

- **SOC Teams:** Reduce alert fatigue and accelerate incident response
- **Intel Analysts:** Eliminate manual research with high-fidelity threat reporting
- **Detection Engineers:** Deploy trusted detection content without starting from scratch
- **Hunting Teams:** Detect advanced threats faster with curated hunting workflows
- **Security Leadership:** Strengthen posture, prove ROI, and align to business risk

[1] These numbers reflect the median inputs provided by customers during pre- and post-sale motions that compare the value of CrowdStrike with incumbent solutions and are not guaranteed. They are intended to demonstrate potential value compared to incumbent solutions and do not represent promised outcomes. Actual value realized will depend on individual customer module deployment and environment.

Prebuilt Detection and Hunting Libraries

Empower detection engineering and hunting teams with ready-to-use content, eliminating the guesswork and effort of building detections from scratch.

- **Detection rule libraries:** Deploy pre-tested YARA and Snort rules built by CrowdStrike experts to detect malware, exploits, and adversary behavior
- **Malware Analysis Agent:** This agent within CrowdStrike's Threat AI suite of agents automates one of the most complex analyst workflows — reversing, classifying, and comparing malware — and recommends a response in seconds, giving defenders the speed and context to stay ahead of today's AI-powered adversaries
- **Hunt Agent:** Another agent within CrowdStrike's Threat AI, Hunt Agent is the industry's first AI agent that brings expert-level threat hunting capabilities based on CrowdStrike's industry-leading threat intelligence. Experience continuous, intelligence-driven hunting with clear guidance and next steps, enabling faster, more decisive action against evolving adversaries
- **Intel-led hunting leads:** Save time with out-of-the-box hunting leads that highlight high-priority adversary tactics, techniques, and procedures (TTPs) and attack paths

Streamlined Security Engineering Processes

Today's fast-evolving threat landscape requires security teams to continuously adjust — at scale — their security controls ahead of the latest threats. Move from intelligence to response faster with workflows that integrate seamlessly into your tech stack.

- **Centralized detection processes:** Accelerate the lifecycle — from research to deployment — with tools that support designing, testing, and scaling detection logic
- **Flexible integration:** Use APIs and prebuilt workflows to push countermeasures into SIEMs, firewalls, EDRs, and Intrusion Detection System solutions across your environment

Attend a hands-on workshop

Request a demo

CrowdStrike Threat Intelligence Products and Services

Feature Categories	Key Features	Falcon Adversary Intelligence	Falcon Adversary Intelligence Premium	Falcon Counter Adversary Operations Elite[2]
Threat Intelligence	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 (Up to 50)			✓
Digital Risk Protection	Dark Web Monitoring	✓	✓	
	Brand and Domain Monitoring	✓	✓	
	Credential Monitoring	✓	✓	
	Dark Web Activity Reports	✓	✓	
Automation and Tools	Malware Sandbox	✓	✓	
	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 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/