CROWDSTRIKE

CrowdStrike Services
Data Sheet

Falcon Complete

Stop breaches with the leader in managed detection and response (MDR), uniting AI and human precision

The new reality of AI-accelerated attacks

In today's threat landscape, speed of detection and response is no longer just an advantage, it is a requirement. In 2025, adversaries leveraging AI increased their activity by 89% year-over-year.[1] AI-driven capabilities speed up phishing campaigns, scale social engineering tactics, and automate reconnaissance. As a result, threat actors can accelerate their attacks and achieve lateral movement in just 27 seconds — the fastest eCrime breakout time CrowdStrike observed in 2025.

To stay ahead of emerging threats, organizations must operate at maximum efficiency and rely on the right combination of AI and machine-speed execution with expert judgment to defend faster and smarter. However, building and operating a modern agentic SOC is a complex effort requiring deep expertise, dedicated resources, and rigorous governance that many organizations cannot maintain on their own.

Stopping breaches through agentic MDR

CrowdStrike Falcon® Complete delivers agentic MDR to stop breaches at machine speed through adaptive AI-driven execution and expert-led operations. Built on the AI-native CrowdStrike Falcon® platform, the service unifies endpoint, identity, cloud, and third-party telemetry to detect, investigate, contain, and remediate threats in minutes, not hours.

Key service capabilities

Agentic MDR

» **Defenses that evolve with the threat landscape:** Falcon Complete delivers agentic MDR by uniting adaptive AI with human oversight. Falcon Complete customers benefit from these agentic capabilities and expert-led outcomes as a core part of the service. CrowdStrike's AI agents use real-time, cross-domain telemetry to apply context-aware reasoning to evolving threats. These agents learn directly from real-world adversary behavior observed across the Falcon platform and extended telemetry, ensuring investigations stay current with the latest attack patterns. By learning from experienced defenders' decisions, these agents achieve >98% triage accuracy.[2]

Key benefits

- Stop breaches at machine speed with adaptive AI and elite expertise
- Maintain human accountability by keeping experts in control of complex decisions
- Achieve full-cycle remediation with decisive action taken on your behalf
- Eliminate blind spots with unified visibility across domains
- Reduce operational burden and increase efficiency with automation and AI-driven investigations

[1] CrowdStrike 2026 Global Threat Report

[2] Accuracy rating is a measure of Charlotte AI triage decisions that match the expert decisions from the CrowdStrike Falcon Complete team.

- **Autonomous response at scale:** Falcon Complete replaces manual intervention for known threats with deterministic automation, ensuring common attacks are neutralized with expert-approved precision. By utilizing playbooks through CrowdStrike Falcon® Fusion SOAR for high-volume tasks — such as isolating compromised hosts or terminating malicious processes — the service executes containment at machine speed. This transition to autonomous execution ensures that response is both immediate and predictable, allowing your security operations to scale without sacrificing human oversight or operational control.
- **Expert supervision:** The defining characteristic of agentic MDR is that human authority remains central to every outcome. While CrowdStrike® Charlotte AI™ and proprietary agents handle routine tasks to reduce investigation time by over 15 minutes,[3] elite analysts focus their judgment on complex, high-stakes adversary behavior. Experts orchestrate how automation is applied, validated, and refined rather than providing simple after-the-fact oversight.

World-Class Expertise

- **Force multiplier for your team:** Fortify your defense with 24/7 protection from elite CrowdStrike Certified Falcon Responder (CCFR) and CrowdStrike Certified Falcon Administrator (CCFA) experts who have an average of 5+ years experience and deliver agentic operations on your behalf. CrowdStrike's team of analysts is trained to investigate, contain, and remediate end-to-end, eliminating delays and providing the decisive action required to stop breaches.
- **Around-the-clock protection:** Adversaries never sleep, and neither does CrowdStrike. With a global footprint and a follow-the-sun model, Falcon Complete delivers seamless real-time protection and accelerated response 24/7 to eliminate advanced cross-domain threats no matter when or where they occur.
- **All-domain threat hunting:** Stop the most sophisticated adversaries with CrowdStrike Falcon® Adversary OverWatch™, which delivers 24/7 hunting in every domain, across endpoints, identities, cloud workloads, and third-party CrowdStrike Falcon® Next-Gen SIEM data using advanced AI, industry-leading threat intelligence, and unrivaled human expertise.
- **A single view into MDR operations:** Get immediate access to critical MDR actions, expert guidance, and essential resources in the Falcon Complete Hub. CrowdStrike experts deliver immediate threat guidance, prioritize alerts, and provide actionable intelligence directly to your unified interface. See critical security communications from the analyst team instantly, and ensure expert-driven insights reach the right stakeholders without delay.

Full-Cycle Remediation

- **Fastest containment speeds in the industry:** Falcon Complete delivers a rapid 1-minute median time to contain (MTTC),[4] setting the benchmark for speed against today's adversaries.
- **Delivering results, not homework:** Achieve rapid response with full-cycle remediation delivered by the Falcon Complete team. Expert analysts act immediately to contain threats, kill malicious processes, quarantine files, and remove persistence, preventing downtime and costly reimaging.

[3] Time savings represents the amount of time and manual effort an analyst would have spent triaging and investigating detections, and can now use that time for other skilled work while Charlotte AI performs analysis.

[4] Falcon Complete measures this as median time to contain (MTTC). MTTC is the measured duration between the initial detection of a security threat and the successful implementation of containment controls that effectively contains a threat and prevents further malicious activity on an endpoint. This metric reflects full-cycle response, spanning automation, platform enforcement, and expert-led operations through to complete containment. Actual results may vary based on incident complexity or other environment variables such as offline hosts.

Unified Cross-Domain Visibility

Falcon Complete unifies managed protection from the AI-native Falcon platform across the attack surface:

- **Secure endpoints:** CrowdStrike Falcon® Insight XDR (endpoint security and extended detection and response), CrowdStrike Falcon® Prevent (next-gen antivirus), and CrowdStrike Falcon® Discover (IT hygiene) stop advanced attacks
- **Stop identity-based attacks:** CrowdStrike Falcon® Identity Threat Protection delivers real-time identity threat prevention and IT policy enforcement.
- **Secure cloud workloads:** CrowdStrike Falcon® Cloud Security delivers comprehensive managed protection for cloud workloads and containers.
- **Extend protection to critical data sources:** Falcon Next-Gen SIEM accelerates threat investigation and eradicates threats earlier in the kill chain.

  Third-party domains include:

  - Email security
  - Cloud user workspace
  - Network perimeter
  - Infrastructure
  - Identity / single sign-on (SSO)
  - And more

Falcon Complete warranty

The CrowdStrike Falcon Complete Warranty provides built-in financial support for ransomware-related expenses up to $2 million USD for Falcon Complete customers — demonstrating CrowdStrike's confidence in its expert-led defense and providing added assurance if ransomware strikes. See FAQs for terms and exclusions.

Schedule a demo

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 at https://www.crowdstrike.com/
Start a free trial today: https://www.crowdstrike.com/free-trial-guide/