CROWDSTRIKE

CrowdStrike Services
Data Sheet

Falcon Complete for Service Providers

Grow your business with the industry-leading MDR service

Challenges

Building and maintaining effective in-house managed detection and response (MDR) operations has become increasingly challenging for service providers. While customer demand for advanced security services continues to grow, providers face significant obstacles in delivering competitive MDR solutions.

The challenge is further intensified by AI-empowered adversaries that are moving faster, automating reconnaissance and exploitation, and scaling sophisticated campaigns beyond the capacity of traditional SOC models. In 2025, attacks by threat actors leveraging AI increased 89% year-over-year.[1]

Establishing 24/7 security operations requires substantial investment in infrastructure and specialized talent, while the rapidly evolving threat landscape demands continuous training and expertise that is difficult to recruit and retain. Building comprehensive in-house MDR capabilities from scratch can take months or years — and in the meantime, a managed service provider misses immediate market opportunities while competitors gain ground.

Solution

CrowdStrike Falcon® Complete for Service Providers empowers managed service providers (MSPs) and managed security service providers (MSSPs) to rapidly deliver and scale high-margin MDR offerings — without the cost, complexity, or delays of building in-house.

Built on the industry-leading CrowdStrike Falcon® Complete service, Falcon Complete for Service Providers enables partners to deliver 24/7 protection, backed by demonstrated industry-leading speed and efficacy, including 1-minute median time to contain (MTTC).[2] CrowdStrike's agentic MDR delivers an outcome-owned, expert-led service uniting automation, adaptive AI, and human oversight to stop breaches at machine speed.

Partners maintain full ownership of customer relationships, choose between white-labeling or leveraging CrowdStrike's trusted brand, and drive real business outcomes — accelerating growth while reducing client risk.

Key benefits

- Rapid time-to-market with agentic MDR capabilities built on CrowdStrike's proven technology and expertise
- White-labeled or co-branded with CrowdStrike, and bundled with your existing services to create new revenue streams
- 1-minute MTTC and 2.7M+ detections remediated monthly
- Revenue scaled with minimal operational overhead

[1] CrowdStrike 2026 Global Threat Report

[2] 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.

Key service capabilities

Around-the-Clock Protection

With a global footprint and a follow-the-sun model, Falcon Complete delivers 24/7 protection with industry-leading speed and efficacy. CrowdStrike's flat fire-team structure eliminates handoff delays, enabling specialized experts — from threat hunters to security advisors — to deliver rapid, scalable response. This comprehensive visibility and rapid response helps ensure threats are identified and eliminated before they become breaches, providing your customers with proven, measurable security outcomes.

World-Class Expertise

Falcon Complete acts as your trusted security partner, combining elite detection and response, proactive threat hunting, agentic workflows, and integrated world-class threat intelligence from the CrowdStrike Falcon® platform to stay ahead of evolving threats. While CrowdStrike® Charlotte AI™ and proprietary AI agents handle routine tasks to reduce investigation time by over 15 minutes,[3] CrowdStrike's elite analysts focus their judgment on complex, high-stakes adversary behavior. With over 2.7 million detections remediated monthly,[4] CrowdStrike's expert team works seamlessly behind the scenes to deliver enterprise-grade protection at scale while you maintain full control of customer relationships.

- **Experts in the Falcon platform:** The Falcon Complete team holds CrowdStrike Certified Falcon Responder (CCFR) and CrowdStrike Certified Falcon Administrator (CCFA) certifications with an average of 5+ years experience.
- **Elite threat hunting and intelligence:** Threat hunters from CrowdStrike Falcon® Adversary OverWatch™, combined with AI-driven intelligence, proactively identify and stop sophisticated threats before they become breaches.
- **AI trained by elite defenders:** CrowdStrike's agentic capabilities are trained directly by real-world decisions from the Falcon Complete team, achieving >98% triage accuracy.[5]

Unified Cross-Domain Visibility

Falcon Complete for Service Providers delivers unified protection across your customers' entire attack surface through a single, powerful agentic MDR service — securing endpoints, cloud workloads, and identities while providing next-gen SIEM and SOAR capabilities to stop threats across the complete kill chain.

The Falcon Complete service includes:

24/7 expertise:

- Falcon Complete analyst team of global security experts
- Falcon Adversary OverWatch threat hunting team

Managed Falcon modules:

- CrowdStrike Falcon® Prevent next-gen antivirus
- CrowdStrike Falcon® Insight XDR endpoint security and extended detection and response
- CrowdStrike Falcon® Discover IT hygiene
- Add-ons:
    - CrowdStrike Falcon® Identity Threat Protection
    - CrowdStrike Falcon® Next-Gen SIEM
    - CrowdStrike Falcon® Cloud Security

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

[4] Falcon Complete team operational metric

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

Built on Transparency and Visibility

Get frictionless, transparent, and secure communication. Service providers can communicate with the Falcon Complete team at their convenience and via the Falcon Message Center, email, and API.

Falcon Complete Hub is your single view into MDR operations, delivering immediate access to critical MDR actions, expert guidance, and essential resources. See important security alerts and announcements immediately, and help prevent critical security information from slipping through the cracks.

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

Full-Cycle Remediation

Falcon Complete analysts can remotely access affected systems (via native Falcon capabilities), surgically remove the threat — end processes, stop services, remove persistent mechanisms, network-contain hosts, and clear any other latent artifacts — and restore systems to an operational state, relieving teams of the burden of reimaging systems, all without disrupting end users.

Once an incident is remediated, service providers receive a detailed report, showing all actions the Falcon Complete team took and including supporting data that can be shared with customers for post-mortem analysis.

A trusted partnership delivering seamless security

Falcon Complete for Service Providers — Endpoint

Falcon Complete leverages key Falcon platform modules including Falcon Insight XDR, Falcon Prevent, and Falcon Discover to identify security gaps and stop threats targeting your environment.

Roles and Responsibilities		CrowdStrike	Partner
Onboarding and Planning	Onboard customers		✓
	Manage the customer relationship		✓
	Install sensors		✓
	Remove conflicting services		✓
	Create and set up customer IDs	✓	✓
	Create and update policies	✓	
	Activate Falcon Complete monitoring	✓	
Steady State	Respond to Falcon Complete escalations and communications		✓
	Provide required reporting		✓
	Conduct sensor troubleshooting		✓
	Manage additional Falcon modules (not managed by Falcon Complete)		✓
	Communicate with end customers		✓
	Respond to Falcon Adversary OverWatch alerts	✓	
	Respond to Falcon platform detections	✓	
	Manage allowlists	✓	

Falcon Complete for Service Providers — Identity Threat Protection

Falcon Complete stops identity-based attacks in their tracks with Falcon Identity Threat Protection, delivering real-time identity threat prevention and IT policy enforcement.

Roles and Responsibilities		CrowdStrike	Partner
Onboarding and Planning	Create and apply ATI policy		✓
	Configure MFA Connector and IDaaS Connector(s)		✓
	Implement, tune, and configure policy rules		✓
Monitoring and Remediation	Triage supported identity-based detections	✓	
	Respond to supported identity-based detections	✓	
	Take action with countermeasures as defined by Falcon Complete	✓	
	Take recommended recovery actions per escalation/remediation ticket		✓

Falcon Complete for Service Providers — Next-Gen SIEM

With unified threat data from Falcon Next-Gen SIEM, Falcon Complete expands the scope of visibility and protection beyond native Falcon telemetry to accelerate threat investigation and eradicate threats earlier in the kill chain.

Roles and Responsibilities		CrowdStrike	Partner
Onboarding and Initial Deployment	Deliver operating model/SoP	✓	
	Provide requirements and next steps for Falcon Complete Next-Gen SIEM detection and response	✓	
	Implement and configure data connectors		✓
	Validate data ingestion and health		✓
	Notify Falcon Complete of preferred security postures		✓
	Troubleshoot product issues		✓
	Notify Falcon Complete of additional data connectors		✓
Monitoring	Provide 24/7/365 coverage	✓	
	Triage Falcon Next-Gen SIEM incidents and detections created by a Falcon Complete published correlation rule to determine nature and positivity	✓	
Response	Respond to Falcon Next-Gen SIEM incidents and detections created by a Falcon Complete published correlation rule based on pre-approved countermeasures	✓	
	Respond to Falcon Complete escalation tickets and calls		✓
Remediation	Apply countermeasures	✓	
	Apply recommended recovery action(s) per escalation or remediation ticket		✓
Content	Create detection content for third-party sources ingested into Falcon Next-Gen SIEM for the purposes of detecting malicious threat actor activity	✓	
	Create custom detection content tailored to organization-specific use cases and/or dashboards		✓
Maintenance	Maintain configuration and health of data connectors and/or log sources		✓

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