

# Falcon Complete for Service Providers



Empowered security services for seamless and powerful protection

## Challenges

Securing an organization is a monumental task, especially in today's sophisticated threat environment. Businesses of all sizes recognize the need for comprehensive detection and response across critical attack surfaces and are looking for partners to manage their deployment and provide the protection they need.

With the fastest eCrime breakout time observed at **just 7 minutes**, every second counts. This acceleration in pace and adversary sophistication increases the challenge for service providers to keep up with the latest tactics, techniques and procedures (TTPs) and secure their customer environments.

To maintain a proactive stance and deliver business resiliency, service providers must enhance their security capabilities with powerful technology and managed security services to streamline operations, improve visibility and most importantly, stop breaches.

## Solution

Combat threats at scale and improve cyber protection with CrowdStrike Falcon® Complete managed detection and response (MDR). Falcon Complete for Service Providers enables service providers to build customized services on top of CrowdStrike's industry-leading MDR service to provide their customers with 24/7 comprehensive and specialized threat detection, threat hunting, integrated intelligence and full-cycle response across endpoints, identities and cloud workloads.

With Falcon Complete's team of elite experts actively monitoring the CrowdStrike Falcon® platform and capable of remotely remediating incidents in minutes on average, service providers can grow revenue while introducing new value to customers by delivering elite protection as part of a seamless, single-vendor service.

## Key benefits

24/7 expert protection and focused security expertise by MDR leader and pioneer

Advanced protection with proactive threat hunting, native threat intelligence and surgical remediation

Rapid response actions against sophisticated attacks

Frictionless single-vendor coverage for end-customer businesses of all sizes

## Key service capabilities

### Always-on protection

The 24/7 protection and visibility provided by Falcon Complete enables service providers to gain a comprehensive view of threats across the environments they manage. With detections triaged, investigated and resolved quickly, our team helps ensure threats to your customers are dealt with long before they become a problem.

### Layers of expertise

Falcon Complete acts as a trusted partner, with capabilities spanning detection and response, threat hunting and integrated threat intelligence to gain the insights needed to proactively address risks in customer environments. While the environment operates at its most optimal level, Falcon Complete works behind the scenes to secure it.

- **Experts in the CrowdStrike Falcon platform:** The Falcon Complete team holds CrowdStrike Certified Falcon Responder (CCFR) and CrowdStrike Certified Falcon Administrator (CCFA) certifications.
- **Elite threat hunting and intelligence:** The CrowdStrike® Falcon OverWatch™ threat hunting team and CrowdStrike's AI-driven intelligence built into the Falcon platform deliver integrated insights to strengthen defenses and disrupt attacks before they can turn into breaches.

### Comprehensive protection

Falcon Complete for Service Providers delivers comprehensive MDR protection for endpoints plus advanced protection of cloud workloads, containers, and Kubernetes, and frictionless real-time identity threat prevention.

The Falcon Complete MDR service includes:

#### 24/7 expertise:

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

#### Managed Falcon platform modules:

- CrowdStrike Falcon® Prevent next-generation antivirus
- CrowdStrike Falcon® Insight XDR detection and response for endpoint and beyond
- CrowdStrike Falcon® Discover IT hygiene
  - Add-ons:
    - CrowdStrike Falcon® Identity Threat Protection
    - CrowdStrike Falcon® Cloud Security — Cloud Workload Protection

### Transparent secure communication

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 or API.

### Surgical 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.

## Built for the way you do business

**Protection:** Deliver powerful 24/7 monitoring, detection and response capabilities with human threat hunting for proactive and secure protection through the CrowdStrike Falcon platform

**Partnership:** Co-brand with Falcon Complete to offer powerful and specialized managed security services

**Profit:** Own the relationship with your customers and maximize profits through license and customer pricing control while lowering your own costs

# A trusted partnership delivering seamless security

## Falcon Complete for Service Providers — MDR

Elite managed protection across endpoints, cloud workloads and identities stops attacks in real time.

| Roles and Responsibilities  | CrowdStrike | Partner |
|---|-------------|---------|
| <b>Onboarding and Planning</b>                                    |             |         |
| 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                               | ✓           |         |
| <b>Monitoring and Remediation</b>                                 |             |         |
| 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 OverWatch alerts                                | ✓           |         |
| Respond to Falcon platform detections                             | ✓           |         |
| Manage allowlists   | ✓           |         |

## Falcon Complete for Service Providers — Identity Threat Protection

Falcon Identity Threat Protection available as an add-on augments the core CrowdStrike Falcon Complete managed endpoint protection offering, delivering industry leading security for identities and identity stores.

| Roles and Responsibilities  | CrowdStrike | Partner |
|---|-------------|---------|
| <b>Onboarding and Planning</b>                                      |             |         |
| Create and apply ATI policy   |             | ✓       |
| Configure MFA Connector and IDaaS Connector(s)                      |             | ✓       |
| Implement, tune and configure policy rules                          |             | ✓       |
| <b>Monitoring and Remediation</b>                                   |             |         |
| 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 |             | ✓       |

## 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.**

Follow us: [Blog](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

© 2023 CrowdStrike, Inc. All rights reserved.



**Schedule a Demo**