CROWDSTRIKE

FALCON COMPLETE: PROVEN, PROFESSIONAL MANAGED DETECTION AND RESPONSE

DELIVERING OPTIMIZED PROTECTION FOR ALL OF YOUR SYSTEMS, ALL OF THE TIME

INTRODUCTION

The shortage of cybersecurity resources and expertise can lead organizations to struggle with taking full advantage of the security technology they acquire, leaving them unnecessarily exposed and vulnerable. This can result in damage and remediation efforts that could have been prevented if the security technologies had been configured properly and kept up to date, or if the security alerts that preceded an incident had been noticed, investigated and remediated promptly.

CrowdStrike® Falcon Complete™ is a managed detection and response (MDR) service that solves these challenges for CrowdStrike Falcon® customers by augmenting the effectiveness of the Falcon platform with the efficiency of a dedicated team of security professionals. Falcon Complete delivers relentless focus on managing and monitoring your endpoint security and responds to threats with speed and precision — so you don't have to.

Falcon Complete is a turnkey solution for organizations that do not have extensive security budgets. Defending against today's threats demands constant vigilance by skilled staff, and the cost of building a comprehensive security program that is staffed 24/7 by security experts can be out of reach for many organizations. But even for organizations that possess the financial means to build such programs internally, the Falcon Complete team is often the fastest and easiest track to a comprehensive, mature endpoint security program.

CrowdStrike stands so strongly behind its breach protection capabilities that Falcon Complete comes with a Breach Prevention Warranty of up to $1 million[1] if a breach occurs within the protected environment.

Falcon Complete complements your investment in Falcon technology with the dedicated professionals and mature processes needed to stop breaches wherever and whenever they may happen.

This white paper explores the challenges associated with getting the most out of your endpoint security solution and how the Falcon Complete team is uniquely positioned to solve these challenges.

Falcon Complete delivers relentless focus on managing and monitoring your endpoint security and responds to threats with speed and precision — so you don't have to.

1 Restrictions apply. Please see the Falcon Complete Breach Prevention Warranty FAQ for details.

COMMON CHALLENGES TO MAXIMIZING SECURITY POSTURE

Organizations are faced with some common challenges when implementing an endpoint security program, driving the demand for MDR services such as Falcon Complete:

- **Difficulty managing the technology.** In order to ensure proper levels of protection, any security solution requires regular proactive management. This ensures that protection is properly deployed across every endpoint in the organization and properly configured to defend against modern threats. Often, IT teams don't have the tools and bandwidth to continuously manage their endpoint protection. Furthermore, they might lack the time and experience required to know how to best configure the security policies to match their security needs and keep their endpoints protected. This situation can result in an endpoint solution being partially deployed and poorly configured, leaving unseen security gaps that expose the organization to intrusions.
- **Inability to reliably act on threats in time to stop a breach.** Security alerts provide critical insights into emerging threats, allowing defenders to respond in the critical early stages before a breach can occur. However, they're only valuable if analysts can review and act on them in time. Managing alerts takes time, energy and expertise. Many organizations suffer a shortage of these important cybersecurity resources. Even for organizations that have a dedicated security team or a SOC (security operations center), handling the alerts generated by an endpoint security product can be overwhelming, leading to alert fatigue and leaving alerts unvalidated — which can open the door to attackers.
- **Difficulty properly remediating incidents.** It takes skill and experience to quickly determine the best way to remediate an incident. Unfortunately, many organizations lack the time and expertise needed to fully understand the nature and scope of an incident when one occurs. This can result in IT and security teams struggling for weeks to remediate a situation — often taking unnecessary and burdensome action such as reimaging, or worse, believing an environment has been cleaned when it hasn't.

"By 2024, 25% of organizations will be using MDR services, up from less than 5% today. By 2024, 40% of midsize enterprises will use MDR as their only managed security service."

Gartner Research
Market Guide for Managed Detection and Response Services, July 15, 2019[2]

2 Craig Lawson, Toby Bussa, Sid Deshpande, Pete Shoard, Kelly Kavanagh, "Market Guide for Managed Detection and Response Services" July 15, 2019

THE FALCON COMPLETE TEAM: 24/7 EXPERT MANAGEMENT, MONITORING AND RESPONSE

Falcon Complete augments CrowdStrike's proven protection technologies with the people, expertise and processes necessary to provide a hands-off approach to endpoint security.

Built on the CrowdStrike Falcon platform, Falcon Complete is CrowdStrike's most comprehensive endpoint protection solution. It delivers unparalleled security by augmenting Falcon Prevent™ next-gen antivirus (NGAV), Falcon Insight™ endpoint detection and response (EDR) and Falcon OverWatch™ managed threat hunting, together with the expertise and 24/7 engagement of the Falcon Complete team. The team manages and actively monitors the Falcon platform for customers, remotely remediating incidents as needed. The Falcon Complete team solves the challenge of implementing and running an effective and mature endpoint security program without the difficulty, burden and costs associated with building one internally.

A HIGHLY SKILLED AND MOTIVATED TEAM

The Falcon Complete team is in charge of managing and monitoring the Falcon platform, as well as responding to the threats it detects. The team is composed of seasoned security professionals who have experience in incident handling, incident response, forensics, SOC analysis and IT administration. The team has a global footprint, with members located in the United States, the United Kingdom and Australia, allowing true 24/7 "follow the sun" coverage.

Through years of providing incident response services, these experts have honed their skill sets, making them both highly efficient and very effective. Because they are continually focused on managing the Falcon platform, they have developed the "muscle memory" necessary to rapidly triage and respond to threats. This is one factor that sets them apart from other security practitioners who may wear many hats and be tasked with a myriad of IT responsibilities and security technologies, often leaving them unable to achieve full mastery of a specific area.

In fact, many of the team members chose to join the Falcon Complete team because it allows them to apply and refine their skills on a daily basis, which is not always the case when working for an individual organization. Falcon Complete team members can focus on the work they enjoy the most, such as incident handling, malware analysis or remediation. This environment is why CrowdStrike attracts and retains the top talent across the globe.

The entire team is CCFA and CCFR certified, ensuring they are extremely skilled at using the Falcon platform and are very familiar with its tools and data structure. As a result, the team knows how to conduct rapid triage in a way that many customers are unable to achieve because they don't have the necessary experience or intuition.

The Falcon Complete team also enjoys a close relationship with other CrowdStrike security experts. Collaboration with the CrowdStrike Intelligence team enables access to a massive treasure trove of cyber threat information. This access to real-time intelligence results in faster, more precise and timely detections,

THE FALCON COMPLETE TEAM

Experts in the CrowdStrike Falcon platform: CrowdStrike Certified Falcon Responder (CCFR) and CrowdStrike Certified Falcon Administrator (CCFA)

Experts in incident response: Multiple years of experience in digital forensics and incident response (DFIR)

Always watching — 24/7/365

the ability to anticipate what attackers might do, more detailed and comprehensive recommendations, and superior incident handling, resolution and remediation.

MANAGING, MONITORING AND RESPONDING TO THREATS

The three primary areas in which the Falcon Complete team operates — managing the Falcon platform, monitoring the platform and responding to threats — combine to provide comprehensive security that starts on the first day.

Onboarding: A True Partnership with You

Becoming a Falcon Complete customer is a fast and efficient process that takes just a few days for a typical organization. The onboarding process starts with the Falcon Complete team working with you to select the appropriate security posture for your environment and documenting it in an "Operating Model." The Operating Model articulates how Falcon needs to be configured and also how the customer wants the team to respond to threats. It defines the flow of how the team will triage detections and how in certain circumstances it will respond to these detections or escalate issues to your organization for approval. This ensures that you and the Falcon Complete team are on the same page and know what to expect of each other.

To define your security posture, you will complete a brief checklist that provides a high-level view of your desired security strategy and what matters most to you. The Falcon Complete team translates that information into the proper security posture, including how the Falcon platform should be configured.

To make this process quick and straightforward, the Falcon Complete team provides baseline recommendations. These recommendations can be summarized as different levels of security posture: active, measured or cautious.

- **Active** means that the Falcon platform's prevention policies are set to be fairly restrictive, according to CrowdStrike's recommendations and predefined countermeasures that the customer has authorized the Falcon Complete team to take when threats are observed in your environment. An active posture means that proactive prevention is turned on, and if there is a detection, the team is able to respond immediately and remotely.
- A **measured** posture means that some of the prevention policies are not turned on, but the team can still take some predefined actions, with the exception of any response that may be disruptive to IT, such as isolating (network-containing) a device.
- With a **cautious** posture, the team monitors detections only. Only the highest-confidence preventions are enabled, and no remediation actions will be automatically initiated by the team as a result of an incident. This is an option for areas of the network where the customer wants the Falcon Complete team to be hands-off.

These simple choices allow the team to create a tailored endpoint security strategy for a customer and apply different posture levels to different parts of the environment. An organization could, for example, require an aggressive posture for protecting its workstations, because that's where most of its alerts come from and where most intrusions begin. However, the customer may want a more cautious posture for certain systems due to internal change management requirements or other concerns. To implement such a tailored model, the Falcon Complete team, in collaboration with the customer, can divide the environment into logical groups.

All of these inputs are gathered during the onboarding process, and at the conclusion of that process, the team prepares an Operating Model with a defined security posture that is tailored to your organization. The team then takes the actions required to implement the

Becoming a Falcon Complete customer is a fast and efficient process that takes just a few days for a typical organization.

model, such as configuring prevention policies or enabling the countermeasures the team will take when faced with different situations. Onboarding can be completed in a matter of days for most organizations.

Ongoing Management

The process described above is not a one-time occurrence. Over time, your organization evolves, your needs can change, or the product itself can change. The team meets with you regularly, ensuring that the Operating Model and its implementation are kept up-to-date over time. The team also keeps a watchful eye for changes in your environment. For example, if the Falcon agent is deployed on new endpoints, the Falcon Complete team will check to ensure that appropriate logical groups exist to manage those endpoints, and that the endpoints are added to the correct groups. This guarantees that new agents coming online are added to the right groups and get the appropriate prevention policies.

The team also looks for unmanaged devices and related risks, using the Falcon Discover™ technology included in Falcon Complete. Changes in the number of deployed endpoints, such as a sizable number of new installations, are also monitored. Regularly verifying that all agents are up-to-date and have the right prevention policies ensures a healthy agent population and an optimum level of protection at all times.

Frequently verifying that all agents are up-to-date and have the right prevention policies ensures a healthy agent population and an optimum level of protection at all times.

Management of Falcon Platform Before and After Falcon Complete

Before Falcon Complete	With Falcon Complete Expert Management
• Challenges with visibility and control over unmanaged systems • Unprotected, exposed systems linger unnoticed at the fringes	• Comprehensive control of unmanaged systems • Falcon Complete helps customers ensure all assets are properly grouped, sorted and protected
• Delays in updating Falcon agent • Machines with an outdated Falcon agent may be lacking the latest protection techniques	• Tight control over Falcon agent • Falcon Complete ensures the current Falcon agent is installed, delivering the best level of protection available
• Numerous policies, applied inconsistently • Over time, a patchwork of policies evolves, creating confusion, complicating threat investigations and potentially leaving dangerous protection gaps	• Rigorous configuration management • Proven, best-practice policies are systematically applied to all systems
OUTCOME: Hand-tuned protection for all of your systems, all of the time	

Monitoring the Falcon Platform

The Falcon Complete team monitors your Falcon platform 24 hours a day, seven days a week, looking for new security alerts. Every detection, regardless of severity, is investigated by the team. Triage starts with an understanding of the original source of the detection. For example, if the Falcon machine learning engine determines that a file is malicious, the team will research when that file was first introduced to the endpoint and what process wrote it to the system. The team will then trace the process tree back to find out how that chain of events originally started, which user account was associated with those processes, and how the user was logged in. The team then investigates whether the malicious file was seen on other systems, so it can determine if the attack hit multiple endpoints or is isolated to just one. The team answers these questions in the first few minutes of a detection.

The team enjoys a major advantage over most incident handlers, thanks to its direct access to other CrowdStrike teams. For example, the Falcon Complete team works closely with Falcon OverWatch, the team that is in charge of proactively hunting for threats. It also leverages its internal relationships with CrowdStrike Services, CrowdStrike Intelligence and CrowdStrike Support. This allows the team to take each detection through a process of triage, containment, eradication and recovery that is lightning-fast, thorough and effective.

This efficient and comprehensive process enables the team to dispatch every detection, in the process determining with certainty if the detection is a false positive, if it's isolated to a single endpoint, or if it's a widespread incident. This information guides how the team responds.

The Falcon Complete team monitors your Falcon platform 24 hours a day, seven days a week, looking for new security alerts. Every detection, regardless of severity, is investigated by the team.

Monitoring Before and After Falcon Complete

Before Falcon Complete	With Falcon Complete Expert Monitoring
• 8 hours/day active monitoring • Attackers do not honor business hours or holidays, and threats that happen during off-hours are likely to go ignored until the next business day	• 24 hours/day active monitoring • Falcon Complete is always watching, ensuring that emerging threats are addressed in real time, as they happen
• Majority of detections go unexamined • Lower-severity detections, including successfully blocked malware, are often ignored but represent critical evidence of potential future attacker activity	• Human eyes on every detection • Falcon Complete investigates all critical, high-, medium- and low-severity detections in a timely manner, ensuring that intrusions are identified at the earliest possible stage
• 6 hours: Average time to begin response[3] • Response is delayed because teams often lack the necessary knowledge, threat intel and experience	• 10 minutes: Average time to begin response[4] • Falcon Complete builds and continuously tunes a repeatable playbook to ensure all threats are investigated quickly and efficiently
OUTCOME: Expert threat monitoring, 24/7/365, to respond to attacks in minutes as they happen	

3 Vanson Bourne, "The 2019 Global Security Attitude Survey," November 2019

4 Median time for Falcon Complete to investigate and respond to security incidents, measured over the first half of 2020. Individual investigation and response times will vary.

Responding to Threats

The third area handled by the Falcon Complete team is responding to threats. When a critical, high- or medium-severity detection occurs, the team begins by validating that it is a legitimate threat.

If the team determines that an alert is a true positive, it follows the playbook that was developed with the customer and responds according to the requirements. That may involve taking containment actions such as blocking a hash or a network containing an affected device. The Falcon agent allows those actions to be taken immediately.

Next, and if needed, the team moves to the remediation phase. This can involve remotely accessing an endpoint to disrupt an attack in progress, cleaning up a compromised endpoint or removing malware artifacts. This is a major benefit for the customer because the team does not stop at alerting that there is an issue — the Falcon Complete team fully resolves the problem so that the customer does not have to, without cumbersome and expensive tactics such as reimaging systems.

In the event an alert is determined to be a false positive, the team works to ensure that no unnecessary actions are triggered. The team selects the best approach for each customer and each situation. For example, the Falcon Complete team will determine if the best resolution is whitelisting, exclusions or working with CrowdStrike's Support and Security Response teams to create new patterns and eliminate further false positives.

The Falcon Complete team fully resolves the problem so that the customer does not have to, without cumbersome and expensive tactics such as reimaging systems.

Response Before and After Falcon Complete

Before Falcon Complete	With Falcon Complete Surgical Response
• 6-8 hours: Time for IT to reimage system • Reimaging is the most common remediation technique — it's reliable but labor-intensive	• 45 minutes: Time to perform surgical remediation[4] • Falcon Complete executes surgical remediation remotely, often without the need for reimaging
• 6-8 hours: Downtime for end user during system reimaging • Reimaging is not only expensive but also has a high impact on user productivity and can erase valuable forensic evidence	• 0 minutes: Typically, no downtime for the end user during surgical remediation • Falcon Complete can often perform remediation without the user being aware that it has happened
• Uncertainty • Once initial response is complete, responders may be rushed to the next case, perhaps leaving doors open for the threat to re-emerge in the future	• Confidence • Falcon Complete performs comprehensive analysis on every intrusion, enabling full and complete remediation, backed by CrowdStrike's Breach Prevention Warranty
OUTCOME: Surgical remediation eradicates threats with speed and precision	

How Falcon Complete Works with an MSSP

Many organizations ask the question, "Do I need Falcon Complete if I have a managed security service provider (MSSP)?" MSSP offerings can vary widely, but generally speaking, MSSPs are focused on broad monitoring and management of security tools within an enterprise. This typically includes basic triage of security alerts, along with a variety of other services such as technology management and upgrades, compliance, and vulnerability management.

Falcon Complete provides a very different focus. Falcon Complete delivers fast, turnkey integration, with unmatched expertise in the CrowdStrike Falcon platform. Falcon Complete services are laser-focused on their mission to manage, monitor and respond to threats with maximum effectiveness and in a minimum amount of time. Because of this focus, Falcon Complete can deliver immediate value, at a low cost and within a very short time window — and back up the work with the industry's most comprehensive Breach Prevention Warranty.

Falcon Complete services are laser-focused on their mission to manage, monitor and respond to threats with maximum effectiveness and in a minimum amount of time.

Falcon Complete vs. MSSP

Phase	Activity	Falcon Complete	MSSP
Manage	Staffed by experts in the Falcon platform and DFIR	x	
	Helps identify and eliminate unmanaged systems	x	
	Maintains the current version of Falcon sensors on protected endpoints	x	
	Configures and continuously optimizes Falcon policies	x	
	Ensures all systems are properly grouped and appropriately protected by the Falcon platform	x	
	Includes proactive check-ins and reporting	x	x
Monitor	Provides 24/7/365 monitoring of the Falcon platform	x	x
	Investigates critical and high-severity detections	x	x
	Investigates medium- and low-severity detections	x	?
	Includes proactive human threat hunting	x	?
	Benefits from deep access to CrowdStrike Intelligence and OverWatch experts	x	
Respond	Determines response strategy	x	x
	Provides response advice	x	x
	Proactively contains compromised systems	x	
	Conducts surgical remediation	x	
	Provides a post-intrusion summary with hardening recommendations	x	
	Provides investigation and response service-level agreements (SLAs)	x	x
	Includes Breach Prevention Warranty	x	

DELIVERING INSTANT HANDS-ON HELP TO CUSTOMERS

IMMEDIATELY OPERATIONAL

The first and most obvious advantage of using CrowdStrike to manage all aspects of endpoint security is time-to-value. Organizations that attempt to build an effective SOC that can respond to and remediate threats effectively find that it's a long, complex and expensive process. From finding and hiring the right talent and acquiring the appropriate technology, to defining policies and creating an incident response process, the entire undertaking can take months, if not years.

One complicating factor is that such programs often suffer from a lower priority than other urgent IT projects, resulting in long implementation times that leave organizations vulnerable. Cost can also be an issue. Building a minimally staffed 24/7-coverage model requires at least four full-time employees (FTEs), which can put the required level of security maturity out of reach for many companies. For those that have the budget, it is still challenging to find and retain the necessary expertise. Recruiting, training and retaining a staff skilled enough to square off against the advanced and sophisticated adversaries organizations face can be daunting. This is a significant problem for an industry that, in general, suffers from a shortage of qualified security experts.

In contrast, the Falcon Complete team delivers immediate time-to-value, instantly adding experienced security experts that work alongside the customer's staff, and assuming the management of the Falcon platform. For each new customer, the Falcon Complete team provides recommendations and a proven operating model that includes a tailored playbook and a fully operational 24/7 team that can start monitoring as soon as the customer is onboarded.

DELIVERING RESULTS, NOT HOMEWORK

Another important benefit provided by the Falcon Complete team is remote remediation. In situations where endpoints are compromised, the Falcon Complete team provides an additional set of hands, not just more alerts — taking action to remediate the systems so customers don't have to. The team's unique skill set allows it to respond to incidents efficiently, swiftly and with confidence. This skill set is so hard to develop that many organizations elect to completely reimage a system as their remediation procedure when it is deemed to be infected or compromised.

Reimaging can be an effective solution, but it is also very costly. In addition, it often becomes a pain point both for IT departments and for end users, whose productivity is disrupted when they need to turn in their laptops to the helpdesk. In turn, the helpdesk is forced to spend a significant amount of time performing this reimaging task, to assure end users that their workstations are known to be trusted.

What makes the Falcon Complete team unique is its ability to fully and quickly analyze and understand the scope and details of an incident, enabling them to remediate with confidence without defaulting to reimaging.

The team will do the analysis necessary to understand the incident. For instance, is it a commodity malware infection, or is it an attacker that's left a backdoor in the environment? The team will then use the same skills that would be used in a full investigation, but apply them in a rapid, tactical manner on a single system to understand how the attack is progressing, the persistence methods being used and the nature of the backdoor or malware used by the attacker to access the system. Once the team understands the attack comprehensively, it can with full confidence remotely remove backdoors, clean up malware, kill persistence methods and stop malicious processes that are running in memory. The team can do this far more comprehensively than what can be accomplished using only antivirus solutions or automated processes.

This removes a huge burden from customers who are reimaging endpoints that don't need such extreme measures. With the Falcon Complete team by their side, doing the right kind of analysis and taking the right actions, most of the systems that a customer has been reimaging won't need to be reimaged at all. This provides a far less disruptive way to remediate incidents: addressing the real problem and fixing the actual issue in a cost-effective approach that's far more efficient then reimaging.

CONCLUSION

Falcon Complete provides your organization with a mature and effective endpoint security program at a speed, cost and level of efficacy that very few organizations can achieve on their own, or even with the help of other third parties.

Off-loading endpoint security management to CrowdStrike saves organizations countless months of effort spent building an endpoint security program, implementing it, managing it, handling alerts and responding to incidents.

By bringing in a team that is specifically dedicated and highly skilled at using and managing the CrowdStrike Falcon platform, organizations of all sizes immediately reach the highest level of maturity in their endpoint security strategy, elevating their overall cybersecurity program and instantly improving security posture.

The most obvious benefit of the Falcon Complete team is peace of mind.

Customers find peace of mind knowing that the best security experts in their respective fields are watching the organization's endpoints 24 hours a day — including weekends, at night and when they are in meetings or otherwise occupied. Falcon Complete customers can rest assured that the Falcon Complete team will take action to remediate incidents — so they don't have to.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: **We stop breaches.**

Learn more about Falcon Complete