CrowdStrike Products

CROWDSTRIKE

CROWDSTRIKE FALCON COMPLETE

How to Achieve Instant Cybersecurity Maturity for Organizations of All Sizes

CROWDSTRIKE FALCON COMPLETE

EXECUTIVE SUMMARY

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

CrowdStrike® Falcon Complete™ solves these challenges by combining the effectiveness of the Falcon endpoint protection platform (EPP) with the efficiency of a dedicated team of security professionals focused on managing and monitoring your endpoint security and responding to threats, so you don't have to.

Falcon Complete is a great solution for customers who do not have extensive security budgets. 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 endpoint security program. In addition, CrowdStrike stands so strongly behind its breach protection capabilities that Falcon Complete comes with a breach prevention warranty of up to $1 million if a breach occurs within the protected environment.

Falcon Complete makes the highest level of endpoint security maturity — and ultimately, the peace of mind that it brings — instantly achievable for many companies.

Falcon Complete makes the highest level of endpoint security maturity — and ultimately, the peace of mind that it brings — instantly achievable for many companies.

INTRODUCTION

Operating an effective security program can be extremely challenging. It requires resources to appropriately implement, use, support and maintain the program over time. As a result, lots of organizations fail to get the most out of the security technologies they have acquired.

The situation is even worse for organizations that want to establish a strong endpoint security posture, as higher levels of security usually require even more resources.

As a result, many organizations have not successfully implemented a fundamental security program, let alone a comprehensive one. This situation is exacerbated when serious incidents occur and the organization does not have the time or expertise to properly remediate the situation, potentially endangering the safety of the organization.

This white paper explores the challenges associated with getting the most out of your endpoint security solution and how the Falcon Complete Team solves these challenges in a unique way.

COMMON CHALLENGES TO MAXIMIZING SECURITY POSTURE

There are some common challenges that organizations are faced with when implementing an endpoint security program:

- **Difficulty implementing the technology they acquired**
  Depending on the size and workload of their IT teams, some organizations might not have the tools and bandwidth to quickly and fully implement a solution to their endpoints. Furthermore, they might lack the time and research 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, resulting in security gaps that leave the organization vulnerable to breaches.

- **Difficulty managing alerts and incidents day-to-day**
  Managing alerts can consume resources, and security expertise is often required to properly investigate them. Many organizations suffer a shortage of these important cybersecurity resources. Even for organizations that have a dedicated security team or an SOC (security operation center), handling the potentially huge number of alerts generated by an endpoint security product can be overwhelming, leading to alert fatigue and leaving alerts unvalidated, which can open the door to breaches.

- **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 re-imaging, or worse, believing an environment has been cleaned when it hasn't.

Depending on the size and workload of their IT teams, some organizations might not have the tools and bandwidth to quickly and fully implement a solution to their endpoints.

THE FALCON COMPLETE TEAM: A FORCE MULTIPLIER THAT PROVIDES INSTANT SECURITY MATURITY

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

Built on the CrowdStrike Falcon® platform, CrowdStrike Falcon Complete is CrowdStrike's most comprehensive endpoint protection solution. It provides unparalleled security by combining 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.

It is the Falcon Complete Team that 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.

MANAGING, MONITORING AND RESPONDING TO THREATS

The Falcon Complete Team operates in three primary areas: First, the Team manages the Falcon endpoint protection platform; second, they monitor the platform; and third, they respond to threats.

Managing Falcon Endpoint Protection
Managing Falcon means that all customers are required to do is to install the Falcon agent to their endpoints. The Falcon Complete Team takes over from that point on.

Onboarding: A True Partnership with the Customer
The onboarding process starts with the Falcon Complete Team working with the customer to select the appropriate security posture for their 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 is going to triage alerts and in certain circumstances, how they respond to these alerts or escalate issues to the customer for approval. This ensures that the Falcon Complete Team is on the same page as the customer's team and that both know what to expect of each other.

To create the operating model, the customer provides a high-level view of their desired security strategy and what matters to them. 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 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 plans specifying countermeasures that the customer has authorized the Falcon Complete Team to take when they observe threats in the customer's environment. To summarize, an active posture means that prevention is turned on and if there is a detection, the Team is able to respond immediately and remotely.

A measured posture means only 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.

FALCON COMPLETE

All the components needed to instantly implement and continuously run the most mature and efficient endpoint security program.

Prevention, EDR and Asset Management

Proactive Threat Hunting

Onboarding, Configuration, Tuning and Maintenance

Alert Monitoring, Triage and Analysis

Remote Response and Remediation

Breach Prevention Warranty

With the cautious posture, the Team just monitors alerts. Only the highest confidence preventions are enabled and no remediation will be initiated by the Team automatically 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 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. The customer 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 mission-critical servers because any disruption, even for the sake of cybersecurity, could have a large impact on its business. 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 a document called the Operating Model for each customer. The Team then takes the actions required to implement the model, such as configuring the prevention policies or enabling the countermeasures that the team will take when faced with different situations.

On-Going Management

The process that is described above is not just a one-time occurrence. Since the customer's needs can change, or the product itself can change, the Team meets with the customer regularly. This ensures that the Operating Model and its implementation are kept up to date over time. The Team keeps a watchful eye for changes. For example, if the customer deploys Falcon agents on new endpoints, the Falcon Complete Team will check and ensure that appropriate logical groups to manage those endpoints exist 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. They use the Falcon Discover technology included in Falcon Complete for that purpose. Changes in the number of deployed endpoints, such as a sizeable number of new installations, are also monitored. Frequently verifying that all agents are up to date and that they have the right prevention policies ensures a healthy agent population and an optimum level of protection at all times.

Monitoring the Falcon Endpoint Protection Platform

The second area that the Falcon Complete Team manages is monitoring. The Team monitors the Falcon platform 24 hours a day, looking for new detections. 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 Falcon 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.

Each alert triage starts with an understanding of the original source of the alert. 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. These are the questions that the team answers in the first few minutes of a detection.

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

The The Falcon Complete Team operates in three primary areas: First, the team manages the Falcon endpoint protection platform; second, they monitor the platform; and third, they respond to threats.

Responding to Threats

This brings us to the third area handled by the Falcon Complete Team: responding to threats. When a critical, high or medium severity detection occurs, the team begins by validating that it is a legitimate threat. If it is 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 Team will determine if the best resolution is whitelisting, exclusions or working with CrowdStrike's Support and Security Response Team to create new patterns and eliminate further false positives.

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 its requirements. That often involves 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 eradication 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 — it fully resolves the problem so that the customer does not have to deal with it.

A HIGHLY SKILLED AND MOTIVATED TEAM

As this paper has detailed, 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.

Years of providing incident response services has allowed these experts to hone 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 of the factors 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 have chosen 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 a specific customer. The Falcon Complete Team members can focus on the work they enjoy the most, such as incident handling, malware analysis and remediation. This environment is why CrowdStrike attracts and retains the top talent across the globe.

The Team is also extremely skilled at using the Falcon platform and 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. Access and collaboration with the Falcon 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 ability to anticipate what attackers might do, more detailed and comprehensive recommendations, and superior incident handling, resolution and remediation.

The Falcon Complete Team is composed of seasoned security professionals who have experience in incident handling, incident response, forensics, SOC analysis and IT administration.

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. It can take a long time to build an effective security operations center that can respond to and remediate threats effectively. 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 make 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 assumes the management of the Falcon endpoint protection 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 on-boarded.

REMEDIATING INCIDENTS FOR CUSTOMERS

The next 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. This unique skill set developed by the Team allows the Team to respond to incidents efficiently, swiftly and with confidence. This skill set is so hard to develop that many organizations elect to completely re-image a system, as their remediation procedure, when it is deemed to be infected or compromised.

Re-imaging can be an effective solution, but it is also very costly. In addition, it often becomes a pain point for both IT departments and 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 re-imaging task, so that end users are assured they have workstations that 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 re-imaging.

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 forensics 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.

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 re-imaging.

This takes away a huge burden from customers that are re-imaging endpoints that don't need such extreme measures. With the Falcon Complete Team by their sides, doing the right kind of analysis and taking the right actions, most of the systems that customers have been re-imaging won't need to be re-imaged 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 re-imaging.

EXAMPLE: ERADICATING "SUPER MALWARE" FROM CUSTOMER ENVIRONMENTS

The following example, that of an organization that reached out to CrowdStrike for assistance with a challenging malware problem, illustrates how Falcon Complete is able to remediate very complex incidents rapidly and effectively. This organization was experiencing an outbreak of the EMOTET malware in its environment and had been unsuccessful at cleaning up the infected systems on its own.

EMOTET malware contains a self-propagation mechanism that allows a single infected endpoint to reach out to its neighbors and infect them. It propagates laterally by brute-forcing user accounts, making note of successfully cracked credentials and using them to log in and spread to other systems. Cleaning up one system at a time is inefficient, as the malicious botnet will "heal itself" by re-infecting its neighbors. The only way to remediate it effectively is to clean all infected systems simultaneously, often requiring comprehensive action throughout the environment

The organization decided to implement Falcon Complete to solve this issue. Following deployment, the Falcon Complete Team quickly realized that the problem was far worse than the customer had estimated. Originally, the customer estimated that the EMOTET outbreak had happened only a couple of weeks prior to detection. However, analysis from the Falcon Complete Team concluded that the outbreak actually had been going on for six months and was much more widespread than the customer first realized. Once onboarding was complete, it took the Falcon Complete Team only two days to solve the problem.

Thanks to a new level of visibility delivered by the Falcon platform and with the help and expertise of the Falcon Complete Team, it took only two days to solve an incident that the customer had been unaware of for six months and had been struggling to remediate for several weeks.

CONCLUSION

Falcon Complete provides a mature 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 the burden of endpoint security to CrowdStrike saves organizations countless months of efforts spent on 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 endpoint protection platform, organizations of all sizes immediately reach the highest level of maturity for their endpoint security strategy, elevating their overall cybersecurity program and instantly improving security posture.

However, the most obvious benefit of the Falcon Complete Team is probably peace of mind.

Customers find peace of mind knowing that the best security experts in their fields are watching their endpoints 24 hours a day, including on weekends, at night or 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 is the leader in cloud-delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. Falcon seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches.

Learn more at www.crowdstrike.com