CrowdStrike Products and Services

CROWDSTRIKE

FALCON COMPLETE

Fully managed endpoint protection delivered as a service by a CrowdStrike team of experts

SOLVES THE CHALLENGE OF MANAGING, RESPONDING TO AND REMEDIATING THREATS

Operating an effective endpoint security program can be extremely challenging. The necessary tools can be difficult to use, requiring an abundance of resources to appropriately implement, support and maintain them over time. As a result, many organizations fail to get the most out of the endpoint security technologies they have acquired.

The situation is even worse for organizations that want to establish a strong endpoint security posture. Higher levels of security require even more resources as they can be costlier to maintain and more complex to manage.

The result? Many organizations do not successfully implement a fundamental endpoint security program, let alone a comprehensive one. The situation is exacerbated when serious incidents emerge and the organization does not have the time or expertise to properly remediate the situation, potentially endangering the safety of the organization.

CYBERATTACKS STRAIN IT SECURITY RESOURCES

- **63 hours:** This is the average time it takes for an organization to detect and remediate a threat. (VansonBourne - July 2018).
- **3.5 million:** These are the cybersecurity positions projected to be unfilled by 2021, as organizations struggle to keep pace with the dramatic rise in cybercrime.(Cybersecurity Jobs Report 2018-2021 - CyberSecurity Ventures)

There are some specific challenges that organizations can struggle with in their implementation of an endpoint security program:

- **Difficulty fully implementing and properly configuring 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 successfully deploy the solution to their endpoints. In addition, they may lack the time and expertise needed to properly configure policies that match their security requirements and keep endpoints protected. This situation can result in an endpoint solution that is only partially deployed and poorly configured — resulting in gaps in protection that leave the organization vulnerable to breaches.

- **Difficulty managing alerts and incidents day-to-day:** Handling the potentially huge number of alerts generated by an endpoint security product can be overwhelming, even for organizations that have a dedicated security team or a SOC (security operation center). It not only takes manpower to manage alerts, it requires staff with enough cybersecurity expertise to understand the alerts and determine how to properly respond to them. Unfortunately, most organizations suffer from a shortage of both manpower and expertise, leaving alerts unvalidated and opening the door to high-profile breaches.

- **Difficulty properly remediating incidents:** The shortage of resources and expertise can lead organizations to struggle with understanding the nature and scope of an incident in a timely manner. This can mean incidents are not remediated efficiently, fully addressed, or handled in a timely manner, leaving organizations vulnerable or compromised. It takes skill and experience to know what to do to properly remediate an incident. Many organizations that lack resources are forced to go through the arduous process of reimaging endpoints, because the alternative of precisely combining countermeasures such as network containment, hash prevention, delete/modify registry key values or stop/disable/restart services is not possible. Yet, even reimaging does not ensure that the incident is fully remediated.

- **Not having the budget to build a comprehensive endpoint security program:** The cost of building a comprehensive security program that is staffed 24/7 by security experts is out of reach for many organizations, making the required level of security maturity unachievable for many companies.

- **Time it takes to implement the program:** Even if an organization possesses the financial means to build an internal endpoint security program, it can take a long time to implement a mature security strategy. From finding and hiring the right talent and acquiring the appropriate technology, to defining policies and creating an incident response (IR) process, the entire undertaking can take months if not years. In addition, such programs often are given a lower priority than other urgent IT projects, resulting in long implementation processes that leave organizations vulnerable.

- **Difficulty finding and retaining the required expertise:** It can be challenging for an organization to acquire the expert staff needed to efficiently secure their endpoints. For those who can afford it, recruiting, training and retaining the staff and skills to match an advanced and sophisticated threat landscape can be very difficult. This shortage of qualified expertise is an industry-wide problem.

- **Some required components do not exist:** Even if organizations decide to outsource their endpoint security, rather than build it internally, they will find that not all the necessary components can be easily found. One of the most difficult and sensitive steps is remediation. Most security providers will shy away from offering such a component because it requires a level of skill and experience they do not possess.

USE CASE: DIFFICULTY IMPLEMENTING TECHNOLOGY

		BENEFITS
Challenge	Depending on the size and workload of your IT teams, you may not have the tools and bandwidth necessary to quickly and fully implement endpoint security, leaving your organization vulnerable to breaches.	Falcon Complete handles all aspects of endpoint security, from deployment, configuration, maintenance and monitoring, to alert handling, incident response and remediation, ensuring you have effective endpoint security and reducing the risk of a breach.
Solution	Falcon Complete™ helps you successfully operationalize and optimize your endpoint security with: ■ **Configuration expertise:** CrowdStrike® helps you create the policy management groups and apply the desired prevention policies for you based on your expertise and experience. ■ **Tuning and refinement:** Prevention and detection policies are continually reviewed with you to ensure the optimal operation of all the capabilities of the Falcon platform. ■ **Ongoing management:** Over time, the endpoints on a given network change. From technology refreshes, to joiners, movers, and leavers, there is a significant churn in any given organization that needs to be managed to ensure that the correct prevention policies and the health of endpoint agents are being maintained.	

USE CASE: DIFFICULTY MANAGING ALERTS AND INCIDENTS DAY-TO-DAY

Challenge	Handling a large volume of alerts generated by an endpoint security product can be overwhelming. This can lead to alert fatigue and leave alerts invalidated or incorrectly handled, opening the door to breaches.	You benefit from 24x7x365 monitoring and incident handling assistance, ensuring that all alerts are effectively handled, reducing the risk of a serious breach.
Solution	Falcon Complete will manage all of these alerts and undertake the necessary actions: ■ **Incident handling:** The Falcon Complete team works with you to create a set of incident handling playbooks to articulate what types of countermeasures will be taken in a given detection scenario. ■ **Remote incident triage:** When the Falcon platform generates an alert, the Falcon Complete team triages it to identify if it is a false positive or a true incident, then classifies it appropriately in the incident management system. ■ **Remote incident remediation:** In accordance with the playbooks created for you, the Falcon Complete team may initiate incident response countermeasures to completely stop attacks and remediate incidents.	

USE CASE: DIFFICULTY IN PROPERLY REMEDIATING INCIDENTS

Challenge	A lack of skill and experience can lead to teams struggling for weeks to remediate a situation, wasting valuable resources and believing an environment has been cleaned when it hasn't.	The Falcon Complete team will fully resolve the incident so that you don't have to deal with it.
Solution	Falcon Complete will step in and undertake all of the actions needed to respond and remediate an incident: ■ **Remote incident remediation:** In accordance with the defined playbooks, Falcon Complete will seek to understand the nature of the alert and then build a strategy for remediation by combining specific countermeasures. ■ **Remote access to the endpoint:** The team will act to disrupt and eradicate attacks in progress, cleaning up a compromised endpoint or removing malware artifacts for further analysis.	

FALCON COMPLETE — CROWDSTRIKE EXPERTISE AND TECHNOLOGY, YOUR SECURITY

CrowdStrike Falcon Complete uniquely provides the technology, platform, actionable intelligence and skilled expertise required to provide comprehensive endpoint security from beginning to end. With Falcon Complete, customers can entrust the implementation, management and incident response of their endpoint security to CrowdStrike's proven team of security experts. The result is an instantly optimized security posture without the burden, overhead and cost of managing a comprehensive endpoint security program internally.

Built on the CrowdStrike Falcon® platform, 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 with the expertise and 24/7 engagement of the CrowdStrike team. The team manages and actively monitors the Falcon platform for customers and remotely remediates incidents as needed. Falcon Complete combines the effectiveness of the Falcon platform with the efficiency of a dedicated team of security professionals, executing focused, incident-handling playbooks on your behalf.

ENDPOINT SECURITY DELIVERED

Falcon Complete is the comprehensive endpoint security lifecycle solution that takes care of all aspects of endpoint security, including remotely remediating incidents with confidence, so you don't have to. It allows you to gain the highest level of endpoint security while simplifying the implementation and day-to-day operations of your endpoint protection program. Falcon Complete uniquely provides the technology, platform, actionable intelligence and skilled expertise required to fully handle endpoint security, from beginning to end.

WHAT MAKES FALCON COMPLETE UNIQUE?

- Offloading Falcon endpoint protection to experienced CrowdStrike staff
- Assisting in deployment and configuration
- Providing 24x7 alert and incident handling
- Delivering proactive incident triage and containment
- Effectively handling incident remediation
- Ensuring transparent management reporting and metrics

WHY CROWDSTRIKE

CrowdStrike Falcon provides a cloud-delivered solution that safeguards your organization while satisfying your mission requirements. The threats you face are constantly evolving and you require a solution that proactively detects and prevents these events from occurring. CrowdStrike has built its solutions around the ability to detect and prevent breaches by even the most sophisticated adversaries. With a platform that seamlessly deploys and scales with your enterprise and a dedicated team of security professionals, CrowdStrike protects your enterprise with a solution designed to stop the breach and evolve with you.

LEARN MORE AT
WWW.CROWDSTRIKE.COM
Phone: 1.888.512.8906
Email: sales@crowdstrike.com
Web: www.crowdstrike.com