DETAILS

Vendor CrowdStrike, Inc

Price Starts at $50.00

Contact crowdstrike.com

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
Ease of Use:	★★★★★

OVERALL RATING ★★★★★

Strengths The real-time remediation is a great addition to this already rich toolset.

Weaknesses Cloud only management is the only option, so if you need to support an air-gapped environment, this isn't your tool.

Verdict With the addition of real-time response to the EDR module, this product becomes even more attractive. If you aren't using CrowdStrike, you really need to take a good hard look at Falcon.

CROWDSTRIKE

Sunnyvale, CA
888.512.8906
https://www.crowdstrike.com/

CrowdStrike, Inc
CrowdStrike Falcon

W e've looked at CrowdStrike's Falcon product in the past, and it continues to shine. We continue to be impressed with the completeness of this comprehensive security tool. It is easy to deploy, the dashboard is intuitive, and the support portal provides you with solid information in the event you run into issues. While we feel that this tool is finely polished, the folks at CrowdStrike are continuing to regularly add features to make this product really stand out. The recent updates to Falcon X and Falcon Insight unquestionably raise the bar.

BEST BUY

The updates to Falcon X deliver increased information but also provide the steps to automate the threat analysis process, providing threat intelligence in a usable format that will allow security teams to take appropriate measures to protect their organization from future threats. Utilizing the indicators of compromise, security teams can share this information with other security solutions and improve the overall security posture of the environment. This is accomplished by using the threat intelligence gained from the attacks targeting your environment and providing advanced threat intelligence to protect your organization from all known variants of those threats.

In addition to the customized indicators of compromise, Falcon X provides detailed information to the security team to help answer the who, the what and, most importantly, the how

of an attack. With the information around the attack, security teams will be better equipped to prioritize the alerts and take the appropriate action. Using the information gathered, security teams can cut response times from days to minutes.

While updates to the Falcon X were really nice to see, the updates to Falcon Insight, including the real time response, are the major upgrades that were anticipated by the SC Labs team. With the real time response feature, not only are security teams able to view EDR data to help understand the threat, but they are able to take remediation steps to kill processes and remove files from the system with only a few quick clicks. What really makes Falcon Insight stand out is that all this is done through the cloud platform, meaning that there is no script or executable on the client, which may be used in future attacks.

CrowdStrike has been one of the standout products SC Labs has had the privilege of reviewing, and these recent updates makes it stand out in the endpoint protection crowd. With CrowdStrike providing great customer service, a wealth of support information, and a well-rounded solution - Falcon is a product that needs to be on your radar.

– Michael Diehl
tested by: Michael Diehl