# CrowdStrike
# Falcon

CrowdStrike Falcon® is, largely, a threat-hunting tool that ties the endpoint tightly into its threat-hunting ecosystem. The focus is on malware, particularly very sophisticated malware, such as ransomware and advanced persistent threats. However, it is not restricted to attacks that depend on malware. The product also has excellent intrusion prevention/blocking capabilities as well. This includes exploit blocking, machine learning, behavioral blocking, IOC blocking, custom whitelisting/blacklisting, endpoint detection and response, forensic level visibility, along with its managed hunting. CrowdStrike Falcon is SaaS and requires no on-premise management hardware or infrastructure, but it does require a lightweight sensor at the endpoint.

We deployed our sensors to a couple of virtual machines in our virtual test beds and went out to the management console to see what it could find. This is a no-nonsense console. There are no graphs showing statistics. What you see is a menu of choices down the left side, all represented with icons that represent activity, investigate, hosts, configuration, dashboards, intelligence, users and support. This is a logical order, so we began with activity. All of the icons have submenus. When we hovered over activity we saw a submenu for detections. Going there, we saw nothing, as we expected.

Next, we attacked our endpoints with some malware and went back to the submenu. The ballgame had changed materially. We saw a high-risk threat. Expanding the selection, we saw a complete picture of how the malware attacked the system and attempted to spread and do its mischief. The malware was our old friend Locky. We saw that when we introduced it to the system it attempted to execute Winlogon, Userinit and, finally, Explorer. At that point, it was ready to begin executing which, we were assured, it did not do. The analysis was complete with hashes and attack chain. From this we could conclude that the file that introduced the malware into our system was Winlogon.

Intelligence is just what the name implies and takes advantage of CrowdStrike's superior intelligence feeds, plus others as you wish to add them. Ours took feeds from NetWitness, Snort/Suricata and Yara. The overall machine learning is a graph model so it has a sophisticated approach to analysis.

We were impressed with the CrowdStrike website. There is easy access to Falcon support and assistance is comprehensive with basic no-cost aid for the life of your contract with CrowdStrike. There are fee-based advanced options and CrowdStrike has a threat-hunting support team, called OverWatch, to help you with difficult hunting problems.

*– Peter Stephenson, technology editor*

## DETAILS

**Vendor** CrowdStrike

**Price** $50 per endpoint.

**Contact** crowdstrike.com

| | |
|---|---|
| Features | ★★★★★ |
| Performance | ★★★★★ |
| Documentation | ★★★★★ |
| Support | ★★★★★ |
| Value for money | ★★★★★ |

**OVERALL RATING** ★★★★★

**Strengths** Solid threat hunting tool kit with strong emphasis on the endpoints.

**Weaknesses** None that we found.

**Verdict** This is a very sophisticated but rather specialized tool for the endpoint. If you are a large organization or one with high-value information assets, this is well worth your time. For what it does, we know of no better tool available. We make this our cloud-based Recommended product.

CROWDSTRIKE

**150 Mathilda Place, Suite 300, Sunnyvale CA 94086**
**1.888.512.8906**
**crowdstrike.com**