IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

Momentum Builds: Fal.Con 2017, CrowdStrike Cybersecurity Conference

November 21, 2017

By: Frank Dickson, Christina Richmond

IDC's Quick Take

CrowdStrike passed a maturation "inflection point," holding its first user conference in San Diego from November 6 to 8. The theme of the event was the application of CrowdStrike's unique "big data" approach to endpoint security and the benefits it can deliver to its results from the platform and its analytics achieving critical mass. CrowdStrike's announcement of its new vulnerability management module, CrowdStrike Falcon Spotlight, was the most significant announcement of the event, which addresses the "failed patch" problem use case. The vulnerability module is a component that CrowdStrike adds to its current modularized offering, which is delivered from a cloud-assisted single endpoint agent and also includes antimalware, endpoint detection and response, managed threat hunting, IT hygiene, and threat intelligence.

Event Highlights

CrowdStrike held its user event in San Diego, California, entitled Fal.Con, from November 6 to 8, 2017. The event was the first of its kind for CrowdStrike, signaling a maturation of the company from new market entrant to one that actively needs to manage and invest in its user community.

IDC viewed CrowdStrike's announcement of its new vulnerability management module, CrowdStrike Falcon Spotlight, as the most significant. Now if you feel that maybe the world does not need another vulnerability management tool, IDC would not necessarily be in disagreement. The complexity of our security architectures and the proliferation of point products has certainly reached troubling problematic levels. However, attributes of CrowdStrike's vulnerability module make IDC a fan.

Falcon Spotlight addresses a valuable use case, the "failed patch" problem. Simply put, the "failed patch" problem exists when a patch is delivered to an endpoint but the patch is not applied because of any number of issues such as a need for reboot. The issue was illuminated to CrowdStrike during the WannaCry epidemic. CrowdStrike customers reported that their endpoints were patched while Falcon reported that a percentage of endpoints were still vulnerable. The new Falcon Spotlight module is intended to address such use cases in which vulnerability management tools report a patch success based on the device's registry listing of installed patches but that actually have suffered a failure in the installation process or delay in the application of the patch. Falcon Spotlight leverages applications and modules that are actually loaded in memory, providing real-time information on vulnerability status.

In addition, Falcon Spotlight is simply another analysis module, performing its analytics in the cloud and leveraging the same single agent used for the Falcon solution set. The module is practically 100% analytics, so there is nothing to install and upgrades to the Falcon agent are not needed. The existing endpoint agent provides all the endpoint sensory telemetry needed. Given the integrated nature of the feature in the solutions set, scans are essentially continuous rather than periodic. In addition, as new vulnerabilities are identified, the Falcon Spotlight can identify vulnerable systems in near real time.

CrowdStrike additionally presented its future road map. CrowdStrike's cloud-delivered, platform approach to endpoint protection has to be kept in mind when viewing the road map. Essentially, the endpoint agent provides three key functions: algorithmic protection, sensoring, and implementation. Thus new features on the road map are simply a function of cloud-based analytics, leveraging the sensor telemetry from the agent and implementing protection using the same agent. Future features look to address use cases such as insider threat, encryption/password management, application control, mobile, deception, and compliance. One future road map feature that is not necessarily platform driven is an integrated sandbox, which is quickly becoming a must-have feature in any modern endpoint security solution.

IDC was also very impressed with the level of focus on CrowdStrike's professional services. The services center upon and feature CrowdStrike products, but the company also incorporates third-party vendor products for incident response as required by the customer. Investments have been substantial into this side of the business, and significant growth has been the reward. We fully expect CrowdStrike to remain a top competitor in breach readiness and response as well as compromise and maturity assessment markets.

IDC's Point of View

CrowdStrike is certainly building momentum. It continues to roll out new, value-added features that leverage the analytics platform solution approach of its offering and enhance existing professional services. The road map is logical and promising.

The conference and its corresponding announcements were heavy on feature discussion but light on pricing details. Falcon Spotlight was not an exception, as prices were not announced. The most common objection that IDC hears about CrowdStrike from CISOs is that "it is expensive." Pricing is certainly a noteworthy attribute to discuss when considering CrowdStrike. However, please keep in mind that IDC is not necessarily implying that CrowdStrike is expensive or appropriately priced. CrowdStrike's offering though is more comprehensive than a traditional endpoint security solution, incorporating product, SaaS, and security professional services in its offering. Comparing CrowdStrike's Falcon complete solution set with a software-only endpoint security offering would not yield an apples-to-apples comparison. Granted, CrowdStrike has adjusted its pricing to be more modular, making comparisons more transparent.

In the professional services arena, CrowdStrike is also not underpriced — but then emergency services rarely are. However, the provider is quite flexible in its use of retainer dollars to extend preparedness and to further the security posture of its clients.

Subscriptions Covered:
Security Products, Security Solutions: Security as a Service