Carbon Black always has been a leader in anti-malware protection. Its approach was among the earliest to use cloud-based analysis along with threat intelligence. The result has been universally satisfactory and this product is no exception. Although Cb Defense has a lot of endpoint protection features, it really shows its malware roots. But among the high points of the product is its visualization. Visualization starts out fairly plain vanilla, but the deeper you drill down the more you understand what has happened in an attack and what is likely to continue to happen if the attack is allowed to go on. The level of detail is excellent and the graphical representation is intuitive. One little feature that can make a lot of difference is a space for you to take notes that are preserved with the record of the alert.

For our review, we dropped into the dashboard landing page. This is fairly typical of what we see in many other, similar products. However, when we started to drill down we got to an increasingly useful level of detail. Depending on who you are – executive, analyst, IT engineer, security engineer – you can drill into information that suits your individual requirements. We used some creative filtering to get rid of noise to leave us with events of particular interest or severity. That resulted in seeing an alert that appeared to be worth following up. More drill-down...

This got us to the graphical representation of the attack and its behavior on our enterprise. This allowed us to take manual action, but we could have set up policies that took the action automatically. The graphical representation allowed us to see exactly how the threat evolved within our enterprise including infection branches, PowerShell spawns and memory compromises among other things.

We always have been fans of Carbon Black. The company seems to have carved a niche in the area of threat intelligence applied to malware protection. This latest offering is typical of what we’ve expected to see from them. Their website is complete and their support is comprehensive. There is eight-hours-a-day/five-days-a-week standard support at no additional cost, plus the company offers premium support for an extra fee.

On large enterprises, this tool can be a bit pricey but for what it does it’s reasonable. The Carbon Black cloud system is quite advanced and the user experience is quite good making discovery and remediation of events efficient.

– Peter Stephenson, technology editor

Carbon Black Inc.
1100 Winter St., Waltham, MA 02451
United States
www.carbonblack.com
Sales: (855) 525-2489 • contact@carbonblack.com

Reprinted from SC Magazine, July 2017 • www.scmagazine.com