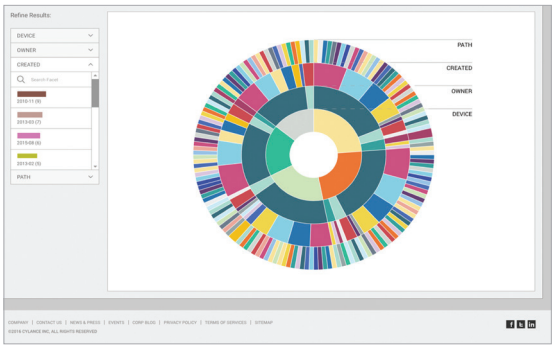

Cylance

CylancePROTECT with CylanceOPTICS

As many of our readers know, we've been Cylance fans ever since we designated them SC Lab Approved a couple of years back. In fact, we recently looked at them again in our One Year Later segment, so we won't spend a lot of time on the basic Cylance product, leaving us time for the new CylanceOPTICS option. One note of caution: While we have been at some pains to point out pricing among next-generation endpoint products – taking the position that they are a bit pricey for large enterprises – please note that the pricing here, while decidedly at the high end, is for the combination of CylancePROTECT and CylanceOPTICS. This makes the price a bit more reasonable, especially, as you will see, given the significant level of analysis and protection the combination provides.

CylanceOPTICS is, to put it simply, a set of sophisticated analyst tools that takes everything provided by CylancePROTECT and assists in the task of understanding what the data mean. CylancePROTECT is a next-generation anti-malware endpoint tool that has evolved into several other areas of endpoint protection, such as host-based intrusion detection monitoring and blocking, as well as remediation. With its backend AI engine and big data management in the Cylance cloud, the tool can perform deep analysis of a variety of malware, scripted and other events that may signal an attack against an endpoint. CylancePROTECT is predominantly an alerting tool, although there are some analytical capabilities exposed for the analyst and SOC engineer. CylanceOPTICS puts that relatively small bit of exposed analytics on steroids.

Cylance has all of the data necessary to perform advanced analytics and, in fact, it must do so to provide the level of alerting that it does. However, CylanceOPTICS applies those analytics in a user environment and they appear on the CylancePROTECT dashboard menu as an added option - if you deploy the new tool.

Once you have an artifact in analysis you can go to Focus and see all of the related events that preceded and followed the alert. This is laid out on a timeline with graphics that are quite clear. The chart shows the CylancePROTECT and all of the network events and running processes on the timeline.

Each device can be managed individually and details can be viewed easily. As we have reported before, the support and website for this product is first-rate. The CylanceOPTICS add-in can be downloaded or pushed out from the CylancePROTECT dashboard in exactly the same way that you deploy CylancePROTECT. When we have needed support from Cylance, it always has been fast and completely appropriate to the problem we were having. We needed a little help with this one and it was rapidly forthcoming.

– Peter Stephenson, technology editor

DETAILS

Vendor Cylance

Price Starting at $71.50/endpoint (up to 250 endpoints).

Contact cylance.com

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

OVERALL RATING ★★★★★

Strengths Quality is consistent with CylancePROTECT and it provides easy-to-use, meaningful analytics deriving from the wealth of data in the Cylance cloud.

Weaknesses None that we found.

Verdict If you are using Cylance-PROTECT this is a no-brainer. If you are not, it's a good reason to consider it. Because CylancePROTECT is one of our SC Lab Approved products, it already has our highest rating, but we are naming the OPTICS add-on Recommended for the value that it adds to PROTECT.

CYLANCE™
18201 Von Karman Ave., Suite 700
Irvine, CA 92612
1-844-CYLANCE
www.cylance.com