Cylance jumps into detection and response fray with new release

FERNANDO MONTENEGRO, PATRICK DALY
14 JUL 2017

Looking to capitalize on the broad aversion to multiple security agents on the corporate endpoint and capture a bigger piece of the endpoint security pie, Cylance has launched CylanceOPTICS, a detection and response product.
Vendors competing in the endpoint security space have three main dimensions to address: functionality, nonfunctional requirements and business. The first entails effective prevention in the face of constantly changing tactics, in addition to activity data that security teams need to respond to new or emerging threats. Nonfunctional requirements include resource consumption, changes to operational processes and integration points with other security components. The business dimension represents how well the vendor competes and stands out in a crowded marketplace, making it easy for prospects to evaluate the merits of the offering and incorporate it into their procurement processes.

As with other vendors, Cylance has been competing on all these fronts. Its CylancePROTECT offering was originally focused as a replacement for legacy antivirus/anti-malware offerings, with an emphasis on being easy to deploy and operate. The company has found an audience for its message, and has been active in the market since the product release in 2014. It has now released a detection and response module called CylanceOPTICS.

THE 451 TAKE
We have seen a consistent trend toward consolidation in the endpoint security space. Functionality that used to be offered as independent products – disk encryption, host firewall/IDS and others – is eventually incorporated into broader product suites or basic OS functionality. With the rise of multiple segments in new approaches to endpoint security, this consolidation continues, most notably in products that combine detection and response capabilities with threat protection. Cylance has seen moderate success with its initial protection-based offering. The release of CylanceOPTICS attempts to capitalize on this brand recognition, adding detection and response capabilities via an additional module. Cylance is among those poised to break from the pack of endpoint upstarts, and is aiming higher in the market, with brand recognition and a message of replacing existing solutions rather than coexisting. Its success in doing so will depend on meeting the multiple customer needs that drive an endpoint security deployment to begin with – an effective security offering meeting both security and compliance needs, able to be deployed efficiently, from a reputable vendor that is easy to deal with.

CONTEXT
Cylance has been making waves in the information security world since it was founded in 2012 by CEO Stuart McClure (previously Global CTO at McAfee) and chief scientist Ryan Permeh (previously chief scientist at McAfee). According to 451 Research’s Q1 2017 Voice of the Enterprise: Workloads and Key Projects survey, enterprise IT decision-makers were more likely to consider Cylance’s products more innovative than any other vendor. The Irvine, California security vendor has exhibited rapid growth since inception, and is backed by $177m in venture funding spread across four rounds. The most recent funding came in the form of a $100m series D round, led by Blackstone Group (Tactical Opportunities) and Insight Venture Partners, that resulted in a $990m pre-money valuation. Cylance primarily markets its endpoint protection products to the critical infrastructure, education, energy, finance, healthcare, government and retail industries. The company employs approximately 800 people, although it recently went through a round of layoffs.

TECHNOLOGY
Cylance is among those capitalizing on the values of cloud-based delivery to alleviate demands on local infrastructure; its offering is implemented by a combination of multi-tenant cloud hosted infrastructure and the endpoint agent itself. The company claims the agent uses 1-3% of CPU and 40MB of memory, and takes up to 1GB of local disk space, used by both the endpoint functionality and as a data store for relevant security information. This approach leads to a reduced footprint and simpler deployment model, although it does so by making architectural trade-offs that not all organizations may want to make, such as storing security-relevant information directly on the endpoint.
The cloud-based component of the infrastructure is hosted on Amazon Web Services and is claimed to number in the thousands of virtual machines. It provides back-end services such as management interfaces for the individual deployments, including integration with SIEM if desired, as well as implementing the machine-learning functionality at the core of the Cylance offerings. Initially, the Cylance endpoint agent provided protection capabilities under the ‘Protect’ moniker. The company advertises its use of machine learning and artificial intelligence to perform predictive analysis with a high degree of confidence, to determine whether a particular file – be it .EXE, .DLL, .SYS or other type of file, as well as attachments – is malicious. Since its initial release, it has also introduced mechanisms for memory protection aiming to defend against ‘fileless’ malware.

The company claims it analyzes ‘up to six million code features’ for each file. In practice, this likely means that the company’s machine-learning pipeline is trained on datasets with large numbers of features that are then used to generate a model for implementation on the endpoint. That model is then applied to local files at load or execution times without requiring a network connection. This is useful for scenarios where network connectivity is non-existent or unstable, such as in public Wi-Fi zones.

The new addition to its offering is named CylanceOPTICS, which was released earlier this year, with an update in the late spring. CylanceOPTICS is targeted at providing detection and response capabilities to a Cylance deployment, and is being marketed as an ‘incident response’ and ‘threat hunting’ offering – a strategy that has characterized endpoint detection and response technology from the segment’s beginnings.

CylanceOPTICS is implemented as an additional system service on the existing agent, and creates a local data store of up to 1GB on each endpoint to store security-relevant data. The key capabilities offered by CylanceOPTICS include performing distributed searches for typical indicators of compromise (IOCs), such as file type, hashes and others, in addition to some timely response capabilities. The distributed searches can be used to support typical IR functions, such as activity validation, root-cause analysis and investigative searches. For response capabilities, users can take response actions such as quarantining files and quickly locking down endpoints. Plans for an upcoming release scheduled for later in the year include supporting automated responses that can be configured based on a threat-detection engine.

Overall, this combined protection and detection/response offering has the potential to simplify operations for a response team, allowing them to use the same infrastructure for investigation and forensics that they use for threat protection. Operationally, it is potentially advantageous to reduce the number of distinct products running on the endpoint by having detection/response and prevention on the same infrastructure. This approach may fit well with organizations that have significant resource constraints on their response/hunting teams.

**STRATEGY**

In addition to working on product engineering and traditional sales/marketing pursuits, Cylance has been pursuing an aggressive campaign around the evaluation of security products. Recently, the company has been vocal in challenging the ecosystem built around third-party security testing, even as it joins initiatives such as Virus Total and the Anti-Malware Testing Standards Organization (AMTSO), and participates in vendor bake-offs and third-party tests. The company publicly claims that most current test environments do not reflect the reality of customers’ environments or the product capabilities of modern solutions such as its own. It also contends that the current cost structures around vendor testing skew toward supporting larger vendors with deeper pockets to support multiple testing rounds.

As an alternative, the company recommends that customers conduct their own testing. This approach does have its benefits, but it also introduces costs to the overall transaction that not all customers will be willing to bear, as well as variability in approach from one customer to the next – variability for which vendors may seek to compensate by offering an evaluation approach. The drawback of that course of action is that vendors may be subject to charges of promoting an evaluation that favors their own product. The AMTSO seeks to address that issue in anti-malware testing by equipping evaluating organizations with a transparent and consistent set of techniques to overcome these and many other issues that have plagued product testing in the space to date.
**COMPETITION**

The overall endpoint security market has one of the largest sets of competitors in the information security industry, covering the entire spectrum – from stalwarts such as Symantec, Trend Micro, McAfee, Sophos and Kaspersky Lab to the myriad challengers in various stages of evolution and functionality. It is within this market that Cylance finds itself, often grouped alongside Carbon Black, Endgame, SentinelOne and (until its recent acquisition by Sophos) Invincia. These vendors aim to capitalize on the high levels of dissatisfaction expressed by customers when referring to their current endpoint vendors, while claiming the mantle of post-AV protection and detection capabilities.

As Cylance wades further into the detection and response market, it will face established vendors such as FireEye/Mandiant, Tanium and Guidance Software, as well as upstarts such as CrowdStrike, CounterTack and Cybereason. In this section of the market, success will require a combination of product functionality alongside a robust ecosystem of threat-intelligence sources and services to assist customers. Cylance’s heritage may be an asset in this case.

**SWOT ANALYSIS**

<table>
<thead>
<tr>
<th>STRENGTHS</th>
<th>WEAKNESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cylance's message of machine learning has been accepted by a number of customers and given it more visibility in a crowded marketplace. Its technical architecture can be appealing for those customers looking for simplified footprints. Adding detection/response as a module to the existing product can simplify procurement for customers in both segments and strengthen vendor relationships - all reasons why we expect to see consolidation in this space continue.</td>
<td>The resiliency of the product may be challenged by sophisticated adversaries that can delete local data. The functionality offered by the newer module may lag established detection and response vendors.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OPPORTUNITIES</th>
<th>THREATS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise customers are often unsatisfied with the many options available for endpoint security. Cylance’s offer to simplify footprint can be appealing, which may augment the company’s traction to date in the emerging field of post-AV endpoint security.</td>
<td>The endpoint space is fiercely competitive, and all vendors - both established and upstarts - keep the pace of innovation high and the jostling for position among customers anxious to improve endpoint security very active.</td>
</tr>
</tbody>
</table>