REPORT REPRINT

Carbon Black brings its community together and releases new cloud-centric threat hunting

FERNANDO MONTENEGRO

12 NOV 2018

Simplified operations and faster product releases are usually among the many potential benefits of cloud adoption. Endpoint security vendor Carbon Black is betting on these as it consolidates its offerings around its cloud architecture and releases new products at an accelerated pace.

451 Research®

As customers adopt more modern, cloud-based infrastructure options, they expect to be able to reap the benefits not only directly, but also indirectly by having their existing vendors adopt these patterns themselves. In the endpoint security space, this translates into being able to leverage cloud-based endpoint security management, which removes much of the operational legwork needed for managing endpoint security across a large fleet. Endpoint security vendor Carbon Black very much wants to be a key player in that space, and the company took a stance with the announcement of its Predictive Security Cloud (PSC) platform earlier this year. At its user conference in early October (Cb Connect), Carbon Black reported on this strategy and released new functionality for advanced threat hunting in the cloud.

THE 451 TAKE

As organizations of all sizes scramble to do more with less, there's increased appetite for reviewing existing security practices. Gone are the days of heavy lifting to support endpoint security, and vendors need to show not only security functionality, but also efficient operations and agility to respond to market demands or to new threats. Carbon Black placed strong emphasis on its cloud-centric approach, and the results appear positive: customers are accepting the delivery model, and the company was able to release new functionality based on its Predictive Security Cloud. The adoption of technology such as 'osquery' points to an understanding of how to incorporate community-driven innovations. The cloud-based model should also allow the company to quickly incorporate additional functionality on its offering, particularly as it competes with vendors with, in some cases, broader portfolios. If Carbon Black can demonstrate that it can use its cloud to offer more with minimal effort by the customer, the results will likely be positive.

CONTEXT

Waltham, Massachusetts-based endpoint security vendor Carbon Black went public in 2018 and trades on the Nasdaq. The company has roughly 1,200 employees and additional offices in Japan, Australia, Singapore and the UK. Carbon Black is led by CEO Patrick Morley and claims to have roughly 4,600 customers across several verticals and geographies. The Cb Connect conference took place in New York and hosted about 700 people consisting of Carbon Black staff, customers and partners, including both technology and service provider partners.

STRATEGY

Carbon Black's strategy is centered around capturing the momentum from the broad industry shifts unleashed by digital transformation. This allows the company to capitalize on customers looking to consolidate elements of their security architecture. There are four dimensions to this: cloud, community, APIs and partners.

Last year when Carbon Black released its 'Predictive Security Cloud,' leveraging the assets it acquired with Confer, it indicated it saw cloud as the centerpiece of its strategy. Cloud-delivered services offer significant efficiencies for the vendor and customers alike. While Carbon Black can have much better control over how its functionality is consumed and is able to quickly innovate and release new products, customers benefit from a much simpler back-end management effort, easier rollouts of new products, and cloud-based analysis of streams of endpoint activities and behavior. Also key to Carbon Black's strategy is its focus on enabling collaboration among the user community. The company announced it has more than 17,000 security and incident response (IR) users within its community, sharing lessons learned, developing repeatable playbooks, sharing IOCs and watch lists, and pushing the boundaries of integration between Carbon Black products and others.

Carbon Black places strategic importance on continuing to support integrations with other security products by offering open APIs for all platform capabilities. This enables other tools to leverage endpoint data to provide additional context surrounding attacks, in addition to enabling other tools to leverage endpoint remediation capabilities offered through Carbon Black's products. The flexibility of extending how a product will work within one's environment is a welcome capability not only for customers themselves, but for partners as well. Technology partners can fine-tune product integration, while services partners can easily integrate the products into their internal workflows.

The focus on a strong partner ecosystem completes the approach. As customers look to partners to address areas outside their core competencies, or areas where they have a skills shortage, Carbon Black promotes both service and technology partners, which have a multiplier effect for the company. Key partnerships include Red Canary, Secureworks, IBM, VMware and Kroll, but the broader ecosystem includes more than 100 partners overall.

PRODUCTS

The centerpiece of Carbon Black's architecture is its Predictive Security Cloud, which aims to secure endpoints by continuously collecting unfiltered data from the endpoints under management, then apply streaming analytics to the data to detect and stop malicious behavior. Also available on the platform is the ability to query real-time current state, which helps both security and IT teams investigate attacks and vulnerabilities. The company then looks to provide additional new services on top of this platform and migrate functionality to it as appropriate.

The PSC is derived from the cloud-native endpoint protection platform it acquired with Confer. 'Cb Defense,' its NGAV offering, is the first product Carbon Black brought to market on the PSC. The product aims to provide a replacement for legacy antivirus protection, which the company claims that 70% of its Cb Defense customers use the product for. The product has endpoint detection and response capabilities that help users understand attacks and remediate issues. The company also offers a VMware-optimized version of Cb Defense, aimed at more efficiently using virtualization technology to deploy endpoint security to virtual machines in the datacenter.

Cb ThreatSight is a managed alert monitoring and triage service, using Carbon Black experts to assist resource-constrained teams.

Cb LiveOps is one of the new services released on Carbon Black's PSC this year, and it aims to provide immediate query capability across the endpoint fleet. The objective is to complement the 'unfiltered data' that is normally obtained with Cb ThreatHunter or Cb Response with additional environmental data. This capability is built on top of 'osquery,' an open source project for endpoint querying using standard SQL. Carbon Black is one of the initial vendors adopting the technology, and it plans to complement that with its Live Response remote access remediation capability, which can also be scripted via APIs.

At Cb Connect, Carbon Black announced the launch of Cb ThreatHunter, which is a cloud-based threat hunting and IR service that incorporates functionality inspired by Cb Response. It will be generally available in November. The product currently supports Windows endpoints, with additional OS coverage to follow. Cb ThreatHunter offers new advanced search capabilities; plus, it leverages the single agent, single console and elastic scalability offered through the Predictive Security Cloud platform. The company expects Cb ThreatHunter will be the migration path for Cb Response customers that want a cloud-based offering.

Carbon Black still maintains and is committed to its earlier products. Cb Protection is the application control technology originally from Bit9. Application control is a powerful mechanism against unauthorized executions, but it best suits organizations that are committed to controlling change and value the level of protection that a default-deny posture brings. The product is primarily used through on-premises deployments, but Carbon Black indicated that supporting cloud-based deployments is on its roadmap.

The company also indicated that it continues its commitment to Cb Response, widely used by SOC teams and IR vendors for threat hunting and incident response. The product is well received by customers and partners, notably MSSPs that use it as the basis for their services. It is available on-premises or in the cloud. The product supports continuous recording of unfiltered endpoint data, query and watch lists, Live Response remote remediation, and extensive open APIs.

The company disclosed that its roadmap includes improvements to its PSC infrastructure, improved coverage for other operating systems and new services. Planned PSC infrastructure improvements include more granular role-based access control, localization and certifications. The operating system support will expand Cb ThreatHunter, Cb Defense and Cb LiveOps to Linux, as well as provide better support for container and cloud workloads. Finally, the company expects to add support for detection of unmanaged/rogue devices, vulnerability management, compliance and application control on the PSC.

COMPETITION

With networks growing less visible and users having more mobility, visibility on the endpoints – be it the endpoint itself or on the application side – is becoming critical. Numerous vendors have released endpoint-centric security tooling. The main competition for Carbon Black stems from the broad pool of other enterprise-focused vendors, ranging from longstanding endpoint security vendors to newer entrants. Symantec, McAfee, Trend Micro, Kaspersky Lab and Sophos are representative of the first group, as are FireEye, Tanium and RSA Security. Carbon Black faces newer entrants as well, primarily Crowdstrike and Cylance, but also Cybereason, Endgame and SentinelOne.

Carbon Black's cloud-centric architecture is a model that other security vendors have embraced. Qualys was one of the first vendors to offer this delivery architecture, and it has waded into endpoint security as well. Palo Alto Networks is on a path for bringing together endpoint security data with other network and cloud-centric products. In addition to these and other vendors, Microsoft itself stands out as aggressively working on improving endpoint security with its Defender endpoint product and Defender ATP offering, which is heavily cloud-centric. Finally, the market dynamics of increased native protection in endpoints is driving several endpoint security vendors to add endpoint detection and response capabilities to their suites. The list includes Bitdefender, ESET, F-Secure and Webroot.

SWOT ANALYSIS

STRENGTHS

Carbon Black's cloud-centric vision can potentially provide significant operational benefits over traditional approaches. The company's focus on robust APIs and community integration is a strong positive, as is adoption by several MSSP partners.

WEAKNESSES

Even as the company recognizes the importance of Linux workloads in cloud deployments, the support for newer types of workloads such as containers appears to be further along the roadmap.

OPPORTUNITIES

As organizations rethink their security strategies and consider technology refreshes and changes in operations practices, a streamlined cloud-centric approach may offer significant benefits, particularly if it can help consolidate additional security functionality.

THREATS

Endpoint security is a highly competitive environment, and larger enterprises may prefer to align with vendors with a broader security portfolio.