Carbon Black.

Carbon Black Introduces CB ThreatHunter, Delivering Advanced Threat Hunting and Incident Response (IR) Capabilities on the CB Predictive Security Cloud™ (PSC)

October 10, 2018

CB ThreatHunter leverages unfiltered data on the PSC, an endpoint security platform with a single agent and single console to consolidate prevention, detection, response, managed services and advanced threat hunting

WALTHAM, Mass. and NEW YORK, Oct. 10, 2018 (GLOBE NEWSWIRE) -- Carbon Black (NASDAQ: CBLK), a leader in next-generation endpoint security delivered via the cloud, today introduced CB ThreatHunter, delivering powerful, new, advanced threat hunting and IR capabilities on the CB Predictive Security Cloud (PSC). The new offering will be the fourth service delivered on the PSC this year. The CB ThreatHunter announcement was made from the company's sold-out annual user conference, #CBConnect18, in New York.

Tweet this: The CB Predictive Security Cloud gets stronger! @CarbonBlack_Inc announces CB ThreatHunter, delivering advanced threat hunting & IR capabilities in the cloud leveraging unfiltered data, one agent and one console – http://ow.ly/B0i030m90G4 #infosec #threathunting #CBConnect18 #PSC

"One year ago at CB Connect in San Francisco, we outlined our vision to rapidly extend the CB Predictive Security Cloud to make it easier for our customers to move off legacy AV and address multiple security use cases through a single cloud platform and single sensor," said Patrick Morley, Carbon Black's Chief Executive Officer. "With the addition of CB ThreatHunter, this market-leading platform will have five offerings and delivers customers the ability to prevent, detect, respond to, predict and now, hunt threats in the cloud using a single agent, single console and single platform."

LIVESTREAM: Sign up to view a livestream of the #CBConnect18 keynotes by clicking here

---

Adding Advanced Threat Hunting to the PSC

CB ThreatHunter is delivered through the PSC, Carbon Black's powerful endpoint protection platform that consolidates multiple critical endpoint security capabilities supporting both IT and security operations, including: next-generation antivirus (NGAV) + endpoint detection and response (EDR); advanced threat hunting and IR; virtualized data center security; real-time endpoint query and remediation; and managed threat hunting and triage.

Threat Hunting Powered by Continuous Collection of Unfiltered Data

Most EDR and IR tools on the market collect only a limited set of historical data. As a result, SOCs and IR teams struggle to get their hands on the information they need to investigate, proactively hunt and remediate.

CB ThreatHunter solves this problem by continuously collecting unfiltered data, giving security teams all the information they need to: proactively hunt threats, uncover suspicious behavior, disrupt active attacks, repair damage quickly and address gaps in defenses. Investigations that often take days or weeks can be completed in just minutes with CB ThreatHunter.

"CB ThreatHunter has simplified incident response by allowing quick discovery of both simple and advanced threats, and quickly making decisions to take conclusive actions," said Denis Xhepa, IT Systems Security Engineer of MidCap Financial Services. "Its simplicity and responsiveness are amazing, especially when you are running an investigation where every minute matters. When I find something, I can prevent it for the future, and also look for other related or similar things. All this can be done very intuitively. Anomaly detection is also going to be enhanced by the backend intelligence applied to the data. Endpoint security ***used to be*** difficult."

"The combination of rapidly searchable, unfiltered endpoint data for advanced threat hunting, combined with an array of prevention and response capabilities built-in to one endpoint sensor is a significant step forward. CB ThreatHunter further enhances our ability to deliver rapid incident detection and response to our global customers," said Marc Brawner, Principal at Kroll's Cyber Risk practice.

Inspired by CB Response, an EDR market pioneer with more than 2,000 active customers, CB ThreatHunter is a brand new product, built from the ground up on the PSC, offering security teams advanced threat hunting and IR capabilities, including:

More Powerful Search Fields: CB ThreatHunter equips security teams with the ability to flexibly hunt threats, even if an endpoint is offline. With this level of visibility, researchers can see what happened at every stage of an attack with intuitive attack-chain visualizations, and uncover advanced threats, while minimizing attacker dwell time. This insight provides immediate answers with comprehensive behavioral context to stop attacks as quickly as possible.

Enhanced Threat Intel Matching: CB ThreatHunter's sophisticated detection combines custom and cloud-delivered threat intel, automated watchlists and integrations with the rest of the security stack to efficiently scale hunting across the enterprise. This advanced level of detection allows security teams to proactively explore environments for abnormal activity, leverage cloud-delivered threat intelligence and automate repeat hunts. Additionally, the PSC's platform extensibility allows developers to create custom watchlists to power real-time detection and correlate data across the security stack.

Elastic Cloud Scalability: CB ThreatHunter is natively built on the PSC, allowing security teams to rapidly deploy and scale the solution across their enterprise without investing in (or maintaining) on-premise infrastructure. By eliminating these costs and processes, CB ThreatHunter enables teams to simplify their operations and focus their energy on hunting and responding to threats.

CB ThreatHunter will be generally available in November 2018.

Resources
CB ThreatHunter Blog
CB ThreatHunter Data Sheet
CB Predictive Security Cloud
Register Today: Become a Threat Hunter
#CBConnect18

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the CB Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) enabling customers to defend against the most advanced threats. More than 4,300 global customers, including 35 of the Fortune 100, trust Carbon Black to keep their organizations safe.

Carbon Black Contact
Ryan Murphy, Carbon Black
Senior PR Manager
rmurphy@carbonblack.com
917-693-2788

Carbon Black.

Source: Carbon Black, Inc.