PARTNER SUCCESS STORY

Strengthens means of identifying and responding immediately to threats

Provides an increased amount of information to correlate and make better decisions to stakeholders

Streamlines ability to ask questions of endpoints en masse

Charles River Associates Improves Incident Response Times with VMware Carbon Black Cloud

Charles River Associates (CRA) is a global consulting firm that specializes in cybersecurity and incident response (IR), providing services to help their clients respond to, recover from and best mitigate future cybersecurity threats. Bill Hardin, VP at CRA, explains that the majority of CRA's projects involve ransomware, extortion, business email compromise, nation-state attacks, insider threats and malware outbreaks.

For ransomware events, clients may have up to 10,000 devices on their network with over 75 percent of them encrypted. To best address the broad spectrum of IR matters, CRA relies on VMware Carbon Black Cloud™, an advanced, cloud native endpoint protection platform (EPP) built with intrinsic security, to assist them with containment, eradication and ongoing monitoring of clients' environments.

Matt Ahrens, who has managed hundreds of ransomware investigations from RYUK, BitPaymer, Sodinokibi and all other types of ransomware, states "we use VMware Carbon Black in our processes and in assisting our clients to limit disruptions so they can get back to normal operations."

INDUSTRY

Consulting

HEADQUARTERS

Boston, Massachusetts

ABOUT THE PARTNER

Charles River Associates is a global consulting firm that specializes in cybersecurity and incident response, providing services to help their clients respond to, recover from and best mitigate future cybersecurity threats.

VMWARE FOOTPRINT

VMware Carbon Black Cloud Endpoint™ Standard
VMware Carbon Black Cloud Audit & Remediation™
VMware Carbon Black Cloud Enterprise EDR™

Quicker Insights, Faster Response Times, Less Disruption

In a recent incident, a healthcare provider initially discovered an event based on the identification of encrypted files on their network. They contacted CRA to help respond to the massive disruption affecting the vast majority of their computers. CRA brought in VMware Carbon Black to help identify and enumerate the encryption software, contain and eradicate the malware, and monitor the network going forward.

CRA used VMware Carbon Black Cloud Audit and Remediation to "very quickly get questions and answers from the endpoints, and then orchestrate that at a larger scale." During the engagement, their initial queries looked at persistence mechanisms via scheduled tasks, autoruns and so on, followed by the analysis of various file locations for the identification and enumeration of files on the network.

The Live Response and Live Query functionalities of the platform were a huge benefit during the IR engagement. According to Ahrens, CRA was able to "collect information quickly via Live Query to narrow the scope of where we needed to access it via Live Response." Live Query provides fast answers and Live Response delivers reliable answers–using them together gives CRA the best results possible.

"The value of Carbon Black Cloud Audit and Remediation is the speed and the ability to quickly ask questions of endpoints en masse," notes Ahrens. From a time savings perspective, "it provides me with more information to correlate and make better recommendations to lawyers and the client engagement teams. Before using VMware Carbon Black, I would be pulling information from multiple data sources to seek the answers I need rapidly. The Live Query function enables our teams to quickly gain insights into the situation."

Providing the Best-of-Breed Endpoint Threat Detection and Response

According to Ahrens, the most predominant issue organizations face today is phishing. Business email compromise continues to plague the industry, and *the FBI has estimated that business losses in 2019 were more than $1.7 billion.* The psychology that threat actors use to trick clients to click on documents and links they should not can bring all sorts of disruption to the organization. In addition to phishing, Ahrens sees misconfiguration of appliances that are internet-facing, users who have the same password on multiple systems, as well as clients not applying patches to systems in a timely manner, which allow threat actors to gain access to the network.

According to Ahrens, one way companies can improve their security hygiene is to employ an email protection solution, where companies can better identify and understand the contents of an email, the documents with macros and more from a deployment perspective. Another recommendation is to have an endpoint detection and response (EDR) solution in place. For example, VMware Carbon Black Cloud Endpoint Standard is a moderate option, and for teams who want something more advanced, there's Carbon Black Cloud Audit and Remediation, and VMware Carbon Black Cloud Enterprise EDR. VMware Carbon Black Cloud is also effective in its ability to identify the malware's signatures and its actions too.

The value of VMware Carbon Black Cloud is that "the interaction between the EDR product and the Live Query side is a continuous feedback loop. You identify an indicator you want to search for that may be latent inside the EDR functionality, then you go ask a question of all the endpoints on the network that may identify it, then you feed back the response with the Live Response sessions to make sure it's actually contained."

> "VMware Carbon Black Cloud Audit and Remediation provides me with more information to correlate and make better decisions to lawyers and the client engagement teams."
>
> MATT AHRENS
> PRINCIPAL, CHARLES RIVER ASSOCIATES

Looking ahead

Ahrens notes that in the IR world, and for CRA specifically, "everything we do must be able to contain and eradicate the disruption as well as be scalable and quick to deploy." Thankfully for Ahrens, "VMware Carbon Black is scalable and responds quickly, so having this tool available to ask quick questions of endpoints and not worry about what's online or offline … increases value to our team."

As a valued member of the VMware Carbon Black IR Partner ecosystem, CRA is appreciative of the commitment VMware Carbon Black has to providing the highest level of support. Hardin summarizes our relationship as being "instrumental in both companies' visions of creating a dynamic that keeps organizations safe and proves very resourceful when attacks come from threat actors."

vmware Carbon Black

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com