Partner Story

DeepSeas helps clients intercept advanced attacks faster with Carbon Black

For more than three decades, DeepSeas has been keeping mid-market and enterprise organizations secure with in-depth cyber defense services and threat analytics that cover the entire converged attack surface. Over 700 clients across every industry rely on this team of threat intelligence experts, security analysts, and executives to help them close their security gaps and mitigate incidents.

Industry

Computer and Network Security

"The biggest reason our customers choose Carbon Black XDR is due to the extra telemetry data captured beyond traditional EDR. Other vendors simply cannot provide that same experience".

Mike Johnson
Vice President of Global Partners & Alliances
DeepSeas

Partner

DeepSeas is a Managed Detection and Response (MDR) partner helping customers solve the most complex requirements of their IT environments.

Carbon Black footprint

- Carbon Black XDR
- Carbon Black Enterprise EDR
- Carbon Black Vulnerability Management

The problem

DeepSeas is committed to meeting clients wherever they are in their cyber journey. Unfortunately for many of those clients, that means seeking help from the company after experiencing a service-impacting breach.

"Many prospective clients have felt the severe pain of a breach, and their businesses needed quick recovery and then ongoing managed detection and response to prevent that pain from returning," shared Mike Johnson, Vice President of Global Partners and Alliances at DeepSeas.

It's common for DeepSeas to serve in an overwatch capacity after an incident has been reported to a business's insurance firm. While the investigation is carried out, DeepSeas is put in charge of ensuring the situation doesn't escalate. That means keeping a very close eye on everything happening in the client's environment—and the ability to get up and running at lightning speed.

The DeepSeas team has the right expertise for the job in-house, but finding the right tech has been a moving target. At times, DeepSeas deploys point software from legacy network security tool vendors to capture the telemetry. They know the value of network appliances, having developed their own long ago, but shipping, deploying, and integrating the 1U server is complex. Also, the exorbitant cost would have to be passed through to the client. Considering this, the team turned to Carbon Black's innovative endpoint detection and response solution.

The solution

Today, DeepSeas can rapidly install Carbon Black Enterprise EDR into a client's environment and feed its telemetry and high-fidelity alerts into the DeepSeas Cyber Defense Platform. There, the DeepSeas team can easily view threat detections, execute a pre-arranged playbook, and notify the client.

As of 2023, DeepSeas is also deploying Carbon Black's eXtended Detection and Response (XDR) solution, which increases visibility to endpoints, network, cloud workloads, identity intelligence, and more—and it doesn't require the client to replace existing solutions or contend with physical network taps to their infrastructure.

To supplement this technology, a dedicated Carbon Black team collaborates closely with DeepSeas to ensure their team of experts are fully enabled with product training, integration support, and sales guidance.

The results

Together, Carbon Black and DeepSeas have turned into a Managed XDR powerhouse. Rapid deployment is no longer an obstacle, nor are exorbitant costs. And most importantly clients are more secure than ever, with a faster end-to-end process of detection, investigation, and response.

“The time-to-resolution for incidents has been greatly reduced, and we’re able to protect our clients from advanced threat vectors,” said Johnson. “When an attacker meets a DeepSeas client, they will likely move on to a lesser defended business where it’s easier to meet their objectives.”

Carbon Black’s ability to provide network threat detection has also proven to be an invaluable asset—something a client discovered when attackers attempted to invade their business using Cobalt Strike, a red team pen testing toolkit hijacked by malicious actors. Fortunately, Carbon Black detected the “Beacon” agent and prevented attackers from communicating through the infected host.

Incident response (IR) overwatch has also become easier. Roughly 30 times per month, DeepSeas deploys Carbon Black in a client’s environment to assist in recovery and protect them moving forward. Overwhelmingly, these clients choose Carbon Black over other vendors.

“Our SOC analysts and threat detection engineers are highly skilled individuals, and they could use many tools to do their job,” says Johnson. “The fact that they are executing at our high standard with Carbon Black is all you really need to know. If the tool wasn’t excellent, we wouldn’t use it.”

Looking ahead

With Carbon Black and DeepSeas combined, clients are benefiting from unmatched technology and top cyber defense expertise. Moving forward, DeepSeas and Carbon Black will be evaluating other innovations, including Carbon Black’s Cloud Native Detection and Response (CNDR) and Host-Based Firewall solutions, to further the joint mission of continuously delivering enhanced security to clients.