Case Study

BINARY DEFENSE™

Aluminum boat manufacturer enlists Binary Defense to help protect from ransomware and malware attacks

Business

Manufacturer of aluminum commercial and recreational boats serving the Pacific Northwest (US).

Challenges

One person IT staff handles all aspects of IT for the business

Several ransomware attacks over a five-year period halted business operations until data was restored from backups

Employees unaware of cybersecurity best practices, such as recognizing suspicious links and phishing emails

Results

Binary Defense is an extension of the team, monitoring 24/7/365 through the Security Operations Center

Binary Defense Managed Detection & Response can detect suspicious activity, such as a ransomware attack, immediately

Customer has peace of mind that Binary Defense is monitoring the company's network

---

"Network and port-wise, if something starts encrypting, the Binary Defense MDR software is going to pick up on that. Sooner or later it's going to hit a honeypot file. At that point Binary Defense would step in, and we are going to mitigate it." – Fred Warren, Chief Information Officer, North River Boats

Manufacturer of boats with small IT staff faced ongoing ransomware threats

Located in Oregon, North River Boats is the largest manufacturer of custom aluminum boats for commercial and recreational use. Founded in 1994, the company employs close to 150 staff. Of those, 50 are office employees. Fred Warren is the Chief Information Officer, but is the sole IT staff member, and thus has responsibilities that run the gamut from running cables to maintaining the network infrastructure, and everything in between. "I will change hats at any given moment," Warren said of his day-to-day responsibilities.

This is not an unusual story for companies of this size. Typically, one full-time IT staff member fulfills all the responsibilities of maintaining the network for an organization. Security is just a fraction of the job. Unfortunately, this makes organizations prime targets for cybercriminals. "As attacks are becoming more sophisticated, even with training it is difficult for employees to know what a weird attachment or suspicious website looks like," Warren said.

Three ransomware attacks over a five-year period brought the company to a halt temporarily after each attack. "This is despite having current, up-to-date antivirus," Warren said.

For years, North River Boats has relied upon multiple backups of data to ensure nothing was lost in the event of a breach. Warren maintains backups onsite and offsite, separate from his corporate network so it would not be affected by a breach of that network. After each of the three ransomware attacks, Warren had to restore his system from those backup files. He realized this was not an efficient cybersecurity strategy.

Deception techniques set Binary Defense apart from other MDR vendors

In speaking with colleagues in IT who had faced similar challenges, Warren learned that those organizations had leveraged managed security services providers to provide next-generation protection beyond antivirus. He discovered Binary Defense.

Binary Defense Managed Detection & Response (MDR) is proprietary, flexible and scalable cloud-based software combined with expert monitoring by expert analysts to protect businesses from emerging threats that can't be found with traditional security tools. Binary Defense behavior-based technology uses multiple sources to correlate indicators of compromise and attack. The Security Operations Task Force analysts are an extension of a company's IT team, providing 24/7/365 coverage to monitor, detect and alert the customer if suspicious activity occurs.

Binary Defense MDR, SOC

Protects businesses from ransomware, phishing and other cyberattacks

24/7 around-the-clock event monitoring

Real-time analysis of threat behavior

Lightweight and easy deployment

Expert and trusted extension of your team

"No one has had to call me at two in the morning. That makes me very happy." – Fred Warren

Warren evaluated several MDR vendors, but one differentiator that influenced his choice to go with Binary Defense was their use of honeypots as a deception technique. "No one else that I evaluated was doing this," Warren said. "Network and port-wise, if something starts encrypting, the Binary Defense MDR software is going to pick up on that. Sooner or later it's going to hit a honeypot file. At that point Binary Defense would step in, and we are going to mitigate it."

Binary Defense also stood out to him because of the expertise of the analysts in the Binary Defense Security Operations Task Force. "I had a network issue and was doing some troubleshooting. I was looking into different possibilities and starting to panic a little bit. I could have a hacker on premise compromising some or most of my equipment. Then I thought, wait a minute, I have Binary Defense," Warren said. "There's no way I have this activity happening without them noticing. I was able to have confidence in Binary Defense and could focus on determining the cause of the problem."

Confidence in Binary Defense's expertise allows focus on other areas

Warren noted that in the year that North River Boats has been using Binary Defense Managed Detection & Response, they have not had another ransomware attack. "It has made my job much easier," Warren said. "Binary Defense has given me the confidence that I don't have to assume I'm operating in a state of emergency if an issue arises. I can look at things more likely to be wrong than have to go after a network security issue."

"No one has had to call me at two in the morning, which makes me very happy," he added. "I haven't had to clear spyware off of anyone's system. I haven't even really thought about it. It's been hassle-free and worth the money."