Case Study

Binary Defense helps one-person IT staff keep marketing agency data secure

Business

Marketing agency serving clients in the US with a strong focus on healthcare clients

Challenges

Single IT staff member responsible for all aspects of IT across the organization with security as one of many priorities

Antivirus and antimalware didn't stop an intrusion, and staff was unable to diagnose issue

Results

Binary Defense is an extension of the team

Binary Defense MDR has replaced the outdated antivirus and antimalware programs to ensure that client information is protected

IT Manager is able to focus on other tasks, knowing that security is being handled by a team of professionals

---

"I can actually sleep at night again knowing that Binary Defense has an eye on things when I can't." -Jay Ketchaver, Manager of Information Technology and Security, Fathom

Fathom is a marketing agency located in Cleveland, Ohio, serving clients across the United States, with a strong focus in the healthcare industry. Agencies that deal with healthcare data are bound by HIPAA regulations, which are safeguards set in place by the U.S. Department of Health & Human Services to keep private health information secure from breaches. Fathom, with under 100 employees, was relying upon antivirus and antimalware programs through a managed services provider (MSP). Jay Ketchaver, the Manager of Information Technology and Security, serves as a one-person team and handles all IT-related needs for the entire organization, with support from the MSP. Understandably, Ketchaver cannot focus solely on security, due to the competing priorities he manages throughout each day.

Suspicious activity on admin laptop prompts need for security beyond antivirus

In mid-2019, an incident occurred that made Ketchaver realize that he needed to beef up his security beyond the antivirus and antimalware programs. Ironically, it was his own laptop that had the issue. He had noticed strange activity originating from his laptop. Being the IT admin and having the proverbial keys to the kingdom, it gave him significant cause for alarm. If a hacker had gained control of his laptop, they could potentially obtain key customer data, including healthcare-sensitive data. He immediately contacted the MSP, and they triaged the issue by removing Ketchaver's laptop from the network while continuing to investigate. It was then that Ketchaver decided he needed dedicated security professionals watching over his network.

Ketchaver had known of Binary Defense because both companies are headquartered in Northeast Ohio. In addition, Ketchaver was aware of the work that Binary Defense co-founder and Chief Technology Officer, David Kennedy, has done in the industry. "Binary Defense is the best in the business. David Kennedy knows his stuff and I trust his judgement. Therefore, I trust Binary Defense," Ketchaver said.

Binary Defense MDR up and running on 85 endpoints within two weeks

Within two weeks of signing the contract, Fathom was up and running with Binary Defense Managed Detection & Response on their 85 endpoints, including workstations, laptops, service machines and servers. "It was extremely easy to get started," said Ketchaver. "I had all the support I needed. I talked to the Binary Defense implementation team quite a bit and they walked me through the process."

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

"Replacing antivirus and antimalware was not much more money for a much-improved service. It was pretty much a no-brainer to go with Binary Defense." – Jay Ketchaver

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. Fortunately, Ketchaver has not had a major incident since deploying Binary Defense MDR. "The team has flagged some things for me to review. They have all been false positives. I'm happy with the response rate that I receive from Binary Defense. The communication is really good."

Security Operations Task Force is an extension of the Fathom IT Team

The Security Operations Task Force is essentially a supplemental security staff for Ketchaver and Fathom. "They have most definitely made that aspect of my job a lot easier," he says. "I can actually sleep at night again knowing that Binary Defense has an eye on things when I can't."

He noted that he appreciates the shift change operation alerts, so he knows exactly who on the Binary Defense staff he can contact if he needs to. He also enjoys having the ability to access the MDR dashboard if he needs to take a look at what's happening on his network.

"Replacing antivirus and antimalware was not much more money for a much-improved service. It was pretty much a no-brainer to go with Binary Defense," says Ketchaver.