Case Study

BINARY DEFENSE™

Technology Firm Relies on Binary Defense to Monitor and Detect for Cyberattacks

Business

Stowe Research is a global technology group experienced in developing enterprise applications for clients in the public and private sectors

Challenges

International office with a diverse group of clients--and therefore, client data to keep secure

Need to update exsiting cybersecurity from solely antivirus

Results

Visibility and insight through advanced cybersecurity

Peace of mind knowing the Security Operations Center team is making informed decisions about alarms

A partner advancing the security industry forward

"The fact that you have so many pairs of eyes watching our network while we are sleeping ... I don't sleep well, but the day we signed up with Binary Defense, I came to realize that we are quite adequately protected and I don't lose sleep over that anymore." -Nick Nair, President, Stowe Research International

Global IT firm specializing in software development

Formed as an IT consulting firm in 1989, Stowe Research International has grown into an global organization specializing in software development and services for clients in a variety of industries.

Nick Nair, President and founder of Stowe Research, has kept an eye on the changes in cybersecurity over his career. However, it wasn't until a client was a victim of a breach that he decided it was time to take action with his own company's data and upgrade his cybersecurity beyond antivirus.

Identifying the gaps in security was the first step

Nair, a long-time follower of Binary Defense and TrustedSec founder David Kennedy, had recommended TrustedSec to a client that had experienced a breach via business email compromise (BEC). BEC is when a cybercriminal gains access to a typically high-profile email account within an organization and uses that email account to commit fraud by requesting wire transfers or other payments. If successful, BEC can be financially devastating to a company. Moreover, BEC is one of the types of cyberattacks that is not going to be caught by antivirus, as it is behavior-based rather than malware-based.

TrustedSec conducts penetration tests that determine the effectiveness of an organization's current cybersecurity defenses and identifies where improvements could be made. Once TrustedSec helped his client, Nair decided to put them to the test at Stowe Research, as well. "We have always had the basic security loaded–antivirus, etc., but never something that could notify us of zero day threats," Nair said. Zero day threats are flaws in software that could be exploited by a cybercriminal until a patch is developed and deployed. Antivirus might catch a known piece of malware, but wouldn't detect abnormal behavior occurring on the network, or new types of malware the antivirus program hasn't been designed to catch.

Identifying gaps through the penetration test helped to shine a light on what was needed to strengthen the cybersecurity strategy at Stowe Research. Nair knew he needed additional cyber defense to protect against attacks that evade antivirus.

At BlackHat in 2018, Nair met several members of the Binary Defense team. "I was impressed with the people I met and their approach to problem solving. Binary Defense became my go-to company for anything IT security or infosec," Nair said. "We are a highly technical company, so we can very quickly weed out competent technical organizations from those that are just blowing smoke."

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

"We trust the product implicitly."
-Nick Nair

Informed decisions cut down on phone calls

After meeting the team, Nair purchased Binary Defense Managed Detection & Response (MDR) and installed the software on 300 devices (laptop and desktop computers, servers). Binary Defense MDR helps to protect businesses' data from ransomware, phishing and other threats 24/7/365. Data is collected from each device that has the MDR software installed on it, and that information and behavior is analyzed in real time by security experts. These experts can determine whether an actual threat is present, and alert the client if necessary.

"We've had fantastic results," Nair said. With the Security Operations Center watching over his endpoints 24/7/365, Nair feels a true benefit from knowing the SOC analysts are acting as an extension of his team and can make informed decisions. "If Binary Defense called us for every alert, we would hang up on them. We get a report, but very few get escalated to a phone call. That says Binary Defense is staying in touch with us. We trust the product implicitly."

Caught within 60 seconds

Nair was pleasantly surprised when he himself was toying around with Mimikatz (an open source tool that hackers sometimes use to steal credentials) on his laptop. "Within 60 seconds, I received a call from the Binary Defense SOC," he said. "They informed me that one of my company's workstations had fired up [the Mimikatz] application." That was the proof in the pudding, so to speak, for Nair to know that Binary Defense MDR worked.

After eighteen months of using MDR, Nair "doesn't have one single complaint. Not one."

As a trusted advisor, Nair recommends Binary Defense to clients

With clients in the IT industry who are seeking cybersecurity solutions of their own, Nair recommends Binary Defense. "Whenever they are willing to listen, I tell them the story of Binary Defense and the SOC. The fact that you have so many pairs of eyes watching our network while we are sleeping … I don't sleep well, but the day we signed up with Binary Defense, I came to realize that we are quite adequately protected and I don't lose sleep over that anymore."