Case Study

MDR Helps Protect The Assets Of One Of The Nation's Top Coal Suppliers

Business Overview

Large, publicly-traded holding company with a major coal company subsidiary

Challenges

Small cybersecurity team with competing priorities

Need for non-intrusive method of protecting key executives' information

Critical company data needs to be protected

Results

Binary Defense's Managed Detection & Response (MDR) platform provides protection for all NACCO workstations

Around the clock monitoring and alerting NACCO of any potential threats or incidents

Security analysts act as extension of the team, providing real-time alerts, reporting and guidance

"The comfort of just knowing that [our] key users' computers are covered 24x7x365 provided me with a world of relief."

NACCO Industries, Inc.
Dating back to 1913 when it began as The Cleveland & Western Coal Company, NACCO Industries Inc. is the parent company of the North American Coal (NACoal) Corporation, one of the 10 largest coal providers in the US. NACoal operates surface mines that supply coal to power generation and natural resource companies. NACCO Industries, Inc. is a publicly-traded, billion-dollar company committed to long-term growth.

Small IT team; large assets to protect
Ed Slusarski, Director of IT Audit & Cybersecurity for NACCO Industries, Inc. in Cleveland Ohio, works with a small, remote IT team located at the NACoal headquarters in Dallas, Texas. He is charged with not only securing NACCO's huge volume of proprietary and operational data, but also protecting the executive team from cyber threats. When tasked with developing and implementing a sound cybersecurity strategy at NACCO, Slusarski realized that he needed to find a Managed Detection & Response (MDR) solution that:

- Served as an extension to the remote IT department, as he did not have the proper staffing to sustain a 24/7 solution at NACCO HQ
- Was not labor-intensive for himself and the remote IT team
- Did not interfere with or slow down individual workstations
- Proactively searched for threats or abnormalities within the network and made recommendations when issues arose
- Protected proprietary company information that resides on the network
- Provided functionality even when employees and executives worked remotely

Binary Defense Managed Detection & Response provided seamless protection and peace of mind
The Binary Defense MDR solution met all of Slusarski's criteria. Within about an hour's time, the security platform was installed on every user's computer, as well as the NACCO servers, and began reporting back to the Binary Defense Security Operations Center (SOC), where a team of cybersecurity experts monitors customers' endpoints around the clock. Under most conditions, the MDR platform takes up minimal space on a workstation, has limited impact on performance and is nearly invisible to the end user.The software also continues to monitor workstations even when they are not on premises; for example, when an executive is traveling or working remotely.

"The comfort of just knowing that [our] key users' computers are covered 24x7x365 provided me with a world of relief," said Slusarski.

Get another cup of coffee
Slusarski noted that the proactive monitoring done by the Binary Defense team was a huge time-saver for him and the remote IT Team. "The Binary

Binary Defense MDR

Advanced Endpoint Detection

24/7 around-the-clock event monitoring

Real-time analysis of threat behavior

Lightweight and easy deployment

Expert and trusted extension of your team

"[The Binary Defense Team] is open with information and that helps. We have updated our incident response plan based on the valuable insight they give us." -Ed Slusarski, Cybersecurity Director, NACCO Industries, Inc.

Defense team is able to help with the baselining and proactively scrubbing to help eliminate the false positives in my environment. I can go get another cup of coffee and work on other more important cybersecurity control requirements," Slusarski said. "When an issue is identified, the Binary Defense analysts are notifying me as to the potential problems and their thoughts or risk so it narrows down the potential avenues that I have to review with the remote IT team members."

False positives in cybersecurity occur when something appears to be coming from a malicious source, but is actually a legitimate activity. They account for 40% of alerts that a cybersecurity team receives daily and are critical to investigate, as they could be real threats. However, investigating these alerts is extremely time consuming – especially without dedicated personnel. In one instance, the Binary Defense team passed along a suspicious IP address to Slusarski and his team to investigate. Though they suspected it was a false positive, they took precautions nonetheless. "We blacklisted the IP address. It could have been nothing, but if anything tried to come through, it would have been blocked."

Serving as a true extension of the IT Security team

The option to chat with a Binary Defense analyst on an as-needed basis to seek guidance and advice on issues has come in handy for Slusarski, as well. With a small team with other priorities, it's impossible for them to stay current on cybersecurity threats and trends. "They are open with information and that helps. We have updated our incident response plan based on the valuable insight they give us," he said.

Binary Defense gives Slusarski and his team the peace of mind that their valuable data and individual workstations are being proactively monitored, managed and kept secure. Slusarski could not be more satisfied with the MDR solution and is a huge proponent of Binary Defense. "When people ask me what type of monitoring I use and why, I sing the praises of Binary Defense. They are fantastic!"