



# CALCASIEU PARISH SCHOOL BOARD



## INDUSTRY

K-12 Education

## THE CHALLENGE

With nearly 40,000 endpoints to defend, Calcasieu Parish School Board, the 5th largest school district in Louisiana, needed more visibility into what was happening in their IT environment. The former BitDefender customer found it difficult to prioritize incidents and correlate data and never felt like they knew what malicious activity might be taking place prior to the existence of EDR features.

Calcasieu Parish's specific operational challenges included:

- Small, over-taxed IT security staff that wears many different hats
- Large, complex, and constantly changing environment
- Varied IT resources, including 12 on-prem BitDefender servers that required management
- Inability to see the entire attack story with alerts arriving individually from detection tools

## THE CHOICE OF CYBEREASON WAS AN EASY ONE TO MAKE

When the Calcasieu Parish School Board signed its contract with BitDefender 5 years ago, its security analysts quickly realized they needed more data and context to make sense of the alerts they were receiving.

"When we first purchased BitDefender, all it basically did was detect and stop," said Michael Franks, the Parish Network Administrator. "Because we opted for the on-prem version, it required 12 servers on-prem, including three databases, two web servers, and two update servers. You couldn't really dig deep."

When the time came to renew their contract with BitDefender, the Parish had research to do before making a decision. "As good stewards, we always look at at least three different companies before we renew a contract," said Yvette Ardoin, Network Operations Coordinator for Calcasieu Parish. "We knew we needed more insight into what was happening."

Ardoin formed an evaluation team to look at BitDefender, Cybereason, and Palo Alto. She then told the evaluation team to list their first, second, and third choice without considering cost as a factor. "It came down to the back end," she said. "The back end of Cybereason outshined the other two. And that's how we decided to go with Cybereason."

## ANXIETY REMOVED, SECURITY IMPROVED

With more than 40,000 endpoints to defend and only seven in-house specialists, Calcasieu Parish faced a significant challenge staying on top of alerts that required investigation and gathering the necessary context to understand the breadth and depth of the attack.

The school district's Help Desk team, for example, often writes its own scripts to automate routine tasks. One such script is a Powershell script that connects to other machines, adds a user to the administrator group, and adds a scheduled task to run remedial software cleanup, which they do regularly. Although this activity is legitimate, it is also an activity that can often be associated with a malicious operation.

The evaluation team watched in real-time as BitDefender failed to alert to the activity since EDR features were not present. But Cybereason detected it and flagged it for investigation. "While it was one of our guys responsible for it, that could have just as easily been a bad guy doing the same thing, and we would have had no idea that that was going on," Franks said.

"Cybereason just gives us so much more information, and the MalOp™ inbox enables me to get to the critical incidents that nobody has put eyes on yet, saving me so much time," he said. "Because we didn't have that deep insight into what was going on, there was always that anxiety in the back of your mind. You kind of hope it's protecting you, but you don't really know. With Cybereason, we know we're being taken care of and protected."

Jason Ogea, Network Operations Center Analyst, agreed. "The MalOp Management capability with filtering built-in comes in handy," he said. "We're able to immediately see problems and remediate them quickly."

For Ardoin, going with Cybereason took Calcasieu Parish's endpoint security program to the next level. "When we did our proof of concept for all three vendors, my team liked Cybereason's features more, especially the backend dashboard," she said. "My team had a warm and fuzzy with Cybereason. It's well worth the peace of mind and the money we invested. It lets my team sleep at night."

## SOLUTION

- Cloud-based Cybereason detection servers eliminated Calcasieu Parish's management footprint and consolidated a large part of its security stack behind a single pane of glass.
- Cybereason Managed Detection and Response (MDR) services directly assisted with tuning the rules and detection logic to ensure Calcasieu Parish was blocking what needed to be blocked, limiting false positives, and improving response times.
- The operation-centric MalOp Detection Engine provided analysts the context they needed to be proactive, from root cause to every affected endpoint and user, with real-time, multi-stage displays of the complete attack details.



"Cybereason just gives us so much more information, and the MalOp™ inbox enables me to get to the critical incidents that nobody has put eyes on yet, saving me so much time..."

**MICHAEL FRANKS**

Parish Network Administrator



LEARN MORE AT [CYBEREASON.COM](https://cybereason.com)

