

MCBEE ASSOCIATES



COMPANY

McBee Associates

INDUSTRY

Healthcare

NUMBER OF ENDPOINTS

4,030

OUTCOME

- Greater endpoint visibility, including on machines not connected to the network
- A proactive approach to security leading to immediate detection and remediation of advanced threats
- Collapsed the technology stack

Executive Summary

McBee Associates provides clinical, financial and operational consulting services to healthcare organizations. The firm's perimeter defenses weren't providing it with endpoint visibility. Cybereason's EDR platform helps McBee's security team take an offensive, proactive approach to security and immediately detect and stop malicious endpoint activity. McBee also uses Cybereason's managed security services to augment its security program and replaced its antivirus solution with Cybereason's next-generation antivirus software to reduce the number of agents running on its endpoints.

The Challenge

"Being in healthcare, we process and store protected health information so HIPAA compliance and security is at the forefront of everything we do," said McBee CTO Alan Yagoda.

While this 370-person company had network perimeter defenses like a firewall and antivirus software, they lacked an endpoint tool that provided full visibility. Greater endpoint visibility was especially important since more McBee employees were working from home and client sites, placing those endpoints beyond the protection offered by network perimeter tools.

"We had no visibility into what people were doing, what programs they were running, what data they were using. We were completely dependent on traditional antivirus," Yagoda said.

He also wanted an EDR tool that would work with McBee's security stack, specifically their antivirus software.

McBee needed an EDR tool that:

- Provided visibility into all endpoints, not just machines on the company's network
- Helped the security team proactively defend their clients' healthcare data from ransomware, malware and other advanced threats
- Wouldn't clash with its antivirus software

The Solution

McBee deployed Cybereason on 4,030 endpoints, including multiple servers. Cybereason's impact was immediate. Armed with the ability to trace an entire attack operation, knowledge of the specific users and computers affected and information about any lateral movement, Yagoda's team quickly identified and stopped malicious activity.

"We were remediating an hour after deploying Cybereason. We were in a much better offensive position with more visibility to protect the internal network," he said.

Additionally, Yagoda replaced his antivirus software with Cybereason's next-generation antivirus to reduce agent fatigue, simplify vendor management and reduce the risk of software conflicts. In fact, during one EDR evaluation McBee had to turn off its antivirus software for the EDR to work.

"Combining the EDR and next-generation antivirus in one solution enables us to use a single tool. Cybereason worked seamlessly in the environment. We had no conflict and it was easy to deploy," Yagoda said.

McBee also used Cybereason's managed security services to monitor the firm's environment for malicious activity. Yagoda considers Cybereason's security analysts an extension of his team and appreciates how quickly they spot suspicious activities, sometimes "even before we notice them."

"It's a good partnership for a company in the healthcare space that's trying to avoid ending up in the newspaper. It's comforting knowing that you've got a good tool that's protecting you and backed up a fantastic support team," he said.

The Outcome

"The combination of Cybereason software and the active monitoring team allows us to constantly evolve with the adversaries," Yagoda said.

Instead of endpoints being a blind spot at McBee, Yagoda's team now has endpoint information at their fingertips and can protect computers no matter where they are. With Cybereason, McBee's security analysts can collect endpoint data, understand how end users are behaving and can follow malicious activity through all of the firm's machines.



"Cybereason took a very complicated problem and presented it to the user in a very simple tool. This gives us more visibility than we had before when we were just trying to keep people out. Instead, we're seeing what's happening within the organization."

ALAN YAGODA

CTO
MCBEE ASSOCIATES



Learn more at [Cybereason.com](https://www.cybereason.com) →

