CASE STUDY:

RTI SURGICAL_

COMPANY:

RTI Surgical

INDUSTRY:

Medical device manufacturing

NUMBER OF ENDPOINTS:

2,000

OUTCOME

- Greater endpoint visibility, including on machines not connected to the network
- Increased efficiency around investigating security incidents by automating endpoint data collection and analysis
- The ability to proactively detect and block ransomware attacks

EXECUTIVE SUMMARY

RTI Surgical manufactures medical devices as well as biological and synthetic implants for surgeons around the world. The company, which reported revenue of $279.6 million in 2017, was maturing its security program and wanted an EDR (endpoint detection and response) platform that provided endpoint visibility and allowed the security team to see threats across the entire company without overwhelming analysts with data. Additionally, ransomware protection was a must for RTI, which had experienced multiple ransomware attacks. Cybereason helped RTI's security team become more efficient at identifying malicious behavior in their IT environment and blocking ransomware attacks.

THE CHALLENGE

RTI had antivirus software and a firewall, but neither tool provided it with deep endpoint visibility. Monitoring endpoints that weren't connected to RTI's network was a top concern for Jeff Wright, the company's security manager, who had remediated breaches that occurred after an employee connected to an infiltrated Wi-Fi network at conference.

"I need 100 percent visibility into my endpoints. I need to know that when employees travel I can get a report on what their machines are doing or not doing," he said.

RTI had faced 14 ransomware attacks in 12 months, making ransomware protection a top priority. Wright, who had experienced ransomware's aftermath on several occasions, wanted to stop worrying about employees opening a malicious email attachment and triggering a ransomware download. "We had antivirus and firewalls like everybody else, but we didn't have anything that handled ransomware," he said.

RTI needed:

- **Visibility into all endpoints, not just those connected to the company network**
- **A way to detect and block ransomware attacks before they started**
- **The ability to detect threats across the entire enterprise without inundating the security team with information**

THE SOLUTION

RTI deployed Cybereason on several thousand endpoints. The platform provided RTI with the deep endpoint visibility that it wasn't getting from firewalls and antivirus software, said Wright.

"We had nothing beyond the standard tools, which give you limited visibility, especially if you're performing incident response. Cybereason not only lets us know when we have a problem, but allows us to see the how, why and when," he said.

THE OUTCOME

With Cybereason, RTI's security team is more efficient and proactive. Instead of manually reviewing SIEM logs, a process that Wright said can bury analysts under data logs, Cybereason automatically collects and correlates endpoint data and issues security alerts.

"[Cybereason] only shows the things that are super important, so you're not getting inundated with information," he said.

Additionally, the security team can immediately remediate a compromised machine that's not connected to RTI's network instead of waiting for it to reconnect to the network. And Wright uses Cybereason's threat hunting function to proactively search for adversaries who are already in RTI's network.

"I look for things that I would do if I were an attacker and see if I can find them on my network. I couldn't do that before," he said, adding that he usually looks for PowerShell activity since attackers use this tool to carry out fileless malware attacks.

Cybereason's use of behavioral analysis instead of signatures to detect malicious activity means RTI is protected from ransomware attacks, including variants and new strains.

"Knowing that I don't have to worry about a major server being taken off the line because someone clicked a link is huge for me," he said.

> "Cybereason not only lets us know when we have a problem,
> but allows us to see the how, why and when."

JEFF WRIGHT
SECURITY MANAGER
RTI SURGICAL