CASE STUDY:

FORTUNE 500 BANK_

INDUSTRY:

Financial services

NUMBER OF ENDPOINTS:

400,000

OUTCOME

» Helped resolve the bank’s big data problem by automating endpoint data collection and analysis

» Allowed the security team to become more efficient and focus on incidents that threatened the bank’s security

» Placed endpoint data in context to form a complete attack story

EXECUTIVE SUMMARY

A Fortune 500 bank needed to replace its EDR (endpoint detection and response) tool with one that provided the security team with a complete attack story by automatically collecting and analyzing endpoint data. The security team also needed its new EDR tool to help it transition to a behavioral-based detection model. Cybereason helped the security team better detect abnormal behavior across the entire company by automating endpoint data collection and analysis.

THE CHALLENGE

The bank, which has more than 60 million customers across the world, had a big data problem. The EDR tool it was using collected reams of endpoint data from the bank’s hundreds of thousands of servers and computers but didn’t provide security analysts with any context on this information. Instead, analysts had to undertake the time-consuming process of manually querying the data to make sense of it.

“Our previous EDR tool just provided lots of data. That’s not helpful when you have such a large infrastructure. You just get overwhelmed with data,” said the bank’s deputy CISO.

Greater endpoint visibility into malicious activity across the enterprise was also a requirement. The bank’s previous EDR tool failed to detect a red team simulating attackers. The deputy CISO knew that if a red team could use these techniques to evade the EDR tool, attackers could use them to infiltrate the bank’s network.

The bank needed an EDR tool that:

» Automatically gathered and analyzed endpoint data and used it to provide analysts with a complete attack story

» Used behavioral analysis to detect malicious activity

» Increased endpoint visibility and provided advanced threat detection across the entire company

THE SOLUTION

Cybereason's ability to automatically sort through endpoint data and place context around it impressed the security team and lead to the bank purchasing the platform. The bank decided to deploy Cybereason on 400,000 endpoints. Deployment began in early September 2017 and, by the end of the year, Cybereason was on 200,000 endpoints.

With Cybereason, the security team had visibility into what was normal behavior in their IT environment and what was an anomaly that required further investigation. "Lots of tools are very good at providing visibility, but no other product could say, 'This is the thing you need to look at.' That's what Cybereason provides. We need a tool that gives us those unique alerts because we're a big bank and a big target," said the deputy CISO.

Cybereason was quickly put to test: two weeks into the deployment process, when Cybereason was on 20,000 machines, the Apache Struts server vulnerability was publicly disclosed. The bank used Cybereason to monitor its environment and see if attackers were exploiting the vulnerability.

"When Struts came out and that was a challenge for us because we have such a large infrastructure [to patch]. We needed to be sure that while patching was happening we could see if anyone was exploiting the vulnerability. We immediately deployed Cybereason to those [impacted] systems to increase visibility," said the deputy CISO.

THE OUTCOME

The bank's security team became more efficient with Cybereason. Instead of manually querying endpoint data, they used Cybereason's in-memory graph database to automatically collect and correlate endpoint data and alert them when malicious behavior was detected. This allowed the security team to spend more time investigating incidents that threatened the bank's security.

"The magic of Cybereason is that it doesn't just take all your data. The graph database will tell you what is normal in your environment and what isn't normal. That's valuable because you can focus on what's unusual," said the deputy CISO.

Using Cybereason also helped the security team adopt a behavioral-based detection model and rely less on indicators of compromise, which weren't providing them with enough visibility. Attackers easily changed indicators of compromise to evade antivirus software, said the deputy CISO. Additionally, he had noticed an increase in fileless malware attacks, which can't be detected by looking for indicators of compromise. Using behavioral analysis to detect attacker tools, techniques and procedures is the best way to discover fileless malware attacks.

"Indicators are an aging thing in security. You have to move beyond them. You have to detect techniques and tools, which are much harder for adversaries to change," he said.

> "Lots of tools are very good at providing visibility, but no other product could say, 'This is the thing you need to look at.' That's what Cybereason provides."
>
> **BANK DEPUTY CISO**