CASE STUDY:

CADWALADER, WICKERSHAM & TAFT_

CADWALADER

COMPANY:

Cadwalader, Wickersham & Taft

INDUSTRY:

Legal

NUMBER OF ENDPOINTS:

2,000

OUTCOME

- Reduced the amount of time analysts spent detecting and investigating incidents across the entire firm
- Provided analysts with a complete incident timeline without requiring them to manually investigate incidents
- Implemented behavioral-based detection

EXECUTIVE SUMMARY

The security team at Cadwalader, Wickersham & Taft, an international law firm with more than 400 lawyers in five offices around the globe, wanted an EDR (endpoint detection and response) platform that allowed them to efficiently detect and investigate incidents across its entire IT environment. Additionally, the tool had to be intuitive to use. Cybereason reduced the investigation process from hours to minutes and the security team was able to use the platform with minimal training.

THE CHALLENGE

Cadwalader's security team wanted to streamline the threat investigation process. Before Cybereason, the team combed through firewall logs and conducted packet analysis to build an attack picture, a time-consuming, labor-intensive process, said Dimitri Josh, a member of Cadwalader's security team.

"Investigating events was disjointed and involved a lot of manual labor with individual teams doing things ad hoc. You'd spend two or three hours looking at what's being blocked or what the source addresses are and you'd have to run antivirus and scans," he said.

Cadwalader needed an EDR tool that:

- **Helped the security team more efficiently detect and investigate threats throughout the firm**
- **Provided an end-to-end view of incidents in the firm's IT environment without requiring analysts to manually review and analyze data**
- **Didn't require extensive training to learn how to use**

THE SOLUTION

The Cybereason EDR platform was deployed on approximately 2,000 endpoints. Compared to other tools the security team had used, Cybereason was easy to learn. They began investigating suspicious activity immediately with minimal training.

"[Cybereason] isn't a tool that requires spending multiple days in a classroom to learn. Being able to look at files that are open on an endpoint and have that level of detail and not have a cumbersome deployment, that's a great value," Josh said.

THE OUTCOME

Using Cybereason, Cadwalader's security team had a complete timeline of incidents in minutes instead of hours without sifting through firewall logs. Cybereason quickly generates a whole attack story by using an in-memory graph to correlate data from all of an organization's endpoints and automatically detect suspicious activity. Spending less time manually piecing together attack stories allowed the security team to focus on compliance work and tactical projects aimed at protecting Cadwalader.

"[Without Cybereason] we wouldn't be as nimble as we are. We would have to leverage multiple tools just to get half of the information we have now. We have the power to look at the entire environment from end to end. The time that's freed up is one of the great pluses of Cybereason," Josh said.

Additionally, Cybereason helped Cadwalader's security team adopt a behavioral-based approach to threat detection. Looking for attack behavior instead of indicators of compromise allowed them to spot more advanced threats like fileless malware attacks, which use PowerShell for malicious activity. While the firm used antivirus software, Josh knew that layered security was the best approach for staying ahead of adversaries.

"You need to have security in-depth, not just one solution to fix your problems. That's what brought us to Cybereason. We can look at the big picture of what's going on and can correlate events and troubleshoot issues in a timelier fashion," he said.

"[Without Cybereason] we wouldn't be as nimble as we are. We would have to leverage multiple tools just to get half of the information we have now. We have the power to look at the entire environment from end to end."

DIMITRI JOSH
CADWALADER, WICKERSHAM & TAFT