CASE STUDY

How Cybereason Edged the Competition and Automated Threat Hunting for a Global Aerospace Manufacturer

cybereason

THE CUSTOMER

A global manufacturer with diverse aerospace product lines and annual revenue in the billions of dollars.

THE PROBLEM

The manufacturer was in search of a better way to monitor endpoints and determine signs of compromise.

THE BOTTOM LINE

Cybereason outperformed every other endpoint detection and response product tested by the organization's security team.

The customer streamlined its endpoint security process and automated threat detection.

Just a few days after deploying Cybereason, the company had cleaned the infected servers.

DATA OVERLOAD AND A LACK OF QUALIFIED SOLUTIONS

The organization's security team, which included some of the world's greatest security talent, manually reviewed data logs for suspicious activity. With thousands of endpoints deployed across the world generating reams of data, the security team spent several hours a day determining which threats warranted investigation.

The security team needed an endpoint detection and response platform that continuously monitored all of the company's PCs and servers and used data analysis to automatically detect threats. Unfortunately, after searching for three years, the company failed to find a product with these features. The security team was close to giving up its search when they discovered Cybereason.

THE SOLUTION: AUTOMATING THE HUNT

Security executives believed that facing advanced persistent threats (APTs) required proactively hunting for adversaries that had already breached an organization's defenses, a mindset shared by Cybereason. Cybereason's platform uses behavioral analysis to hunt for adversaries that are in the network and helps security teams detect unknown threats that could slip past traditional security tools. Interested to see if Cybereason could improve the company's detection capabilities, the manufacturer deployed the platform on several thousand endpoints.

IMMEDIATE, HASSLE-FREE DEPLOYMENT

Deploying Cybereason only took a few hours and did not require the security team to write customized rules or configure the platform to work on its endpoints. According to the company's CISO, the organization had previously rolled out products to its endpoints with disastrous results, including multiple PC crashes and excessive amounts of downtime. With Cybereason, though, deployment and system operation were hassle-free.

REAL-TIME DETECTION WITH NO KERNEL AGENTS

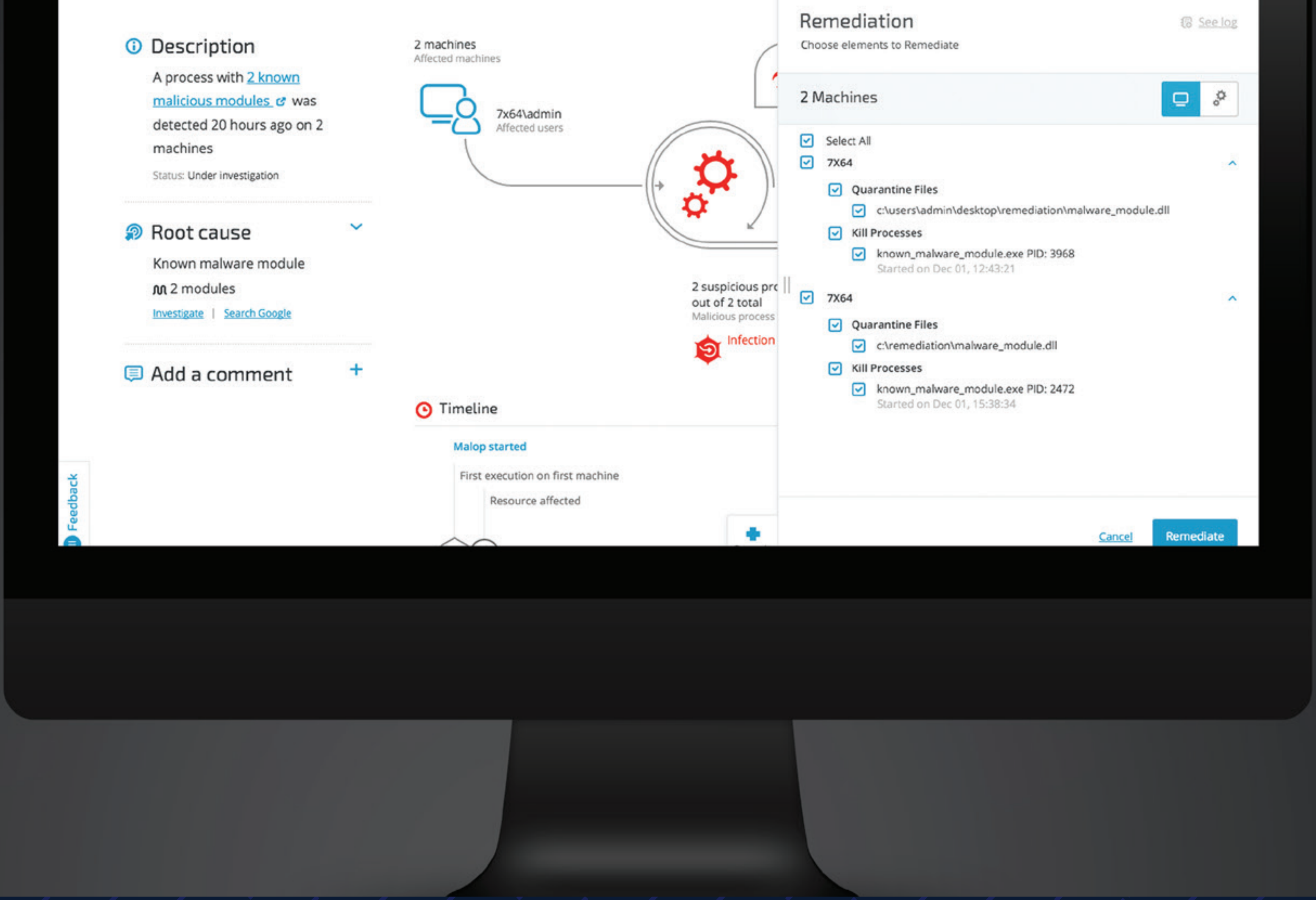
Unlike other endpoint products, Cybereason operates in user space instead of the kernel. This prevents the endpoint agent from clashing with other tools, causing blue screens and slowing processor times. The customer was impressed with Cybereason's ability to collect data from thousands of devices in real time without crippling the network. Even though the system monitors every activity taking place on the endpoint, Cybereason transmits less than 10MB of data per device per day to the Cybereason Hunting Engine, which automatically queries the data in real time and looks for malicious activities.

To monitor the endpoints in real time, Cybereason maintains an open communication channel between the Cybereason Endpoint Sensors and the Cybereason Malop Hunting Engine, allowing the platform to know what devices are connected. Other security solutions the customer considered only periodically check-in with the endpoints in intervals of 15 or 30 minutes (not in real time).

MEETING THE ORGANIZATION'S STRICT SECURITY NEEDS

During its multi-year search for an advanced endpoint visibility solution, our customer looked into several tools. One cloud-based product collected endpoint data and sent it to the vendor's data center for analysis and interpretation by an analyst. However, our customer had very strict security rules. Endpoint data couldn't leave the company because some of the sophisticated adversaries our customer faced attacked its service providers in an effort to gain access to the organization.

Another product that the company vetted relied on indicators of compromise (IOCs) to detect threats, causing the CISO to question if this approach would effectively reveal attacks. The IOCs that the vendor used were specific to industries outside of the defense and aerospace fields, and our customer knew that attackers could easily change IOCs to deceive security tools.



Description

A process with 2 known malicious modules was detected 20 hours ago on 2 machines

Status: Under investigation

Root cause

Known malware module

2 modules

Investigate | Search Google

Add a comment +

2 machines
Affected machines

7x64\admin
Affected users

2 suspicious pro
out of 2 total
Malicious process

Infection

Timeline

Malop started

First execution on first machine

Resource affected

Feedback

Remediation

Choose elements to Remediate

See log

2 Machines

☑ Select All

☑ 7X64

☑ Quarantine Files

☑ c:\users\admin\desktop\remediation\malware_module.dll

☑ Kill Processes

☑ known_malware_module.exe PID: 3968
Started on Dec 01, 12:43:21

☑ 7X64

☑ Quarantine Files

☑ c:\remediation\malware_module.dll

☑ Kill Processes

☑ known_malware_module.exe PID: 2472
Started on Dec 01, 15:38:34

Cancel

Remediate

> *"Cybereason has the correct mindset to understand what you need to do and what to look for to discover threats. This mindset is not present in most security companies."*

- Chief Information Security Officer

AUTOMATIC THREAT DETECTION THAT SCALES

Data analysis capabilities were a requirement for our customer. Given the amount of advanced threats the company faced, they needed a solution that analyzed data to automatically identify threats and connect suspicious instances to uncover a full attack. While nearly all of the products our customer considered performed some type of data analysis, their various approaches had several shortcomings. One platform collected massive amounts of endpoint data, including processes that ran on the device, file information and registry information but just placed it in a database. This left analysts with the arduous task of sifting through all the data to find suspicious activities. Our customer also had reservations about the product's ability to monitor its thousands of endpoints.

DATA ANALYSIS WITHOUT ALERT OVERLOAD

For other vendors, big data analysis meant filtering data, assigning risk scores and issuing prioritized threat alerts based on how malicious a threat appeared. But this approach overwhelmed analysts with alerts.

"Cybereason reduces an analyst's workload by allowing them to focus on what matters. The platform automatically detects threats by monitoring all endpoint activity in real time and applies machine learning and behavioral analysis techniques to identify suspicious behaviors and ties together related behaviors. No other security tool does this."

- Chief Information Security Officer

AUTOMATICALLY INVESTIGATING MALICIOUS TOOLS

Cybereason proved its value soon after the platform was deployed. The customer detected malware on an endpoint, copied it from the machine and executed it in a sandbox to analyze it and gather IOCs. Curious to see what Cybereason could detect, the lead security architect used the platform to study the malware as it ran on the endpoint. He discovered several IOCs that were missed by manually studying the malware in the sandbox.

"We were able to see that the malware was doing other things. Cybereason detected what we saw during our analysis and provided so much more information along with it."

- Lead Security Architect

ABOUT CYBEREASON

The Cybereason Detection and Response Platform leverages big data, behavioral analytics and machine learning to uncover, in real time, complex cyber attacks designed to evade traditional defenses. It automates the investigation process, connects isolated malicious events and visually presents a full malicious operation. The platform is available as an on-premise solution or a cloud-based service.

Founded by members of the Israeli intelligence agency's elite cyber security Unit 8200, Cybereason mirrors the founders' expertise in managing some of the world's most complex hacking operations. Cybereason developed the world's only military-grade, real-time detection and response platform and has a proven track record of protecting global enterprises. The company has received many awards and accolades since its founding. Cybereason is privately held and headquartered in Boston with offices in Tel Aviv, Tokyo, and London.

cybereason