Protecting the Financial Services Industry

Customer challenges

An international banking and asset management group, with annual revenue in the billions, faced unique challenges.

- Securing a range of products and services for a client base around the globe
- Not using any advanced threat hunting tools
- Advanced, mature security team spending their time manually writing rules and queries

The situation before

Manual investigation

- Security team was spending their time writing rules, creating queries, and manually interpreting results

Lack of visibility

- Knew they were extremely vulnerable to advanced attacks, but lacked visibility into their entire network of endpoints

Poor detection

- Had no way to correlate seemingly disparate events, so they were unable to detect previously unknown threats and fileless malware

The situation after

Automated hunting	◦ Quickly up and running because of pre-configured advanced detection models and no rule-writing required ◦ Manual investigation became automated, so analysts can focus on higher-level work
Broad visibility	◦ Gained visibility across Windows, Mac, and Linux machines
Improved detection	◦ Correlation of data across all endpoints allowed them to identify malicious activity within their environment through the use of machine learning technology, rather than just physical eyes on glass

Why Cybereason

More
automated
than Carbon Black

Designed with an
intuitive UI
that reduces time spent gathering data

Offers
behavioral detection
with preconfigured behavioral models

The customer decision process

- Customer was exploring automated hunting solutions and ran POCs with Cybereason and Carbon Black.
- Red Team/Blue Team test showed the customer they were extremely vulnerable to advanced attacks.
- The team was initially very used to, and comfortable with, their current manual approach to creating alerts, but changed their philosophy when they saw the value of automated detection during the Cybereason POC.
- The security team championed for Cybereason because they were impressed by the platform's intuitive UI and its ability to automate their hunt.

“The UI is so easy and intuitive. Right at the beginning of the POC, before any training had even occurred, our team was able to dig in and use the platform.”

-SOC manager, financial services company