CYLANCE

Finance **CASE STUDY**

INDUSTRY

Finance

ENVIRONMENT

- 3,000 global hosts
- 21 locations worldwide

CHALLENGES

Determine if systems had been compromised by undetected existing threats

Reduce the vast amount of manual work required to analyze potential threats

SOLUTIONS

Engage Cylance® Consulting to perform a full Compromise Assessment to determine if the company's systems had been breached

Deploy CylancePROTECT® enterprise-wide to contain potentially unwanted programs, reduce the total cost of antivirus protection, and stop threats BEFORE they cause costly harm to critical systems

The Company

A $40 billion multi-national private equity, investment banking, alternative asset management and financial services corporation based in New York City.

The Situation

This high-profile financial services institution had a team of resources and multiple products in place to detect and stop any executed threats. The problem, however, was they had no way of knowing if their systems had already been compromised by threats that might be either laying dormant, or occurred beyond the scope of the measures already in place. Additionally, each time a potential threat was detected, their solutions, which lacked "intelligence", required a vast amount of manual review by incident responders to determine whether or not a threat actually existed.

The Process

Cylance was asked to perform a full Compromise Assessment on all servers, desktops and laptops across 3,000 global hosts. Combining both its artificial intelligence technology and compact process, Cylance was able to extract insightful data from all 3,000 hosts in just a matter of days using a lightweight, agent-less system that reported meta data back to Cylance. With the data now outside the customer's environment, Cylance incident analysts aggregated and analyzed it for idiosyncrasies and abnormalities.

The Results

Cylance found hacking tools and evidence that the company's systems had been compromised. Using indicators that were gathered during data collection, Cylance's cybersecurity experts were able to dig into specific systems looking for precisely the threats that had not been found by the company's existing antivirus solutions.

Cylance discovered that penetration testers left tools and open vulnerabilities during a standard penetration test report performed by a third-party vendor six months earlier. It was also discovered that malware had been dropped on the company's systems over three years earlier and had gone completely undetected.

The company had previously used McAfee™ and FireEye™ on their endpoints, though they dropped FireEye when it became cost prohibitive to continue expansion and

yearly maintenance. Thus, Cylance not only replaced the company's traditional antivirus solutions that were not discovering advanced attacks, but also reduced the company's total cost for antivirus protection.

As a final security measure, shortly after the Compromise Assessment was complete, Cylance's next-generation antivirus product, CylancePROTECT, was rolled out to all of the company's systems to contain potentially unwanted programs and prevent the execution of malware.

With CylancePROTECT running on the company's endpoints, three security analysts that once spent nine hours total per day weeding out false positives now spend only 1.5 total hours on that same task. In addition, all of the time required for these analysts to review alerts has been virtually eliminated.

Free Consultation

Want to see how CylancePROTECT and Cylance Consulting will empower your organization in the fight against cyberattacks? Contact us today for a free consultation!

Cylance Privacy Commitment
Cylance is committed to protecting your organization against advanced threats, which includes privacy disclosure. We do not publish the names of our case study partners for this reason.

"We were surprised to learn that a third-party vendor performing a security test was actually responsible for a breach that had been going on for six months. Cylance not only found and remediated that threat but also a number of threats that were up to three years old. Moving forward, we're going to trust our security to Cylance."

-IT Manager
Financial Company

+1 (877) 97DEFEND
proservices@cylance.com
www.cylance.com
18201 Von Karman, Ste. 700 Irvine, CA 92612

R1_20160427