CASE STUDY

Industry

FINANCIAL SERVICES

Falcon Host Deployment

MORE THAN 60,000 ENDPOINTS, AND 15,000 SERVERS, SPREAD ACROSS WINDOWS, LINUX AND MAC OS

Services Used

» Falcon Host
» Falcon Overwatch
» Falcon Intelligence

Summary

This Global 1000 financial services company offers credit cards and related services for businesses and individuals worldwide. Anticipating advanced attacks targeting their environment, the company did extensive testing of a variety of "next-generation" endpoint solutions. Only CrowdStrike Falcon, with its cloud-based architecture and unique behavioral analysis capabilities, was able to provide the level of protection and visibility necessary to defend the organization in an increasingly hostile and unpredictable threat environment.

The Challenge

The company has been working to consolidate its data center, IT and security operations across all its business units. This brought many advantages, but the security organization still was challenged by the lack of real-time visibility and protection of endpoints operating on or off its global network. Their existing method of scanning and detecting infected endpoints -- and containing and re-imaging them -- was inefficient, time-consuming and labor-intensive. Additionally, they were concerned that their existing tools were inadequate for protecting the company against emerging advanced attacks. Finally, the security team wanted to better integrate incident response into their daily security operations and improve overall operational efficiency.

The Solution

The company launched a formal project to analyze various endpoint solutions and determine their ability to meet the evolving needs of both its security and IT operations. The process surfaced a number of key insights. The first was that only a cloud-based solution could provide the degree of real-

CASE STUDY

Key Benefits

- Protection against advanced attacks, leveraging CrowdStrike's Indicators of Attack (IOA) technology and Falcon Overwatch threat-hunting team
- Next-generation architecture featuring a lightweight endpoint sensor, with cloud-based scalability to meet the needs of a growing global enterprise
- Operational efficiency and immediate time-to-value, achieved by delivering prevention, full visibility and extensive real-time and historical search capabilities for their endpoint
- Falcon's highly integrated UI provided both SOC and internal intelligence teams with easy access to Falcon Intelligence, all within the same management portal

time visibility they required. Next, the solution would have to protect them from sophisticated "beyond malware" techniques that confounded conventional malware-based endpoint protection products. They also needed to bolster their existing security resources, specifically the team that was engaged in actively hunting for new and unknown threats. Finally, the IT and security operations teams agreed that they needed an endpoint sensor that was lightweight, unobtrusive to the user, and easy to manage.

The customer conducted an exhaustive "bake-off" between multiple vendors that included leveraging an internal "red team" for testing effectiveness against advanced attacks. The exercise clearly identified Falcon Host as the most robust and effective solution for their needs.

The Results

As part of its testing, the evaluation team identified severe limitations with on-premise solutions, including lack of scalability and operational headaches. Conversely, CrowdStrike Falcon Host was easily deployed, and provided immediate visibility and value for endpoints both on and off-network. Enhanced detection and prevention in the areas of privilege escalation, sticky-keys and malicious web advertisements quickly proved their value to the customer. In addition, Falcon OverWatch was able to quickly detect advanced attacks, further differentiating the Falcon Platform from competing solutions. The customer's Security Operations team liked the full visibility provided by Falcon Host event search.

The test culminated in a decision to deploy Falcon systemwide -- which was achieved in a matter of a few hours, with no reboots and no help desk tickets.