



CASE STUDY

Industry

FINANCIAL SERVICES

CrowdStrike Falcon® Deployment

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

Key Benefits

- » Protection against advanced attacks, leveraging CrowdStrike's indicator 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

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 had been working to consolidate its data center, IT and security operations across its many 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. The company's 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.





CASE STUDY

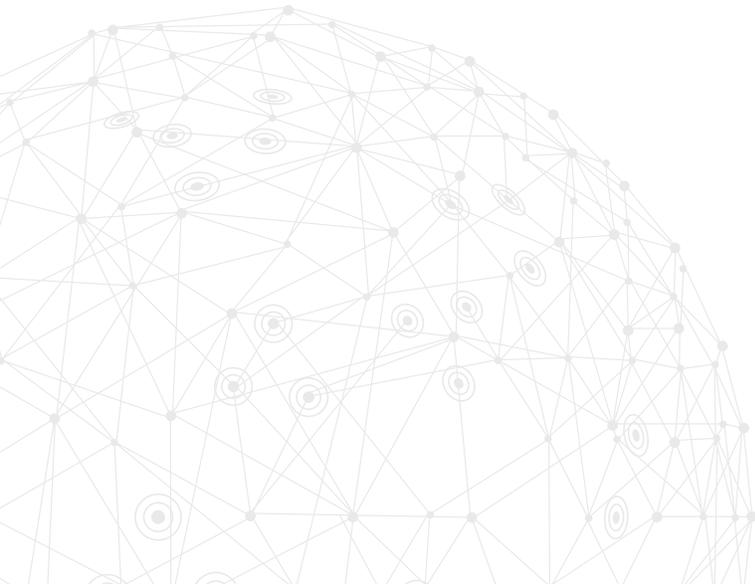
Key Benefits (cont.)

- » Operational efficiency and immediate time-to-value, achieved by delivering prevention, full visibility and extensive real-time and historical search capabilities across their endpoints
- » CrowdStrike Falcon's highly integrated UI providing both SOC and internal intelligence teams with easy access to Falcon Intelligence™, all within the same management portal

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-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" involving multiple vendors. This included leveraging an internal "red team" for testing effectiveness against advanced attacks. The exercise clearly identified the CrowdStrike Falcon platform as the most robust and effective solution for their needs.





CASE STUDY

CrowdStrike® Services Used

- » Falcon Prevent™
- » Falcon Insight™
- » Falcon Discover™
- » Falcon OverWatch™
- » Falcon Intelligence™

Why CrowdStrike

- » **Better efficacy**
- » **Scale:** The ability to quickly deploy without disruption and, given their size, to provide real-time visibility and results
- » **Confidence in the capability of the technology and people**

The Results

As part of its testing, the evaluation team identified severe limitations with on-premises solutions, including lack of scalability and operational headaches. Conversely, CrowdStrike Falcon 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, StickyKeys and malicious web advertisements quickly proved their value to the customer. In addition, the Falcon OverWatch threat hunting team was able to quickly detect advanced attacks, further differentiating the Falcon platform from competing solutions. The customer's security operations center (SOC) team liked the full visibility provided by Falcon's event search capability. It was also noted by the company that red teams involved in the test routinely moved onto softer targets after encountering Falcon running on Windows machines.

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



www.crowdstrike.com | 15440 Laguna Canyon Road Suite 250, Irvine, CA 92618

