CROWDSTRIKE

GLOBAL 1000 FINANCIAL SERVICES COMPANY
CASE STUDY

GLOBAL FINANCIAL INSTITUTION UNIFIES SECURITY ACROSS A WIDELY DISTRIBUTED NETWORK WHILE MAXIMIZING THREAT RESPONSE

This Global 1000 financial services company offers credit cards and related services for businesses and individuals worldwide. Anticipating advanced attacks targeting its environment, the company did extensive testing of a variety of next-generation endpoint protection solutions. Only the CrowdStrike Falcon® platform, 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 was still challenged by the lack of real-time visibility and protection of endpoints operating on and off its global network. The company's existing method of scanning and detecting infected endpoints and then containing and reimaging them was inefficient, time-consuming and labor-intensive. Additionally, the company was concerned that its existing tools were inadequate for protecting against emerging advanced attacks. Finally, the security team wanted to better integrate incident response into their daily security operations and improve overall operational efficiency.

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® indicator of attack (IOA) technology and the Falcon Overwatch™ threat-hunting team

Next-generation architecture featuring a lightweight endpoint agent, with cloud-native scalability that can 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 across endpoints

The CrowdStrike Falcon highly integrated UI provides both SOC and internal intelligence teams with easy access to threat intelligence, all within the same management portal

CrowdStrike Case Study

GLOBAL 1000 FINANCIAL SERVICES COMPANY

CROWDSTRIKE SERVICES USED

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

THE SOLUTION

The company launched a formal project to analyze various endpoint solutions and determine each of their ability to meet the evolving needs of both its security and IT operations. The process surfaced a number of key insights. First, only a cloud-based solution could provide the degree of real-time visibility required. Next, the solution would have to protect the company from sophisticated "beyond malware" techniques that confound conventional malware-based endpoint protection products. The company also needed to bolster its 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 agent 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 to test effectiveness against advanced attacks. The exercise clearly identified the CrowdStrike Falcon platform as the most robust and effective solution for the defined needs.

THE RESULTS

As part of its testing, the company's 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, Sticky Keys 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. The company also noted 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.

WHY CROWDSTRIKE

Better efficacy

Scale: The ability to quickly deploy without disruption, given the company's size, and to provide real-time visibility and results

Confidence in the capability of the technology and people

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: **We stop breaches.**

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**