CASE STUDY

Industry

HEALTHCARE

Falcon Host **Deployment**

750 ENDPOINTS

Key **Benefits**

- Increased security and protection against known and unknown threats
- End-to-end visibility across their environment
- "Force multiplier" capability provided by Falcon Overwatch 24/7 proactive adversary hunting activities

Services Used

- Falcon Host
- Falcon Overwatch

Summary

This rapidly growing managed healthcare provider was concerned about its ability to defend against advanced targeted attacks. The company was looking to leapfrog the traditional layered approach and find two solutions to assist with advanced protection: network and endpoint. They turned to CrowdStrike's next-generation endpoint solution -- Falcon Host -- to provide them with protection against sophisticated targeted attacks, along with visibility into what and who was targeting their environment.

The **Challenge**

The customer had undertaken a significant upgrade and refresh of their infrastructure. They had focused on standardizing and updating their security stack and regarded this as an imperative, given the sector they operate in.

They had focused on a standard layered security approach, and while the current security stack was effective if the attacker was "noisy," they were concerned about more sophisticated and stealthy attackers and techniques. In addition, they wanted more prevention and detection capability with respect to advanced targeted attacks.

They embarked upon a Proof of Value (POV) project to evaluate Falcon Host. The project quickly confirmed their suspicions regarding unknown malware and attacks currently targeting their environment. Although the organization was experiencing rapid growth, it was not large enough to resource and staff a 24/7 Security Operations Center. Lacking a fully staffed SOC, they were unable to realize their goal of proactively hunting for adversary activity, as opposed to always feeling they were "on the treadmill" of reactively remediating.

CASE STUDY

The Solution

Falcon Host, Falcon Overwatch

The Results

The customer reported that Falcon Host immediately detected two previously unknown pieces of malware that were active in their environment, having evaded their existing industry-standard antivirus tools. Falcon also discovered a targeted phishing attack directed against a number of key C-Level executives.

Proactive hunting by the Falcon Overwatch team has been instrumental in spotting adversarial activity in the environment, such as the use of compromised credentials, allowing the customer to quickly respond by disabling user access and removing compromised endpoints from the environment within 15 minutes of being alerted.

The organization realized its goal of achieving significantly enhanced and expanded visibility into what was happening on their endpoints, and oversight across the kill chain. They are further empowered by the detailed visibility provided by Falcon Host's process explorer capabilities. Additionally, the prioritization of alerts helps them optimize the use of their finite security resources to respond to threats more efficiently and effectively.

CROWDSTRIKE

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