CASE STUDY

Industry

MANUFACTURING

Falcon Host Deployment

50,000 MAC OS AND WINDOWS ENDPOINTS

Key Benefits

- Improved endpoint visibility, providing fast and efficient access to real-time and historical information across a complex global operating environment
- The ability for Levels 1, 2 and 3 IR teams to streamline and improve their automation and orchestration processes
- Enhanced prevention, both for malware-based threats and importantly, sophisticated malware-free attacks that had become a growing concern
- The ability to provide effective endpoint protection across machines running Windows and MacOS, all via a single unified solution

Summary

This multinational consumer manufacturing organization wanted more visibility into possible threats, including malware-free attacks that their existing antivirus and other tools could not see or prevent. The security team also wanted a solution that would enhance efficiency and coordination between their security operations center (SOC) and incident response (IR) investigators. The challenge they faced was to respond faster and with greater efficacy, to better secure their global environment. It was also important to them to have a single, integrated solution and platform that could orchestrate triage and remediation efforts across their Levels 1, 2 and 3 investigation teams.

The Challenge

Globally dispersed, with tens of thousands of total endpoints, the organization was relying on multiple "point" products to defend its global environment. For example, the team depended on separate tools for a range of security functions, such as detection, prevention and remediation, as well as the ability to contain infected machines and take action remotely.

Operating with multiple, limited-function solutions was inherently ineffective and cumbersome. They determined they would be better served by adopting a single, unified solution that could truly span the entire prevention, detection, response and investigation spectrum, allowing their support and IR teams to coordinate their efforts using one platform.

CASE STUDY

Services Used

- Falcon Prevent
- Falcon Insight
- Falcon Discover
- Falcon Intelligence
- Falcon OverWatch
- CrowdStrike Services

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 Solution

As an existing customer of CrowdStrike's Falcon Intelligence service, it was an easy decision for them to include the Falcon Platform in their evaluation process, which involved several possible endpoint protection solution providers. The evaluation proved to them that it was indeed possible to combine next-generation prevention and detection, together with powerful response and visibility capabilities, in a single solution. Falcon provided that one unified platform and holistic view of their environment that they were seeking, enabling the SOC and IR teams to protect the global organization in a consistent and coordinated fashion. Falcon's powerful real-time and historical analytics enabled the teams to improve both their reactive and proactive threat hunting capabilities. The CrowdStrike Services team contributed specific training on how best to leverage the capabilities of Falcon, while the Falcon OverWatch team offered further threat-hunting resources to augment the customer's efforts.

The Results

Adopting Falcon endpoint protection immediately resulted in improved workflow between SOC, IR and forensics teams, and more efficient and effective security processes across their global environment. Roll-out was fast and painless, allowing them to deploy globally in a controlled manner. With the implementation of the Falcon Platform, the teams quickly began to detect advanced attacks targeting their environment, some using sophisticated, malware-free techniques. The customer also reported improvements in their ability to prevent malware that their existing AV tool had missed, potentially allowing malicious files to enter their environment. Falcon was able to eliminate this "silent failure" by correctly identifying the suspicious files and preventing their execution.

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