CASE STUDY

Industry

OIL AND GAS

Falcon Host Deployment

MORE THAN 100,000 ENDPOINTS

Key Benefits

- Ability to detect and prevent "unknown unknowns" spanning the complete attack timeline
- Real-time, in-depth visibility into endpoints operating on or off the network
- Reduction in alert fatigue by filtering out "noise" and allowing the security team to focus on what is truly important and worthy of attention

Services Used

- Falcon Host
- Falcon Overwatch
- Falcon DNS
- Falcon Intelligence - Premium

Summary

The customer is a leading global oil and gas company. They operate a full stack of security products, but they wanted to have more robust endpoint protection. They also needed much better visibility into and prevention against sophisticated attacks across the full spectrum of the kill chain. Specifically, they wanted alerting on new unknown hashes propagating throughout their environment. As a result, the company turned to Falcon Host to provide the extensive prevention, detection and visibility they needed, especially for sophisticated unknown attacks.

The Challenge

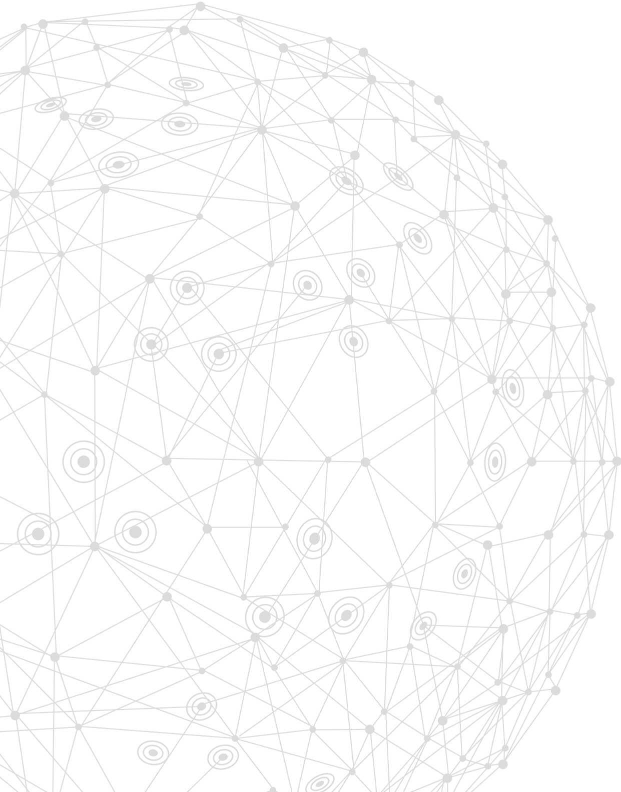
The customer lacked unhindered visibility into attacker activity on their endpoints. They needed the ability to see both signature- and non-signature-based attacks in real time, and the ability to contain those attacks. The customer also needed real-time alerting whenever new "unknown unknowns" were executing or propagating across their environment. Furthermore, they wanted the ability to prevent these events in real time. They had a well defined and resourced security operation that wanted to alleviate "alert fatigue" and focus on the most urgent threats targeting their environment.
In addition, they wanted to augment those resources with proactive threat hunting to detect possible threats at an earlier stage and prevent attacks from succeeding. Given the size and complexity of their global operations, the customer needed the ability to fine-tune and completely control prevention settings and capabilities on their endpoints.

Why CrowdStrike

- Better efficacy with respect to detection and prevention of unknown threats
- Development of specific functionality to address unknown hash propagation
- Ability to quickly deploy without disruption and, regardless of the organization's size, provide real-time visibility and results

The Solution

The customer looked at a variety of endpoint solutions, but only Falcon Host was able to provide real-time answers to the question, "What is running in my environment that is unknown?" Falcon Host was able to provide the customer with real-time alerts indicating when unknown threats were executing in or propagating across the enterprise, allowing the customer to prevent these unidentified threats from executing and compromising the environment. The ability to deploy quickly with no endpoint impact, no on-premise infrastructure and with full visibility across on- and off-network machines were all major factors in the customer's decision. Detecting adversary behaviors across the attack timeline also set Falcon apart from competing endpoint solutions. Finally, to further augment the their own internal security resources, they took advantage of the 24/7 proactive threat "hunting" capabilities provided by the Falcon Overwatch team.



The Results

CrowdStrike worked with the customer to ensure that they were alerted whenever new unknown hashes began to propagate in their environment. This was taken a step further with the ability to escalate alerts based on the rate of propagation.

nexus
technologies, inc.

ps-sec@nexustech.com.ph | nexustech.com.ph | (+632) 8555.2400 |
+63 9088869563 | +63 9178524653

CROWDSTRIKE

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